KNX SICHERHEIT IN GEBÄUDEN

Arbeiten mit KNX Secure

Inhalt

Zweck des Dokuments **2**

Arbeiten mit KNX Secure **2**

KNX Secure in der ETS **2**
- ETS-Kompatibilität mit KNX Secure 3
- KNX-Infrastruktur muss Extended Frames unterstützen 3
- Routing- und Topologie-Anforderungen für die Inbetriebnahme 3
- Einsatz von mobilen (Roaming) KNX-Schnittstellen 4
- ETS-Projekt-Passwort 4
- Erstinbetriebnahme 5
- Offline-Zertifikatseingabe in ETS 6
- Online-Inbetriebnahme mit Gerätezertifikaten 8
- KNX-Gerätesicherheitseinstellungen 9

ETS-Reports **10**
- Projekt-Sicherheits-Report 11
- Projekt-Zertifikate 11
- Allgemeine Grundsätze der Secure KNX-Kommunikation 12
- Wann konfiguriert ETS eine Gruppenadresse als Secure? 13

Externe KNX-Kommunikationspartner **15**
- KNX Data Secure und externe Kommunikationsteilnehmer 16
- Gruppenadressen sind mit einem KNXnet/IP Tunnel verbunden 17
- ETS-Dummy-Anwendung 18
- Wartung eines KNX Secure Projekts 19

Koexistenz von KNX Plain und KNX Secure Geräten **19**

KNX-Projektübergabe **21**
- Auswirkungen des EU Cyber Resilience Act (CRA) 21
- ETS-Berichte, Sicherheitszertifikate und Passwortverwaltung 21

Zweck des Dokuments

Dieser Leitfaden enthält wichtige Informationen zur effektiven Nutzung von KNX Secure innerhalb der ETS (Engineering Tool Software). Es behandelt Schlüsselthemen wie die Erstellung von ETS-Reports, das Verständnis der allgemeinen Prinzipien der sicheren Kommunikation und der Koexistenz von Standard- und Secure KNX-Geräten. Zeil dieses Leitfadens ist Information zu liefern, die die Implementierung von KNX Secure erleichtern.

Arbeiten mit KNX Secure

Bei der Arbeit mit KNX Secure müssen einige wichtige Punkte beachtet werden, um eine reibungslose und sichere Implementierung zu gewährleisten.

1. Verständnis der beiden Varianten:

- KNX IP Secure verschlüsselt die Kommunikation ausschließlich über IP-Netzwerke.
- KNX Data Secure: Verschlüsselt die Kommunikation auf jedem Medium, insbesondere auch auf Twisted-Pair (TP). Die Verschlüsslung ist durchgängig von Sender zu Empfänger.

Wählen Sie je nach Netzwerktyp und Sicherheitsanforderungen die passende Variante.

2. Kompatibilität der Geräte:
Gemischte Systeme (KNX Secure und Standard KNX Geräte) sind möglich, erfordern aber eine sorgfältige Planung, um Sicherheitslücken zu vermeiden. Eine Übersicht, welche Geräte KNX Secure unterstützen, sollte so früh wie möglich im Planungsprozess eingeholt werden.

3. Sichere ETS Passwort- und Zertifikatsverwaltung:
Verwenden Sie ein sicheres ETS-Passwort und bewahren Sie alle Geräte-Zertifikate sicher auf. Geben Sie diese niemals an Unbefugte weiter.

4. ETS-Anforderungen:
ABB empfiehlt die Verwendung der ETS 6.x oder höher zur Projektierung von KNX Secure Geräten. Schützen Sie die ETS-Projektdatei mit einem Passwort und sichern Sie regelmäßig ein Backup der Daten.

KNX Secure in der ETS

Die Engineering Tool Software (ETS) ist zentral für die Implementierung von KNX Secure, da die ETS alle wichtigen Sicherheitsfunktionen innerhalb des Systems verwaltet:

- **Geräteprojektierung:** Die Standardprozesse der Geräteverwaltung und -projektierung werden durch den Einsatz symmetrischer Verschlüsselung unter Verwendung des ETS-Tool-Schlüssels abgesichert.
- **Verschlüsselung der Gruppenkommunikation:** Jeder Gruppenadresse wird ein eindeutiger Verschlüsselungscode zugewiesen, um Telegramme zu sichern.
- **Verschlüsselung der Punkt-zu-Punkt-Kommunikation**: Für die direkte Kommunikation (z. B. mit Konfigurations-Properties) verwendet jedes Gerätepaar einen eigenen symmetrischen Schlüssel.

Die Sicherheit des KNX-Systems, einschließlich der Geräte, der Kommunikation und der Konfiguration, wird in erster Linie, durch die in der ETS vorgenommenen Einstellungen definiert.

ETS-Kompatibilität mit KNX Secure

KNX Data Secure wird ab der **ETS-Version 5.5.0** unterstützt. Für optimale Leistung und Zuverlässigkeit wird jedoch dringend empfohlen, die **ETS-Version 6.x oder höher** zu verwenden.

Die Verwendung von Versionen vor ETS 6.x kann aufgrund der eingeschränkten Unterstützung neuerer Sicherheitsfunktionen zu Problemen bei der Inbetriebnahme führen, insbesondere beim Austausch von Geräten oder bei Konfigurationsänderungen.

KNX-Infrastruktur muss Extended Frames unterstützen

Um das Routing oder die Weiterleitung der KNX Data Secure Kommunikation, einschließlich der Kommunikation mit dem Inbetriebnahme Tool ETS, zu ermöglichen, müssen die KNX-Infrastrukturkomponenten in der Lage sein, Extended Frames - Telegramme mit einer maximalen Länge von 263 Byte - zu verarbeiten. Diese Anforderung gewährleistet die Kompatibilität mit den größeren Nutzdaten, die in KNX Data Secure Nachrichten verwendet werden.

Kompatible ABB-Geräte
Die folgenden ABB-Komponenten erfüllen diese Anforderung und können KNX Data Secure Kommunikation unterstützen, auch wenn sie selbst keine KNX Secure Geräte sind:

- USB/S 1.2 USB-Schnittstelle (2CDG110243R0011) - Produktinformation
- IPS/S 3.1.1 IP-Schnittstelle (2CDG110177R0011) - Produktinformation
- IPS/S 3.5.1 IP-Schnittstelle Secure (2CDG110204R0011) - Produktinformation
- IPR/S 3.1.1 IP-Router (2CDG110175R0011) - Produktinformation
- IPR/S 3.5.1 IP-Router Secure (2CDG110176R0011) - Produktinformation
- LK/S 4.3 Leitungskoppler Secure (2CDG110310R0011) - Produktinformation

Die Geräte sind in der Lage, größere APDU-Längen zu verarbeiten und können daher in sicheren KNX-Installationen eingesetzt werden, um die Kommunikation zu erleichtern.

Routing- und Topologie-Anforderungen für die Inbetriebnahme

KNX-Koppler und Router ermöglichen das Routing von -Telegrammen. Eine korrekte Konfiguration der Infrastrukturkomponenten ist auch für die Inbetriebnahme und Konfiguration der Geräte mit ETS erforderlich.

Adressierungsanforderungen, damit das Routing auch bei Projektierungsarbeiten mit der ETS korrekt ausgeführt wird:

- Alle eingesetzten Infrastrukturkomponenten benötigen eine eindeutige physikalische KNX-Adresse, die ihrer Position innerhalb der KNX-Topologie entspricht; zudem müssen sie korrekt parametriert werden.
- Die Infrastrukturkomponenten müssen ordnungsgemäß projektiert sein. Dabei ist zu beachten, dass bei Projektänderungen auch die Einstellungen der Infrastrukturkomponenten angepasst werden.
- Für die Inbetriebnahme und Konfiguration verwendete Schnittstellen muss eine eindeutige physikalische KNX-Adresse vergeben werden.

Diese Anforderungen sind Bestandteil des KNX-Systemdesigns und gewinnen insbesondere beim Einsatz von KNX Data Secure an Bedeutung.

Einsatz von mobilen (Roaming) KNX-Schnittstellen

Wird ein KNX-Segmentkoppler in Verbindung mit einem KNX DATA Secure-Gerät eingesetzt, wird der Secure Proxy des Kopplers automatisch aktiviert. Dieser Proxy filtert die Kommunikation analog zu Linien- oder Bereichskopplern. Im Gegensatz zu anderen Kopplern ist der Segmentkoppler jedoch nicht in der Lage, den Standort eines Geräts allein anhand seiner physikalischen Adresse zu bestimmen. Daher müssen Geräte bei Verwendung eines Segmentkopplers manuell den jeweiligen Segmenten zugewiesen werden.

Eine mobile KNX-Schnittstelle, die häufig als „Floating Device“ klassifiziert wird, ist üblicherweise nicht im ETS-Projekt enthalten und somit keinem Liniensegment zugeordnet. ETS kann Roaming-Schnittstellen effizient verwalten. Vorausgesetzt, die Einstellungen für die lokale physikalische Adresse sind korrekt in ETS hinterlegt und stimmen mit der aktuellen Position der Roaming-Schnittstelle innerhalb der KNX-Topologie überein, kann ETS erkennen, auf welcher Seite des Segmentkopplers sich die Schnittstelle befindet. Zusätzlich konfiguriert ETS den sicheren Proxy so, dass die Schnittstelle auf die Whitelist gesetzt wird. Dadurch wird sichergestellt, dass die notwendige Kommunikation für Inbetriebnahme und Konfiguration korrekt weitergeleitet wird – selbst wenn die Schnittstelle nicht formell Teil des ETS-Projekts ist.

Konfigurationstools von Drittanbietern:
Bei KNX-Konfigurationstools, die nicht Teil der ETS sind (z. B. ABB i-bus® Tool), ist eine automatische Handhabung möglicherweise nicht verfügbar. In solchen Fällen ist eine Verbindung zum System über eine KNX-Schnittstelle auf der Hauptlinie oder Bereichslinie möglich, die eine Ebene über der Linie mit dem Segmentkoppler in der Topologie liegt.

