TAPKO
TECHNOLOGIES GMBH

Smart Building Fair Milano 2021

KNX Secure
OEM Devices & Highlights

Sales & Technical Consultant: Peter Sperlich
23.11.2021

Dipl.-Ing. (FH) Peter Sperlich

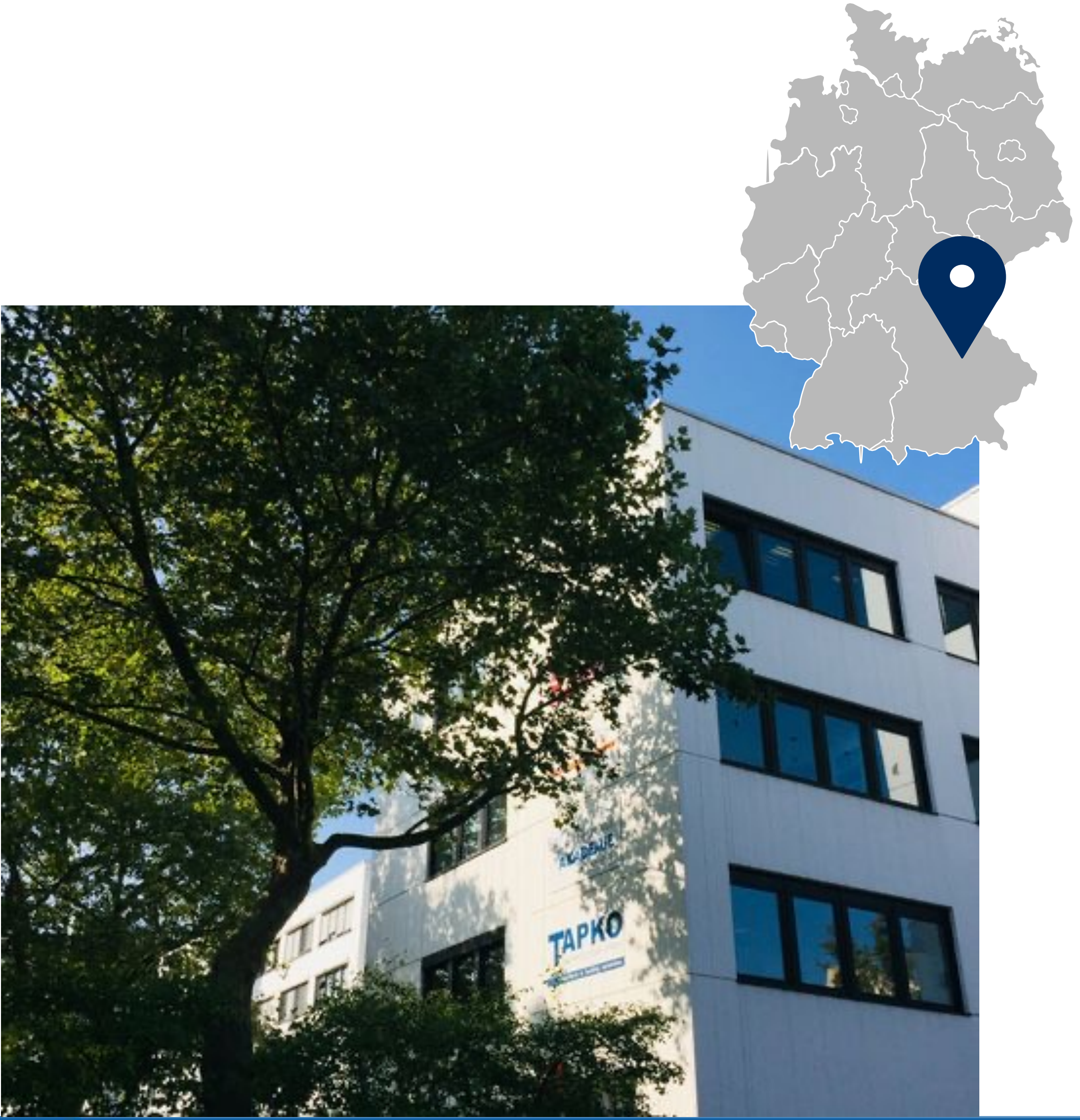
- since 28 Years (instabus EIB) KNX
- since 20 Years in Switzerland
- since 10 Years Owner SBD GmbH Switzerland
- since 8 Years Owner SBS GmbH Switzerland
- since 3 Years Sales Agent TAPKO Technologies GmbH

