IPR/S 3.5.1: Diagnostic tools, part 1
Verifying secure communication
Diagnostics via Wireshark

GPG BUILDING AUTOMATION					
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:	1/5	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 communicates 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 decrypt the telegrams via Wireshark 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 in the Wireshark network tool for diagnostic purposes.

Content

1. How is it checked in ETS whether secure communication is activated?

For this purpose, select **all** IPR/S 3.5.1 devices contained in the topology in the project and check “Secure Commissioning” under the Properties.

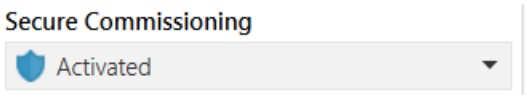

Fig. 1: ETS parameters for “Secure Commissioning”

Secure communication can be checked under the topology properties in Figs. 2 and 3. Communication is regarded as secure when the blue shield + “IP” are visible under “Backbone Medium.” If the blue shield is not visible, the backbone is unencrypted.

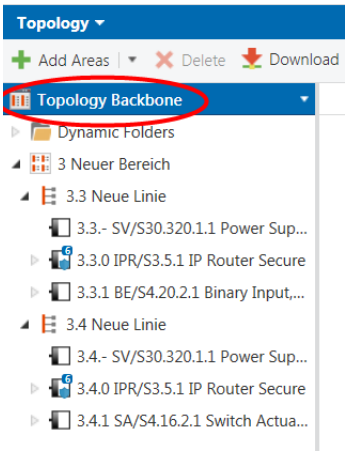

Fig. 2: ETS view

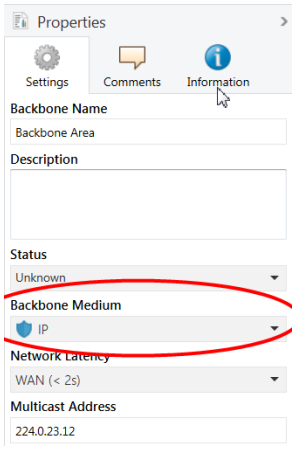

Fig. 3: ETS properties

© ABB
No liability for printing errors.
This version is from the 23 April 2020

2. What do encrypted IP telegrams look like, and how can I verify encryption on an IP telegram recording?

KNXnet/IP telegrams can be recorded using a network tool, such as Wireshark. If the telegrams are encrypted, all relevant information about them, such as the physical address, group address and values, is shown in encrypted form.
See Fig. 4 for this purpose.

In this example, the telegrams are multicast routing telegrams (224.0.23.12).

37	71.096224	169.254.57.73	224.0.23.12	KNXnet/IP	97 SecureWrapper $000009AFD72F.00027BC4B550.0051
38	76.090925	169.254.57.73	224.0.23.12	KNXnet/IP	97 SecureWrapper $000009AFEAB1.00027BC4B550.0052
39	76.150889	169.254.57.73	224.0.23.12	KNXnet/IP	97 SecureWrapper $000009AFEAED.00027BC4B550.0053
40	81.075559	169.254.57.73	224.0.23.12	KNXnet/IP	97 SecureWrapper $000009AFFE2A.00027BC4B550.0054
41	85.139406	169.254.57.73	224.0.23.12	KNXnet/IP	97 SecureWrapper $000009B00E09.00027BC4B550.0055

Fig. 2: Wireshark telegram recording

3. How can encrypted KNX telegrams be decoded in Wireshark for diagnostic purposes?

The Backbone Key is required for decoding!

Caution: A Backbone Key will be generated only if all Routers in the topology are set to “Secure.” See item 1 in this document to check this.

The Backbone Key is provided in ETS via the Reports function under the “Project Security” category.

