Using IP VPN encryption solutions from Crypto AG over BGAN

Version 1

3 September 2009

inmarsat.com/bgan

Contents

1 Overview

IP-based applications make up an ever-increasing share of communications, offering a single layer of protocol for all the user group requirements. In addition, IP networks are increasingly low-cost, because many off-the-shelf components are available on both network and user levels.

There is, however, even greater potential for IP communications when combined with Inmarsat BGAN satellite links. BGAN terminals can be deployed on land, in vehicles (land mobile), on ships (maritime) and in aircrafts (aeronautical) – which means that flexible and portable IP communication solutions are available even in locations without traditional infrastructure.

However, over BGAN links encryption takes place 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. High security can only be guaranteed via the user's own, individual encryption solution for the whole connection (including terrestrial), and if possible end-to-end.

IP VPN Encryption Solutions from Crypto AG have proven highly reliable with public authorities and security organisations.

2 Typical user scenarios

IP VPN Encryption Solutions from Crypto AG are the preferred choice of public authorities, ministries, diplomatic services as well as security and defence organisations, due to the security concept based on hardware encryption and customer-specific algorithm. These solutions are used in "satellite terminal to satellite terminal" configurations, as well as "satellite terminal to HQ (or another station) via land earth station" configurations.

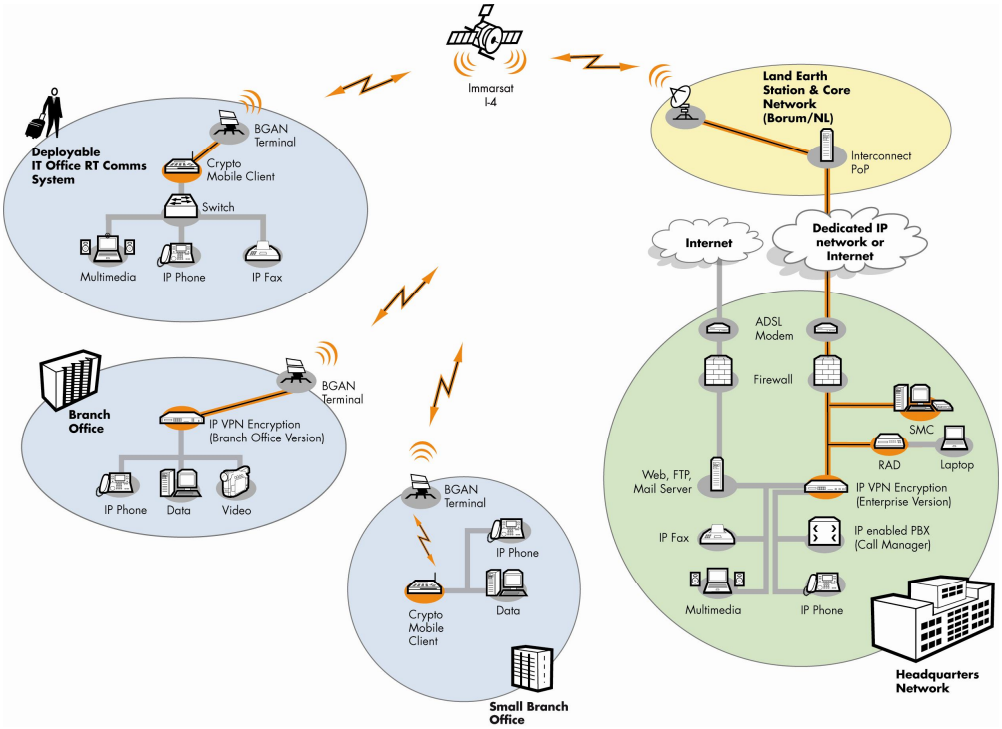
The solution establishes a secure virtual tunnel via the BGAN link through to the ICT infrastructure at headquarters, or to another mobile user. All transported applications such as data, VoIP, video, images, audio/video streaming and so on are protected and cannot be read or edited by unauthorised third parties. The authenticated user can get secure remote access to confidential data in their own organisation over a number of connections (IP network, Ethernet, WLAN, ADSL, UMTS network).

