

KNX Data Secure

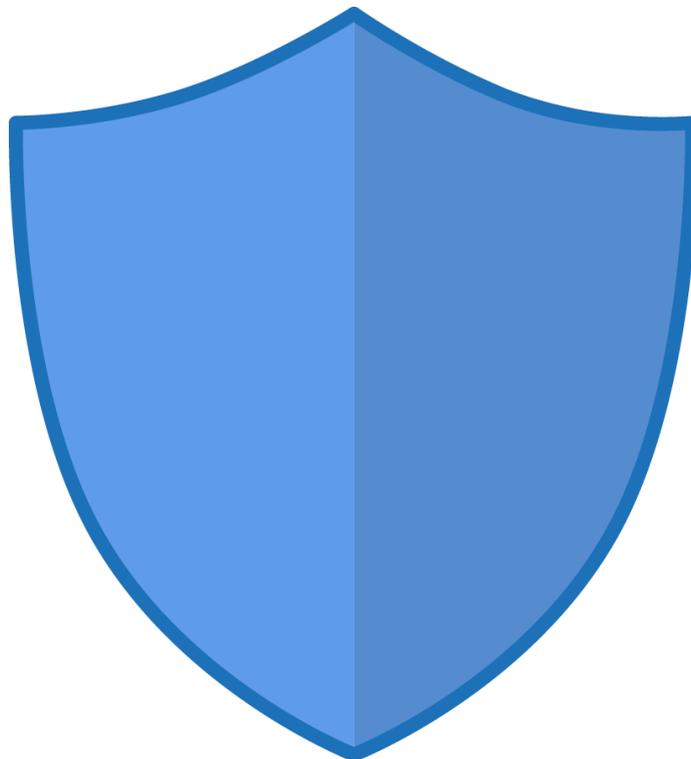


Table of Contents

1	What is KNX Data Secure?	3
2	Why KNX Data Secure?	10
3	What does this mean?	12
4	How do I identify KNX Data Secure?	15
5	How does KNX Data Secure work in the ETS?	18
	5.1 Project design	18
	5.2 Commissioning	23
	5.3 Compatibility and versions	30
6	What else should I observe?	31
7	Appendix	33
	7.1 Overview of system components	33

1 What is KNX Data Secure?

Introduction

Switching lights, controlling shutters or Venetian blinds, regulating room temperature and centrally controlling individual building functions have always been core applications of KNX digital building systems. These applications usually only involve minor risks of sabotage and control loss, especially when using wired networking via the KNX media Twisted-Pair (TP) or Powerline (PL).

Today, a KNX system is not only capable of handling simple control and monitoring tasks, but also facilitates many everyday tasks through added intelligence and automation. Particularly the use of new KNX media such as KNXnet/IP and radio (RF) makes this evolution possible. At the same time, networked homes and smart office buildings create considerable risks if important protective measures are neglected. Every networked and unsafe device creates gateways that can be used to access the building installation and consequently personal devices.

For these reasons, the understanding of customers and installation engineers with regard to the reliability of a KNX installation goes far beyond stability and interoperability. Modern requirements for a reliable and safe KNX installation are...

- protection against unauthorized manipulation of configurations
- fail-safe operation of building functions
- fault-free visualization and functional logic
- backup of the transmitted data
- sustainable control of the entire building installation

A sound protection concept is necessary to ensure these requirements. This is based on carefully shielding the system against unauthorized access. In the case of a KNX system, only authorized persons (installation engineers, users, maintenance personnel) have access to the components and functions of the system. The critical system parts (especially when using open media such as IP and RF) must be protected with KNX Data Secure already at the planning and installation stage.

KNX Data Secure

KNX Data Secure signs and encrypts the communication in the KNX network and ensures secure data transmission of telegrams. The communication in the course of commissioning processes with the ETS as well as the runtime communication between devices and to visualizations is thus secure. The concept ensures that all or only selected KNX telegrams are authenticated and encrypted regardless of the medium. Thus the communication between sender and receiver can neither be interpreted nor manipulated. Consequently, KNX Data Secure effectively protects user data against unauthorized access and manipulation.



Image 1: KNX Data Secure protects against unauthorized access and manipulation

For the security architecture, KNX Data Secure relies on ISO 18033-3 standardized security algorithms such as AES-128 encryption. KNX Data Secure is standardized according to EN 50090-3-4. KNX protects against hacker attacks on the digital infrastructure of networked buildings.

- i** KNX Data Secure is specified in the KNX standard for all manufacturers. Certified KNX Data Secure-capable devices of different manufacturers can communicate securely with each other.

KNX Data Secure enables secure communication at telegram level from sender to receiver (end-to-end protection). The participants establish a secure communication channel, including authentication of the authorized communication partners and encryption of the transmission. This is done during commissioning of KNX Data Secure devices by the ETS and, if required, also after commissioning, when devices exchange data and information (see figure 2).

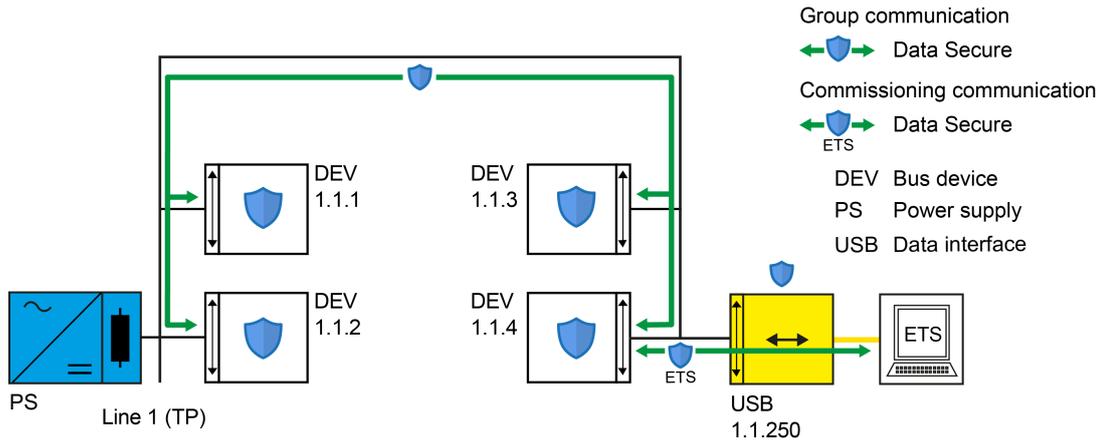


Image 2: Topology diagram 1 (example)
"Secure communication in a TP line"

KNX Data Secure devices use a longer KNX telegram format (Extended Frames) for the transmission of authenticated and encrypted data than conventional devices. This has no effect on the reaction speed of the devices. Unsecured devices can be used in the same installation and on the same media (see figure 3). This means that KNX Data Secure can be used as an additional measure to implement reliable security for selected devices or functions in new or existing systems.

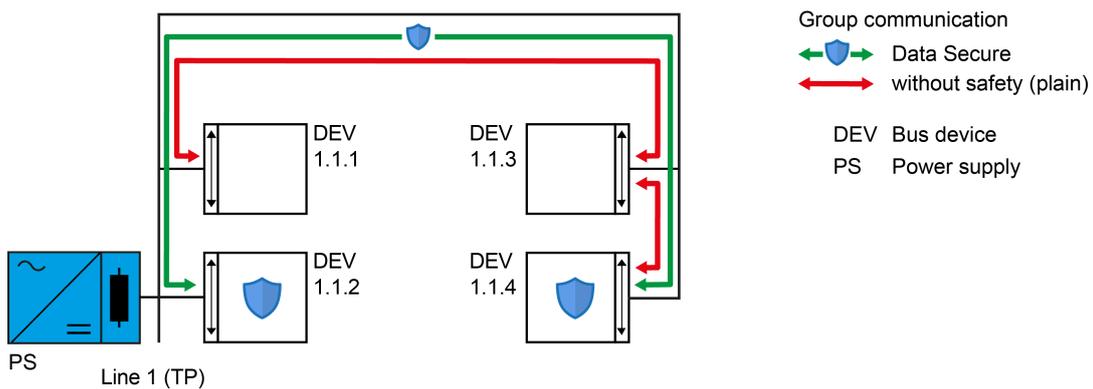


Image 3: Topology diagram 2 (example)
"Secured and unsecured communication in the same KNX installation"

KNX Data Secure-capable devices, which have been securely commissioned by the ETS and also exchange secure data with other KNX Data Secure-capable devices via communication objects at runtime, can generally also communicate in a conventional and unsecured manner via selected group addresses. Mixed operation of safe and conventional communication on a sensor or actuator via different communication objects is possible. However, secured and unsecured communication via one and the same communication object is not possible!

