



Smart home and building solutions.  
Global. Secure. Connected.



# KNX Secure & New KNX Secure Products



# Why KNX Secure

Recently smart building installations are increasingly the subject of cyber-attacks. These cyber-attacks can be easily avoided in case of KNX by ensuring that installations are never directly (without vpn) accessible via the internet.

## KNX Secure offers maximum protection

Home and building automation with KNX is secure. Our technology follows all necessary security regulations. The KNX Secure technology is standardised according to EN 50090-3-4, which means that KNX successfully blocks hacker attacks on the digital infrastructure of networked buildings. Thus **minimising the risk of digital break-ins**.

Moreover, KNX Secure meets **the highest encryption standards** (according to ISO 18033-3, such as AES 128 CCM encryption) in order to effectively prevent attacks on the digital infrastructure of buildings and to achieve the highest level of data protection.

KNX Secure guarantees maximum protection by offering a double protection. **KNX IP Secure** extends the IP protocol in such a way that all transferred telegrams and data are completely encrypted. **KNX Data Secure** effectively protects user data against unauthorised access and manipulation by means of encryption and authentication.

## Secure your installation by following the KNX Secure checklist

To ensure maximum security in your KNX Installations, we designed a KNX Secure Checklist, where you can find a step-by-step overview on everything that needs to be considered to achieve a secure KNX installation.

This checklist has been designed to make sure that people are not trying to take advantage of possible security loopholes in installations.

In many installations, such loopholes are unfortunately very straightforward.

Download the KNX Secure Checklist here:

[https://www.knx.org/wAssets/docs/downloads/Marketing/Flyers/KNX-Secure-Checklist/KNX-Secure\\_Checklist\\_en.pdf](https://www.knx.org/wAssets/docs/downloads/Marketing/Flyers/KNX-Secure-Checklist/KNX-Secure_Checklist_en.pdf)

We also offer a more comprehensive KNX Secure guide, intended for both installers as well as KNX manufacturers to learn about the current measures that can be undertaken to increase security of KNX installations.

Download the KNX Secure Guide here:

[https://www.knx.org/wAssets/docs/downloads/Marketing/Flyers/KNX-Secure-Position-Paper/KNX-Secure-Position-Paper\\_en.pdf](https://www.knx.org/wAssets/docs/downloads/Marketing/Flyers/KNX-Secure-Position-Paper/KNX-Secure-Position-Paper_en.pdf)

# New KNX Secure Products

## Eelectron IPSBA01KNX - KNX Bridge with IP interface and KNX+AUX power supply 640mA

**Eelectron SpA** - The IPSBA01KNX integrates, in a compact size of 4 DIN modules, a KNX power supply with aux. output at 30V DC with a total current of 640mA and, an IP interface allowing KNX installations to be implemented quickly and efficiently. It can be linked to a Cloud platform standard secure protocols and share relevant data from connected devices. The KNX IP interface allows to connect a KNX network to an IP backbone. The device uses KNX Data Secure protocol and is configurable with ETS. Logic blocks are available for simple or complex expressions with conditional operators. It combines also the “Virtual Holder Logic” for hotel application deducing the presence of people in the room using dedicated sensors. It implements the control logic called “OnLine-OffLine”, checking if all KNX TP devices of the subnet connected to the power supply are “On-line”.

Contact: <http://www.eelectron.com>



## Enertex® ENA<sup>2</sup>

**Enertex** - The ENA<sup>2</sup> offers Remote access without “Cloud”. The device is configured only with your Web browser. The optional “Relay server” forwards your VPN connections to be independent of the internet connection type (IPv4, IPv6, DS-Lite) and Router configuration without lowering security. VPN data still can only be decrypted by the user. The ENA<sup>2</sup> can manage a “Protected Network” to prevent “Cloud” IoT-devices from accessing the building automation. All KNX telegrams are stored into an integrated database. The device website visualizes telegram data in time-value-charts and offers error analysis.

Contact: [www.enertex.de/e-index.html](http://www.enertex.de/e-index.html)



## Gira S1 KNX Secure

**Gira Giersiepen GmbH & Co. KG** - Data security is important in a Smart Home. The Gira S1 remote access module enables users to connect to their KNX Smart Home easily and absolutely securely even when they're not at home: Switching off the lights, checking camera images, turning on the heating or closing blinds is possible via remote access while on the move, but third-party access is impossible. This is because communication is encrypted. In addition, the Gira S1 is ideal for use together with the Gira X1, the Gira HomeServer, the Gira Alarm Connect security system, and the Gira door communication system. In addition, the Gira S1 has been awarded the “Smart Home - Information Security Tested” certificate by the VDE Institute.

