Using the Crypto DSSS-1021 over BGAN
Deployable Secure Satellite System
Version 01
22.12.2009
1 Overview

The DSSS-1021 is a secure, robust and elegant deployable system that includes the communications capabilities and the components for a small mobile office anywhere in the world. Using Satcom and its power autonomy it is fully independent of local infrastructure. The latest generation of BGAN satellites offers TCP/IP services, accessible via small, lightweight devices. Remote access to a central IT infrastructure therefore becomes reality for travellers wherever they are located.

Crypto AG has created a family of fully independent secure BGAN satellite systems housed in portable cases. The “Satellite Office Client Systems” provide a remote office using secure access and thus IP-based services such as e-mail, file transfer, VoIP, FoIP, video conferencing etc. It is using Inmarsat BGAN (Broadband Global Area Network) or terrestrial networks with Internet or provider networks and is enabled also to use terrestrial networks as Internet, GSM/UMTS or the PSTN.

The product “IT Office RT Comms” is a member of the “Satellite Office Client Systems” and a product of the Deployable Secure Satellite System family.

2 Key Features

- Small, lightweight, mobile and highly secure communication system & office platform
- All equipment packed into a “fly-away” case and fully interconnected: Satcom, security, user terminals, power supply
- Excellent connectivity to the headquarters by using Satcom Inmarsat BGAN from any location and alternative connections via any available IP-based terrestrial network/Internet access (in hotels, hotspots, GSM/UMTS, etc.)
- Power autonomy: built-in battery with DC/AC and solar panels input for operation or charging
- Modular: equipment/applications can be varied
- Reliable: robust, mobile, independent, easy operation
- Fast deployment: Connection to the BGAN Satcom terminal (or where there is a terrestrial access to the Internet or PSTN respectively)

3 Deployment Scenarios

The product can be used where:

- .. the terrestrial bandwidth is not sufficient or does not exist
- .. independence from the terrestrial network is required
- .. redundant communication, i.e. backup communication, is required
- .. mobility is required
- .. VSAT is not available or too costly.

4 Typical users
• Ministries of Foreign Affairs; missions, small embassies, travelling diplomats, military attachés
• Ministries of Interior of large countries with partially poor communication infrastructure; police, customs, homeland security, etc.
• Ministries of Presidency
• Border control for small locations or mobile teams
• Intelligence organisations
• In general: VIP’s

5 Network scenario

A typical user scenario is shown in Fig. 1 below. It involves two deployable systems in a standard and a light version, the Inmarsat core network and its gateways into the terrestrial IP and telephone network. All the IP-based applications are connected to the ICT infrastructure of headquarters.

As a backup communication channel a (Bluetooth) phone can be used to call any telephone subscriber using the BGAN terminal directly. This mitigates the dependence on an ICT infrastructure and its services in an emergency case. Any IP-based application is fully protected by a single IP VPN encryption unit on each side.

Also shown is a possible Internet access which is realised by an additional firewall in headquarters to enable security policy enforcement.
6 Product Description

6.1 Product concept

“IT Office RT Comms” is a platform for many applications and includes all the required hardware – built into a case and fully interconnected and ready to be configured.

All the required applications and components have to be configured and programmed before the case can be commissioned. There are normal application settings, but mainly all the networking configurations which must be able to fit into the available IT environment of the user.

There is a start-up packet available from Crypto AG which includes equipment for the central ICT infrastructure, engineering and commissioning to get an operative system for VoIP and possibly IT application which are operated in a first phase. Access to BGAN services is achieved by using a SIM card (as for GSM networks) which is provided by an airtime or service provider.

There are many providers offering airtime for BGAN – various subscriptions and price plans are available. For the initial phase after the commissioning of the system, Crypto AG can supply such a subscription on a temporary base (as pre-paid).

6.2 Main applications

The Deployable Secure Satellite System is a platform which is ready for IT and/or real-time application to be installed. The operating system has already some applications installed. Standard IT applications such as email, FTP or Intranet are possible as are real-time applications such as VoIP or video. It depends on the operated ICT system in the HQ which applications are supported or enabled.

