



Setting Up a Secure Connection with KlasTA over Satellite

KB article reference no. Q103001

Version: 1.0

Keywords: KlasTA, KIV-7, OMNIxi

The information in this article applies to:

- KlasTA
- KIV-7/OMNIxi
- KlasRouter
- KlasHopper

Table of Contents

1.0	Introduction.....	2
2.0	Mobile Side.....	2
2.1.	INMARSAT M4 Terminal	3
2.2.	KlasTA	3
2.3.	Type-1 Serial Encryption Device.....	3
2.4.	RS-530 Synchronous Serial Device.....	4
3.0	Home Side.....	4
3.1.	ISDN NT-1.....	4
3.2.	KlasTA.....	4
3.3.	Type-1 Serial Encryption Device.....	5
3.4.	RS-530 Synchronous Serial Router	5

Table of Figures

Figure 1.	Sample Scenario for a Deployed User.....	2
Figure 2.	Rear View of Mobile Side KlasTA	3
Figure 3.	Rear View of Home Side KlasTA	4

1.0 Introduction

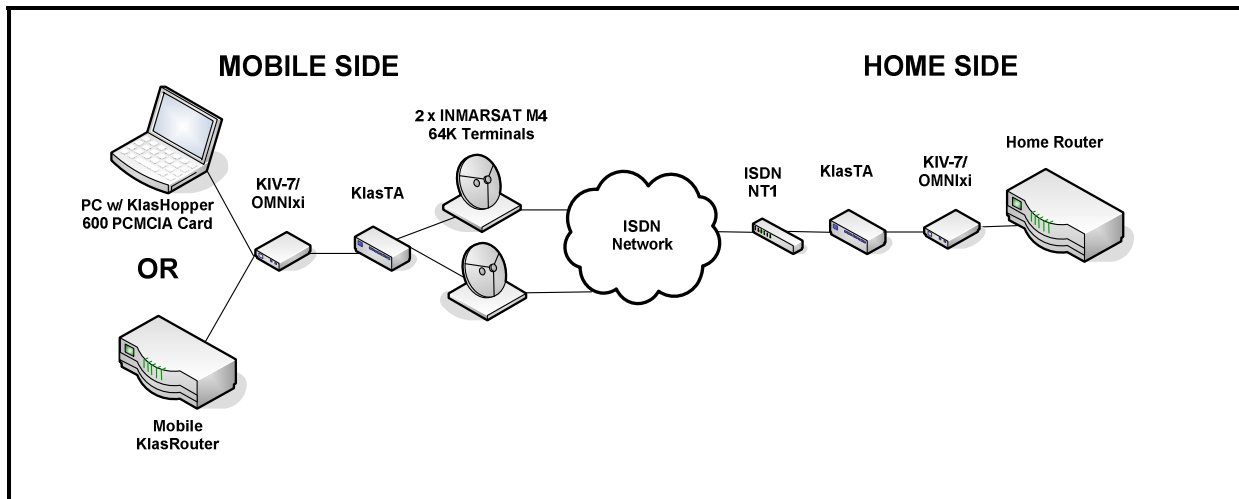


Figure 1. Sample Scenario for a Deployed User

This document describes how to physically set up each device needed to establish a secure connection over satellite using KlasTA, as shown in Figure 1. The sample scenario includes a Mobile and a Home Side of the communications session. The Mobile Side represents a user in a deployed environment and the Home Side represents a fixed terrestrial network with an established ISDN BRI connection. Typically, the Mobile Side will initiate the session by using the KlasTA to dial out through the INMARSAT M4 Terminals. The KlasTA on the Home Side will answer the call, establish the necessary parameters, and complete the connection with Mobile Side KlasTA. Once the KlasTAs have synchronized with each other, the KIV-7/OMNixi will initiate the exchange of security parameters and establish a Type-1 encrypted session. Finally, once the KIV-7/OMNixi have authenticated each other and the connection is secure, the end user communications devices can begin to exchange data through a PPP or HDLC session. Follow the instructions in the sections below to physically set up the devices needed to conduct a secure communications session over satellite.

