inmarsat
The mobile satellite company™

HAGELIN-CRYPTOS
CRYPTO AG

Using the Crypto AG Voice Encryption system over BGAN

Voice Over IP (VOIP) Encryption – using Wi-Fi.

V6

Whilst the above information has been prepared by Inmarsat in good faith, and all reasonable efforts have been made to ensure its accuracy, Inmarsat makes no warranty or representation as to the accuracy, completeness or fitness for purpose or use of the information. Inmarsat shall not be liable for any loss or damage of any kind, including

Revision history table if required.

Document Issue	Date	Stratos Owner	Notes
V5	05/09/2012	P.Fry	

Contents

1. The Crypto AG Voice Encryption System overview

With Crypto AG's SD-card sized encryption unit "Crypto Mobile HC-9100" and the corresponding Security Application HA-2400, many of the commercially available Nokia handsets can be turned into high grade voice cryptology handsets.

This alone is a unique application, but adding the capability to use these crypto enabled Nokia handsets over a WiFi enabled BGAN as an access point, permits these handsets to be used where no GSM, GPRS/UMTS terrestrial service is available.

When used with BGAN, the Wi-Fi capable Nokia handsets are able to extend their reach of operation away from terrestrial GSM/GPRS/UMTS nodes by using the BGAN's IP bearer as an access bearer instead.

1.1 Basic Network Topology

The following network topology shows the situation when a satellite network is used. This is the case mainly if no terrestrial network as a cellular UMTS/GPRS/EDGE networks or Wi-Fi hot spot are available or can't be used for any reason.

Any BGAN terminal can be used (standard, vehicular, Fleet broadband and Swift broadband), however the terminals with an integrated Wi-Fi interface fit the solution best. (for others an external Wi-Fi router has to be used).

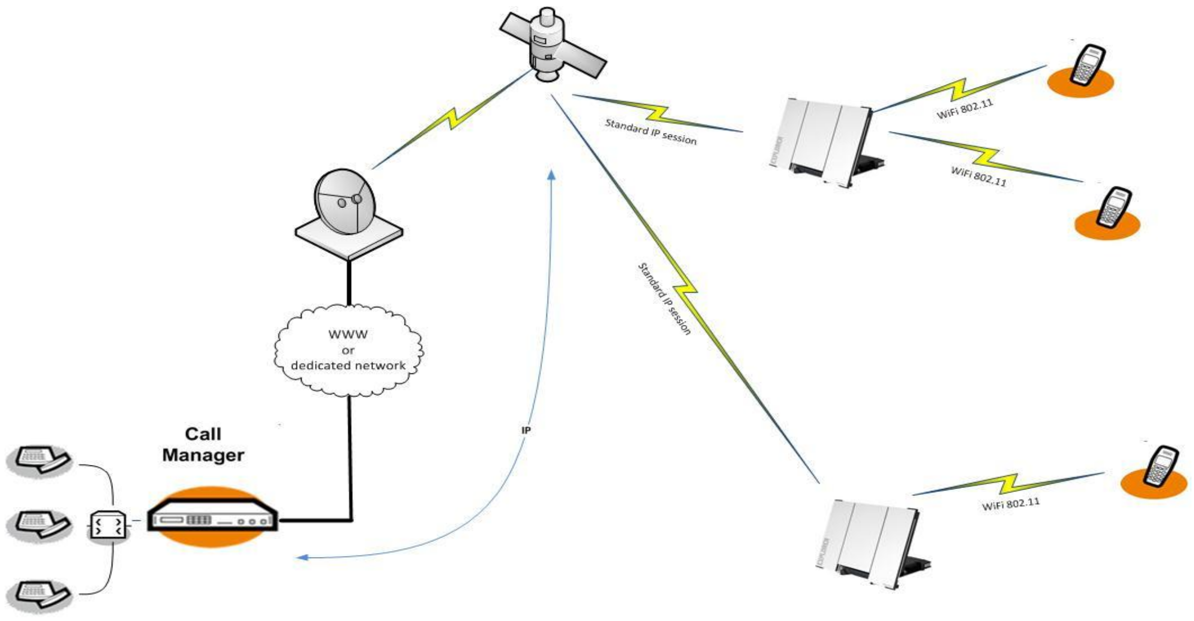


Figure 1- Basic Wi-Fi SIP topology

1.2 The Crypto Call Manager- the HA-2100 based at the HQ

As can be seen from Figure-1, a centrally operated (customer owned) Crypto Call Manager is required in the network.