All communication to the central ICT infrastructure is protected by Crypto AG’s IP VPN Encryption (VPN tunnels). The following applications can be in operation on the platform:

Office applications:

- Messaging/Email
- File Transfer (FTP)
- Any Client/Server applications
- Intranet etc.
Real time applications:

- VoIP
- FoIP (using an IP or a legacy Fax or Fax over Email)
- Video conferencing
- Plain telephony using a phone (BT or 2-wire phone) and the Explorer 500 (e.g. as a backup communication)

Additional security services:

- Besides these applications there is a Secure Data Storage which can be mounted as a network share to the Netbook. Optional there is also a File and Message Encryption application available using the security services of the Crypto Mobile Client HC-7835 IP VPN.

6.3 Product components

The IT Office RT Comms system DSSS-1021 includes:

- Satcom terminal Explorer 500 (streamlined for this, compact, including antenna)
- Crypto Mobile Client HC-7835 IP VPN
- User terminal (multimedia Netbook)
- IP phone
- Phone adapter (optional, to connect an external legacy phone and/or fax, mainly used over terrestrial networks in case of insufficient connectivity over satellite)
- A6 Printer
- Scanner (optional, e.g. for document scanning or Fax over Email T.37)
- Network components (switch, etc.)
- UPS Battery, power supply and distribution
- BT phone assigned to the BGAN terminal (optional as a backup communication) or a compact 2-wire phone
6.4 The power supply concept

The case has a built-in Li-Ion battery which enables power autonomy for about four hours. The Netbook, the printer, the BT phone and the BGAN terminal have their own battery.

The BGAN terminal has, depending on usage, about the same autonomy of 3-4 hours. The battery can be charged and/or the system supplied by AC input (priority if in parallel) or DC input from different power sources as DC from a car battery or solar panels.

The BGAN terminal and the BT phone can also be charged using the power supply of the case, the others have their own AC adapters.

6.5 Communication access scenarios

a) Remote access scenario

To put the Deployable Secure Satellite System into operation, it must typically be connected to the central ICT infrastructure where all the applications run (server, PBX, etc.). This can be achieved using the way over satellite or a terrestrial network. However using the path over the satellite involves also a terrestrial network between the land earth station (LES) and the location of the HQ.

Technically it is possible to have peer to peer connections to other DSSS-1021 (also using VPN) but such peer-to-peer applications are rather exceptions for IT or real time applications and typically require a registration server to enable the routing.

There are basically two different transport network scenarios for the terrestrial part of the communication:

A) Using the Internet as the transport network.
That’s the easiest way and copes with the good/bad qualities of the Internet. There are many access ways via Internet to remotely access your ICT; Satellite, Hotspot, ADSL, GSM/UMTS

B) Using dial-up or leased lines of the PSTN or dedicated IP/MPLS networks of a provider as the transport network.
The BGAN service provider takes the traffic from the land earth station (LES) and routes it trough the PSTN (dial-up or leased lines) or through his dedicated IP network to your HQ. This approach excludes the bad qualities of the Internet but also reduces the access ways to satellite and terrestrial to selected access points of the provider (dedicated IP network) or the PSTN.
Using the Internet as the transport network includes the bad qualities of the Internet but also the good ones such as the possibility of many connectivity options for the remote access and much cheaper running costs for the terrestrial part.

In order to reach the HQ via the Internet the DSSS-1021 can be connected:

1. to the BGAN satellite terminal Explorer 500 (LAN interface)
2. to an available ADSL modem (LAN interface, e.g. in a hotel, etc.)
3. to an GSM/UMTS router (LAN interface, optional built-in)
4. to a public or private Hotspot (WLAN interface)
5. to a GSM handy with a running "walking hotspot" application (WLAN interface)
6. to a GSM handy using the BT interface using DUN (dial up networking) profile (BT interface)

b) Peer-to-peer scenario

Technically it is possible to have peer to peer connections to other DSSS-1021 (also using VPN) but such peer-to-peer applications are rather an exception. In case of a peer-to-peer scenario with mobile to mobile communication there is a registration server required (Crypto AG MS-1100) since NAT/NAPT is used or it requires fix IP addresses. Peer-to-peer between a fix station and mobile station port forwarding is applied.
6.6 Central ICT infrastructure

