TAPKO
TECHNOLOGIES GMBH

KNX®

Warum KNX SECURE?

Vor Jahren, machte ein Hack, also ein krimineller Zugriff auf das KNX System eines Hotels, auf sich aufmerksam. Dies war der Beginn weitreichender Diskussionen in der KNX Community. Hinzu kam der veränderte Bedarf durch den Einsatz der Medien IP und RF in den letzten Jahren.

Welche Szenarien sind in einem ungeschützten KNX-System denkbar?

- Kopieren von gesendeten Telegrammen
  Beispiel: Garagentor auf
- Manipulieren von Telegrammen
- Manipulieren von Installationen / Konfigurationen
  (Umprogrammieren von Funktionen)
- Mitlesen von Telegramminhalten
- Blockieren von Funktionen

Welche Schutzmaßnahmen gibt es?

Bei KNX Secure unterscheiden wir zwischen KNX Data Secure, das alle KNX-Geräte betrifft, und KNX IP Secure, das nur IP-Geräte betrifft. Zusätzlich sind die Grundsätze der „Security of Installation“ zu berücksichtigen.

Security of Installation:
Berücksichtigung von Sicherheitskriterien bei der Planung und Installation einer KNX-Installation, siehe auch Checkliste KNX-Sicherheit der KNX-Organisation, wie schon bei der „klassischen“ KNX Installation z.B. Zugänglichkeit der Leitungen.

KNX Data Secure:
Mit KNX Date Secure erfolgt eine signierte und verschlüsselte Kommunikation im KNX-Netzwerk und stellt damit eine gesicherte Übertragung von Telegrammen sicher. Grundlage ist eine End zu End Verschlüsselung, d.h. nur die Endgeräte verstehen die Nachrichten, die Linienkoppler leiten die Telegramme transparent weiter. Dadurch ist die Kommunikation im KNX-Netzwerk weder interpretierbar noch manipulierbar.

Voraussetzungen: KNX Data Secure fähige Geräte bzw. alle Systemkomponenten, die zwischen den SECURE-Teilnehmern liegen, müssen SECURE kompatibel sein. Secure kompatibel heißt: die Geräte müssen lange Telegramme (Long Frames) verarbeiten können.

KNX IP Secure:
Alle Geräte mit KNX IP Security unterstützen auch Data Security. KNX IP Secure wird zur sicheren Übertragung von KNX Telegrammen über KNX IP Linien- oder Bereichskoppler sowie KNX IP Interfaces verwendet.

Diese Eigenschaften werden durch die KNX SECURE Mechanismen sichergestellt:

Freshness
Bei IP Security wird die Aktualität der Daten mittels Zeitstempel sichergestellt, Frames mit veralteten Zeitstempeln werden (beim Empfangen) verworfen. Damit wird verhindert, dass Telegramme aufgezeichnet und später aufgerufen werden können.

Bei Data Security wird Freshness durch die Sequenznummer sichergestellt.

Vertraulichkeit
Durch Verschlüsselung wird das Interpretieren von ausgelesenen Telegrammen verhindert.

Datenintegrität
Datenintegrität bedeutet, zu verhindern dass ein Angreifer durch einspeisen von manipulierten Meldungen Kontrolle über die Anlage gewinnt.

