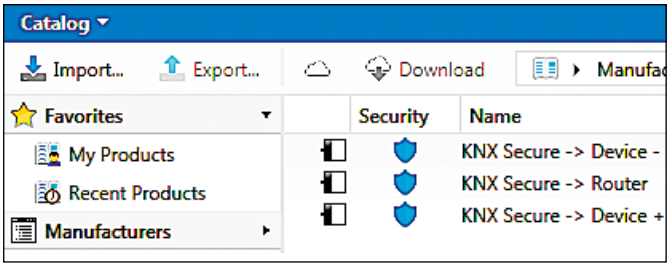

# KNX Secure Products

# Simple Planning and Configuration of KNX Secure Products

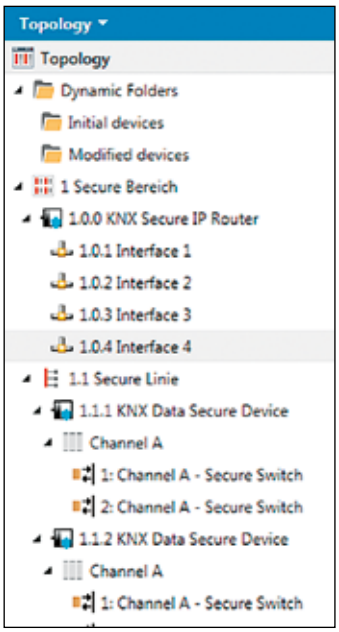
## ETS monitors parameters, generates security keys and safeguards projects

Whether it is an office building, industrial facility or a smart home ETS is always a guarantee of an expert KNX installation implemented using compatible products from different manufacturers. Planners, installers and system integrators all over the world rely on this tool for professional automation of building technology. In light of an increase in cyber criminality and a growing need for data security, you can always count on ETS. With continual further development, the software is now also fit for the new security architecture KNX Secure. As a result, ETS users can in future also ensure that their customers have maximum protection against hackers.

The current ETS version 5.6 fully supports KNX Secure. Its main tasks include the project design, parameterisation and commissioning of the devices as well as the project security. Intelligent functions make the configuration of KNX Secure products easy. Once an ETS project has been opened and the topology has been configured, the corresponding KNX Secure products can be imported as usual. They are easy to recognise by a blue “protective shield”.




*KNX Secure products can be recognised by the Secure icon.*




*Topology with KNX Secure products*

### Monitoring of the status

ETS makes parameters available to carry out device security settings for KNX IP Secure: ‘on’, ‘off’ or ‘automatic’. ETS processes the Group Address security for KNX Data Secure in the same way.

An automatic procedure ensures that devices or Group Addresses which are related to each other always have the same status. If a conventional IP router was inserted for example in a KNX IP Secure medium, it would be rejected by ETS. It behaves in the same way with Group Addresses for KNX Data Secure. ETS indicates if secured and unsecured data points should be linked to a Group Address and suggests solutions for this scenario. A mixed operation is possible if

**No more digital break-ins!**
*“Only KNX has been delivering the most appropriate responses”*

**Highest encryption standards**
*“Relying on security algorithms standardised according to ISO 18033-3, such as AES 128 CCM encryption”*

**Double protection concept for twice the security**
*“KNX IP and Data Secure can be combined and used in parallel to achieve maximum security”*

**KNX as secure as online banking**
*“KNX Secure is using the same security mechanisms as your bank, making KNX most trustworthy”*

secure and unsecure functions are kept separate. For example, with multiple channel actuators, the Group Addresses of the channel functions can be set as ‘secure’ and ‘unsecure’ but then the device itself is ‘secure’.

## Certification of devices

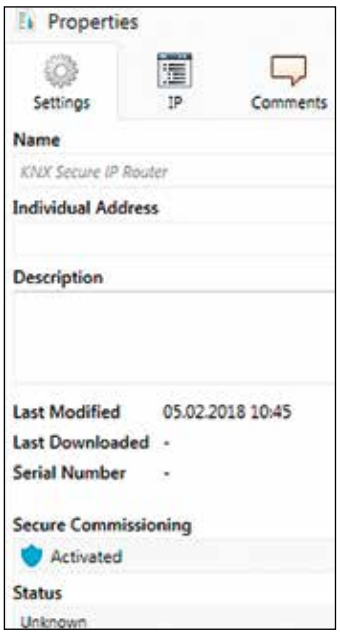
When the device security and Group Address security is activated, a password must of course be set for the project. This protects the program against unauthorised access. It must also be possible to authenticate each device in the telegram traffic. ETS thus requires an individual device certificate for each KNX Secure product as well as KNX IP Secure and KNX Data Secure. This consists of a device-specific factory key and a serial number. The factory key is located either on the device or is available for example as a code. It can be entered during the project design or at the latest at the commissioning stage if ETS requests it automatically.

The factory key is not sent via the bus but entered externally in ETS or scanned for security reasons. After the initial registration, the ETS automatically generates a new device key which is valid immediately. The original factory key is archived. It can only be activated by resetting the device. A safety principle is thus applied which corresponds to the handling of a home router or the written registration of online banking access.

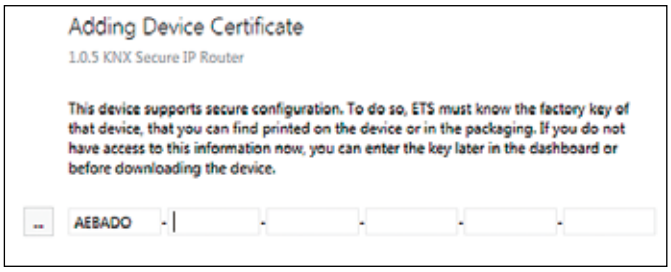
## Management of the security keys

The management of the security key is an integral part of the ETS functionality. During the parameterisation of the project, ETS generates as many runtime keys as required for the group communication that is being protected. The runtime key is stored and can be exported for other applications, for example for visualisation. Finally, all the security keys are stored in the ETS project. They are required for the commissioning phase. They are the last resort if a project is lost as a KNX project cannot be reconstructed without a security key. This process therefore requires reliable archiving of the project software. The list of security keys should be printed out just in case and kept somewhere safe.

*For more information about KNX Secure visit:* ***https://KNXsecure.knx.org***




*KNX Secure product – Secure commissioning activated / deactivated*




*When KNX security is activated, ETS requests the factory key.*


*For secure archiving, ETS makes documents available with all the device keys.*

# KNX IP Secure and KNX Data Secure Products

***For further informationen about KNX Secure, please visit: http://KNXsecure.knx.org***

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

**ABB** Nowadays security is one of the key decision factors when it comes to smarter buildings. ABB's IP Secure devices protect the KNX installation and offer the highest security which is available on the building automation market. KNX telegrams are now transmitted in encrypted form between KNX IP routers on the IP network. Runtime communication on IP as well as commissioning via ETS is secure now, ensuring that KNX telegrams cannot be read on IP.

*Contact: www.new.abb.com*


## GT – Glas Touch Sensor

**CONTROLTRONIC GMBH** KNX Glass Touch Sensor and KNX Room Thermostat with KNX Data Secure: The CONTROLtronic glass touch series Living Emotions® offers innovative technology and superior design: Real glass in different colors and finishes, Icons self-exchangeable for one to seven sensor fields, Color LED illumination RGBW, Proximity detection, Temperature and air humidity sensor and Flat in-wall mounting with invisible magnetic fixing. With the support of KNX Data Secure, the CONTROLtronic KNX Glass Touch Sensors and KNX Room Thermostats make it possible to set up a secure and protected KNX installation. In commercial buildings, hotels and in outside and public areas of residential buildings – so wherever the KNX Line is free accessible – protection of the installation by data encryption is essential.

*Contact: www.controltronic.com*

## IO16F01KNX

**EELECTRON** The IO16F01KNX has 16 inputs/16 outputs, 16a rated module for lights, fan coils, venetians and valve controls. It controls up to four analogue inputs, has manual control and an SD card to save ETS configuration for fast recovery. The product supports KNX Data Secure, allowing ETS security activation over Group Addresses with data protection password. The device allows: device authentication, where sender MAC address is decrypted and authenticated to avoid fraudulent message replication; message confidentiality, were message content is encrypted and decrypted from authorised receivers; or both.

*Contact: www.eelectron.com*

## Enertex KNX IP Secure Interface

**ENERTEX** The KNX IP Secure Interface (2TE) authenticates and encrypts KNX and IP telegrams. Up to eight tunnel connections can be used encrypted or unencrypted. The communication performance is impressive with up to 49 telegrams per second. The interface has a buffered real-time clock and SNTP server. An OLED display shows important device parameters. Telnet provides further parameterization and diagnostics functions. The interface is powered directly from the KNX bus.

*Contact: www.enertex.de*

## Enertex KNX IP Secure Router

**ENERTEX** The KNX IP Secure Router (2TE) authenticates and encrypts KNX and IP telegrams. Up to eight tunnel connections can be used encrypted or unencrypted. The communication performance is impressive with up to 49 telegrams per second. The device can be used as a line or area couple. The router has a buffered real-time clock and SNTP server. An OLED display shows important device parameters. Telnet provides further parameterization and diagnostics functions. The router is powered directly from the KNX bus. *Contact: www.enertex.de*


## Gira KNX IP-Router Secure

**GIRA GIERSIEPEN GMBH & CO. KG** The Gira KNX IP-Router connects KNX Lines via IP networks with the function of a Line/Area coupler und serves as ETS data interface. Next to the many benefits of an IP infrastructure, it also offers of course an obvious threat of being tampered with. Thanks to the support of KNX Secure for protected communication, the Gira KNX IP Router is the first choice to counter this kind of attacks. Smart additional functions, such as a KNX timer or the KNX telegram recording on microSD card, top the device off.

*Contact: www.gira.de*

## RNX-GW1

**REDFISH** The RNX-GW1 is a modern security focused interface between the KNX network and the rest of the world. At its core, it supports the KNXnet/IP Secure protocol, with up to 25 concurrent tunnelling connections. Secure end-to-end remote access (including programming with the ETS) is included with the KNX Anywhere cloud service. Also included: web ready (management app, web services), configured for guaranteed automatic security updates, multi-user support with roles, google home integration, modbus, ...

*Contact: www.redfish.com.au/edge*

## KAIstack-secure

**TAPKO** Due to growing demand for secure communication, TAPKO is offering full KNX Secure support in its latest KNX communication software release, KAIstack-secure. In spite of increased complexity, the application developer has almost no additional effort despite KNX Secure. Updating existing KAIstacks and applications is straightforward. The required update ability is satisfied with a sophisticated robust remote update process for reprogramming the complete firmware – KAIstack-secure together with application. Since KNX Secure has also hardware impacts, new hardware EVAL boards are offered for evaluation.

*Contact: www.tapko.com*

## MECtp-secure

**TAPKO** presents the Line/Area Coupler MECtp-secure as first system component supporting KNX Secure. Its ability to process secured telegrams guarantees safe commissioning. Being particularly important for Couplers and Routers, the configuration communication is protected. To prevent access to the Main Line, MECtp-secure can block device-oriented messages from the secondary Line. The function button, originally introduced by TAPKO for temporary deactivation of message filtering, is further improving the comfort and reliability of this device.

*Contact: www.tapko.com*



## TAI4-secure

**TAPKO** TAPKO´s proven TAI4-secure 4-fold binary I/O module is now available with KNX Secure. Any kind of manipulation during runtime communication and commissioning is not possible anymore. All usual input functions of the I/O module like switching, dimming, shutters, blinds control and scenes can be used in a common way. Besides the input functionality of TAI4-secure for sensing NO/NC floating contacts of push-buttons, conventional switches and contact sensors, it is also a perfect binary output for driving various loads, like status LEDs, with a comparably high amount of power. Even dimming of the connected LEDs is possible. Due to its small housing, TAI4-secure finds place in a flush-mounted box behind the switch.

*Contact: www.tapko.com*

## UIMip-secure

**TAPKO** In times of hackers intrude in building technology, UIMip-secure, the security enhanced version of our existing UIMip, is the proper answer. While KNX Secure is a red-hot subject, UIMip-secure connects the ETS for commissioning and monitoring in a reliable and secure way over IP. UIMip-secure protects the tunnelling protocol successfully against intrusion, according to the standard EN 50090-4-3. UIMip-secure is preserving valuable features like no external power supply, device info and firmware update via web frontend. Also available as OEM.

*Contact: www.tapko.com*


## MECip-secure

**TAPKO** MECip-secure is the security enhanced version of our existing high performance KNXnet IP Router, connecting the upper KNXnet IP Line and the lower KNX TP Line. MECip-secure protects successfully against intrusion attempts, according to the standard EN 50090-4-3. Of course, valuable features like: no external power supply, reduction of unnecessary traffic in case of misconfiguration, manual suspending of filtering, device access and firmware update via web frontend are preserved. The integrated tunnelling protocol connecting ETS for commissioning and monitoring is also secured. Also available as OEM.

*Contact: www.tapko.com*

## IPS640-secure

**TAPKO** IPS640-secure, the security enhanced version of our existing intelligent KNX Power Supply. IPS640-secure is fully protected against hacker attacks, according to the standard EN 50090-4-3. This way crucial functions like KNX bus reset of a Line, sending of alarm messages like: internal temperature, overload, short-circuit, device start-up and measurement alarms (after threshold value crossing) are protected against misuse. IPS640-secure is the slimmest intelligent 640 mA KNX Power Supply on the market at only 2 TE (35 mm). It is minimising costs as more KNX devices can be mounted on a single DIN-rail. Also available as OEM.

*Contact: www.tapko.com*



## KNX IO 511 (Secure)

**WEINZIERL ENGINEERING** With the KNX IO 511 Secure, Weinzierl has expanded its product range of the IO product family with a device with support for KNX Data Secure. The compact switch actuator with one bi-stable output and two binary inputs provides functions for universal outputs including scene control, on / off delay, staircase light switching and control of heating valves. The inputs can be connected to conventional switches with an external voltage of 12 to 230 V. The actuator combined with input B1 serves as a latching relay. Input B2 is used for zero crossing detection. The configuration is encrypted with the ETS5.

*Contact: www.weinzierl.de*

## KNX RF Push Button Insert 440

**WEINZIERL ENGINEERING** The KNX RF Push Button Insert 440 by Weinzierl is compatible with standard switch housings and is characterised by a soft pressure point of the buttons. It is suitable as an alternative for wired switches without routing bus cables. The device is commissioned with the ETS5 and supports KNX Data Secure. The push button is freely configurable as single or double rockers for switching, dimming and blind functions. In addition, values can be sent and scenes can be called up. The connection to KNX TP is made via a KNX TP/RF Coupler (e. g. new Weinzierl KNX TP/RF 672). An integrated USB interface is used both to configure the device and to program other KNX RF devices. It is powered by a standard CR2032 battery.

*Contact: www.weinzierl.de*

www.knx.org