KNX Secure Produkte

KNX Secure Produkte ganz einfach projektieren

ETS überwacht Parameter, generiert Sicherheitsschlüssel und sichert Projekte

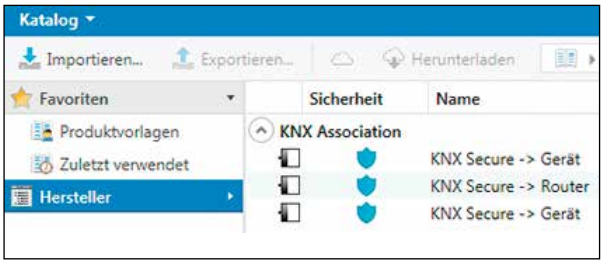
Ob Bürohaus, Industriegebäude oder Smart Home – immer ist die Engineering Tool Software ETS als Teil des KNX Systems Garant für fachgerechte KNX Installationen mit kompatiblen Produkten unterschiedlicher Hersteller. Weltweit verlassen sich Planer, Installateure und Systemintegratoren auf ihr Werkzeug, um Gebäudetechnik professionell zu automatisieren. Auch angesichts zunehmender Cyberkriminalität und wachsendem Bedarf an Datensicherheit können Sie mit der ETS jederzeit rechnen.

Durch kontinuierliche Weiterentwicklung ist die Software nun auch fit für die neue Sicherheitsarchitektur KNX Secure. Durch die Erweiterung können ETS-Anwender ihren Kunden künftig maximalen Schutz gegen Hacker sicherstellen.

Die aktuelle ETS5.6 unterstützt KNX Secure vollständig. Zu den Hauptaufgaben dabei zählen Projektierung, Parametrierung und Inbetriebnahme der Geräte sowie die Projektsicherung.

Intelligente Funktionen machen die Konfiguration der KNX Secure Produkte leicht.

Nachdem ein ETS Projekt eröffnet und die Topologie projektiert ist, kann man wie üblich die entsprechenden KNX Secure Produkte importieren. Leicht zu erkennen sind diese durch ein blaues „Schutzschild“.



KNX Secure Produkte sind durch das Secure Icon zu erkennen.

Kontrolliert Status

Die ETS stellt Parameter zur Einstellungen der Gerätesicherheit bei KNX IP Secure zur Verfügung: „Ein“, „Aus“ oder „Automatisch“. Genauso verfährt die ETS mit der Gruppenadressensicherheit bei KNX Data Secure.

Ein Automatismus stellt sicher, dass Produkte oder Gruppenadressen, die zueinander in Bezug stehen, immer den gleichen Status haben.

Würde man zum Beispiel in ein KNX IP Secure Medium einen herkömmlichen IP Router einfügen, würde dieser von der ETS abgelehnt. Genauso verhält es sich mit Gruppenadressen bei KNX Data Secure.

Topologie mit KNX Secure Produkten

Schluss mit digitalen Einbrüchen!
„Nur KNX gibt die passenden Antworten“

Höchste Verschlüsselungsstandards
„Sicherheitsarchitektur von KNX Secure setzt auf ISO 18033-3 normierte Sicherheitsalgorithmen, wie die AES 128 Verschlüsselung“

Doppelte Sicherheit dank doppeltem Schutzkonzept
„KNX IP und Data Secure können miteinander kombiniert und parallel eingesetzt werden, um ein Höchstmaß an Sicherheit zu erreichen.“

KNX so sicher wie Online-Banking
„KNX Secure verwendet die gleichen Sicherheitsmechanismen wie Ihre Bank“

Die ETS weist darauf hin, wenn gesicherte und ungesicherte Datenpunkte an einer Gruppenadresse verknüpft werden sollen und schlägt Lösungen dafür vor. Mischbetrieb ist dann möglich, wenn sichere und unsichere Funktionen auseinander gehalten werden.
So lassen sich zum Beispiel bei Mehrfachaktoren die Gruppenadressen der Kanalfunktionen wahlweise „secure“ und „unsecure“ einstellen, das Produkt selbst ist dann „secure“.

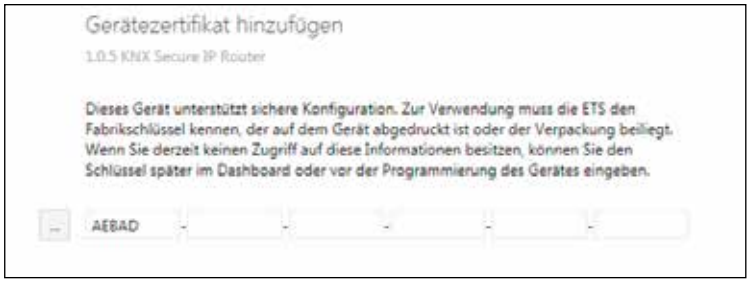
Zertifizierte Produkte

Selbstverständlich muss bei aktivierter Gerätesicherheit und Gruppenadressensicherheit für das Projekt ein Passwort gesetzt werden.
Dieses schützt das Programm vor unerlaubtem Zugriff. Auch muss im Telegrammverkehr jedes Produkt authentifizierbar sein. So fordert die ETS für jedes KNX Secure Produkt, KNX IP Secure und KNX Data Secure, das individuelle Gerätezertifikat.
Dieses besteht aus einem gerätespezifischen Fabrikschlüssel und einer Seriennummer. Der Fabrikschlüssel findet sich entweder auf dem Produkt oder steht zum Bespiel als Code zur Verfügung. Man kann ihn während der Projektierung eintragen, oder aber spätestens bei der Inbetriebnahme, wenn ihn die ETS automatisch anfordert.
Der Fabrikschlüssel wird nicht über Bus gesendet, sondern aus Sicherheitsgründen extern in die ETS eingetragen oder eingescannt.
Nach erstmaliger Anmeldung generiert die ETS automatisch einen neuen, ab jetzt gültigen Schlüssel, den Werkzeug- oder Geräteschlüssel. Der ursprüngliche Fabrikschlüssel wird archiviert. Er lässt sich dann nur noch durch Zurücksetzen des Produktes aktivieren. Damit kommt ein Sicherheitsprinzip zur Anwendung, das analog dem bekannten Handling eines Heimrouters oder der schriftlichen Anmeldung eines Online-Bankzuganges entspricht.

Verwaltet Schlüssel

Das Management der Sicherheitsschlüssel ist Bestandteil der ETS Funktionalität. Während der Parametrierung des Projektes erzeugt die ETS so viele Laufzeitschlüssel, wie für die zu schützende Gruppenkommunikation benötigt wird. Die Laufzeitschlüssel werden gespeichert und können für andere Anwendungen exportiert werden, zum Beispiel für eine Visualisierung. Schließlich werden alle Sicherheitsschlüssel im ETS-Projekt gespeichert. Sie sind nötig für die Inbetriebnahme. Bei einem Verlust des Projektes sind sie die letzte Rettung. Denn ohne Sicherheitsschlüssel lässt sich kein KNX Projekt rekonstruieren. Deshalb erfordert dieses Verfahren eine zuverlässige Archivierung der Projektsoftware. Die Liste der Sicherheitsschlüssel sollte für alle Fälle ausgedruckt und sicher verwahrt werden.

KNX Secure Produkt – Parameter Sicherheit aktiviert / deaktiviert



Bei aktivierter KNX Sicherheit verlangt die ETS den Fabrikschlüssel.

Die ETS stellt zur sicheren Archivierung Dokumente mit allen Geräteschlüsseln zur Verfügung.

KNX IP Secure und KNX Data Secure Produkte

Für weitere Informationen über KNX Secure, besuchen Sie: http://KNXsecure.knx.org

ABB i-bus® KNX IP Secure – IPR/S 3.5.1

ABB Heutzutage ist Sicherheit einer der wichtigsten Entscheidungsfaktoren, wenn es um „Smarter Buildings" geht. ABB's IP Secure-Geräte schützen die KNX Installation und bieten die höchste Sicherheit, die auf dem Markt der Gebäudeautomation verfügbar ist. KNX Telegramme werden nun verschlüsselt über ein IP-Netzwerk zwischen den KNX IP-Routern im IP-Netzwerk übertragen. Sowohl die Laufzeitkommunikation in IP als auch die Inbetriebnahme via ETS sind somit sicher. KNX Telegramme können demnach nicht über IP gelesen werden.

Kontakt: www.new.abb.com

GT – Glas Touch Sensor

CONTROLTRONIC GMBH KNX Glas Touch Sensor und KNX Raumtemperaturregler mit KNX Data Secure: Die CONTROLtronic Glas Touch Serie Living Emotions® bietet innovative Technik in edelstem Design: Echtglas in verschiedenen Farben und Ausführungen, frei austauschbare Symbole für ein bis sieben Sensorflächen, farbige LED-Beleuchtung RGBW, Annäherungserkennung, Temperatur- und Luftfeuchtesensor und flache Unterputzmontage mit unsichtbarer Magnetbefestigung. Durch die Unterstützung von KNX Data Secure ist es mit den CONTROLtronic KNX Glas Touch Sensoren und KNX Raumtemperaturreglern nun möglich, eine sichere und geschützte KNX Installation zu errichten. Insbesondere im Gewerbebau, im Hotel oder in den Außen- und Allgemeinbereichen im Wohnbau – also überall wo die KNX Leitung frei zugänglich ist – darf auf einen Schutz der Installation durch Datenverschlüsselung nicht verzichtet werden.

Kontakt: www.controltronic.com

IO16F01KNX

EELECTRON Das IO16F01KNX hat 16 Ein- und Ausgänge, 16 a-klassifizierte Module für Beleuchtung, Fan Coils, Jalousie und Ventilsteuerung. Es steuert bis zu vier analoge Eingänge, verfügt über manuelle Steuerung und über eine SD-Karte, um ETS-Konfigurationen zu speichern und schnell wiederherzustellen. Das Produkt unterstützt KNX Data Secure, bei denen die ETS-Sicherheitsfunktionen über Gruppenadressen mit Datensicherungspasswort einsetzt. Die Sicherung geschieht über: Gerätauthentifizierung, bei der die MAC-Adresse des Senders, um verfälschte Nachrichten zu unterbinden, entschlüsselt und bestätigt wird sowie Geheimhaltung von Nachrichten durch Ver- und Entschlüsselung von autorisierten Empfängern oder Sendern.

Kontakt: www.eelectron.com

Enertex KNX IP Interface

ENERTEX Das KNX IP Secure Interface (2TE) authentifiziert und verschlüsselt KNX- und IP-Telegramme. Bis zu acht Tunnelverbindungen können verschlüsselt oder unverschlüsselt genutzt werden. Die Kommunikationsperformance überzeugt mit bis zu 49 Telegrammen pro Sekunde. Das Interface verfügt über eine gepufferte Echtzeituhr und SNTP-Server. Ein OLED-Display dient zur übersichtlichen Anzeige von wichtigen Geräteparametern. Mittels Telnet werden weitere Parametrierungs- und Diagnosefunktionen zur Verfügung gestellt. Das Interface wird direkt vom KNX Bus gespeist.

Kontakt: www.enertex.de

Enertex KNX IP Router

ENERTEX Der KNX IP Secure Router (2TE) authentifiziert und verschlüsselt KNX- und IP-Telegramme. Bis zu acht Tunnelverbindungen können verschlüsselt oder unverschlüsselt genutzt werden. Die Kommunikationsperformance überzeugt mit bis zu 49 Telegrammen pro Sekunde. Das Gerät dient als Linien- oder Bereichskoppler. Der Router verfügt über eine gepufferte Echtzeituhr und SNTP-Server. Ein OLED-Display dient zur übersichtlichen Anzeige von wichtigen Geräteparametern. Mittels Telnet werden weitere Parametrierungs- und Diagnosefunktionen zur Verfügung gestellt. Der Router wird direkt vom KNX Bus gespeist.

Kontakt: www.enertex.de

Gira KNX IP-Router Secure

GIRA GIERSIEPEN Der Gira KNX IP-Router verbindet KNX Linien über IP-Datennetzwerke mit der Funktion eines Linien-/Bereichskopplers und dient als ETS-Datenschnittstelle. Neben den vielen Vorteilen einer IP-Infrastruktur bietet diese natürlich auch ein besonderes Angriffspotential. Dank der zukünftigen Unterstützung von KNX Secure zur sicheren Kommunikation ist der Gira KNX IP Router die erste Wahl, um diesen Angriffen angemessen zu begegnen. Clevere Zusatzfunktionen wie ein KNX Zeitgeber oder die KNX Telegrammaufzeichnung auf microSD-Karte runden das Gerät ab.

Kontakt: www.gira.de

RNX-GW1

REDFISH Das RNX-GW1 ist eine moderne Schnittstelle zwischen dem KNX Netzwerk und dem Rest der Welt. Dabei hat es einen Fokus auf Sicherheit inne, da es KNX IP Secure mit bis zu 25 Gleichzeitigen Tunneling-Verbindungen unterstützt. Mit dem KNX Anywhere Cloud Service kommt eine gesicherte End-to-End-Fernsteuerung, welche die Programmierung mit der ETS unterstützt. Auch mit dabei: Web Ready (eine Management App, Web Services). Voreingestellte Sicherheitsupdates, Multi-User-Unterstützung mit Rollen, Google Home Integration, und vielen weiteren Funktionen.

Kontakt: https://redfish.com.au/edge.html

KAIstack-secure

TAPKO Aufgrund der wachsenden Nachfrage nach sicherer Kommunikation bietet TAPKO in seiner neuesten Version der KNX Kommunikationssoftware KAIstack-secure volle KNX Secure-Unterstützung. Trotz erhöhter Komplexität hat der Applikationsentwickler mit KNX Secure fast keinen zusätzlichen Entwicklungsaufwand. Die Aktualisierung bestehender KAIstacks und Anwendungen ist einfach. Die erforderliche Update-Fähigkeit wird mit einem ausgereiften, robusten Remote-Update-Prozess zur Neuprogrammierung der kompletten Firmware – KAIstack-secure mit Applikation – erfüllt. Da KNX Secure auch Einfluss auf die Hardware hat, werden neue Hardware EVAL Boards zur Evaluierung angeboten.

Kontakt: www.tapko.com

MECtp-secure

TAPKO TAPKO präsentiert den Linien-/Bereichskoppler MECtp-secure als erste Systemkomponente mit KNX Secure. Seine Fähigkeit, verschlüsselte Telegramme zu verarbeiten, garantiert eine sichere Inbetriebnahme. Der Schutz der Konfigurationskommunikation ist besonders wichtig für Koppler und Router. Um Zugriffe auf die Hauptleitung zu vermeiden, kann der MECtp-secure geräteorientierte Telegramme der Nebenlinie vollständig blockieren. Die Funktionstaste, ursprünglich von TAPKO zur vorübergehenden Deaktivierung der Nachrichtenfilterung eingeführt, verbessert zudem Komfort und Zuverlässigkeit des Geräts.

Kontakt: www.tapko.com

TAI4-secure

TAPKO Das bewährte TAI4-secure binäre 4-fach I/O-Modul von TAPKO ist jetzt mit KNX Secure erhältlich. Ein Manipulieren der Laufzeitkommunikation oder der Inbetriebnahme ist nicht mehr möglich. Alle gebräuchlichen Eingangsfunktionen wie Schalten, Dimmen, Rollladen, Jalousie und Szene können auf herkömmliche Weise mit Tastern, konventionellen Schaltern und Kontaktsensoren kombiniert werden. Neben der Nutzung als Eingang für potentialfreie Schließer/Öffner-Kontakte sind die Kanäle des TAI4-secure auch perfekt geeignet, um als Binärausgang verschiedenartige Lasten, wie Status-LED, auch mit relativ hoher Leistung anzusteuern. Sogar Dimmen der LED ist möglich. Das kleine Gehäuse des TAI4-secure findet in der Unterputzdose hinter dem Schalter leicht Platz.

Kontakt: www.tapko.com

UIMip-secure

TAPKO In Zeiten von Hackern, die in die Gebäudetechnik eindringen, ist der UIMip-secure, die sicherheitsoptimierte Version unseres bewährten UIMip, die richtige Antwort. Während KNX Security ein brandaktuelles Thema ist, verbindet der UIMip-secure die ETS zur Inbetriebnahme und Überwachung auf zuverlässige, sichere Weise über IP. Der UIMip-secure schützt das Tunneling-Protokoll erfolgreich vor unbefugten Zugriffen, gemäß Norm EN 50090-4-3. Im UIMip-secure sind alle wichtigen Funktionen und Eigenschaften wie keine externe Stromversorgung, Geräteinfo und Firmware-Update über das Web-Frontend auch weiterhin vorhanden. Erhältlich als OEM.

Kontakt: www.tapko.com

MECip-secure

TAPKO Der MECip-secure ist die sicherheitsoptimierte Version unseres etablierten Hochleistungs-KNXnet/IP-Routers zur Verbindung von KNXnet/IP- und KNX TP-Buslinie – eine der wichtigsten Komponenten in der digitalen Infrastruktur heutiger moderner Gebäude. Der MECip-secure schützt erfolgreich vor Eindringversuchen, gemäß Norm EN 50090-4-3. Alle wichtigen Eigenschaften wie keine externe Stromversorgung, Unterdrücken von unnötigem Datenverkehr bei Fehlkonfigurierung, manuelles Abschalten der Filterung, Gerätezugriff und Firmware-Update per Web-Frontend sind vorhanden. Das integrierte Tunneling-Protokoll, mit dem die ETS die Verbindung zur Inbetriebnahme und Überwachung aufbaut, ist ebenfalls gesichert. Verfügbar als OEM.

Kontakt: www.tapko.com

IPS640-secure

TAPKO Die IPS640-secure ist die sicherheitsoptimierte Version unserer intelligenten KNX Stromversorgung, eine wichtige zentrale Komponente in der digitalen Infrastruktur moderner Gebäude. Die IPS640-secure ist vollständig gegen Hackerangriffe gesichert, gemäß Norm EN 50090-4-3. Auf diese Weise sind auch alle wichtigen Funktionen wie KNX-Bus-Reset einer Linie, Senden von Alarmmeldungen wie Innentemperatur, Überlast, Kurzschluss, Geräteneustart und Messwertalarme (nach Überschreiten von Grenzwerten) vor Missbrauch geschützt. Mit nur 2 TE (35 mm) ist die IPS640-secure, unerreicht von Mitbewerbern, das schmalste intelligente 640 mA KNX Netzteil auf dem Markt. Mehr KNX Geräte auf der DIN-Schiene – weniger Kosten. Verfügbar als OEM.

Kontakt: www.tapko.com

KNX IO 511 (Secure)

WEINZIERL Kompakt und sicher: Mit dem KNX IO 511 Secure erweitert Weinzierl sein Angebot der IO-Produktfamilie um ein Gerät mit Unterstützung für KNX Data Secure. Der kompakte Schaltaktor mit einem bistabilen Ausgang und zwei Binäreingängen bietet Funktionen für universelle Ausgänge einschließlich Szenenschaltungen, Ein- und Ausschaltverzögerung, Treppenlichtschaltung und die Ansteuerung von Heizungsventilen (PWM für thermische Stellantriebe). Die Eingänge können über konventionelle Schalter mit einer externen Spannung von 12 bis 230 V angesteuert werden. Der Aktor zusammen mit Eingang B1 dient als Stromstoßschalter. Eingang B2 dient zur Nulldurchgangserkennung. Die Konfiguration erfolgt verschlüsselt mit der ETS5. Alle Datenpunkte können entweder sicher oder unverschlüsselt kommunizieren.

Kontakt: www.weinzierl.de

KNX RF Push Button Insert 440

WEINZIERL Der KNX RF Tastereinsatz 440 von Weinzierl ist kompatibel mit Standard-Tastergehäusen und zeichnet sich durch einen angenehmen Druckpunkt der Tasten aus. Er eignet sich als Alternative für drahtgebundene Schalter ohne Verlegung von Buskabeln. Der Taster wird mit der ETS5 in Betrieb genommen und unterstützt KNX Data-Security. Die Taster sind als Einzel- oder Doppelwippen für Schalt-, Dimm-und Jalousiefunktionen frei konfigurierbar. Zudem können Werte gesendet und Szenen aufgerufen werden. Die Anbindung an KNX TP erfolgt über einen KNX TP/RF Koppler (z. B. den neuen Weinzierl KNX TP/RF 672). Eine integrierte USB-Schnittstelle dient sowohl zur Konfiguration des Gerätes als auch zur Programmierung anderer KNX RF-Geräte. Die Versorgung erfolgt durch eine Standard Batterie CR2032.

Kontakt: www.weinzierl.de

www.knx.org