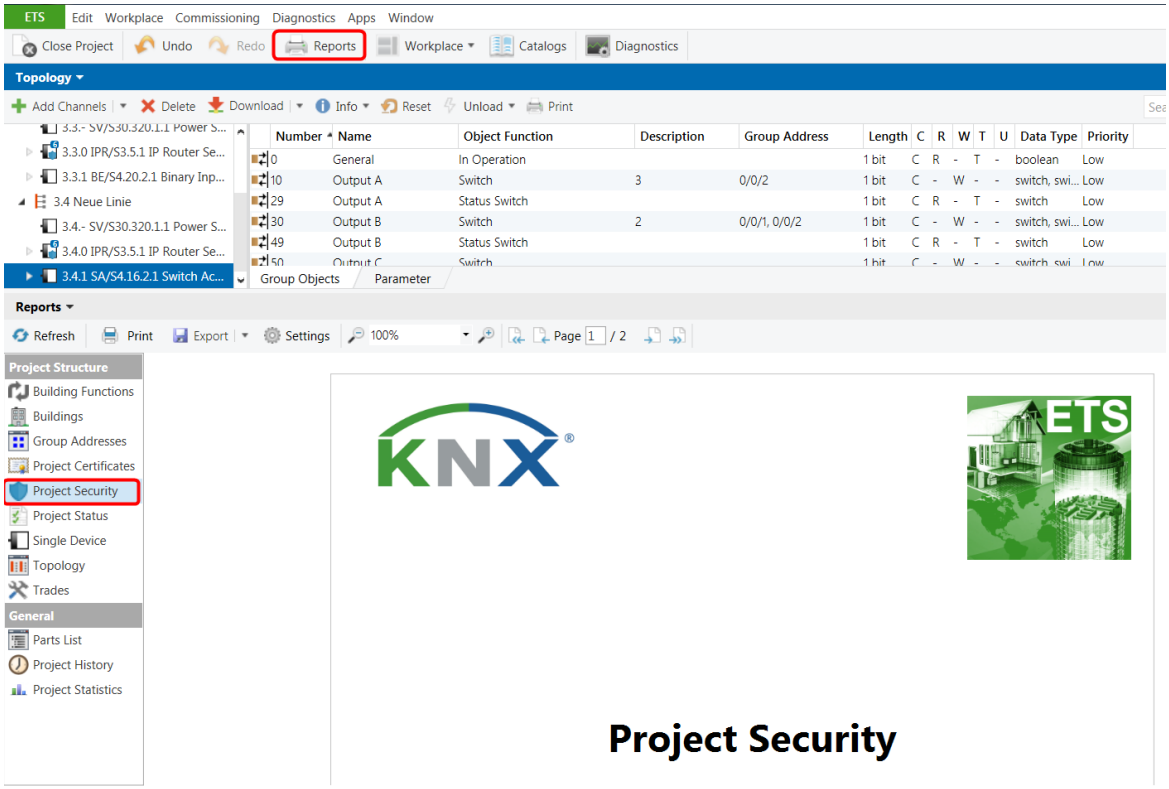

Fig. 3: ETS report

This report includes security relevant information. Please keep it protected.