The Crypto Call Manager consists of the Crypto Desktop HC-9300 encryption unit running the Crypto Call Manager HA-2100 Security Application. This server basically performs two tasks. The first one is that it acts as the management platform. For operational users it provides them online updates of encryption keys and individual contact list updates reflecting the latest changes in the network. For new users the encryption units are issued with the Crypto Call Manager like mobile operators issue SIM cards.

The second and main task of the Crypto Call Manager is to act as secure VoIP PBX for the fixed and mobile users of this CLOSED User GROUP network.

An IP path is established from the mobile users through the HQ based HA-2100 Crypto Call Manager.

2. Features of the Crypto Mobile HC-9100

The Crypto AG's HC-9100 is a complete security processor embedded into a Micro SD card.

The 1 GB Flash memory is divided into a regular and un-protected partition of 900 MB and an encrypted – from the outside inaccessible – Crypto Data store which holds the security data and contact list associated with the user's community

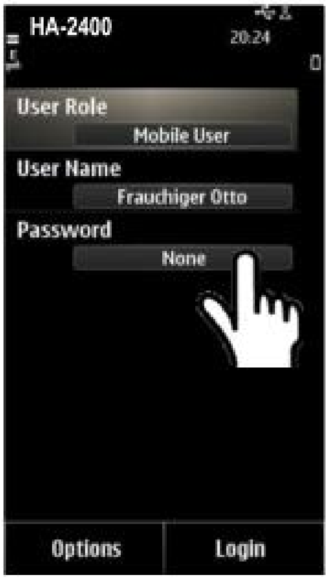
The security processor controls access to both memory partitions ensuring that no sensitive information ever can leave the security processor of the HC-9100.

2.1 The HA-2400 - the security application running on the Nokia handset.

In parallel to the Crypto Mobile HC-9100 a corresponding Security application called Voice Encryption Mobile HA-2400 has been developed by Crypto AG

The HA-2400 is the application that runs on selected Nokia smart phones. It provides a GUI (Graphical User Interface) that combines all the tasks required for the functioning of such a system such as:

- Placing and answering secure calls including handling of various audio devices, connection establishment and encrypting / decrypting voice data.
- Establishing and maintaining the packet data connection to the Crypto Call Manager over EDGE / 3G / Wi-Fi Networks.
- Synchronizing local network data (contacts) and security data (keys) with the Crypto Call manager.
- Dealing with local security issues such as user login, checking and monitoring integrity of the relevant software (HA-2400, Nokia Libraries) and auto-start to detect / prevent the installation of malware, emergency clear etc.



User Role: Mobile User

User Name: Frauchiger Otto

Password: None

3. HC-9100 Cryptography & Security

As part of the unique Crypto Security Architecture, encryption is performed by hardware in the security processor integrated in the micro SD card. The same processor controls and protects the built-in flash memory.

The Crypto Mobile HC-9100 can be installed in several high-end Nokia smart phones using the existing memory card slot and therefore remains invisible to others.

To utilise the HC-9100's high security features in the mobile phone Crypto AG specially designed the Security Application HA-2400 Voice Encryption Mobile. Together they protect voice communication reliably and at the highest level.

Should the mobile phone end up in the wrong hands by accident or theft, the data on the card remains inaccessible. All security information is stored encrypted in a tamper resistant area.
The internal memory is password protected.

The card provides top security not only for voice communication but also for the content of the flash memory.

3.1 Algorithm & Keys

3.1.1 Algorithm

- Customer specific high security cipher algorithm HCA-820.
- Customer managed profiling of algorithm with variety > 10^{506}
- Built-in high quality true random generator.