2.1 Applications

- Messaging, Email
- File Transfer (FTP)
- Client/Server applications
- Intranet
- VoIP (voice over IP) telephony
- FoIP (fax over IP)
- Videoconferencing

T he Crypto Mobile Client HC-7835 offers two additional security services:

- Secure local data storage
- File/message encryption (compatible with PC Security HC-6360)



The diagram above assumes access to the Internet via satellite. Locations may also have other means of Internet access and use the satellite as a backup solution. Stations using the Crypto Mobile Client can access the Internet over wireless (hotspot or via a GSM mobile phone).

2.2 Solutions

There are different models and types of BGAN terminals for different types o deployment. For all of these scenarios, there is a corresponding IP VPN encryption solution available from Crypto AG. Crypto AG offers also a range of compact, fully integrated solutions. They are based on the Crypto Mobile Client HC-7835 and the Thrane & Thrane EXPLORER 500 satellite terminal

3 Key features

- IP VPN Encryption from Crypto AG creates a Virtual Private Network (VPN) which has no contact with the transport network.
- IP data packets are encrypted and cannot be access by third parties, regardless of the application in use.
- IP VPN Encryption units can be integrated directly into the ICT infrastructure of a LAN.
- For individuals or small office users, there are desktop units and the Crypto Mobile Client, which can be installed directly between the end device (e.g. a laptop) and the network connection.
- Simple connectivity – no security knowledge is required, and encryption takes place automatically in the background.

- Centralised administration via the optional Security Management Centre SMC-1100 in offline or online mode.
- Fully scalable IP VPN product family comprises a suitable model for any scenario. The Crypto Mobile Client HC-7835, for example, is for use on the move, and can easily be combined with a BGAN satellite terminal. Using a Hughes 9201 or Thrane & Thrane EXPLORER 700 BGAN terminals offers a comfortable wireless (WLAN) to them.

4 Product range

This section describes the IP VPN encryption products available from Crypto AG.

- For headquarters we recommend the IP VPN Encryption Enterprise Version HC-7825
- For smaller offices with BGAN access, we recommend the Desktop Version HC-7805
- For mobile applications, we recommend the Crypto Mobile Client HC-7835.
- For military requirements, we recommend the MultiCom Radio Encryption HC-2650-200 IP.

4.1 Common features

Security Management

- Manual key input via user interface.
- Copy/backup of key and installation data by Security Data Carrier (SDC).
- Offline management by Security Management Centre and Security Data Carrier.
- Online management by Security Management Centre (SMC).

Access protection

- Tamper-proof design.
- Password protection user level specific.
- Block/unblock function.
- Emergency clear.

User interfaces

- Keypad
- 2 lines of LCD with backlight
- Status LEDs
- Browser-based user interface
- Built-in smart card reader for reading/writing key and setup data
- Diagnostic user interface

Management

- Security Management Centre (SMC)
- Remote Access Device (RAD) to remotely manage IT parameters
- Out-of-band management via ethernet
- Local management via keypad and display
- or via web-based user interface

- SNMPv1 (to be used by a network management tool)
- Standard MIB II

Control interface

Serial RS-232 RJ45 (diagnostics)

Quality system

ISO 9001:2000

Conformity

CE (European conformity)

Note: Please refer to the individual product data sheet for all details (especially the cryptographic data)

4.2 IP VPN Encryption HC-7805

This portable desktop IP VPN encryption unit can easily be connected by cable between the terminal and the network connection, with plug-and-play start-up. All applications based on the IP protocol, such as IP telephony, data or video, are protected. It offers a high transmission speed (10 Mbps) and supports all standard access technologies. So you can use it virtually anywhere and independent of the technology.

Category	Details
Housing	Office desktop version Power supply AC input 230 Vac nominal (100...240 Vac/50/60 Hz) Maximum power consumption 6 W
Dimensions	220 x 205 x 44 mm
Weight	1.5 kg

Environmental	Operating temperature: 0 ºC...+50 °C Storage temperature: -25 ºC...+70 °C Humidity: 5 %...95 %, non-condensing
Line interfaces	IEEE 802 Ethernet/RJ45: - Home 10BASE-T/100BASE-TX DHCP server RIP-II - World 10BASE-T DHCP client NAT support QoS: TOS/DSCP forwarding

4.3 IP VPN Encryption HC-7825

This powerful IP VPN Encryption unit (20/100 Mbps) is designed for direct integration into your IT infrastructure. It transforms your communication nentwork intoa secure Virtual Private Network, regardless of which nationally or internationally accessible LAN/WAN you use. The Security Architecture enables simple creation of crypto groups in star, mesh or mixed network topologies.

