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 via the KNX physical media

2.1.1 Twisted Pair

- Cable ends should not be visible, hanging outside the wall on the out- or inside of the building.
- Appliances should be fix-mounted, so that they cannot be easily removed to allow accessing the cable.
- When possible, anti-theft measures provided by certain Application Modules should be used.

2.1.2 Powerline

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

2.1.3 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 clause 5).

2.1.4 IP

- The IP infrastructure should not allow unknown MAC addresses to access the communication medium. Although not a watertight measure, this will already at least prevent from very basic attacks on the KNX network.
- If possible, Building Automation should run over a dedicated LAN and WLAN.
- IP passwords should not be communicated to unauthorised persons.
- If possible, the runtime multicast address should be set differently than the IANA approved system setup multicast address. Although not a watertight measure, this will at least masquerade the communication, so that it cannot be immediately recognized as KNXnet/IP.

2.1.5 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.
- This can be prevented by the following:
    - Ensuring access to the KNX installation through VPN connections: this however requires a router that supports VPN server functionality or a server.
    - Any of the many dedicated manufacturer specific solutions 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.

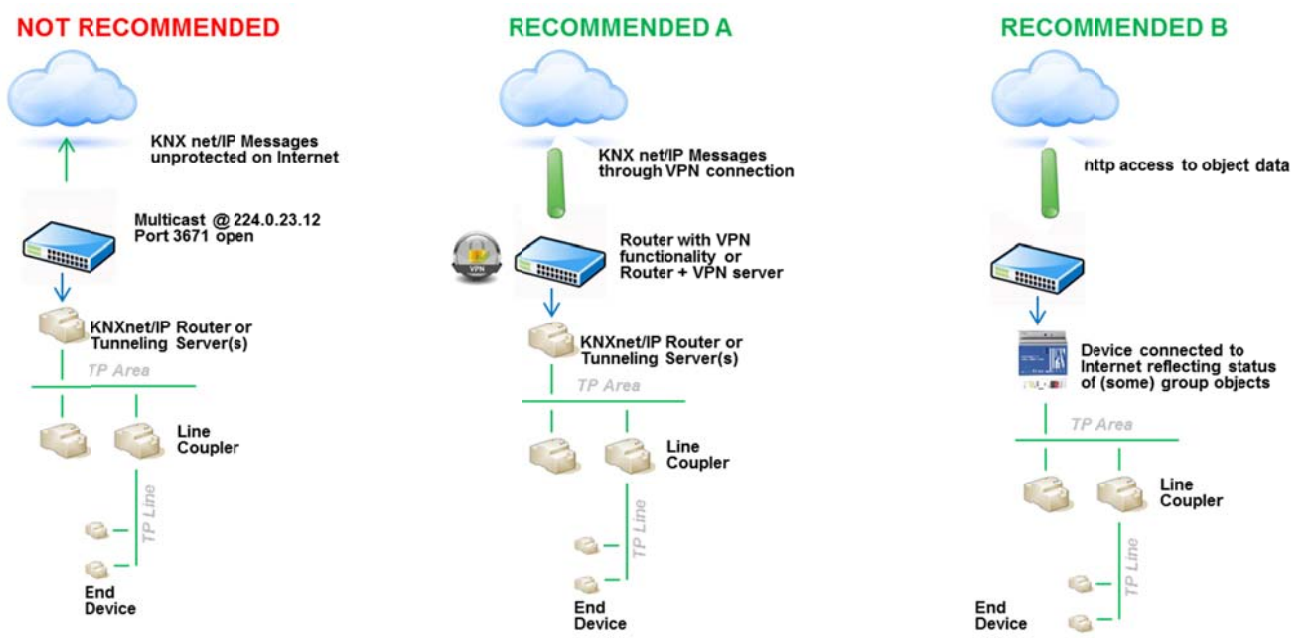

Figure 1: Access to KNX networks via Internet

3 Limiting unwanted communication inside the network

- The Individual Addresses shall be properly assigned 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 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.

