www.knx.org

KNX Security

Position Paper

Contents

1 Introduction

This paper is intended as a guide for both installers as well as KNX manufacturers to learn about the current measures that can be undertaken to increase security of KNX installations.

2 Preventing access to the network to the various KNX physical media

2.1.1 Introduction

A proper security concept is based on ensuring proper prevention against unauthorized access. In case of a KNX installation this implies that only authorized persons (the installer, caretaker, user) shall have physical access to the KNX installation. When designing and installing, for each KNX medium the critical elements shall be protected in the best way possible.

2.1.2 Installation of cable and devices

- Generally, applications and devices shall be properly fixed to avoid that they can be easily removed, in this way allowing unauthorized persons access to a KNX installation.
- Enclosures and distribution boards containing KNX devices shall be properly closed or be mounted in rooms, to which only authorized persons have access.
- In outside areas devices shall be mounted in sufficient heights (e.g. weather station, wind sensor, movement detector, …).
- In all public areas that are not sufficiently surveilled, it shall be contemplated to make use of conventional devices in connection with binary inputs mounted in protected areas (e.g. in distribution boards) or push button interfaces, in this way preventing access to the bus.
- When available, anti-theft measures provided by certain Application Modules should be used (e.g. securing devices by screws, only removable with tools, high pull-off resistance, …).

2.1.3 Twisted Pair

- Cable ends should not be visible, hanging outside the wall on the out- or inside of the building.
- Bus cable in outside areas poses a higher risk. Physical access to KNX Twisted Pair cable shall in this case be made even more difficult than in the home/building itself.
- For extra protection, devices installed in areas with limited surveillance (outside, underground parking lot, toilet, etc.) can be connected to an extra line. By activation of the filter table in line couplers according clause, it can be prevented that hacker is able to access the entire installation.

2.1.4 Powerline

- Electronic filters should be used to filter incoming - and outgoing signals.

2.1.5 Radio Frequency

- As Radio Frequency is an open medium, *physical* protection measures cannot be taken to prevent access. For this, other measures need to be taken that are outlined in clauses 3 to 6 (and especially those listed in clause5).

2.1.6 IP

- Building Automation should run over a dedicated LAN and WLAN with own hardware (routers, switches, etc.).
- Regardless of the type of KNX installation, one shall at any rate observe the usual protection mechanisms for IP networks. These may include:
  - MAC filters
  - Encryption of wireless networks in conjunction with strong passwords (change of the default password – WPA2 or higher) and protection of them against unauthorized persons.
  - Change of the default SSID (SSID is the name, under which a wireless access point is visible in the network, mostly manufacturer and product type). Default SSIDs can point to product specific weaknesses of the used access points and are in this way particularly vulnerable to hackers). The access point can moreover be set in such a way that beaconing (periodical transmission of amongst others the SSID) is prevented.
- For KNX IP multicast another IP address shall be used as the default one (224.0.23.12). A suitable address can be agreed upon with the network administrator.
- IT network specialists shall be involved in larger size projects with connection to KNXnet/IP: in this way the network configuration can still be optimized (managed switches, virtual LAN, access points with IEEE 802.X, etc.) and further protection mechanisms like E-Mail filtering and anti-virus can be implemented.

2.1.7 Internet

- KNXnet/IP Routing and KNXnet/IP Tunnelling are not designed for use over the Internet. Because of that, it is not advisable to open ports of routers towards the internet, in this way making KNX communication visible over the Internet.
  - The (W)LAN installation shall be protected by means of a firewall.
  - In case no external access to the installation is necessary, the default gateway can be set to 0, in this way blocking any communication to the internet.
- When one wishes to realize access to an installation via internet, this can be realized in the following way:
  - Ensuring access to the KNX installation through VPN connections: this however requires a router that supports VPN server functionality or a server with VPN functionality.
  - Any of the dedicated manufacturer specific solutions available in the market and visualisations (e.g. allowing http access).
  - KNX is currently in the specification phase with the goal to lay down a KNX standardized solution for accessing to KNX installations over the internet via web services.