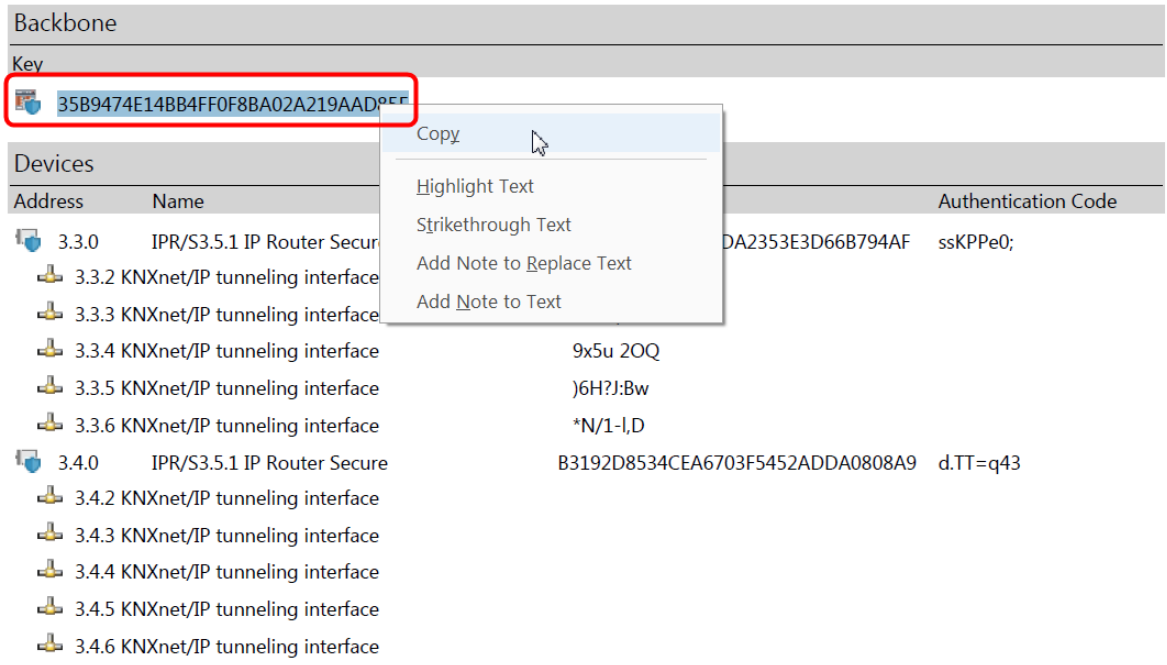

Fig. 4: Copying Backbone Key

This key is added in Wireshark to decode the telegrams. It is a good idea to save the report as a PDF file, because the keys can be copied here.
To do this, right-click an encrypted telegram and select “Key file…” under the protocol settings (Fig. 7).

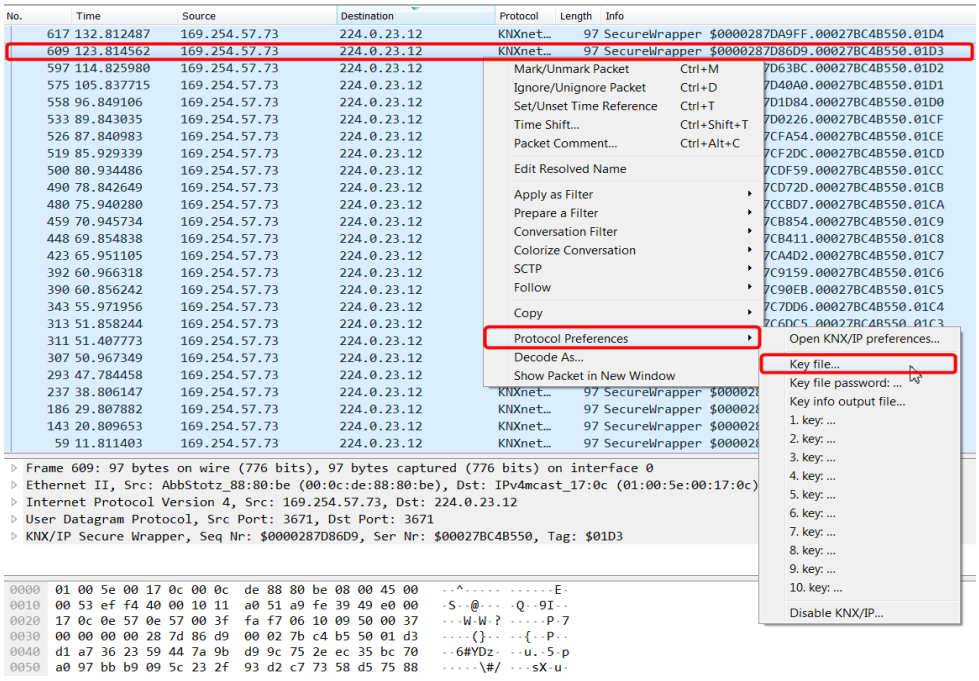

Fig. 5: Decoding telegrams in Wireshark

Now, copy the key and paste it into the “1.key” field.

