Using KNX Secure in ETS5

Principles & Details

KNX Association
2017

Using KNX Secure in ETS5

Agenda

Introduction

- KNX Secure Today
- KNX Secure Overview
- KNX Secure Facts

KNX Secure Types

- KNX IP Secure
- KNX Data Secure
- KNX Secure Combination

KNX Secure in ETS5 (Theory & Praxis)

- KNX IP Secure, Backbone
- KNX IP Secure, Devices
- KNX IP Secure, Interface
- KNX Data Secure, Group Addresses
- KNX Secure, Device Label
- **KNX Secure and ETS Maintenance/ Updates**

Introduction

Using KNX Secure in ETS5

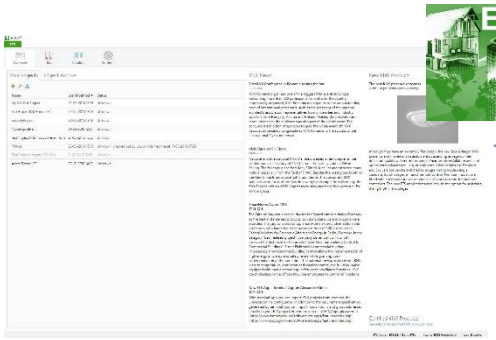
Introduction

KNX Secure Today

At the L+B 2016, KNX presented and announced the new KNX Secure. Since the release of ETS 5.5 version in April 2016, ETS supports this extension to the KNX Standard.

Slides & Details

The KNX Secure features presented here are also described in detail in the corresponding ETS 5.5 Help file. If so, a reference to the respective help item is given in this presentation.



Press F1

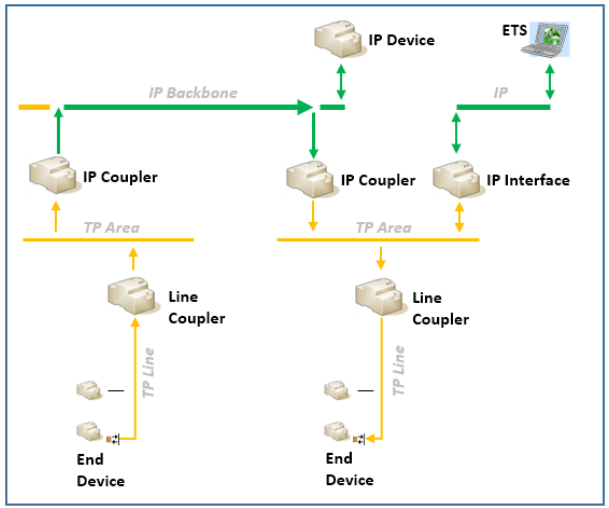
ETS Professional **ETS Professional Help**

Using KNX Secure in ETS5

Introduction

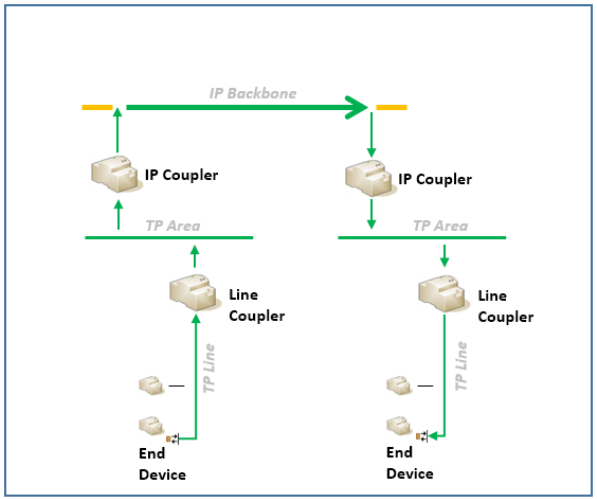
KNX Secure Overview

KNX IP Secure



All KNX telegrams between the two (or more) IP Couplers are encrypted

KNX Data Secure



Unsecured communication
Secured communication

The group communication of a particular sender (one or more group objects) to another group object(s) is encrypted

Using KNX Secure in ETS5

KNX Secure Facts

KNX Secure Application Scope

KNX Secure covers the following main application scenarios in a KNX installation.

