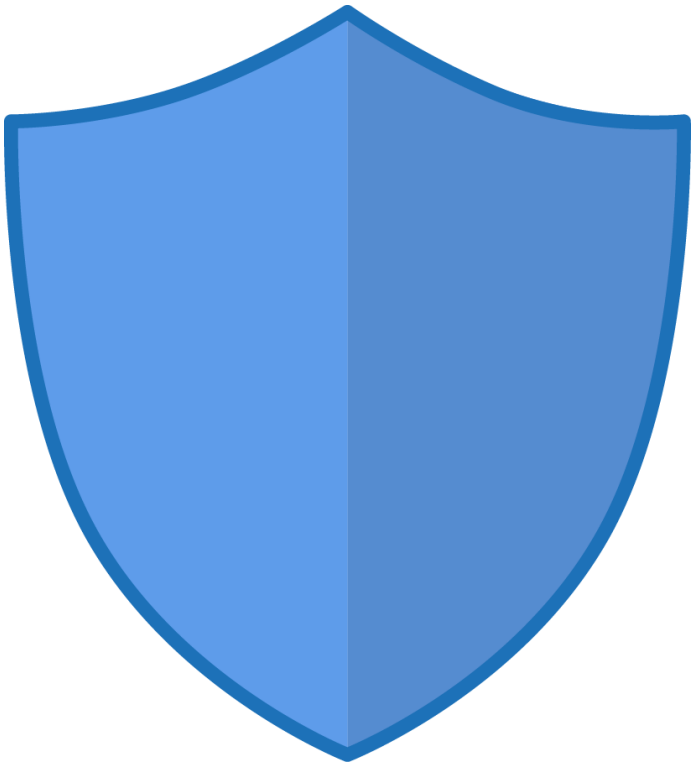
KNX
Systemdokumentation

GIRA

Stand der Dokumentation:
15.06.2020

KNX Data Secure



Inhaltsverzeichnis

1 Was ist KNX Data Secure?

Einleitung

Das Schalten von Licht, das Steuern einer Rolllade oder Jalousie, das Regeln einer Raumtemperatur und das zentrale Kontrollieren einzelner Gebäudefunktionen sind jeher Kernanwendungen einer digitalen Gebäudeinstallation mit KNX. Diese Anwendungen bergen in der Regel nur geringe Risiken in Bezug auf Sabotage und Kontrollverlust, besonders bei Verwendung drahtgebundener Vernetzung über die KNX-Medien Twisted-Pair (TP) oder Powerline (PL).

Eine KNX-Anlage ist heutzutage imstande, nicht nur einfache Steuerungs- und Kontrollaufgaben zu übernehmen, sondern vereinfacht darüber hinaus viele Handgriffe des täglichen Lebens durch zusätzliche Intelligenz und Automatisierung. Besonders die Verwendung neuer KNX-Medien wie KNXnet/IP und Funk (RF) ermöglichen diese Evolution. Doch gleichzeitig erzeugen vernetzte Eigenheime und intelligente Bürogebäude nicht unerhebliche Risiken, wenn wichtige Schutzmaßnahmen vernachlässigt werden. Jedes vernetzte und unsichere Gerät schafft Einfallstore, über die auf die Gebäudeinstallation und folglich auf die persönlichen Geräte zugegriffen werden kann.

Aus den genannten Gründen geht das Verständnis von Kunden und Installateuren in Bezug auf die Zuverlässigkeit einer KNX-Installation weit über Stabilität und Interoperabilität hinaus. Moderne Anforderungen an eine zuverlässige und sichere KNX-Installation sind...

- Schutz vor unberechtigter Manipulation der Konfiguration
- Ausfallsichere Bedienung von Gebäudefunktionen
- Störungsfreie Visualisierung und Funktionslogik
- Sicherung der übertragenen Daten
- Nachhaltige Kontrolle über die gesamte Gebäudeinstallation

Zur Sicherstellung dieser Anforderungen ist ein fundiertes Schutzkonzept erforderlich. Die Basis bildet eine sorgfältige Abschottung des Systems gegen unberechtigten Zugriff. Im Falle einer KNX-Anlage gilt, dass nur befugte Personen (Installateure, Nutzer, Wartungspersonal) Zugriff auf die Komponenten und Funktionen der Anlage erhalten. Schon bei der Planung und Installation müssen die kritischen Anlagenteile (insbesondere bei Verwendung offener Medien wie IP und RF) mit KNX Data Secure geschützt werden.

KNX Data Secure

KNX Data Secure signiert und verschlüsselt die Kommunikation im KNX-Netzwerk und gewährleistet eine gesicherte Datenübertragung von Telegrammen. Die Kommunikation im Zuge von Inbetriebnahmevorgängen mit der ETS und ebenso die Laufzeitkommunikation zwischen Geräten und zu Visualisierungen ist hierdurch gesichert. Das Konzept bewirkt, dass unabhängig vom Medium alle oder nur ausgewählte KNX-Telegramme authentifiziert und verschlüsselt werden. Somit ist die Kommunikation zwischen Sender und Empfänger weder interpretierbar noch manipulierbar. KNX Data Secure schützt Benutzerdaten wirksam vor unberechtigtem Zugriff und vor Manipulation.

Bild 1: KNX Data Secure schützt vor unberechtigtem Zugriff und vor Manipulation

Bei der Sicherheitsarchitektur setzt KNX Data Secure auf ISO 18033-3 normierte Sicherheitsalgorithmen, wie die AES-128-Verschlüsselung. Die KNX Data Secure Technologie ist nach EN 50090-3-4 standardisiert. KNX blockiert Hackerangriffe auf die digitale Infrastruktur von vernetzten Gebäuden.

KNX Data Secure ist herstellerübergreifend im KNX-Standard spezifiziert. Zertifizierte KNX Data Secure fähige Geräte unterschiedlicher Hersteller können miteinander sicher kommunizieren.

KNX Data Secure ermöglicht die sichere Kommunikation auf Telegrammebene vom Sender bis zum Empfänger (Ende-zu-Ende-Sicherung). Die Teilnehmer bauen einen gesicherten Kommunikationskanal auf, einschließlich einer Authentifizierung der zulässigen Kommunikationspartner und Verschlüsselung der Übertragung. Dies erfolgt bei der Inbetriebnahme von KNX Data Secure Geräten durch die ETS und bedarfsweise auch danach, wenn Geräte gemeinsam Daten und Informationen austauschen (siehe Bild 2).

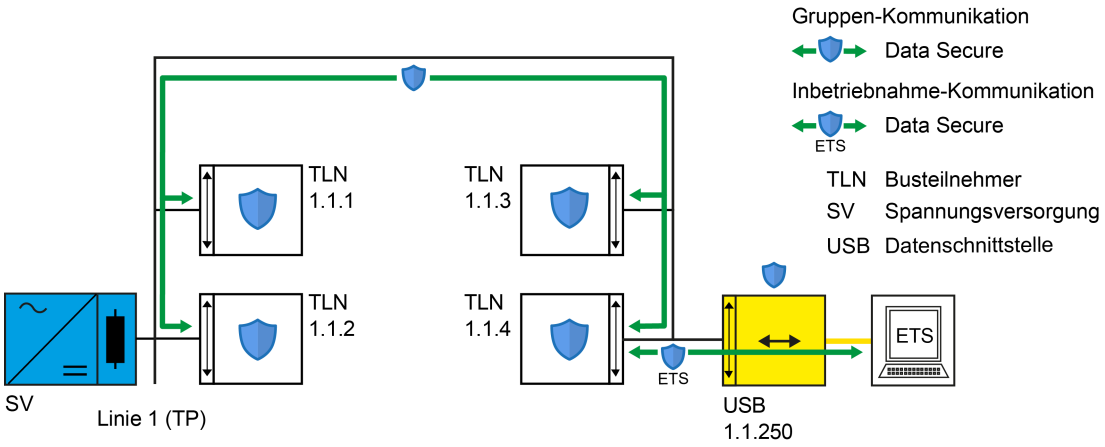


Bild 2: Topologieschema 1 (Beispiel)
"Sichere Kommunikation in einer TP-Linie"

KNX Data Secure Geräte verwenden für die Übertragung der authentifizierten und verschlüsselten Daten ein längeres KNX-Telegrammformat (Extended Frames), als herkömmliche Geräte. Dies hat keine Auswirkungen auf die Reaktionsgeschwindigkeit der Geräte. Unsecure-Geräte können in derselben Installation und auf gleichen Medien eingesetzt werden (siehe Bild 3). Das bedeutet, dass KNX Data Secure als zusätzliche Maßnahme zur Realisierung einer zuverlässigen Sicherheit für ausgewählte Geräte oder Funktionen in neuen oder bestehenden Anlagen verwendet werden kann.

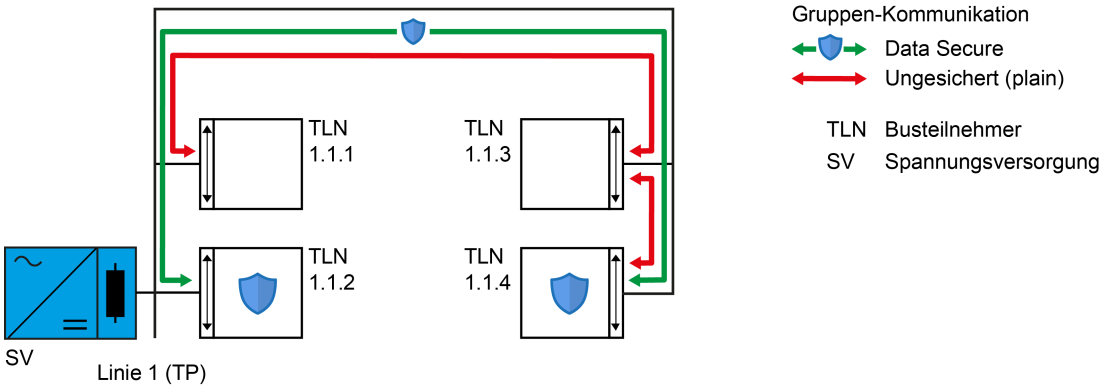


Bild 3: Topologieschema 2 (Beispiel)
"Gesicherte und ungesicherte Kommunikation in derselben KNX-Installation"

KNX Data Secure fähige Geräte, die durch die ETS sicher in Betrieb genommen wurden und auch über Kommunikationsobjekte zur Laufzeit gesicherte Daten mit anderen KNX Data Secure fähigen Geräten austauschen, können grundsätzlich über ausgewählte Gruppenadressen auch auf herkömmlichem Weg ungesichert kommunizieren. Es ist ein Mischbetrieb von sicherer und herkömmlicher Kommunikation an einem Sensor oder Aktor über unterschiedliche Kommunikationsobjekte möglich. Allerdings ist eine gesicherte und ungesicherte Kommunikation über ein und dasselbe Kommunikationsobjekt nicht möglich!
Im ETS-Projekt wird festgelegt, welche Gruppenadressen sicher und welche Gruppenadressen herkömmlich kommunizieren (siehe Kapitel "Projektierung" ▸ Seite 20).

Aufgrund des längeren Telegrammformats müssen auch die verwendeten Systemkomponenten (z. B. Bereichs-/Linienkoppler) und die lokalen Datenschnittstellen der ETS (z. B. USB) Extended Frames unterstützen. In einer KNX Data Secure Installation muss sichergestellt sein, dass alle Systemkomponenten, die zwischen KNX Data Secure Teilnehmern und zwischen der ETS und den Teilnehmern liegen, diese Fähigkeit besitzen (siehe Bild 4). Dies ist immer dann zu beachten, wenn linienübergreifend kommuniziert werden soll und besonders auch dann, wenn bestehende KNX-Installationen um KNX Data Secure erweitert werden. Gegebenenfalls müssen ältere Systemkomponenten durch KNX Data Secure kompatible ersetzt werden.