3.1.2 Keys

- Key length 128 bit or 256 bit:
  - Master Communication Keys.
  - Communication Keys.
- Tamper-proof key storage inside the Crypto Mobile HC-9100.
- Key Change
  - Master Communication Keys according to their Key Activation Time.
  - Communication Keys are randomly generated for each call.

3.2 Tamper Proof Design

- Identity based authentication
- Factory reset
- Emergency clear zeroises out the Master communications keys.
- Tamper evident security processor.
- Tamper proof storage inside the HC-9100.

4. Typical Users.

- Government agencies, Military and defence organizations
- Police and Security Forces
- Banks and Finance institutions
- NGOs, Aid agencies & First Responders

5. Benefits to the BGAN User.

- Ability to use High grade voice cryptology via Standard Nokia mobile "off the shelf" handsets.
- The same Nokia handset can be used on terrestrial cellular UMTS/GPRS/EDGE networks, Wi-Fi hot spots / office Access Points, and of course, BGAN.
- Using IP data paths, the network between the BGAN POP and the HQ server can be secured using lease line topology, VPN's or simply using the internet as a transport route.
- The telephony functionality is based on SIP (Session Initiation Protocol) but the traffic is encapsulated (by default, can be switched off) in order to avoid a simple blocking of unwanted telephony traffic by a network data service provider.
- Mobile to Mobile and Mobile to/from terrestrial calling capability.
- Voice crypto sessions supported whilst other applications such as office LAN data sessions are taking place- multiple bearer capability not tied to one application.
- Once the Nokia is attached to the BGAN via Wi-Fi and an IP PDP session is established on the BGAN, no more interaction is needed between the HC-9100 (Nokia handset) and BGAN simply select the contacts for secure calls.
- Cost to implement will be far reduced due multi bearer capability of the HC-9100 & HA-2400 applet vs. a solution that is tailored to one access type only (circuit switched. Serial, GSM or IP only).

6. Supported Nokia handsets

- Nokia C6-01
- Nokia C7-00
- Nokia N8
- Nokia 808 Pure View
- Nokia 603
- Nokia 700
- Nokia 701

6.1 Nokia Operating System

Symbian Anna or Symbian Belle operating systems.

7. Connecting the Nokia handset to BGAN via Wi-Fi

The Nokia handsets can operate over any IP enabled bearer such as UMTS, GPRS and via Wi-Fi access points such as hotels, offices and BGAN.

For connectivity to the BGAN terminals, Wi-Fi is used between the Nokia & BGAN.

The Hughes 9201, 9202, 9350, Thrane & Thrane Explorer 700 and the Add Value Safari COTM terminal all support Wi-Fi connectivity and act as excellent access points to the Nokia handsets.

For the purpose of this briefing, the Crypto AG mobile voice encryption platform has been tested with both the Hughes 9201 and Thrane & Thrane Explorer 700 acting as Wi-Fi access point, establishing Wi-Fi connectivity between the Nokia handset and any of the Wi-Fi enabled BGAN terminals will be similar in setup.

The smaller class of BGAN terminals can also support the Crypto AG Voice encryption system, but connectivity between the Nokia handsets and the BGAN here will be via an external Wi-Fi router/Access Point connected to the BGAN's Ethernet LAN port.

The configuration of external Wi-Fi routers/Access Points is outside of the scope of this Application note, but the concept of setting up the Nokia handsets and calling through the to the terrestrial server via the BGAN PDP IP session will ultimately be similar.

7.1 BGAN setup

The easiest connection can be realised using a BGAN terminal (UT) with an integrated Wi-Fi interface (e.g. HNS-9201/2 or the TT Explorer 700, etc.). If the UT has no built in Wi-Fi interface, an external WLAN router can be connected to the LAN interface of the UT.   Setting up of external Wi-Fi routers falls outside the scope of this guide, but the following BGAN scenario setups are similar to those steps performed setting up external wireless routers.

7.1.1 BGAN UT Wireless setting

Regardless of the UT, the first step is to setup the Wi-Fi access point of the BGAN to permit the Nokia handset to bond to the BGAN.