- Secure Communication on IP
- Secure Communication between end devices across media
- Secure Communication during configuration

Section ETS How-Tos/ KNX Security/ KNX Security, Applications

KNX Secure Attack Vectors

The following threat scenarios or possible attacks on the KNX system are effectively thwarted by KNX Security:

- Telegram Repetition
- Telegram Manipulation
- Telegram Visibility

Section ETS How-Tos/ KNX Security/ KNX Security, Threat …

Using KNX Secure in ETS5

KNX Secure Facts

KNX Secure used algorithms

KNX Secure uses AES128 CCM for encryption/ authentication and elliptic curve Diffie-Hellman for a secure key exchange

- *Advanced Encryption Standard* (AES) is a standard encryption algorithm (ISO/IEC 18033-3)

  Block size: *128 bit*
  Key size: *128 bit, 192 bit or 256 bit*

  Consists of:

  - Substituting bytes
  - Shifting rows
  - Mixing columns
  - Add round key

  *Several animations exist on the Internet (*https://www.youtube.com/watch?v=mlzxpkdX), *usage in KNX (KNX IP Secure)*

- Elliptic curve Diffie- Hellman key exchange is a worldwide standardized and widely used algorithm to share a common secret key on an unsecure communication channel

Section ETS How-Tos/ KNX Security/ (4) Technology

Using KNX Secure in ETS5

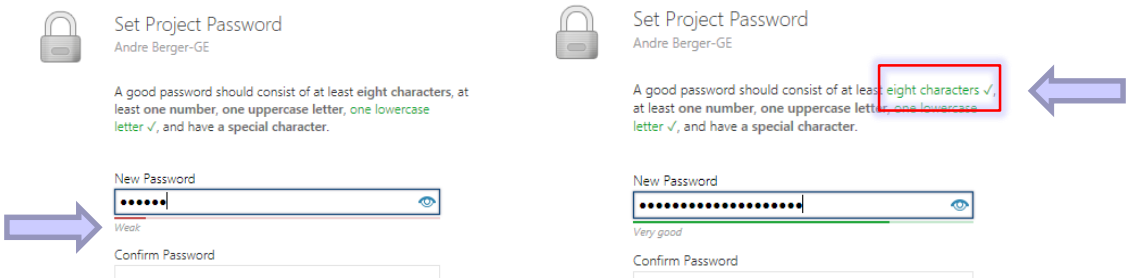
KNX Secure Facts

Security of ETS KNX Projects with KNX Secure #1

- Every ETS project using KNX Secure requires increased security “level” for the project data itself (not allowed to view passwords used in project) → ETS projects therefore need to be password protected

Section ETS How-Tos/ KNX Security/ (6) Properties/ Project

- ETS displays the required password strength.



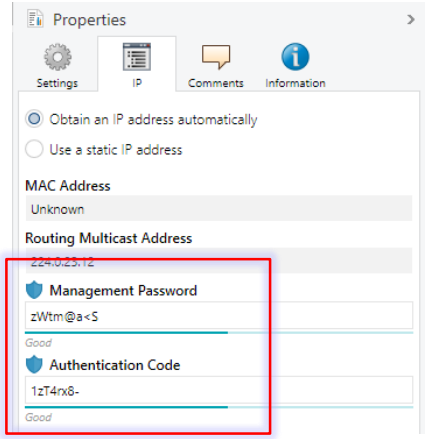
Section ETS Professional/ ETS Interface/ Project Properties/ Det...

Using KNX Secure in ETS5

KNX Secure Facts

Security of ETS KNX Projects with KNX Secure #2

- Every KNX Secure device used in a secure way in a ETS project also has individual passwords. Also here ETS displays the password strength in a proper way.



Section ETS Professional/ ETS Windows/ Types/ Device Panel/ Device

Using KNX Secure in ETS5

KNX Secure Facts

Keys in an ETS KNX Project with KNX Secure #1

- When using KNX Secure features of devices, a individual device and/ or the IP backbone key for the “secure” communication needs to be maintained. These keys are stored and maintained by ETS in a safe way, even when projects are exported.

