KNX Secure
Some Basics

1 Introduction

1.1 Preface

Dear customer,

The KNX world is starting into a new era – the age of digital encryption.

We at Lingg & Janke wish to accompany you on the way into the new era and support your KNX projects with our products complying with the latest KNX Secure Standard.

1.2 What is KNX Secure?

KNX Secure is the systematic further development of the KNX standard. Until now, all data transmitted on the KNX bus were open and readable for anyone having access to this KNX bus, thus permitting manipulation. This is no longer possible with KNX Secure.

Data security and privacy can now also be realized in state-of-the-art electrical installations.

In the KNX standard, KNX Secure is divided into KNX IP Security and KNX Data Security.

KNX IP Security is used when KNX telegrams are transmitted via KNX IP line or area couplers and KNX IP gateways.
For all other KNX bus subscribers, KNX Data Security is used, e.g. for "standard" KNX devices connected to a twisted pair line. Accordingly, KNX Data Security is used by almost all Lingg & Janke KNX products.

1.3 How does KNX Data Security work?

KNX telegrams mainly consist of two parts:

an address and controller part (source address, destination address, telegram type) and a data part (switching value, temperature value or device parameter, etc.).

KNX Data Security only encrypts the data part. This has the benefit that by using the source and destination address, the telegram can be routed via the line and area coupler from the sender to the receiver without the necessity of decrypting and encrypting it in each of the couplers.

This permits conventional programming interfaces (USB and IP) as well as standard line and area couplers to be used in paired-wire KNX installations. However, the couplers must be able to process long-frame telegrams. The data part of an encrypted KNX telegram is slightly longer than the data part of a conventional KNX telegram.

To avoid an encrypted KNX telegram (e.g. "Blinds up") being applied multiple times by repetition, the data part is assigned a new number each time it is sent. This sequential number is transmitted unencrypted, but is included in the data encryption. If a sequential number is already known by a recipient, any telegram with the same number will no longer be accepted and will therefore not be executed. Data content is secured, and there are also protective safeguarding mechanisms against data repetition.

1.4 What must be observed for a secure setup?

Since any data content in a KNX Secure telegram can be encrypted, the individual KNX Secure devices can also be set up in secure mode via the ETS®.

To be able to access a KNX device securely, i.e. using encrypted telegrams from the outset, the ETS® requires an initial device key, the so-called Factory Default Setup Key (FDSK).

Lingg & Janke supplies this FDSK for each KNX Secure device as a QR code. The FDSK is also saved in the corresponding device.

Before setup, the QR code of each device is uploaded into the ETS®. The FDSK also includes the serial number of the device, allowing the ETS® to allocate the keys to their devices. When parameterizing the devices via the ETS®, the serial number of the corresponding device is requested each time the programming button is pressed. This allows the ETS® to allocate the matching FDSK and to apply encrypted communication with the device.

To enhance security even further, the ETS® now automatically creates a new device key. This key is transmitted to the device being parameterized using the FDSK. The new ETS® key is named "Tool Key" and becomes valid as soon as it has been transmitted. It is only known to the ETS® or the ETS® project for the specific KNX installation. Thereafter, the FDSK will no longer provide access to the device.

1.5 How are data encrypted?

In the further parameterization, the ETS® automatically assigns an additional new group key and uploads it into the device for each group address assigned to the KNX device. This means that if a KNX device is parameterized with thirty different group addresses, then thirty assigned group keys will be uploaded into the device as well. Each telegram containing a different group address will be encrypted with a different group key, accordingly. This represents an enormous increase in security. There is no such thing as a master key in KNX Secure. Each device has its own ETS® key, and each group address has its own group key.

1.6 How is project security realized?

So far, so good, but we take it further. The ETS® also assigns each KNX device being parameterized its own sequential number. Then, the ETS® informs all devices connected to the installation (within an ETS® project) which device with which physical address may communicate with which other device. The devices of an installation (within an ETS® project) therefore form a closed group. Accordingly, it is mandatory that an installation is set up with only one specific ETS® project. Newly added devices will not be able to immediately communicate with the other devices of a group. Adding a device requires all existing devices with which it is supposed to communicate to be re-parameterized. This ensures maximum security.

Without the ETS® project for a specific KNX installation, there is practically nothing that can be modified in this installation. Anyone owning the ETS® project has unrestricted control over the project. This ensures installation owners and project creators that unauthorized modifications leading to malfunctions are reliably prevented. The ETS® requires a project password for secure setup. If this password is lost, the ETS® project can no longer be used, and the KNX installation can no longer be modified.

