KNX Secure

KNX Position Paper on Data Security and Privacy
1. Preventing access to the network to the various KNX physical media

1.1 Introduction
A proper security concept is based on ensuring proper prevention against unauthorised access. In case of a KNX installation this implies that only authorised 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.

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 unauthorised 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 authorised 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, ...).

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.
2. 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 messages with inappropriate Source Address. In this way, unwanted communication can 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.
3. Protecting configuration communication

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

4. Protecting runtime communication

- Next to the before mentioned measures, KNX runtime communication can be protected via the specified
  - KNX Data Secure and
  - KNX IP Secure mechanisms

- KNX Data Secure 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.

- The KNX Data Secure 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 been 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 Secure 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.

KNX Data Secure devices use a longer KNX telegram format when transmitting the authenticated and encrypted data. This does not have any effect on the reaction speed of devices. For KNX Data Secure, the devices are protected in the following way:

- A device is shipped with a unique Factory Device Setup 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 device 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, unless the device is reset to factory state, after which all the secure data in the device will be erased.
- 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.
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 authenticate 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 authorises 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) ensures 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.
5. 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.

6. Detecting unauthorised bus access

- Obviously, the bus could be monitored and unusual traffic could be traced.
- KNX Secure devices keep track of hacks in security failure logs: in this way, it is at any time possible to check whether the KNX installation was subject to security attacks.
- 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.

7. Compliance to the EU GDPR regulation

- GDPR is an abbreviation for General Data Protection Regulation (see www.eugdpr.org). The regulation aims to harmonize data protection laws in the whole of Europe.
- In order to comply with the GDPR regulation, the installer shall hand over the ETS project file to the customer. The installer and the customer shall sign a data protection declaration.
- Data that are generated by KNX devices may only be used for the purpose of remote control of the device by the customer (via App), for diagnostic purposes and for further product development. They may not be used for personalized publicity.

Literature

[1] AN 158 KNX Data Security
[2] AN 159 KNX IP Secure