IPR/S 3.5.1: Diagnosetools Teil 2
Verschlüsselung innerhalb der ETS

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:	1/4	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 die ETS für Diagnosezwecke zu nutzen.

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 Telegramme innerhalb der ETS für Diagnosezwecke aufgezeigt werden.

Inhalt

1. Direkte IP-Verbindung

In der ETS gibt es die Möglichkeit bei den Verbindungseinstellungen den Haken bei folgendem Parameter zu setzen.

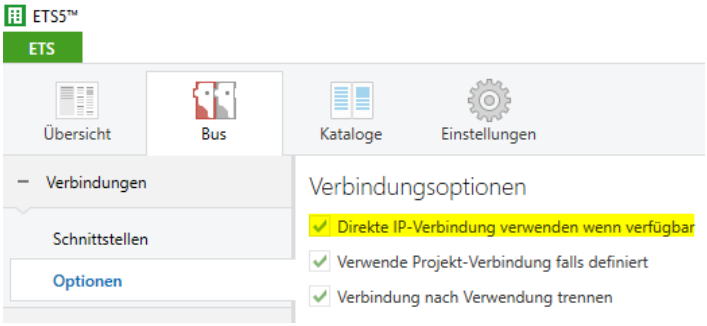

Abb. 1 Verbindungsoptionen ETS

Ist dieser Haken gesetzt, wird die ETS versuchen eine IP-Verbindung mit IP-Geräten aufzubauen und darüber z.B. den Gerätedownload ausführen. Es ist wichtig zu wissen, dass in diesem Modus keine Telegrammaufzeichnungen mit dem ETS Monitor möglich sind.

2. ETS Handling von verschlüsselten Telegrammen

Man kann innerhalb der ETS an zwei Stellen erkennen, ob ein Telegramm verschlüsselt oder unverschlüsselt auf dem Bus versendet wird. Hierzu ein kleines Beispiel anhand einer Konfiguration mit IPR/S 3.5.1 und deaktivierter Funktion bei der direkten IP-Verbindung (siehe Abb. 1). Voraussetzung ist, dass der IP-Router Secure in der Einstellung „Sichere Inbetriebnahme“ auf „Aktiviert“ steht und man den Gruppen- oder Busmonitor mit der „Default“ Schnittstelle startet. Jetzt werden alle Telegramme, die im Monitor aufgezeichnet werden, automatisch von der ETS entschlüsselt.

Option 1:
Hat man ein verschlüsseltes Telegramm mit dem Monitor aufgezeichnet, muss man in den Eigenschaften (rechte Seite des ETS Fensters) eines Telegramms nachsehen. Zunächst kann man im Gruppenmonitormitschnitt Folgendes sehen.

#	Zeit	Dienst	Flags	Quelladresse	Zieladresse	Rout	Typ	Info
153	29.07.2019 11:11:47,316	zum Bus	E	3.3.200	3.3.0	6	FunctionPropertyCommand (S=0)	ObjectIndex=1, PropertyId=56, Command=00 01

Abb. 2 Telegramm verschlüsselt

Dieses Telegramm sieht, auf den ersten Blick, wie ein ganz normales unverschlüsseltes Telegramm aus. Klickt man jetzt in die Eigenschaften findet sich ein Zusatz mit dem Namen „Daten(A+C)“ (siehe Abb. 3). Das heißt, dass das Telegramm verschlüsselt ist, aber die ETS es sofort für den Nutzer entschlüsselt darstellt.

Eigenschaft	Wert
RawData	2E 00 30 60 33 C8 33 00 12 43 F1 90 00 08 79 61 F0 D6 56 F7 D7 BE 92 12 E4 1C B6 11
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	zum Bus
LocalizedType	FunctionPropertyCommand (S=0)
Security	Daten(A+C)
SequenceNumber	0
TPCI	T_Data_Connected
DecryptionStatus	Success
SeqNr	49281102038
APCI	APciFunctionPropertyCommand
PropertyObjectIndex	1
PropertyId	56
Command	00 01

Abb. 3 Verschlüsseltes Telegramm

Eigenschaft	Wert
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	zum Bus
LocalizedType	DeviceDescriptorRead (S=0)
Security	
SequenceNumber	0
TPCI	T_Data_Connected
APCI	APciDeviceDescriptorRead
DescriptorType	0

Abb. 4 Unverschlüsseltes Telegramm

Alle unter dem Zusatz „Daten(A+C)“ stehenden Eigenschaften sind aus dem verschlüsselten Telegramm heraus dekodiert und können ohne den passenden Schlüssel sonst nicht gelesen werden! Ein Beispiel eines unverschlüsselten Telegramms – das Feld „Security“ ist leer – (siehe Abb. 4).