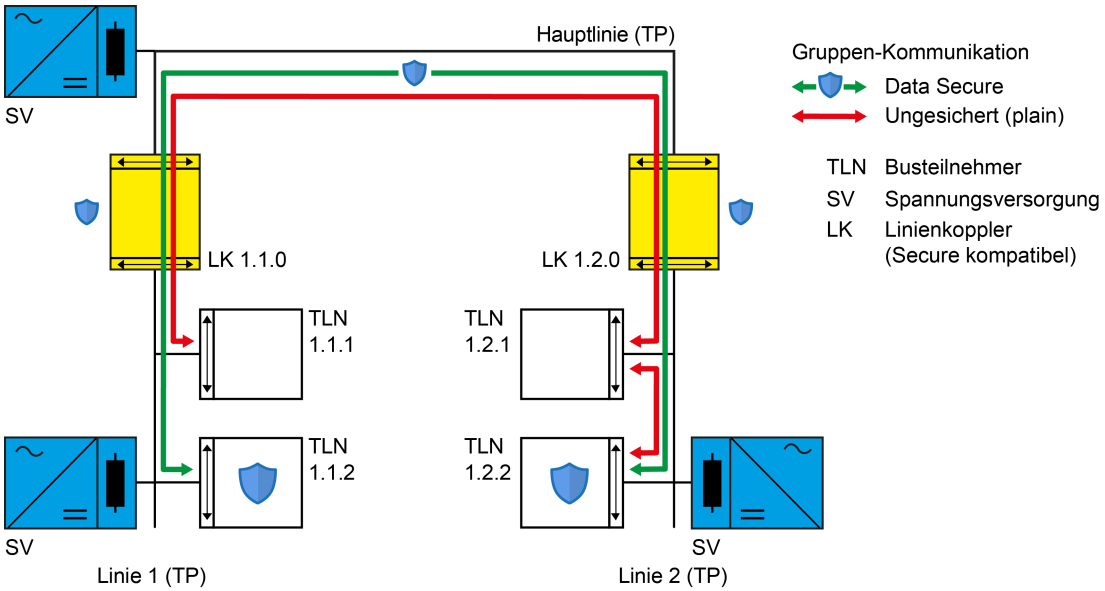


Bild 4: Topologieschema 3 (Beispiel)
"Gesicherte und ungesicherte Kommunikation linienübergreifend - Verwendung von Data Secure kompatiblen Systemkomponenten"

Systemkomponenten sind nicht KNX Data Secure kompatibe, wenn die verwendeten Geräte das erweiterte Telegrammformat nicht unterstützen! Eine sichere Laufzeitkommunikation oder Inbetriebnahme über solche Systemgeräte hinweg ist nicht möglich (siehe Bild 5).
Allerdings können KNX Data Secure fähige Geräte innerhalb einer Linie oder eines Liniensegments stets sicher miteinander kommunizieren und auch sicher mit der ETS in Betrieb genommen werden.

Im Anhang dieser Dokumentation ist eine Übersicht der Systemkomponenten aufgeführt. Anhand dieser Geräteübersicht kann identifiziert werden, welche Systemkomponenten KNX Data Secure kompatibel sind.

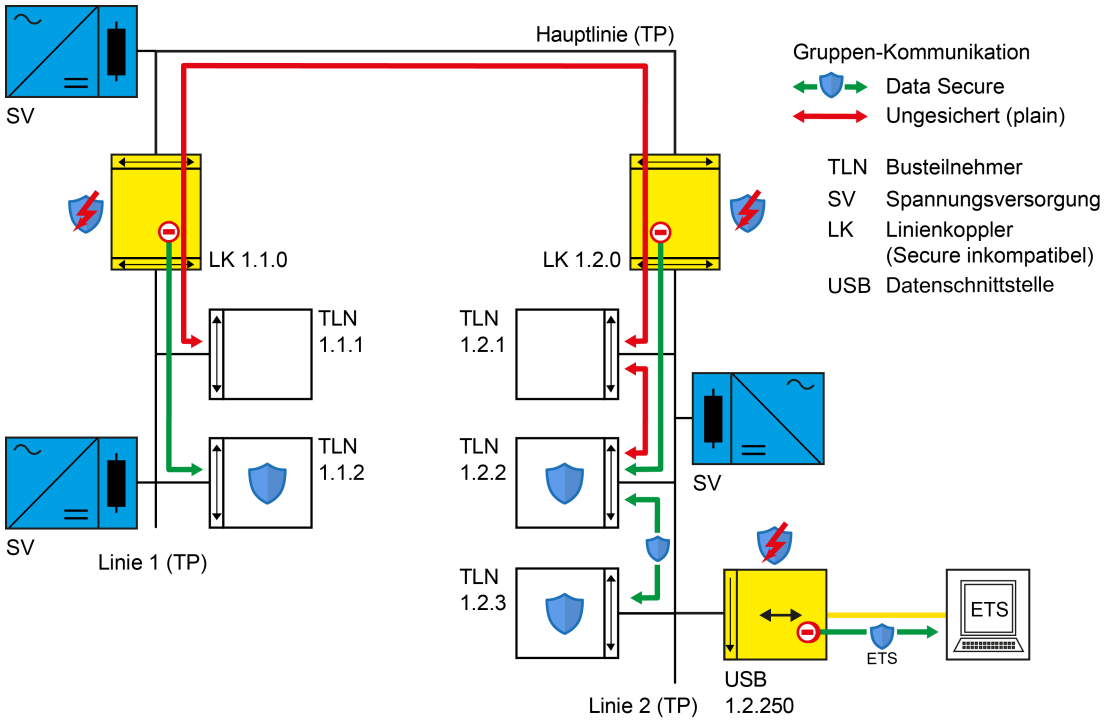


Bild 5: Topologieschema 4 (Beispiel)
"Gesicherte und ungesicherte Kommunikation linienübergreifend - Verwendung von nicht Data Secure kompatiblen Systemkomponenten"

Aufgrund der medienneutralen Eigenschaft von KNX Data Secure kann eine Kommunikation auch linienübergreifend in allen KNX-Medien durchgeführt werden (siehe Bild 6). Ebenso ist eine ETS-Inbetriebnahme medienneutral möglich. Auch hierbei ist zur störungsfreien Kommunikation darauf zu achten, dass die verwendeten Systemkomponenten (Medienkoppler, Datenschnittstellen) KNX Data Secure kompatibel sind!

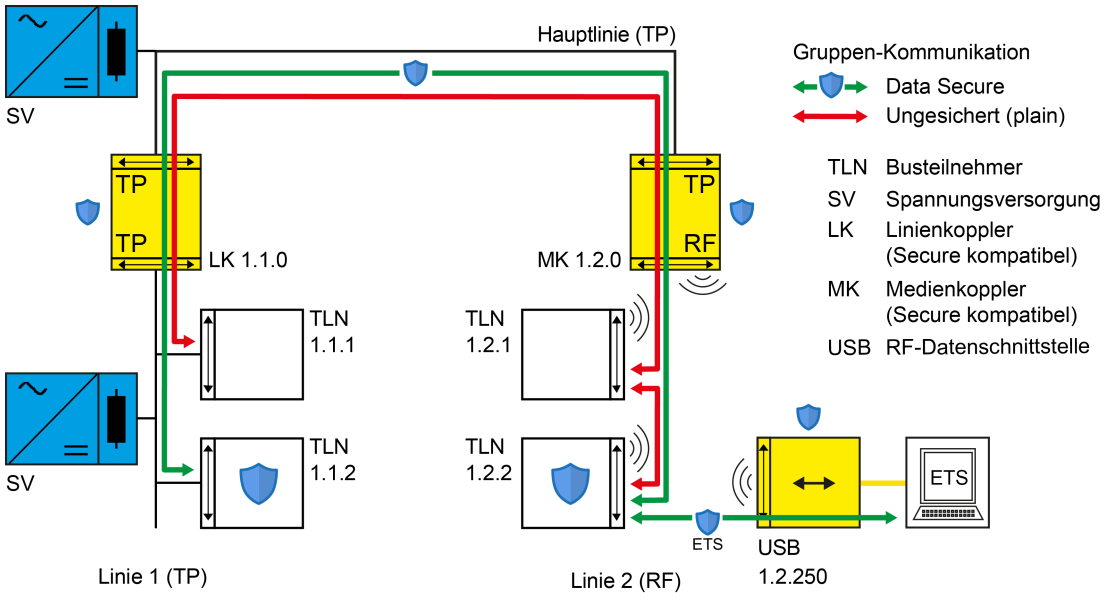


Bild 6: Topologieschema 5 (Beispiel)
"Gesicherte und ungesicherte Kommunikation linienübergreifend in einer TP-RF-Mischinstallation"

Geräte, die KNX Data Secure fähig sind, können bedarfsweise mit der ETS auch auf herkömmlichem Weg in Betrieb genommen werden und infolgedessen zur Laufzeit auch mit ungesicherten Telegrammen kommunizieren. Das Verhalten ist dann genauso wie bei Geräten, die nicht KNX Data Secure fähig sind. Auf diese Weise können auch moderne KNX Data Secure fähige Geräte in bestehenden Anlagen zum Tausch defekter Aktoren oder Sensoren verwendet werden (siehe Bild 7). Es ist nicht erforderlich, die gesamte KNX-Anlage oder Teile davon umzubauen und auf sichere Kommunikation zu aktualisieren.

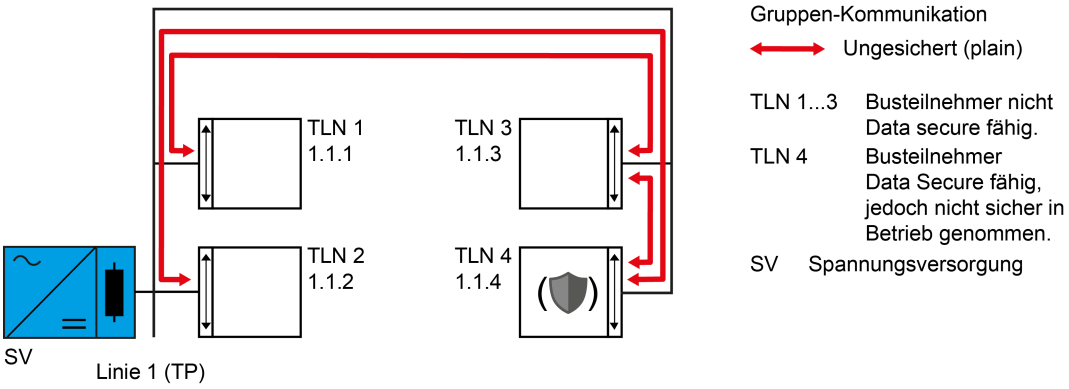


Bild 7: Topologieschema 6 (Beispiel)
"KNX Data Secure fähiges Gerät zwecks Gerätetausch ungesichert in Betrieb genommen"

Expertenwissen
Bei KNX Data Secure wird die Datenprotokoll-Information (APCI) und die Nutzlast (Daten) eines Telegramms verschlüsselt. Telegramm-Header, Quell- und Zieladresse werden nur signiert (im Klartext) übertragen. Dadurch ergibt sich der Vorteil, dass per KNX Data Secure gesicherte Telegramme für ein Telegramm-Routing durch Bereichs-/Linien-Koppler oder Medienkoppler nicht entschlüsselt werden müssen. Die Verwendung ist dadurch medienneutral und beeinflusst nicht die Transaktionsgeschwindigkeit übertragener Telegramme im Vergleich zu einer ungesicherten Kommunikation. KNX Data Secure verwendet den CCM-Modus mit 128-Bit AES-Verschlüsselung (Datenverschlüsselung "Counter-Mode" mit Integritätssicherung "CBC-MAC-Mode") und symmetrischen Schlüsseln. Ein symmetrischer Schlüssel bedeutet, dass der gleiche Schlüssel sowohl durch den Sender für die Verschlüsselung ausgehender Meldungen (Authentifizierung und Integritätssicherung) als auch durch den oder die Empfänger zur Verifikation und Entschlüsselung der empfangenen Meldungen verwendet wird.