Alternativ kann dem ETS-Projekt ein ETS-Dummy-Objekt hinzugefügt werden, das die Schnittstelle darstellt und dem entsprechenden Segment zugewiesen wird. Dies ermöglicht es ETS, die Schnittstelle in die Whitelist des sicheren Proxys aufzunehmen. Sobald diese Änderung heruntergeladen wurde, ist die Kommunikation zwischen dem Tool und dem Zielgerät nicht mehr eingeschränkt

ETS-Projekt-Passwort

Wenn ein KNX Secure Gerät zu einem Projekt hinzugefügt wird, fordert die ETS den Benutzer auf, ein Projektpasswort festzulegen. Dieses Passwort ist wichtig, um das Projekt vor unberechtigtem Zugriff zu schützen.

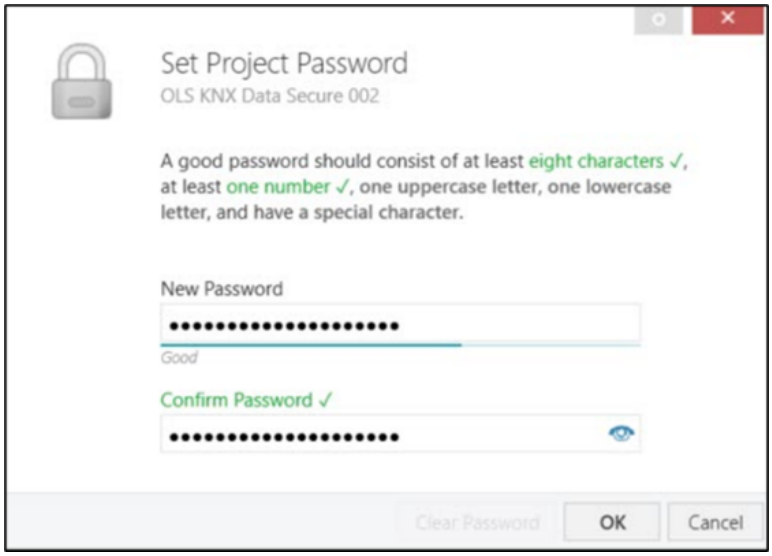


Bild 1: Projektpasswort in der ETS festlegen

Wenn kein ETS-Passwort definiert wird:

- KNX-Geräte können nicht als KNX Secure Geräte konfiguriert werden.
- Die gesamte Kommunikation bleibt unverschlüsselt (plain), das System wird nicht abgesichert.

Das Festlegen eines sicheren Projektpasworts ist daher ein notwendiger Schritt zur Aktivierung der KNX Secure Funktionalität.

Wichtig: Das ETS-Projektpasswort muss sicher aufbewahrt werden, da es die einzige Möglichkeit ist, auf verschlüsselte Projektdateien zuzugreifen. Sobald ein Projekt verschlüsselt ist:

- Kann es ohne Passwort nicht geöffnet werden.
- Weder die KNX Association noch die Hersteller von KNX-Geräten können:
    - Verschlüsselte ETS-Projekte öffnen
    - Vergessene Passwörter zurücksetzen,
    - Daten aus verschlüsselten Dateien wiederherstellen.

Eine Passwortverwaltung für den Zugang zu Ihren KNX Secure Projekten unerlässlich.

Erstinbetriebnahme

Jedes KNX Secure Gerät wird mit einem Gerätezertifikat ausgeliefert, das sich in der Regel auf einem abnehmbaren Etikett befindet, welches am Gerät angebracht ist (erforderlich für die erste Inbetriebnahme des Geräts). Dieses Zertifikat sollte nach der Installation sicher aufbewahrt werden. Das Gerätezertifikat enthält die folgenden Informationen:

- Der Schlüssel für die werkseitige Standardeinstellung (FDSK)
- Die entsprechende Seriennummer

Bild 2: Beispiel eines Gerätezertifikats für ABB-Geräte

Während der Ersteinrichtung des Geräts werden Sie von der ETS aufgefordert, das Gerätezertifikat einzugeben. Diese ist als QR-Code verfügbar, der mit einem QR-Scanner gescannt werden kann. Alternativ kann der Code manuell eingegeben werden.

Sollte kein QR-Scanner zur Verfügung stehen, kann es schwierig sein, die Laptopkamera so zu positionieren, dass die QR-Codes gescannt werden können. In diesem Fall empfiehlt es sich, den QR-Code kurz mit einem Mobiltelefon zu fotografieren und anschließend das Foto des Zertifikats vom Mobiltelefon aus zu scannen. Bitte beachten Sie, dass diese Fotos eine Kopie des Gerätzertifikats darstellen. Sie sollten dementsprechend sicher aufbewahrt oder zügig gelöscht werden.

Das Gerätezertifikat wird ausschließlich während des initialen Authentifizierungsprozesses zwischen der ETS und dem KNX Data Secure Gerät benötigt. Nach dem Einlesen des Zertifikats extrahiert die ETS dessen wesentliche Bestandteile: die Seriennummer und den Factory Default Setup Key (FDSK). Anschließend generiert die ETS einen Toolkey und weist diesen dem Gerät zu. Dieser Toolkey ersetzt das ursprüngliche Zertifikat für die Laufzeitauthentifizierung und den weiteren Inbetriebnahmeprozess.

Erst nach diesem Schritt kann das Gerät als KNX Secure Gerät in der ETS konfiguriert werden.

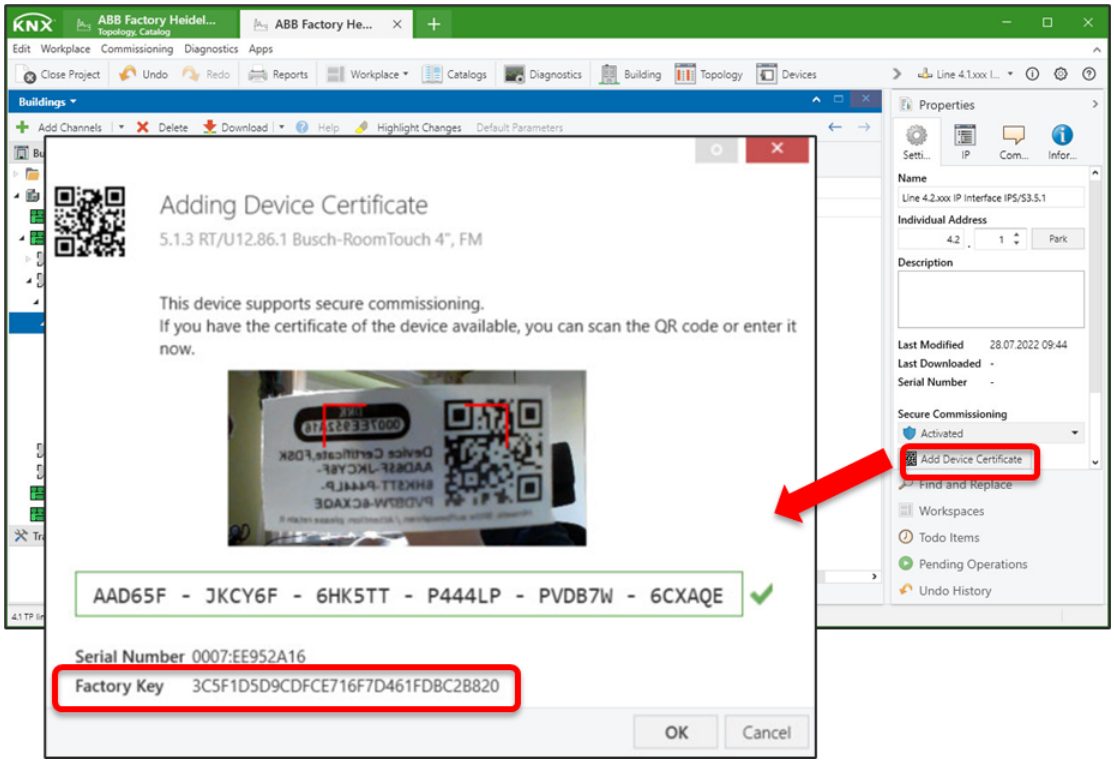


Bild 3: Hinzufügen eines Gerätezertifikats zur ETS

Da das Gerätezertifikat sowohl den FDSK als auch die Seriennummer enthält, kann die ETS bei der Erstinbetriebnahme jedem Gerät automatisch das richtige Zertifikat zuordnen. Dies vereinfacht den Einrichtungsprozess und stellt sicher, dass jedes KNX Secure Gerät sicher und korrekt in das Projekt integriert wird.

Offline-Zertifikatseingabe in ETS

Sie können alle benötigten Gerätezertifikate für Ihre ETS-Projekt in einem einzigen Schritt scannen oder manuell eingeben, auch ohne Live-Verbindung zu den Geräten.

Bei der Erstinbetriebnahme ordnet die ETS jedes Zertifikat anhand der Seriennummer, die sowohl in den lesbaren Produktdaten des Geräts als auch in seinem Zertifikat enthalten ist, automatisch dem richtigen Gerät zu.

Sobald ein Projekt erstellt ist, erscheint es in der ETS-Übersicht unter "Lokale Projekte". Wenn Sie auf eine Projektkachel klicken, erscheint die Option "Details".