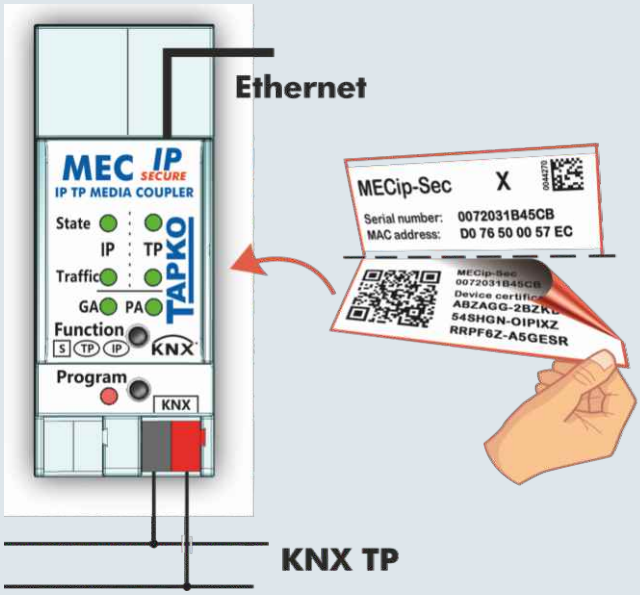

MY
KEY IS
MY
CASTLE

KNX SECURE: Schlüssel und Methoden

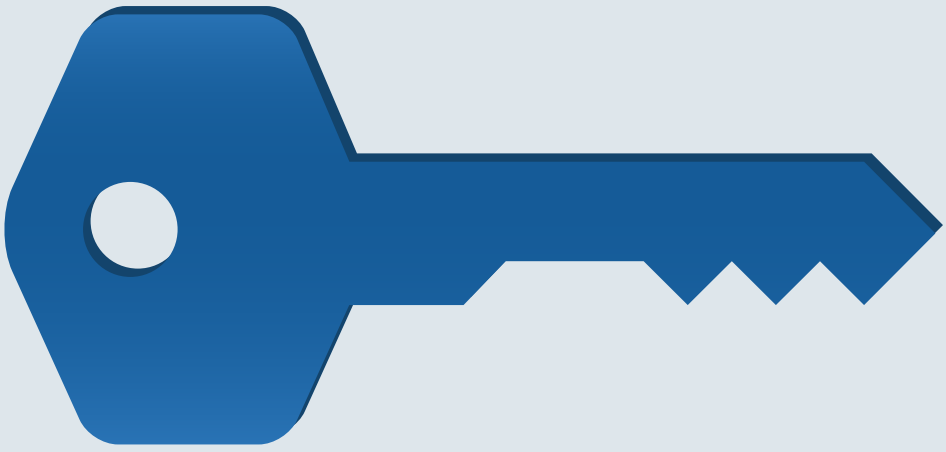
Grundsätzliches zur Verschlüsselung
KNX Secure benötigt keine revolutionären Ideen, sondern nutzt den bewährten Verschlüsselungsmechanismus AES gemäß ISO/IEC 18033-3. AES Advanced Encryption Standard 128 mit CTR-Betriebsmodus und AES-CBC-MAC-Signatur (CCM), mit einer Blockgröße von 128 Bit. Alle Schlüssel werden von der ETS vergeben.

Gerätezertifikat, Geräteetikett
Das Gerätezertifikat besteht aus FDSK und Seriennummer und ist 36 Zeichen lang. Die ETS benötigt ein Gerätezertifikat für die Erstkonfiguration mit KNX Secure, sowohl Data als auch IP Secure. Gerätezertifikate werden im ETS-Projekt gespeichert.

Abtrennbare Etiketten mit Gerätezertifikat (Text + QR-Code) befinden sich auf dem Gerät selbst. Etiketten mit Gerätezertifikat sind vor der Gerätemontage zu entfernen. Gerätezertifikate (Etiketten und Berichte) müssen sicher aufbewahrt werden.



Factory Default Setup Key (Fabrikschlüssel)
FDSK steht für „Factory Default Setup Key“. Es handelt sich um einen „ab Werk“-Wert, das heißt, er wird jedem Gerät während der Produktion vom Hersteller zugeordnet. Die ETS benötigt FDSK für die erste Konfiguration oder nach jedem Master-Reset. Es ist Bestandteil des Gerätezertifikats und kann von der ETS direkt aus dem QR-Code ausgelesen werden. Der FDSK wird nach der ersten Konfiguration inaktiv und die ETS verwendet danach den Tool Key. Der FDSK kann nicht geändert werden!

