KNX SECURITY IN BUILDINGS

KNX Secure Technical Details

Contents

1. Purpose of the Document

This document provides an overview of the KNX Secure Standard, focusing on its two key components: KNX Data Secure and KNX IP Secure. It outlines the benefits of implementing these security measures in building automation systems and explains how they work to protect communication and data integrity. By understanding the functionalities of KNX Data and IP Secure, stakeholders can enhance the security of their KNX installations and safeguard against potential cyber threats.

2. KNX Secure Standard

KNX Secure enhances the KNX standard by introducing advanced security features that safeguard data against unauthorized access and ensure the authenticity and integrity of transmitted messages. As a vendor-neutral solution, it protects KNX communications and systems using end-to-end encryption based on ISO 18033-3 standards, such as AES 128 CCM.

This technology is designed to withstand brute-force attacks and is formally standardized under EN 50090-3-4. It offers robust protection across a range of applications, including:

- Access to the KNX system via the IP network (KNX IP Secure)
- Configuration of devices in the installation (KNX Data Secure, KNX IP Secure Device Management)
- Real-time communication between applications (KNX Data Secure)
- KNX communication over IP networks (KNX IP Secure Routing)
- KNX communication in sub networks and the creation of security zones, where an existing KNX plain installation is extended with KNX Data Secure products. Using the "Secure Proxy" function, secure areas can be established.

Key Features:

- End-to-End Encryption: Ensures that only authorized devices can read or modify data.
- Authentication: Verifies the identity of devices to prevent spoofing.
- Tamper Protection: Detects and blocks altered or replayed messages.
- Backward Compatibility: Can coexist with non-secure KNX devices in the same installation.

KNX Secure plays a crucial role in today’s smart homes and buildings, where ensuring data privacy and system integrity is essential. Its implementation can be carried out through a structured, step-by-step approach:

- Step 1: Securing the IP communication with “KNX/net IP Secure”
- Step 2: Using “KNX Data Secure” to protect KNX communication and prohibiting unauthorized access to KNX Secure devices and their configuration

3. Step-by-Step Guide using KNX Secure

Planning and Design
Identify critical communication paths and devices that require secure communication to ensure data integrity. Define which group addresses should use encrypted communication in the ETS project.

Device Selection
Choose KNX Secure-compatible devices that support KNX IP Secure and/or KNX Data Secure. Ensure interoperability between secure and non-secure devices where needed.

Commissioning with ETS
Use the Engineering Tool Software (ETS) to configure security settings. Assign security keys and define secure group addresses during the commissioning process.

Secure Communication Setup
Enable KNX Data Secure for telegrams on the bus (TP) and KNX IP Secure for IP-based communication. KNX uses Extended Frames to transmit encrypted and authenticated messages.

Testing and Validation
Verify that secure communication is functioning correctly. Ensure that unauthorized devices cannot access or interfere with the system.

Maintenance and Updates
Regularly update device firmware and security keys. Monitor the system for anomalies or unauthorized access attempts.

4. KNX Data Secure

a) Definition

KNX Data Secure utilizes encryption technology to ensure that transmitted data remains secure and cannot be intercepted or altered by unauthorized parties. This mechanism safeguards users and significantly reduces potential security vulnerabilities. Configuration of KNX Secure devices is performed during the commissioning phase using the ETS.

To enable secure and authenticated communication, KNX Secure devices utilize an extended KNX telegram format (Extended Frames). Despite the added security, this has no noticeable effect on device response times.

Importantly, KNX Plain and KNX Secure devices can coexist within the same installation and share the same communication medium without conflict. KNX Secure devices are capable of handling both encrypted (Data Secure) and unencrypted (plain) communication. However, it is not possible to use both secure and non-secure communication through the same communication object.