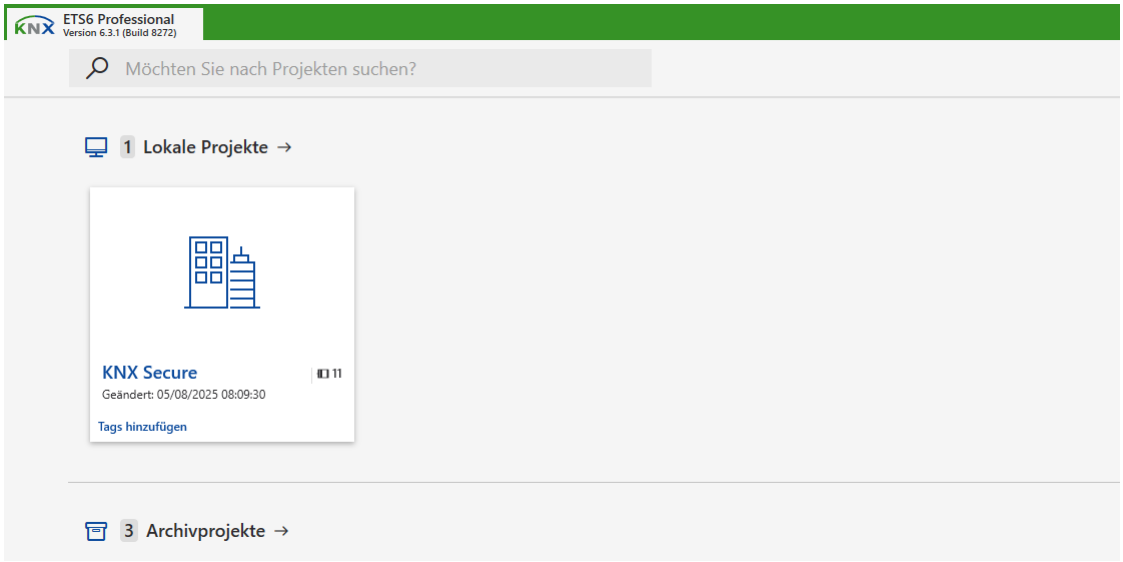


Bild 4: ETS-Startseite mit Ansicht der lokalen Projekte

Durch Klicken auf die Kachel „Sicherheit“ in einem ETS-Projekt werden alle Geräteseriennummern und FDSK-Schlüssel angezeigt. Geräteseriennummern und FDSK-Schlüssel sind jeweils Bestandteil eines Gerätezertifikats. In dieser Ansicht können Sie außerdem neue Gerätezertifikate hinzufügen, wodurch die Verwaltung und Aktualisierung Ihrer KNX Secure-Installation vereinfacht wird.

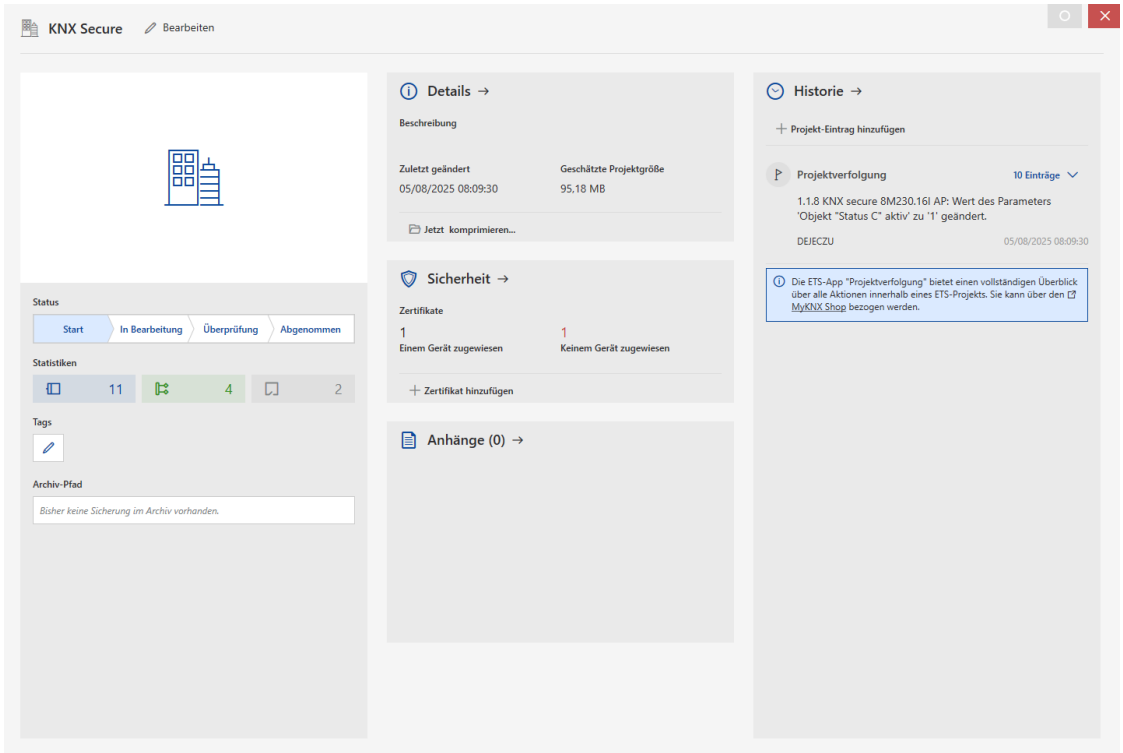


Bild 5: Sicherheitsansicht in den ETS-Projektinformationen

So bald bestätigt ist, dass ein Gerät als Teil des ETS-Projekts verwendet wird, kann sein Zertifikat in die ETS importiert werden - noch bevor das Gerät in der Software erstellt, vor Ort installiert oder an die Baustelle geliefert wird. Dieser proaktive Schritt trägt zur Rationalisierung des Inbetriebnahmeprozesses bei und gewährleistet, dass alle erforderlichen Sicherheitsnachweise bereits vorhanden sind, wenn das Gerät schließlich integriert wird.

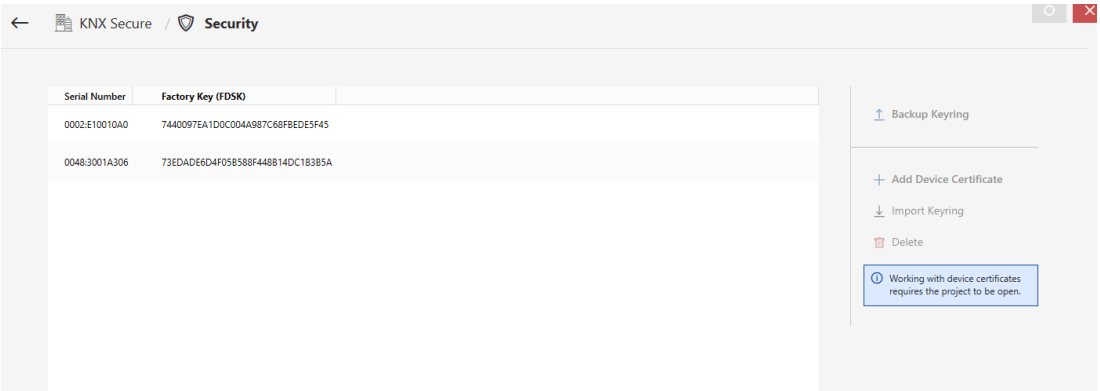


Bild 6: Übersicht der Gerätezertifikate

Dieses Verfahren eignet sich für Geräte, die leicht zugänglich sind und bei denen die individuelle KNX-Adresse einfach durch Drücken der Programmiertaste vergeben werden kann.

Online-Inbetriebnahme mit Gerätezertifikaten

Die Inbetriebnahme von schwer zugänglichen KNX-Geräten stellt häufig eine Herausforderung dar, insbesondere die Betätigung der Programmiertaste. In solchen Fällen bietet die Zuweisung der individuellen Geräteadresse anhand der Seriennummer aus dem Gerätezertifikat eine praktische und effiziente Lösung, die eine direkte Interaktion mit dem Gerät überflüssig macht.

In der ETS können Sie ein bestimmtes Gerät auswählen und manuell mit dem zugehörigen Gerätezertifikat verknüpfen. Dadurch kann die ETS das Gerät anhand der Seriennummer identifizieren und die Inbetriebnahme starten. Diese Vorgehensweise ist insbesondere dann vorteilhaft, wenn der physische Zugang zum Gerät eingeschränkt ist, da die Programmiertaste während der Einrichtung nicht mehr betätigt werden muss.

ABB KNX-Geräte werden mit zwei Gerätezertifikatsaufklebern geliefert. Es wird empfohlen, einen Aufkleber zu entfernen und der Projektdokumentation beizufügen. Hierbei sollten Produktname und Installationsort vermerkt werden. Da mit Hilfe der Projektdokumentation das Gerätezertifikat eindeutig einem Gerät zugeordnet werden kann, ist nun eine Programmierung über die Seriennummer ohne Verwendung der Programmiertaste möglich.

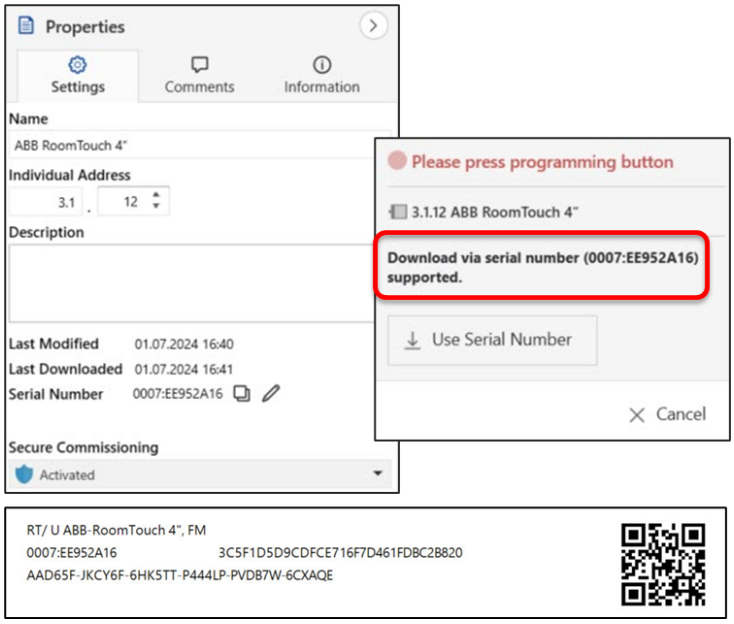
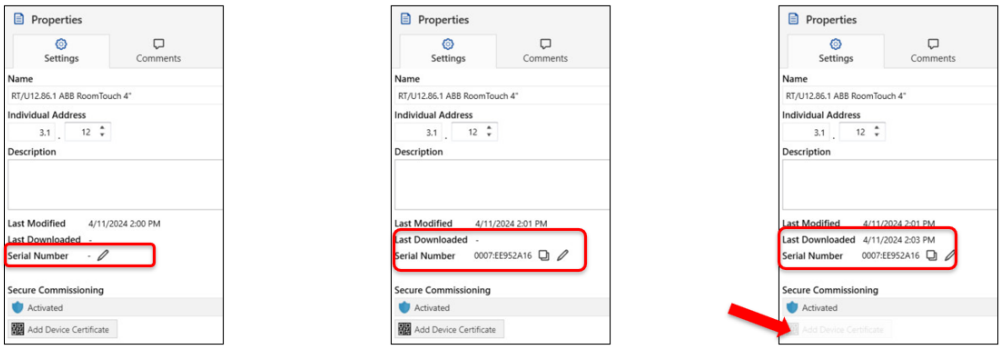


Bild 7: Download über Seriennummer in der ETS

Die ETS-Kachel auf der rechten Seite unter „Eigenschaften“ zeigt an, ob einem Gerät ein Gerätezertifikat zugewiesen wurde. Durch die Zuweisung des Gerätezertifikats wird das Gerät als KNX Secure Produkt dem ETS-Projekt hinzugefügt und erhält eine eindeutige KNX-Adresse. Darüber hinaus zeigt die Kachel, basierend auf der aktuellen Konfiguration, an, ob die KNX Data Secure Unterstützung aktive ist.