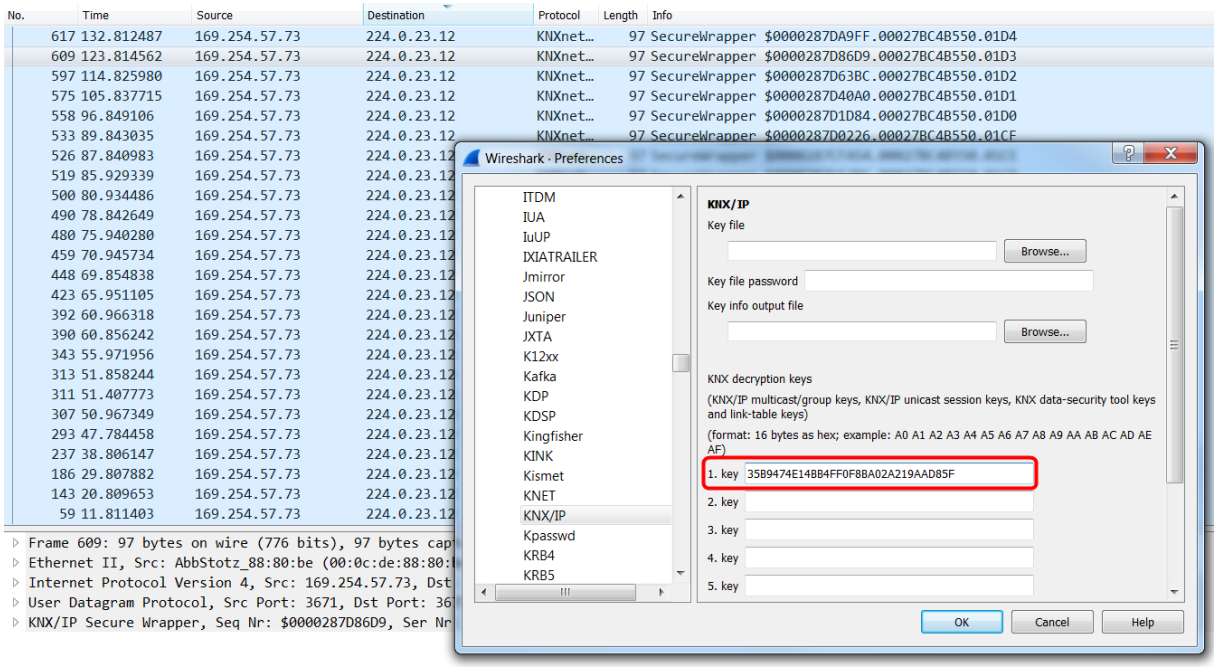

Fig. 6: Wireshark – pasting the key

All KNX telegrams encoded using this key will now be decrypted.

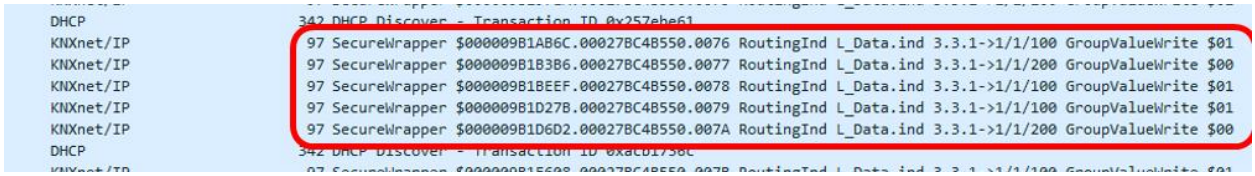

Fig. 7 Decrypted telegrams in Wireshark

All relevant information about the KNXnet/IP telegram will now be visible (Fig. 9).

References to other documents

- FAQ Home and Building Automation
- Engineering Guide Database