Category	Details
Housing	19” rack mounting - 1 unit high
Power supply	Dual power supply unit (hot-pluggable) DC 24 V ± 25 % DC 48 V ± 25 % AC input 230 Vac nominal (100...240 Vac/50...60 Hz) Maximum power consumption 40 W
Dimensions	444 x 260 x 44 mm
Weight	4.2 kg
Environmental	Operating temperature: 0 ºC...+50 °C Storage temperature: -25 ºC...+70 °C Humidity: 5 %...95 %, non-condensing

Network interfaces	IEEE 802 Ethernet/RJ45: - Home 10BASE-T/100BASE-TX DHCP server RIP-II - World 10BASE-T DHCP client NAT support QoS: TOS/DSCP forwarding

4.4 Crypto Mobile Client HC-7835

This small, portable multi-application, high-performance unit has several application options, including IP VPN for secure remote acces via public IP networks (e.g. the Internet), message/file-encryption for sending and receiving encrypted mails, secure data storage for transport of confidential data, and “thin client“ functionality for processing ultra-sensitive data on a laptop or PC.

If no satellite link is available, the Crypto Mobile Client can connect to the Internet via a Hotspot (WLAN), a UMTS Router (Ethernet) or via the GSM network (using a GSM mobile phone and Bluetooth) in order to communicate with the ICT infrastructure at headquarters

Category	Details
Housing	Small mobile unit
Power supply	Via USB (from laptop/PC) Or via power socket: 6…18VDC, max. 3W (Optional external power supply 100...240 Vac/50/60 Hz)
Dimensions	116 x 70 x 25 mm
Weight	Approx. 0.3 kg
Environmental	Operating temperature: -5 °C...+50 °C Storage temperature: -25 °C...+70 °C

Line interfaces	Home: Ethernet/RJ45, IEEE 802.3, 10BASE-T/100BASE-TX DHCP server RIP-II World: Ethernet / RJ45, IEEE 802.3, 10BASE-T WLAN, IEEE 802.11 b/g (optional) Bluetooth version 2.0 (optional) DHCP client NAT support QoS: TOS / DSCP forwarding
USB Memory	USB Memory (4GB) with write protection, possible to boot the notebook with an operating system (thin client
Optional features	Secure local data Mountable encrypted memory drive on the HC-7835 Email and file encryption Encryption service for email and file encryption File and email encryption application for PC's

4.5 MultiCom Radio Encryption HC-2650 - 200 IP

This universal, compatible encryption platform can also be used as an IP VPN encryption device. For IP-based military networks, the HC-2650 secures IP traffic with the IP VPN 7800 application. This application is fully compatible with the other IP VPN products from Crypto AG, which allows the set-up of mixed networks with ruggedised HC-2650 and the IP VPN 7800 family.

Category	Details
Housing	Heavy-duty, sealed and water-proof die-cast Aluminium
Power supply/ consumption	9 - 32 VDC protected against wrong polarity 88 - 264 VAC, 47 … 400 Hz, with AFS 2650 or PSM-3600 Max. 4.3 W LCD backlight: + 1.7 W LCD heating: + 5.5 W

Dimensions	182 x 209.5 x 44 mm W/D/H 198 x 221.5 x 56 mm W/D/H (incl. rubber shock absorbers)
Weight	1.6 kg (1.8 kg incl. shock absorbers)
Environmental	(according to MIL-STD-810F) Operating temperature: -40 to +70 °C Humidity: +60 °C/95 % RH Vibration: random, 10 to 500 Hz, 2.18 g rms; (wheeled vehicles, Annex C)
Line interface	- Home 10BASE-T DHCP server RIP-II - World 10BASE-T DHCP client NAT support, QoS: TOS/DSCP forwarding

4.6 Deployable SAT-Encryption all-in-one-case

Crypto AG has created a family of deployable systems for BGAN, housed in portable cases, completely equipped with encryption unit (e.g. Mobile Client HC-7835), power supply etc. . The built-in UPS battery provides approx. 3 hours of power autonomy from an external power supply. Depending on the version, they can contain:

- VoIP telephone,
- Netbook,
- Fax solution
- Printer
- Scanner.