The ETS project determines which group addresses communicate securely and which group addresses communicate conventionally (siehe Kapitel "Project design" ▶ Page 18).

Due to the longer telegram format, the system components used (e.g. area/line coupler) and the local data interfaces of the ETS (e.g. USB) must also support Extended Frames. In a KNX Data Secure installation it must be ensured that all system components between KNX Data Secure participants and also between the ETS and

the participants have this capability (see figure 4). This must always be taken into account when communicating across lines and especially when existing KNX installations are extended with KNX Data Secure. It may be necessary to replace older system components with components compatible with KNX Data Secure.

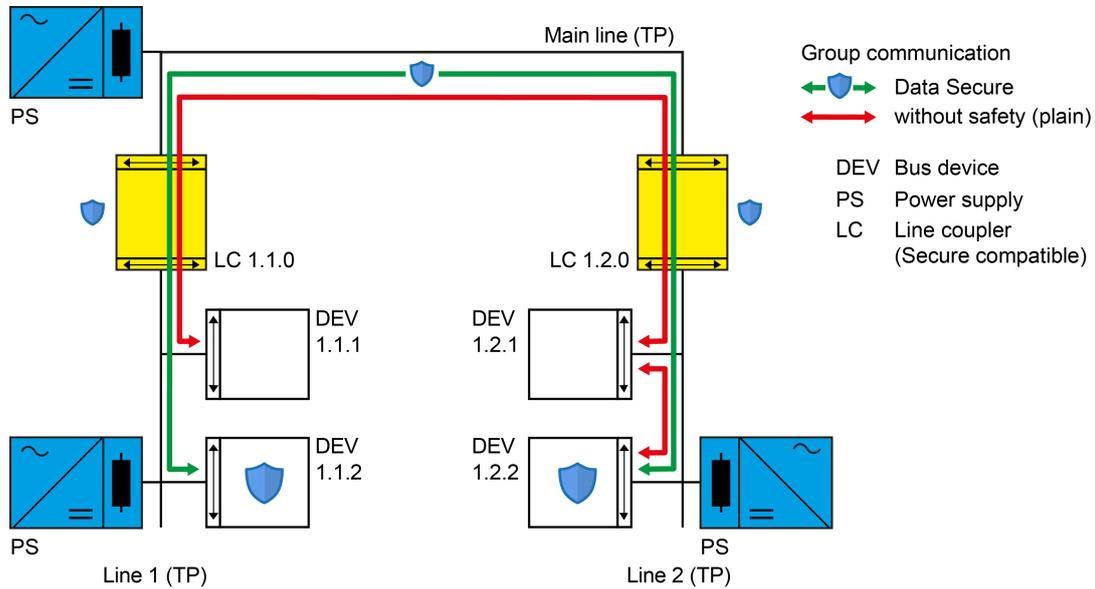


Image 4: Topology diagram 3 (example)

"Secured and unsecured communication across lines – using system components compatible with Data Secure"

System components are not compatible with KNX Data Secure if the devices used do not support the extended telegram format! Secure runtime communication or commissioning across such system devices is not possible (see figure 5). However, KNX Data Secure-capable devices within a line or line segment can always communicate securely with each other and can also be securely commissioned with the ETS.

- i** The appendix of this documentation contains an overview of the system components. This device overview can be used to identify which system components are compatible with KNX Data Secure.

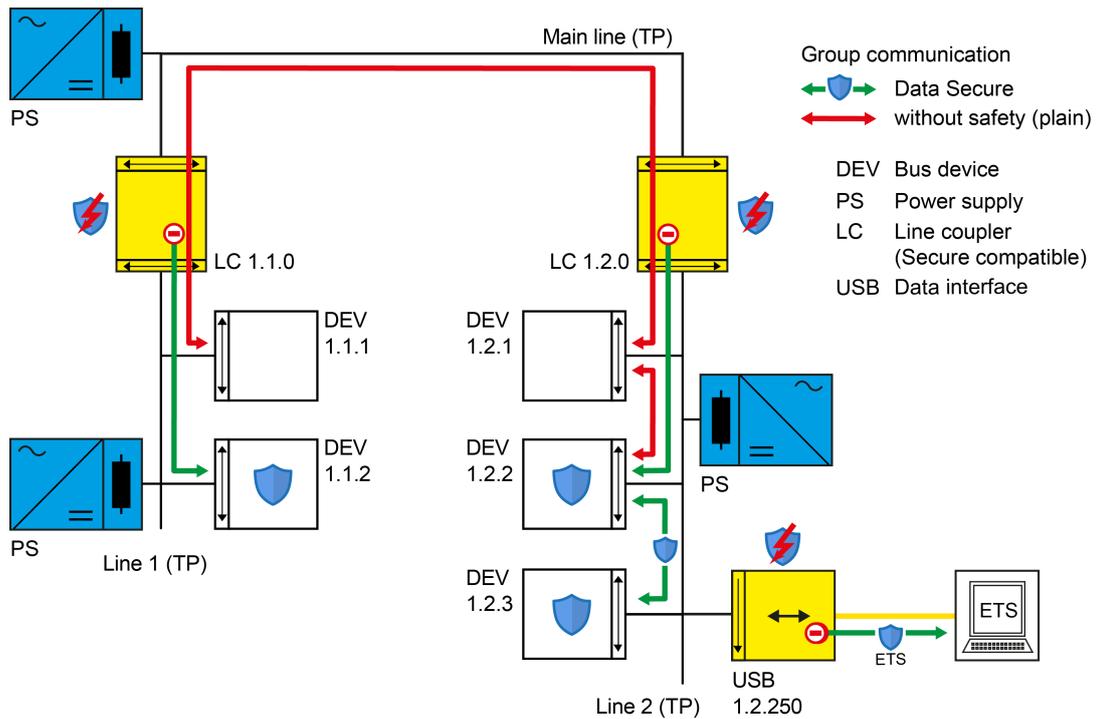


Image 5: Topology diagram 4 (example)

"Secured and unsecured communication across lines – using system components not compatible with Data Secure"

Due to the media-neutral characteristic of KNX Data Secure, communication is also possible across lines in all KNX media (see figure 6). ETS commissioning is also possible in a media-neutral manner. Here, too, it must be ensured that the system components used (media couplers, data interfaces) are KNX Data Secure-compatible to ensure fault-free communication!

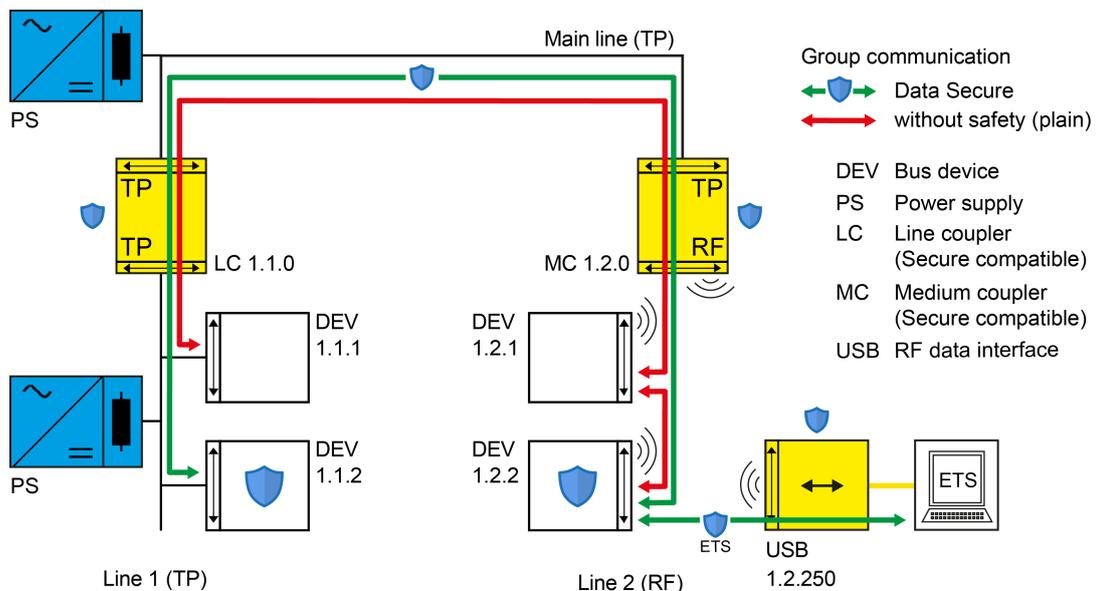


Image 6: Topology diagram 5 (example)

"Secured and unsecured communication across lines in a TP-RF mixed installation"

If required, devices that are KNX Data Secure-capable can also be commissioned with the ETS in a conventional manner and consequently communicate with unsecured telegrams at runtime. The behaviour is the same as for devices that are not KNX Data Secure-capable. In this way, modern KNX Data Secure-capable devices can also be used in existing systems to replace defective actuators or sensors (see figure 7). It is not required to modify the entire KNX system or parts of it, or to update it to secure communication.