2.0 Mobile Side

The devices listed below are required in order to establish a secure connection in a deployed environment:

1. INMARSAT M4 Terminal
2. KlasTA
3. Type-1 Serial Encryption Device (i.e. KIV-7 or OMNixi)
4. RS-530 Synchronous Serial Device (i.e. KlasRouter or KlasHopper)

The following sections will describe the purpose of each device and how it physically connects to its counterpart device.

2.1. INMARSAT M4 Terminal

There are several different manufacturers of INMARSAT M4 Terminals. Each terminal consists of an outdoor unit (ODU) and an indoor unit (IDU). The ODU is the antennae that physically sends and receives satellite signals. When setting up the ODU, ensure that it has an unobstructed line of sight view to the satellite with a strong signal. The ODU connects to the IDU through a coaxial cable. The IDU is a satellite phone and will use the digits it receives from KlasTA to dial up a connection with a Land Earth Station (LES) in order to connect to the public ISDN network. The IDU has an RJ-45 port typically labeled ISDN Input that connects to one of the ISDN Output ports on KlasTA through a standard straight-through Ethernet cable.

2.2. KlasTA

KlasTA is an ISDN Terminal Adaptor (TA) that converts serial data into an ISDN format for use across the public ISDN network. As shown below in Figure 2, KlasTA contains an ISDN NT Input port, two ISDN Output ports and an RS-530 Input Port. Each of the ports is explained below.

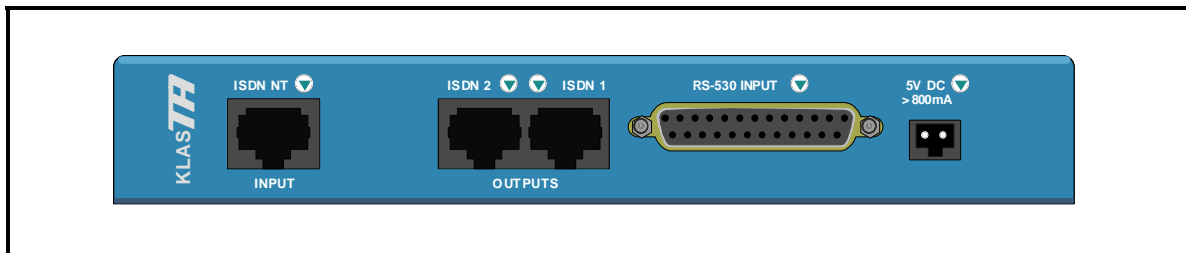


Figure 2. Rear View of Mobile Side KlasTA

1. The ISDN NT Input port is used as a splitter in order to divide a 128K ISDN Input into two separate 64K ISDN channels for transmission over the ISDN 1 and ISDN 2 Output ports. Although not represented in this document, the ISDN NT Input port can be used to accept the output from a STE and in order to send it across a satellite link.
2. ISDN Output ports 1 and 2 each represent an ISDN BRI connection. Each port can handle two ISDN 64K B-channels for a maximum throughput of 128K per port. Connect the Ethernet cable coming from the M4 Terminal into these ports.
3. The RS-530 Input port is a synchronous serial DB-25 port. Using the appropriate cable for the serial encryption device being used, connect the RS-530 Input port to the KIV-7 or OMNIxi.

2.3. Type-1 Serial Encryption Device

The two most commonly used Type-1 Serial Encryption Devices are the KIV-7 and OMNIxi. Each device accepts classified data through one serial port and then after encrypting the data sends it out another serial port as an unclassified encrypted data stream. The port that sends out encrypted data has a male connector and should be connected to the RS-530 Input port on KlasTA. The port accepting classified data has a female connector and connects to the RS-530 Synchronous Serial device.

2.4. RS-530 Synchronous Serial Device

There are two devices that can be used to connect to a Type-1 Serial Encryption Device, a router or a KlasHopper 600 PCMCIA card. With a router, such as KlasRouter, it must have an RS-530 Synchronous Serial connector. KlasRouter has a DB-25 male connector that can be used with a KIV-7 or OMNIxi. Ensure you have the appropriate cable and connect the KlasHopper card to the KIV-7 or OMNIxi. With KlasHopper, slide the card into an available PCMCIA slot on your laptop. Ensure you have the appropriate cable and connect the KlasHopper card to the KIV-7 or OMNIxi.