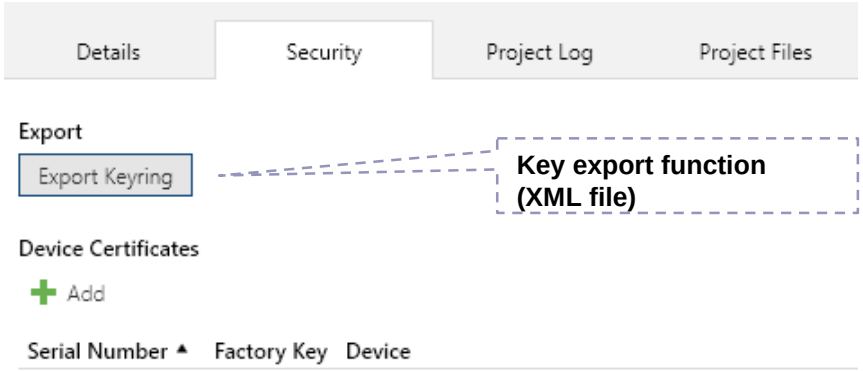
Section ETS Professional/ ETS Interface/ Overview/ Project Properties/ Security

Using KNX Secure in ETS5

KNX Secure Facts

Keys in an ETS KNX Project with KNX Secure #2

- Monitoring a KNX (Secure) installation ➔ for a valid use case (e.g. external visualization) it is necessary to get hold of the keys used in the ETS project in a (secured) way → key ring exported file



Section ETS Professional/ ETS Interface/ Overview/ Project Properties/ Security

KNX Secure Types

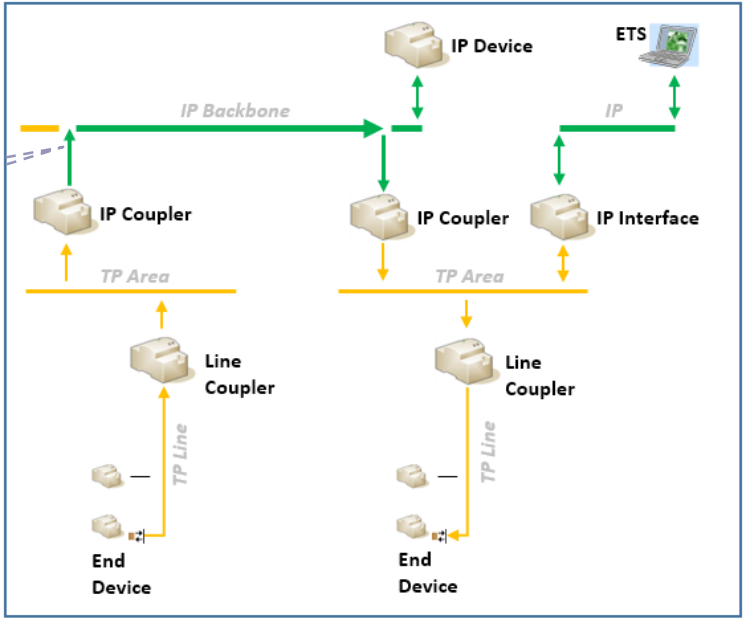
Using KNX Secure in ETS5

KNX Secure Types

KNX IP Secure, Technology

KNX IP Secure encrypts the entire KNXnet/IP frame.

All KNX telegrams between two (or more) IP Couplers are SECURED



Unsecured communication
Secured communication

Section ETS How-Tos/ KNX Security/ **KNX Security, Implementation**

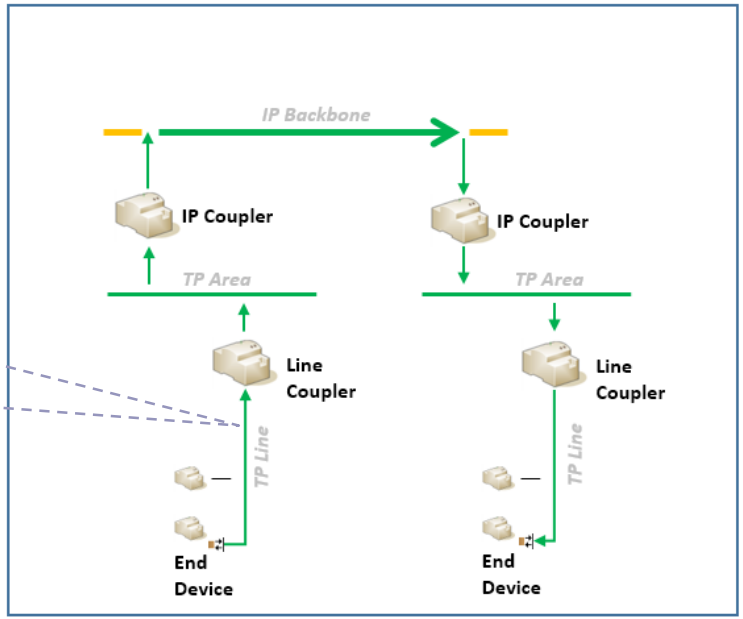
Using KNX Secure in ETS5

KNX Secure Types

KNX Data Secure, Technology

KNX Data Secure only encrypts the APCI and the payload.