Remote access approach
In order to have communication with the *IT Office RT Comms* system there is normally a central ICT infrastructure required; servers which serve all the IT applications, call manager or exchanges to serve the real-time applications as VoIP or video conferencing and of course the partner device for the IP VPN, etc.
7 Setup

7.1 Requirements

- Inmarsat BGAN subscription from an airtime provider. There is a SIM card from the provider to access the network and its services. The subscription is connected with a specific price plan. There are shared IP and/or streaming data services and standard voice (telephony via the PSTN e.g. as a backup communication channel) required. In case of not using the Internet as the terrestrial transport network there is an additional agreement with the provider required to get the appropriate user profiles to activate the routing through the provider’s network and eventually trough the PSTN (e.g. if using a ISDN dial-up access to the HQ).

- ICT infrastructure
  It typically needs an ICT infrastructure with running services/applications in the HQ prepared for remote access and with an IP VPN partner.

- DSSS-1021 system
  Since the Office Client RT Comms DSSS-1021 is an open mobile application and communication platform the applications have to be setup in a system integration phase. As delivered the system is ready to be configured and has its own home network where all components are integrated. The system requires only to be configured for the remote access into the users ICT infrastructure (world side of the DSSS-1021). Of course all the security related issues must also be defined and programmed in the IP VPN device mainly security operating parameters and all the key management issues.

7.2 Back panel of the DSSS-1021

All connections to outside of the case are places underneath a cover of the case. If it is opened the appropriate cables can be connected to the sockets. All the necessary cables and adapters are located somewhere in the case.
7.3 Setting up the BGAN satellite service

Precondition here: The Ethernet interface of the HC-7835 is activated.

Step 1: Connection to the satellite

1. Take out the satellite terminal from the case and place it where there is an open line of sight to the satellite.
2. Plug the Ethernet patch cable to its LAN interface and the SAT/WAN/LAN connector of the DSSS-1021.
3. Press the power on button of the satellite terminal until its LED is on.
4. Enter the PIN if required.
5. Use the satellite modem's pointing sound to adjust the satellite modem to get the best reception (at least about 47dB, the higher the better) and press OK if tuned to the max. and await the READY on the display.
6. Check the status of the battery (see the display symbol). If it is too low for the estimated operating time connect also the AC/DC adapter with its barrel plug to DC IN of the terminal and the mains cable to the mains outlet of the DSSS-1021.

Step 2: Power on the DSSS-1021:

1. If there is AC power available or the battery is low connect the DSSS-1021 to the mains using the appropriate mains cable and plug adapter.
2. Power on the system.
3. If the IP VPN client is setup in a way that a login is required login as a user. The system will automatically connect itself to the satellite terminal, the defined primary BGAN service is automatically setup and a VPN tunnel is built up. The applications (e.g. the VoIP phone) will automatically register themselves at the appropriate servers and are ready.
4. In case the Netbook wants to be used e.g. using IT services as email, FTP or Intranet, etc. take it out of the case and connect the Ethernet cable to its LAN interface and to the LAPTOP connector at the rear of the DSSS-1021. In case the Netbook battery is low connect the appropriate AC/DC converter to it and its mains cable to the mains outlet of the DSSS. As soon as the VPN tunnel is up the remote access is possible and thus the access to all running IT services.

Step 3a: Setting up a streaming data service at the Explorer 500:

For certain application (e.g. video conferencing) the user has to start a streaming data service. Since for these services there is a time tariff the user setup this service only during this session. If the satellite terminal is close use its user interface to start the streaming service;

1. Select CONNECT and then the defined and required profile (service) and select START.
2. Start the application
3. If the application (phone calls, conference, etc.) is terminated you must stop the streaming service; Select CONNECT and then the defined and required profile (service) and select STOP.

Step 3b: Setting up a streaming data service by the LaunchPad:

If the satellite terminal is far away use the Plain Connection feature of the system to use the LaunchPad to start the streaming service;

1. Login as USER into the IP VPN device.
2. Select parameter group SECURITY and then Plain Connection.
3. Change it from "Not permitted" to "Permitted". A plain channel will be available through the device to the satellite terminal for the predefined time period and set plain connection type.