Decide on the Wi-Fi encryption, SSID details and if the BGAN broadcasts it's SSID, or restricts it.

The bonding of the Nokia handset to a BGAN via Wi-Fi is almost identical, so please refer to the specific BGAN terminal user guide for enabling and manipulating the Wi-Fi access point details and security parameters.

For best results, it is best that the BGAN is setup with its SSID broadcasting (so it can be found).

Before going through the Nokia handset Wi-Fi settings, ensure that the BGAN Wi-Fi Access point has been enabled and all the required settings have been noted (SSID, WEP/WAP/WPA etc).

Although the data (voice and protocol data) between the mobile phone and the Wi-Fi Access Point (AP) of the UT is encrypted, it's recommended to use the best algorithm of the Wi-Fi AP to avoid unauthorized access to the WLAN AP and thus the access to the Internet causing running costs.

7.1.2 IP Addressing issues

The Crypto Secure Voice Encryption system can cope with Network Address Translation (NAT) in the networks. Thus for the BGAN subscription there is no need to subscribe to a public IP address. A standard "Private IP Access" subscription is sufficient.

However, for the HQ and the call manager, the Internet access needs to be a fixed Static Public IP address. Also, it's recommend that a dedicated bandwidth for the Call Manager (with reserve about 100kbps per concurrent possible call) is allocated from the HQ ISP supplier.

7.2 Nokia handset Wi-Fi and the HA-2400 application

Some of the menus will be slightly different between the different versions of Nokia handset, but in essence:

From the main handset menu:

Settings > **Connectivity** > **settings** > **Network Destinations** > **Internet** and from the small options tab, > **New Access Point**.

Now, from this menu, based on what has previously been defined in the associated BGAN Wi-Fi settings, enter the BGAN Wi-Fi SSID and the relevant security settings associated with the Wi-Fi network between the BGAN and the Nokia handset.

Once the Access Point has defined, make sure it has priority one or all access points previously stored in the Nokia handset with a higher priority, are unavailable locally.

Ensure the Nokia handset is now attached to the BGAN Access Point by checking that the Wi-Fi signal strength in the Nokia handset reflects healthy status.

8. BGAN IP PDP control

With the BGAN terminal now connected via Wi-Fi to the Nokia, we need to ensure that an IP route has been established over the BGAN to allow the HC-9100 & HA-2400 services within the Nokia handset to establish a connection to the HQ based server.

BGAN's IP (PDP) session can be controlled a number of ways, from having an IP session automatically start at registration, Automatic Context Activation (ACA) based on LAN traffic through to user manual control via Launch pad. The choice is based on the users requirements and the BGAN terminal.

Hughes 9201, 9202 and the Thrane & Thrane Explorer 700, the BGAN terminals with built in Wi-Fi Access Point capability each control the IP (PDP) session in a slightly different manner.

A recommendation would be that the IP PDP session on the BGAN, regardless of manufacturer or version is controlled via ACA, Automatic Context Activation.

With ACA configured, once the BGAN terminal has registered, an IP PDP session will automatically be started because of the presence of the Nokia handset bound to the Wi-Fi Access Point.

The IP PDP session of the BGAN will then automatically be authenticated and an IP route from the Nokia and embedded HA-2400 security application will be available towards the HA-2100 Crypto Secure Call Manager at the HQ.

Manual control of an IP PDP session using the Inmarsat Launch pad, a terminal specific built in MMI/GUI or in the case of the Thrane & Thrrane e700, the use of the external buttons to “connect” a pre defined IP PDP session have all worked successfully with the Nokia handset and the associated Crypto AG Voice Encryption Solution.

- Please ensure that the Nokia handset has successfully been bound to the BGAN by checking that the Wi-Fi connection icon of the Nokia reflects successful attachment to the BGAN Access Point.