3.0 Home Side

The devices listed below are required in order to establish a secure connection in a fixed environment:

1. ISDN NT-1 Device
2. KlasTA
3. Type-1 Serial Encryption Device (i.e. KIV-7 or OMNIxi)
4. RS-530 Synchronous Serial Router (i.e. KlasRouter)

The following sections will describe the purpose of each device and how it connects to its counterpart.

3.1. ISDN NT-1

There are several different manufacturers of ISDN NT-1 devices. In North America, networks require an NT-1 device with an ISDN U-Interface in order to convert the Public ISDN 2-wire connection into a 4-wire S/T connection on a TA, such as KlasTA. Connect the U-Interface on the NT-1 device to the RJ-45 port providing the ISDN BRI connection from the Telecom Company. Connect the S/T Interface on the NT-1 to the ISDN Output ports on KlasTA. (**Note: Klas offers KlasTA II that has two embedded U-Interfaces in it. Using KlasTA II removes the need for an external NT-1 device.**)

3.2. KlasTA

KlasTA is an ISDN Terminal Adaptor (TA) that converts serial data into an ISDN format for use across the public ISDN network. As shown below in Figure 3, KlasTA contains an ISDN NT Input port, two ISDN Output ports and an RS-530 Input Port. Each of the ports is explained below.

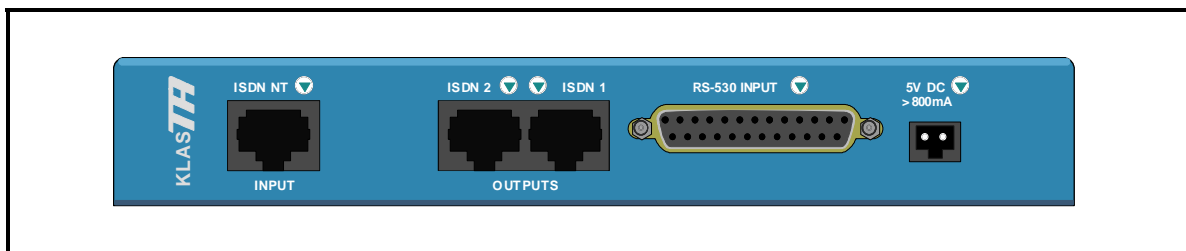


Figure 3. Rear View of Home Side KlasTA

1. The ISDN NT Input port is used as a splitter in order to divide a 128K ISDN Input into two separate 64K ISDN channels for transmission over the ISDN 1 and ISDN 2 Output ports. On the Home Side, there is no need for the ISDN NT Input port.
2. ISDN Output ports 1 and 2 each represent an ISDN BRI connection. Each port can handle two ISDN 64K B-channels for a maximum throughput of 128K per port. Connect the cable coming from the U-Interface on the NT-1 device into these ports.
3. The RS-530 Input port is a synchronous serial DB-25 port. Using the appropriate cable, connect the RS-530 Input port to the KIV-7 or OMNIXi.

3.3. Type-1 Serial Encryption Device

The two most commonly used Type-1 Serial Encryption Devices are the KIV-7 and OMNIXi. Each device accepts classified data through one serial port and then after encrypting the data sends it out another serial port as an unclassified encrypted data stream. The port that sends out encrypted data has a male connector and should be connected to the RS-530 Input port on KlasTA. The port accepting classified data has a female connector and connects to the RS-530 Synchronous Serial device.

3.4. RS-530 Synchronous Serial Router

The data coming from the Mobile Side must be routed to the appropriate destination on the Home Side network. This is accomplished using a router, such as KlasRouter, as a gateway to the rest of the network. Connect the RS-530 Serial port on the router to the serial encryption device. The Mobile and Home Side routers can then establish a PPP or HDLC connection, which will allow the integration of the Mobile Side communications into the entire Home Side network.

MORE INFORMATION

For more information about KlasTA and other Klas products, visit the following Klas website:

<www.klasonline.com>

Copyright © 2006 Klas Ltd. All rights reserved. All company and brand names are trademarks or registered trademarks of their respective owners.

DISCLAIMER OF WARRANTY: THE DOCUMENT IS PROVIDED AS IS, WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, WITH RESPECT TO THE DOCUMENT AND / OR ANY ASSOCIATED ON-LINE INFORMATION, KLAS DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDED BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT.