TAPKO
TECHNOLOGIES GMBH

KNX®

Why KNX SECURE?

Years ago, a hack, i.e. criminal access to the KNX system of a hotel, attracted attention. This was the beginning of far-reaching discussions in the KNX community. In addition, there was a change in demand due to the use of IP and RF media in recent years.

Which scenarios are conceivable in an unprotected KNX system?

- Copying of sent telegrams
  Example: Open the garage door
- Manipulating telegrams
- Manipulating installations / configurations (reprogramming of functions)
- Reading telegram contents
- Blocking functions

(internet network technology <ab2 . net>)
E MAIL SECURITY
p2p
(internet network technology <ab2 . net>)
(internet network technology <ab2 . net>)

What protective measures exist?

For KNX Secure, we distinguish between KNX Data Secure, which concerns all KNX devices, and KNX IP Secure, which concerns only IP devices. In addition, the principles of "Security of Installation" must be taken into account.

Security of Installation:
Consideration of security criteria in the planning and installation of a KNX installation, see also the KNX security checklist of the KNX organisation, as already with the "classic" KNX installation, e.g. accessibility of the cables.

KNX Data Secure:
With KNX Date Secure, a signed and encrypted communication takes place in the KNX network and thus ensures a secure transmission of telegrams. The basis is end-to-end encryption, i.e. only the end devices understand the messages, the line couplers forward the telegrams transparently. This means that communication in the KNX network can neither be interpreted nor manipulated.

Requirements: KNX Data Secure capable devices or all system components that are located between the SECURE participants must be SECURE compatible. Secure compatible means: the devices must be able to process long telegrams (long frames).

KNX IP Secure:
All devices with KNX IP Security also support Data Security. KNX IP Secure is used for the secure transmission of KNX telegrams via KNX IP line or area couplers as well as KNX IP interfaces.

These properties are ensured by the KNX SECURE mechanisms:

Freshness
With IP Security, the timestamp ensures that the data is up-to-date; frames with outdated timestamps are discarded (when received). This prevents telegrams from being recorded and called up later.

With data security, freshness is ensured by the sequence number.

Confidentiality
Encryption prevents the interpretation of telegrams that have been read out.

Data integrity
Data integrity means preventing an attacker from gaining control of the system by feeding in manipulated messages.

MY KEY IS MY CASTLE

KNX SECURE: Keys and methods

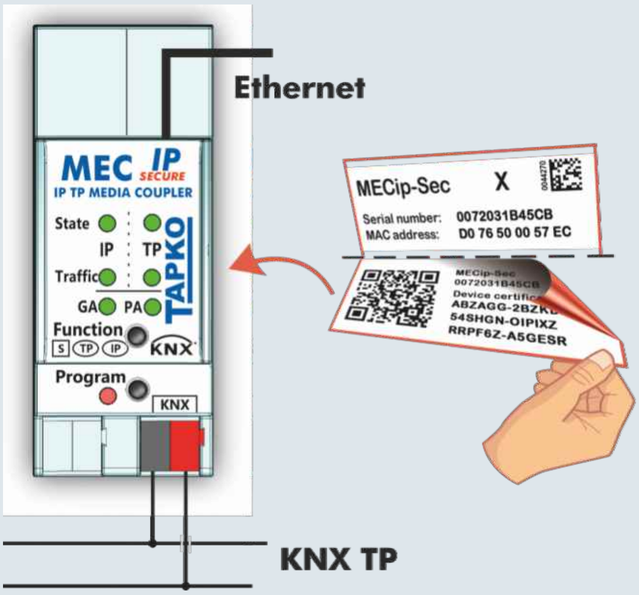
Basic information on encryption

KNX Secure does not require any revolutionary ideas, but uses the proven encryption mechanism AES according to ISO/IEC 18033-3. AES Advanced Encryption Standard 128 with CTR operating mode and AES-CBC-MAC signature (CCM), with a block size of 128 bits. All keys are assigned by the ETS.