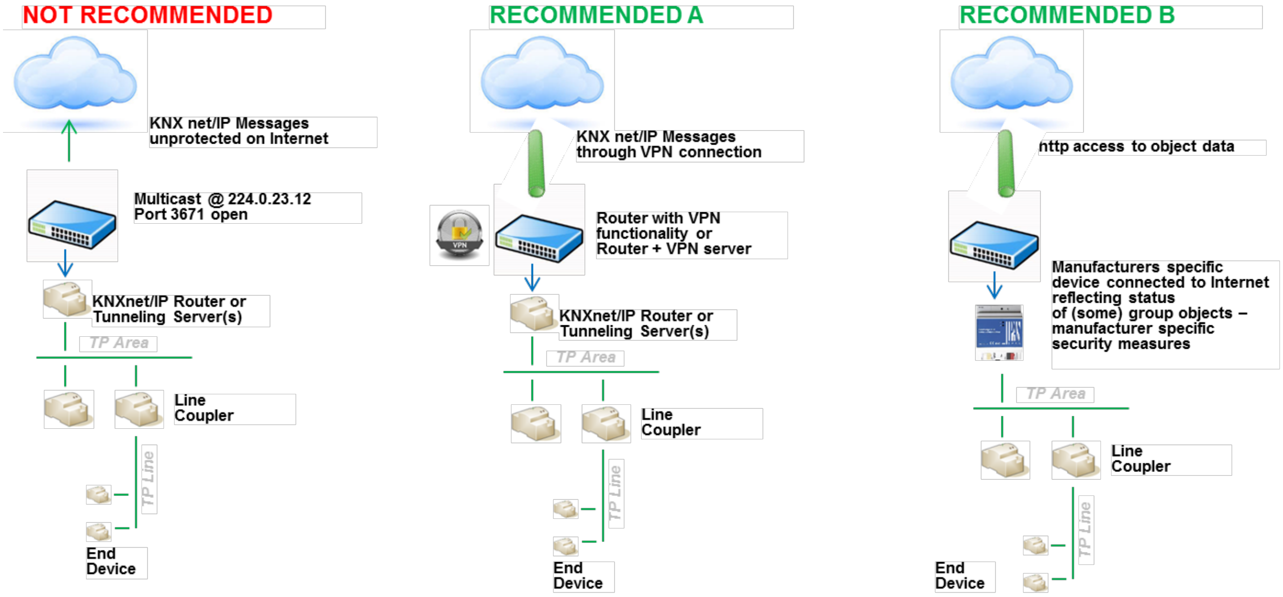

NOT RECOMMENDED
KNX net/IP Messages unprotected on Internet
Multicast @ 224.0.23.12 Port 3671 open
KNXnet/IP Router or Tunneling Server(s)
TP Area
Line Coupler
TP Line
End Device
RECOMMENDED A
KNX net/IP Messages through VPN connection
VPN
Router with VPN functionality or Router + VPN server
KNXnet/IP Router or Tunneling Server(s)
TP Area
Line Coupler
TP Line
End Device
RECOMMENDED B
http access to object data
Manufacturers specific device connected to Internet reflecting status of (some) group objects – manufacturer specific security measures
TP Area
Line Coupler
TP Line
End Device

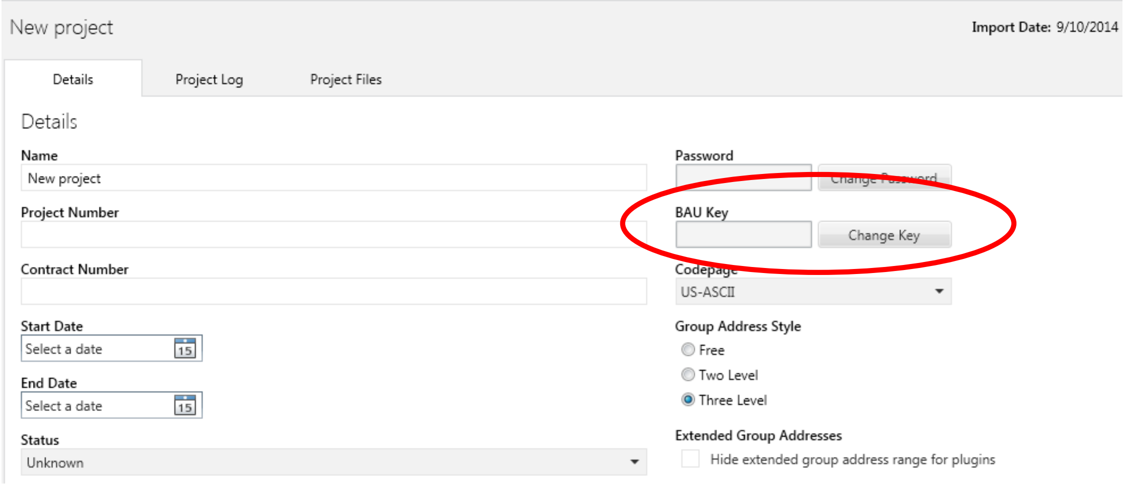
Figure 1: Access to KNX networks via Internet