- KNX-Trainer
- KNX Professional Member
- KNX Coordinator «E-Haus» ZVEH
- KNX Supporter of Smart Living Initiative (at ZVSHK und BMWi)

2. Price Category „Best Project“ at SmartHome Germany Award 2013 in Berlin.

2014 Internationale KNX-Awards: Category «Special» und «People Choice»!!
2020 KNX Award with «E-House»

KNX expertise for more than 20 years



Location: Regensburg (DE)

~125km to Munich

~115km to Nurnberg

~120km to Passau

~0km to your OEM Products

CEO Klaus Adler (left) and CEO Petar Tomic (right)

Company location

2 floors / 750m2 per floor

3rd floor: administration, development, sales, logistics

2nd floor: final assembly

Warehouse on the premises of the Regensburg industrial park

Quality

- Full-fledged KNX member
- Certified to ISO 9001
- Association Connecting Electronics Industries

TEST LAB KNX IPC®

3 decades of expertise in building automation

The TAPKO story is a journey through 3 decades of the technology EIB and today's KNX system. Because: The Owner Klaus Adler and Petar Tomić have been involved in the specification of the EIB and also in the development of the first EIB devices.

Klaus Adler (left) and Petar Tomic (right) with the President of the KNX Association, Franz Kammerl (centre).

1990 Development of the EIB system
1999 Konnex Association was founded
1999 Foundation of TAPKO GmbH
2000 EIB Stack, TAPKO's first customer Projects
2001 Establishment of production with partner APRICUM d.o.o.
2005 ISO 9001 Certification
2006 Foundation of KNX Association
2006 TAPKO becomes KNX Shareholder
2006 First EIB/KNX module from TAPKO: SIM-KNX
2010 Relocation / Expansion into new office premises
2011 Foundation of TAPKO GOSSÉ & TECH
2012 TAPKO stand at the Light & Building trade fair in Frankfurt
2013 Certification as KNX test laboratory
2016 TAPKO is a member of the KNX Technical Board
2019 20th Birthday of TAPKO Technologies GmbH

KNX Security: Is KNX really not Secure??

St. Regis Shenzhen Hotel

https://www.wired.com/2014/07/hacking-hotel-room-controls/

How it began

- 2014 a CCC Member and Security Consultant Jesus Molina was booked into the 5 Star Hotel “St. Regis Shenzhen hotel” near Hong Kong.
- He found out that he can easily control Light, Temperature, blinds, “Do not Disturb Lights” by logging into the WiFi Network.
- “St. Regis” provides iPADs for the Control of TV and KNX Building Automation.
- Jesus Molina logged in the public Wifi Network and sniffed the Telegrams

But:

- The problem is the fact that the St. Regis uses the same **open wireless network** to send these commands that guests use to surf the internet, making it easy for guests---or anyone else within wireless range---to sniff the traffic and record the commands.

Fix:

- IT-Firewall: Separation of the Hotel Guest Network and the technical facility network

KNX Security: Is KNX really not Secure??

Cyber Attacks

Now: Cyber Attacks

- KNX Project got attacked in 2021
- Deleted Application Program
- Reconfigured Devices
- Locked BCU Password

But:

- This Time the Attacker comes from Outside.
- They use open Ports and try to get inside IP Networks

Fix:

- Close Ports of Internet Router!
- Use VPN Connection for Remote!
- Tell your Customers to do so!!

KNX Security: Quick Tipps!

FIRST: Close up your Network!

- If an installation is linked to Internet, the use of a **VPN tunnel** to access it via the internet is an absolute MUST. When using a KNX Secure Tunneling interface, be sure to use the strong passwords suggested by ETS and do not replace them with own weak ones.

- Special attention should go to installations with public areas, i.e. where persons are able to wander around without any surveillance: even a wired KNX system can then be vulnerable to attack;

- Installations using wireless communication are the number 1 attack target, as communication between devices is completely out in the open, compared to when devices communicate over a dedicated wire. Use of **KNX Secure** on this medium is therefore highly recommended;

- If you have a KNX IP Backbone and other IP networks, use a **VLAN separation** and allow communication between the KNX IP network and other networks only via a **suitable firewall.**

KNX Security: KNX Secure is Standard!

The KNX Secure technology is **standardized according to EN 50090-3-4**, which means that KNX successfully blocks hacker attacks on the digital infrastructure of networked buildings.

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.

KNX Secure guarantees maximum protection by offering a double protection.

- KNX IP Secure extends the IP protocol
- KNX Data Secure protects against unauthorized access

KNX Security: Use KNX Secure Products!

Tapko offers key base devices with KNX IP Secure and Data Secure!

Build on a secure digital infrastructure with KNX Secure for the building automation of the future. The data communication in the network is encrypted by IP Secure and an encrypted transmission of the KNX telegrams is guaranteed. In addition, data transmission to the visual interfaces is also secure.

With KNX Data Secure, selected KNX telegrams are authenticated and coded, regardless of the medium they come from. This way no manipulation can take place between actuator and senor. With an Apricum Secure interface the individual rooms are connected and secured via an IP backbone.

TAPKO
TECHNOLOGIES GMBH

Safe in future: KNX Secure technology

KNX SECURE

DATA SECURITY

IP SECURITY

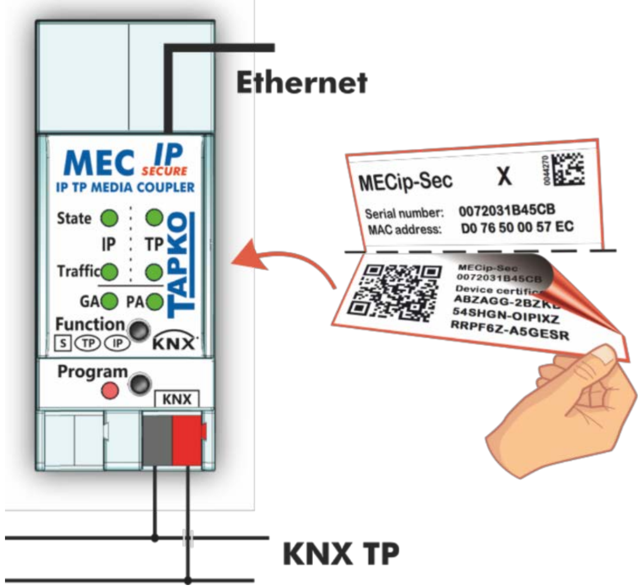
Secure KNX applications - secure building automation

Protection against unauthorized

- manipulation of the configuration
- Operation of functions in buildings
- Display and readout of data