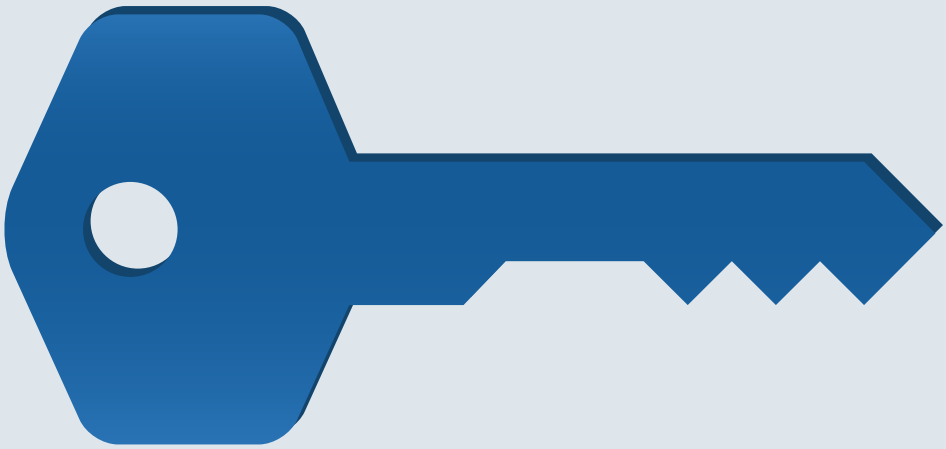


Geräteschlüssel (Tool Key)
Der Geräteschlüssel ermöglicht den Zugriff auf das Gerät während der Konfiguration und wird bei der Punkt-zu-Punkt-Kommunikation verwendet, er ist ebenso wie der FDSK 128 Bit lang. Geräteschlüssel wird in der ETS generiert und bei der Erstinbetriebnahme zugewiesen. Der Geräteschlüssel wird im ETS-Projekt gespeichert. Geht das ETS-Projekt zusammen mit dem Tool Key verloren, ist nur ein Factory-Reset möglich. In diesem Fall wird FDSK wieder aktiv, da ein Werksreset den Gerätschlüssel löscht und FDSK übernimmt.

Laufzeitschlüssel (Runtime Key oder Group Key)
Der Gruppenschlüssel wird während der Laufzeitkommunikation zwischen Gruppenadressen verwendet. In einem Projekt gibt es für jede Gruppenadresse einen individuellen Schlüssel. Dieser Schlüssel ist ebenfalls 128 Bit lang und wird von der ETS vergeben sowie gespeichert und ist im Projektbericht - Projektsicherheit zu finden. Nach dem Zurücksetzen auf die Werkseinstellungen werden auch diese Schlüssel gelöscht.

Seriennummer
Die Seriennummer als Teil des Gerätezertifikats ist eine 6 Byte lange eindeutige Nummer des Herstellers zur eindeutigen Identifizierung jedes KNX Gerätes.

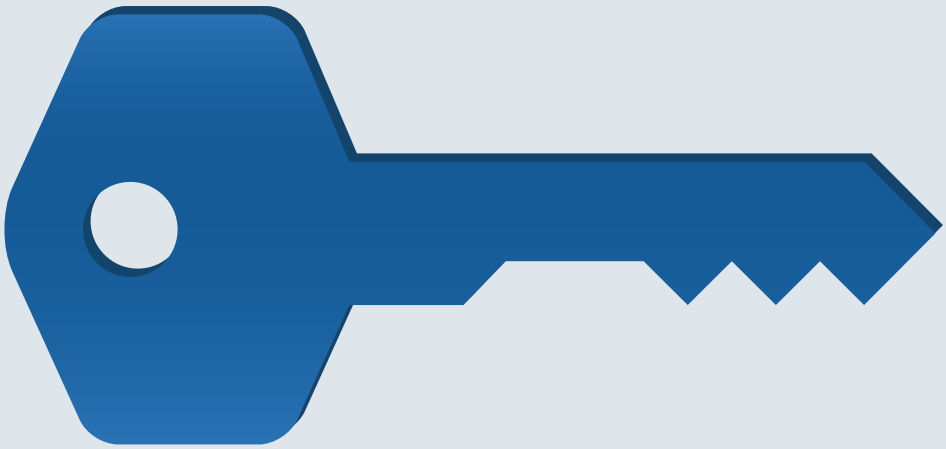
Projektpasswort
Für das ETS-Projekt, das KNX Secure verwendet, ist ein Passwort erforderlich. Dieses Passwort dient zum Schutz von Geräte- und Gruppenschlüsseln (sowie Backbone-Schlüssel bei KNX IP Secure) im Projekt und sicherheitsrelevanten Einstellungen von Geräten.



Sichere Inbetriebnahme
Wenn KNX Data Secure Geräte für die sichere Laufzeitkommunikation vorgesehen sind, müssen diese auch durch die ETS sicher in Betrieb genommen werden. Bei Geräten, die unsecure in Betrieb genommen werden, ist die Runtime-Kommunikation nur einfach möglich. Für jedes einzelne Gerät im ETS-Projekt (das KNX Data Secure unterstützt) kann die sichere Inbetriebnahme in seinen Eigenschaften ein- oder ausgeschaltet werden.

Sequenznummer
Die Sequenznummer ist eine 6 Byte lange Zahl. Bei Data security fügt jeder Sender eine Sequenznummer hinzu, die jeder Empfänger pro Kommunikationspartner überprüft. Wenn das Gerät Telegramme vom KNX-Bus empfängt, akzeptiert es nur Nachrichten mit höheren Sequenznummern. Zusammenfassend lässt sich sagen, dass die Sequenznummer die Aktualität der Daten gewährleistet und verhindert, dass Daten aufgezeichnet und wiedergegeben werden.