4. Start the LaunchPad on the Netbook and press the icon Data.

5. Select the required streaming mode.

6. Set the Plain Connection back to "Not Permitted". The VPN tunnel will come up again.

7. If the application (phone calls, conference, etc.) is terminated you must stop the streaming service; activate the Data icon of LaunchPad and stop the running streaming service.

7.4 Setting up an Internet access via the LAN interface

Precondition here: The Ethernet interface of the HC-7835 is activated.

**Step 1: Connection to the LAN (world side)**

If there is an Internet access available (in a hotel or in your own location) by connecting the system to a LAN this can be done as follows:

1. Connect the Ethernet cable to the switch or router which is connected to the Internet.
2. Switch on the DSSS system.
3. According the system setup login as a user if required.
4. The world interface will automatically get the IP address by DHCP and starts to communicate.
5. In case there is no other login is required and no firewall stops the traffic the VPN tunnel automatically comes up and the applications can register themselves or the applications on the Netbook have access to its servers.

**Step 2: Login in a public Internet access point**

Normally there is a login required if you are using a public Internet access as e.g. in a hotel (or using a hotspot) since one has to pay for it. You have to login at a homepage of this access providers by user name and password. Any entered browser address will be redirected by a proxy to the appropriate login page. Assumed you have done Step 1 above;

6. Login as USER into the IP VPN device.
7. Select parameter group SECURITY and then Plain Connection.
8. Change it from "Not permitted" to "Permitted". A plain channel will be available through the device to the satellite terminal for the predefined time period and set plain connection type.
9. Start the Browser and enter any address into the browsers address line (e.g. www.google.com). The proxy server will redirect this and present the login window.
10. Use the login window of the application to enter the username and password.
11. Set the Plain Connection back to "Not Permitted". The VPN tunnel will come up and the applications can register themselves or the applications on the Netbook have access to its servers.
7.5 Setting up an Internet access using an UMTS router

Precondition here: The Ethernet interface of the HC-7835 is activated.

A UMTS router is normally configured in a way that as soon as powered up within GSM providers' network it sets up the best data service to access the Internet. There is a DC supply cable available from the case to supply the router. The SIM card is located in the router and the router logs it in using the programmed PIN. On the local side of it there is an Ethernet interface which behaves like the local interfaces of a router. A client device which connects itself to it will get an IP address and thus access to the Internet.

1. Connect the Ethernet cable to the UMTS router which is connected via GSM network to the Internet and the SAT/LAN/WAN connector of the DSSS.
2. Switch on the UMTS router and wait until the LED confirms the connection to the Internet.
3. Switch on the DSSS system.
4. If the IP VPN client is setup in a way that a login is required login as a user.
5. By using DHCP the world interface will automatically get the IP address and the system starts to communicate.

7.6 Setting up a Internet access via a hotspot (WLAN)

Normally there is a login required if you are using a public hotspot Internet access as e.g. in a hotel or in public areas as airports etc. since normally one has to pay for it. You have to login at a homepage of this access providers by user name and password. If it is a GSM provider you may get the required username and password by SMS from your provider;

**Step 1: Select the WLAN interface for the world connection** (if not yet active)

1. Login as USER into the IP VPN device and start a PC UI Session
2. Start the browser and connect it to the IP VPN client
3. Select the tab User Connect and select in the Connection menu the "Wireless LAN"
4. Select "Permitted" in the pull down menu of Plain Connection and press <Submit>

**Step 2: Select the required WLAN SSID**

1. Select the menu Wireless LAN and press <Scan>
2. Select the required SSID and in case it is an open WLAN access just press <Connect>
3. If it has security on you need to have the keys. Thus press <Details> and enter the key in the field Password. Check the Auto Connect parameter if practical.
4. If it is a login free access select "Not permitted" in the pull down menu of Plain Connection and press <Submit>
5. VPN tunnel will come up and the applications can register themselves or the applications on the Netbook have access to its servers. Else make also step 2.
Note: If a known WLAN AP is available and setup for automatic connection in the HC-7835 the above SSID selection and its setting is not required and the connection will automatically come up.