Contact: <https://gira.de/goto/GiraS1FlyerEN>



## KNX Data Secure Actuator

**MEAN WELL EUROPE** - The new generation of MEAN WELL KNX actuators supports KNX data secure, ensuring the data interchange processes are protected against tapping and manipulation. The KAA-8RS KNX Secure actuator is an eight-channel device with a high-quality, independent latching relay for a switch, shutter or any possible mixed applications. The compact design with four units (72 mm) wide modular makes it suitable for installation in the distribution board on 35mm mounting rails in the EIB/KNX system. The switching relays are suitable for switching ohmic, capacitive, and inductive loads, and motors in shutter or blind applications. The actuator is powered by the EIB/KNX and does not require an additional power supply.



Contact: <https://building.meanwell.com/productSeries.aspx#tag-6-65>

## KNX Data Secure CV LED Driver

**MEAN WELL EUROPE** - MEAN WELL's PWM-200KN series is a KNX direct constant voltage driver range with Data secure. It features KNX interface and can be implemented to control the lights directly without using a KNX-DALI gateway. With the PWM style output, the driver can maintain the color temperature and the brightness homogeneity when driving all kinds of LED strips.

Data Secure allows users to secure the KNX communication on every medium. The unique QR code called FDSK can be found on the PWM-200KN. It operates from 100-305VAC and is available in different output voltages. The output frequency is changeable up to 4K Hz compliant IEEE 1789-2015, providing an excellent solution for mitigating health risks for humans.



Contact: <https://building.meanwell.com/productSeries.aspx#tag-6-68>

## KNX Flush-mounted actuators

**SIEMENS AG** - More flexibility, more security - that's behind the new KNX actuators for flush-mounted installation. The new models impress with their compact design and flexible installation concept, making them the ideal choice for the retrofit market. The hardware has been upgraded to include three binary inputs. Thanks to the extended logic module, the new devices can also handle complex control tasks and also offer maximum data protection thanks to KNX Data Secure encryption. To ensure that the actuators continue to work perfectly in the future, there is a firmware download tool that keeps products up to date. The new dimming actuator is suitable for LED loads.



Contact: <https://www.siemens.com/knx>

# More KNX Secure Products

Interested in finding more KNX Secure products? You can find them here:

[https://www.knx.org/knx-en/for-professionals/get-started/certified-knx-products/?searchWord=&is\\_secure=1&productfamily=&producttype=](https://www.knx.org/knx-en/for-professionals/get-started/certified-knx-products/?searchWord=&is_secure=1&productfamily=&producttype=)



## OEM SECURE Devices with your brand label from European production



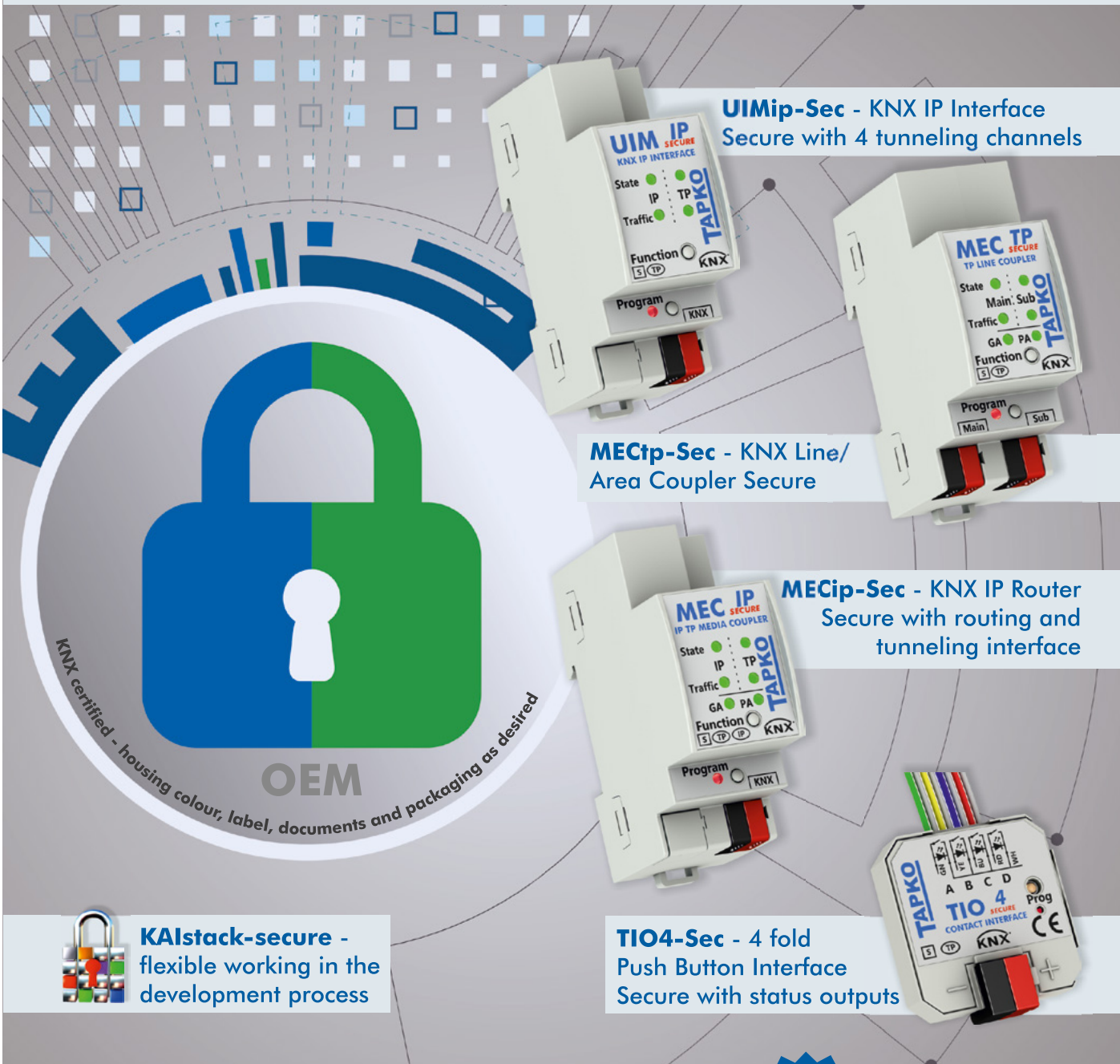
Security of Installation



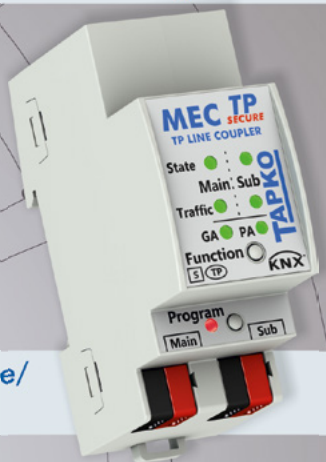
KNX Data Secure



KNX IP Secure



**UIMip-Sec - KNX IP Interface**  
Secure with 4 tunneling channels



**MECtp-Sec - KNX Line/  
Area Coupler Secure**



**MECip-Sec - KNX IP Router**  
Secure with routing and tunneling interface



**TIO4-Sec - 4 fold  
Push Button Interface**  
Secure with status outputs



**KAlstack-secure -**  
flexible working in the  
development process



Phone: +49 941 30 747- 0  
E-Mail: info@tapko.de



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



tapko.de



# theben

## Giving you flexibility Optical presence detector thePixa KNX

thePixa doesn't care who you are or what you are doing. thePixa only detects which part of the room you are in. To regulate the temperature so that you are comfortably warm. To activate the ventilation if there are too many people in the room. To switch on the light there - and exactly when you really need it. To record everything precisely so that you can do what you want to do better, more undisturbed, more comfortably. And to plan better when what should happen. No matter who you are. Exactly because you are.

thePixa - pixel-based, data protection-compliant, DEKRA\*-tested.  
[www.theben.de/thePixa-en](http://www.theben.de/thePixa-en)



