inmarsat

omnisec

Secure Video-Conferencing using Omnisec

Version 01

27th December 2009

Contents

1 Introduction

Satellite communications can be intercepted from almost anywhere. For this reason, protecting one's information against eavesdropping and intrusion is of paramount importance in such scenarios. Videoconferencing as an application, especially from remote or mobile locations connected via satellite, stands or falls on the ability to ensure that the communication via the Internet is entirely secure.

2 Benefits to BGAN Users

The Omnisec IP Encryptor Family products form a secure IP-based VPN, offering the following benefits to BGAN users:

- A security solution built on Swiss-made IP Encryptors and convenient-to-use portable Security Modules, which provides maximum protection for worldwide communications over Inmarsat BGAN and over the Internet
- Remote or mobile users – wherever in the world they may be – are able to participate in a totally secure videoconference
- Strong user authentication and proprietary 256-bit symmetric key encryption assures total confidentiality and guaranteed integrity of all data traffic from any IP-based application.

3 Typical Users

- Traveling government agents
- Mobile military and defense personnel
- Police and security forces
- Oil, gas, and mining organizations
- Traveling private decision-makers of banking, financial, and multinational corporations.Technical Details

3.1 Omnisec IP Encryptor Family Products

Omnisec's family of IP Encryptors together constitute the Omnisec IP-based VPN – a reliable Virtual Private Network solution offering the highest level of security.

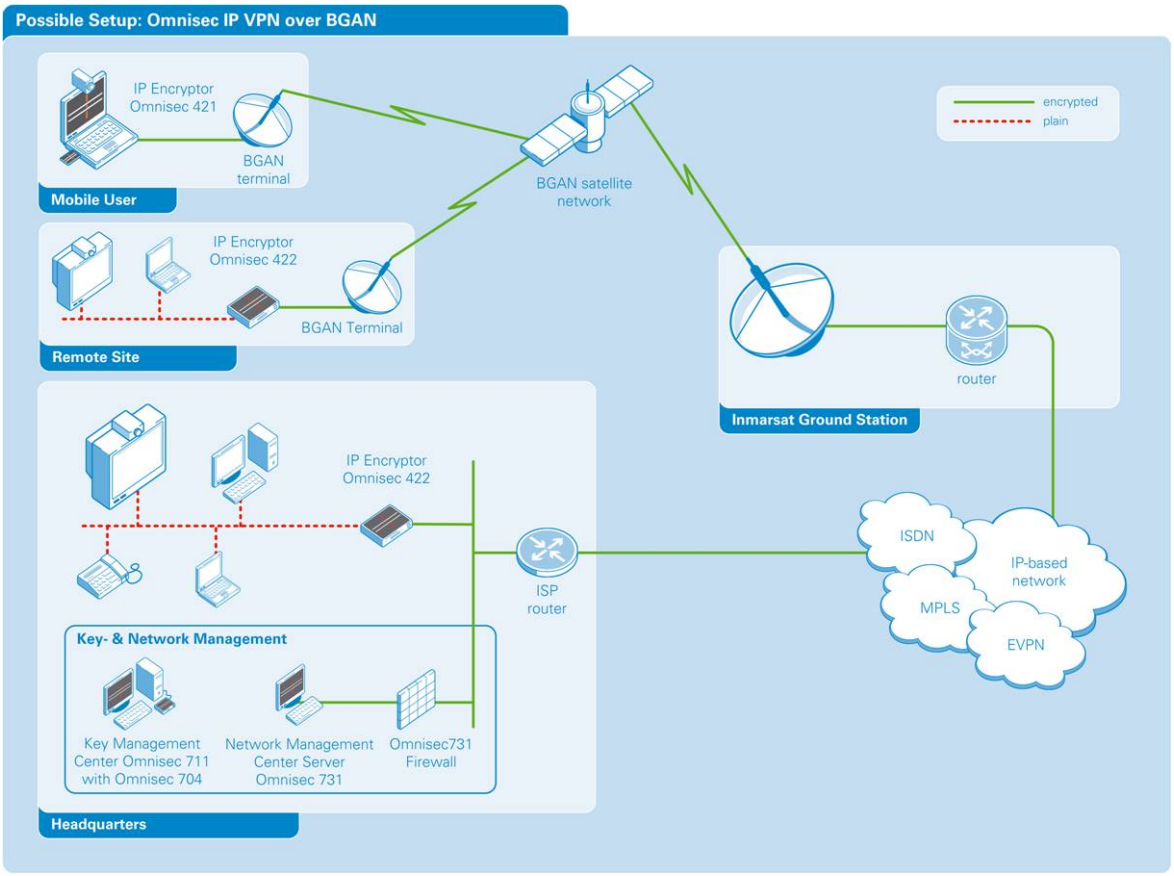
The Omnisec IP-based VPN establishes extremely secure site-to site communications, ideal for videoconferencing within a corporate IP-based network or via the Internet.