The group communication of a particular sender (one/ more group objects) to another group object(s) is SECURED



- Unsecured communication
- Secured communication

Section ETS How-Tos/ KNX Security/ **KNX Security, Implementation**

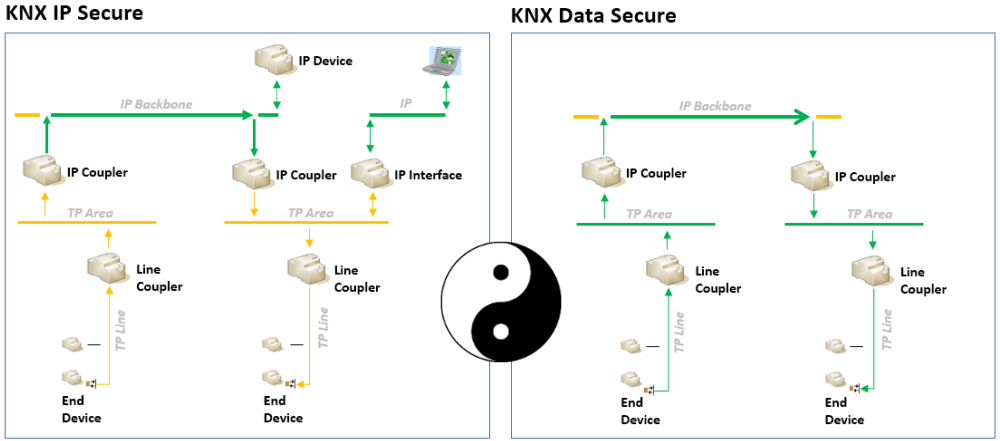
Using KNX Secure in ETS5

KNX Secure Types

KNX Secure, Combined

KNX IP Secure and **KNX Data Secure** can be combined in an ETS project/ installation.

ETS handles key management/ distribution, establishes ‘secure links’ and downloads these links in KNX Secure devices independent of the KNX Secure types.



Section ETS How-Tos/ KNX Security/ **KNX Security, Implementation (6)**

KNX Secure in ETS5

Using KNX Secure in ETS5

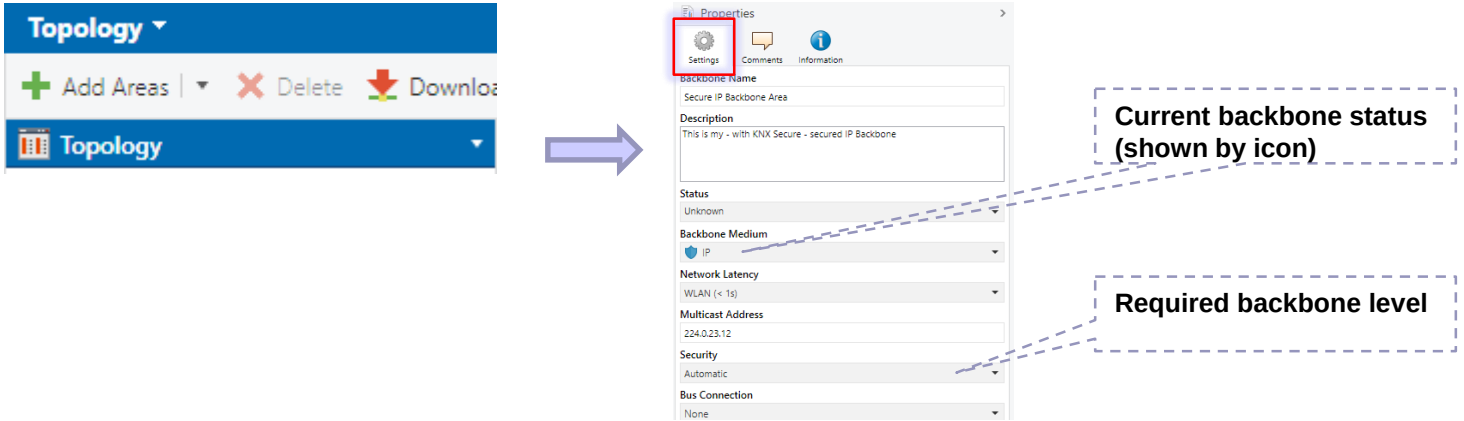
KNX Secure in ETS5

KNX IP Secure, IP Backbone

The KNX secure level of the backbone itself is part of the **backbone** properties.

- Possible levels are ***On/ Off/ Automatic***. There are dependencies between this level and devices on the backbone (e.g. the need to download such devices also *secure* when backbone is secure)

Section ETS Professional/ ETS Windows/ Types/ Topology Panel/ Settings



Using KNX Secure in ETS5

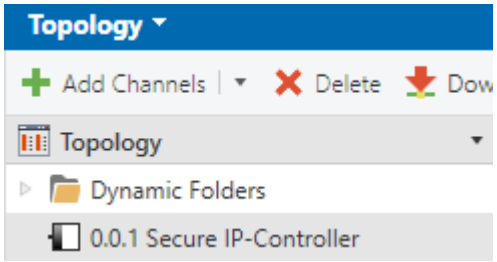
KNX Secure in ETS5

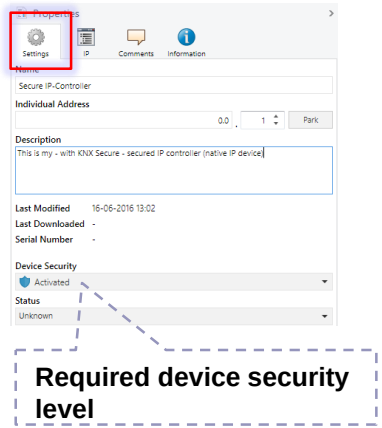
KNX IP Secure, IP Devices

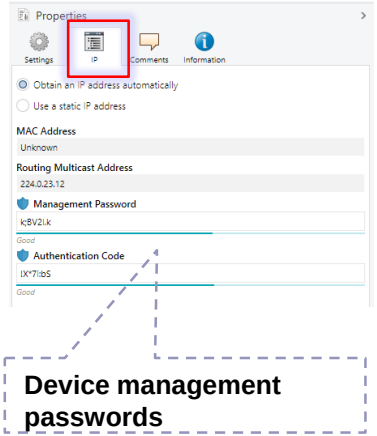
The KNX secure level of IP **devices** (e.g. on the backbone) is part of the **device** properties.

- Possible levels are ***Activated/ Deactivated***. There are dependencies between this level and the backbone (e.g. the need to set the Level to ***Activated*** for such devices when backbone is secure)