Building Automation since 1921



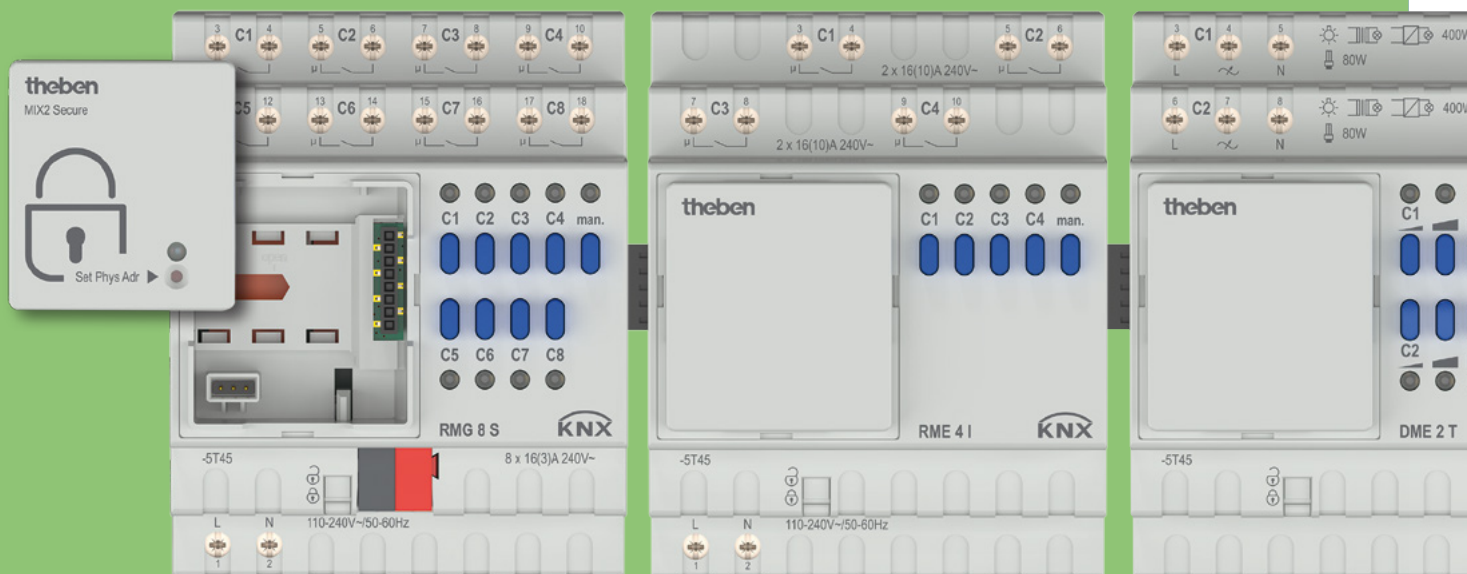
## KNX MIX2-actuators Flexible. Future-proof. Expandable KNX Data Secure

MIX2 KNX actuators leave nothing to be desired in terms of flexibility and security:

- Mix channels and functions via a basic device and up to two extension devices, e.g. a switching actuator with a dimming and a blind actuator.
- Reduce the number of system devices and lower the channel price.
- And all this with maximum security thanks to KNX Data Secure - also retrofittable.



This is only available from Theben!  
More in the free white paper on  
[theben.de/mix2-actuators](http://theben.de/mix2-actuators)



## KNX Compact IO Serie series becomes secure

With the introduction of the Compact IO series, Weinzierl has set new standards in terms of flexibility in KNX installation. The devices for in-line installation with a width of 1 unit (18 mm) cover the essential input: Switching, dimming, blinds and binary inputs. But also dimmers for 230V~ and for RGB LEDs could be realised in a minimal size.

The next step is now targeting the safety of KNX installations. Weinzierl is increasingly focusing on integrating the devices with KNX Security. In the KNX Compact IO series, three devices are making the start and replacing their predecessors:

### KNX IO 510.1 SECURE (20)



#### KNX IO 510.1 secure (20)

Switching actuator  
with two relay outputs

### KNX IO 511.1 SECURE (102I)



#### KNX IO 511.1 secure (102I)

Switching actuator with one relay  
output and two binary inputs

### KNX IO 546.1 SECURE (1D10)



#### KNX IO 546.1 secure (1D10)

Dimming actuator with one output  
for 1..10 V and one relay output

KNX Security protects both the function and the configuration of the devices. Because security can be activated or deactivated individually for each object or for each group address, the new devices can also be connected to non-secure devices without any problems. In this case, the protection of the device configuration can still remain activated.