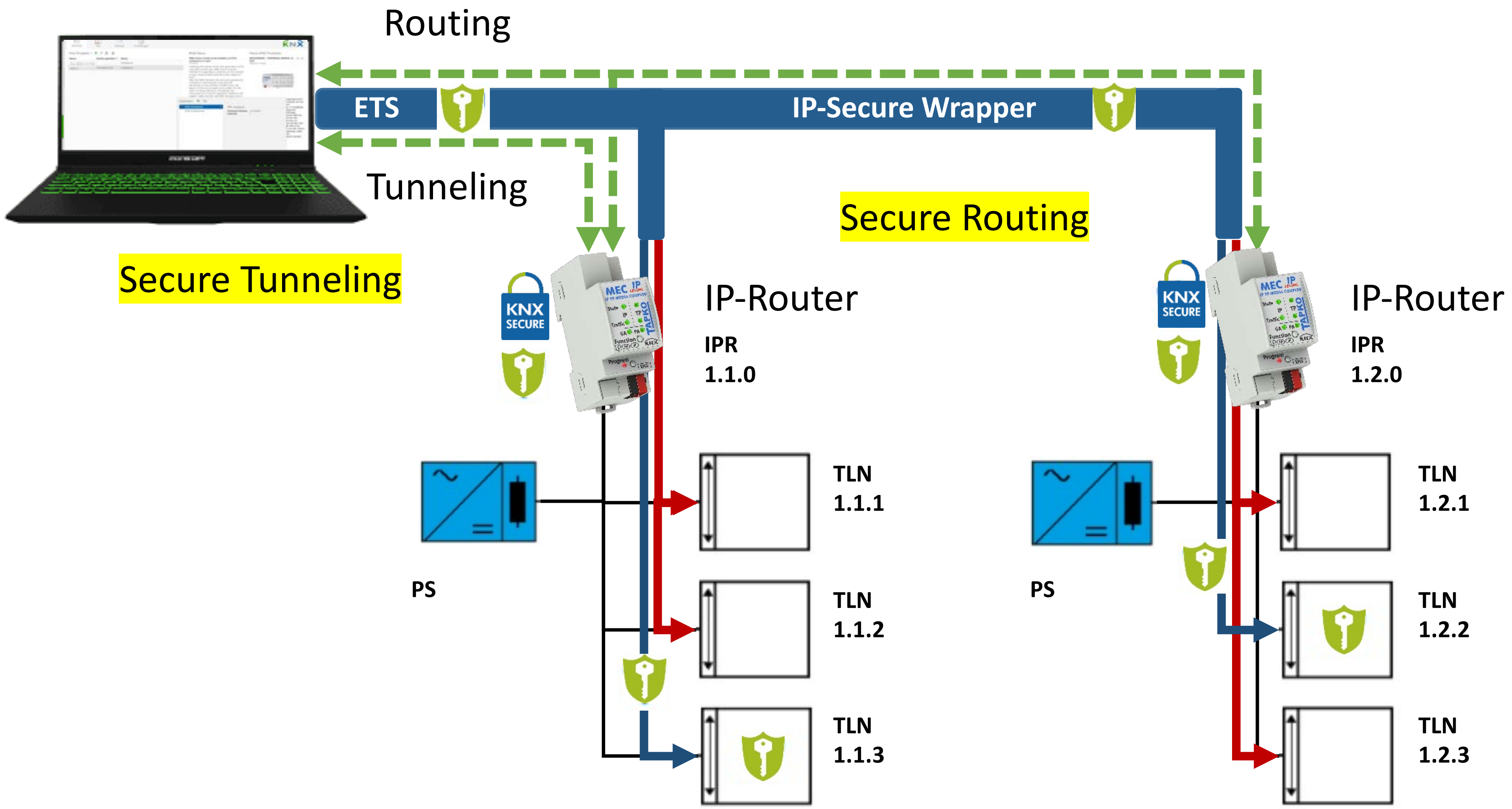
Safe commissioning – with the QR code stuck on it

- Enter ETS project password
- Add IP Secure devices to project
- Import device certificates
- Program IP Secure devices