The terminal can not only be used over BGAN satellites but also via the Internet though hotspots or Internet connections in hotels for example. The system can also connect to the Internet via a GSM/UMTS network with UMTS router or GSM mobile phone.

A Deployable Secure Satellite System is just like a mobile office that can connect to the headquarters in many different ways and almost anywhere.

5 Setting up

5.1 Setting up the IP VPN unit

The IP VPN unit is installed between the satellite terminal and the application terminal (PC/laptop, VoIP Phone, IP fax, etc.) via an Ethernet interface. Note the following:

- When using the Crypto Mobile Client HC-7835 and a BGAN terminal with WLAN interface, you can use a wireless connection.
- If a PC/laptop is used as the application terminal, the satellite terminal can be operated and configured via Inmarsat LaunchPad. Launch Pad or a browser can “view” the satellite terminal via a secure plain connection through the IP VPN unit. During this connection, the VPN tunnel is not active for security reasons (depending on the selected type of plain connection). This plain connection feature is available on HC7805, HC-7805 or HC-2650 VPN.
- In a remote access configuration the partner IP VPN encryption unit is located in the headquarters ICT infrastructure. Usually the HC-7825 is located behind the Internet access and a firewall.

The following settings and notes are BGAN-specific. All standard operational or security-relevant settings have to be made during installation and implementation. Crypto AG offers the relevant product training courses with course notes and detailed technical manuals.

Networking

IP VPN Encryption units from Crypto AG can cope with any address types used by the BGAN terminal: fixed private, fixed public, dynamic public and dynamic private. DHCP is supported and the BGAN terminal can be operated in router or modem mode (bridging). NAT/NAPT is no compatible with the IP VPN units, either. For reasons of Forced Routing in particular territories (for example, the USA or China) a fixed IP address is required. The IP VPN unit has a WORLD and a HOME port, which have to be in different networks.

Monitoring and logs

The IP VPN units support the SNMP protocol for status requests and monitoring (not for configuration), and so are visible for network management applications. Time servers are also supported. Traps and syslogs are sent on the corresponding Syslog server. All these features have to be enabled (for security reasons the default setting is “disabled”).

Client/client communication

It is possible to register default tunnel addresses in the Crypto Mobile Client unit, so that two mobile branches can communicate with each other via HQ. Alternatively, a registration server with a fixed IP address (running on a Message Scheduler or a Remote Access Device) somewhere in the network can enable direct client/client communication. However, this is more complex to handle and manage.

Keep Alive procedure

“Keep Alive” applications, such as VoIP telephony, register on a server periodically (and the server communicates with the client) to signal their availability and correct operation. The IP VPN units have a tunnel maintenance procedure which keeps the VPN tunnel active, or in case of failure re-establishes the connection. The relevant settings should not create too much payable traffic, and it should not take too long for application or the user to realise that the connection has dropped. With the Crypto Mobile Client (branch), a setting of 85 with the server in the HQ set to 900 seconds has proved to be a good compromise.

MTU

Due to the additional overhead caused by encryption, the MTU of the application components should be set as high as possible, in order to avoid network congestion in the satellite network. However, there should be a universal setting for the whole network, and hardware especially should be configured accordingly. HC-7835 supports MTU Discovery; its default value is 1422 Byte but this can be changed. The local components do not require any special configuration.

Firewall (FW) & ports

The encrypted data is sent over the network as ESP (portless) traffic. In case NAT is involved, UDP encapsulation (NAT traversal) is automatically applied. This uses Port 5500 by default (changeable) and must be enabled by the FW. In order to establish the VPN tunnel a key agreement takes place using UDP. The used port can be set and should be set to Port 1500 (Port 500 is the default setting but can cause problems with some routers; Port > 1024 prevents problems with NAT). The relevant port settings have to be the same with all tunnel partners. If a Remote Access Device (RAD) is used then port 1164 (by default) is used and the Management Centre SMC-1100 uses port 1163 by default. The FW (firewall) has to be configured in such a way that all these ports are open for UDP, as do the relevant ports for or the ESP protocol.