No device certificate has been assigned yet (no serial number is displayed)

A device certificate has been assigned (the serial number is displayed)

The device was put into operation with the device certificate (“Add device certificate” button is grayed out)

Bild 8: Gerätezertifikatszuordnung in der ETS-Ansicht "Eigenschaften".

Die ETS-Topologie-Ansicht zeigt, welche KNX-Geräte zugeordnet sind. Geräte mit aktiviertem KNX Secure erscheinen dort mit blauem Label.

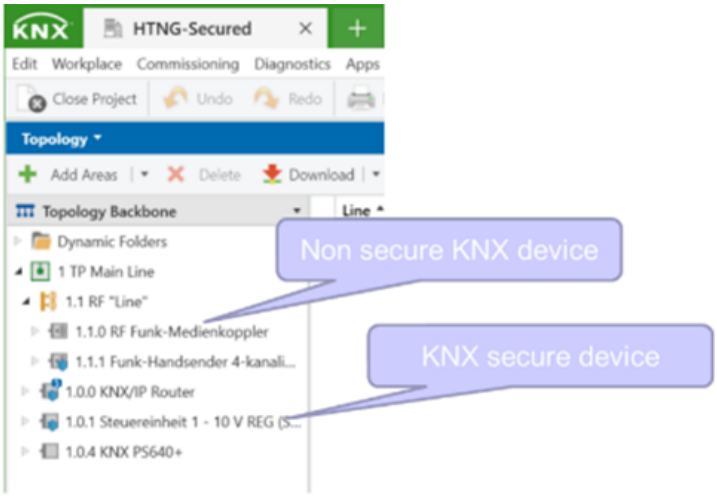


Bild 9: Anzeige der KNX Secure Geräte in der Topologieansicht in der ETS (blaues Schild)

KNX-Gerätesicherheitseinstellungen

Die Sicherheitseinstellungen eines Geräts können angepasst werden. Wird die Option „Sichere Inbetriebnahme“ auf „Deaktiviert“ gesetzt, wechseln alle mit dem Gerät verknüpften Gruppenadressen zur unverschlüsselten Kommunikation (Plain).

Wichtig: Die Änderung dieser Einstellung löst einen Master-Reset aus. Alle Sicherheitsschlüssel werden gelöscht, und das Gerät muss erneut vollständig in Betrieb genommen werden. Bitte beachten Sie, dass dieser Prozess längere Downloadzeiten verursachen kann.

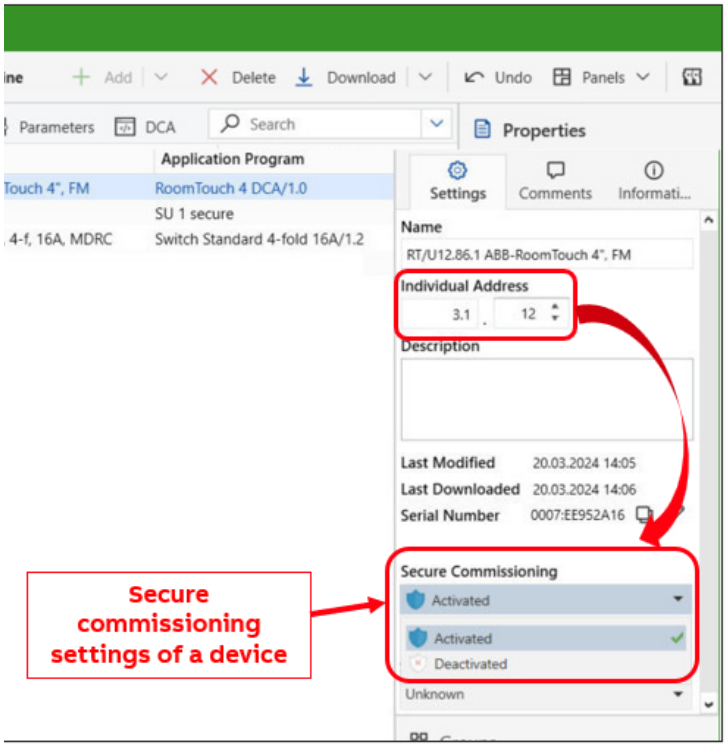


Bild 10: Sichere Inbetriebnahme eines Gerätes in der ETS aktivieren/deaktivieren

Bei der Reaktivierung der sicheren Inbetriebnahme muss ein neuer Toolkey zugewiesen werden. Dadurch werden auch die Sicherheitsschlüssel für alle Gruppenadressen, an die dieses KNX-Gerät Daten sendet, neu generiert.

Anmerkung: Eine Änderung der Sicherheitseinstellung eines Geräts von "Sichere Inbetriebnahme" auf "Deaktiviert" ist selten notwendig und kann zu einem erheblichen Mehraufwand führen.

ETS-Reports

Die ETS bietet die Möglichkeit, eine Vielzahl von Reports zu erstellen. Zusätzlich zu den allgemeinen Projektreports bietet die ETS auch spezielle Reports für KNX Secure, die eine detaillierte Dokumentation der sicherheitsrelevanten Konfigurationen ermöglichen.

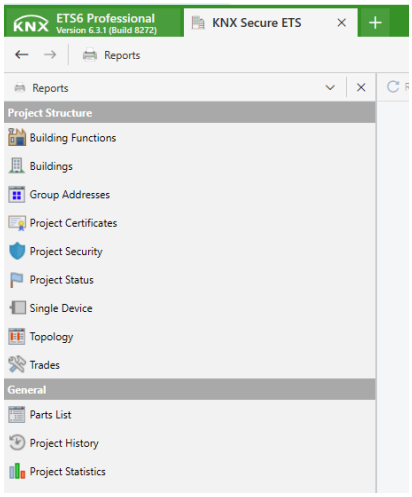


Bild 11: ETS-Berichte im Überblick

Projekt-Sicherheits-Report

Der Projekt-Sicherheits-Report in der ETS zeigt alle Schlüssel und Passwörter an, die während des Konfigurationsprozesses erzeugt wurden. Dazu gehören:

- Tool Keys
- Gruppenadressschlüssel
- KNXnet/IP Secure Backbone Key (verwendet für Routing Services)
- Authentifizierungscodes für KNXnet/IP Tunneling Interfaces

Dieser Bericht bietet einen umfassenden Überblick über die im Projekt eingesetzten Sicherheitszertifikate, die für eine sichere Inbetriebnahme und Kommunikation essenziell sind.

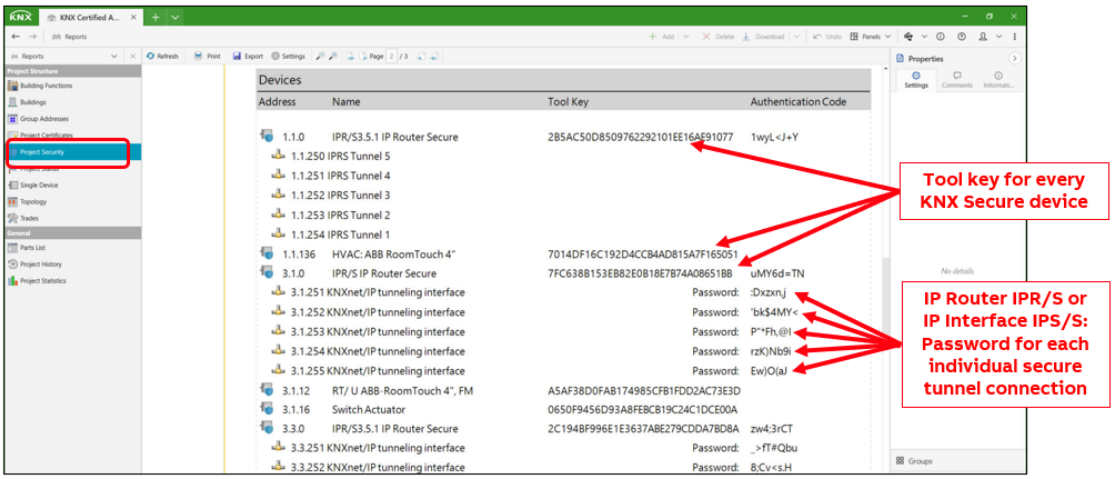


Bild 12: Beispiel für einen Projektsicherheitsbericht

Der Projektsicherheits-Report ist in erster Linie für Dokumentationszwecke gedacht. Der KNX ETS-Keyring Export ermöglicht es, Schlüssel aus einem ETS-Projekt zu exportieren, um sie außerhalb des Projekts zu archivieren oder in andere Anwendungen zu nutzen.

Dies ist besonders nützlich bei der Verwaltung von KNX Secure Geräten mit externen Tools wie dem i-bus Tool, da jedes Gerät einen eigenen Toolkey hat.

Darüber hinaus ist der ETS-Keyring Export unerlässlich, wenn ein Visualisierungssystem oder ein KNX-Client eine Verbindung zu einer KNX Secure Installation herstellen soll.

Projekt-Zertifikate

ETS ermöglicht die Sicherung von Gerätezertifikaten, die mit Geräten innerhalb eines ETS-Projekts verknüpft sind. Die zugehörige Dokumentation ist sicher zu archivieren. Bei der Projektübergabe sollte eine Kopie an den Kunden übergeben werden. Kunden sollten darauf hingewiesen werden, dass die

Dokumentation vertrauliche Sicherheitsinformationen enthält und an einem sicheren Ort aufzubewahren ist.

