IPR/S 3.5.1: Diagnostic tools, part 2
Encryption within ETS

Doc.-Type:	Step-by-Step Guide	Doc.-Nr.	9AKK107492A6836	Revision:	A
Department:	BA Engineering	Author:	Engineering Team BA/DESTO		
System:	i-bus® KNX	Product:	IPR/S 3.5.1		
Page:	1/4	Date:	23 April 2020		

Liability Disclaimer:

This document serves the sole purpose of providing additional, technical information and possible application and use cases for the contained products and solutions. It **does not** replace the necessary technical documentation required for planning, installation and commissioning of the product. Technical details are subject to change without notice.

Despite checking that the contents of this document are consistent with the current versions of the related hard and software of the products mentioned within, deviations cannot be completely excluded. We therefore assume no liability for correctness. Necessary corrections will be introduced as and when new versions of the document are generated.

Introduction

The IP Router Secure devices communicate on the Backbone Medium (IP) using encrypted telegrams in “Secure mode.” This is intended to prevent third parties from reading the data.

These step-by-step instructions show ways to verify secure communication on the Router live and to use ETS for diagnostic purposes.

Objectives of the document

- The system integrator is to be shown a method for verifying secure communication between the IP Router Secure devices.
- The system integrator is to be shown a method for decrypting the IP Secure telegrams within ETS for diagnostic purposes.

Content

1. Direct IP connection

The following parameter can be checked for the connection settings in ETS.

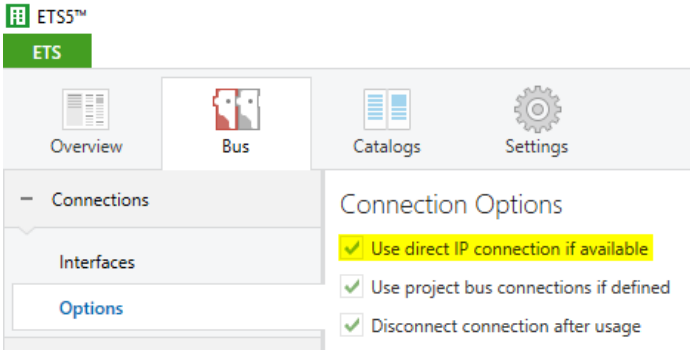


Fig. 1: ETS connection options

If this option is checked, ETS will attempt to set up an IP connection to IP devices and use it to perform device download, for example. Important: telegrams cannot be recorded with the ETS Monitor in this mode.

2. ETS handling of encrypted telegrams

Two places within ETS indicate whether a telegram is sent in encrypted or unencrypted form on the bus. Here is an example based on a configuration with IPR/S 3.5.1 and deactivated function with the direct IP connection (see Fig. 1). The prerequisite is that the “Secure Commissioning” setting is “Active” in the IP Router Secure and that the group or bus monitor is started with the “default” interface. All telegrams recorded in the Monitor will now be automatically decrypted by ETS.

Option 1:
If the user recorded an encrypted telegram with the Monitor, the user must check the properties (right side of the ETS window) of a telegram. The following can be seen in the group monitor recording at first.

#	Time	Service	Flags	Source Address	Destination Address	Rout	Type	Info
151	30.07.2019 10:23:14,537	to bus	E	3.3.200	3.3.0	6	FunctionPropertyCommand (S=0)	ObjectIndex=1, PropertyId=56, Command=00 01

Fig. 2: Telegram encrypted

This telegram looks like a perfectly normal unencrypted telegram at first glance. If the user now clicks on the properties, a new entry named “Data(A+C)” can be found (see Fig. 3). In other words, the telegram is encrypted but ETS immediately displays it in decrypted form for the user.

Property	Value
RawData	2E 00 30 60 33 C8 33 00 12 43 F1 90 00 0B 7E 5B D4 A9 1E A5 FC 98 9E CA A8 5D 08 0B
MessageCode	LDataCon
Source	3.3.200
SourceName	-
Destination	3.3.0
DestinationName	IPR/S3.5.1 IP Router Secure
Acknowledge	Ack
ConfirmFlag	False
RoutingCounter	6
Priority	System
FrameFormat	Extended
Service	to bus
LocalizedType	FunctionPropertyCommand (S=0)
Security	Data(A+C)
SequenceNumber	0
TPCI	T_Data_Connected
DecryptionStatus	Success
SeqNr	49364587689
APCI	APciFunctionPropertyCommand
PropertyObjectIndex	1
PropertyId	56
Command	00 01