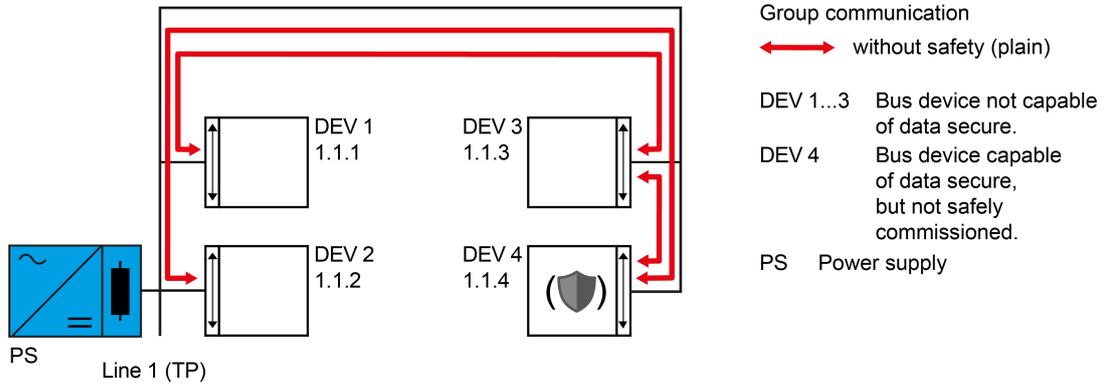


Image 7: Topology diagram 6 (example)

"KNX Data Secure-capable device commissioned in an unsecured manner to replace another device"

Expert knowledge
<p>With KNX Data Secure, the data protocol information (APCI) and the payload (data) of a telegram is encrypted. Telegram header, source and destination address are only transmitted with signature (in plain text). This has the advantage that telegrams secured via KNX Data Secure do not require decryption for telegram routing through area/line couplers or media couplers. The use is therefore media-neutral and does not impair the transaction speed of transmitted telegrams as compared to unsecured communication.</p> <p>KNX Data Secure uses CCM mode with 128-bit AES encryption (data encryption "<u>C</u>ounter mode" with integrity protection "<u>C</u>BC-<u>M</u>AC mode") and symmetric keys. A symmetric key means that the same key is used both by the sender to encrypt outgoing messages (authentication and integrity protection) and by the recipient(s) to verify and decrypt the received messages.</p>

Digression – KNX IP Secure

KNX IP Secure allows KNX telegrams to be authenticated and encrypted in IP networks. This ensures that KNX tunnelling or routing messages on IP cannot be read or manipulated. The KNX IP Secure mechanisms are an additional security layer (wrapper) that protects the complete KNXnet/IP data traffic.

KNX Data Secure and KNX IP Secure can be used coexistently in KNX installations. It is possible to simultaneously secure IP communication between several IP routers or between IP data interfaces and the ETS via KNX IP Secure and, in addition, normal data traffic via group addresses including commissioning communication via KNX Data Secure (see figure 8).

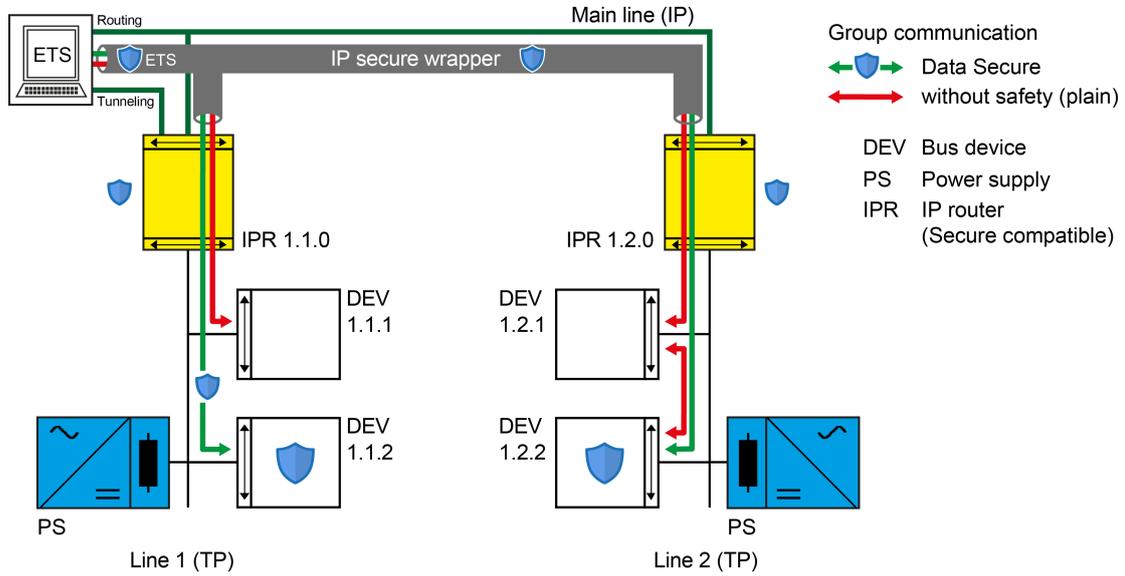


Image 8: Topology diagram 7 (example)
 "Secured and unsecured communication across lines when using IP routers"

2 Why KNX Data Secure?

Benefits

The mechanisms used in KNX Data Secure enable secure communication between KNX devices and the ETS. But how does it work? What benefits are derived from the safety modules for the system and consequently for the users of a KNX Data Secure-compliant KNX installation?

The following list explains the individual components of the KNX Data Secure mechanism and the technical benefits of securing a system in this way:

- Freshness

The "freshness" prevents an attacker from recording permissible telegrams at any time and replaying them again later. This reliably prevents repeating telegrams to trigger known, older actions in a KNX system (e.g. opening a garage door via an illicitly recorded 1-bit switching command).

A receiver only evaluates "fresh" telegrams from a sender.

In combination with data integrity (see next section), "freshness" is an effective security method to prevent unauthorised access to a KNX installation if a person illegally comes into possession of known, possibly recorded, telegram sequences.

- Data integrity

Data integrity effectively prevents an attacker from obtaining control over a KNX system. It prevents telegrams from being manipulated or additional (incorrect) information from being input. This is done by inserting an encrypted authentication code into each telegram. Recipients can use this code to verify whether a message has been illicitly modified.

- Authentication

Authentication is used to verify the identity of the telegram. It ensures that the source of a telegram is indeed an authorized communication partner. A receiver rejects a received commissioning or group telegram if the source address (physical address) of the telegram is unknown.

- Confidentiality

The telegram confidentiality prevents the reading of telegrams at runtime (group communication) and during ETS commissioning by means of encryption. This means that hackers no longer have access to KNX installation data transmitted. It is no longer possible to interpret telegram contents (e.g. ON, OFF, values) without having the group or ETS keys.

Expert knowledge
<p><u>Freshness</u></p> <p>With KNX Data Secure, "freshness" is ensured via a 6-byte long transmission sequence number. A secure communication partner (e.g. actuator) only evaluates a group telegram as valid if the contained sequence number of a sender (e.g. push-button sensor) is at least one value higher than the last received value of the same</p>

Expert knowledge

sender. Telegrams that have a lower or the same value are rejected by the receiver. The transmission sequence number do not always have to be exactly one value higher (n+1). It is important that the number is continuous (n+x).

During a master reset, the transmission sequence number is automatically reset to an initial value by the devices. When replacing a device, the ETS attempts to detect reset devices and replaces the initial value with a valid transmission sequence number using a predefined method.

During a programming procedure, separate sequence numbers are used by the ETS and the device. Transmission sequence numbers can be viewed in the group monitor of the ETS. They are not encrypted, but protected against manipulation.

Expert knowledge

Data integrity

KNX Data Secure uses the "CBC-MAC-Mode" with 128-bit AES encryption included in CCM mode to ensure data integrity. A "Message Authentication Code" (MAC) is attached to the message. This authentication code signs all information contained in the telegram so that manipulation can be detected.

Expert knowledge

Authentication

The identity of a received telegram is verified via the contained physical address of the sender (source address). A recipient only authorizes the telegram if the source address contained was entered in a special communication table. All KNX Data Secure-capable participants have such a communication table. It is automatically programmed by the ETS during commissioning. The table contains a combination of the physical addresses of the permitted communication partners and their transmission sequence numbers in the form of a sorted list.

Telegrams of device addresses that are not entered into the communication table are rejected by recipients. This effect is particularly important if individual devices of an ETS project have been commissioned in advance and an extension of the same project is subsequently made by further participants (sensors or actuators).

Note: All participants that are to communicate properly with each other in a secure KNX system at runtime must be finally programmed (repeatedly, if necessary) in the ETS after final project design has been completed! The correct programming status of all devices in an ETS project can be determined via the programming flags. When changing or adding to an existing configuration (e.g. linking group addresses), the programming status of other linked participants must always be checked as well. It is recommended to use ETS dynamic folders. This way, new devices to be programmed are reliably identified.

Expert knowledge

Confidentiality

AES-128-CCM algorithms with symmetric keys are used to encrypt telegrams. With KNX Data Secure, the data protocol information (APCI) and the payload (data) of a telegram is encrypted. Telegram header, source and destination address are only transmitted with signature (in plain text).

3 What does this mean?

Terms and definitions

When using KNX Data Secure, installation engineers, integrators and ETS users are confronted with new terms and elements that did not exist before, but which are particularly important and therefore must be observed. This chapter lists all elements that are important in the context of KNX Data Secure and describes them.

- i** The illustrations and text representations used are exemplary and are intended to symbolize the different elements and help to differentiate the terms.



The Factory-Default-Setup-Key (FDSK) is used for the initial commissioning of a KNX Data Secure-capable device, but only if this device is to be safely commissioned with the ETS. The FDSK already becomes invalid during the initial secure commissioning when writing the physical address and is replaced by the Toolkey (see below).

The FDSK is 128-bit long and represents the manufacturer's initial key of a KNX Data Secure-capable device. It is available for every Data Secure-capable device worldwide. The FDSK is included in the device certificate (see "Device certificate" below), which is attached to the device upon delivery.

Providing the FDSK has been successfully read in during initial commissioning, it is archived in a readable form in the ETS project together with the device certificates. It can be restored by a master reset of the device and consequently reactivated so that the device can be recommissioned as delivered. In case the device certificate attached to the devices and consequently the FDSK is lost, a device can no longer be securely commissioned by other ETS projects!



The Toolkey is exclusively used by the ETS to program a KNX Data Secure-capable device. It is also 128-bit long, unique for one device in the project and replaces the FDSK already upon initial commissioning. The ETS then uses the Toolkey for each programming procedure in secure mode. Without this special key (e.g. access via other ETS projects), a securely commissioned device can only be reprogrammed if a configuration is lost (see "Master reset" below).

The Toolkey is archived in the ETS project in unreadable form for the ETS user because it is only relevant for ETS in the existing project. If the project is exported, the ETS writes all Toolkeys of the project in an encrypted and signed form to the *.KNXPROJ file.



The Laufzeitschlüssel are the AES keys for group address communication at runtime (also called "Runtime Keys" or "Group Keys"). In an ETS project, each group address has its own 128-bit long runtime key, provided the address is used for secure communication between KNX Data Secure devices.

As with the Toolkey, the runtime keys are archived in unreadable form for ETS users in the ETS project and are written to the project file in a protected form when exporting the project. If required, all or selected runtime keys of an existing project can be exported to a special password-protected export file (*.knxkeys), also known as a project keyring. This export is required if components are to interact with a KNX Data Secure system, but are not configured and commissioned with the ETS (e.g. visualizations). In such cases, the ETS can be used to export a runtime keyring and provide it to the required components via import.

000A:2E671611

The serial number is a 6-byte long identification number of the manufacturer for unique identification of KNX devices. The serial number is determined individually in the course of production (unique for each manufacturer worldwide) and is programmed into the devices in an unchangeable form.

The ETS uses the serial numbers to identify new and already commissioned devices in a KNX installation. The serial numbers are used to qualify read-in device certificates and select them for the commissioning process (siehe Kapitel "Commissioning" ▶ Page 23).

The serial numbers of all read-in device certificates in the project and of all commissioned devices are archived by the ETS in the project keyring and can be viewed there.

AAFC4Z-YWCGQK-DIVDUS-S2NJ5I-VGVKXL-FNV2XS

The device certificate is a character string (36 characters) containing the FSDK and the serial number of a KNX Data Secure-capable device. The device certificate must be communicated to the ETS prior to commissioning in order to be able to securely commission a device. The ETS derives the FSDK corresponding to a serial number from the certificate.



The device certificates are printed on removable labels attached to the devices. These labels must be removed from the devices already during mounting and stored safely! Otherwise, it cannot be ruled out that unauthorised persons obtain the FSDK and manipulate existing devices of a secure KNX installation.



The QR code supplements the character string of the device certificate. It contains the device certificate in machine-readable form and can be read into a project via a PC camera (e.g. webcam) using onboard ETS equipment.

-  A high resolution camera should be used to scan the QR code.



The master reset is a function for resetting a KNX Data Secure-capable device to a functional state intended by the manufacturer. When executing a master reset all user settings are lost. The parameterization is reset to the default setting, the physical address is initialized to 15.15.255, all runtime keys and the Toolkey are deleted, provided the device has been in secure mode prior to reset. In addition, the FDSK becomes active again in the device. The device must then be recommissioned with the ETS.

During secure operation: A master reset deactivates device security. The device can then be securely recommissioned with the device certificate (FDSK).

The firmware of a device is not affected by a master reset. Triggering and signalling of the master reset is device-specific and is explained in the respective product documentation.



Devices can be reset to factory settings with the Gira ETS Service App. This function uses the firmware contained in the device that was active at the time of delivery (delivery state).

Restoring the factory settings causes the devices to lose their physical address and configuration. As with the master reset, the devices must then be recommissioned with the ETS.

See the documentation of the Gira ETS Service App for details on the factory reset.

4 How do I identify KNX Data Secure?

Labelling of KNX Data Secure-capable devices

A device is KNX Data Secure-capable if it can be commissioned securely by the ETS and then communicate securely at runtime (secure group communication). Devices that support KNX Data Secure in this way can be identified by a "X" on the product label or print image. This is a KNX-compliant and manufacturer-independent marking. In addition, KNX Data Secure-capable devices from Gira are marked with a "Secure Shield" symbol .

Devices with the above-mentioned markings are compatible with each other and are KNX Data Secure-capable without restrictions.



Image 9: Example of device labelling of a KNX Data Secure-capable device

-  + X KNX Data Secure-capable device
-  Medium TP (Twisted Pair)
-  S-Mode (ETS-compatible)

KNX Data Secure-capable devices do not necessarily have to be commissioned securely. It is possible to disable security in the ETS for all or individual devices of a project. Devices for which security has been deactivated always communicate in an unsecured manner and behave exactly like devices which are not KNX Data Secure-capable with regard to commissioning and runtime communication, and which consequently lack the above-mentioned markings. Whether KNX devices actually communicate securely can be gathered from the project and not from the label on the product, which only shows the capability.

-  KNX Data Secure-capable devices, which have been securely commissioned by the ETS and also exchange secure data with other KNX Data Secure-capable devices via communication objects at runtime, can generally also communicate in a conventional and unsecured manner via selected group addresses. Mixed operation of safe and conventional communication on a sensor or actuator via different communication objects is possible. However, secured and unsecured communication via one and the same communication object is not possible!

Marking in the ETS

The ETS marks KNX Data Secure-capable devices with a "Secure Shield" symbol. It is displayed in the list view of the devices and in the tree structure of an open ETS project and does not refer directly to the device (hardware), but rather to the application program used (see figure 10).

Using the ETS5 as an example: If a symbol is displayed in the "Sicherheit" column of the list view, this is a KNX Data Secure-capable application program. The colour of the symbol indicates that it is either an application program with activated device security (1) , or alternatively that device security is deactivated in the application used (2) . Application programs for which no such symbol is displayed in the list view (3) are generally not Data Secure-capable.

In the tree structure, devices are also identified with a "Secure Shield" symbol  (4), depending on the application program used. At this point, however, this is only done for application programs with activated device security.