The ETS project configuration determines which group addresses are secured and which operate using conventional communication.

b) Key Benefits and Features

- **End-to-End Encryption:** Data is encrypted from the sender to the receiver. Even if the telegram is intercepted, its contents cannot be read or altered.
- **Authentication:** Devices verify each other's identity before exchanging data. Prevents unauthorized devices from joining or interfering with the network.
- **Integrity Protection:** Ensures that the data has not been tampered with during transmission. Uses cryptographic checksums (Message Authentication Codes).
- **Extended Frames:** KNX Data Secure utilizes a modified Telegram format to convey encrypted payloads. These are called Extended Frames, but they are backward-compatible with existing KNX infrastructure.

c) How KNX Data Secure Works

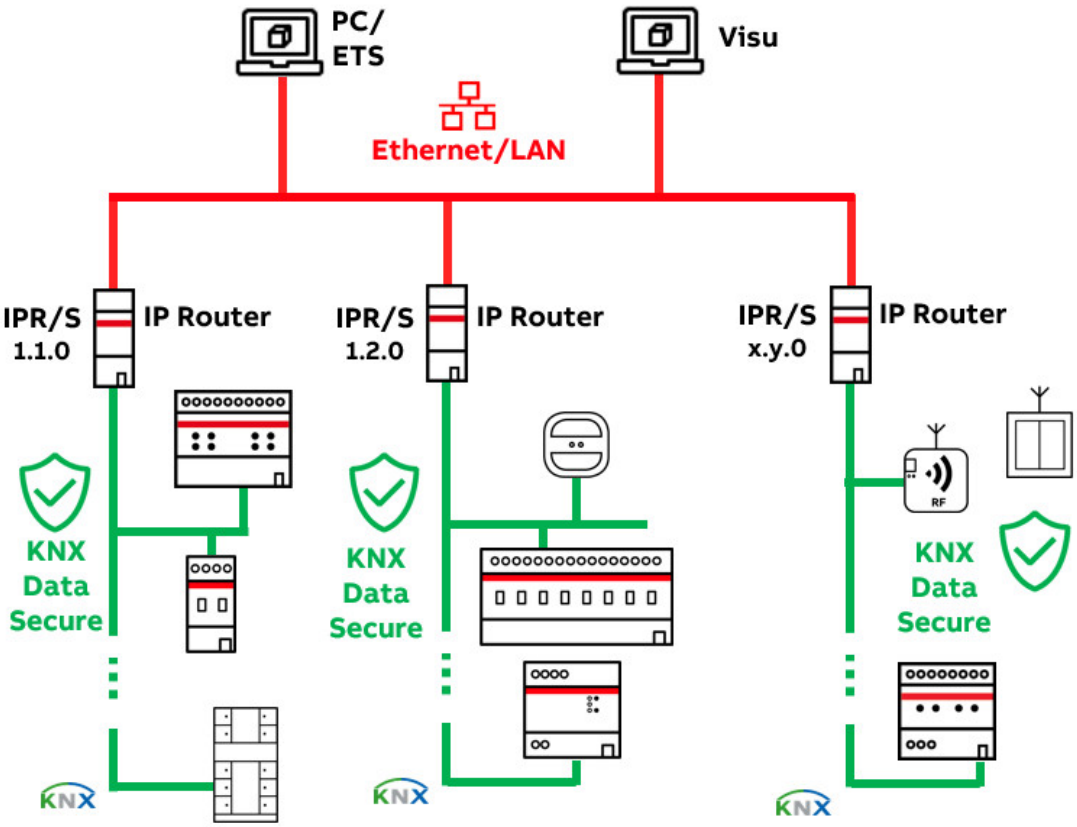

Image 1: KNX Data Secure on TP level

KNX Data Secure devices communicate at the telegram level between sender and receiver using end-to-end encryption. KNX Data Secure is designed to work across all KNX media types —Twisted Pair (TP), IP, and RF —and is configured via the ETS during device commissioning.

A KNX telegram consists of two parts:

- Addressing and control information (destination and origin address, hop count)
- Payload (payload data of the group addresses, e.g., temperature, control commands, ...)

KNX Data Secure only encrypts the payload data. The advantage of this approach is that secure and plain telegrams can be transmitted in parallel. KNX IP routers, line couplers, and repeaters can route both plain and secure telegrams, as addressing and control information are the same for KNX Secure and Plain. Due to encryption, the payload data part contains more information and is longer. KNX Data Secure telegrams are extended frames and require infrastructure components that support Extended Frames.