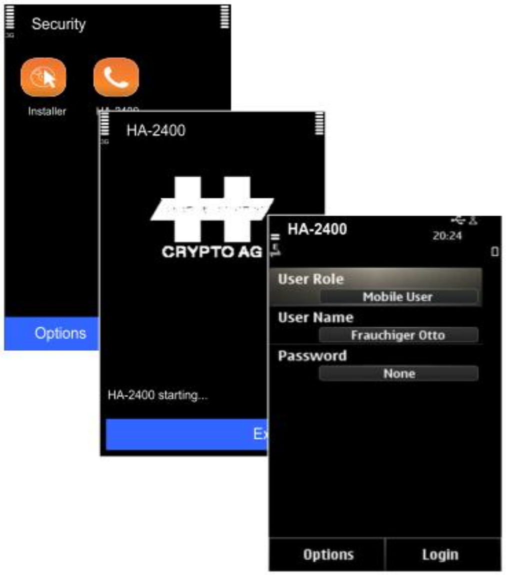
9. Making a crypto call via BGAN.

9.1 Logging into the Crypto HA-2100 Call Manager.

From the Nokia handset, once an IP route has been established (via BGAN), the HA-2400 security application can be started from the handset by tapping the Icon ☎

There are two roles within the HA-2400 security application, “Mobile Administrator” and “Mobile user”. Select the logon appropriate to the role and task assigned to you.

The HA-2400 security application will then automatically connect to the HA-2100 Secure Call Manager via the BGAN IP session. Once authenticated, the secure Contact list will be presented.



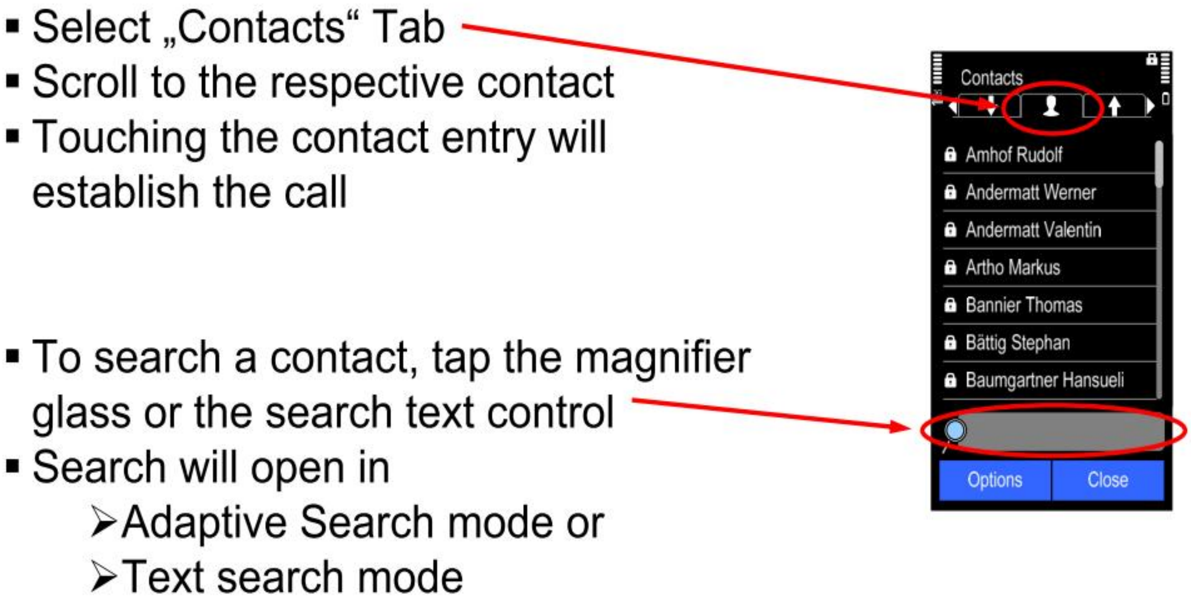
User Role: Mobile User
User Name: Frauchiger Otto
Password: None

9.2 Contact list

Once authenticated onto the HA-2100 Call Manager server, a padlock symbol will be presented at the top of the HA-2400 security application and the user will then be able to access the secure contact list.

This list is managed by the Network Administrator and additions/deletions of contacts can only be managed via the HA-2100 Secure Call Manager server.