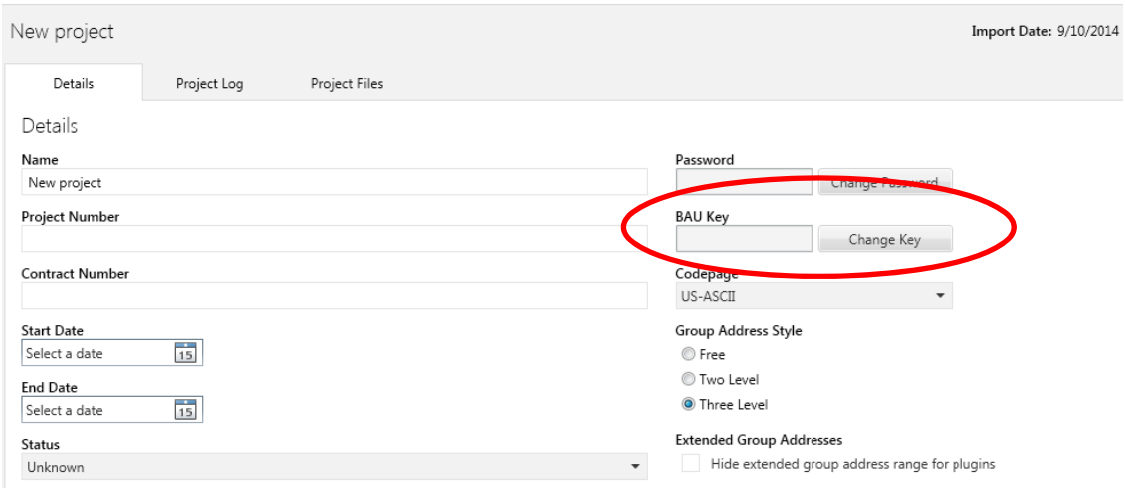

Figure 2: Protecting configuration communication in ETS

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 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 KNXnet-IP Secure mechanisms were defined on top of this.
  In this way, it is ensured that KNX IP tunnelling or routing messages cannot be interpreted on IP. The KNX IP Secure mechanisms so to say ensure that a security wrapper is added around the complete KNXnet/IP traffic.

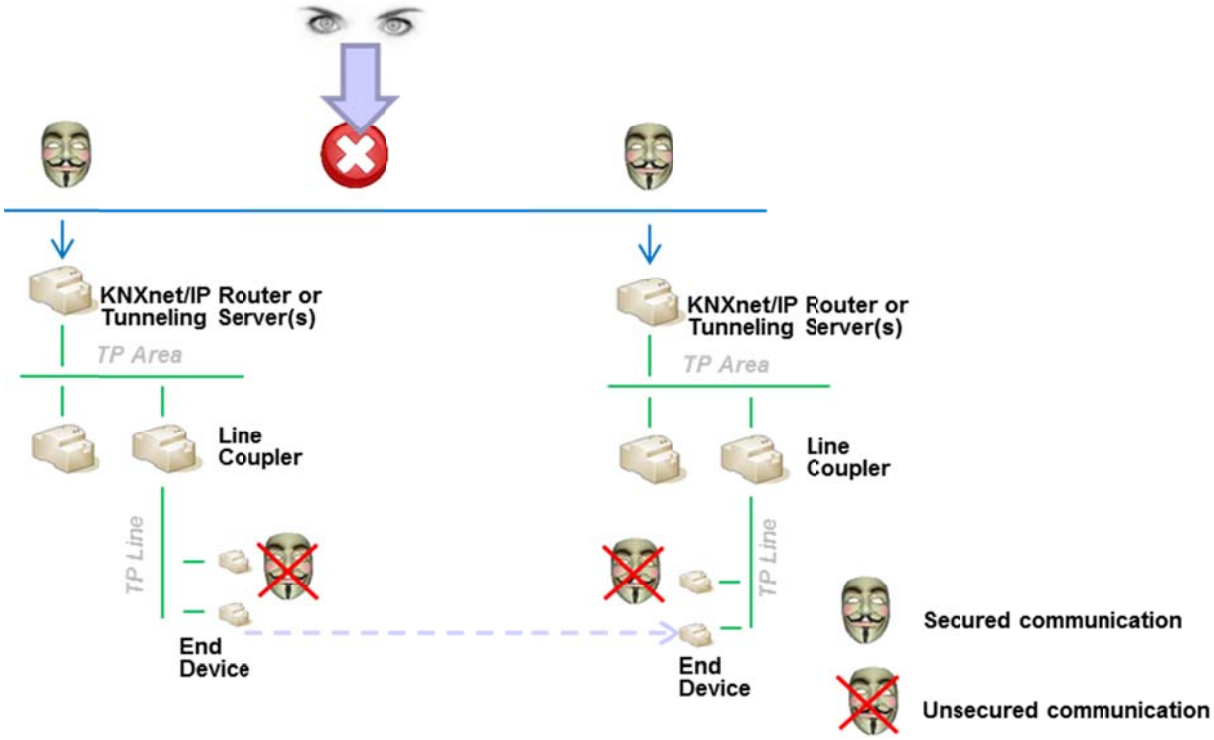

Figure 3: Protecting KNX run time communication on an IP network with KNXnet IP Security

- The KNX Data Security and KNXnet 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 KNXnet 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.

