IPR/S 3.5.1: Diagnosetools Teil 1

Sichere Kommunikation verifizieren

Diagnose via Wireshark

GPG BUILDING AUTOMATION					
Dok.-Typ:	Schritt-für-Schritt Anleitung	Dok.-Nr.	9AKK107492A6836	Revision:	A
Abteilung:	BA Engineering	Autor:	Engineering Team BA/DESTO		
System:	i-bus KNX	Produkt:	IPR/S 3.5.1		
Seite:	1/5	Datum:	07. Aug. 2019		

Haftungsausschluss:

Dieses Dokument dient zur technischen Information und soll Anregungen zum Einsatz geben.

Es ersetzt nicht die technischen Informationen zur Projektierung, Montage und Inbetriebnahme des Produkts. Technische Änderungen und Irrtümer sind vorbehalten.

Trotz Überprüfung des Inhalts dieser Druckschrift auf Übereinstimmung mit der Hard- und Software können Abweichungen nicht vollkommen ausgeschlossen werden. Daher können wir hierfür keine Gewähr übernehmen. Notwendige Korrekturen fließen in neue Versionen des Dokuments ein.

Einführung

Die IP-Router Secure unterhalten sich im „Secure-Modus“ auf dem Backbone Medium (IP) mit verschlüsselten Telegrammen. Dies soll Dritte daran hindern die Daten auszulesen.

Diese Schritt-für-Schritt Anleitung zeigt Wege auf, um die sichere Kommunikation der Router live zu verifizieren und via Wireshark für Diagnosezwecke die Telegramme zu entschlüsseln.

Ziel des Dokuments

- Dem Systemintegrator soll eine Möglichkeit zur Verifizierung der sicheren Kommunikation zwischen den IP-Router Secure aufgezeigt werden.
- Dem Systemintegrator soll eine Möglichkeit zur Entschlüsselung der IP Secure Telegrammen in dem Netzwerktool Wireshark für Diagnosezwecke aufgezeigt werden.

Inhalt

1. **Wie wird in der ETS überprüft, ob die sichere Kommunikation aktiviert ist?**

   Hierzu **alle** im Projekt befindlichen IPR/S 3.5.1 in der Topologie anwählen und unter den Eigenschaften die „Sichere Inbetriebnahme“ prüfen.

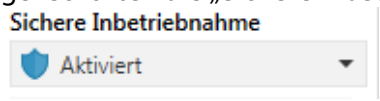

Abb. 1 ETS-Parameter für "Sichere Inbetriebnahme"

In den Eigenschaften der Topologie Abb. 2 und 3 kann die sichere Kommunikation überprüft werden. Die Kommunikation gilt dann als sicher, wenn unter Backbone Medium das blaue Wappen + IP steht. Ist das blaue Wappen nicht zu sehen, so ist der Backbone unverschlüsselt.

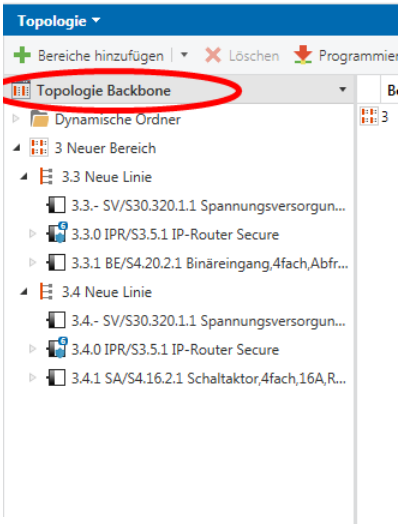

Abb. 3 Ansicht ETS

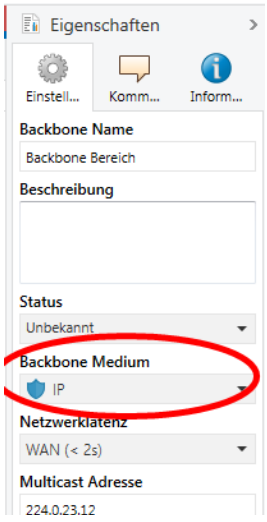

Abb. 2 Eigenschaften ETS

2. Wie sehen verschlüsselte IP-Telegramme aus und wie kann ich die Verschlüsselung auf einer IP Telegrammaufzeichnung verifizieren?