Exkurs KNX IP Secure

KNX IP Secure erlaubt, dass KNX-Telegramme in IP-Netzen authentifiziert und verschlüsselt werden. Auf diese Weise ist sichergestellt, dass KNX-Tunneling oder -Routing Meldungen auf IP nicht mitgelesen oder manipuliert werden können. Die KNX IP Secure Mechanismen sind eine zusätzliche Sicherheitshülle (Wrapper), die den kompletten KNXnet/IP-Datenverkehr schützt.

KNX Data Secure und KNX IP Secure können in KNX-Installationen koexistent verwendet werden. Es ist durchaus möglich, zeitgleich die IP-Kommunikation zwischen mehreren IP-Routern oder zwischen IP-Datenschnittstellen und der ETS per KNX IP Secure zu sichern und darüber hinaus den normalen Datenverkehr über Gruppenadressen inkl. Inbetriebnahmekommunikation per KNX Data Secure (siehe Bild 8).

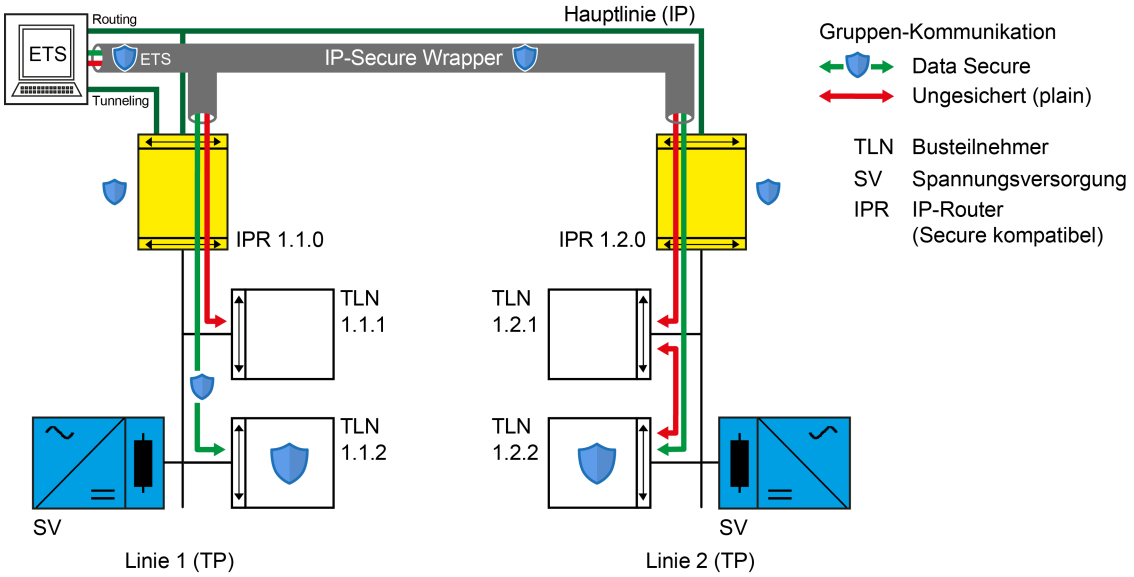


Bild 8: Topologieschema 7 (Beispiel)
"Gesicherte und ungesicherte Kommunikation linienübergreifend bei Verwendung von IP-Routern"

2 Wozu KNX Data Secure?

Nutzen

Die bei KNX Data Secure verwendeten Mechanismen ermöglichen KNX Geräten und der ETS eine gesicherte Kommunikation. Aber wie funktioniert das konkret? Welcher Nutzen leitet sich aus den Sicherheitsbausteinen für die Anlage und folglich für die Benutzer einer KNX Data Secure konformen KNX-Installation ab?

Die folgende Auflistung erläutert die einzelnen Bausteine des KNX Data Secure Mechanismus und erklärt den technischen Nutzen einer auf diese Weise gesicherten Anlage:

– Freshness

  Die "Freshness" verhindert, dass ein Angreifer zulässige Telegramme zu einem beliebigen Zeitpunkt aufgezeichnet und irgendwann später erneut abspielt. Hierdurch werden Telegramm-Wiederholungen zur erneuten Auslösung von bekannten, älteren Aktionen in einer KNX-Anlage sicher unterbunden (z. B. das Öffnen eines Garagentores über einen unerlaubt aufgezeichneten 1-Bit Schaltbefehl).
  Ein Empfänger wertet nur "frische" Telegramme eines Senders aus.

  In Kombination mit der Datenintegrität (siehe nächster Punkt) ist die "Freshness" eine wirksame Sicherungsmethode, um unerlaubten Zugriff auf eine KNX-Installation zu verhindern, wenn man unzulässig im Besitz bekannter, ggf. aufgezeichneter Telegrammsequenzen ist.

– Datenintegrität

  Im Zuge der Datenintegrität wird wirkungsvoll verhindert, dass ein Angreifer Kontrolle über eine KNX-Anlage erhält. Es wird unterbunden, dass Telegramme manipuliert oder zusätzliche (falsche) Informationen eingespeist werden. Dies wird erreicht, indem in jedes Telegramm ein verschlüsselter Authentifikations-Code eingefügt wird. Durch diesen Code können Empfänger verifizieren, ob eine Meldung unzulässig verändert wurde.

– Authentifizierung

  Die Authentifizierung schafft einen Telegramm-Identitätsnachweis. Sie stellt sicher, dass die Quelle eines Telegramms auch wirklich von einem berechtigten Kommunikationspartner kommt. Ein Empfänger verwirft ein erhaltenes Inbetriebnahme- oder Gruppentelegramm, wenn ihm die Quelladresse (physikalische Adresse) des Telegramms unbekannt ist.

– Vertraulichkeit

  Die Telegramm-Vertraulichkeit verhindert durch Verschlüsselung das Mitlesen von Telegramminhalten zur Laufzeit (Gruppenkommunikation) und während der ETS-Inbetriebnahme. Ein Angreifer hat dadurch keinen Einblick mehr in die versendeten Daten einer KNX-Installation. Es ist ohne Besitz der Gruppen- oder ETS-Schlüssel nicht mehr möglich, Inhalte von Telegrammen (z. B. EIN, AUS, Werte) zu interpretieren.

Expertenwissen

Freshness

Bei KNX Data Secure wird die "Freshness" über eine 6-Byte lange Sendesequenznummer sichergestellt. Ein Secure-Kommunikationspartner (z. B. Aktor) wertet nur dann ein Gruppentelegramm als gültig aus, wenn die enthaltene Sequenznummer eines Senders (z. B. Tastsensor) mindestens um einen Stellenwert höher ist als der zuletzt empfangene Wert desselben Senders. Telegramme, die einen niedrigeren oder denselben Stellenwert besitzen, werden durch den Empfänger verworfen.
Die Sendesequenznummer muss nicht immer genau um einen Stellenwert höher sein (n+1). Wichtig ist, dass sie fortlaufend ist (n+x).

Bei einem Master-Reset wird die Sendesequenznummer durch die Geräte selbstständig auf einen Initialwert zurückgestellt. Im Falle eines Gerätetausches versucht die ETS, zurückgestellte Geräte zu erkennen und ersetzt den Initialwert durch eine gültige Sendesequenznummer anhand einer vorgegebenen Methode.

Bei einem Programmiervorgang werden durch die ETS und das Gerät separate Sequenznummern verwendet. Sendesequenznummern können im Gruppenmonitor der ETS abgelesen werden. Sie sind nicht verschlüsselt, aber gegen Manipulation geschützt.

Expertenwissen

Datenintegrität

KNX Data Secure verwendet den im CCM-Modus enthaltenen "CBC-MAC-Mode" mit 128-Bit AES-Verschlüsselung zur Sicherung der Datenintegrität. Dabei wird ein "Message Authentication Code" (MAC) der Nachricht angehangen. Dieser Authentifikations-Code signiert alle im Telegramm enthaltenen Informationen, so dass deren Manipulation erkannt werden kann.

Expertenwissen

Authentifizierung

Der Identitätsnachweis eines empfangenen Telegramms erfolgt über die enthaltene physikalische Adresse des Senders (Quelladresse). Ein Empfänger lässt nur dann das Telegramm zu, wenn die enthaltene Quelladresse in einer speziellen Kommunikationstabelle eingetragen ist. Jeder KNX Data Secure fähige Teilnehmer besitzt eine solche Kommunikationstabelle. Sie wird im Zuge der Inbetriebnahme automatisch durch die ETS programmiert. Die Tabelle enthält wie in einer sortierten Liste eine Kombination aus den physikalischen Adressen der zulässigen Kommunikationspartner und deren Sendesequenznummern.

Telegramme von Geräteadressen, die nicht in die Kommunikationstabelle eingetragen sind, werden durch Empfänger verworfen. Dieser Effekt ist besonders dann zu berücksichtigen, wenn einzelne Geräte eines ETS-Projekts vorab in Betrieb genommen wurden und anschließend eine Erweiterung desselben Projekts durch weitere Teilnehmer (Sensoren oder Aktoren) vorgenommen wird.
Merke: Alle Teilnehmer, die zur Laufzeit in einer sicheren KNX-Anlage ordnungsgemäß miteinander kommunizieren sollen, müssen nach erfolgter finaler Projektierung in der ETS abschließend (ggf. wiederholt) programmiert werden! Der ordnungsgemäße Programmierzustand aller Geräte in einem ETS-Projekt kann über die Programmier-Flags festgestellt werden. Bei Änderung oder Ergänzung einer vorhandenen Konfiguration (z. B. Verknüpfung von Gruppenadressen) muss immer auch der Programmierzustand anderer verknüpfter Teilnehmer geprüft werden. Es wird empfohlen, dynamische Ordner der ETS zu verwenden. Dadurch werden neu zu programmierende Geräte sicher identifiziert.

Expertenwissen

Vertraulichkeit

Zur Verschlüsselung von Telegrammen werden AES-128-CCM-Algorithmen mit symmetrischen Schlüsseln verwendet. Bei KNX Data Secure wird die Datenprotokoll-Information (APCI) und die Nutzlast (Daten) eines Telegramms verschlüsselt. Telegramm-Header, Quell- und Zieladresse werden nur signiert (im Klartext) übertragen.

3 Was bedeutet das?

Begriffe und Bedeutungen

Beim Verwenden von KNX Data Secure werden Installateure, Integratoren und ETS-Benutzer mit neuen Begriffen und Elementen konfrontiert, die es bislang nicht gab, aber die besonders wichtig und folglich unbedingt zu beachten sind. Dieses Kapitel führt alle wichtigen Elemente auf, die im KNX Data Secure Kontext wichtig sind und erläutert deren Bedeutungen.

Die verwendeten Abbildungen und Textdarstellungen sind beispielhaft und sollen die unterschiedlichen Elemente symbolisieren und dabei helfen, die Begriffe zu differenzieren.

Der Factory-Default-Setup-Key (FDSK) wird zur ersten Inbetriebnahme eines KNX Data Secure fähigen Geräts verwendet, jedoch nur, wenn dieses Gerät mit der ETS sicher in Betrieb genommen werden soll. Der FDSK wird bereits im Zuge der ersten sicheren Inbetriebnahme beim Schreiben der physikalischen Adresse ungültig und durch den Toolkey (siehe weiter unten) ersetzt.

Der FDSK ist 128-Bit lang und als Hersteller-Initialschlüssel eines KNX Data Secure fähigen Geräts zu verstehen. Er liegt für jedes Data Secure fähige Gerät weltweit einmalig vor. Der FDSK ist im Gerätezertifikat enthalten (siehe weiter unten bei "Gerätezertifikat"), welches auf dem Gerät im Auslieferungszustand angebracht ist.

Sofern zur ersten Inbetriebnahme erfolgreich eingelesen, wird der FDSK lesbar im ETS-Projekt bei den Gerätezertifikaten archiviert. Er kann durch einen Master-Reset im Gerät wiederhergestellt und folglich reaktiviert werden, so dass ein Gerät wie im Auslieferungszustand neu in Betrieb gesetzt werden kann. Bei Verlust des an den Geräten angebrachten Gerätezertifikats und folglich des FDSK kann ein Gerät nicht mehr durch andere ETS-Projekte sicher in Betrieb genommen werden!

Der Toolkey wird ausschließlich von der ETS zum Programmieren eines KNX Data Secure fähigen Geräts verwendet. Er ist ebenfalls 128-Bit lang, eindeutig für jeweils ein Gerät im Projekt und ersetzt bereits bei der ersten Inbetriebnahme den FDSK. Anschließend verwendet die ETS für jeden Programmiervorgang im gesicherten Betrieb den Toolkey. Ohne Kenntnis dieses besonderen Schlüssels (z. B. Zugriff über andere ETS-Projekte) kann ein sicher in Betrieb genommenes Gerät nur mit Verlust einer Konfiguration neu programmiert werden (siehe "Master-Reset" weiter unten).

Der Toolkey wird, weil er nur für die ETS im vorliegenden Projekt relevant ist, für den ETS-Benutzer unlesbar im ETS-Projekt archiviert. Sofern das Projekt exportiert wird, schreibt die ETS alle Toolkeys des Projekts verschlüsselt und signiert in die *.KNXPROJ-Datei.

Die Laufzeitschlüssel sind die AES-Schlüssel für die Laufzeitkommunikation über Gruppenadressen (auch "Runtime Keys" oder "Group Keys" genannt). Jede Gruppenadresse besitzt in einem ETS-Projekt einen eigenen 128-Bit langen Laufzeitschlüssel, sofern die Adresse zur sicheren Kommunikation zwischen KNX Data Secure Geräten verwendet wird.

Genau wie der Toolkey, werden die Laufzeitschlüssel für den ETS-Benutzer unlesbar im ETS-Projekt archiviert und bei einem Projektexport geschützt in die Projektdatei geschrieben. Bedarfsweise können alle oder vereinzelte Laufzeitschlüssel eines vorliegenden Projekts in eine spezielle und durch ein Passwort geschützte Exportdatei (*.knxkeys), auch Projekt-Schlüsselbund genannt, ausgeleitet werden. Diese Ausleitung ist dann erforderlich, wenn Komponenten mit einer KNX Data Secure Anlage zusammenspielen sollen, diese aber nicht mit der ETS konfiguriert und in Betrieb genommen werden (z. B. Visualisierungen). In solchen Fällen kann mit der ETS ein Laufzeit-Schlüsselbund exportiert und per Import den erforderlichen Komponenten bereitgestellt werden.

000A:2E671611

Die Seriennummer ist eine 6-Byte lange Identifizierungsnummer des Herstellers zur eindeutigen Kennzeichnung von KNX Geräten. Die Seriennummer wird im Zuge der Produktion individuell (weltweit für jeden Hersteller einmalig) festgelegt und unveränderlich in die Geräte programmiert.

Die ETS verwendet die Seriennummern zur Identifikation neuer und bereits in Betrieb genommener Geräte in einer KNX-Installation. Anhand der Seriennummern werden eingelesene Gerätezertifikate qualifiziert und für den Inbetriebnahmeprozess selektiert (siehe Kapitel "Inbetriebnahme" ▸ Seite 27).

Die Seriennummern aller im Projekt eingelesenen Gerätezertifikate und aller damit in Betrieb genommenen Geräte werden durch die ETS im Projekt-Schlüsselbund archiviert und können dort eingesehen werden.

AAFC4Z-YWCGQK-DIVDUS-S2NJ5I-VGVKXL-FNV2XS

Das Gerätezertifikat ist eine Zeichenkette (36 Zeichen), die den FSDK und die Seriennummer eines KNX Data Secure fähigen Geräts enthält. Das Gerätezertifikat muss vor der Inbetriebnahme der ETS mitgeteilt werden, um ein Gerät sicher in Betrieb nehmen zu können. Die ETS leitet aus dem Zertifikat den zu einer Seriennummer passenden FDSK ab.

Die Gerätezertifikate sind jeweils auf ablösbaren Etiketten abgedruckt, die sich an den Geräten befinden. Diese Etiketten sind bereits bei der Montage von den Geräten zu entfernen und sicher aufzubewahren! Andernfalls ist nicht auszuschließen, dass Unbefugte in den Besitz der FDSK gelangen und Manipulationen an vorhandenen Geräten einer sicheren KNX-Installation durchführen.

Der QR-Code ergänzt die Zeichenkette des Gerätezertifikats. Er enthält das Gerätezertifikat in maschinenlesbarer Form und kann über eine PC-Kamera (z. B. Webcam) mit Bordmitteln der ETS in ein Projekt eingelesen werden.

Es wird empfohlen, zum Scannen des QR-Codes eine hochauflösende Kamera zu verwenden.

Der Master-Reset ist eine Funktion zum Rücksetzen eines KNX Data Secure fähigen Geräts in einen vom Hersteller vorgesehenen Funktionszustand. Beim Ausführen eines Master-Reset gehen alle Benutzereinstellungen verloren. Die Parametrierung wird auf die Standardeinstellung zurückgestellt, die physikalische Adresse wird auf 15.15.255 initialisiert, alle Laufzeitschlüssel und der Toolkey, sofern das Gerät zuletzt im sicheren Betrieb war, werden gelöscht. Zudem wird der FDSK im Gerät wieder wirksam. Die Geräte müssen anschließend mit der ETS neu in Betrieb genommen werden.

Bei Secure-Betrieb: Ein Master-Reset deaktiviert die Gerätesicherheit. Das Gerät kann mit dem Gerätezertifikat (FDSK) anschließend erneut sicher in Betrieb genommen werden.

Durch einen Master-Reset wird nicht die Firmware eines Geräts beeinflusst. Das Auslösen und Signalisieren des Master-Resets ist geräteabhängig und wird in der jeweiligen Produktdokumentation erklärt.

Mit der Gira ETS Service-App können Geräte auf Werkseinstellungen zurückgesetzt werden. Diese Funktion nutzt die im Gerät enthaltene Firmware, die zum Zeitpunkt der Auslieferung aktiv war (Auslieferungszustand).

Durch das Zurücksetzen auf Werkseinstellungen verlieren die Geräte ihre physikalische Adresse und Konfiguration. Genau wie beim Master-Reset müssen die Geräte anschließend mit der ETS neu in Betrieb genommen werden.

Details zum Werks-Reset sind der Dokumentation der Gira ETS Service-App zu entnehmen.

4 Wie erkenne ich KNX Data Secure?

Kennzeichnung KNX Data Secure fähiger Geräte

KNX Data Secure fähig ist ein Gerät dann, wenn im Allgemeinen die Fähigkeit existiert, gesichert durch die ETS in Betrieb genommen zu werden und anschließend zur Laufzeit auch gesichert zu kommunizieren (sichere Gruppenkommunikation). Geräte, die auf eine solche Weise KNX Data Secure unterstützen, sind daran zu erkennen, dass auf dem Produktetikett oder -druckbild ein "**X**" angebracht ist. Dies ist die KNX-konforme und herstellerübergreifende Kennzeichnung. Zusätzlich sind KNX Data Secure fähige Geräte aus dem Hause Gira noch mit einem "Secure Shield"-Symbol ⛨ kenntlich gemacht.
Geräte mit den genannten Kennzeichnungen sind zueinander kompatibel und ohne Einschränkungen KNX Data Secure fähig.

Bild 9: Beispiel einer Gerätebeschriftung eines KNX Data Secure fähigen Geräts

⛨ + X KNX Data Secure fähiges Gerät
TP Medium TP (Twisted Pair)
S S-Mode (ETS kompatibel)

KNX Data Secure fähige Geräte müssen nicht zwangsläufig sicher in Betrieb genommen werden. Es ist möglich, die Sicherheit in der ETS für alle oder einzelne Geräte eines Projekts zu deaktivieren. Geräte, bei denen die Sicherheit deaktiviert wurde, kommunizieren immer ungesichert und verhalten sich dann in Bezug auf die Inbetriebnahme- und Laufzeitkommunikation genau wie Geräte, die nicht KNX Data Secure fähig sind und denen folglich die genannten Kennzeichnungen fehlen. Ob KNX Geräte nun tatsächlich sicher kommunizieren, ist dem Projekt zu entnehmen und nicht der Kennzeichnung auf dem Produkt, welche nur die Fähigkeit ausweist.

i KNX Data Secure fähige Geräte, die durch die ETS sicher in Betrieb genommen wurden und auch über Kommunikationsobjekte zur Laufzeit gesicherte Daten mit anderen KNX Data Secure fähigen Geräten austauschen, können grundsätzlich über ausgewählte Gruppenadressen auch herkömmlich kommunizieren. Es ist ein Mischbetrieb von sicherer und herkömmlicher Kommunikation an einem Sensor oder Aktor über unterschiedliche Kommunikationsobjekte möglich. Allerdings ist eine gesicherte und ungesicherte Kommunikation über ein und dasselbe Kommunikationsobjekt nicht möglich!

Kennzeichnung in der ETS

Die ETS kennzeichnet KNX Data Secure fähige Geräte mit einem "Secure Shield"-Symbol. Die Anzeige erfolgt in der Listenansicht der Geräte und in der Baumstruktur eines geöffneten ETS-Projekts und bezieht sich nicht direkt auf das Gerät (Hardware), sondern vielmehr auf das verwendete Applikationsprogramm (siehe Bild 10).

Am Beispiel der ETS5 erklärt: Wenn in der Listenansicht in der Spalte "**Sicherheit**" ein Symbol angezeigt wird, handelt es sich um ein KNX Data Secure fähiges Applikationsprogramm. Die Farbe des Symbols weist darauf hin, dass es sich entweder um ein Applikationsprogramm mit aktivierter Gerätesicherheit handelt (1) , oder alternativ die Gerätesicherheit bei der verwendeten Applikation deaktiviert ist (2) . Applikationsprogramme, zu denen kein solches Symbol in der Listenansicht angezeigt wird (3), sind grundsätzlich nicht Data Secure fähig.
In der Baumstruktur werden Geräte - entsprechend des verwendeten Applikationsprogramms - ebenso mit einem "Secure Shield"-Symbol (4) kenntlich gemacht. Dies erfolgt an dieser Stelle jedoch nur für Applikationsprogramme mit tatsächlich aktivierter Gerätesicherheit.

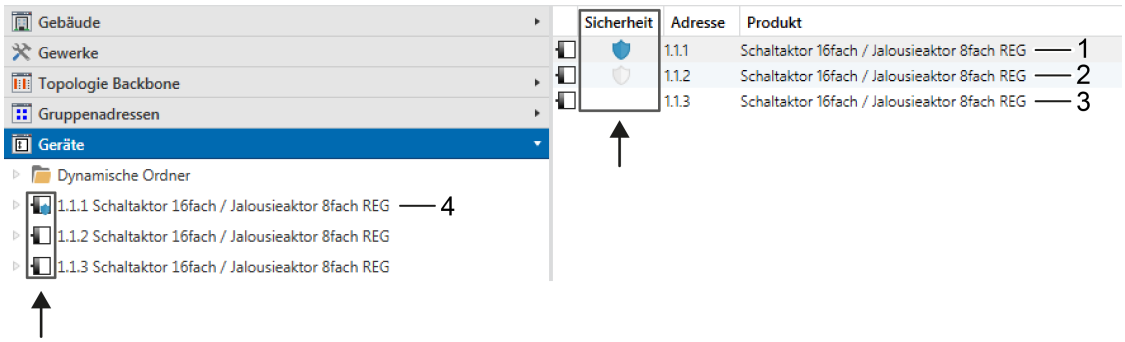


Bild 10: Beispiel einer Kennzeichnung (ETS5) von Geräten in einem ETS-Projekt

(1) KNX Data Secure fähiges Gerät mit aktivierter Gerätesicherheit
(2) KNX Data Secure fähiges Gerät mit deaktivierter Gerätesicherheit
(3) KNX Data Secure unfähiges Gerät (keine Gerätesicherheit)
(4) KNX Data Secure fähiges Gerät mit aktivierter Gerätesicherheit

Kennzeichnung KNX Data Secure kompatibler Systemgeräte

Neben den Geräten, die unmittelbar und selbstständig KNX Data Secure fähig sind, gibt es auch Systemkomponenten, die eine Kompatibilität zu Data Secure aufweisen. Nur durch die Verwendung von KNX Data Secure kompatiblen Systemgeräten (z. B. Bereichs-/Linienkoppler, Medienkoppler, IP-Router und USB-Datenschnittstellen) ist eine ordnungsgemäße Inbetriebnahme durch die ETS und eine stabile linienübergreifende Laufzeitkommunikation möglich!

Systemgeräte von Gira, die eine KNX Data Secure Kompatibilität aufweisen, sind auf dem Etikett oder Druckbild durch ein "Secure Shield"-Symbol kenntlich gemacht. Die "**X**"-Kennzeichnung wie bei KNX Data Secure fähigen Geräten fehlt. Unterstützen die verwendeten Systemkomponenten KNX Data Secure nicht, fehlt das Symbol auf dem Gerät. Folglich sind diese Komponenten nicht Data Secure kompatibel! Eine sichere Laufzeitkommunikation oder Inbetriebnahme über solche Systemgeräte hinweg ist dann nicht möglich.

Bild 11: Beispiel einer Gerätebeschriftung eines KNX Data Secure kompatiblen Geräts (z. B. KNX RF/TP Medienkoppler/Repeater)

KNX Data Secure kompatible Systemgeräte werden in der ETS nicht besonders durch Symbole gekennzeichnet.

Im Anhang dieser Dokumentation ist eine Übersicht der Systemkomponenten aufgeführt. Anhand dieser Geräteübersicht kann identifiziert werden, welche Systemkomponenten KNX Data Secure kompatibel sind.

5 Wie funktioniert KNX Data Secure in der ETS?

5.1 Projektierung

Projektpasswort

ETS-Projekte, die KNX Data Secure benutzen, benötigen immer ein Projektpasswort. Das Passwort schützt die im Projekt verwendeten Secure-Schlüssel (Toolkeys, Laufzeitschlüssel) sowie die sicherheitsrelevanten Einstellungen und Geräteeigenschaften. Zudem werden durch das Projektpasswort die Secure-Inhalte einer exportierten Projektdatei (*.knxproj) gegen Veränderung geschützt. Es ist dann auch nicht möglich, die Secure-Daten der Projektdatei zu lesen.
Das Projektpasswort wird im ETS-Dashboard in den Projektdetails durch den Benutzer vergeben und editiert. Beim Öffnen oder Importieren eines Secure-Projektes muss immer das Projektpasswort eingegeben werden.

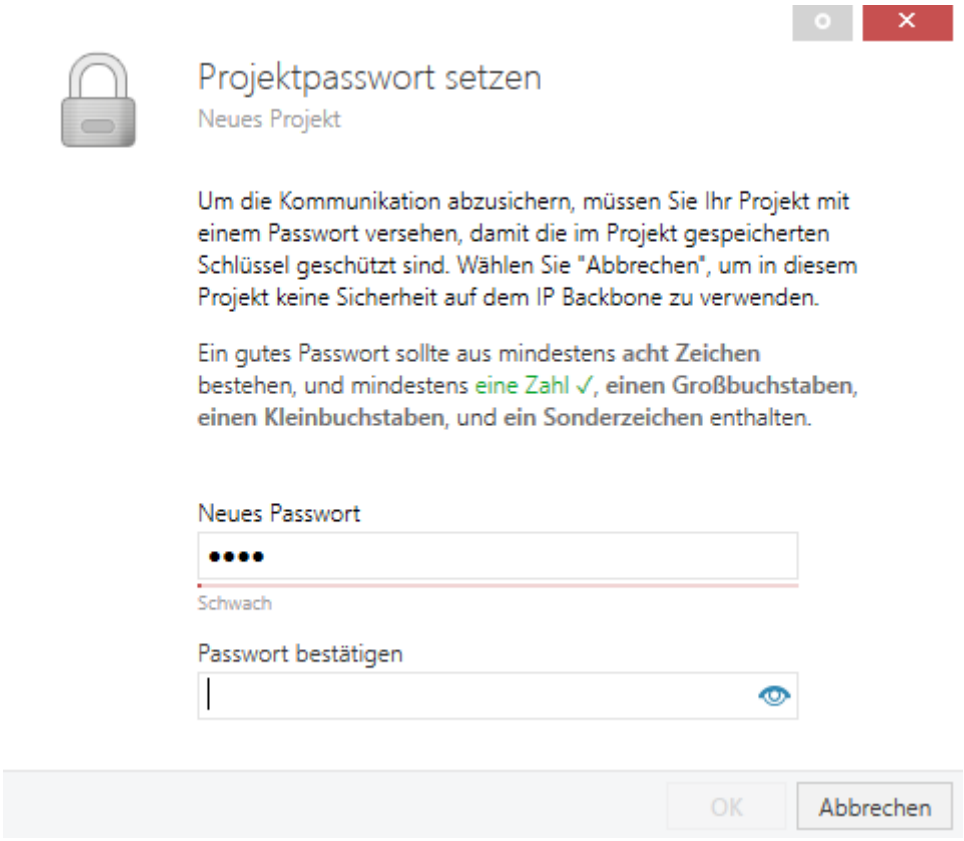


Bild 12: Setzen eines Projektpassworts am Beispiel der ETS5

Die ETS fragt beim Einfügen eines KNX Data Secure fähigen Geräts in ein Projekt immer automatisch nach einem Projektpasswort, sollte noch keines vergeben worden sein. Wenn die eingefügten Geräte sicher im Projekt verwendet werden sollen, muss ein Passwort vergeben werden! Wird der Dialog "Passwort setzen" abgebrochen, können die Geräte ausschließlich herkömmlich verwendet werden. Die ETS stellt die Gerätesicherheit dann automatisch auf "unsicher".
Beim nachträglichen Aktivieren der Gerätesicherheit eines beliebigen Geräts im Projekt, verlangt die ETS auf ein Neues das Setzen eines Passwortes.

Ist das Passwort unbekannt oder verloren gegangen, kann das ETS-Projekt nicht mehr verwendet werden! In diesem Fall sind die enthaltenen Projektierungsdaten nebst allen relevanten Inbetriebnahme- und Laufzeitschlüsseln verloren! Die in der betroffenen KNX-Anlage enthaltenen Geräte können dann nicht mehr umprogrammiert oder sonst wie durch die ETS beeinflusst werden! Die betroffene Anlage kann dann nur neu projektiert werden (betroffene Geräte müssen über einen Master-Reset zurückgesetzt und erneut in Betrieb genommen werden).

Wenn ein Projektpasswort gelöscht wird, deaktiviert die ETS nach Bestätigung die Gerätesicherheit aller Geräte im Projekt, sofern es die Einstellungen der verwendeten sicheren Gruppenadressen erlauben (siehe "Projektierung der Gruppenadressen" weiter unten).

Gerätesicherheit (sichere Inbetriebnahmekommunikation)

Geräte, die zur Laufzeit über Gruppenadressen sicher kommunizieren sollen, müssen auch durch die ETS sicher in Betrieb genommen werden. Werden Geräte herkömmlich mit der ETS programmiert, erfolgt auch die Laufzeitkommunikation immer ungesichert. Der ETS-Benutzer hat im ETS-Projekt die Möglichkeit, zu jedem KNX Data Secure fähigen Gerät die Gerätesicherheit ein- oder auszuschalten. Dies erfolgt in den Eigenschaften eines solchen Geräts durch das Sicherheitsattribut "Sichere Inbetriebnahme" (siehe Bild 13).

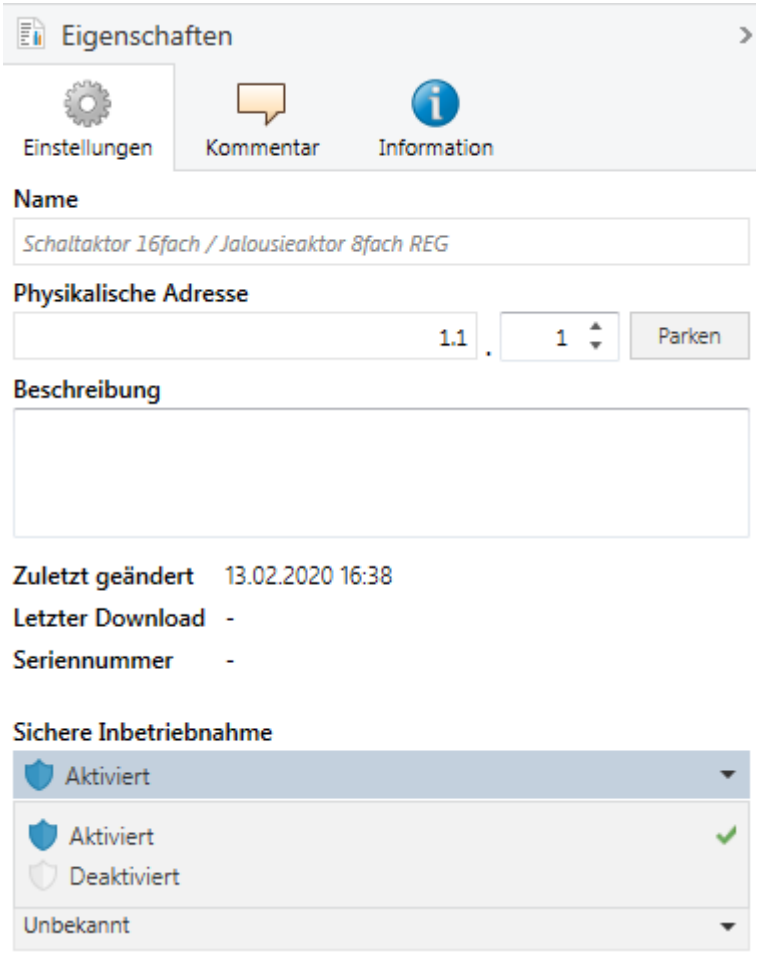


Bild 13: Editieren der Gerätesicherheit eines KNX Data Secure fähigen Geräts am Beispiel der ETS5

– Sichere Inbetriebnahme = "Aktiviert"

  Diese Einstellung ist die Standardeinstellung des Sicherheitsattributs eines Geräts, sofern dies KNX Data Secure unterstützt. Beim Einfügen eines solchen Geräts aktiviert die ETS als Voreinstellung die Gerätesicherheit. Das betroffene Gerät wird durch die ETS sicher in Betrieb genommen. Die ETS erwartet dann bei einem Programmiervorgang das passende Gerätezertifikat und vergibt im Laufe des Inbetriebnahmeprozesses einen individuellen Toolkey. Eine aktivierte sichere Inbetriebnahme ist die Voraussetzung, dass das Gerät auch mit sicheren Gruppenadressen verknüpft werden kann (siehe "Projektierung der Gruppenadressen" weiter unten).