3 Limiting unwanted communication inside the network

- The Individual Addresses of devices shall be properly assigned according to the topology and the Routers shall be configured not to pass message with inappropriate Source Address. In this way, unwanted communication can be limited to a single line.
- Point-to-point and possibly broadcast communication across Routers should be blocked. In this way, reconfiguration can again be limited to a single line.
- The Couplers shall be configured to use the Filter Tables actively and not pass Group Addresses that are not used inside a specific line. If not, communication inserted into a specific line risks spreading uncontrolled over the entire KNX installation.

4 Protecting configuration communication

- ETS allows defining a project specific password by means of which one can lock devices for unauthorized access. This prevents that the installation configuration can be read out or modified by unauthorised persons.



New project

Import Date: 9/10/2014

Details

Name: New project

Project Number:

Contract Number:

Start Date: Select a date

End Date: Select a date

Status: Unknown

Password:

BAU Key:

Codepage: US-ASCII

Group Address Style
○ Free
○ Two Level
● Three Level

Extended Group Addresses
□ Hide extended group address range for plugins

Figure 2: Protecting configuration communication in ETS

5 Protecting runtime communication

- KNX runtime communication can be protected via the specified
  - KNX Data Security and
  - KNX IP Secure mechanisms
- KNX Data Security ensures that regardless of the KNX medium selected messages sent by KNX devices can be authenticated and/or encrypted.
  In order to ensure that even in the case where such communication would not be secured and such networks would be connected to IP, the KNX IP Secure mechanisms were defined on top of this.
  In this way, it is ensured that KNX IP tunnelling or routing messages cannot be recorded or manipulated on IP. The KNX IP Secure mechanisms ensure that a security wrapper is added around the complete KNXnet/IP data traffic.