Barcode can be scanned by Laptop Camera or connected USB-Camera

KNX IP Secure and Data Secure



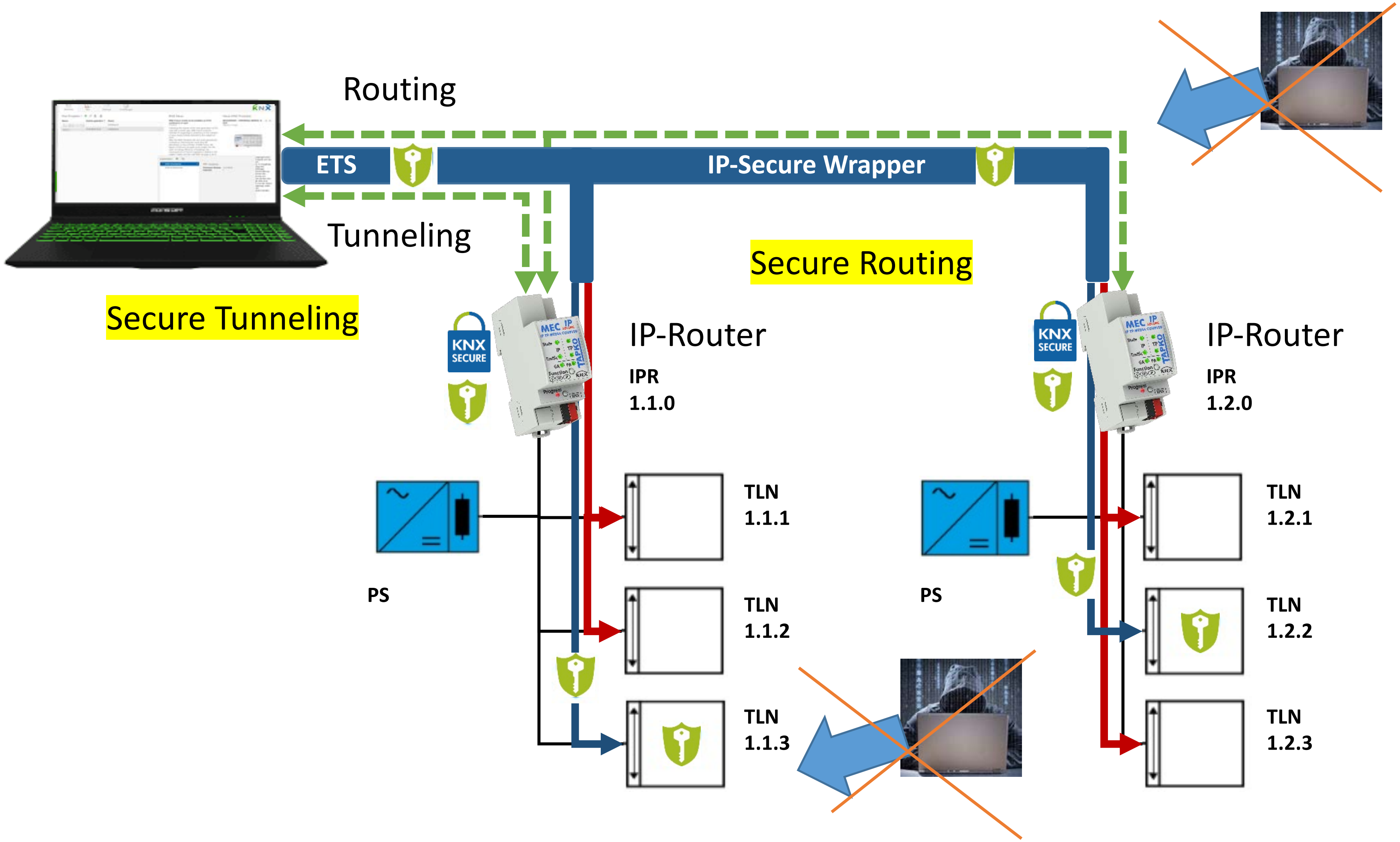
Group Communication

Data Secure

Unsecure (Plain)

TLN	Bus Device
PS	Power Supply
IPR	IP Router (Secure Compatible)