Section ETS Professional/ ETS Windows/ Types/ Device Panel/ Device, Settings/IP







Using KNX Secure in ETS5

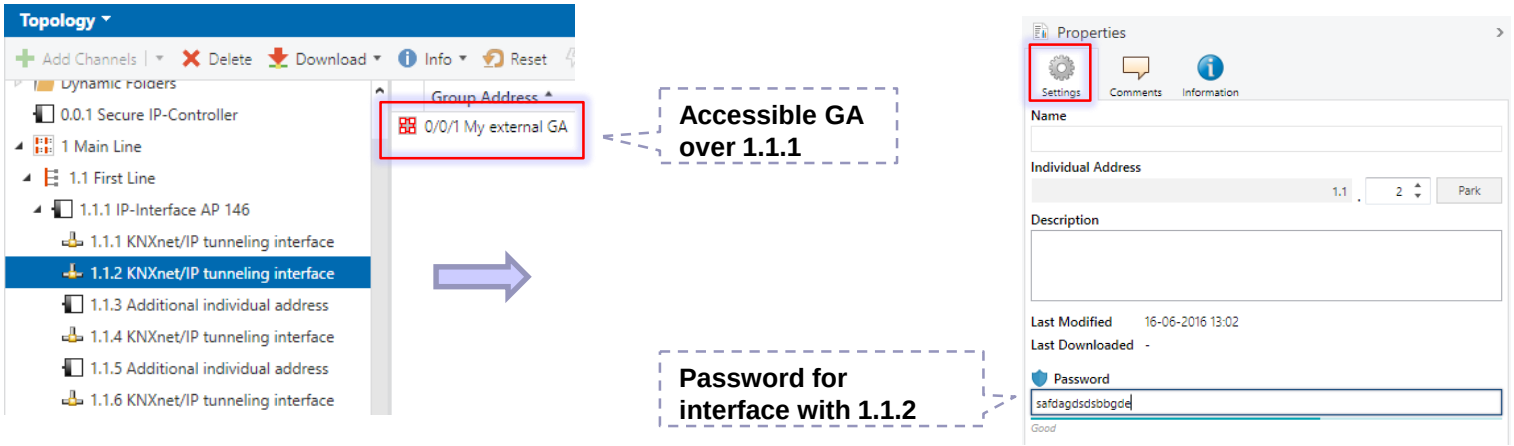
KNX Secure in ETS5

KNX IP Secure, IP Interfaces

The KNX secure level of IP **interfaces** is (also) part of the **device** properties.

- For external (visualization) access via (additional) interfaces Individual Addreses, an interface password and a GA explicitly assigned to the interface is needed (passwords can be made available via ***Export Keyring***, see previous slide 10)

Section ETS Professional/ ETS Windows/ Types/ Device Panel/ Device/ Additional Interfaces



Using KNX Secure in ETS5

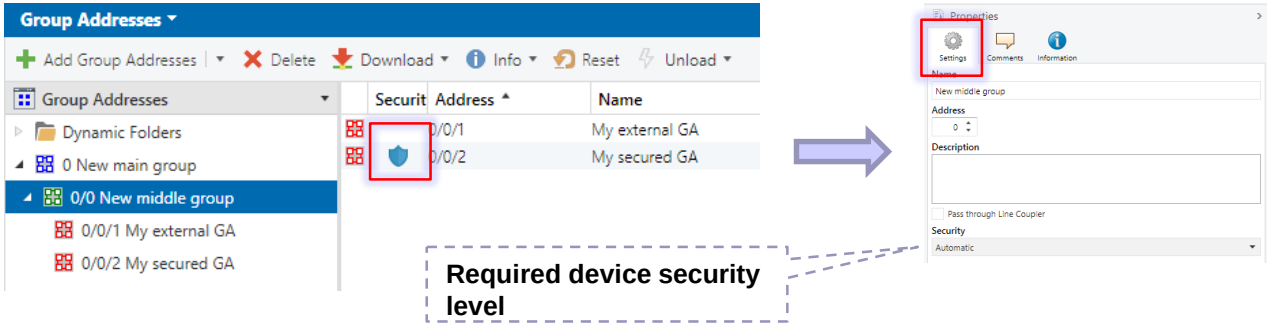
KNX Secure in ETS5

KNX Data Secure, Group Addresses

The KNX secure level of a group address is part of the **GA** properties.

- Possible levels are ***On/ Off/ Automatic***. There are dependencies between this level and the GAs assigned to the GOs (e.g. the need to download such devices also *secure* when the GA is secure)