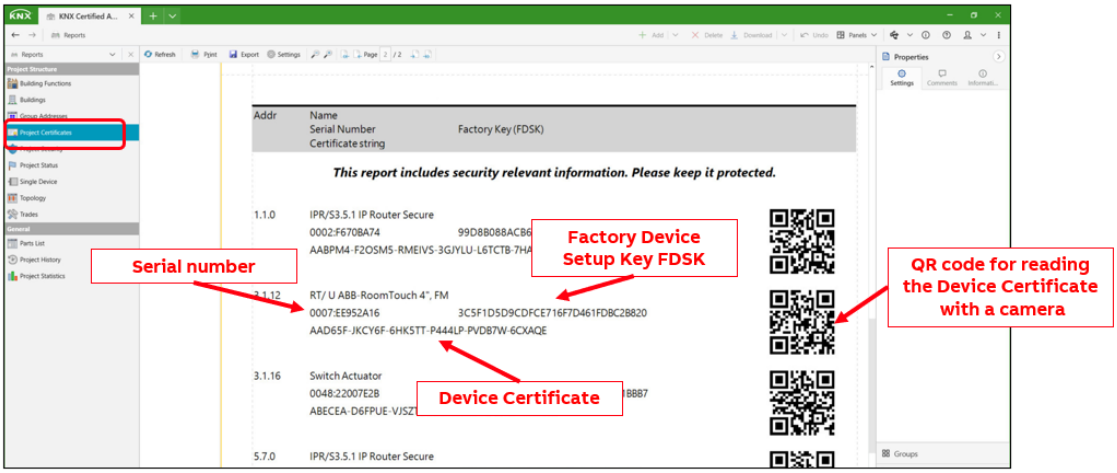


Bild 13: Übersicht der Projektzertifikate in der ETS (empfohlen für die Kundendokumentation)

Die von der ETS erstellte Dokumentation beinhaltet eine digitale Kopie des dem Produkt beiliegenden Gerätezertifikats. Diese digitale Kopie ermöglicht die Wiederinbetriebnahme des Geräts als KNX Secure Produkt nach einem Master-Reset auf die Werkseinstellungen, falls das Originalzertifikat nicht mehr verfügbar ist.

Allgemeine Grundsätze der Secure KNX-Kommunikation

Duale Kommunikationsfähigkeit
KNX Secure Geräte sind in der Lage, sowohl verschlüsselt (Secure) als auch unverschlüsselt (Plain) zu kommunizieren. Sie können sogar beide Modi gleichzeitig mit unterschiedlichen Kommunikationsobjekten nutzen.

Beschränkungen für Kommunikationsobjekte
Ein Kommunikationsobjekt kann entweder im verschlüsselt (Secure) oder im unverschlüsselten (Plain) Modus arbeiten, aber nicht in beiden gleichzeitig.

Alle Gruppenadressen, die mit einem Kommunikationsobjekt verknüpft sind, müssen dessen Sicherheitsmodus entsprechen.

Sicherheitsmodi für Gruppenadressen
Über Gruppenadressen kann entweder unverschlüsselt oder verschlüsselt kommuniziert werde.

Ausnahme: Wenn ein Secure Proxy verwendet wird, kann eine Gruppenadresse in einem KNX-Segment oder einer Linie unverschlüsselt sein, der Proxy kann diese Gruppenadresse in eine verschlüsselte Kommunikation beim Routen in einem anderen Segment oder einer Linie übersetzen.

Verwaltung von Sicherheitsschlüsseln
KNX Secure Geräte verwenden für jede sichere Gruppenadresse einen eigenen Sicherheitsschlüssel. Diese Schlüssel werden von der ETS während der Inbetriebnahme generiert und automatisch in die Geräte geladen. In der ETS-Oberfläche sind die Schlüssel nicht sichtbar.

Wann konfiguriert ETS eine Gruppenadresse als Secure?

Ob die ETS eine Gruppenkommunikation als Secure (verschlüsselt) konfiguriert wird, hängt von mehreren Faktoren ab:

1. Inbetriebnahme / Gerätesicherheit
Die Inbetriebnahme eines KNX-Geräts als KNX Secure-Gerät erfolgt durch Verwendung des Factory Default Setup Key (FDSK). Geräte, denen von der ETS ein Toolkey zugewiesen wurde, sind mit einem blauen Symbol gekennzeichnet. Diese Geräte können sicheren Gruppenadressen zugeordnet werden. Wurde ein Gerät nicht mithilfe des FDSK in Betrieb genommen und ist kein Toolkey durch die ETS zugewiesen, kann das Gerät keine sichere Kommunikation unterstützen, auch wenn es technisch KNX Secure-fähig ist.

2. Laufzeit / Gruppenadresse Sicherheitseigenschaften
Mit dieser Einstellung kann der ETS-Benutzer bestimmen, ob die Verschlüsselung von Gruppenadressen während der Laufzeit aktiviert (erzwungen ein) oder deaktiviert (erzwungen aus) sein soll. Diese Konfiguration erfolgt individuell pro Gruppenadresse und ermöglicht eine flexible Absicherung der KNX-Installation.

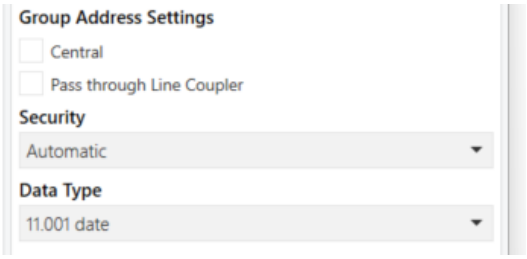


Bild 14: Sicherheitseigenschaften der Gruppenadresse

In der ETS ist die Standardeinstellung für die Sicherheit von Gruppenadressen **"Automatisch".** Das Verhalten der einzelnen Einstellungen ist wie folgt:

Automatisch:
Die Sicherheitsstufe einer Gruppenadresse richtet sich nach der höchsten Sicherheitsstufe der zugehörigen Kommunikationsobjekte. Sind an eine Gruppenadresse sowohl ein KNX Secure-Gerät (mit Secure-Kommunikationsobjekt) als auch ein KNX Plain-Gerät (mit Plain-Kommunikationsobjekt) angeschlossen, wird die Gruppenadresse auf KNX Plain gesetzt, da nicht alle Geräte sichere Kommunikation unterstützen. Unterstützen alle angeschlossenen Geräte und ihre Kommunikationsobjekte Secure, wird die Gruppenadresse entsprechend auf Secure gesetzt.

Erzwungene An:
Wird diese Option ausgewählt, wird die Gruppenadresse auf „Secure“ (verschlüsselt) gesetzt. Diese Gruppenadresse kann ausschließlich mit Kommunikationsobjekten von KNX Secure Geräten verwendet werden. Geräte oder Kommunikationsobjekte, die keine verschlüsselte Kommunikation unterstützen, können nicht mit dieser Gruppenadresse verbunden werden.

Erzwungenes Aus
Diese Einstellung erzwingt eine **plain (unverschlüsselte)** Kommunikation für die Gruppenadresse, unabhängig davon, ob die angeschlossenen Geräte KNX Data Secure unterstützen. Die gesamte Kommunikation über diese Gruppenadresse erfolgt unverschlüsselt.

KNX Secure Gruppenadressen sind in der ETS mit einem blauen oder weißen Aufkleber gekennzeichnet.

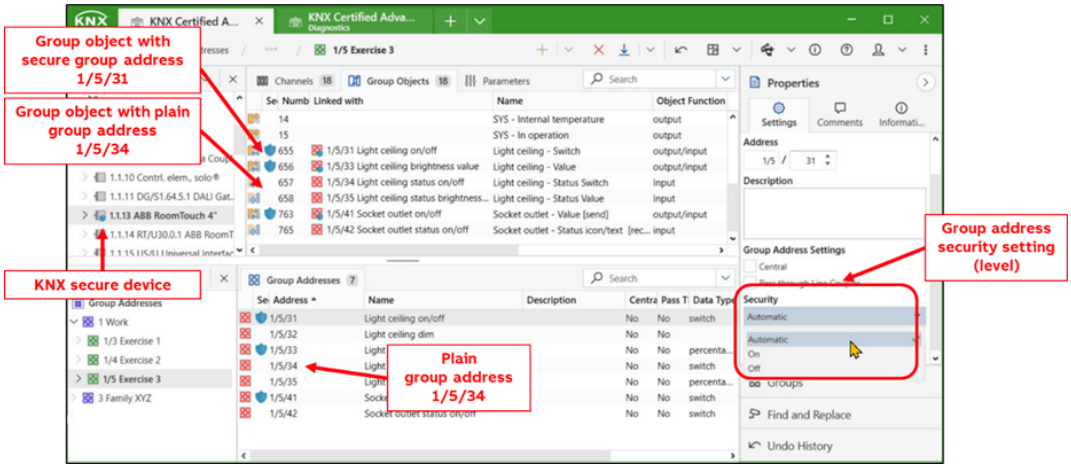


Bild 15: Anzeige der sicheren Kommunikation in der ETS (blaues Schild)

Eine blaue Anzeige signalisiert, dass die sichere Kommunikation zwischen Sender und Empfänger kontinuierlich aufrechterhalten wird. Ein weißes Schild hingegen zeigt an, dass eine Gruppenadresse mindestens in einem KNX-Segment oder einer Linie verschlüsselt wird. In einem Secure Proxy wird die Verschlüsselung so modifiziert, dass diese Gruppenadresse in anderen Segmenten oder Linien unverschlüsselt ist.