– Sichere Inbetriebnahme = "Deaktiviert"

  Bei dieser Einstellung nimmt die ETS das entsprechende Gerät herkömmlich in Betrieb. Der Inbetriebnahmevorgang gleicht dann dem bekannten Programmiervorgang eines älteren Geräts, dass nicht KNX Data Secure fähig ist.
  Wenn ein Gerät durch die ETS herkömmlich in Betrieb genommen wurde, ist es nicht möglich, eine sichere Gruppen-Kommunikation zur Laufzeit zu realisieren. Es können keine sicheren Gruppenadressen mit den Kommunikationsobjekten dieser Geräte verknüpft werden.

Die Gerätesicherheit kann im ETS-Projekt, auch für Geräte, die bereits in Betrieb genommen wurden, jederzeit verändert werden. Dabei ist zu beachten, dass die Änderung einer Sicherheitseinstellung dazu führt, dass Geräte anschließend neu programmiert werden müssen! Beim Deaktivieren der sicheren Inbetriebnahme gehen alle Sicherheitskonfigurationen der betroffenen Geräte verloren. Die ETS prüft dann verknüpfte Gruppenadressen entsprechend ihrer Sicherheitseinstellung und zeigt dem ETS-Benutzer in einem Dialog an, welche Adressen fortan unsicher kommunizieren oder sogar vom Gerät entfernt werden.

Ein über ein ETS-Projekt sicher in Betrieb genommenes Gerät kann auch nur mit demselben Projekt erneut programmiert und bedarfsweise in der Konfiguration verändert werden. Auch das Deaktivieren der Gerätesicherheit kann nur mit demselbem Projekt erfolgen. Wenn ein anderes ETS-Projekt verwendet wird, das den Toolkey des Geräts nicht besitzt, kann das Gerät nur über den Master-Reset zurückgesetzt und im Anschluss neu in Betrieb genommen werden.

Projektierung der Gruppenadressen (sichere Laufzeitkommunikation)

KNX Data Secure hat den Zweck, zur Laufzeit einer Anlage die Kommunikation auf Gruppen-Telegrammebene vom Sender bis zum Empfänger zu sichern (Ende-zu-Ende-Sicherung). Gruppenadressen werden vom Benutzer der ETS angelegt und erhalten dabei ein besonderes Sicherheitsattribut, das nachträglich editiert werden kann (siehe Bild 14). Es ist möglich, Gruppenadressen so zu kennzeichnen, dass diese entweder immer herkömmlich, immer sicher (Secure), oder alternativ automatisch herkömmlich oder sicher (abhängig von der Verknüpfung zu Objekten) kommunizieren.
Nur die sicheren Gruppenadressen besitzen in einem ETS-Projekt eigene 128-Bit lange Laufzeitschlüssel. Der Laufzeitschlüssel kann nicht beeinflusst werden.

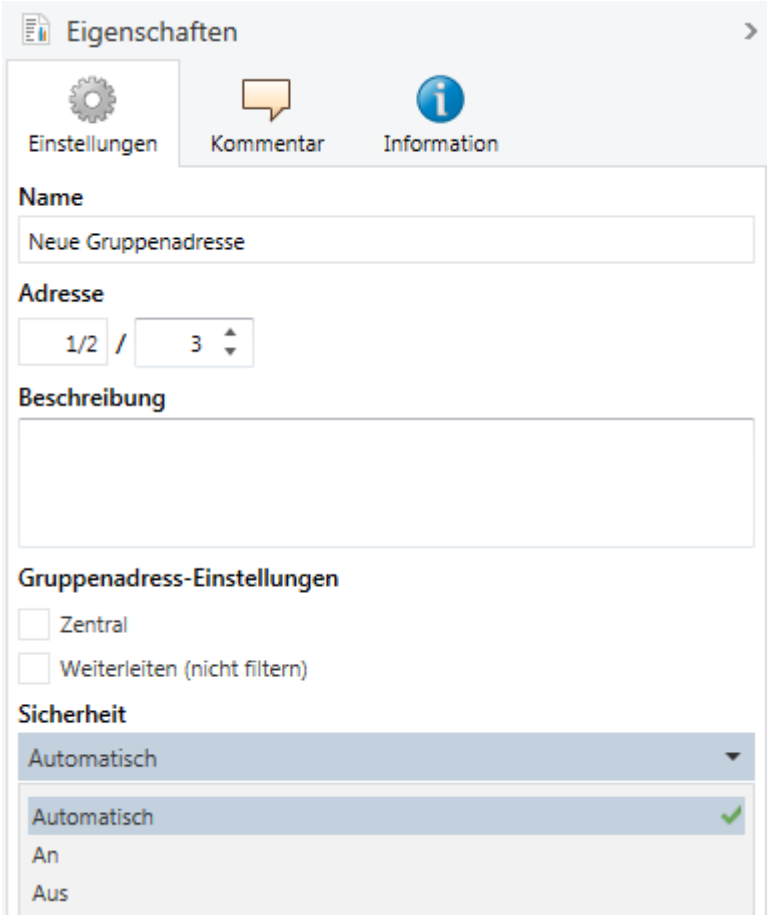


Bild 14: Editieren des Sicherheitsattributs einer Gruppenadresse am Beispiel der ETS5

Die folgende Tabelle erklärt die unterschiedlichen Sicherheitsattribute von Gruppenadressen in der ETS.

– Sicherheit = "Automatisch" /

  Diese Einstellung ist die Standardeinstellung des Sicherheitsattributs einer Gruppenadresse. In diesem Fall entscheidet die ETS immer selbstständig, ob die Gruppenadresse sicher oder herkömmlich kommuniziert. Dies ist abhängig davon, ob die Adresse nur mit Objekten verknüpft ist, die eine sichere Kommunikation unterstützen (Data Secure fähige Geräte), oder darüber hinaus auch mit Objekten von Geräten, die nicht Data Secure fähig sind. Sollte die

betroffene Gruppenadresse ausschließlich mit Objekten verknüpft sein, die sicher kommunizieren können, aktiviert die ETS immer auch eine sichere Kommunikation. Sobald die betroffene Adresse allerdings mit einem Kommunikationsobjekt verknüpft wird, das keine sichere Laufzeitkommunikation unterstützt, schaltet die ETS automatisch die sichere Kommunikation für diese Adresse ab! Die ETS weist in solch einem Fall den Benutzer der ETS auf den Umstand hin, dass die verknüpften Objekte dann fortan nur noch herkömmlich kommunizieren.

Beispiel
In einer KNX-Installation befinden sich drei Geräte (1 x Sensor und 1 x Aktor A, beide Data Secure fähig / 1 x Aktor B nicht Data Secure fähig). Ein Objekt des Sensors wird mit einem Objekt des Aktors A verknüpft. Die ETS entscheidet auf sichere Kommunikation und vergibt der betroffenen Gruppenadresse einen Laufzeitschlüssel. Nun wird dieselbe Gruppenadresse zusätzlich auch mit einem Objekt von Aktor B verknüpft. Die ETS erkennt, dass die neue Verknüpfung nicht mehr sicher kommunizieren kann, entfernt den Laufzeitschlüssel und schaltet bei der betroffenen Adresse die Sicherheit ab. Fortan kommunizieren alle betroffenen Geräte über die verknüpften Objekte nur noch herkömmlich!

– Sicherheit = "An"

  Bei dieser Einstellung erzwingt die ETS eine sichere Laufzeitkommunikation der verknüpften Kommunikationsobjekte. Folglich kann diese Adresse nur noch mit Objekten verknüpft werden, die eine sichere Kommunikation ermöglichen. Die Gruppenadresse kann daher nicht mit Geräten verknüpft werden, die nicht KNX Data Secure fähig sind!

– Sicherheit = "Aus"

  Bei dieser Einstellung erzwingt die ETS eine herkömmliche Laufzeitkommunikation der verknüpften Kommunikationsobjekte. Wenn eine solche Gruppenadresse mit Objekten verknüpft wird, erfolgt die Gruppen-Kommunikation stets herkömmlich (auch dann, wenn das Objekt grundsätzlich sicher kommunizieren könnte).

KNX Data Secure fähige Geräte, die durch die ETS sicher in Betrieb genommen wurden und auch über Kommunikationsobjekte zur Laufzeit gesicherte Daten mit anderen Data Secure fähigen Geräten austauschen, können grundsätzlich über ausgewählte Gruppenadressen auch herkömmlich kommunizieren. Es ist ein Mischbetrieb von sicherer und herkömmlicher Kommunikation an einem Sensor oder Aktor über unterschiedliche Kommunikationsobjekte möglich. Allerdings ist eine gesicherte und ungesicherte Kommunikation über ein und dasselbe Kommunikationsobjekt nicht möglich!

Hersteller können in den Applikationsprogrammen von KNX Data Secure fähigen Geräten auch an den Kommunikationsobjekten Sicherheitsattribute definieren. So ist es beispielsweise möglich, dass ein Objekt grundsätzlich nur sicher kommunizieren darf. Der Hersteller kann also eine sichere Gruppenkommunikation zur Laufzeit über alle oder einzelne Objekte seines Geräts erzwingen. In solchen Fällen ist es nicht mehr möglich, herkömmliche Gruppen-

adressen mit den Kommunikationsobjekten zu verknüpfen. Im Normalfall erzwingen die Kommunikationsobjekte der Applikationsprogramme keine sichere Kommunikation, so dass den ETS-Benutzern über die Sicherheitsattribute der Gruppenadressen die Möglichkeit bleibt, selbst zu entscheiden, ob eine Adresse sicher oder herkömmlich kommuniziert.

Sicherheitsattribute von Gruppenadressen können im ETS-Projekt jederzeit verändert werden. Dabei ist zu beachten, dass die Änderung einer Sicherheitseinstellung dazu führt, dass Geräte anschließend neu programmiert werden müssen! Es sind dann alle Geräte betroffen, die mit der Gruppenadresse verknüpft sind, deren Einstellung verändert wurde (auf Programmierflags der Geräte achten). Dies ist besonders bei Zentraladressen in einem ETS-Projekt zu berücksichtigen, die auf viele Geräte verknüpft wurden. Es wird empfohlen, in der ETS einen dynamischen Ordner zu verwenden und diesen so zu konfigurieren, dass er stets alle noch zu programmierenden Geräte enthält.