Mit einem Netzwerktool wie z.B. Wireshark können KNXnet/IP Telegramme aufgezeichnet werden. Sind diese verschlüsselt sind alle relevanten Infos zu dem Telegramm wie physikalische Adresse, Gruppenadresse und deren Wertigkeit verschlüsselt dargestellt.
Siehe hierzu Abb. 4.

In diesem Beispiel handelt es sich um Multicast Routing Telegramme. (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

Abb. 4 Wireshark Telegrammaufzeichnung

3. Wie kann man verschlüsselte KNX-Telegramme in Wireshark zu Diagnosezwecke decodieren?

Für die Decodierung ist der Backboneschlüssel erforderlich!

Achtung: Ein Backboneschlüssel wird nur generiert, wenn alle Router in der Topologie auf „Secure“ eingestellt sind. Zur Überprüfung siehe hierzu Punkt 1 des Dokuments.

Der Backboneschlüssel wird in der ETS über die Reportfunktion unter der Kategorie Sicherheit zur Verfügung gestellt.

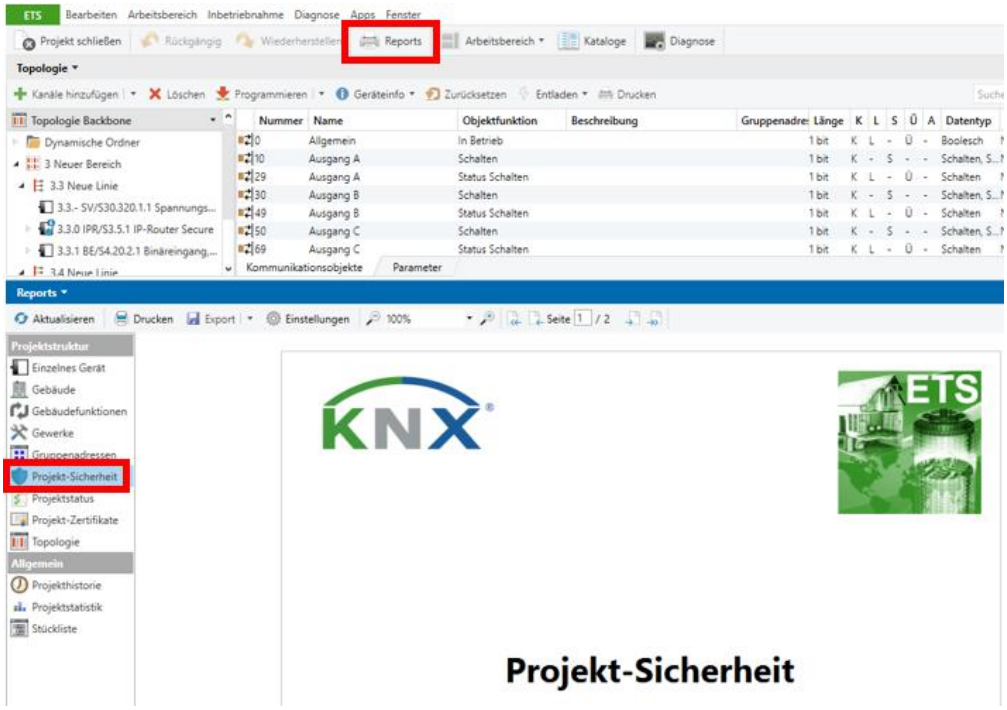

Abb. 5 ETS Report

Dieser Report enthält sicherheitsrelevante Daten. Bitte bewahren Sie ihn geschützt auf.