Real-time applications, QOS

If your network supports QoS/DiffServ, this feature is not affected by our IP VPN solutions. The relevant TOS/DSCP information for network components is copied to the new IP header so that packets can be treated according to priority. You must use a streaming IP data connection over the satellite. The whole terrestrial portion of the network QoS/DiffServ must be supported, because this feature is only effective end-to-end. As Crypto AG's IP VPN products have Replay Protection with a sliding window (64 packets per VPN tunnel), it is important that the relevant network elements use prioritising of the packets (queuing) and do this in a "fair" manner so that delayed packets do not fall out of the window or are discarded.

Multicast

BGAN terminals and the ground network infrastructure do not support multicast services yet. Inmarsat is going to implement this service in the near future. IP VPN solutions from Crypto AG support multicast in the newest release. It is very important to carefully investigate the exact operation of multicast in order to clarify the compatibility and finally to implement the security in an appropriate way. Typical scenarios are video broadcasting, video conferencing or other streaming services.

TCP Accelerators

There is also a free software solution from Inmarsat, consisting of a software client (accelerates traffic to HQ) and a server (accelerates traffic to client). Inmarsat's software client and the PEP Enterprise Accelerator are compatible with Crypto's IP VPN Encryption. Other TCP accelerator solutions can be tested by Crypto AG on request.

TCP Windows Size & Send Buffer

TCP window size has an effect on transfer efficiency and final throughput. This parameter can be set in the operating system (using Windows registry editor); the long round trip delays on satellite links require a large windows size for TCP over satellite. Some specific applications (e.g. a TCP accelerator proxy which uses special tricks to work around the OS) sometimes also allow you to let set this parameter, however normally the OS setting overrides the application setting.

Plain connection

When a Crypto AG IP VPN unit (in particular, HC-7805, HC-7835 and HC-2650 VPN) is connected to a BGAN terminal, you must enable the parameter “Plain Connection”, and set it to “unrestricted” mode. This temporarily (timeout can be set) enables secure access through the encryption unit using the Launch Pad to operate and control the BGAN terminal. This Plain Connection operating mode enables the BGAN terminal to be operated and configured using BGAN LaunchPad, and allows to login to Hotspots.

IP address

The IP VPN unit can use a public or fixed IP address. Crypto AGs IP VPN solutions can cope with NAT.

5.2 Setting up the BGAN terminal

There are no special settings required on the BGAN terminal for use with Crypto AGs IP VPN units. Note the following:

Header Compression

Crypto AGs IP VPN solution is compatible with the IP header compression supported by the BGAN terminals. However, we recommend that you only use header compression on good quality connections, as header compression increases traffic and so reduces efficiency on bad connection. To improve throughput, use TCP Accelerator.

IP Address

The IP VPN unit can use a public or fixed IP address.

5.3 Setup of applications

Generally, we recommend that you configure all applications so that the data volume or the IP overhead are kept as low as possible. This is important especially using the Shared IP, as they directly add to the running costs..

Some hints influencing the data volume and costs

- “Keep Alive” procedures to maintain VPN tunnels or virtuell connections of real time applications
  Enlarge the periode to an extend which still hit the target keep the channels alive
- FAX over IP
  Use fax with T.38 instead of G.711 in “Path Trough” mode (or ax over email T.37)
- VoIP
  Use efficient modern voice coder (rather G.729 instead of G.711) and set where possible to 30ms or bigger voice packet instead of 20ms
- Video
  Use efficient video solutions which operate reasonably with 128kbps or less.
  Use video clips having a resolution of 640x480 or even 320x240 pixel and rather a 4:3 then a 16:9 image format.
  Use rather the file format FLV (flash video) and MPEG1 (Moving Pictures Expert Group) then AVI or WMV (Microsoft Media Video).
- FTP
  Enlarge the send buffer size to 3268

6 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