Step 2: Login in a provider or public Internet hotspot

If the WLAN connection is active;

1. Enter any address into the browser's address line (e.g. www.google.com)
2. The proxy server will redirect this and present the login window.
3. Use the login window to enter the given username and password.
4. Address the PC UI of the VPN client again and select "Not permitted" in the pull down menu of Plain Connection and press <Submit>
5. VPN tunnel will come up and the applications can register themselves or the applications on the Netbook have access to its servers.

Note: If a private WLAN AP is available there is typically no login required.

7.7 Setting up an Internet access via a UMTS hotspot (WLAN)

This setting is very similar to the above one using an ordinary Hotspot. The only difference is that the user uses his own GSM handheld to setup a Hotspot on it.

Step 1: Start the WLAN hotspot on your GSM by starting the appropriate application

Proceed with the steps above; setting up an Internet access via a hotspot (WLAN). The username and passwords for users are defined by the GSM user himself and are needed to be entered into profile (details) of this Wireless LAN. If the entry is defined for auto connect the DSSS-1021 will automatically connect to the hotspot, the VPN tunnel will come up and the applications can register themselves or the applications on the Netbook have access to its servers

7.8 Setting up an Internet access via BT and a DUN profile

This approach requires having a GSM handheld using it as a data modem. Data services to access the Internet must be available (GPRS up to 3.5G UMTS services). The appropriate BT DUN profile is provider individual. It has a profile name, phone number, username, password and a GSM initialisation string.

Precondition here: The Dialup Profile is configured on the HC-7835 and the Bluetooth pairing between the handheld and the HC-7835 has been done before. Then start with step 1, otherwise with step 0.

Step 0: Pairing the Bluetooth GSM phone with the HC-7835 (only once)

1. Mobile GSM phone: Enable the BT interface/service and let it be visible for a limited time.
2. HC-7835: Access it by using the PC UI and select tab "User Connect" and menu Connection, select "Bluetooth" and press <Submit>
3. HC-7835: Press <Scan> and select out of the list your BT phone
4. HC-7835: Press <Details>
5. Enter the Bluetooth PIN, select the DUN profile and enter the required profile details
6. Press <Submit>

Step 1: Select the Bluetooth interface for the world connection

1. Ensure the GSM handheld is ready and the BT is activated.
2. Login as USER into the IP VPN device and start a PC UI Session
3. Start the browser and connect it to the IP VPN client
4. Select the tab User Connect and select in the Connection menu the "Bluetooth"

Step 2: Select the Bluetooth device and connect to the Internet

1. Select the appropriate Device Name (handheld) and press <Connect>. Afterwards enter the Bluetooth PIN at the handheld, wait until the status displays connected.
2. VPN tunnel will come up and the applications can register themselves or the applications on the Netbook have access to its servers.
3. At the end of communication power disconnect the data service at the GSM handheld or use the disconnect key on the HC-7835's PC UI.

8 Operating after setup

Since the "IT Office RT Comms" is platform for many applications the operation for them can't be described here. It depends what applications are installed and how they are setup. However some basics can be described here.

Precondition here:
The system is powered up, connected to the central ICT infrastructure and the VPN tunnel is up.

8.1 Using the VoIP phone(s)

Before the VoIP phone can be used it must be registered at the appropriate IP PBX (this is normally automatically done) and this is indicated by green LED's assigned to a line.

If you have more then 1 line/number defined on the phone, select the required line by pressing the line key. Off hook and dial the number manually or from the phonebook. At the end put the handset on the cradle (off hook). If it rings with a number specific ring tone the appropriate user takes the call by taking the handset and on hook at the end.

Note: In addition to the VoIP phone there might be a soft phone installed on the Netbook. Then a user can make phone calls using this or the hard phone, even simultaneously.

An additional external VoIP can be connected to the system as well. Both, soft phone and the external VoIP phone have to be integrated into the VoIP environment (networking, subscriber number, etc.)
8.2 Using a legacy FAX (external)

Before the legacy Fax can be used it must be connected to the system, be powered on and the phone adapter must be registered at the appropriate IP PBX (this is normally automatically done after the VPN tunnel is up) and this is indicated by green LED.