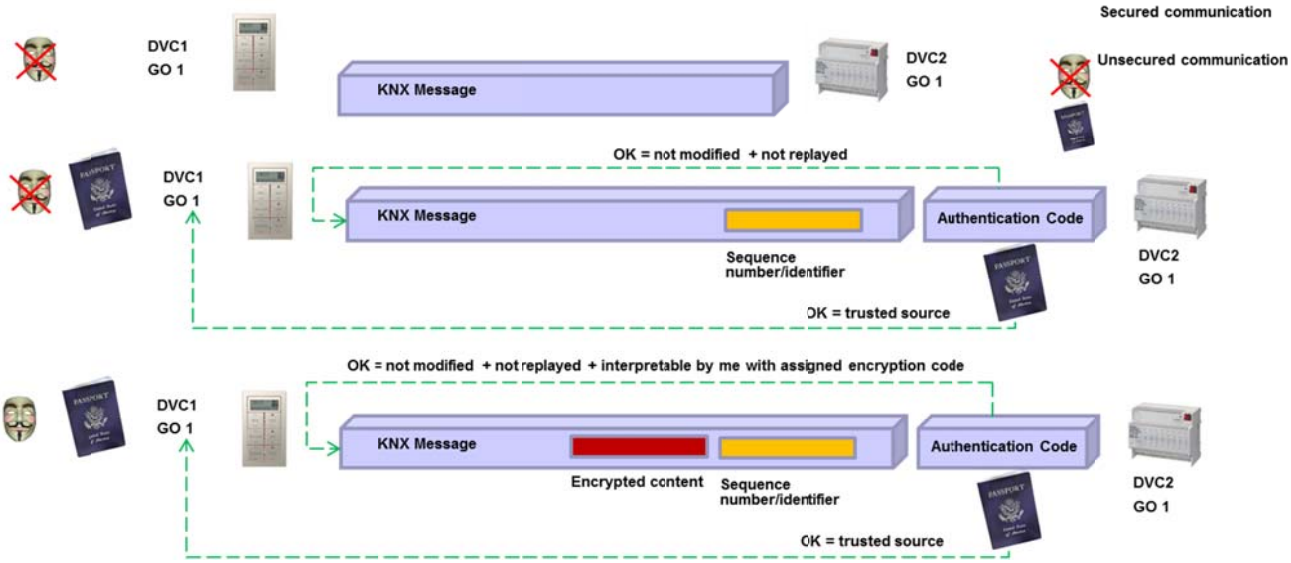

Figure 3: Overview of the KNX Data Security Mechanisms

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 (this action is at any rate not done via the bus).
- The configuration tool creates a project specific tool key.
- Via the bus, the tool 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. The FDSK is no longer used.
- The configuration tool creates runtime keys (as many as necessary) for the group communication that needs to be secured.
- Via the bus, the tool 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.