9.2.1 Connecting to a member of the contact list



- Select „Contacts“ Tab
- Scroll to the respective contact
- Touching the contact entry will establish the call

- To search a contact, tap the magnifier glass or the search text control
- Search will open in
  - ➢Adaptive Search mode or
  - ➢Text search mode

Contacts

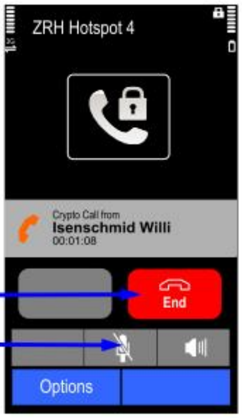
- Amhof Rudolf
- Andermatt Werner
- Andermatt Valentin
- Artho Markus
- Bannier Thomas
- Bättig Stephan
- Baumgartner Hansueli

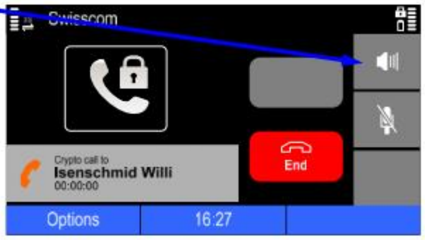
9.2.2 Secure call progression

- After selecting the user, the call dialog is displayed
- The icon ☎ indicates a Crypto Call*

Possibilities:

- End Call
- Microphone Mute
- Activate / deactivate LS



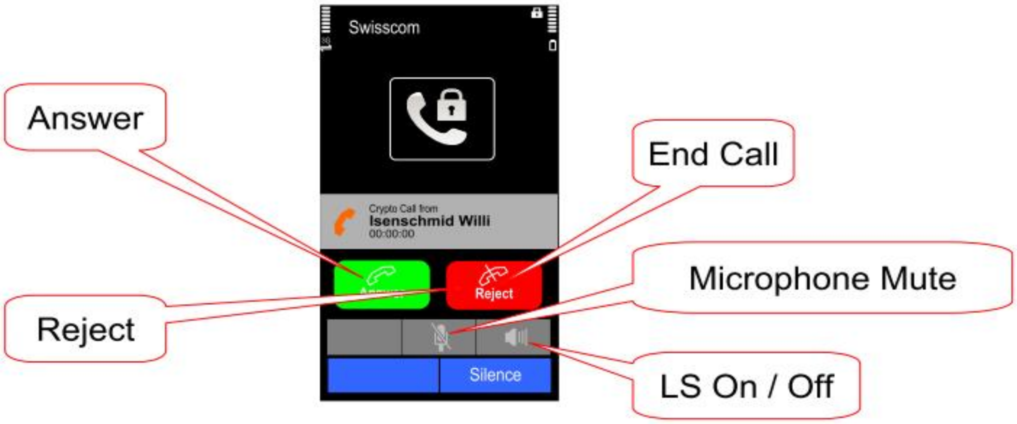


* This Icon can be customized to display a customer specific image

9.2.3 Incoming call

The HA-2400 User Interface is activated and the phone is ringing with the ringing tone as defined in the current profile:

Possibilities while ringing: **Possibilities during call:**

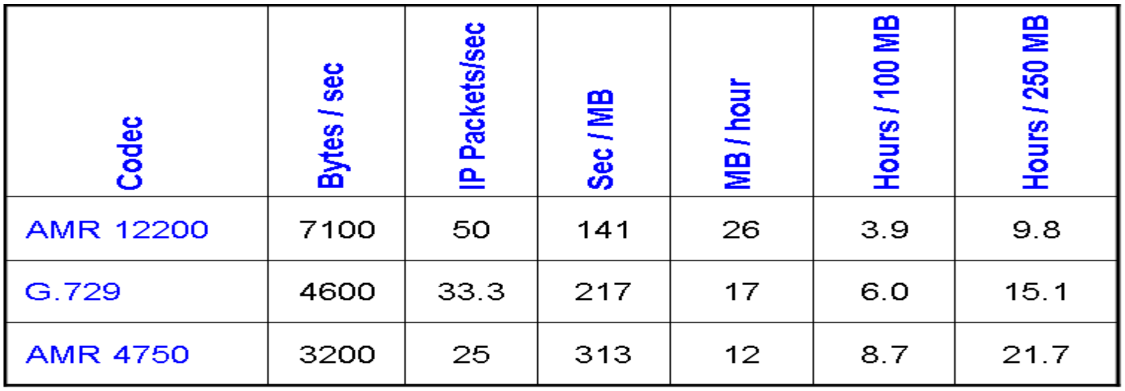


10. Data usage summary

10.1 Codec and Data Usage

The table below is based on estimations between a single Crypto node and the Crypto Call Manager, but doesn't include traffic related to the connection handler nor call establishment.

Figures are estimations of the payload sum for the Transmit and Receive paths of the call without activated silence suppression. If silence suppression is activated the reduction will be about 20-40% (parameter called " Use silent frames" On/Off).



Codec	Bytes / sec	IP Packets/sec	Sec / MB	MB / hour	Hours / 100 MB	Hours / 250 MB
AMR 12200	7100	50	141	26	3.9	9.8
G.729	4600	33.3	217	17	6.0	15.1
AMR 4750	3200	25	313	12	8.7	21.7

The used BGAN Standard IP service has a volume tariff and thus the codec selection has impact to the running costs. It's up to the user to make the desired compromise between voice quality and costs and to set the appropriate parameter.

Please note that where more than one user share a BGAN, terminal it's recommended to select the codec with the lowest possible bandwidth to increase the possibility to support more than one calls at the same time, within the limited bandwidth of a shared Standard IP BGAN channel.

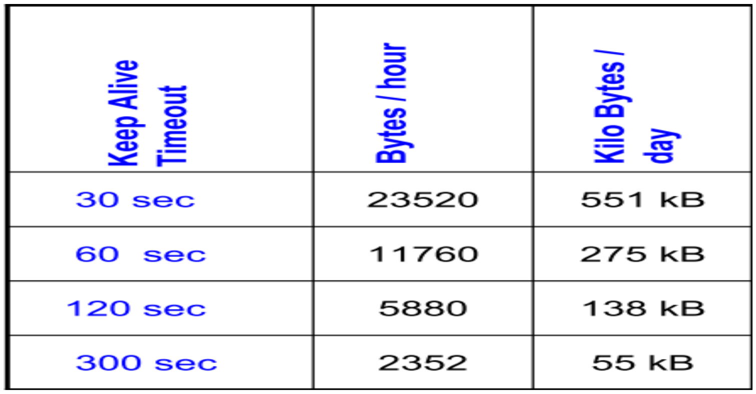
10.2 Keep alive sessions between the handset and the Call Manager

Keep alive traffic is required to maintain the connection between the HA-2400 application on the handset and the HA-2100 Crypto Call Manager at the HQ.

One keep alive consists of:

- 70 Byte keep alive request
- 66 Byte keep alive response
- 60 Byte TCP ACL (acknowledgement)