KNX IP Secure and Data Secure



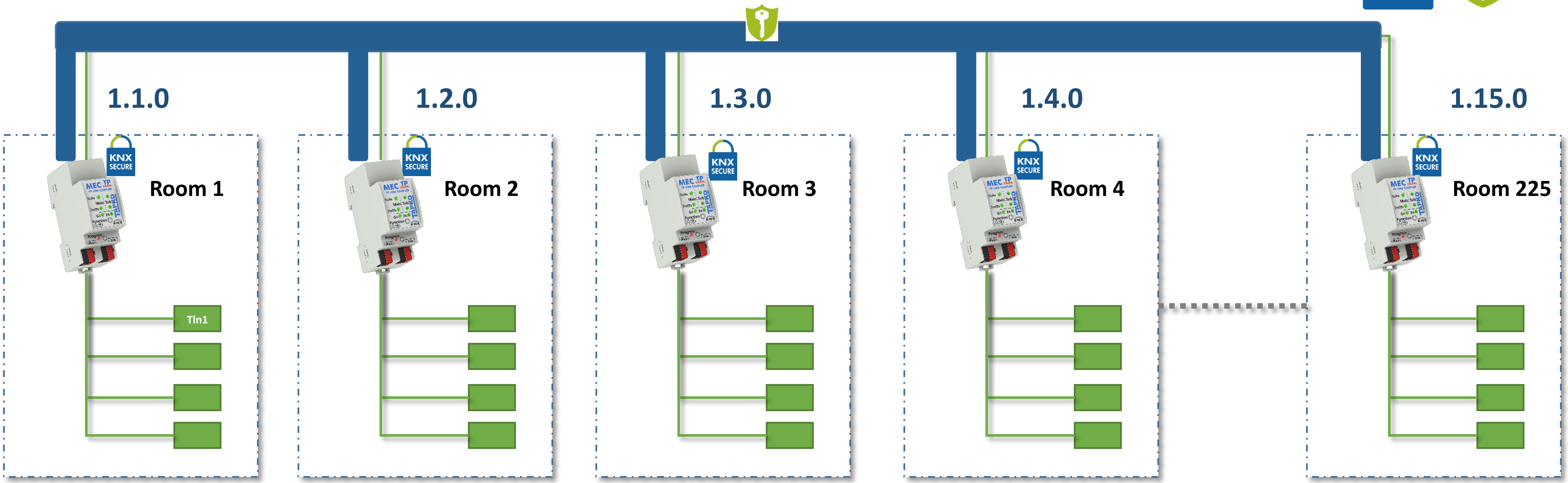
Group Communication

⇄	Data Secure
⇄	Unsecure (Plain)

TLN	Bus Device
PS	Power Supply
IPR	IP Router (Secure Compatible)