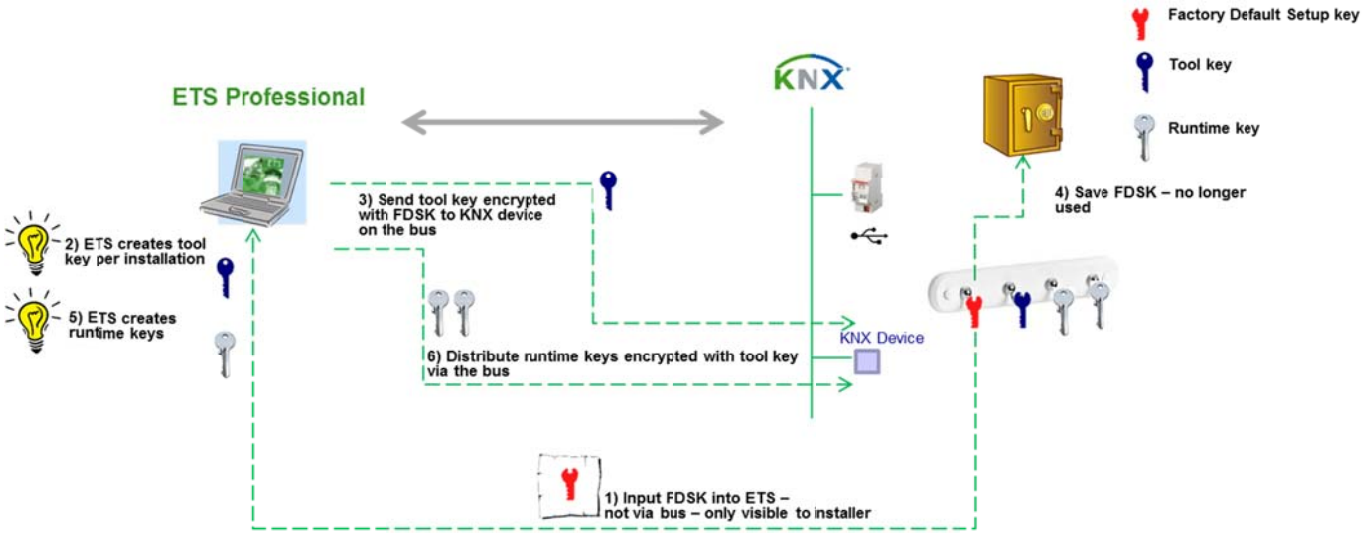

Figure 4: Procedure for securing KNX devicees

For KNX IP Security, 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.

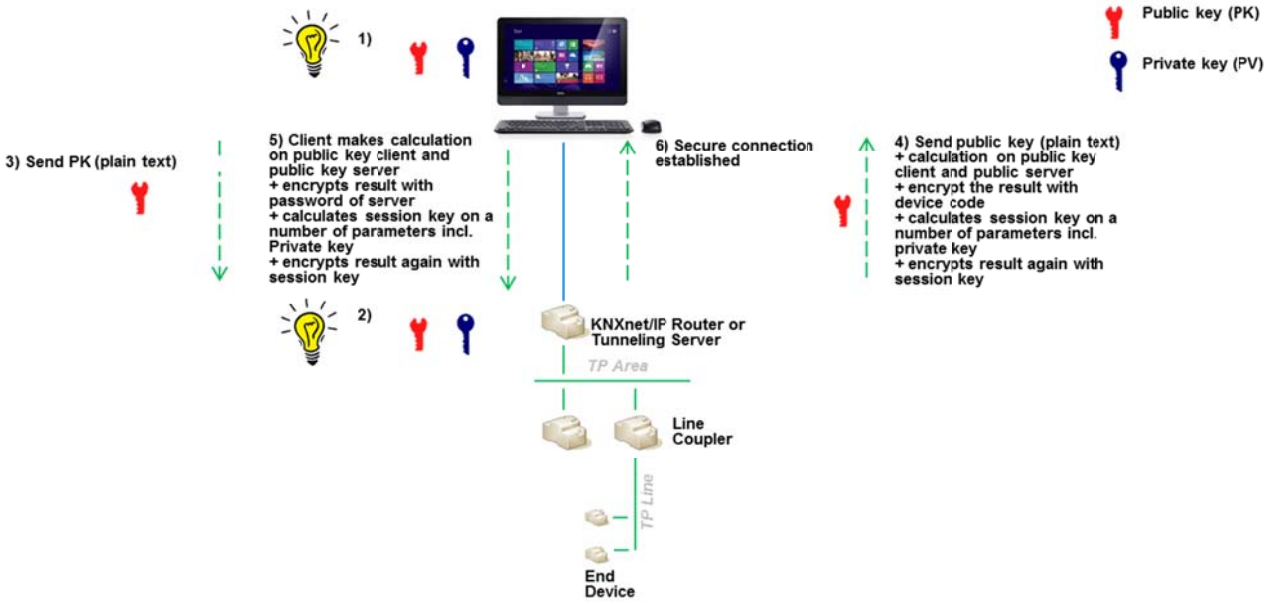

Figure 5: Setting up a KNXnet/IP Secure Connection

6 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 no longer 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.

7 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