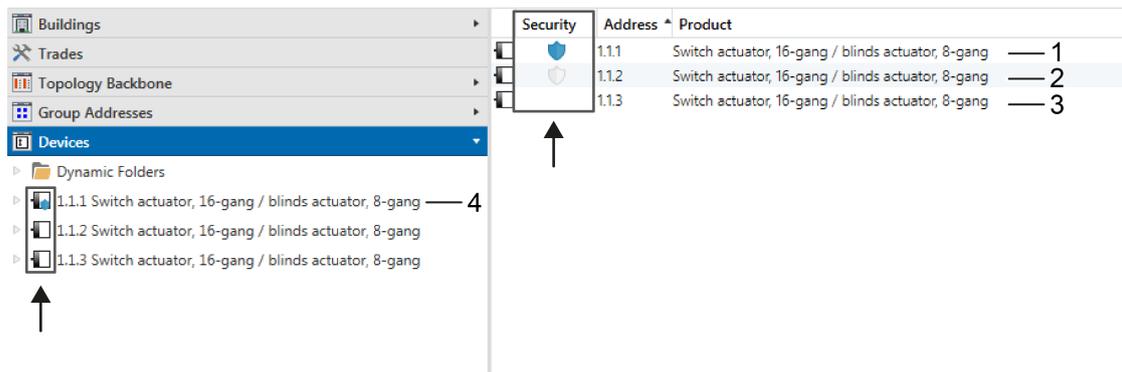


Image 10: Example of device identification (ETS5) in an ETS project

- (1)  KNX Data Secure-capable device with activated device security
- (2)  KNX Data Secure-capable device with deactivated device security
- (3) KNX Data Secure-incapable device (no device security)
- (4)  KNX Data Secure-capable device with activated device security

Identification of KNX Data Secure-compatible system devices

In addition to devices that are directly and independently KNX Data Secure-capable, there are also system components that are compatible with Data Secure. Proper commissioning by the ETS and stable cross-line runtime communication is only possible by using KNX Data Secure-compatible system devices (e.g. area/line couplers, media couplers, IP routers and USB data interfaces)!

System devices from Gira that have KNX Data Secure compatibility are identified by a "Secure Shield" symbol  on the label or print image. The "X" marking as found on KNX Data Secure-capable devices is missing.

If the system components used do not support KNX Data Secure, the symbol is missing on the device. Consequently, these components are not compatible with Data Secure! Secure runtime communication or commissioning across such system devices is not possible.



Image 11: Example of device labelling of a KNX Data Secure-compatible device (e.g. KNX RF/TP media coupler/repeater)

- i** KNX Data Secure-compatible system devices are not specially marked by symbols in the ETS.
- i** The appendix of this documentation contains an overview of the system components. This device overview can be used to identify which system components are compatible with KNX Data Secure.

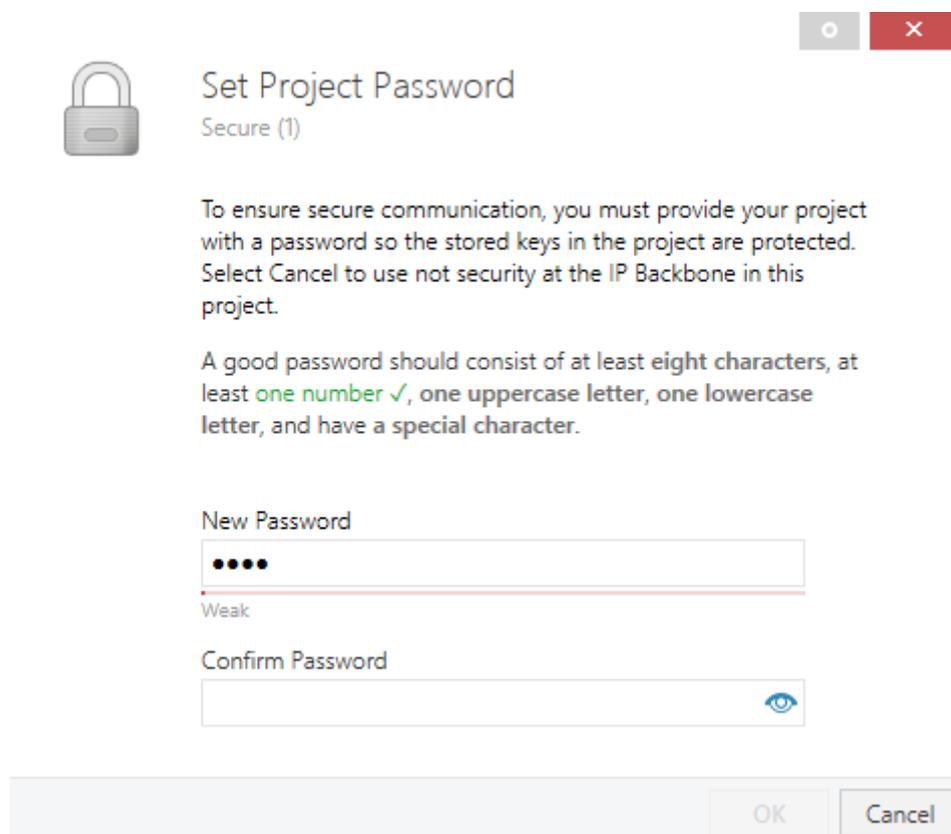
5 How does KNX Data Secure work in the ETS?

5.1 Project design

Project password

ETS projects using KNX Data Secure always require a project password. The password protects the secure keys (Toolkeys, runtime keys) used in the project as well as the security-relevant settings and device properties. The project password also protects the secure contents of an exported project file (*.knxproj) from being modified. It is thus not possible to read the secure data of the project file.

The project password is assigned and edited in the ETS dashboard in the project details by the user. When opening or importing a secure project, the project password must always be entered.



Set Project Password
Secure (1)

To ensure secure communication, you must provide your project with a password so the stored keys in the project are protected. Select Cancel to use not security at the IP Backbone in this project.

A good password should consist of at least eight characters, at least one number ✓, one uppercase letter, one lowercase letter, and have a special character.

New Password
●●●●
Weak

Confirm Password

OK Cancel

Image 12: Setting a project password using the example of the ETS5

When adding a KNX Data Secure-capable device to a project, the ETS always asks for a project password automatically, in case a password has not been assigned yet. If the added devices are to be used securely in the project, a password must be assigned! If the "Set Password" dialog is cancelled, the devices can only be used conventionally. The ETS then automatically sets the device security to "unsafe". When subsequently activating the device security of any device in the project, the ETS requires a new password to be set.

- i** If the password is unknown or lost, the ETS project can no longer be used! The project design data contained in the project as well as all the relevant commissioning and runtime keys are also lost! The devices contained in the affected KNX system can then no longer be reprogrammed or otherwise modified by the ETS! The affected system can only be reconfigured in this case (affected devices must be reset via a master reset and then recommissioned).
- i** If a project password is deleted, the ETS deactivates the device security for all devices in the project following confirmation, provided the settings of the secure group addresses used permit this (see "Project design of group addresses" below).

Device security (secure commissioning communication)

Devices that are to communicate securely via group addresses at runtime must also be commissioned securely by the ETS. If devices are conventionally programmed with the ETS, runtime communication is always done in an unsecured manner. In the ETS project, the ETS user has the possibility to switch the device security for each KNX Data Secure-capable device on or off. This is done in the properties of each device using the safety attribute "Secure commissioning" (see figure 13).

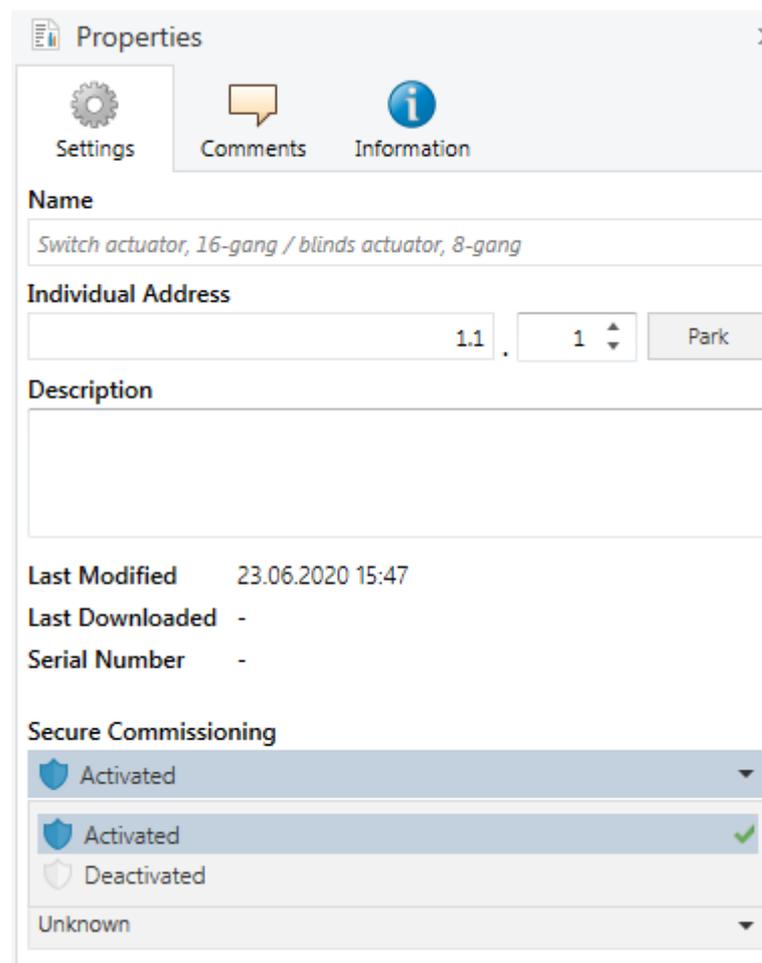


Image 13: Editing the device security of a KNX Data Secure-capable device using the example of the ETS5