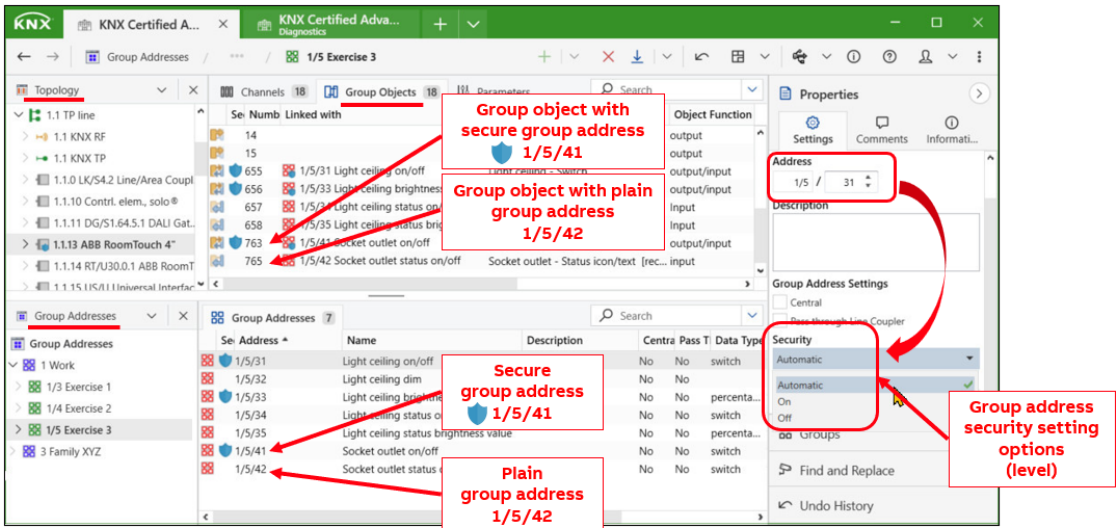


Bild 16: Sichere Kommunikation, gekennzeichnet durch ein blaues Schild neben der Gruppenadresse

Vordefinierte Sicherheitseigenschaften in KNX-Geräten

Die Sicherheitseigenschaften eines KNX-Gerätes werden vom Gerätehersteller vordefiniert. Für bestimmte Kommunikationsobjekte kann der Hersteller angeben, dass eine sichere Kommunikation zwingend erforderlich ist - dies ist typischerweise der Fall, wenn die Funktion ein hohes Maß an Sicherheit erfordert (z. B. ein Tür- oder Fensterkontakt).

Achtung! Wenn die sichere Kommunikation vom Hersteller für ein bestimmtes Kommunikationsobjekt erzwungen wird, erlaubt die ETS nicht, dass dieses Objekt mit einer KNX Plain-Gruppenadresse verbunden wird. Diese Einschränkung ist beabsichtigt und gewährleistet die Integrität und Sicherheit der kritischen Funktionen.

Externe KNX-Kommunikationspartner

Gebäudemanagementsysteme, Visualisierungssysteme oder andere Clients, die außerhalb der ETS betrieben werden, benötigen Zugriff auf den Gruppenadressschlüssel, um die sichere Gruppenkommunikation entschlüsseln zu können. Diesen Zugriff erhalten sie durch den Import und die Auswertung des Keyring-Exports (Schlüsselbund) der ETS.

Geräte, die mit KNX kommunizieren, aber nicht über die ETS in Betrieb genommen werden, gelten als externe KNX-Kommunikationspartner. Diese Geräte fallen nicht unter den KNX-Standard und sind daher nicht KNX-zertifiziert und nicht bei der KNX Association registriert. Auch wenn solche Geräte angeben, dass sie KNX Data Secure unterstützen, ist dies keine Garantie dafür, dass das Gerät selbst sicher ist. Die Sicherheitsgarantie muss mit dem Gerätehersteller abgeklärt werden.

ETS Schlüsselanhänger Export
Der ETS-Schlüsselbund-Export bietet die notwendigen Zugangsdaten für eine sichere Kommunikation und umfasst:

- Alle Gruppenadressen-Laufzeitschlüssel
- Tool Keys für jedes sichere Gerät
- Passwörter für IP-Tunneling-Verbindungen
- Die exportierte Datei wird mit der Erweiterung: .knxkeys gespeichert.

Wichtiger Sicherheitshinweis:

Die xxx .knxkeys-Datei selbst ist nicht verschlüsselt, aber die Schlüssel darin sind verschlüsselt.

Passwortschutz
Beim Erstellen eines Keyring-Exports (Backup Schlüsselbund) wird der Benutzer aufgefordert, ein Passwort festzulegen. Dieses Passwort ist erforderlich, um die in der Datei gespeicherten Schlüssel zu entschlüsseln und zu verwenden.

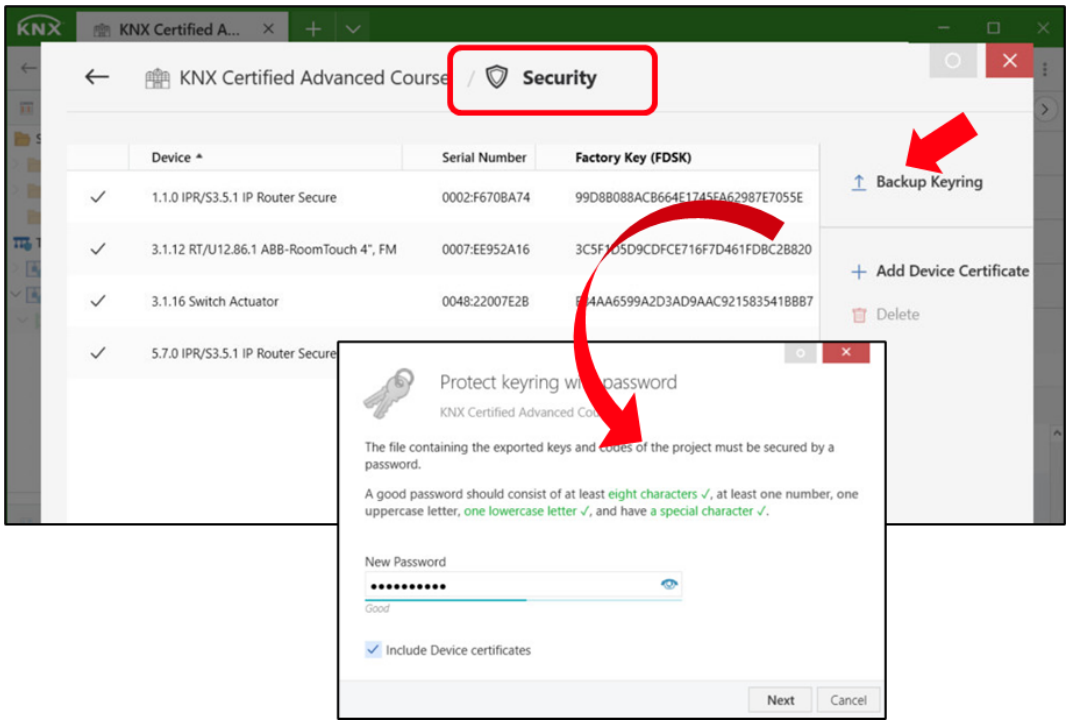


Bild 17: Passwort zum Schutz des Schlüsselanhänger-Exports festlegen

Wichtig: Stellen Sie vor dem Exportieren des Keyrings (Schlüsselrings) sicher, dass die physikalische Adresse des externen Kommunikationsgeräts (Dummy) im ETS-Projekt angelegt ist. Dies muss vor dem Export geschehen. Die Adresse kann entweder sein:

- Die individuelle Adresse der KNXnet/IP-Tunnelschnittstelle, oder
- Die individuelle Adresse eines in der ETS erstellten Dummy-Objekts.

Diese Adresse muss genau mit der individuellen Adresse übereinstimmen, die beim externen Kommunikationsteilnehmer als "eigene Adresse" konfiguriert ist.

Unten sehen Sie ein Beispiel dafür, wie diese Einstellung in der EisBaer-Software erscheint. ABB bietet diese Software, die von der Alexander Maier GmbH entwickelt wurde, in zwei Versionen an:

- **EisBaer SCADA3** - für Standardanwendungen
- **EisBaer 4.0** - für fortschrittliche Lösungen, einschließlich vollständiger Aufzeichnung und Speicherung historischer Daten

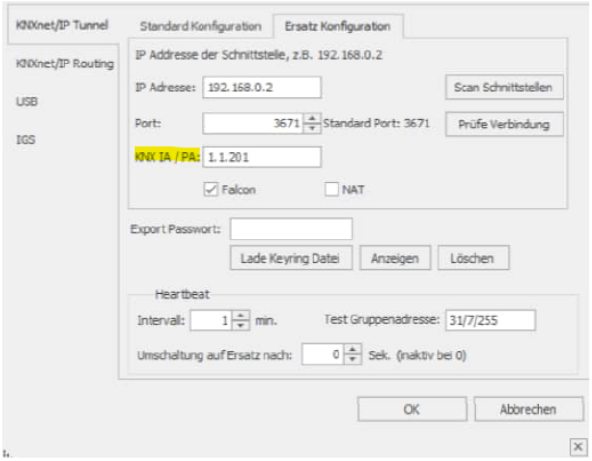


Bild 18: Physikalische Adresse des externen Kommunikationsgeräts in der EisBaer-Software

Sicherheitshinweis:
Die Sicherheitseigenschaften von KNX Secure Kommunikationsgeräten, die nicht KNX-zertifiziert sind – unabhängig davon, ob sie KNXnet/IP Secure, KNX Data Secure oder beides unterstützen – sind nur teilweise durch den KNX-Standard geregelt. Daher können ihre Sicherheitseigenschaften variieren und können durch die Norm allein nicht vollständig gewährleistet werden.

KNX Data Secure und externe Kommunikationsteilnehmer

Bei KNX Data Secure wird jedes Telegramm mit zwei Sicherheitsschlüsseln geschützt:

- Authentifizierungsschlüssel des Absenders - zur Überprüfung der Identität des Absenders.
- Gruppenadressen-Verschlüsselungsschlüssel - zur Sicherung der Kommunikation auf der Ebene der Gruppenadressen.

Diese Schlüssel sind für eine sichere Kommunikation unerlässlich und werden in den ETS-Keyring-Export (auch als Backup-Schlüsselbund bezeichnet) aufgenommen. Zusätzlich zu den Schlüsseln ist jedes Telegramm auch durch einen Sequenzzähler und die Quelladresse geschützt, die während der Kommunikation ausgewertet werden.