Device certificate, device label

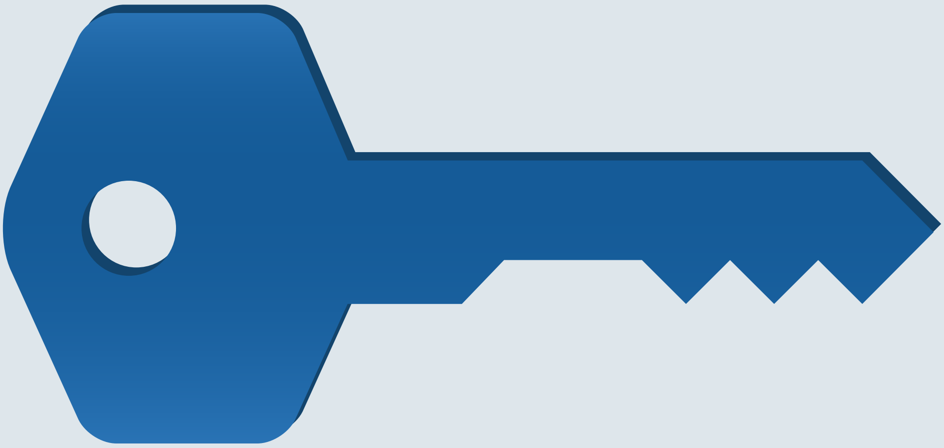
The device certificate consists of FDSK and serial number and is 36 characters long. The ETS requires a device certificate for the initial configuration with KNX Secure, both Data and IP Secure. Device certificates are stored in the ETS project.

Detachable labels with device certificate (text + QR code) are on the device itself. Device certificate labels must be removed before mounting the device. Device certificates (labels and reports) must be stored safely.



Factory Default Setup Key

FDSK stands for "Factory Default Setup Key". It is a "factory" value, i.e. it is assigned to each device by the manufacturer during production. The ETS requires FDSK for the first configuration or after each master reset. It is part of the device certificate and can be read directly from the QR code by the ETS. The FDSK becomes inactive after the first configuration and the ETS then uses the tool key. The FDSK cannot be changed!



Tool Key

The tool key enables access to the device during configuration and is used for point-to-point communication; like the FDSK, it is 128 bits long. Tool key is generated in the ETS and assigned during initial commissioning. The tool key is saved in the ETS project. If the ETS project is lost together with the tool key, only a factory reset is possible. In this case, FDSK becomes active again, as a factory reset deletes the tool key and FDSK takes over.

Group Key

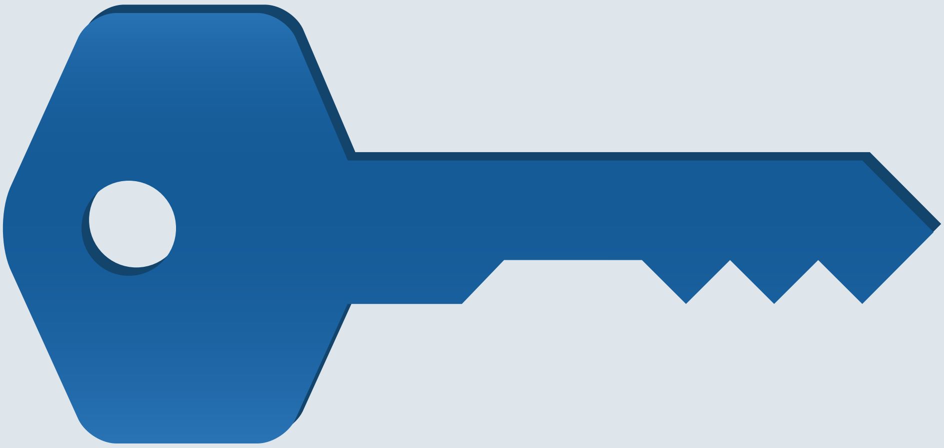
The group key is used during runtime communication between group addresses. In a project, there is an individual key for each group address. This key is also 128 bits long and is assigned and stored by the ETS and can be found in the project report - project security. After resetting to the factory settings, these keys are also deleted.

Serial number

The serial number as part of the device certificate is a 6 byte long unique number of the manufacturer for the unique identification of each KNX device.

Project password

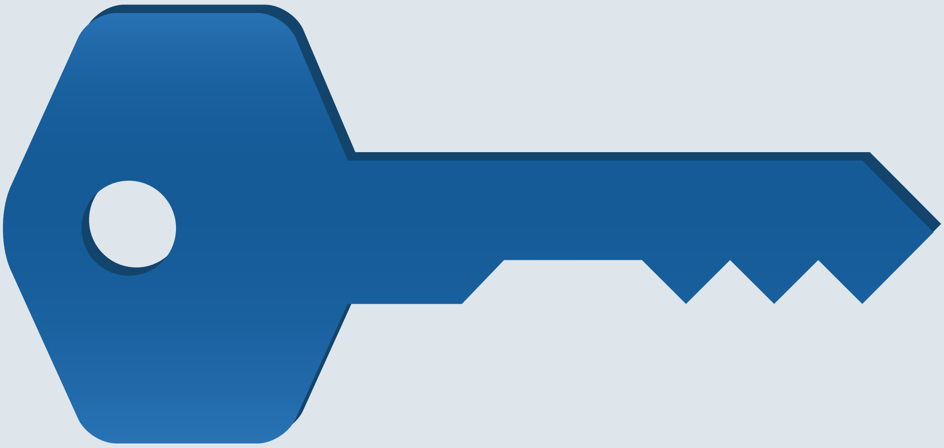
A password is required for the ETS project using KNX Secure. This password is used to protect tool and group keys (as well as backbone keys for KNX IP Secure) in the project and security-relevant settings of devices.



