inmarsat

Cellcrypt

Using Cellcrypt over BGAN

BlackBerry and Nokia

Voice Encryption

Version 1.0

08.10.2009

The mobile satellite company™

Contents

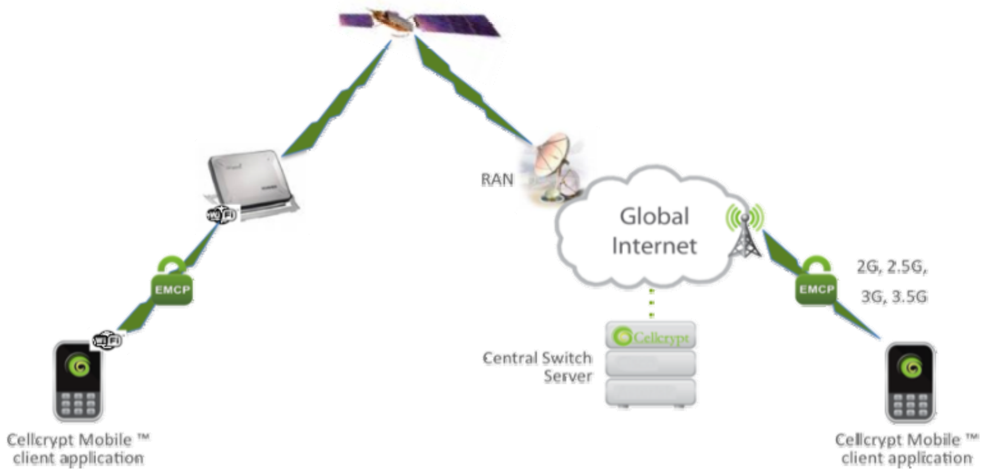
1 Overview

Cellcrypt enables standard smartphones to connect to BGAN terminals and make voice calls secured with government-level encryption.

Cellcrypt Mobile™ is an easy-to-use mobile software application that runs on standard mobile phones (RIM BlackBerry and Nokia Symbian S60) and uses the data (IP) network to deliver unparalleled voice quality, high strength security and low voice delay.

Because Cellcrypt Mobile runs on popular smartphones all the latest market-leading phone features are available and a single device is also used for making encrypted calls over cellular networks (GPRS /CDMA, 1xRTT and above) as well as BGAN terminals.

2 Network Topology


RAN
Global Internet
EMCP
EMCP
2G, 2.5G,
3G, 3.5G
Cellcrypt
Central Switch Server
Cellcrypt Mobile ™ client application
Cellcrypt Mobile ™ client application

3 Typical Users

- Government agencies
- Military and defence organizations
- Police and Security Forces
- Oil, Gas and Mining organizations
- Banks, Finance and multinational corporations
- Vessels and Maritime
- NGOs and Aid agencies

4 Key Features

Security

Strong end-to-end encryption between any two devices running Cellcrypt Mobile™ including 2048-bit RSA and Diffie Hellman (DH) for strong authentication and key exchange, and 256-bit AES wrapped in 256-bit RC4 for voice encryption

US Government FIPS 140-2 certification (in progress)

Smartphone & BGAN Support

WiFi®-enabled versions of RIM BlackBerry (Bold), Nokia Symbian S60 (N-series, E-series), and Windows Mobile smartphones

Supports any WiFi-enabled BGAN terminal (Land and Maritime)

Easy to use

Simple application: as easy to use as making a standard phone call

Integrates with device phonebook for single contact address book

Minimal configuration of BGAN terminal, only WiFi® access point setup

Low latency and unparalleled voice quality

Useable Beyond BGAN Terminals

Make standard cellular calls and use all smartphone features

Make encrypted calls on any IP-enabled network including cellular 2G (GPRS, EDGE, 1xRTT), 3G (UMTS, HSDPA, EV-DO) and standard WiFi®

Call between any combination of endpoints: BGAN, cellular, WiFi

5 Benefits to BGAN users

Cellcrypt Mobile offers the following benefits:

- No specialist equipment required to make encrypted voice calls – use popular off-the-shelf smartphones from leading cell phone manufacturers
- Use the same smartphone to make encrypted calls on Wi-Fi and cellular networks – use a single device with a single contact address book
- Uses the IP network to reduce the cost of voice calls
- Highly convenient allowing multiple devices to call simultaneously, all connected wirelessly with no specialist configuration of the BGAN terminal required

6 Security Architecture

6.1 CellCrypt Technology

Cellcrypt's advanced solution leads the industry in delivering multi-layered security to establish a high-performance encrypted voice call between trusted devices.

Cellcrypt utilises Encrypted Mobile Content Protocol (EMCP), a set of standards-based protocols for optimising delivery of encrypted real-time content between mobile phones over low-bandwidth wireless networks. Cellcrypt’s products are undergoing certification to FIPS 140-2 standard, approved by the US National Institute of Standards & Technology (NIST).

6.2 Cryptography & Random Number Generation

Public Cryptography
(RSA & DH, all 2048 bits)

RSA is used for authentication. The key pairs are generated on the phone during the installation and are unique to each phone. A private key is never shared. The Diffie-Hellman (DH) and RSA algorithms are used for key exchange. The session key is only valid for one phone call and securely destroyed after use.

Symmetric Cryptography
(AES & RC4 both 256 bits)

Both encryption algorithms are used at the same time. The data packet is first encrypted with AES and the crypto-data is then encrypted again with RC4, using the exchanged session key and are used in Counter Mode (CTR).

Hashing Algorithms
(SHA512, MD5)

Two industry standard hashing algorithms are used for increased integrity assurance.

Random Number Generation

A 2048 bit seed pool is generated during the installation and is periodically updated. The initial seed measures the fluctuation of the least significant bit of the microphone noise, the phone's internal random number pool and the timestamp. The pseudo-random function is implemented according to the IPSec specification defined in RFC-4306.

7 Setting up

7.1 Cellcrypt Configuration

This section describes how to setup Cellcrypt’s Mobile voice encryption application for use over Inmarsat’s BGAN terminals. Cellcyrpt’s Mobile application was tested over the EXPLORER 700 and the HNS 9201 terminals using the built-in Wi-Fi access points.

While the other BGAN terminals do not have built-in Wi-Fi access points, it is anticipated that the Cellcrypt Mobile application will work just as well via an external Wi-Fi access point. Simply connect the Wi-Fi access point and BGAN terminal to a standard router. This should provide the user the ability to use Cellcrypt’s Mobile application over other terminals. It is noted that some of the other terminals do not support some of the higher bandwidths, so call latency may be affected as the number of simultaneous calls increases.

Before you start

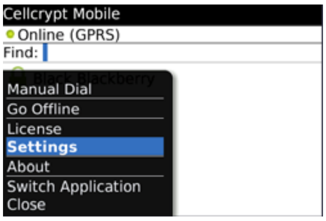
Ensure you install and license the appropriate Cellcrypt Mobile application on a Cellcrypt supported Smartphone and then simply connect the device to the BGAN terminal via Wi-Fi access. Please review your Smartphone's user manual on how to successfully configure and connect to Wi-Fi access points.

7.2 Configuring Cellcrypt Mobile Client for access to BGAN terminal

Configuring the Cellcrypt Mobile Client for access to Inmarsat's EXPLORER 700 or the HNS 9201, requires little to no interaction with the client software provided that you are using Cellcrypt's Central Switch. If you posses your own Cellcrypt Central Switch, then you will need to change the SIP Server Address and Server Port by following these basic instructions.