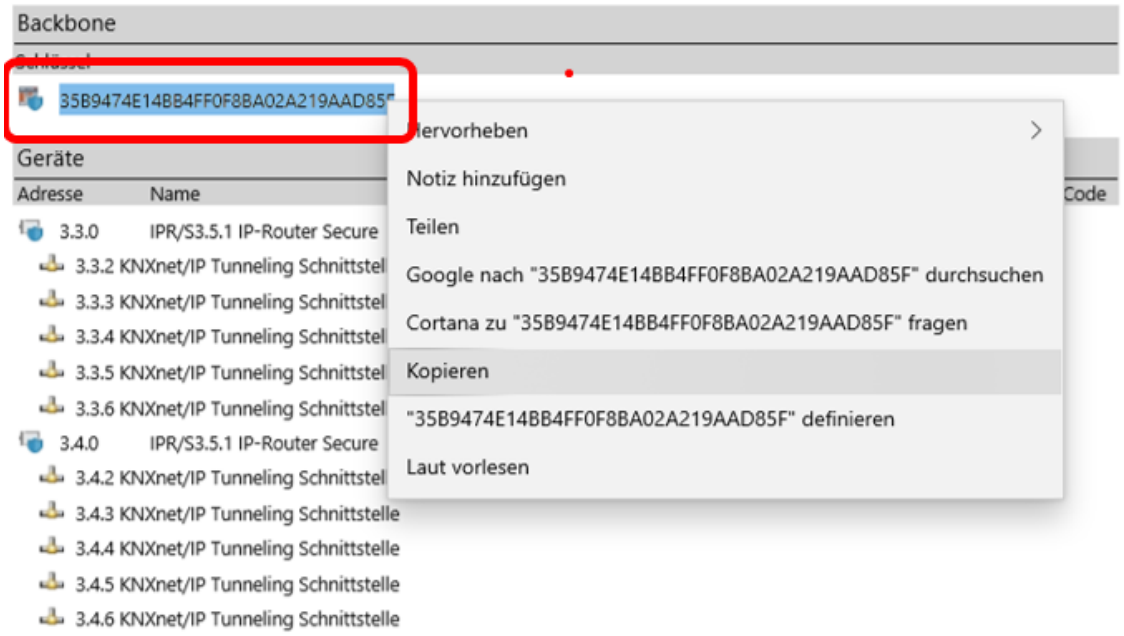

Abb. 6 Backboneschlüssel kopieren

Dieser Schlüssel wird in Wireshark eingefügt um die Telegramme zu decodieren. Es bietet sich an den Report als .PDF Datei abzuspeichern, da hier die Schlüssel kopiert werden können.
Hierzu ein verschlüsseltes Telegramm mit der rechten Maustaste anklicken und unter Protokolleinstellungen „Key file…“ wählen (Abb. 7).

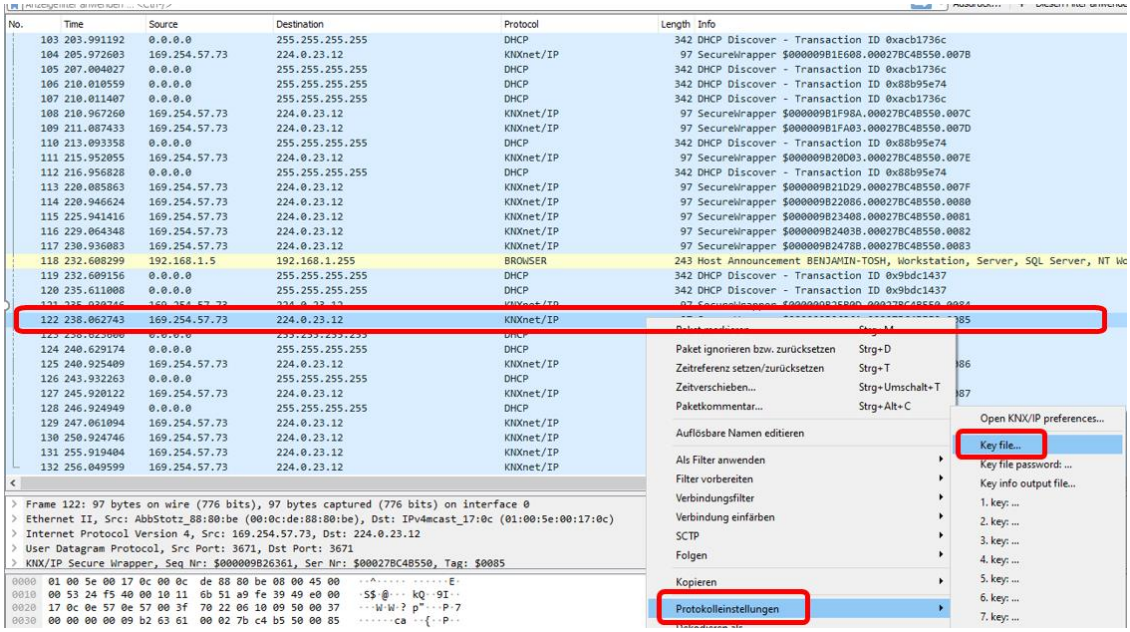

Abb. 7 Telegramme in Wireshark decodieren

Nun den Schlüssel kopieren und in das Feld „1. Key“ einfügen.