- Secure commissioning = "🛡️ Activated"

This is the default setting for the security attribute of a device, if it supports KNX Data Secure. When such a device is added, the ETS activates device security by default. The affected device is securely commissioned by the ETS. The ETS then requires the appropriate device certificate during programming and assigns an individual Toolkey during the commissioning process. Activating secure commissioning is the prerequisite for the device to be able to be assigned secure group addresses (see "Project design of group addresses" below).

- Secure commissioning = "🛡️ Deactivated"

With this setting, the ETS commissions the corresponding device conventionally. Commissioning then resembles the familiar programming process of an older device that is not KNX Data Secure-capable. If a device has been conventionally commissioned by the ETS, it is not possible to implement secure group communication at runtime. No secure group addresses can be assigned to the communication objects of these devices.

i The device security can be changed at any time in the ETS project, even for devices that have already been commissioned. Please note that changing a security setting means that devices must be reprogrammed afterwards! When secure commissioning is deactivated, all security configurations of the affected devices are lost. The ETS then checks the assigned group addresses according to their security settings and provides the ETS user with a dialog that shows which addresses will no longer communicate securely or even be removed from the device.

i A device securely commissioned via an ETS project can only be reprogrammed with the same project and then reconfigured as required. Deactivating the device security can also only be done with the same project. If another ETS project is used that does not have the toolkey of the device, the device can only be reset via the master reset and then recommissioned.

Project design of group addresses (secure runtime communication)

The purpose of KNX Data Secure is to secure the communication at group telegram level from sender to receiver at runtime of a system (end-to-end protection). Group addresses are created by the ETS user and are given a special security attribute that can be subsequently edited (see figure 14). It is possible to define group addresses so that they either always communicate conventionally, always securely, or automatically conventionally or securely (depending on the objects assigned).

Only secure group addresses in an ETS project have their own 128-bit long runtime keys. Runtime keys cannot be changed.

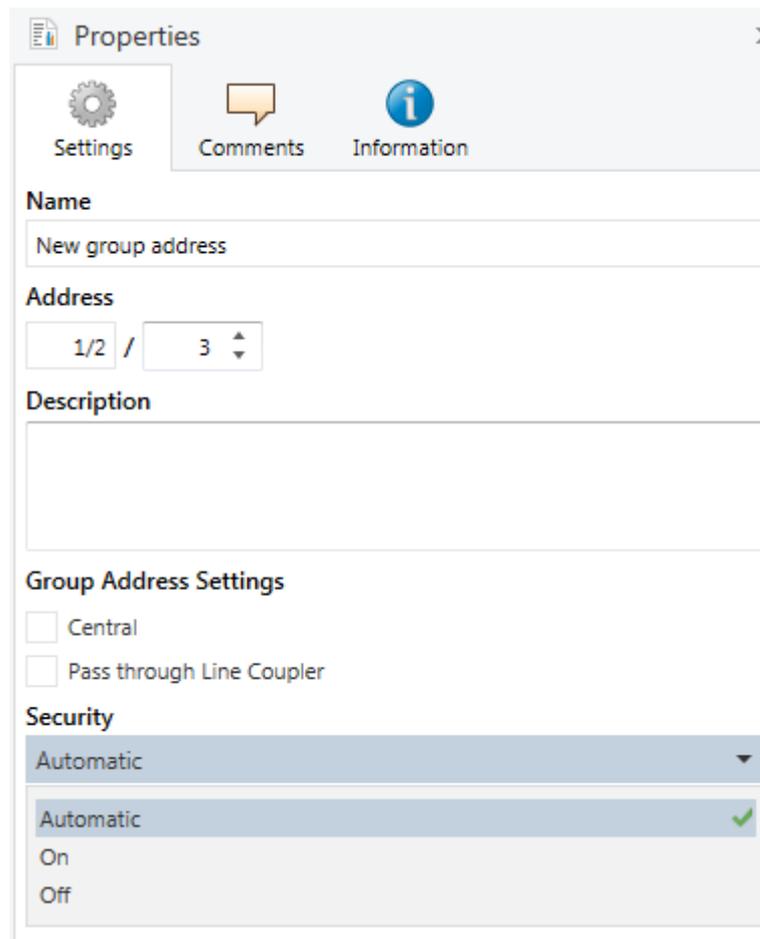


Image 14: Editing the security attribute of a group address using the example of the ETS5

The following table explains the different security attributes of group addresses in the ETS.

- Security = "Automatic"  / 

This is the default setting for the security attribute of a group address. In this case, the ETS always decides autonomously whether the group address communicates securely or conventionally. This depends on whether the address is only assigned to objects that support secure communication (Data Secure-capable devices), or also to objects of devices that are not Data Secure-capable. If the respective group address is assigned exclusively to objects that can communicate securely, the ETS always activates secure communication. However, if the respective group address is assigned to a communication object that does not support secure runtime communication, the ETS automatically switches off secure communication for this group address! In such cases, the ETS informs the ETS user that the assigned objects can only communicate conventionally.

Example

There are three devices in a KNX installation (1 x sensor and 1 x actuator A, both are Data Secure-capable / 1 x actuator B that is not Data Secure-capable). An object of the sensor is assigned to an object of actuator A. The ETS chooses secure communication and assigns a runtime key to the respective group address. That same group address is then also assigned to an object of actuator B. The ETS recognizes that the new connection can no longer communicate securely, removes the runtime key and switches off security at the affected address. From this point on, all affected devices will only communicate conventionally via the assigned objects!

– Security = "On" 

With this setting, the ETS forces a secure runtime communication of the assigned communication objects. Consequently, this address can only be assigned to objects that support secure communication. The group address can therefore not be assigned to devices that are not KNX Data Secure-capable!

– Security = "Off" 

With this setting, the ETS forces a conventional runtime communication of the assigned communication objects. If such a group address is assigned to objects, the group communication is always conventional (even if the objects do support secure communication).

KNX Data Secure-capable devices, which have been securely commissioned by the ETS and also exchange secure data with other KNX Data Secure-capable devices via communication objects at runtime, can generally also communicate in a conventional and unsecured manner via selected group addresses. Mixed operation of safe and conventional communication on a sensor or actuator via different communication objects is possible. However, secured and unsecured communication via one and the same communication object is not possible!

i In the application programs of KNX Data Secure-capable devices, manufacturers can also set security attributes for the communication objects. For example, it is possible to only specify secure communication for an object. The manufacturer can thus force secure group communication at runtime across all or individual objects of a device. In such cases, it is no longer possible to assign conventional group addresses to the communication objects. As a rule, the communication objects of the application programs do not force secure communication, meaning the ETS users can define via the security attributes of the group addresses whether an address should communicate securely or conventionally.

i Security attributes of group addresses can be changed at any time in the ETS project. Please note that changing a security setting means that devices must be reprogrammed afterwards! This means that all devices assigned to the group address whose setting is changed will be affected (observe the programming flags of the devices). This is particularly important for central addresses in an ETS project that have been assigned to multiple devices. It is recommended to use a dynamic folder in the ETS and to configure it so that it always contains all devices still to be programmed.

5.2 Commissioning

Using system components

KNX Data Secure devices use a longer KNX telegram format for the transmission of authenticated and encrypted data, mainly due to the 128-bit long keys contained (Extended Frames). However, this has no effect on the reaction speed of the devices, which can easily be used with conventional devices in the same installation and on the same media. This means that KNX Data Secure can be used as an additional measure to implement reliable security for selected devices or functions in new or existing systems.