Data Secure – where to use it

Excample: Hotel



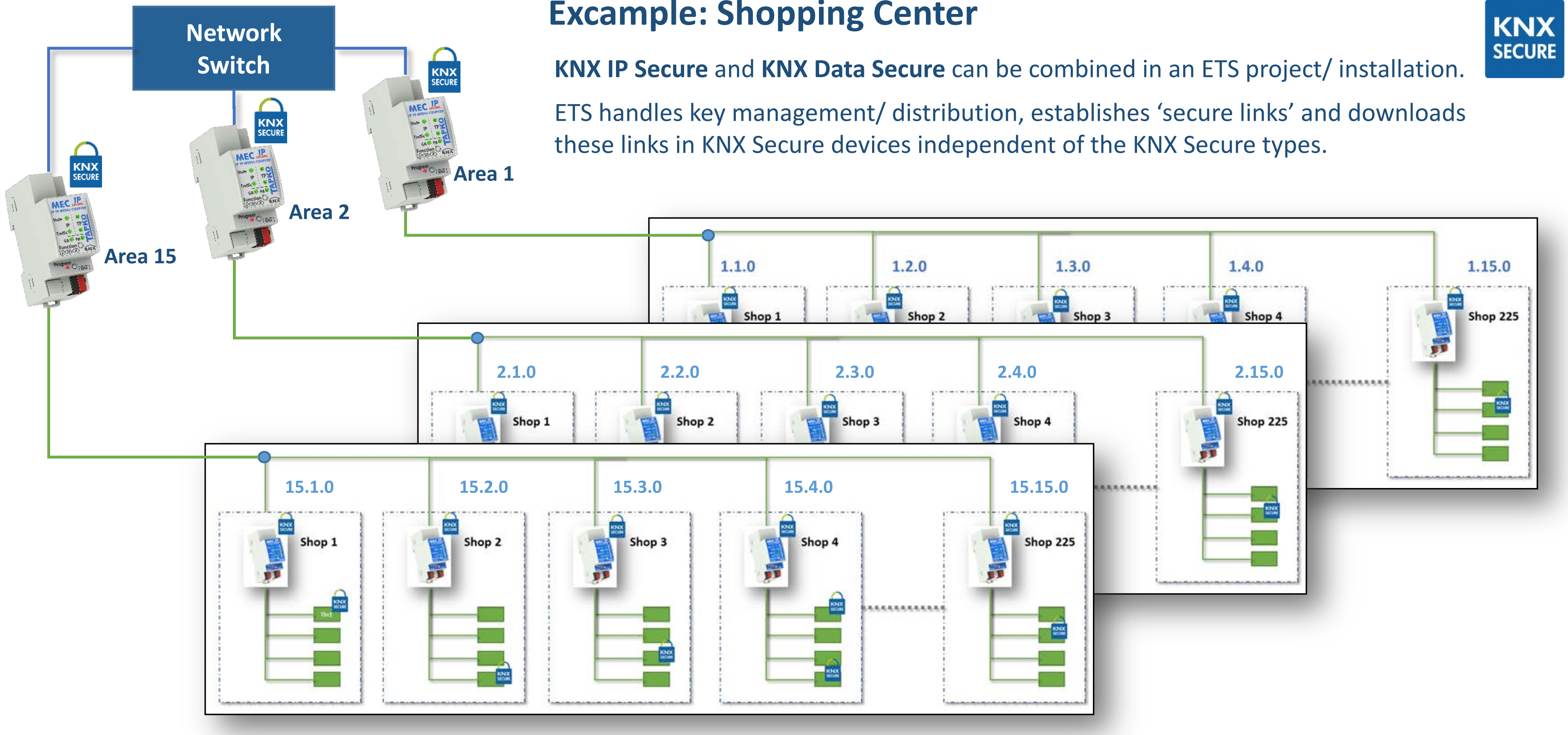
15 x 15 = 225 Rooms in one «KNX World» possible

IP Secure and Data Secure – where to use it

Excample: Shopping Center

KNX IP Secure and **KNX Data Secure** can be combined in an ETS project/ installation.

ETS handles key management/ distribution, establishes 'secure links' and downloads these links in KNX Secure devices independent of the KNX Secure types.