Secure commissioning
If KNX Data Secure devices are intended for secure runtime communication, they also have to be commissioned in secure way by ETS. For devices that are commissioned in plain way, runtime communication is possible in plain way only. For each individual device in ETS project (which supports KNX Data Secure) secure commissioning can be switched on or off in its properties.

Sequence number
The sequence number is a 6-byte long number. With Data security, each transmitter adds a sequence number that each receiver checks per communication partner. When the device receives telegrams from the KNX bus, it only accepts messages with higher sequence numbers. In summary, the sequence number ensures that the data is up-to-date and prevents data from being recorded and replayed.

Backbone Key (at IP Security)
The backbone key is used for secure IP routing. All IP devices in a project have the same backbone key. After resetting to factory settings, the backbone key is also deleted.



Good to know

The use of KNX Secure is necessary or recommended in these areas

- If KNX devices are easily accessible in public areas.
- To perform separation in case of different areas of responsibility, e.g. office buildings with several users, hotels
- For access via IP networks / remote maintenance

Use of KNX Secure in existing installations

- To make an existing Non-Secure KNX installation with IP lines more secure, KNXnet/IP routers should be replaced with KNXnet/IP Secure routers. The transmission between KNXnet/IP devices can then be done with KNX IP Secure.
- Secure devices can always be used in Unsecure mode in a Non-Secure KNX installation as a replacement for Unsecure devices. This allows parts of an existing installation to be upgraded with new KNX Data Secure devices.
- Secure devices / communications can also be used in a Non-Secure installation. For Secure devices, the individual group objects Secure or Unsecure can be configured / used. For an individual object, the following applies: Either Secure or Unsecure.

TAPKO KNX SECURE

UIMip-Sec - KNX IP Interface Secure with 4 tunneling channels

UIMip-Sec connects the PC (e.g. ETS) to the KNX bus for commissioning and monitoring over IP. The secure version protects the tunnelling protocol by using KNX IP secure.

MECtp-Sec - KNX Line/Area Coupler Secure

MECtp-Sec connects KNX segments (lines, areas). It provides various routing filters for group and individual telegrams. The secure version MECtp-Sec supports encrypted configuration using KNX Data Secure .

MECip-Sec - KNX IP Router Secure with routing and tunneling interface

It connects a KNX TP line to a KNXnet/IP Backbone. Via IP Tunnelling, ETS can communicate with the KNX bus. The secure version supports encryption using KNX Data Secure and KNX IP Secure.

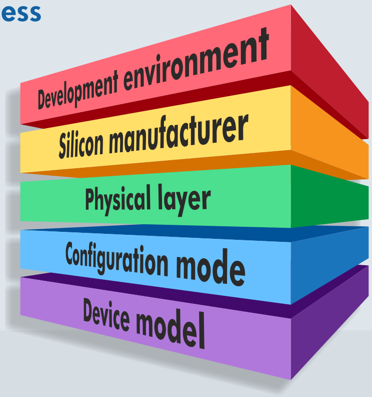
TIO4-Sec - 4 fold Push Button Interface Secure with status outputs

The 4-fold push button interface TIO4-Sec is the further development of the well-known TAI4. TIO4-Sec now also supports KNX Data Secure. The channels of TIO4-Sec can be used as outputs to reflect LEDs' status .

Flexible Working in the Development Process

KAIstack-secure

KAIstack-secure includes the functionality of KNX Secure.



click here

Online overview of these products

TAPKO Technologies GmbH

Photos: tapko.de, istock.com | Conecept+Design: marktwert.net | Edition: 09.2021 | Subject to change

TAPKO
TECHNOLOGIES GMBH

KNX

www.tapko.de - info@tapko.de

TAPKO Technologies GmbH I Germany
Im Gewerbepark A15 I D-93059 Regensburg

Phone: +49 941 30 747- 0
Fax: +49 941 30 747- 29

KNX®