Due to the longer telegram format, the system components used (e.g. area/line coupler/media coupler) and the local data interfaces of the ETS (e.g. USB, IP tunnelling, IP routing) must also support Extended Frames. If this support is not provided, the ETS cannot perform secure commissioning and displays an error during the programming process.

The ETS user must therefore ensure that the local data interface of the ETS and all system components located between the ETS and the device to be programmed support Extended Frames. This is particularly important if existing KNX installations are to be enhanced with KNX Data Secure.

The appendix of this documentation contains an overview of the Gira system components. This device overview can be used to identify which system components are compatible with KNX Data Secure.

Expert knowledge

When using RF/TP media couplers, the telegram format is not the only decisive factor for KNX Data Secure compatibility. For a media coupler to correctly process and forward a KNX Data Secure telegram at runtime (routing), a system property must be present in the device that enables the forwarding of secured telegrams. The device overview in the appendix of this documentation contains a list of available media couplers and explains which device version is compatible with KNX Data Secure.

Reading in device certificates

In order for the ETS to securely commission a device, it requires the appropriate device certificate. The device certificate is a character string, containing the FSDK and the serial number of a KNX Data Secure-capable device. The device certificate must be communicated to the ETS prior to the programming process in order to be able to securely commission a device. The ETS derives the FSDK corresponding to a serial number from the certificate and uses this for initial commissioning communication.

- i The device certificates are printed on removable labels attached to the devices. These labels must be removed from the devices already during mounting and stored safely! Otherwise, it cannot be ruled out that unauthorised persons obtain the FDSK and manipulate existing devices of a secure KNX installation.

Device certificates can be read into the ETS at different locations and in different situations.

- Project dashboard

In the ETS dashboard, the project keyring for each project can be viewed under the "Security" tab in the form of an overview of all read-in device certificates. Initially this list is empty for a new project. The device certificates can be added step by step (individually) by clicking the + button (see figure 15). The ETS then opens the dialog for reading in the device certificate via keyboard or camera (see figure 16).

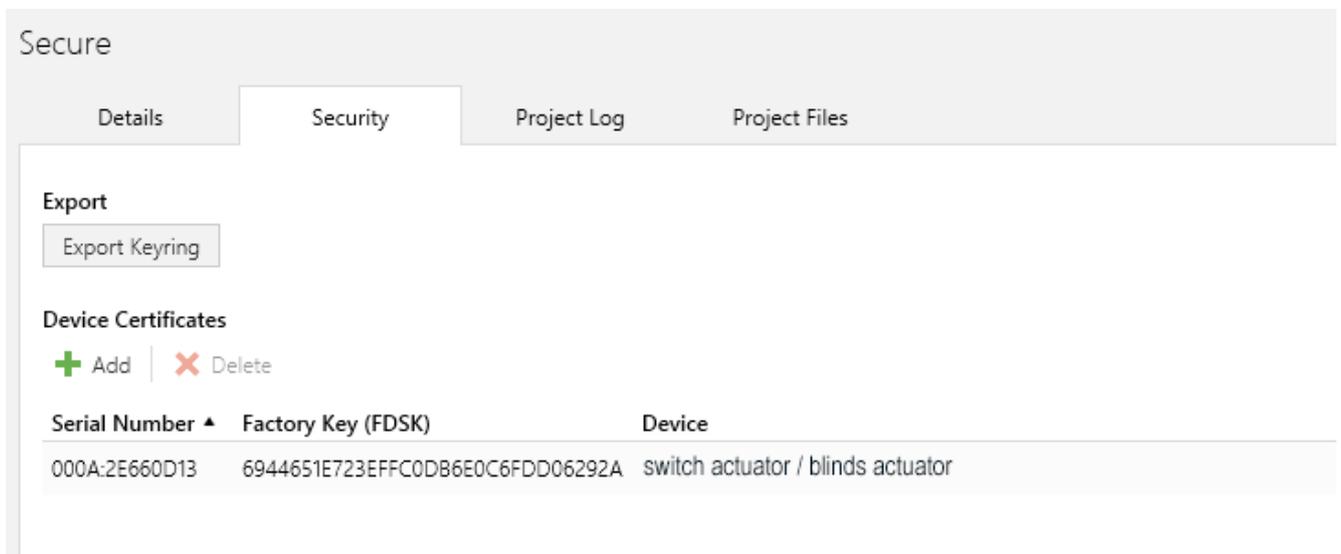


Image 15: Example of an overview of the device certificates for a project in the ETS dashboard (ETS5)



Adding Device Certificates

Secure

Please scan or enter the device certificates for all devices in your project that you intend to download using secure commissioning.



AAFC4Z - QNCPQZ - WVMHEH - 44OTTO - KOPUKJ - Z2FQCQ ✓

Serial Number 000A:2E660D13

Factory Key 6944651E723EFFF0DB6E0C6FDD06292A

OK

Image 16: Example of the dialog for reading in a device certificate (ETS5)

- i** The project keyring shows all device certificates (serial number + FDSK) read into the ETS project. If a certificate has already been successfully used for commissioning (known serial number), the device name and physical address of this device are also listed. If the device name and physical address are missing, the certificate has only been read in successfully and has not yet been used by the ETS.
- i** The ETS determines whether a read-in certificate is already present in the project keyring. In this case the existing certificate remains unchanged.
- i** A high resolution camera should be used to scan the QR code.

– In the project in the device settings

As an alternative to the ETS dashboard, it is also possible to add existing device certificates directly to an open project. To do this, select a device in the properties under "Settings" and click the "Add Device Certificate" button. The ETS then opens the dialog for reading in the device certificate via keyboard or camera.

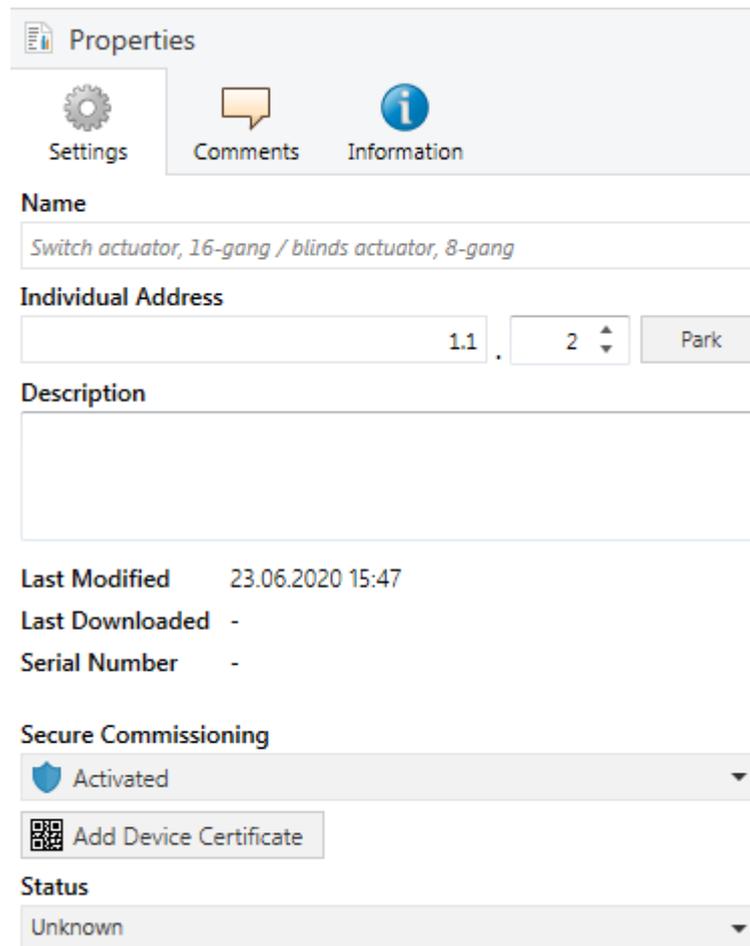


Image 17: Example of a setting for reading a device certificate directly into the ETS project (ETS5)

- i** A device certificate added in the device settings is immediately assigned to the selected device in the project. The serial number contained in the certificate is visibly transferred to the device settings. The ETS also transfers the certificate to the project keyring (ETS dashboard).
- i** If the read-in device certificate is already being used with another device in the same project, the ETS displays a notification message in the read-in dialog. If the confirmation is positive, the ETS assigns the certificate to the device for which the certificate was last read in. The serial number and programming flags of the previously assigned device are then deleted.
- When adding a KNX Data Secure-capable device
 Already when adding a new KNX Data Secure-capable device to a project (from the product catalogue or when copying a device), the ETS requests the device certificate (see figure 18) from the user, if device security has been activated for this device. When adding individual devices, this method is very helpful and helps to collect all device certificates relevant for the planned commissioning in the project as early as possible.