5.2 Inbetriebnahme

Verwendung von Systemkomponenten

KNX Data Secure Geräte verwenden für die Übertragung der authentifizierten und verschlüsselten Daten, im Wesentlichen aufgrund der enthaltenen 128-Bit langen Schlüssel, ein längeres KNX-Telegrammformat (Extended Frames). Dies hat jedoch keine Auswirkungen auf die Reaktionsgeschwindigkeit der Geräte, die problemlos neben herkömmlichen Geräten in derselben Installation und auf gleichen Medien eingesetzt werden können. Das bedeutet, dass KNX Data Secure als zusätzliche Maßnahme zur Realisierung einer zuverlässigen Sicherheit für ausgewählte Geräte oder Funktionen in neuen oder bestehenden Anlagen verwendet werden kann.

Aufgrund des längeren Telegrammformats müssen auch die verwendeten Systemkomponenten (Bereichs-/Linienkoppler, Medienkoppler) und die lokalen Datenschnittstellen der ETS (USB, IP-Tunneling, IP-Routing) Extended Frames unterstützen. Ist diese Unterstützung nicht gegeben, kann die ETS keine sichere Inbetriebnahme durchführen und zeigt einen Fehler beim Programmiervorgang an.
Der ETS-Benutzer muss also sicherstellen, dass die lokale Datenschnittstelle der ETS und alle Systemkomponenten, die sich zwischen ETS und dem zu programmierenden Gerät befinden, Extended Frames unterstützen. Dieser Sachverhalt ist besonders dann zu beachten, wenn bestehende KNX-Installationen um KNX Data Secure erweitert werden sollen.

Im Anhang dieser Dokumentation ist eine Übersicht der Gira Systemkomponenten aufgeführt. Anhand dieser Geräteübersicht kann identifiziert werden, welche Systemkomponenten KNX Data Secure kompatibel sind.

Expertenwissen
Bei Verwendung von RF/TP Medienkopplern ist nicht alleine das Telegrammformat bezüglich einer KNX Data Secure Kompatibilität entscheidend. Damit ein Medienkoppler ein KNX Data Secure Telegramm zur Laufzeit (Routing) ordnungsgemäß verarbeiten und weiterleiten kann, muss eine Systemeigenschaft im Gerät vorhanden sein, die das Weiterleiten von gesicherten Telegrammen ermöglicht. Die Geräteübersicht im Anhang dieser Dokumentation enthält eine Liste der verfügbaren Medienkoppler und erklärt, welche Geräteversion KNX Data Secure kompatibel ist.

Einlesen von Gerätezertifikaten

Damit die ETS ein Gerät sicher in Betrieb nehmen kann, benötigt sie das passende Gerätezertifikat. Das Gerätezertifikat ist eine Zeichenkette, die den FSDK und die Seriennummer eines KNX Data Secure fähigen Geräts enthält. Das Gerätezertifikat muss der ETS vor einem Programmiervorgang mitgeteilt werden, um ein Gerät sicher in Betrieb nehmen zu können. Die ETS leitet aus dem Zertifikat den zu einer Seriennummer passenden FDSK ab und verwendet diesen dann zur ersten Inbetriebnahmekommunikation.

Die Gerätezertifikate sind jeweils auf ablösbaren Etiketten abgedruckt, die sich an den Geräten befinden. Diese Etiketten sind bereits bei der Montage von den Geräten zu entfernen und sicher aufzubewahren! Andernfalls ist nicht auszuschließen, dass Unbefugte in den Besitz der FDSK gelangen und Manipulationen an vorhandenen Geräten einer sicheren KNX-Installation durchführen.

Gerätezertifikate können der ETS an unterschiedlichen Stellen und in verschiedenen Situationen eingelesen werden.

– Projekt-Dashboard

  Im ETS-Dashboard kann zu jedem Projekt unter dem Reiter "Sicherheit" der Projekt-Schlüsselbund in Form einer Übersicht aller eingelesenen Gerätezertifikate eingesehen werden. Zunächst ist diese Liste bei einem neuen Projekt leer. Die Gerätezertifikate können durch Klicken des Buttons ✚ schrittweise (einzeln) hinzugefügt werden (siehe Bild 15). Die ETS öffnet dann den Dialog zum Einlesen des Gerätezertifikats per Tastatur oder Kamera (siehe Bild 16).

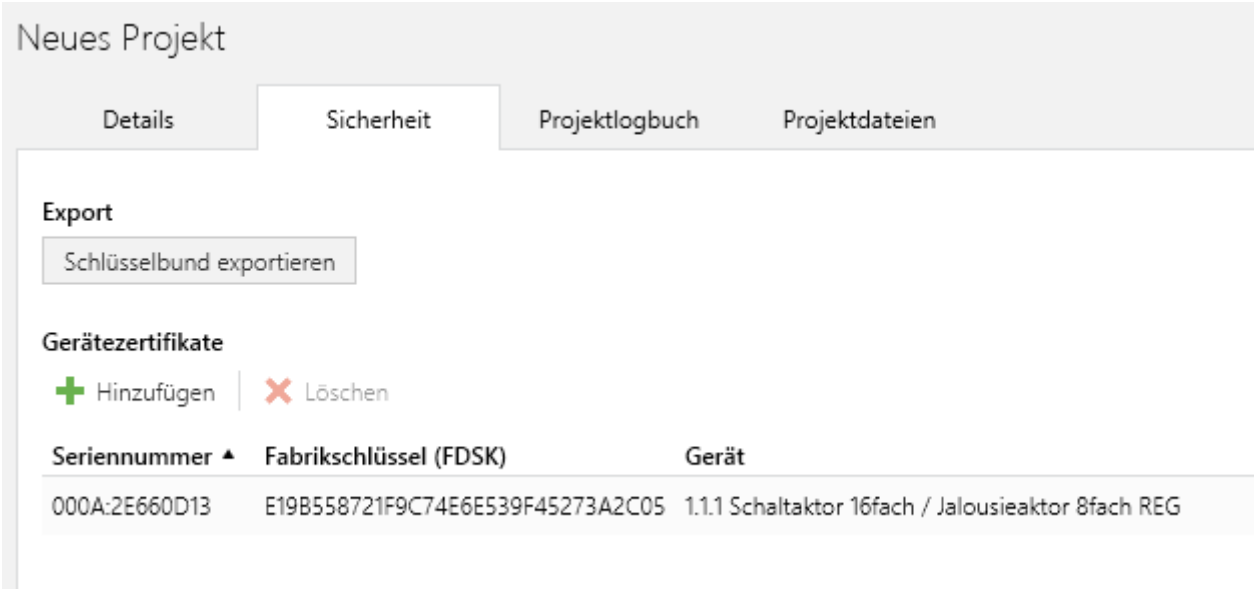


Bild 15: Beispiel einer Übersicht der Gerätezertifikate eines Projekts im ETS-Dashboard (ETS5)

Bild 16: Beispiel des Dialogs zum Einlesen eines Gerätezertifikats (ETS5)

Der Projekt-Schlüsselbund zeigt alle in das ETS-Projekt eingelesenen Gerätezertifikate (Seriennummer + FDSK) an. Sofern ein Zertifikat bereits erfolgreich für eine Inbetriebnahme verwendet wurde (bekannte Seriennummer), ist zusätzlich auch der Gerätename und die physikalische Adresse dieses Gerät gelistet. Fehlen Gerätename und physikalische Adresse, wurde das Zertifikat lediglich erfolgreich eingelesen und noch nicht durch die ETS benutzt.

Die ETS erkennt, ob ein eingelesenes Zertifikat bereits im Projekt-Schlüsselbund vorhanden ist. In diesem Fall bleibt das vorhandene Zertifikat unverändert erhalten.

Es wird empfohlen, zum Scannen eines QR-Codes eine hochauflösende Kamera zu verwenden.

– Im Projekt bei den Geräteeinstellungen

  Als Alternative zum ETS-Dashboard ist es möglich, vorhandene Gerätezertifikate auch direkt in einem geöffneten Projekt hinzuzufügen. Hierzu ist ein Gerät auszuwählen und in den Eigenschaften unter "**Einstellungen**" der Button "**Gerätezertifikat hinzufügen**" auszuwählen. Auch hier öffnet die ETS dann den Dialog zum Einlesen des Gerätezertifikats per Tastatur oder Kamera.

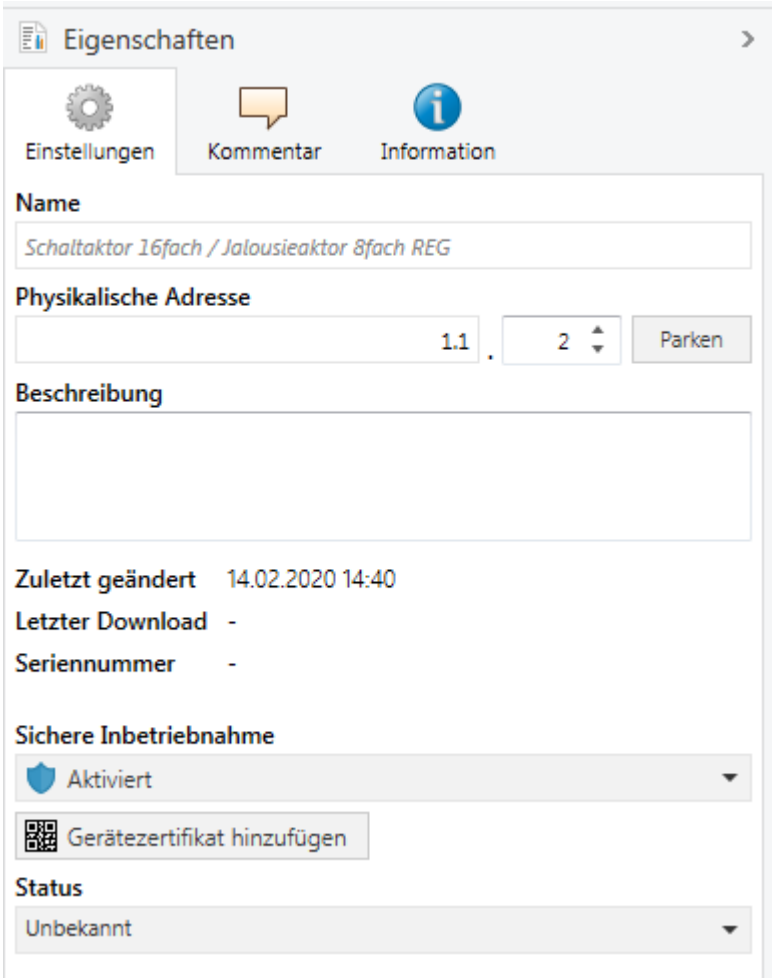


Bild 17: Beispiel einer Einstellung zum Einlesen eines Gerätezertifikats direkt im ETS-Projekt (ETS5)

Ein bei den Geräteeinstellungen hinzugefügtes Gerätezertifikat wird unmittelbar auf das ausgewählte Gerät im Projekt verknüpft. Die im Zertifikat enthaltene Seriennummer wird sichtbar in die Geräteeinstellungen übernommen. Die ETS übernimmt zudem das Zertifikat auch in den Projekt-Schlüsselbund (ETS-Dashboard).

Wenn das eingelesene Gerätezertifikat bereits bei einem anderen Gerät im selben Projekt verwendet wird, zeigt die ETS eine Hinweismeldung im Einlesedialog an. Bei positiver Bestätigung verknüpft die ETS das Zertifikat mit dem Gerät, für das das Zertifikat zuletzt eingelesen wurde. Seriennummer und Programmier-Flags des zuvor verknüpften Geräts werden dann gelöscht.