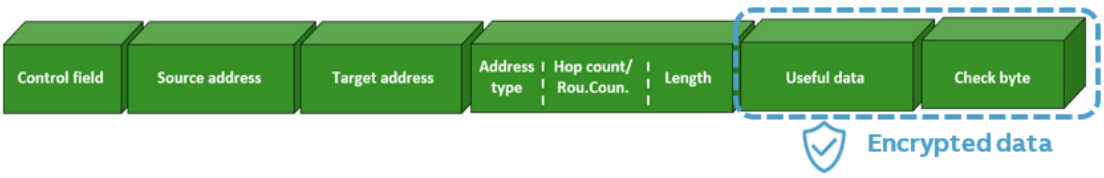

Image 2: KNX telegram structure with encrypted payload data

The KNX Data Secure Mechanism consists of four key components:

1. Freshness
To prevent replay attacks, KNX Data Secure ensures that only “fresh” telegrams are accepted.

Each telegram carries a 6-byte sequence number. The receiving device verifies that this number is greater than the last one received from the same sender. If the number is equal to or lower than, the telegram is discarded.

The sequence number doesn’t need to increment by exactly one—any higher value is acceptable. If a device is reset or replaced, the ETS tool detects this and updates the security objects accordingly. During programming, ETS uses its sequence number, which must match the tool key. These numbers are visible in the ETS group monitor. While not encrypted, they are protected against tampering.

2. Confidentiality
Telegram confidentiality is maintained through encryption using the AES algorithm with 128-bit symmetric keys.

A symmetric key means the same key is used by the sender to encrypt messages and by the receiver to decrypt and verify them. This ensures that the content of the telegram remains private and secure.

3. Data Integrity
Data integrity ensures that telegrams are not altered or injected with false information.

Each telegram includes an encrypted authentication code, allowing the receiver to verify its authenticity. KNX Data Secure uses AES encryption to generate a Message Authentication Code (MAC), which is appended to every telegram. This MAC validates the integrity of the message and detects any unauthorized modifications.

4. Authentication
Authentication guarantees that telegrams originate from trusted devices.

Each telegram includes the sender’s physical address, which the receiver checks against a list of known devices. If the sender’s cryptographic key is not found in the communication table, which is automatically generated by ETS during setup, the telegram is rejected. This applies to all types of telegrams, including broadcast, unicast (for configuration), and group messages.

5. KNX IP Secure

a) Definition

KNX IP Secure enables the secure transmission of KNX telegrams over IP networks using KNX IP Secure routers or interfaces. It is especially beneficial for existing installations where a complete upgrade to KNX Data Secure is either cost-prohibitive or technically unfeasible.

Typical use cases:

- Retrofitting existing installations: Ideal for upgrading older KNX systems where complete migration to KNX Data Secure is not feasible.
- Remote access protection: Prevents unauthorized access to KNX systems over the internet or local IP networks

b) Key Benefits and Features

- **Enhanced Security:** Encrypts communication between KNX devices over IP to prevent eavesdropping and tampering. Ensures data integrity and authenticity using advanced cryptographic techniques, including AES-128 encryption.

- **Futureproofing:** Complies with international security standards such as ISO 18033-3. Designed to meet the growing cybersecurity demands of smart buildings and critical infrastructure.
- **Seamless Integration:** Fully compatible with existing KNX installations and devices. Easily integrates into both new and retrofit projects, requiring minimal modifications. Can operate alongside standard KNX and KNX Data Secure TP communication.
- **Precondition for Secure Remote Access:** Provides a layer of security when remotely configuration and monitoring KNX systems over IP.
- **Protection Against Common Threats:** Defends against man-in-the-middle attacks, replay attacks, and unauthorized access.