Put the documents into the Fax paper slot, dial the number and press the Start key.

**Note:**
- If the connection goes over the satellite and not on a terrestrial way (e.g. the Internet) to the HQ then an ordinary legacy Fax will hardly will succeed because of the long round trip times. An appropriate satcom compatible Fax model must be used and setup for long distance to have a chance for any connectivity in this mode. If the connectivity is not acceptable the alternative is using Fax over Email T.37. Thus the document is scanned (scanner is an optional accessory), attached to an Email and sent to the fax gateway server (where the attachment is extracted from the Email and sent to an ordinary Fax).
- There is normally a good chance to send Fax using the 2-wire interface of the Explorer 500 using the Audio 3.1 kHz service (at least to a fixnet location with one satellite hop). However doing this means plain communication!

8.3 Using an IP FAX (external)

Before the IP Fax can be used it must be connected to the system, be powered on and it must be registered at the appropriate IP PBX (this is normally automatically done after the VPN tunnel is up). Thus the IP Fax must have been integrated in the network and logically in the telephony system (IP PBX).

Put the documents into the Fax paper slot, dial the number and press the Start key.

**Note:**
If using the Fax over IP T.38 as the communication protocol there is a chance to succeed also over satellite if it is a "good" connection. However also T.38 was developed for terrestrial IP networks and it might work with a sufficient connectivity only over terrestrial networks. Then Fax over Email T.37 is also the alternative means to fax (see above).

8.4 Using a legacy Phone (external)

Instead a legacy Fax one can also connect a legacy phone to the FAX connector of the system. The phone adapter will recognize whether a Fax or phone call is going on. Such a call can of course go on in parallel with any other VoIP calls (question of the bandwidth and the used voice coders). The use of such a legacy phone is just simple. Advantage: any 2-wire phone can be used typically without any configuration. Disadvantage: Many of the used VoIP comfort telephony features may be not supported.

8.5 Using Any applications on the Netbook

Connect the Netbook to the Laptop connector of the system using the LAN patch cable, start it up and start the appropriate application. If multi media or real time applications are used an audio in/out device has to be connected (e.g. a headset). To use the printer it must first be connected to the Netbook using the USB cable and the battery of it must still have power (otherwise charge it by its own AC adapter).
Note: The printer would have a BT interface to connect it wireless. However don’t use this interface since it radiates your plain and maybe sensible information into your local area. It easily can be tapped.

8.6 Using the BT phone to make a ordinary plain phone call

Precondition here: The BT handset has to be paired in advance to use it for phone calls via the Explorer 500 terminal. The Explorer 500 must be registered and ready for phone calls (phone symbol on the display of it). The BT phone must also be located within the range of the BT radio signal.

Switch on the BT phone and wait until it is registered at the Explorer 500. Dial the ordinary PSTN subscription number or use the build-in phonebook. Press the off-hook key and make the call. At the end press the on-hook key.

Note: The only things which must work are the BT phone and the Explorer 500. Thus it can be seen as an emergency backup communication. Besides that it can be used just to communication outside of a closed and secured VoIP network to any PSTN/GSM user. This communication is in plain and unprotected!

8.7 Charging the different batteries

The following components use batteries and have to be charged frequently. All the specific AC adapters are located somewhere in the case:

- **DSSS-1021 system itself**
  Check the status of the battery by pressing the metallic key on the UPS (underneath the printer). It is empty if no LED is on or shows some green LED's according the remaining energy.
  a) Supply the system with AC between 85–264 VAC, 50/60Hz and use the appropriate mains cable and the country specific mains plug adapter (all available in the case).
  b) Supply the system with using the DC_IN connector and supply DC 12~16V from an AC/DC adapter or from a 12V car battery (e.g. from a cigarette lighter plug) using the adapter cable and plug. C) Optional: You might also use solar panels. Using the DC_IN normally a voltage limiter is used to protect the system against over voltage. Alternatively you can use the 3-pin connector at the battery and the 3-pin smart "Sunbooster" (voltage limiter and Sunbooster are optional accessories).