Backbone Key (bei IP Security)
Der Backbone-Schlüssel wird für das sichere IP-Routing verwendet. Alle IP-Geräte in einem Projekt haben den gleichen Backbone-Schlüssel. Nach dem Zurücksetzen auf die Werkseinstellungen wird auch der Backbone-Schlüssel gelöscht.



Gut zu wissen

In diesen Bereichen ist der Einsatz von KNX Secure notwendig oder empfehlenswert

- Wenn in öffentlichen Bereichen KNX-Geräte leicht erreichbar sind.
- Um eine Trennung bei unterschiedlichen Verantwortungsbereichen durchzuführen, z.B. Bürogebäude mit mehreren Nutzern, Hotels
- Bei Zugriffen über IP-Netzwerke / Fernwartung

Einsatz von KNX Secure in vorhandenen Installationen

- Um eine bestehende Non-Secure KNX Installation mit IP-Linien sicherer zu machen, sollten KNXnet/IP Router durch KNXnet/IP Secure Router ausgetauscht werden. Die Übertragung zwischen KNXnet/IP-Geräten kann dann mit KNX IP Secure erfolgen.
- Secure Geräte können jederzeit im Unsecure-Modus in einer Non-Secure KNX Installation als Ersatz für Unsecure Geräte eingesetzt werden. Damit können Teile einer bestehenden Installation mit neuen KNX Data Secure-Geräten aufgerüstet werden.
- Es können auch Secure Geräte / Kommunikationen in einer Non-Secure Installation verwendet werden. Bei Secure Geräten können die einzelnen Gruppenobjekte Secure bzw. Unsecure konfiguriert / verwendet werden. Für ein einzelnes Objekt gilt: Entweder Secure oder Unsecure.

TAPKO KNX SECURE

UIMip-Sec - KNX IP Schnittstelle Secure mit 4 Tunneling-Kanälen

UIMip-Sec verbindet den PC (z.B. ETS) mit dem KNX Bus zur Inbetriebnahme und Überwachung über IP. Die sichere Version schützt das Tunneling-Protokoll durch die Verwendung von KNX IP Secure.

MECtp-Sec - KNX Linien-/ Bereichskoppler Secure

MECtp-Sec verbindet KNX-Segmente (Linien, Bereiche). Es bietet verschiedene Routing-Filter für Gruppen- und Einzeltelegramme. Die sichere Version MECtp-Sec unterstützt die verschlüsselte Konfiguration mit KNX Data Secure .

MECip-Sec - KNX IP Router Secure mit Routing- und Tunneling-Schnittstelle

Sie verbindet eine KNX TP Linie mit einem KNXnet/IP Backbone. Über IP Tunnelling kann die ETS mit dem KNX Bus kommunizieren. Die Secure Version unterstützt die Verschlüsselung mit KNX Data Secure und KNX IP Secure.

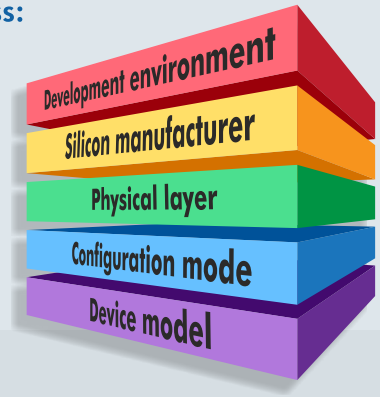
TIO4-Sec - 4fach Drucktasten-Schnittstelle Secure mit Statusausgängen

Die 4-fach Tasterschnittstelle TIO4-Sec ist die Weiterentwicklung des bekannten TAI4. TIO4-Sec unterstützt nun auch KNX Data Secure. Die Kanäle von TIO4-Sec können als Ausgänge zur Ansteuerung von Status-LEDs verwendet werden.

Flexibles Arbeiten im Entwicklungsprozess:

KAIstack-secure

KAIstack-secure beinhaltet die Funktionalität von KNX Secure.



click here

Online Übersicht zu diesen Produkten

TAPKO Technologies GmbH

Photos: tapko.de, istock.com | Conecept+Design: marktwert.net | Edition: 09.2021 | Subject to change

TAPKO
TECHNOLOGIES GMBH

www.tapko.de - info@tapko.de

TAPKO Technologies GmbH I Germany
Im Gewerbepark A15 I D-93059 Regensburg

Phone: +49 941 30 747- 0
Fax: +49 941 30 747- 29