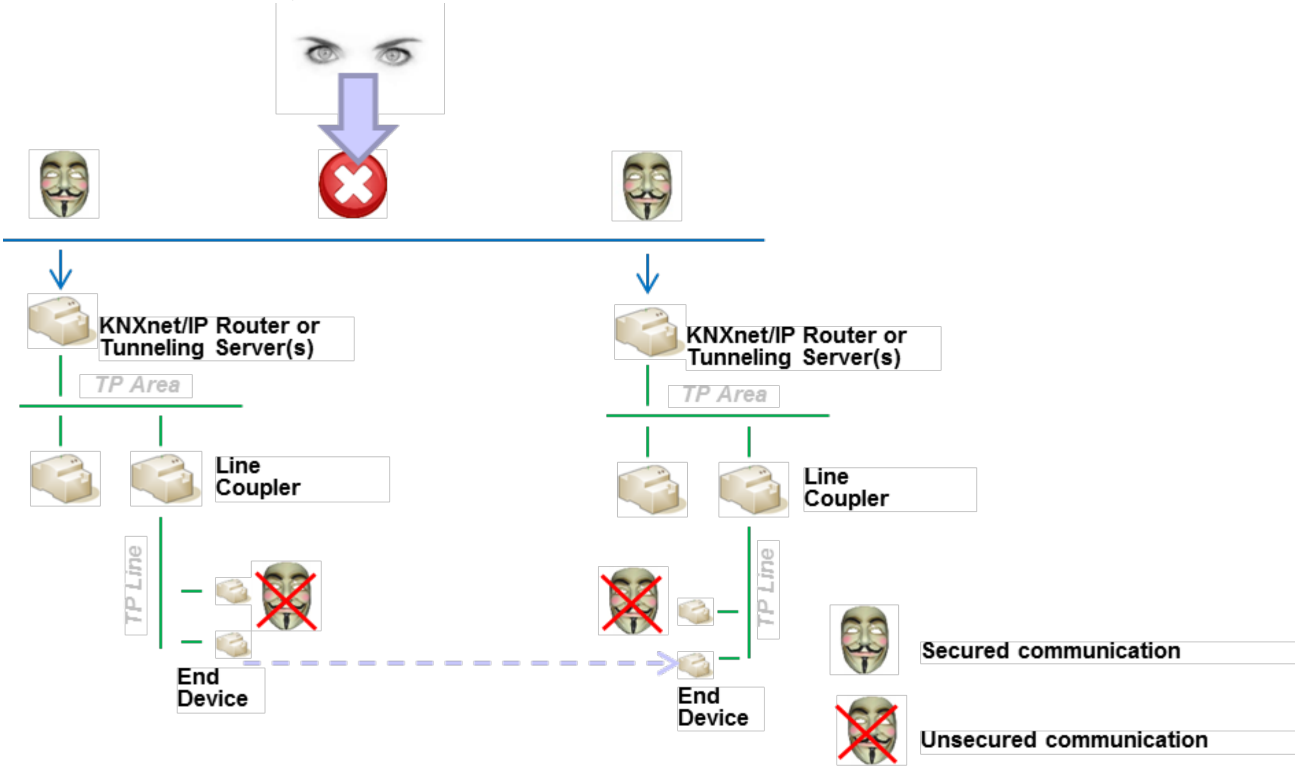


Figure 3: Protecting KNX run time communication on an IP network with KNXnet IP Security

- The KNX Data Security and KNX IP Secure Mechanisms ensure that:
  Devices can establish a Secured Communication Channel thereby ensuring:
  - *Data Integrity*, i.e. preventing an attacker from gaining control by injecting manipulated frames. In KNX this is ensured by appending an **authentication** code to every message: this appended code allows verification that the message has not be modified and that it effectively originates from the trusted communication partner.
  - *Freshness*, i.e. preventing an attacker from recording frames and playing them back at a later time without manipulating the content. In KNX Data Security this is ensured by a sequence number and in KNX IP Secure by a sequence identifier.
  - *Confidentiality*, i.e. encrypting network traffic to ensure that an attacker has the lowest possible insight into the data actually transmitted. When allowing **encrypting** KNX network traffic, the KNX devices ensure at least encryption according to the AES-128 CCM algorithms together with a symmetrical key.

A symmetrical key means that the same key is used by the sender to protect an outgoing message (authentication + confidentiality!) as well as by the receiver(s) to verify when receiving this message.

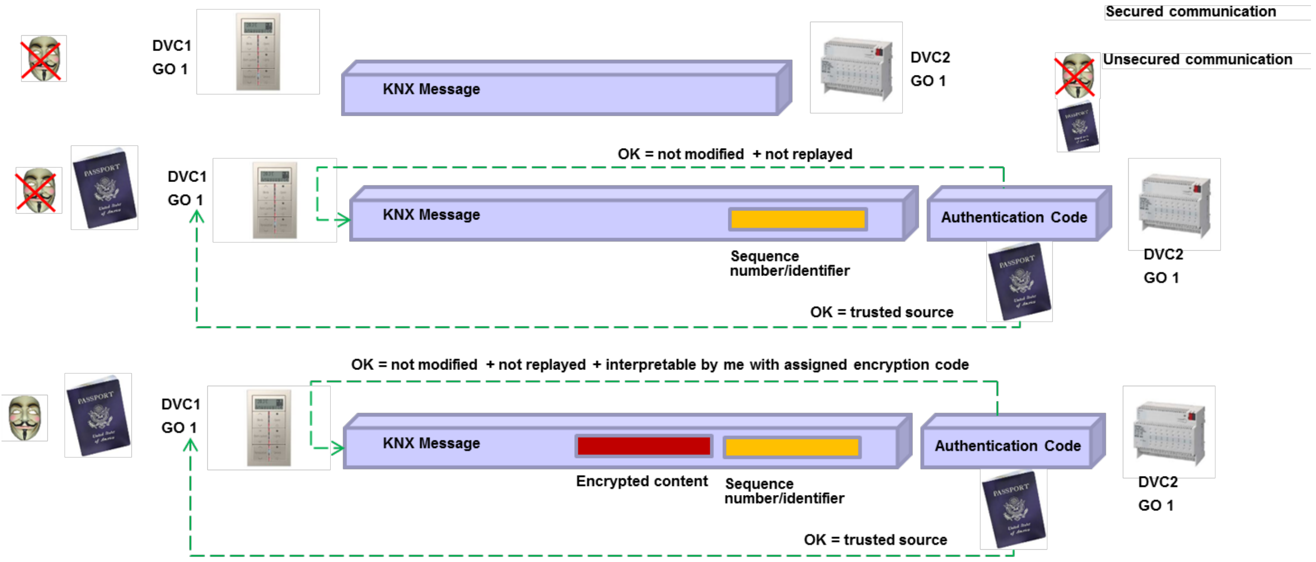


Figure 3: Overview of the KNX Data Security Mechanisms

For KNX Data Security, the devices are protected in the following way:

- A device is shipped with a unique Factory Device Set up Key (FDSK).
- The installer enters this FDSK into the configuration tool ETS (this action is at any rate not done via the bus).
- The configuration tool creates a project specific tool key.
- Via the bus, the ETS sends to the device to be configured its tool key, however by encrypting and authenticating this message with the previously entered FDSK. Neither the tool nor the FDSK key are at any time transmitted in plain text on the bus.
- The device from then onwards only accepts the tool key for further configuration with the ETS. The FDSK is no longer used during subsequent communication.
- The ETS creates runtime keys (as many as necessary) for the group communication that needs to be secured.
- Via the bus, ETS sends to the device to be configured these runtime keys, however by encrypting and authenticating these messages with the tool key. The runtime keys are never transmitted in plain text on the bus.

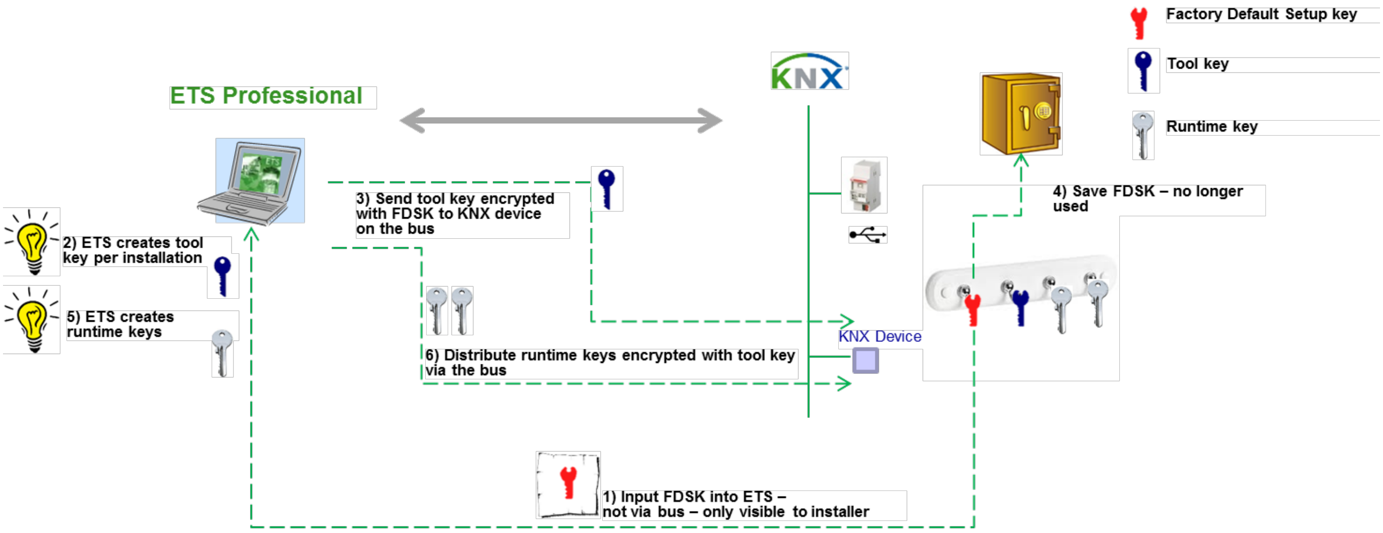

Factory Default Setup key
Tool key
Runtime key
ETS Professional
KNX
2) ETS creates tool key per installation
5) ETS creates runtime keys
3) Send tool key encrypted with FDSK to KNX device on the bus
4) Save FDSK – no longer used
KNX Device
6) Distribute runtime keys encrypted with tool key via the bus
1) Input FDSK into ETS – not via bus – only visible to installer

Figure 4: Procedure for securing KNX devicees

For KNX IP Secure, a secure connection (Tunnelling or Device Management) is established in the following way:

- Both the client as well as the server creates an individual public/private key pair. This is referred to as an asymmetrical encryption.
- The client sends its public key to the server as plain text.
- The server responds with its public key in plain text, appended with the result of the following calculation: it calculates the XOR value of its server public key with the client’s public key, encrypts this with the device code to authentify itself to the client and encrypts this a second time with the calculated session key.

  The device authentication code is either assigned by the ETS during configuration or the tool key. This device authentication code needs to be provided to the operator of the visualisation wishing to establish a secure connection with the relevant server.
- The client performs the same XOR operation, but authorizes itself by encrypting this firstly with one of the passwords of the server and again a second time with the session key.
  It shall be noted that the encryption algorithm used (Diffie Hellmann) ensured that the session key of the client and the server are identical.