– Beim Einfügen eines KNX Data Secure fähigen Geräts

Schon beim Einfügen eines neuen KNX Data Secure fähigen Geräts in ein Projekt (aus dem Produktkatalog oder beim Kopieren eines Geräts) fragt die ETS den Benutzer nach dem Gerätezertifikat (siehe Bild 18), sofern die Gerätesicherheit dieses Geräts aktiviert ist. Beim Einfügen einzelner Geräte ist diese Methode recht hilfreich und trägt dazu bei, möglichst frühzeitig alle für die anstehende Inbetriebnahme relevanten Gerätezertifikate im Projekt zu sammeln.

Bild 18: Beispiel des Dialogs zum Einlesen eines Gerätezertifikats beim Einfügen eines Geräts (ETS5)

In manchen Situationen, besonders beim Aufsetzen eines neuen Projekts oder dann, wenn die Zertifikate noch nicht vorliegen, kann die Abfrage nach den Gerätezertifikaten beim Einfügen von Geräten störend sein. Aus diesem Grund bietet die ETS die Möglichkeit, den Einlesevorgang des Zertifikats abzubrechen und die Information erst später einzulesen (Button "Später"). Alternativ kann der Dialog beim Hinzufügen von Geräten für das gesamte Projekt abgeschaltet werden. Hierzu muss das Kontrollfeld "Beim Hinzufügen von Geräten nicht fragen" im Dialog angeklickt, oder in den Projekteinstellungen im

ETS-Dashboard die Option "Beim Hinzufügen sicherer Geräten nach Gerätezertifikat fragen" deaktiviert werden (ETS5: "Einstellungen -> Ansicht -> Sicherheit").

Ein beim Einfügen hinzugefügtes Gerätezertifikat wird unmittelbar auf das neu eingefügte Gerät im Projekt verknüpft. Die im Zertifikat enthaltene Seriennummer wird sichtbar in die Geräteeinstellungen übernommen. Die ETS übernimmt zudem das Zertifikat auch in den Projekt-Schlüsselbund (ETS-Dashboard).

Wenn das eingelesene Gerätezertifikat bereits bei einem anderen Gerät im selben Projekt verwendet wird, zeigt die ETS eine Hinweismeldung im Einlesedialog an. Bei positiver Bestätigung verknüpft die ETS das Zertifikat mit dem Gerät, für das das Zertifikat zuletzt eingelesen wurde. Seriennummer und Programmier-Flags des zuvor verknüpften Geräts werden dann gelöscht.

– Unmittelbar vor einem Programmiervorgang

  Spätestens dann, wenn die ETS ein KNX Data Secure fähiges Gerät sicher in Betrieb nehmen soll (Programmieren der physikalischen Adresse), ist das Gerätezertifikat und die darin enthaltene Seriennummer und der FDSK relevant. Bei aktivierter sicherer Inbetriebnahme verlangt die ETS daher beim Programmieren auf jeden Fall nach dem Gerätezertifikat, sofern ihr zu der aus dem Gerät ausgelesenen Seriennummer noch kein Zertifikat im Projekt-Schlüsselbund vorliegt. In solch einem Fall öffnet die ETS den Dialog zum Einlesen des Gerätezertifikats per Tastatur oder Kamera (siehe Bild 19).

  Sobald per Tastatur oder Kamera ein gültiges Gerätezertifikat eingegeben wird, startet die ETS im Anschluss sofort den Programmiervorgang. Liegt das Gerätezertifikat nicht vor, kann der Button "Klartext" angeklickt werden. In diesem Fall deaktiviert die ETS für das betroffene Gerät die sichere Inbetriebnahme und nimmt das Gerät herkömmlich in Betrieb. Die ETS prüft dann verknüpfte Gruppenadressen entsprechend ihrer Sicherheitseinstellung und zeigt dem ETS-Benutzer in einem Dialog an, welche Adressen fortan herkömmlich kommunizieren oder sogar vom Gerät entfernt werden.

  Alternativ kann der Button "Download überspringen" angeklickt werden. Dabei bricht die ETS den Programmiervorgang des im Dialog angezeigten Geräts ab.

Bild 19: Beispiel des Dialogs zum Einlesen eines Gerätezertifikats beim Programmieren eines Geräts (ETS5)

Ein beim Programmieren hinzugefügtes Gerätezertifikat wird unmittelbar auf das Gerät im Projekt verknüpft und beim Programmieren verwendet. Die im Zertifikat enthaltene Seriennummer wird sichtbar in die Geräteeinstellungen übernommen. Die ETS übernimmt zudem das Zertifikat auch in den Projekt-Schlüsselbund (ETS-Dashboard).

Sollte das eingelesene Gerätezertifikat nicht für das zu programmierende Gerät geeignet sein (Seriennummer des Geräts nicht gleich der Seriennummer des eingelesenen Zertifikats), akzeptiert die ETS das Gerätezertifikat nicht und führt den Programmiervorgang nicht aus.

5.3 Kompatibilität und Versionen

Generell wird KNX Data Secure in der ETS5 ab Version 5.5.0 unterstützt. Es wird empfohlen, bei der Projektierung und Inbetriebnahme von KNX Data Secure fähigen Geräten die ETS5 mindestens ab Version 5.7.4 oder die ETS6 einzusetzen! Der Einsatz von älteren ETS-Versionen kann dazu führen, dass Fehler bei der Projektierung und Probleme bei der Inbetriebnahme (z. B. beim Gerätetausch) und bei der Diagnose von Gruppenadressen und Geräten auftreten.

Die ETS2, ETS3, ETS4 und die ETS5 bis einschließlich Version 5.0.8 sind grundsätzlich nicht dazu geeignet, KNX Data Secure zu nutzen.

6 Was sollte noch beachtet werden?

Grundsätzliche Empfehlungen zum Schutz einer KNX-Anlage

Wer seine KNX-Installation effektiv schützen möchte, sollte mit den Schutzmaßnahmen bereits bei der Installation beginnen. KNX Data Secure hilft, die Inbetriebnahme und Laufzeitkommunikation manipulationssicher zu machen. Die Methode schützt jedoch nicht vor unerlaubter Beeinflussung oder Manipulation der KNX-Leitung und der eingesetzten Hardware. An dieser Stelle müssen andere Schutzmechanismen zur Anwendung kommen.

Allgemein gilt, dass Geräte und Leitungen fest installiert werden sollten, um zu verhindern, dass diese leicht entfernt oder beschädigt werden und hierdurch unbefugte Personen Zugang zur KNX-Anlage erhalten. Die folgenden Schutzmaßnahmen werden in Bezug auf die Montage grundsätzlich empfohlen...

- Haupt- und Unterverteilungen mit KNX-Geräten sollten verschlossen sein und sich in Räumen befinden, zu denen nur befugte Personen Zutritt haben.
- Montagehinweise des Herstellers beachten, besonders für Diebstahlschutzeinrichtungen. Unterputzgeräte sollten in geeignete UP- oder Hohlwanddosen montiert und fest mit der Einbauumgebung verbunden sein (z. B. durch die vom Hersteller vorgesehene Verschraubung).
- Im Außenbereich sollten Geräte (z. B. Wetterzentrale, Windsensor, Bewegungsmelder) in ausreichender Höhe installiert werden, damit diese vor Fremdzugriff geschützt sind.
- In öffentlichen Bereichen (z. B. Einkaufszentren, Schulen) sollte die Verwendung von konventionellen Bediengeräten anstelle von KNX-Geräten bevorzugt werden. Die konventionellen Geräte können dann mit den KNX-Komponenten (z. B. Tasterschnittstellen, Binäreingänge), die idealer Weise in einer zutrittskontrollierten Einbauumgebung montiert sind, elektrisch verbunden werden. Hierdurch wird ein Zugang zur KNX-Installation (Busleitung) deutlich erschwert.
- KNX-Leitungen oder Geräte im Außenbereich stellen immer ein erhöhtes Risiko dar. Lässt sich eine Außenanwendung nicht vermeiden (z. B. zur Vernetzung weiterer Liegenschaften oder Gebäudeteilen), sollte der Zugang zur KNX-Leitung besonders erschwert werden (z. B. durch tief im Erdreich verlegte KNX-Kabel oder Schutzrohre). Grundsätzlich sollten KNX-Installationen in ungeschützten Bereichen (Außenbereich, Tiefgarage) als eigene TP-Linie oder RF-Domäne ausgeführt werden.
- Im Falle einer IP-Kommunikation sollte ein getrenntes LAN oder WLAN Netzwerk mit eigener Hardware (Router, Switches) verwendet werden. Es sind unbedingt die üblichen Sicherheitsmechanismen für IP-Netzwerke anzuwenden (MAC-Filter, Verschlüsselung von Drahtlosnetzwerken mit Verwendung starker Passwörter). Alternativ ist auch die Verwendung eines virtuellen lokalen Netzwerks (VLAN) möglich.

Neben den Sicherheitsvorkehrungen, die schon bei der Montage zu berücksichtigen sind, müssen auch Regeln bei der Konfiguration von Kopplern oder IP-Routern eingehalten werden. Dazu gehören...

- Vorhandene Bereichs/Linien- oder Medienkoppler so konfigurieren, dass Filtertabellen aktiv sind.
- In Kopplern, die über ihre untergeordnete Linie öffentliche oder außenliegende Bereiche anbinden, nach der Inbetriebnahme einer Anlage möglichst den Programmierschutz aktivieren (Abweisen von physikalisch adressierten Telegrammen).
- Zudem die Punkt-zu-Punkt- und wenn möglich auch die Broadcast-Kommunikation über Koppler und Router hinweg nach der Inbetriebnahme blockieren. Auf dieser Weise wird das unerlaubte Verändern der Gerätekonfigurationen auf eine einzige Linie begrenzt.
- Bei Internet-Zugriff auf KNX-Installationen: VPN Verbindungen (keine öffentlichen Portweiterleitungen etc.) oder eigens für einen geschützten Internet-Zugriff vorgesehene herstellerspezifische Lösungen verwenden.

7 Anhang

7.1 Übersicht Systemkomponenten

Produktbezeichnung	Artikelnummer	Release	APDU [Byte]	Data Secure kompatibel
Bereichs-/Linienkoppler REG	1023 00	I00	40	nein
Bereichs-/Linienkoppler REG	1023 00	I01	55	ja
Bereichs-/Linienkoppler REG	1023 00	I02	55	ja
Bereichs-/Linienkoppler REG	1023 00	I03	55	ja

Tab. 1: Bereichs-/Linienkoppler

Ältere Koppler (582 00, 611 00, 1096 00) sind grundsätzlich nicht KNX Data Secure kompatibel.

Produktbezeichnung	Artikelnummer	Release	APDU [Byte]	Data Secure kompatibel
RF/TP Medienkoppler/Repeater	5110 00	I00	233	nein
RF/TP Medienkoppler/Repeater	5110 00	I01	233	ja

Tab. 2: Medienkoppler

Produktbezeichnung	Artikelnummer	Release	APDU [Byte]	Data Secure kompatibel
USB Datenschnittstelle REG	1080 00	alle	15	nein
USB Datenschnittstelle UP	1070 00	alle	15	nein
USB-Datenschnittstelle	2014 00	alle	233	ja
USB-Datenschnittstelleneinsatz	2024 00	alle	233	ja
RF USB Datenschnittstelle	5120 00	alle	240	ja

Tab. 3: USB-Datenschnittstellen

Ältere RS-232-Datenschnittstellen (0504 xx, 0558 xx, 1153 00) sind grundsätzlich nicht ETS5 und folglich nicht KNX Data Secure kompatibel.

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