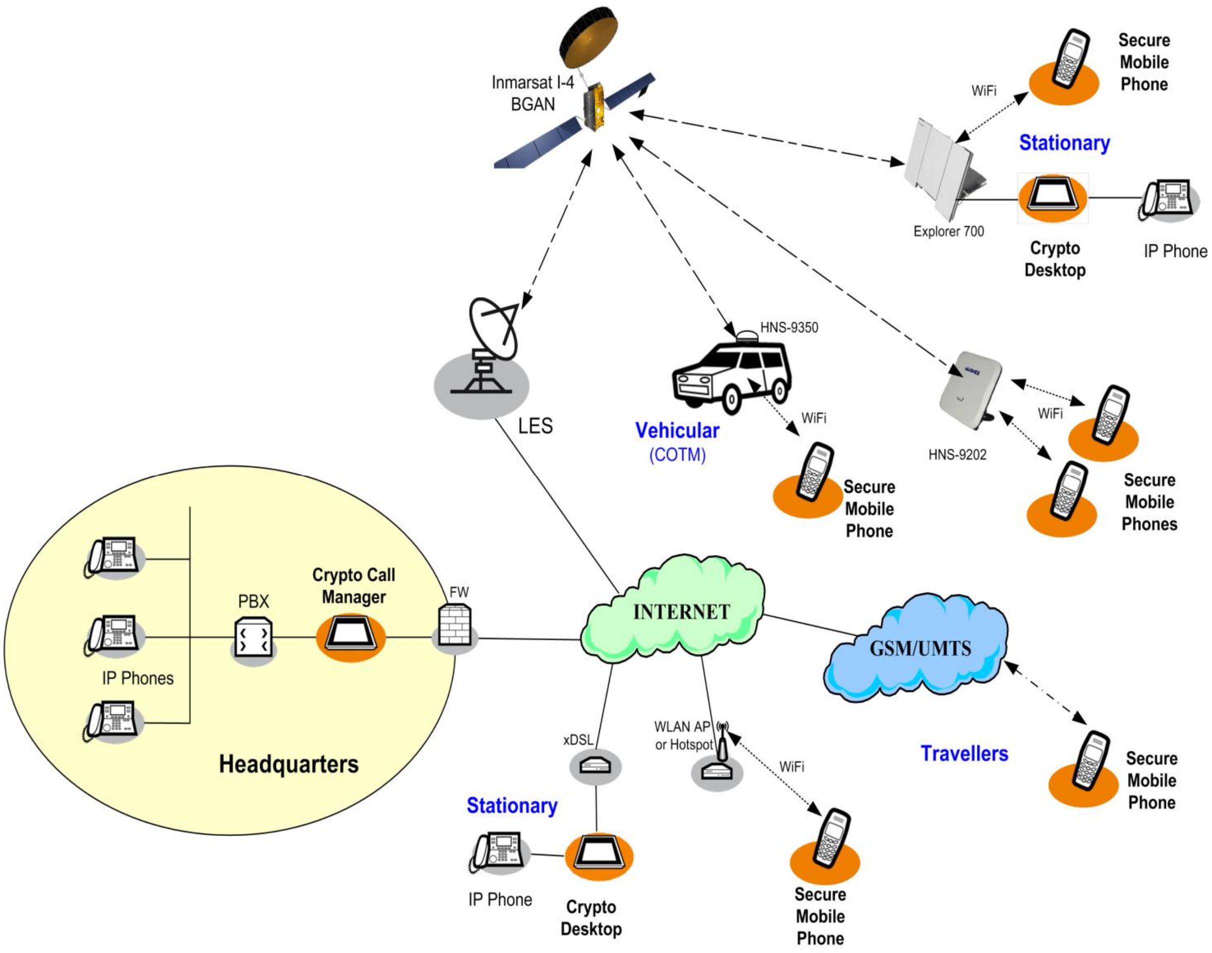
Total Bytes: **196** (includes the IP header and overhead).



Keep Alive Timeout	Bytes / hour	Kilo Bytes / day
30 sec	23520	551 kB
60 sec	11760	275 kB
120 sec	5880	138 kB
300 sec	2352	55 kB

11. Typical larger deployment network.

The following graphic shows a typical network scenario with several possibilities to access the channel to the call manager managing all the calls. The Internet, a cellular GSM/UMTS or the Inmarsat BGAN satellite network can be used to interconnect the users.



Thus the Secure Mobile Phone has a great connectivity, especially together with appropriate Inmarsat BGAN terminals. Almost wherever a user is located there is a possibility to make secure calls to any other user who are online and registered.

The Satcom hardware from Inmarsat gives independence from local terrestrial communication infrastructure which might be non-existent, not available / accessible, or be too poor in quality.

At the headquarters, users can also talk to any other user by using the Red Enclave Voice Gateway (Option) running on the Crypto Call Manager.

There are a number of products from Crypto AG that permit the integration of other voice devices such as analogue telephones (POTS (Plain Old Telephone)) as well as Nokia GSM smart phones

12. Further Details and Support

Inmarsat Contact

Email: customer_care@inmarsat.com

Crypto AG contact

Email: info@crypto.ch
Website: http://www.crypto.ch