  The passwords of the server need to be provided to the operator of the visualisation wishing to establish a secure connection with the relevant server.

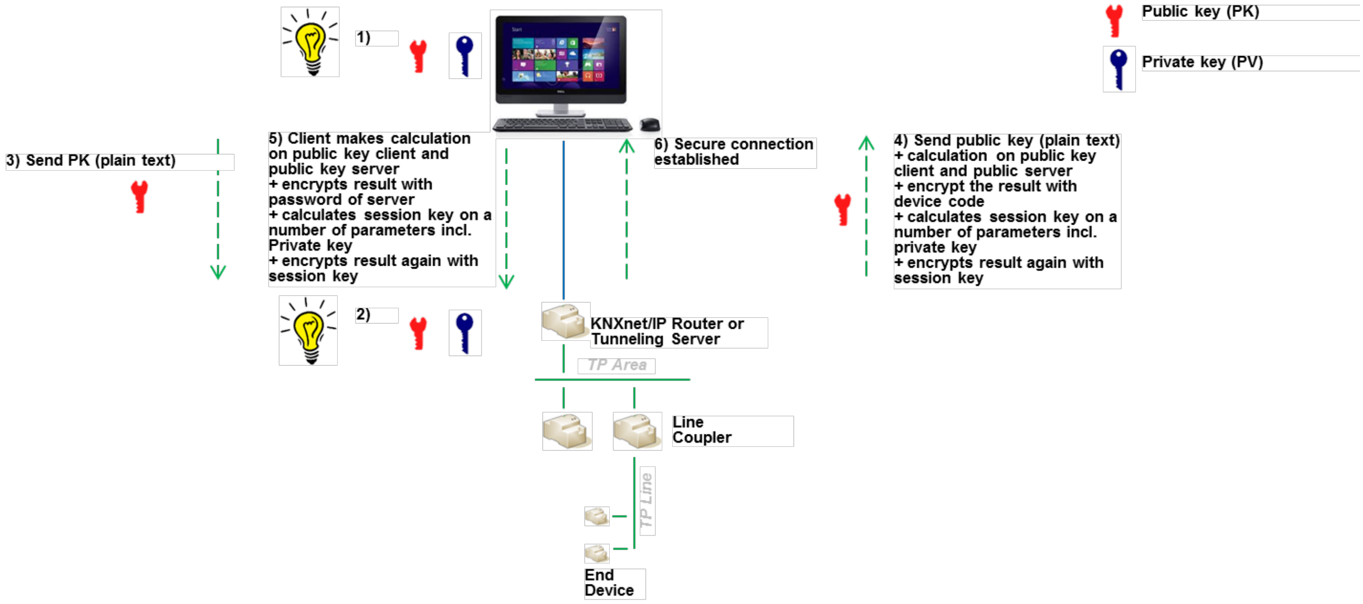

1)
Public key (PK)
Private key (PV)
3) Send PK (plain text)
5) Client makes calculation on public key client and public key server + encrypts result with password of server + calculates session key on a number of parameters incl. Private key + encrypts result again with session key
6) Secure connection established
4) Send public key (plain text) + calculation on public key client and public server + encrypt the result with device code + calculates session key on a number of parameters incl. private key + encrypts result again with session key
2)
KNXnet/IP Router or Tunneling Server
TP Area
Line Coupler
TP Line
End Device

Figure 5: Setting up a KNX IP Secure Connection

6 Coupling KNX to security systems

When coupling KNX to such applications like burglar/fire protection/door opening systems, this can be ensured through:

- KNX devices or interfaces with appropriate certification by local loss insurers;
- potential free contacts (binary inputs, push button interfaces, …);
- appropriate interfaces (RS232, …) or gateways: in this case it shall be ensured that the KNX communication is unable to trigger security relevant functions in the security part of the installation.

7 Detecting unauthorised bus access

- Obviously, the bus could be monitored and unusual traffic could be traced.
- Some device types can detect if another device sends Telegrams with their Individual Address. This is not spontaneously announced in the network, but it can be read in PID_DEVICE_CONTROL.
- Very recent implementation may already exhibit the PID_DOWNLOAD_COUNTER. Comparing the read out value (periodically) with a reference value will signal changes in the device configuration.

8 Literature

[1] AN 158 v02 KNX Data Security DP Version

[2] AN 159 v04 KNX IP Secure DP Version

[3] Volume 3/8/x KNXnet/IP Specifications – KNX Standard Version 2.1