Option 2:
Es ist auch möglich, direkt im ETS Gruppenmonitor eine Spalte „Sicherheit“ einzufügen – mit Rechtsklick auf die Spalten des Monitors klicken – (siehe Abb. 5). Dann ist sofort im Monitor die Verschlüsselung sichtbar (siehe Abb. 6).

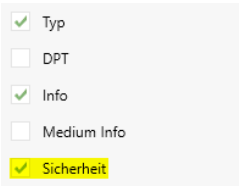

Abb. 5 Spalte "Sicherheit"

#	Zeit	Dienst	Flags	Quelladresse	Zieladresse	Rout	Typ	Info	Sicherheit
153	29.07.2019 11:11:47,316	zum Bus	E	3.3.200	3.3.0	6	FunctionPropertyCommand (S=0)	ObjectIndex=1, PropertyId=56, Command=00 01	Daten(A+C)

Abb. 6 Telegramm verschlüsselt mit Sicherheit

3. Netzwerkkarte und IP Secure

Die ETS kann auch, mit ausgewählter Netzwerkkarte als Schnittstelle, verschlüsselte Telegramme auf den Bus senden. In diesem Fall sind die versendeten Telegramme doppelt verschlüsselt:

1. Die Telegramme sind Data Security verschlüsselt, ersichtlich an dem Zusatz „Daten(A+C)“ (siehe Abb. 8)
2. Die Telegramme sind zusätzlich noch einmal in einen „SecureWrapper“ auf IP eingepackt (siehe Abb. 7)

Zum Dekodieren braucht man also den Backbone Key um die „SecureWrapper“ zu entschlüsseln und in diesem Fall den „Tool Key“ um die Kommunikation zwischen ETS und Gerät zu entschlüsseln. Beides hat die ETS verfügbar und kann deswegen die Kommunikation entschlüsseln!

Beispielsweise anhand folgender Screenshots gut erkennbar:

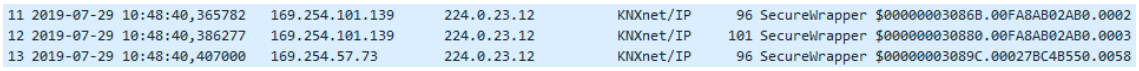

Abb. 7 SecureWrapper Wireshark

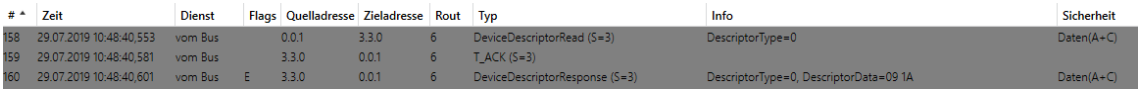

Abb. 8 Netzwerkkartenmitschnitt ETS Gruppenmonitor

Man sieht auf der Abbildung 7, dass die Telegramme auf IP verschlüsselt sind. Im Gegensatz dazu, erkennt man auf der Abbildung 8, dass die ETS für den Nutzer die Telegramme automatisch dekodiert.

Hinweis:
Die ETS ist in der Lage auch Gruppenadressen verschlüsselt mit dem Backbone zu versenden. Dazu beispielsweise die Netzwerkkarte als Schnittstelle auswählen, einen Gruppenmonitor starten und „Gruppenadresse Lesen/Schreiben“ ausführen.
Achtung, wenn die Gruppenadresse die Einstellung „Security – On“ hat, benötigt die ETS ein KNX Secure Gerät um Gruppenkommunikation zu versenden.

Verweise auf andere Dokumente

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