- **The satellite terminal Explorer 500**
  Use the specific AC/DC adapter of the Explorer 500 and connect it to the mains (e.g. at the AC outlet at the DSSS-1021 or directly). If the DSSS-1021 is AC supplied alternatively you can use the DC supply cable to charge the terminal from the DC_OUT of the DSSS-10221.

- **The Netbook**
  Use the specific AC/DC adapter of the Netbook and connect it to the mains (e.g. at the AC outlet at the DSSS-1021 or directly).

- **The Printer**
  Use the specific AC/DC adapter of the printer and connect it to the mains (e.g. at the AC outlet at the DSSS-1021 or directly).

- **The BT phone handset**
  If the DSSS-1021 is AC or DC supplied then the BT phone can be charged using the
specific charger cable being in the accessory box. Switch the DSSS-1021 on and connect the cable to the BT phone. A symbol on the display confirms the charging.

9 **Technical Summary**

For all details check the data sheet on the homepage of Crypto AG.

9.1 **Deployable Secure Satellite System DSSS-1021**

<table>
<thead>
<tr>
<th>Category</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Housing</strong></td>
<td>Robust and elegant aluminium case (traveller case), attachable trolley</td>
</tr>
<tr>
<td><strong>Power supply</strong></td>
<td>External AC power supply 100...240, 50/60 Hz, max. 50W DC IN 12..16V (from a AD/DC adapter, 12V car battery, solar panel DC OUT 15VDC/50W (if connected to the mains, else = DC IN) Built-in UPS battery for power autonomy with power autonomy of:</td>
</tr>
<tr>
<td></td>
<td>- Operating hours network components: ~3 hours</td>
</tr>
<tr>
<td></td>
<td>- Satellite terminal Explorer 500: ~3 hours</td>
</tr>
<tr>
<td></td>
<td>- Netbook: ~7 hours</td>
</tr>
<tr>
<td></td>
<td>- UPS Battery: 50Wh</td>
</tr>
<tr>
<td><strong>Dimensions</strong></td>
<td>490 x 370 x 160 cm</td>
</tr>
<tr>
<td><strong>Weight</strong></td>
<td>Approx. 14 kg</td>
</tr>
<tr>
<td><strong>Environmental data</strong></td>
<td>Range for the various built-in components:</td>
</tr>
<tr>
<td></td>
<td>Operating temperature: -5°C…+50°C</td>
</tr>
<tr>
<td></td>
<td>Storage temperature: -20°C…+70°C</td>
</tr>
<tr>
<td></td>
<td>Humidity: 93%RH/+55°C (according to EN 60068-2-30)</td>
</tr>
<tr>
<td></td>
<td>Vibration: 10 …150Hz, 0.8g effective (random)</td>
</tr>
<tr>
<td></td>
<td>Drop: 0.75m, Shock: 25g, 6ms</td>
</tr>
<tr>
<td></td>
<td>Internal protection: IP54</td>
</tr>
<tr>
<td><strong>Line interfaces (world)</strong></td>
<td>SAT/LAN/WAN (World):</td>
</tr>
<tr>
<td></td>
<td>Ethernet / RJ45, IEEE 802.3, 10BASE-T</td>
</tr>
<tr>
<td></td>
<td>WLAN, IEEE 802.11 b/g (optional)</td>
</tr>
<tr>
<td></td>
<td>Bluetooth version 2.0 (optional)</td>
</tr>
<tr>
<td></td>
<td>DHCP client, NAT support</td>
</tr>
<tr>
<td></td>
<td>QoS: TOS / DSCP forwarding</td>
</tr>
<tr>
<td><strong>Home</strong></td>
<td></td>
</tr>
<tr>
<td><strong>PC</strong></td>
<td>Ethernet/RJ45, 10/100</td>
</tr>
<tr>
<td><strong>Fax</strong></td>
<td>2-wire FXS ports RJ11</td>
</tr>
<tr>
<td><strong>IP Phone/Fax</strong></td>
<td>Ethernet/RJ45, 10/100</td>
</tr>
<tr>
<td>Cryptographic data</td>
<td>Algorithm</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Customer-specific cipher algorithm</td>
<td></td>
</tr>
<tr>
<td>Customer managed profiling of algorithm by CMP</td>
<td></td>
</tr>
<tr>
<td>Built-in high-quality true random generator</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Key management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual key input via user interface</td>
</tr>
<tr>
<td>Copy / backup of key and installation data by Security Data Carriers (SDCs)</td>
</tr>
<tr>
<td>Online/Offline by Security Management Centre SMC-1100</td>
</tr>
<tr>
<td>Tamper-proof design</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Application IP VPN</th>
<th>Services supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unicast &amp; Multicast IP VPN tunnels (tunnel mode)</td>
<td></td>
</tr>
<tr>
<td>Optional: Throughput approx. 1, 4 or 8 Mbps with 1500 byte IP packets (limited with Bluetooth)</td>
<td></td>
</tr>
<tr>
<td>Up to 8 tunnels (1 Mbps) or 32 tunnels (4 / 8Mbps)</td>
<td></td>
</tr>
<tr>
<td>Star and/or mesh topologies</td>
<td></td>
</tr>
<tr>
<td>Traffic types: data/voice/video</td>
<td></td>
</tr>
<tr>
<td>Quality of service (QoS) support, TOS/DSCP forwarding</td>
<td></td>
</tr>
<tr>
<td>Configuration of TOS/DSCP for key agreement</td>
<td></td>
</tr>
<tr>
<td>Replay protection window size 64 packets</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>User interface</th>
<th>Keypad, LCD and LED (HC-7835 and VoIP Phone)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browser-based user interface (all components)</td>
<td></td>
</tr>
<tr>
<td>Smart card reader (HC-7835)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Netbook: Windows XP home</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telephony: SIP (CISCO on request)</td>
<td></td>
</tr>
</tbody>
</table>