Fig. 3: Encrypted telegram

Property	Value
RawData	2E 00 B0 60 33 C8 33 00 01 43 00
MessageCode	LDataCon
Source	3.3.200
SourceName	-
Destination	3.3.0
DestinationName	IPR/S3.5.1 IP Router Secure
Acknowledge	Ack
ConfirmFlag	False
RoutingCounter	6
Priority	System
FrameFormat	Standard
Service	to bus
LocalizedType	DeviceDescriptorRead (S=0)
Security	
SequenceNumber	0
TPCI	T_Data_Connected
APCI	APciDeviceDescriptorRead
DescriptorType	0

Fig. 4: Unencrypted telegram

All properties under the new entry “Data(A+C)” are decoded from the encrypted telegram and cannot be read in any other way without the suitable key. Example of an unencrypted telegram – the “Security” field is empty – (see Fig. 4).

Option 2:
It is additionally possible to add a “Security” column directly in the ETS group monitor by right-clicking the columns of the Monitor – (see Fig. 5). The encryption is then immediately visible in the Monitor (see Fig. 6).

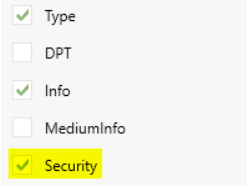


Fig. 5: “Security” column

#	Time	Service	Flags	Source Address	Destination Address	Rout	Type	Info	Security
151	30.07.2019 10:23:14,537	to bus	E	3.3.200	3.3.0	6	FunctionPropertyCommand (S=0)	ObjectIndex=1, PropertyId=56, Command=00 01	Data(A+C)

Fig. 6: Telegram encrypted with security

3. Network card and IP Secure

ETS can additionally send encrypted telegrams on the bus when the network card is selected as the interface. The sent telegrams are doubly encrypted in this case:

1. The telegrams are Data Security encrypted, recognizable by the new entry “Daten(A+C)” (see Fig. 8).
2. The telegrams are additionally packed in a “SecureWrapper” on the IP (see Fig. 7).

Decoding therefore requires the Backbone Key to decrypt the “SecureWrapper” and, in this case, the “tool key” to decrypt communication between ETS and the device. ETS has both and can therefore decrypt communication.

This is readily apparent based on the following screen shots, for example:

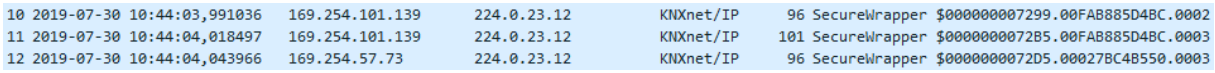
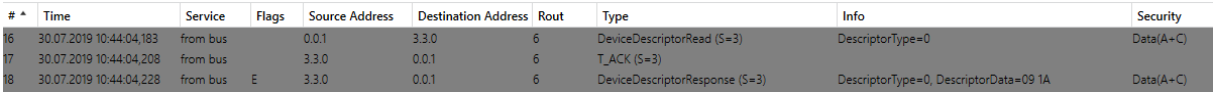


Fig. 7: Wireshark SecureWrapper



#	Time	Service	Flags	Source Address	Destination Address	Rout	Type	Info	Security
16	30.07.2019 10:44:04,183	from bus		0.0.1	3.3.0	6	DeviceDescriptorRead (S=3)	DescriptorType=0	Data(A+C)
17	30.07.2019 10:44:04,208	from bus		3.3.0	0.0.1	6	T_ACK (S=3)		
18	30.07.2019 10:44:04,228	from bus	E	3.3.0	0.0.1	6	DeviceDescriptorResponse (S=3)	DescriptorType=0, DescriptorData=09 1A	Data(A+C)

Fig. 8: Network card recording of ETS group monitor

Fig. 7 shows that the telegrams are IP encrypted. By contrast, Fig. 8 shows that ETS automatically decrypts the telegrams for the user.

Note:
ETS can additionally send encrypted group addresses on the backbone. Select the network card as the interface, start a group monitor and run “Read/Write group address” to do this, for example.
Attention: If the group address setting is “Security – On,” ETS will require a KNX Secure device to send group communication.

References to other documents

- FAQ Home and Building Automation
- Engineering Guide Database