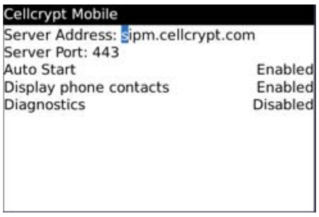
a. Launch the Cellcrypt application by clicking on the Cellcrypt Mobile icon:

b. Click the Blackberry button and on Nokia, please select Options | Tools | Settings:

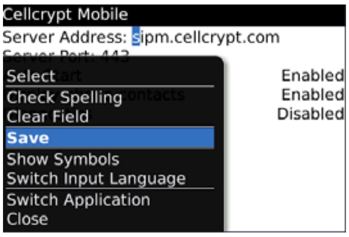


c. The change the Server Address and Server Port to your private Cellcrypt Central Switch. You may need to coordinate with your IT staff to get this information.

d. Select the Blackberry button again and then select the Save button and on Nokia, select the Back button:



Server Address: sipm.cellcrypt.com
Server Port: 443
Auto Start Enabled
Display phone contacts Enabled
Diagnostics Disabled



Server Address: sipm.cellcrypt.com
Enabled
Enabled
Disabled

e. Ensure you activate your BGAN Standard IP connection, connect your Smartphone via Wi-FI to the BGAN terminal, and click on the Cellcrypt Mobile icon via the Smartphone's user interface.

7.3 Making a Secure Call

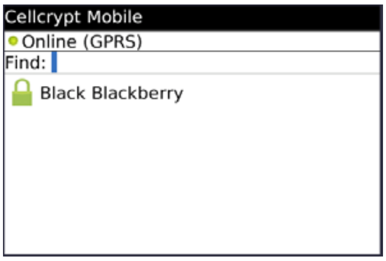
A secure call can be made in two different ways.

- Dial the contact manually
- Selecting an existing contact from the Cellcrypt address book.

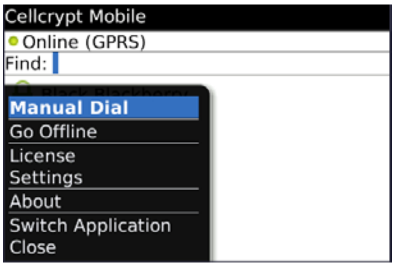
A secure calls recipient must also be online.

Dial the contact manually

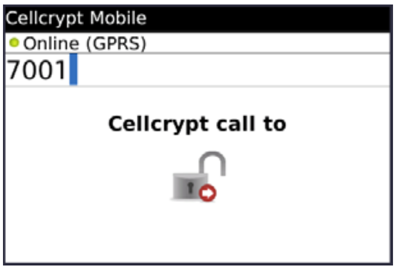
a. If you do not have the contact details already stored on the address book, the contact can dial the number manually. Open the Cellcrypt application and verify you are online:



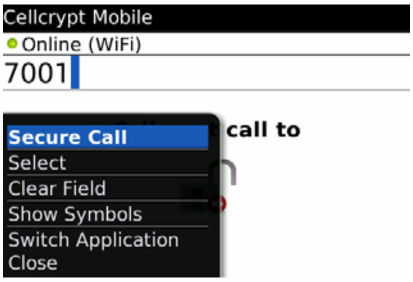
b. Click the BlackBerry ‘BB’ button and select Manual Dial and on Nokia, press the right button on the silver D-pad to get to the main Cellcrypt status screen then select the Options button and then Manual Dial:



c. Enter the known Phone Secure Number:

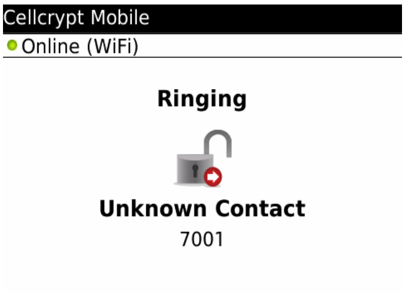


d. Click the BlackBerry ‘BB’ button again and Select ‘Secure Call’ and on Nokia, select the Secure Call button:



e. Cellcrypt application will now Secure a Channel to the dialled number, as it is the first time the two devices have called each other.

f. Once the channel has been secured between the two devices, the mobile originating call will ring the other device.



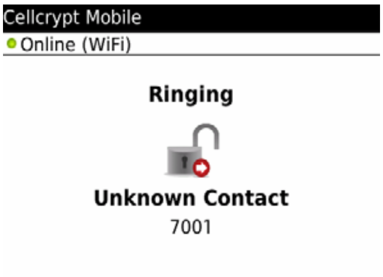
Cellcrypt Mobile
Online (WiFi)

Ringing

Unknown Contact
7001

g. The recipient of the call will be notified by the device a secure call is being received from an ‘Unknown Contact’:

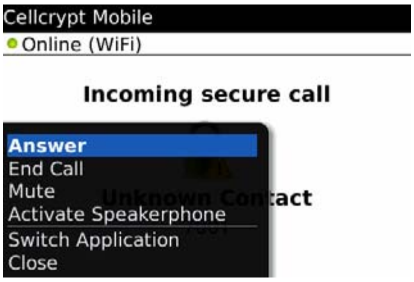
h. The recipient of the call will be notified an incoming secure call has been received and clicking the BlackBerry ‘BB’ button will give the user option to answer the call and on Nokia, select the green phone icon:



Cellcrypt Mobile
Online (WiFi)

Ringing

Unknown Contact
7001



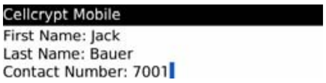
Cellcrypt Mobile
Online (WiFi)

Incoming secure call

i. Selecting ‘Answer’ on the device will connect the two users and they will be able to make a secure call.

j. To end the call, click the BlackBerry ‘BB’ button and select ‘End Call’ and on Nokia, select the Hang Up button or select the red phone icon.

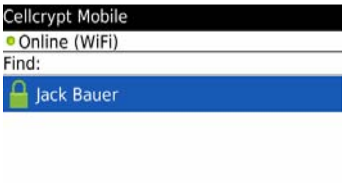
k. On ending the call, the user will be able to enter the contact details in the next window (First Name, Last Name and Contact Number). On Nokia, select Options | Create New Contact or if the contact already exists in your standard address book, select Options | Copy Name from Phone.



Cellcrypt Mobile
First Name: Jack
Last Name: Bauer
Contact Number: 7001

l. Enter the contact details as shown above and save the details by clicking the BlackBerry ‘BB’ button again and selecting Save’ and on Nokia, select Done.

m. This contact has now been added to the Cellcrypt address book and will appear with a green closed padlock denoting a secure contact/connection.



Cellcrypt Mobile

● Online (WiFi)

Find:

Jack Bauer

7.4 Latency

Latency is subject to network conditions (bandwidth, signal strength, congestion) on all segments between the devices particularly if a segment is cellular, but typical one-way latency between a device connected to a BGAN terminal and a receiving device on another network are shown below:

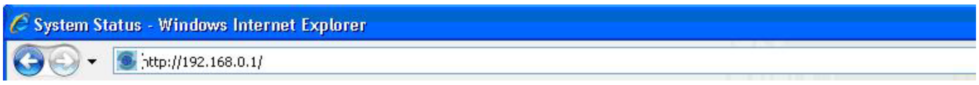
Receiving Device Connectivity	Latency
GPRS	2,000 Ms
EDGE	1,500 Ms
3G	1,200 Ms
WiFi	800 Ms

8 BGAN Step by Step Setup

8.1 Thrane EXPLORER™ 300/500/700 and 527

Background IP service should be initiated from the BGAN terminal and can be configured from either the EXPLORER™ 700's built-in web server (via a laptop's web browser) or using the LCD MMI.

a. Open your internet web browser and type the following IP address in the address bar: 192.168.0.1



System Status - Windows Internet Explorer

http://192.168.0.1/

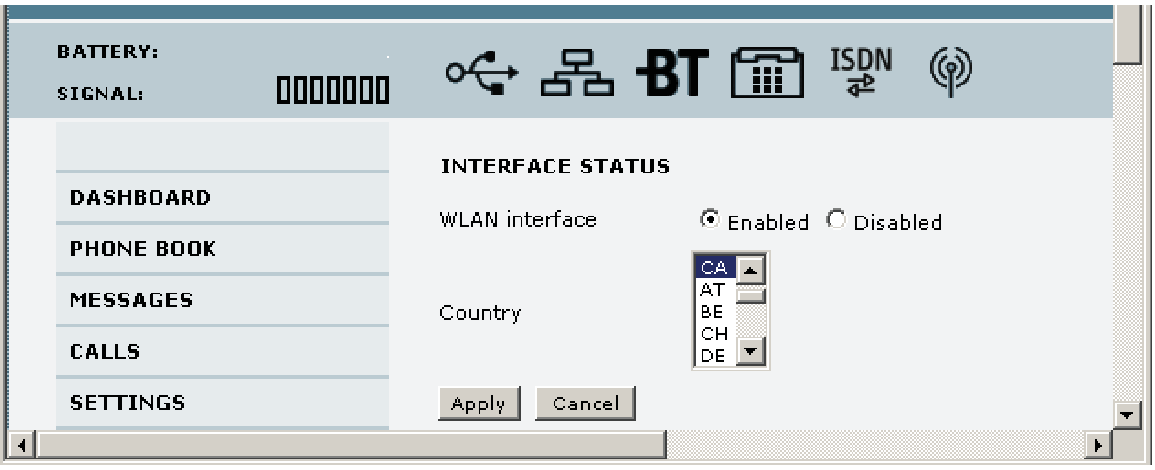
b. Click on Settings and then LAN

c. Now you should see the web server interface. The screenshot below shows the settings required as configured via the EXPLORER™'s web server interface, ensure you click apply before leave the web page. Please consult your EXPLORER™ manual for more detailed information.

d. Now your terminal is configured to start a Standard connection after you register on the network.

e. We need to configure the WLAN by clicking on SETTINGS and then WLAN on the left menu.

f. WLAN interface should be Enabled



INTERFACE STATUS

WLAN interface ● Enabled ○ Disabled

Country CA AT BE CH DE

Apply Cancel

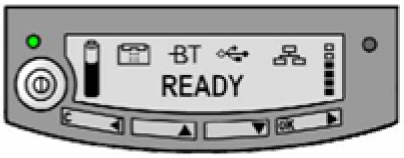
g. Change the SSID to desired name and enable security options as desired.

h. Restart your terminal and click OK after properly pointing the terminal. Once the Explorer is register on the BGAN network you will be connected automatically with a Standard connection.

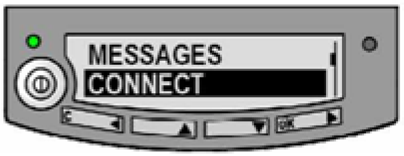
Connecting to BGAN via LCD MMI (When Automatic Activation is disabled)

The screenshot below shows the settings required as configured via the EXPLORER™ LCD MMI.

To initiate a connection from the LCD MMI, go to the main view of the LCD.

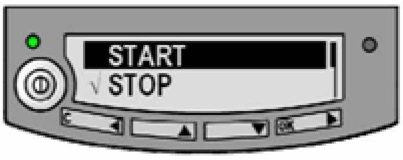


a. Press Arrow Down button until **CONNECT** menu is selected



b. Press **OK**

c. Select Standard and press **OK** button



d. Select **START** and press **OK** button

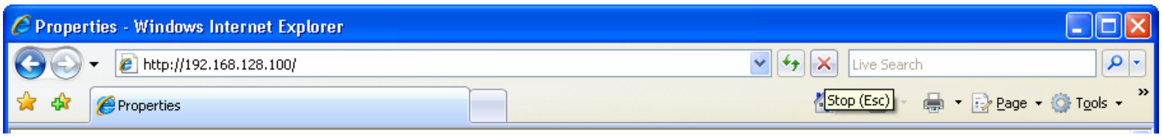
e. Press OK button to confirm Standard connection and wait a minute or two to allow the EXPLORER™ to register the Packet Switched connection with the BGAN system. After registration the LCD main screen will show **DATA ACTIVE**. See LCD below.

Now you need to configure your NOKIA of BLACKBERRY phone to connect to the terminal via WiFi with the security settings you configured.

8.2 HNS 9201 and 9250

Standard service should be initiated from the BGAN terminal and needs to be configured from the Hughes™ HNS9201's built-in web server (via a PC's web browser).

a. Open your internet web browser and type the following IP address in the address bar: **192.168.128.100**



b. Click on **WLAN.**

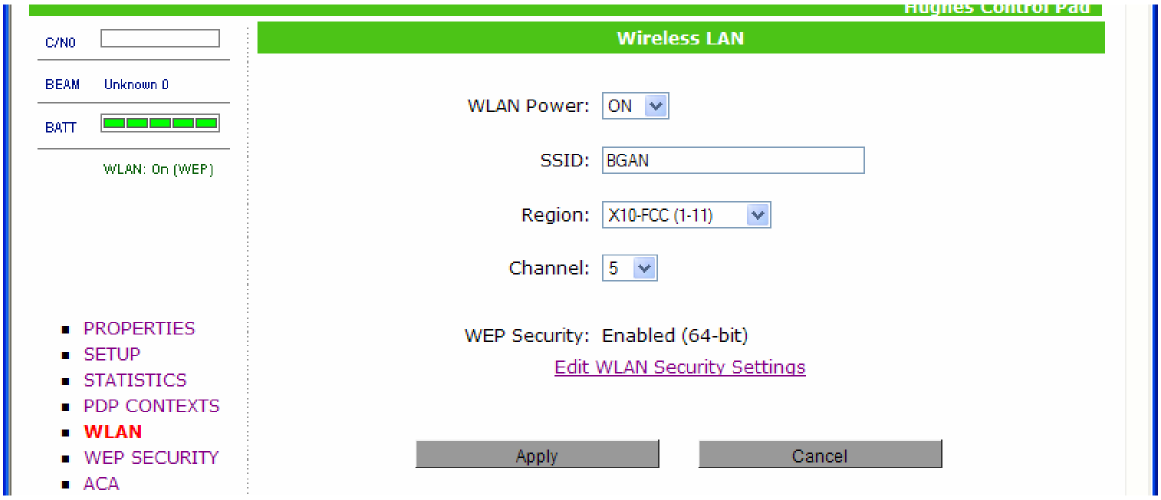
c. Click on the **WLAN** Power drop down menu and select **ON.**

d. Configure your SSID if you want to change it from the default BGAN.

e. Select your region.

f. Select your channel.

g. Click **APPLY**.



BEAM Unknown 0

WLAN: On (WEP)

WLAN Power: ON

SSID: BGAN

Region: X10-FCC (1-11)

Channel: 5

WEP Security: Enabled (64-bit)

h. Click on **WEP SECURITY** on the left menu.

i. Click on **WEP Protection** status drop down menu and select **ON.**

j. Select 64 bit or 128 bit encryption.

k. Configure your key and select your DEFAULT key by selecting the radio button.

l. Click **APPLY.**

m. Click on **ACA** on the menu on the left.

n. Select ACA settings for TEs using DHCP assigned IP address '**ON**'

o. Click **Apply**

p. Then Click **Restart Terminal**

q. Now register the terminal by pressing the Audio button until the signal strength lights go off.

r. The terminal will automatically recognize the DHCP Request and start the Background service automatically.

s. Now you need to configure your NOKIA of BLACKBERRY phone to connect to the terminal via WiFi with the security settings you configured.

9 Further Details and Support

Inmarsat Contact

Email: customer_care@inmarsat.com

Cellcrypt Contact

Email: info@cellcrypt.com

Website: www.cellcrypt.com