| USB Memory | USB Memory (4GB) with write protection, possible to boot the notebook with an operating system (thin client) |

<table>
<thead>
<tr>
<th>Optional features</th>
<th>Secure local data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mountable encrypted memory drive on the HC-7835</td>
<td></td>
</tr>
<tr>
<td>Email and file encryption</td>
<td></td>
</tr>
<tr>
<td>Encryption service for email and file encryption</td>
<td></td>
</tr>
<tr>
<td>File and email encryption application for PCs</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Approvals</th>
<th>EMC: EN 55022 class B/EN 55024</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety: EN 60950</td>
<td></td>
</tr>
<tr>
<td>Quality system: ISO 9001:2000</td>
<td></td>
</tr>
<tr>
<td>Conformity: CE (European conformity)</td>
<td></td>
</tr>
</tbody>
</table>
The system employs the **Crypto Mobile Client HC-7835 IP VPN**. Please refer to the appropriate data sheet for details. All of its functions, the performance etc. are a perfect fit with the Inmarsat BGAN system and your ICT infrastructure. However Crypto AG has a whole product family for IP VPN products. See the appropriate paper "Using IP VPN encryption solutions from Crypto AG over BGAN" at the same Inmarsat homepage location.

### 9.2 Accessories

Possible accessories are:

- **Solar panel T55 Multi-Device Kit** (to charge the built-in battery and the battery of the Explorer 500) together with the required adapters and cables.

- **Advanced Power Autonomy Kit** available to expand the power autonomy - consisting of rechargeable batteries, DC/AC input and solar panels charger, AC output (optional)

### 9.3 Product hierarchy

Crypto AG has planned a whole set of different Deployable Secure Satellite Systems. The graphic shows the product hierarchy (the required applications are the main key for the hierarchy).

![Product hierarchy diagram]

### 10 Further Details and Support

**Inmarsat Contact**

[customer_care@inmarsat.com](mailto:customer_care@inmarsat.com)

**Crypto AG Contact**

Crypto AG  
P.O. Box 460  
CH-6301 Zug  
Switzerland  
Tel. +41 41 749 77 22  
Fax +41 41 741 22 72

E-Mail: [crypto@crypto.ch](mailto:crypto@crypto.ch)  
Support: [support@crypto.ch](mailto:support@crypto.ch)  
Web site: [www.crypto.ch](http://www.crypto.ch)

Product Manger: Bruno FURRER