Adding Device Certificate

--- Schaltaktor 24fach 16 A/Jalousieaktor 12fach 16 A Komfort

This device supports secure commissioning.

If you have the certificate of the device available, you can scan the QR code or enter it now.



AAFC4Z - QNCPQZ - WVMHEH - 44OTTO - KOPUKJ - Z2FQCQ ✓

Serial Number 000A:2E660D13

Factory Key 6944651E723EFFC0DB6E0C6FDD06292A

Don't ask when adding devices OK

Image 18: Example of the dialog for reading in a device certificate when adding a device (ETS5)

- i** In some situations, especially when setting up a new project or when certificates are not yet available, the request to read in device certificates can be disruptive when adding devices. For this reason, the ETS offers the possibility to abort the certificate read-in process and to read in the information at a later time ("Later" button). Alternatively, the dialog can be disabled for the entire project when adding devices. For this, click the "Don't ask when adding devices" checkbox in the dialog or deselect the "When adding secure device ask for device certificate" option in the project settings on the ETS dashboard (ETS5: "Settings -> Presentation -> Security").
- i** When a device certificate is added, it is immediately assigned to the newly added device in the project. The serial number contained in the certificate is visibly transferred to the device settings. The ETS also transfers the certificate to the project keyring (ETS dashboard).
- i** If the read-in device certificate is already being used with another device in the same project, the ETS displays a notification message in the read-in dialog. If the confirmation is positive, the ETS assigns the certificate to the device for which the certificate was last read in. The serial number and programming flags of the previously assigned device are then deleted.

– Immediately prior to the programming process

At the latest when the ETS is to securely commission a KNX Data Secure-capable device (programming of the physical address), the device certificate and the contained serial number and FDSK become relevant. When secure commissioning is activated, the ETS therefore always requests the device certificate during programming if it does not yet have a certificate in the project keyring for the serial number read in from the device. In such a case, the ETS opens the dialog for reading in the device certificate via keyboard or camera (see figure 19).

As soon as a valid device certificate is entered via keyboard or camera, the ETS immediately starts the programming process. If a device certificate is not available, click on the "Plain" button. In this case, the ETS deactivates secure commissioning for the respective device and commissions the device conventionally. The ETS then checks the assigned group addresses according to their security settings and provides the ETS user with a dialog that shows which addresses will no longer communicate securely or even be removed from the device.

Alternatively, click on the "Skip download" button. This will cause the ETS to cancel the programming process of the device displayed in the dialog.



Add Device Certificate

1.1.1 Schaltaktor 16fach 16 A/Jalousieaktor 8fach 16 A Komfort
Serial Number 000A:72FF1812

This device is configured for secure commissioning but its device certificate is missing. If you do not have access to this information now, you can either skip the download or deactivate secure commissioning by selecting "Plain".



_____ - _____ - _____ - _____ - _____ - _____

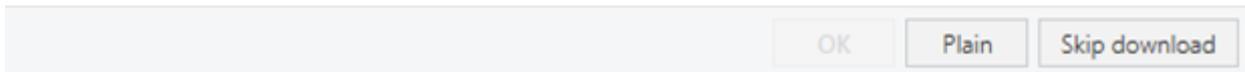


Image 19: Example of the dialog for reading in a device certificate when programming a device (ETS5)

- i** A device certificate added during programming is assigned directly to the device in the project and used during programming. The serial number contained in the certificate is visibly transferred to the device settings. The ETS also transfers the certificate to the project keyring (ETS dashboard).
- i** If the read-in device certificate is not suitable for the device to be programmed (serial number of the device not identical to the serial number of the read-in certificate), the ETS does not accept the device certificate and does not carry out the programming procedure.

5.3 Compatibility and versions

In general, KNX Data Secure is supported in the ETS5 from version 5.5.0. It is recommended to use the ETS5 at least from version 5.7.4 or the ETS6 for project design and commissioning of KNX Data Secure-capable devices! The use of older ETS versions can lead to errors during project design as well as problems during commissioning (e.g. when replacing devices) and diagnosis of group addresses and devices.

- i** The ETS2, ETS3, ETS4 and ETS5 up to and including version 5.0.8 are generally not suitable for using KNX Data Secure.

6 What else should I observe?

Basic recommendations for protecting a KNX installation

If you want to effectively protect your KNX installation, you should start with the protective measures already during installation. KNX Data Secure is designed to make commissioning and runtime communication tamper-proof. However, this method does not provide protection against unauthorized manipulation or modification of the KNX line and hardware used. Other protective mechanisms must be applied for this.

As a general rule, devices and lines should be permanently installed to prevent damages or quick removal, which would allow unauthorised persons to access the KNX installation. The following protective measures are generally recommended with regard to mounting...

- Main and sub-distribution units with KNX devices should be locked and located in rooms to which only authorised persons have access.
- The manufacturer's mounting instructions should be observed, particularly with regard to theft protection. Flush-mounted devices should be mounted in suitable flush-mounted or hollow-wall sockets and firmly connected to the installation environment (e.g. by means of the screw connection provided by the manufacturer).
- In outdoor areas, devices (e.g. weather station, wind sensor, motion detector) should be mounted at a sufficient height so that they are protected against unauthorised access.
- In public areas (e.g. shopping centres, schools), the use of conventional control devices instead of KNX devices should be preferred. The conventional devices can then be electrically connected to the KNX components (e.g. button interfaces, binary inputs), which are ideally mounted in an access-controlled installation environment. This significantly hinders access to the KNX installation (bus line).
- KNX lines or devices in outdoor areas always present an increased risk. If an outdoor application cannot be avoided (e.g. for networking other properties or building parts), access to the KNX line should be made particularly difficult (e.g. by laying KNX cables or protective pipes underground). In principle, KNX installations in unprotected areas (outdoor area, underground car park) should be designed as a separate TP line or RF domain.
- In case of IP communication, a separate LAN or WLAN network with its own hardware (router, switches) should be used. It is essential to use the standard security mechanisms for IP networks (MAC filters, encryption of wireless networks using strong passwords). Alternatively, it is also possible to use a virtual local network (VLAN).

In addition to the safety measures that have to be taken into account already during mounting, there are also rules to be observed when configuring couplers or IP routers. These rules include...

- Configuring existing area/line couplers or media couplers so that filter tables are active.

- If possible, activating the programming protection (rejection of physically addressed telegrams) in couplers that connect public or outdoor areas via their subordinate line after commissioning of a system.
- Also blocking point-to-point communication and, if possible, also broadcast communication across couplers and routers after commissioning. In this way, unauthorized modification of device configurations is limited to a single line.
- For Internet access to KNX installations: Using VPN connections (no public port forwarding etc.) or manufacturer-specific solutions specifically designed for secured Internet access.

7 Appendix

7.1 Overview of system components

Product designation	Article number	Release	APDU [byte]	Data Secure compatible
Area / Line coupler RMD	1023 00	I00	40	no
Area / Line coupler RMD	1023 00	I01	55	yes
Area / Line coupler RMD	1023 00	I02	55	yes
Area / Line coupler RMD	1023 00	I03	55	yes

Table 1: Area / Line coupler

- i** Older couplers (582 00, 611 00, 1096 00) are generally not KNX Data Secure-compatible.

Product designation	Article number	Release	APDU [byte]	Data Secure compatible
RF/TP Media coupler/repeater	5110 00	I00	233	no
RF/TP Media coupler/repeater	5110 00	I01	233	yes

Table 2: Media coupler

Product designation	Article number	Release	APDU [byte]	Data Secure compatible
USB data interface RMD	1080 00	all	15	no
USB data interface concealed	1070 00	all	15	no
USB data interface	2014 00	all	233	yes
USB data interface insert	2024 00	all	233	yes
RF USB data interface	5120 00	all	240	yes

Table 3: USB data interfaces

- i** Older RS-232 data interfaces (0504 xx, 0558 xx, 1153 00) are generally not ETS5-compatible and therefore not KNX Data Secure-compatible.

Gira
Giersiepen GmbH & Co. KG
Elektro-Installations-
Systeme

Industriegebiet Mermbach
Dahlienstraße
42477 Radevormwald

Postfach 12 20
42461 Radevormwald

Deutschland

Tel +49(0)21 95 - 602-0
Fax +49(0)21 95 - 602-191

www.gira.de
info@gira.de