Im Gegensatz zur unverschlüsselten KNX-Kommunikation muss bei KNX Secure jeder Teilnehmer (auch ein Nicht-KNX-Teilnehmer z.B. Visu) der Gruppenkommunikation eine eindeutige individuelle Adresse haben. Diese Adresse muss:

- im ETS-Projekts angelegt werden

- Der Teilnehmer nutzt diese individuelle Adresse als Sendeadresse

Für Geräte, die nicht direkt in der ETS verwaltet werden, ist es zwingend erforderlich, dass sie:

- eine individuelle Adresse erhalten, die im KNX-Projekt definiert ist, und
- dass sie Telegramme über diese Adresse senden und empfangen .

Dies kann erreicht werden durch:

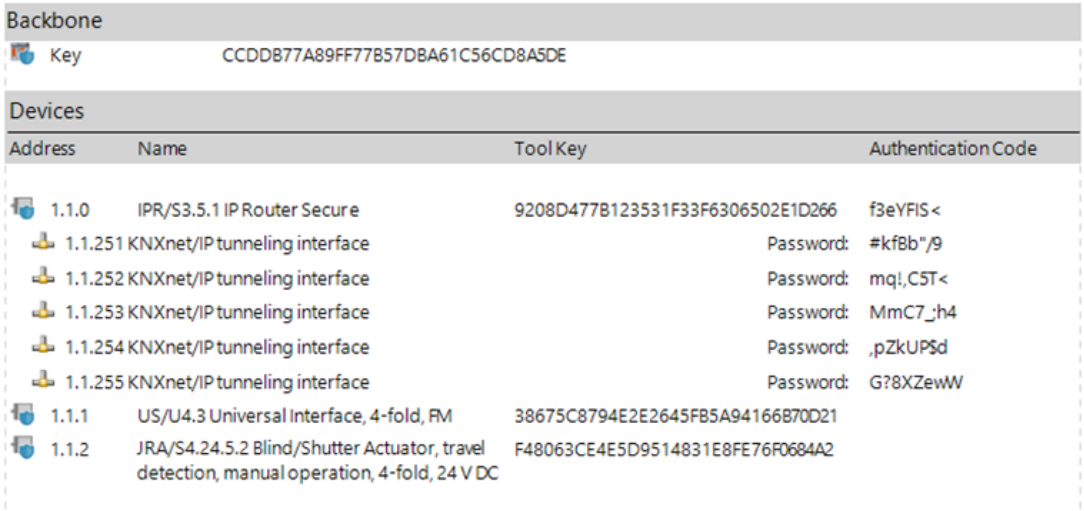
- Nutzung eine Data Secure Dummy-Objekts, oder
- Verwendung einer geeigneten Secure IP-Schnittstelle (> 5.0 ETS-Datenbankeintrag)

Das Dummy-Objekt muss KNX DATA Secure unterstützen und korrekt positioniert sein. Alle Gruppenadressen, die mit dem NON-KNX-Kommunikationsteilnehmer ausgetauscht werden sollen, müssen mit einem Secure Dummy oder der Secure Schnittstelle verbunden sein.

Gruppenadressen sind mit einem KNXnet/IP Tunnel verbunden

KNX IP Router und IP-Schnittstellen mit einem > 5.0 ETS-Datenbankeintrag (unterstützen die Verknüpfung von Gruppenadressen mit einer KNXnet/IP Tunneling Verbindung). In dieser Konfiguration wird die Kommunikation über die individuelle Adresse der KNXnet/IP Tunnelschnittstelle getunnelt.

Dieser Aufbau ermöglicht eine sichere und strukturierte Kommunikation, insbesondere in KNX Secure Umgebungen, indem sichergestellt wird, dass jede Tunneling-Verbindung eindeutig identifizierbar und ordnungsgemäß in das ETS-Projekt integriert ist.



Backbone

Key	CCDDB77A89FF77B57DBA61C56CD8A5DE

Devices

Address	Name	Tool Key	Authentication Code
1.1.0	IPR/S3.5.1 IP Router Secure	9208D477B123531F33F6306502E1D266	f3eYFIS<
1.1.251	KNXnet/IP tunneling interface	Password:	#kfBb"/9
1.1.252	KNXnet/IP tunneling interface	Password:	mq!,C5T<
1.1.253	KNXnet/IP tunneling interface	Password:	MmC7_;h4
1.1.254	KNXnet/IP tunneling interface	Password:	,pZkUP$d
1.1.255	KNXnet/IP tunneling interface	Password:	G?8XZewW
1.1.1	US/U4.3 Universal Interface, 4-fold, FM	38675C8794E2E2645FB5A94166B70D21	
1.1.2	JRA/S4.24.5.2 Blind/Shutter Actuator, travel detection, manual operation, 4-fold, 24 V DC	F48063CE4E5D9514831E8FE76F0684A2	

Bild 19: KNXnet/IP Tunneling Verbindungen

Die KNXnet/IP-Schnittstelle dient lediglich als Kommunikationspfad. Alle KNX Data Secure Prozesse erfordern die Unterstützung externer Kommunikationsteilnehmer.

Neben der IP-Adresse der Schnittstelle muss bei KNX DATA Secure auch die individuelle KNX-Adresse der KNXnet/IP Tunneling Schnittstelle im externen Kommunikationsgerät korrekt konfiguriert sein.

Weicht die Konfiguration im externen Kommunikationsteilnehmer von den im ETS-Projekt definierten Daten ab, schlägt die KNX Data Secure Kommunikation fehl.

ETS-Dummy-Anwendung

Für Systeme mit USB-Schnittstellen oder IP-Schnittstellen, die in ETS-Versionen vor 5 nicht unterstützt werden, steht eine alternative Methode zur Einbindung externer Kommunikationsteilnehmer zur Verfügung: Erstellen von sicheren KNX Dummy-Objekten im ETS-Projekt.

Was ist ein Dummy-Objekt?
Ein Dummy-Objekt ist ein virtueller KNX-Geräteeintrag in der ETS, der nicht einem physikalischen Gerät entspricht. Sie dient mehreren wichtigen Zwecken:

- Topologische Platzierung: Es ermöglicht die logische Positionierung externer Geräte innerhalb der ETS-Projektstruktur.
- Konfiguration der Filtertabelle: Es ermöglicht die Bearbeitung von Filtertabellen in KNX-Routern und -Kopplern, um eine korrekte Weiterleitung von Gruppentelegrammen zu gewährleisten.

Obwohl die Dummy-Anwendung nicht auf ein physisches Gerät heruntergeladen werden kann, beeinflusst sie das Verhalten des Netzes, indem sie die Filtertabellen verändert. Diese Änderungen müssen auf die Router und Koppler heruntergeladen werden, damit sie wirksam werden.

Hinweise zur Umsetzung:
Da es sich bei einem Dummy-Objekt um einen rein virtuellen Datenbankeintrag handelt, kann jedes im ETS-Online-Katalog verfügbare Dummy-Objekt für diesen Zweck verwendet werden.

Das Dummy-Objekt muss als sicher konfiguriert und topologisch korrekt platziert werden, um die physikalische Busschnittstelle zu repräsentieren, damit ein ordnungsgemäßer Kommunikationsfluss und die Einhaltung der Sicherheitsvorschriften gewährleistet sind.

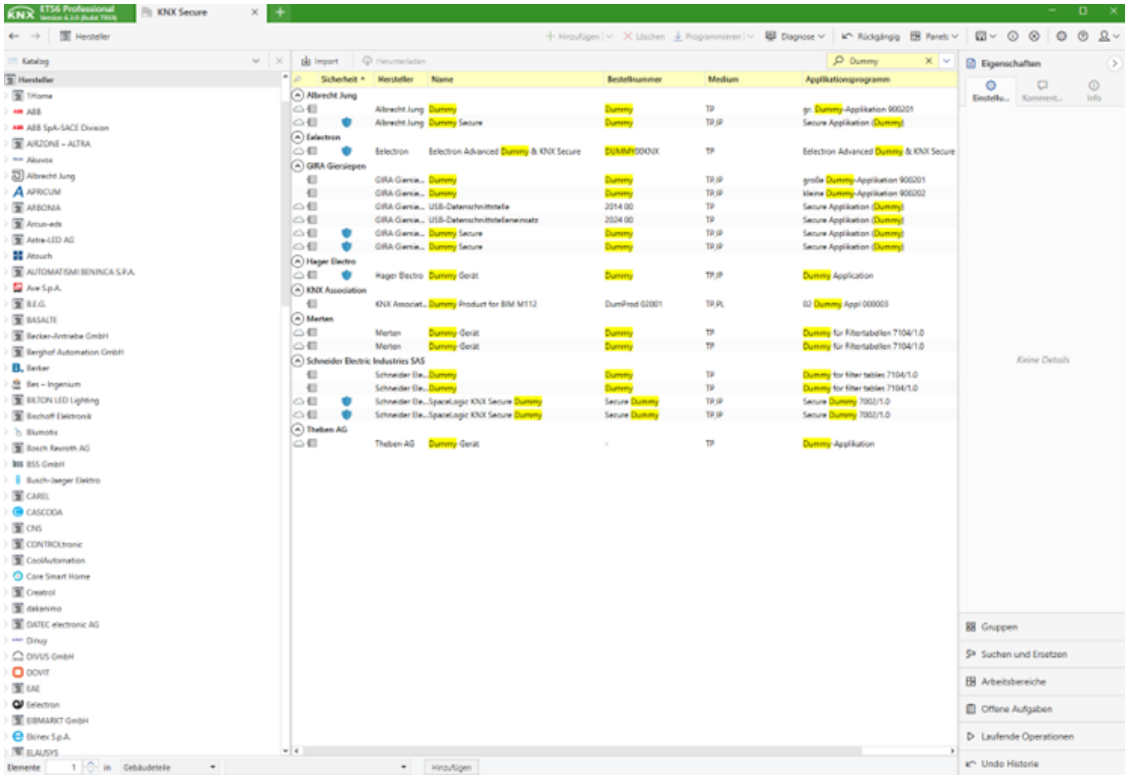


Bild 20: Beispiele für ETS-Dummy-Anwendungen

Wenn Sie Dummy-Objekte verwenden, um externe Kommunikationsgeräte in eine KNX Secure Einrichtung zu integrieren, ist es wichtig, den richtigen Typ von Dummy-Objekt aus dem ETS Online-Katalog auszuwählen.

Secure Dummy-Objekte sind im Katalog deutlich mit einem "Secure"-Symbol gekennzeichnet.