Section ETS Professional/ ETS Windows/ Types/ Group Address Panel/ Group …



Section ETS Professional/ ETS Windows/ Types/ Device Panel/ Device

Using KNX Secure in ETS5

KNX Secure in ETS5

KNX Data Secure, Group Addresses

Scene "*Besenkammer*", simple Example

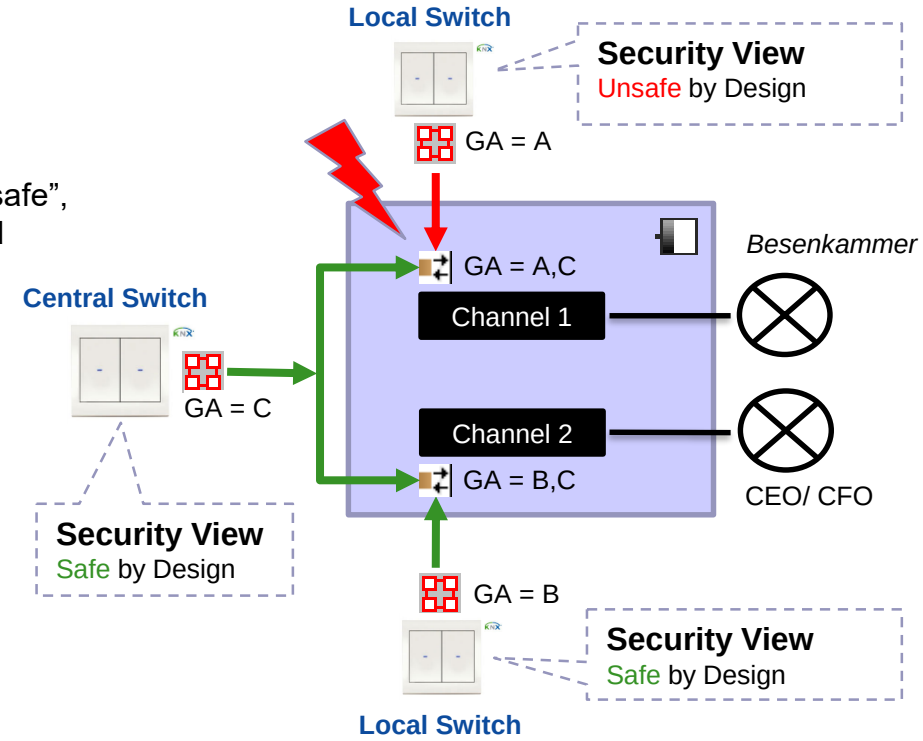
- **KNX Secure** Device is configured by ETS in a secure way

ETS 5.5.0 starts with "all associations must be safe", when discussion with KSG/ members is finished we are able to allow such "Mixed Associations"
→ Links are done via ASSOC Table!

Allowing such an scenario
(is possible with KNX Secure specification) has
PRO/ CONS

- Opens a backdoor
- Owns "uncontrollable" dependencies
- Reuse existing (non secure) (switch) devices
- Cost sensitive extension of existing installation with secure functions

Security inactive
Security active



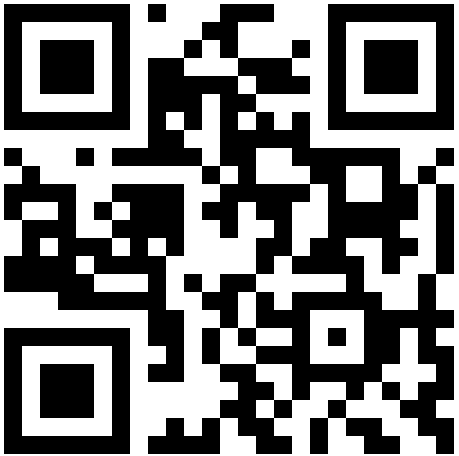
Using KNX Secure in ETS5

KNX Secure in ETS5

KNX Secure, Device Label

How to label them?

How to use labels (and *KNX Secure* devices) in ETS? → **Life Demo**



Using KNX Secure in ETS5

ETS Maintenance

Release ETS 5.5

Version 5.5.0, delivery (12.04.16) → Release Notes @ www.knx.org, tools section

- KNX Secure

Version 5.5.2, delivery (08.07.16) → Release Notes @ www.knx.org, tools section

- New features
  - *update of non certification relevant data*
- Bug correction

Version 5.5.3, November 2016 → Final test workshop 29.11 - 30.11

- New features
  - *search field in dashboard*
  - *printing of panel detail view*
  - *serialization for Falcon connection properties*
  - ***Improved handling of KNX Secure devices***
- Bug correction

Using KNX Secure in ETS5

ETS Maintenance

Planned Future Extensions

Plug In “replacement strategy” for ETS Professional/ ETS Inside

- Details see chapter ETS Inside

Channel oriented design/ view for ETS Professional/ ETS Inside

- ETS test workshop; 29.11-30.11
- KNX Tech Day #2; 23.11

KNX RF Multi (S-Mode)

- Improve reliability on RF media (up to 5 RF channels, 3 fast/ 2 slow) with fast acknowledge mechanism (ETS supports today RF Ready with one RF channel)
- Kick off KSG Class meeting (Frankfurt, 03 May 2016), online meeting + specification ongoing
- Implementation start depends on specification (RfV), finalization of current ETS and system subjects including resource/ budget availability

Using KNX Secure in ETS5

Summary

Feel free to contact us when experiencing open points, e.g. in ETS Help file!

Using KNX Secure in ETS5

Thanks!