However, the actual KNX products can be reused. After a reset to the factory settings (Factory Reset), the device can be programmed again. All keys, group addresses, etc. used by then will be deleted, removing the device from the installation.

1.7 Can KNX Secure devices communicate with KNX devices already installed?

Secure setup and secured, encrypted communication are not mandatory, though. Prior to parameterization, a decision can be made for each device whether it shall be set up in secure mode, i.e. encrypted, or in unsecured mode, i.e. unencrypted. In Lingg & Janke systems, all KNX Secure devices for which a conventional unsecured ETS® application exists, can be set up with the application used by then as well. The KNX Secure device then behave like conventional KNX devices. All Lingg & Janke devices are supplied in unsecured mode.

It is also possible to define encrypted or unencrypted transmission for each group address and for each group telegram created by it. This allows earlier KNX devices not yet supporting KNX Secure to communicate with new KNX Secure devices. Earlier and later devices can therefore be mixed without a problem.

However, if secure communication is the call of duty, secure setup must be used. Otherwise, all group keys could be read out in unsecured mode, and secure transmission would not be ensured.

So far for a brief introduction to KNX Secure.

In practice, all you will notice of these technical features is that you can turn them on or off. Everything else is handled automatically by the devices.

All the best with your KNX Secure devices from Lingg & Janke!

Sincerely, Peter Janke

ETS® is a registered trademark of the KNX Association in Brussels

1.8 Frequently Asked Questions

Must a KNX Secure device be set up in secure mode?
NO
All devices are delivered in unsecured mode. Secure setup can be enabled or disabled in the ETS®.

Must group telegrams for KNX Secure devices always be transmitted encrypted?
NO
In the ETS®, you can define encrypted or unencrypted conventional transmission for each group address and each group telegram created from it. To do so, secure mode is enabled or disabled in the settings. If you select "Automatic", the ETS® decides on its own whether secure mode is possible or not. Secure mode can be established if all participating devices support KNX Secure and are set up in secure mode.

Can earlier KNX devices communicate with later KNX Secure devices?
YES
Secure mode must then be disabled for the corresponding group addresses.

Can KNX Secure devices set up in secure mode be re-parameterized later on?
YES
This requires a reset to the factory settings (Factory Reset).
Proceed as follows: Disconnect the bus connector / Press and hold the programming key / Connect the bus connector / Programming LED lights up / Release the programming key / Wait until the programming LED extinguishes (approx. 5 sec.) / Device is now reset to its factory settings.

Does secure setup require extra effort?
YES
Only minimum effort is required, however.
All QR codes of the products used must be uploaded into the ETS®. This is done using the camera integrated into the notebook or a USB camera connected to it.
The set-up time for each device increases slightly. For Lingg & Janke devices, the additional time required is approx. 10 – 20 sec. In unsecured mode, approx. 30 sec. are needed for the download. This means a total time of approx. 40 – 50 sec. for the secure setup of each device is required.

Does a KNX Secure installation require additional maintenance effort?

NO

However, the availability of the corresponding ETS® project is a prerequisite.
If the ETS® project is open, all telegrams in the ETS® can be displayed and recorded unencrypted.
There is practically no difference to a conventional KNX installation.

Can the keys of an ETS® project be exported?

YES

You can create an XML file with all keys used in this project. This “keyring” file must be protected by a password.

Is there any means of visualizing KNX Secure?

YES

Lingg & Janke offers a matching KNX visualization tool that supports KNX Secure standard. The keys required are transmitted in the “keyring” file.

Should KNX Secure only be used if so required by the customer?

NO

An encrypted KNX project provides optimal project security for the installer or system integrator as well.

Does KNX IP Security provide sufficient security for an entire KNX installation?

NO

KNX IP Security provides security on the IP network only. All telegrams on the remaining parts of the KNX bus are unprotected.
However, the reverse does not apply: If KNX Data Security is used, all telegrams on the KNX bus are secure, including those transmitted via the IP network.

Can I modify a KNX Secure installation if the corresponding ETS® project is no longer available?

NO

Without the corresponding ETS® project containing all keys, you can neither re-parameterize devices nor add any devices. If this was an option, the installation would not be secure.
The only way to go is to reset all devices to their factory settings and to set them up again.

1.9 Notes