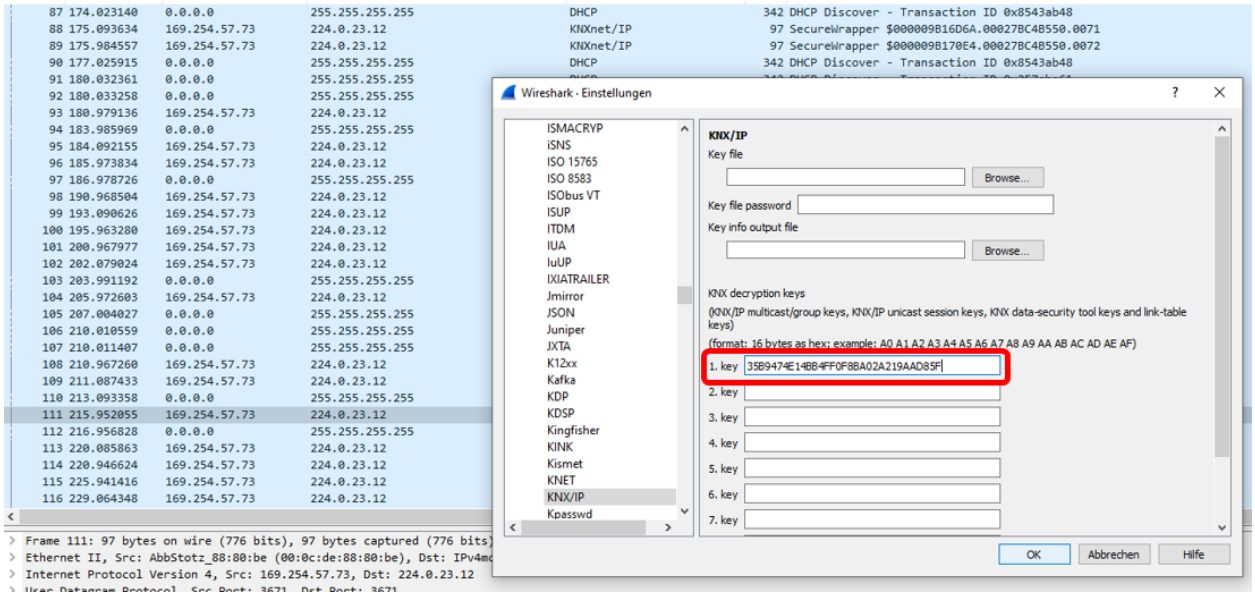

Abb. 8 Wireshark - Key einfügen

Nun werden alle KNX-Telegramme, die über diesen Schlüssel codiert waren entschlüsselt.

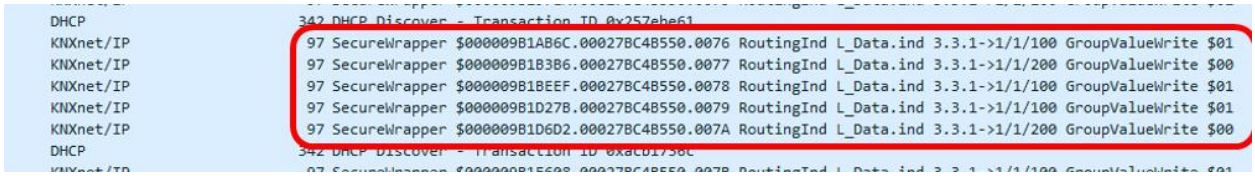

Abb. 9 Entschlüsselte Telegramme in Wireshark

Alle relevanten Infos zu dem KNXnet/IP Telegramm sind nun sichtbar (Abb. 9).

Verweise auf andere Dokumente

- FAQ Home and Building Automation
- Engineering Guide Database
- Video: IP-Router Secure Inbetriebnahme