c) How KNX IP Secure Works

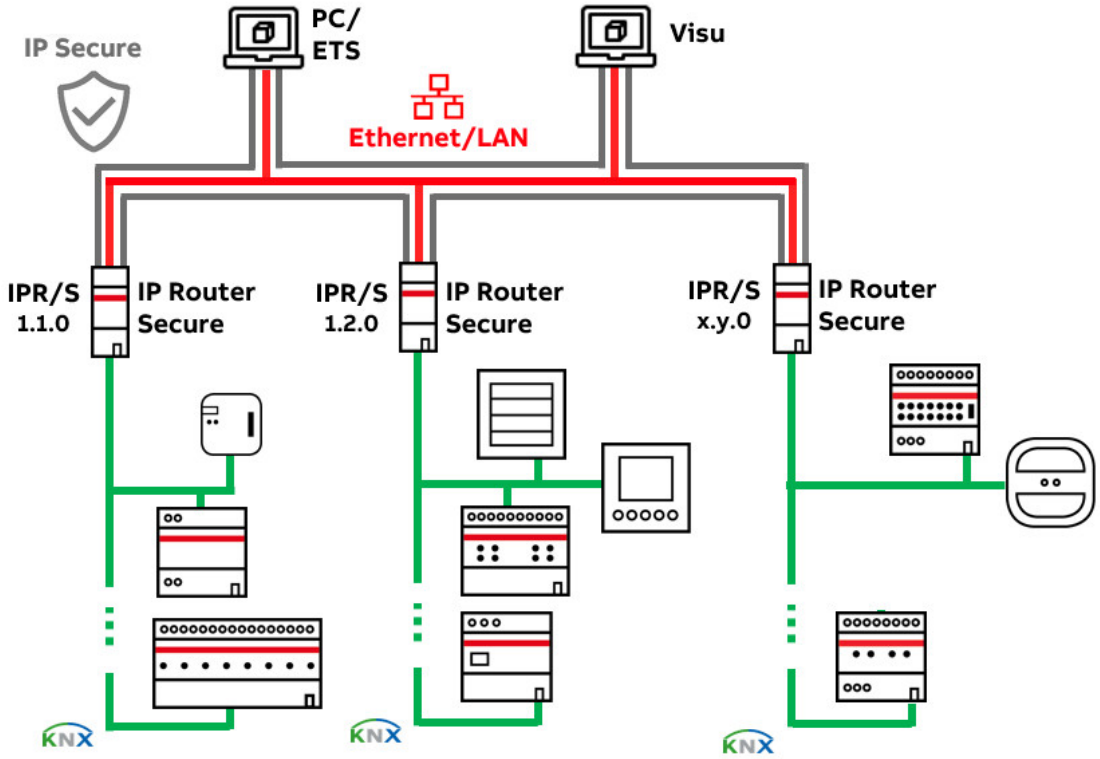

Image 3: KNX IP Secure on IP level

KNXnet/IP Secure protects KNX telegrams transmitted over IP by encrypting them to prevent unauthorized access and manipulation. While telegrams on KNX TP lines can be sent in either plain or secure mode, once routed over IP, they are encrypted using AES-128 and encapsulated in a secure IP wrapper. This ensures secure communication between KNX devices via IP routers or interfaces, even if the underlying KNX installation does not support KNX Data Secure. Notably, the original KNXnet/IP services and frame structures remain unchanged. Instead of altering the telegrams, KNXnet/IP Secure wraps them in a secure envelope, preserving full compatibility while adding a robust layer of encryption.

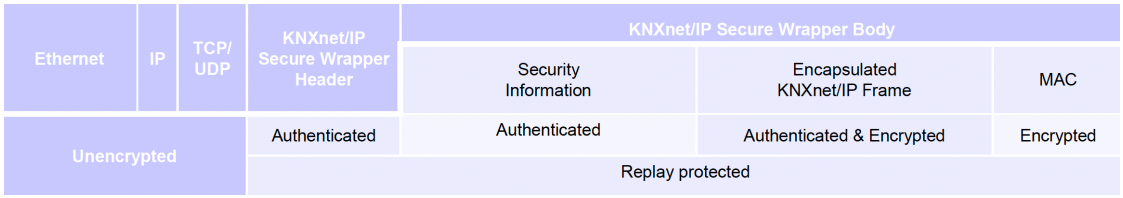

Image 4: Structure of a KNX telegram on IP level

- **Encrypted IP Communication:** KNX telegrams are encapsulated within encrypted IP packets. Only devices that possess the correct Backbone Key can decrypt and interpret these messages, ensuring confidentiality across the IP network.
- **Replay Protection**: Each telegram includes a sequence number based on millisecond intervals. This mechanism ensures that every telegram is unique and timely, effectively preventing replay attacks.
- **Secure IP Routing**: Communication over the IP backbone is restricted to KNX IP devices that share the same Backbone Key. This ensures that only authorized devices can participate in the network.
- **Secure Tunneling (Point-to-Point Communication):** For configuration and management tasks, KNX IP Secure uses the Diffie-Hellman key exchange to establish a secure session between two devices. This guarantees confidentiality and integrity in point-to-point communications.
- **Device Management Security:** All configuration and management operations conducted over IP are protected through secure sessions, safeguarding against unauthorized access and manipulation.

6. Further Information

- KNX Cybersecurity Hardening Guide
- KNX Cybersecurity Hardening Checklist
- Working with KNX Secure
- KNX Data Secure training presentation