Wenn stattdessen ein "Plain" (Non Secure) Dummy-Objekt verwendet wird, stuft die ETS die Kommunikation automatisch auf KNX Plain zurück und deaktiviert damit KNX Data Secure für diesen Kommunikationspfad. Daher ist es wichtig, dass bei der Konfiguration von sicheren Kommunikationsteilnehmern nur als sicher gekennzeichnete Dummy-Objekte verwendet werden.

Wartung eines KNX Secure Projekts

Zugang und Sicherheit von ETS-Projekten in KNX Secure Systems
Um ein KNX Secure System zu warten oder Fehler zu beheben, ist der Zugang zum ETS-Projekt unerlässlich. Dies liegt daran, dass alle Parameter der sicheren Kommunikation, einschließlich der Schlüssel und Gerätekonfigurationen, innerhalb des ETS-Projekts verwaltet werden.

Passwortschutz

- Jedes ETS-Projekt ist durch ein Passwort geschützt.
- Ohne das richtige Passwort ist der Zugang unmöglich - selbst für kleinere Wartungsarbeiten.
- Es gibt keine Möglichkeit, das Passwort zurückzusetzen oder wiederherzustellen. Wenn das Passwort verloren geht, ist das Projekt dauerhaft unzugänglich.

Passwortverwaltung und Projektfreigabe
Ändern des Passworts für das ETS-Projekt:

- Hat keinen Einfluss auf ToolKeys oder MaC Keys.
- Eine erneute Inbetriebnahme des KNX Secure Systems ist nicht erforderlich.

Die Passwortänderungen gelten nur für die lokale Instanz des Projekts.

- Wenn ETS-Projekte von mehreren Personen genutzt oder bearbeitet wurden (z. B. mehrere Installateure oder Systemintegratoren), können diese weiterhin mit dem ursprünglichen Kennwort auf ihre lokalen Kopien zugreifen.
- Mit Zugang zu ihrer Kopie können sie Telegramme senden, empfangen, entschlüsseln und Änderungen am System vornehmen.

Sicherheitsrelevante Implikationen
Aus diesem Grund ist eine strenge Kontrolle über den Zugang zu ETS-Projekte von entscheidender Bedeutung.

Unbefugter Zugriff auf eine Projektdatei – auch ohne Kenntnis des aktuellen Passworts – kann die Integrität und Vertraulichkeit des KNX Secure Systems gefährden, sofern das ursprüngliche Passwort auf anderen Kopien noch gültig ist.

Koexistenz von KNX Plain und KNX Secure Geräten

KNX-Installationen können sowohl KNX Plain als auch KNX Secure Geräte enthalten, die auf dem gleichen physikalischen Medium arbeiten. Diese Flexibilität ermöglicht schrittweise Upgrades und gemischte Sicherheitsumgebungen.

Vollständig gesicherte Installationen
Wenn alle Geräte in der Anlage - vom Sensor bis zum Aktor - KNX Data Secure-fähig sind, kann die gesamte Installation durchgängig mit KNX Data Secure gesichert werden. Dies gewährleistet eine verschlüsselte und authentifizierte Kommunikation über alle Gruppenadressen und Medien hinweg.

Aktuelle Marktrealität
KNX Data Secure ist jedoch noch relativ neu, und nicht alle Gerätetypen oder Anwendungen verfügen derzeit über Secure-fähige Optionen. Dies schränkt die Möglichkeit ein, in einigen Szenarien eine vollständige Systemsicherheit zu gewährleisten.

Die Rolle des KNX Secure Proxy
Ein KNX Secure Proxy spielt eine entscheidende Rolle bei der Ermöglichung der Interoperabilität zwischen herkömmlichen KNX (Plain) und KNX Secure Geräten, während gleichzeitig das höchstmögliche Sicherheitsniveau innerhalb des Systems erhalten bleibt.

Anwendungsfälle: Erstellung von sicheren virtuellen Segmenten:
Diese Funktion erleichtert die Koexistenz von sicheren und unsicheren Geräten innerhalb einer einzigen Installation, indem Kommunikationsdomänen isoliert werden (Kopplerfunktionalität) und gleichzeitig zwischen verschlüsselter und unverschlüsselter Kommunikation übersetzt wird. Ein Koppler oder Router mit Proxy kann verwendet werden, um sichere Zonen innerhalb einer größeren KNX-Installation zu definieren und so den Schutz sensibler Kommunikation zu gewährleisten. **Der Proxy gewährleistet auch bei Legacy-Geräten sichere Kommunikation.** Es ist wichtig zu verstehen, dass der Secure Proxy die Kommunikation zwischen Geräten übersetzt, was darauf hindeutet, dass es sich um "virtuelle Zonen" handelt. Ein virtuelles sicheres Segment ist nur dann sicher, wenn alle KNX-Geräte innerhalb des Segments KNX-Secure Geräte sind und die gesamte Kommunikation innerhalb des Segments als Secure konfiguriert ist.

Umsetzung:
Der KNX Secure Proxy ist keine eigenständige Geräteklasse, sondern eine funktionale Komponente, die in verschiedenen Arten von KNX-Kopplern implementiert werden kann, darunter Segmentkoppler, Linienkoppler und Bereichskoppler (Backbone). Diese Koppler fungieren mit der Secure-Proxy-Funktionalität als Übersetzer zwischen sicheren und unsicheren KNX-Geräten, die sich in verschiedenen Segmenten befinden. Sie setzen bei Bedarf Verschlüsselungs- und Authentifizierungsregeln um.

Beschränkungen und Konfiguration des KNX Secure Proxy:
Ein KNX Secure Proxy unterstützt nicht die Übersetzung von Unicast-Kommunikation (Punkt-zu-Punkt) oder System-Broadcasts zwischen gesicherten und ungesicherten Domänen. Diese Einschränkung ist beabsichtigt und dient einem wichtigen Sicherheitszweck: Nur ETS-Instanzen mit gültigen Sicherheitsschlüsseln dürfen KNX-Geräte programmieren, die KNX Data Secure verwenden.

Einschränkungen bei der Umsetzung:
Die Secure Proxy-Funktion kann nur in Kopplern implementiert werden. Segmentkoppler sind nicht kaskadierbar, d.h. sie dürfen nicht auf der Sekundärseite eines anderen Segmentkopplers eingesetzt werden.

Abhängigkeiten bei der Konfiguration:
Zwischen dem Koppler und der Secure Proxy-Funktionalität bestehen mehrere Abhängigkeiten. Die Verfügbarkeit der Secure Proxy-Funktion hängt davon ab, wie der Koppler in der ETS 6 konfiguriert ist:

- Ist der Koppler als KNX Secure Gerät konfiguriert und wird in der ETS ein weiteres KNX Secure Produkt angelegt, wird die Secure Proxy Funktion automatisch aktiviert.
- Bei Konfiguration als KNX Plain-Gerät ist die Secure Proxy-Funktion nicht verfügbar.

Nach der Aktivierung werden die Secure Proxy-Einstellungen vollständig von der ETS verwaltet, basierend auf der Projektkonfiguration.

KNX-Projektübergabe

Auswirkungen des EU Cyber Resilience Act (CRA)

Der EU Cyber Resilience Act (CRA) führt verbindliche Cybersicherheitsanforderungen für alle Produkte mit digitalen Elementen ein, einschließlich KNX-Systeme. Ein zentraler Grundsatz des CRA ist, dass Kunden davon ausgehen können, dass ein Produkt standardmäßig sicher ist. Jegliche Einschränkung dieser Sicherheit – unabhängig davon, ob sie technisch kritisch ist oder nicht – muss dem Kunden eindeutig kommuniziert werden.

Bei der Übergabe eines KNX-Projekts ist es wichtig zu beachten:

- Übertragen Sie alle sicherheitsrelevanten Daten zusammen mit den allgemeinen Projektdaten.
- Erklären Sie dem Kunden die Sicherheitsmerkmale des Systems, einschließlich aller bekannten oder unvermeidbaren Risiken.
- Dokumentieren Sie diese Informationen und nehmen Sie sie in das technische Dokumentation auf, um künftige Haftungen zu vermeiden.

ETS-Berichte, Sicherheitszertifikate und Passwortverwaltung

1. ETS-Reports
Die ETS erstellt zwei Reports, die wichtige Sicherheitsinformationen enthalten:

- Projekt-Sicherheitsreport
- Projektzertifikatsreport

Diese Reports sollten:

- mit dem Kunden besprochen werden.
- In der Dokumentation zur Projektübergabe enthalten sein.

2. Kundenwahrnehmung und Zugang
Die Kunden - insbesondere diejenigen ohne ETS-Zugang - müssen über Folgendes informiert werden:

- Die zentrale Rolle des ETS-Projekts bei der Wartung von KNX Secure Systemen.
- Die Notwendigkeit einer kontinuierlichen Zusammenarbeit mit dem Systemintegrator, um das Projekt sicher und auf dem neuesten Stand zu halten.

3. Passwortverwaltung
Das ETS-Projekt ist durch ein Passwort geschützt, das für die Planung und Wartung erforderlich ist. Wenn der Kunde eine ETS-Lizenz hat, kann er ein neues lokales Kennwort vergeben, aber:

- Diese Änderung betrifft nur ihre lokale Kopie.
- ToolKeys, MaC Keys und Gruppentasten sind davon nicht betroffen.
- Wenn der Systemintegrator eine Kopie des Projekts behält, kann er weiterhin auf das System zugreifen und es ändern.

Es wird empfohlen, dies zu tun:

- Einigen Sie sich auf eine klare Richtlinie für die Verwaltung von ETS-Projektkopien und Passwörtern.
- Führen Sie eine Liste der Personen, die Zugang zum ETS-Projekt haben.

4. Geräte-Zertifikate

Für die Wiederverwendung von KNX Secure Geräten nach einem Master-Reset oder in einem neuen Projekt wird das Gerätezertifikat benötigt. Die Art der Speicherung und des Abrufs von Zertifikaten variiert je nach Hersteller und Produkt. Es ist von entscheidender Bedeutung, ein Verfahren zur Erfassung, Verwaltung und Übertragung dieser Zertifikate zwischen dem Systemintegrator und dem Kunden einzurichten.