3.2 Videoconferencing Scenario Over BGAN

The sample application scenario illustrated below shows how a mobile user or a remote site can use BGAN's streaming IP service at 256 kbit/s over the BGAN network and then over two ISDN connections, MLPS, EVPN or the Internet to the corporate headquarters. The bandwidth of the leased line connection to headquarters needs to correspond to the numbers of BGAN users working with streaming IP. Such a scenario can be altered to be used for secure video conferencing or voice-over-IP.

A mobile user or remote site with a BGAN terminal makes an encrypted satellite connection to an Inmarsat Ground Station. From there the secure communication continues via the Internet to the corporate headquarters site, which is equipped with one of the other members of the IP Encryptor family, Omnisec 422 or Omnisec 423. A videoconferencing application establishes the secure decentralized meeting.

The headquarters typically also houses the Key Management Center (for generating the secret Master Keys and programming the Security Modules), and the firewall-protected Network Management Center (for configuring and monitoring all IP Encryptors in the network).



4 Omnicrypt™ Security Architecture

The multi-barrier Omnicrypt™ Security Architecture, OSA, raises IP encryption to the highest level of security. The strength of OSA is based among other things on the following fundamental security building blocks:

4.1 Key and Network Management

Secret bilateral Master Keys are generated either by means of the Built-in Key Equipment (BIKE) utility within the IP Encryptor Omnisec 422 or Omnisec 423 (for small networks), or by the Key Management Center application, Omnisec 711, in conjunction with the Security Module Programmer Omnisec 704 (for networks of any size). Efficient and flexible Network Management is assured by the Network Management Center, Omnisec 731, a decentralized client-server application.

All network traffic is encrypted using short-lived symmetric 256-bit Session Keys, derived from the secret Master Keys.

4.2 Security Modules

All the secret information required for encryption and decryption is safely contained in a convenient, portable Security Module (SM). The integrated microprocessor within the SM controls an electronic data store, which is protected both against read-out and tampering.

4.3 Cryptography

The 256-bit symmetric encryption algorithms developed by Omnisec offer unsurpassed levels of security.

5 Special BGAN Considerations

5.1 Quality of Service for Real-Time Applications

Real-time applications (voice, video, …) normally require a minimum bandwidth and work with small UDP packets. Inmarsat offers a guaranteed IP streaming service over BGAN from the end user terminal to the Internet POP (Point of Presence). In order to maintain the required guaranteed speed from the Inmarsat core network to the headquarters site, it is recommended to use leased-line services (ISDN, MPLS, …) from a worldwide operation provider. The required leased-line bandwidth depends on the concurrent use of the provided bandwidth by multiple BGAN mobile users.

Best results are achieved by limiting the application to work in 128 kbit/s streaming mode. Such a setup will work perfectly over a standard IP connection. QoS support requires a streaming 256 kbit/s connection.

5.2 MTU Setting

Consider changing your client computer's MTU size to a maximum of 1300 bytes in order to avoid network congestion within the satellite network. The reason to do so lies in the IP overhead added by the encryption process (up to 86 bytes per packet). Best performance is achieved when this setting is not only applied on the client end but also at the HQ site.

Note: The MTU Size is set on the Omnisec Virtual Adapter Property Dialog under Ethernet Settings.

When the MTU Size is set, any Path MTU Discovery features in the network devices can be turned off. This will stop the devices from checking the network for the best MTU size.

Note: In Windows, the Path MTU Discovery is turned off (0 = false) by altering the value of the registry key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\EnablePMTUDiscovery.

5.3 Handling of the Security Module

As soon as the Security Module is inserted into your computer's USB port, all IP connectivity is cut off. You first have to authenticate yourself to the Security Module by entering your PIN or passphrase at this prompt.

6 Required Equipment

Typical example:

- At least one IP Encryptor, Omnisec 422 or Omnisec 423, at the headquarters site (including one programmed Security Module per unit)
- One Omnisec 421 for the remote or mobile client computer (including a programmed Security Module)
- Key Management Center Omnisec 711 with SM Programmer Omnisec 704 (or BIKE utility for small networks) and two Network Security Modules (N-SMs)
- Network Management Center Omnisec 731, Omnisec 731 Firewall, two programmed Configuration Security Modules (C-SMs), and one programmed Personal Security Module (P-SM)
- BGAN terminal: Thrane & Thrane Explorer™ 500, or Explorer™ 700, or Hughes HNS 9201 with terminal adapter
- BGAN SIM card from the local Inmarsat service provider
- A professional videoconferencing solution, such as Tandberg, Polycom PVX, or VPoint_HD.

7 Further Details and Support

Inmarsat Contact:

E-mail: customer_care@inmarsat.com

Omnisec AG Contact:

E-mail: bgan@omnisec.ch

Web: www.omnisec.ch/421

Postal address: Rietstrasse 14
CH-8108 Dällikon
Switzerland

Phone: +41 44 847 67 11