Our OEM Portfolio – your new devices

Successful Start to the KNX World with our OEM devices

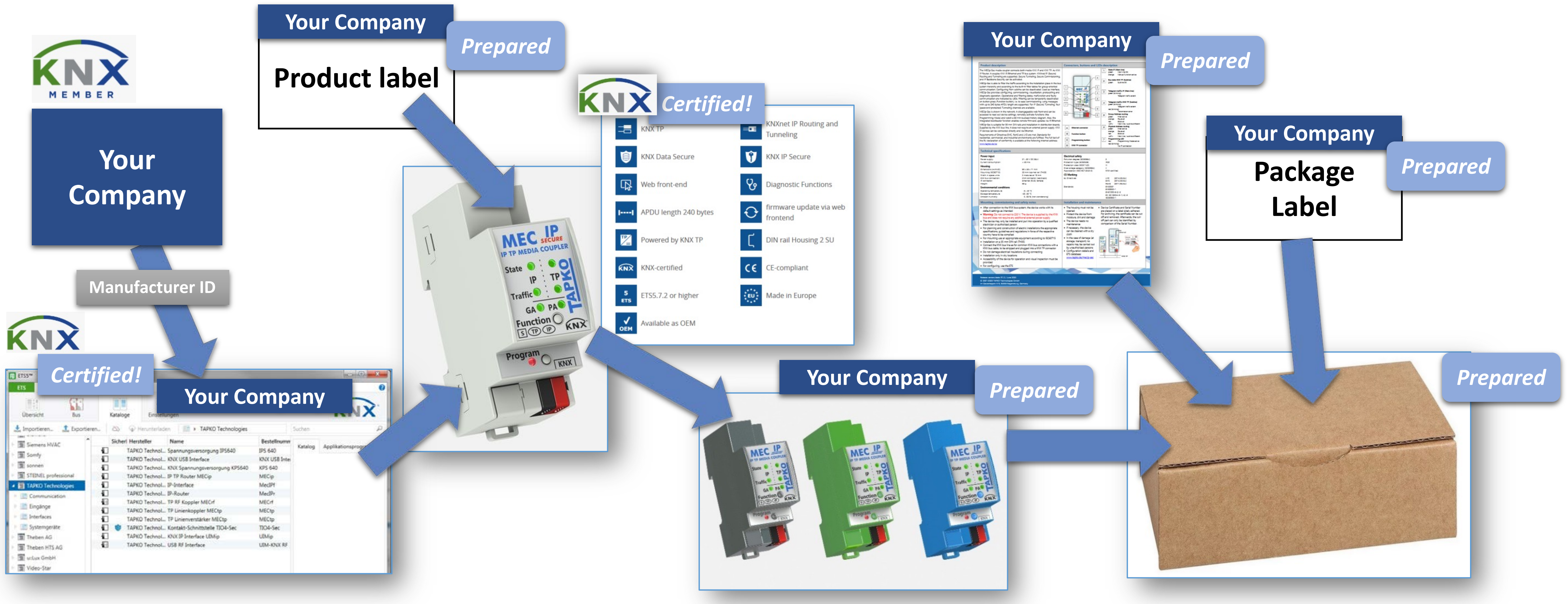
For the OEM products, the entire process is optimized, and of course for the best price / performance ratio.

Overview of the advantages of OEM products:

- KNX Certification and Testing done!
- Case available in different colors
- Device labeling on customer request
- Instruction leaflet can be printed and enclosed
- Packing and other services as required
- Device can be adapted or configured
- ETS database entries exist and can be individualized on customer request
- Serial numbers and keys can be assigned within the customer's specified number range
- No own certification necessary
- Complete service for OEM devices as ready goods-in-store
- Complete service provider from A to Z

TAPKO TECHNOLOGIES GMBH

Your easy way to TAPKO OEM-Products



ETS5™

Übersicht | Bus | Kataloge | Einstellungen

Importieren... Exportieren... Herunterladen ▸ TAPKO Technologies Suchen

Siemens HVAC
Somfy
sonnen
STEINEL professional
TAPKO Technologies
Communication
Eingänge
Interfaces
Systemgeräte
Theben AG
Theben HTS AG
u::Lux GmbH
Video-Star

Sicherl	Hersteller	Name	Bestellnumm
	TAPKO Technol...	Spannungsversorgung IPS640	IPS 640
	TAPKO Technol...	KNX USB Interface	KNX USB Inte
	TAPKO Technol...	KNX Spannungsversorgung KPS640	KPS 640
	TAPKO Technol...	IP TP Router MECip	MECip
	TAPKO Technol...	IP-Interface	MecIPf
	TAPKO Technol...	IP-Router	MecIPr
	TAPKO Technol...	TP RF Koppler MECrf	MECrf
	TAPKO Technol...	TP Linienkoppler MECtp	MECtp
	TAPKO Technol...	TP Linienverstärker MECtp	MECtp
	TAPKO Technol...	Kontakt-Schnittstelle TIO4-Sec	TIO4-Sec
	TAPKO Technol...	KNX IP Interface UIMip	UIMip
	TAPKO Technol...	USB RF Interface	UIM-KNX RF

Katalog | Applikationsprog

- KNX TP
- KNX Data Secure
- Web front-end
- APDU length 240 bytes
- Powered by KNX TP
- KNX-certified
- ETS5.7.2 or higher
- Available as OEM
- KNXnet IP Routing and Tunneling
- KNX IP Secure
- Diagnostic Functions
- firmware update via web frontend
- DIN rail Housing 2 SU
- CE-compliant
- Made in Europe

UIMip-Sec – KNX IP Interface Secure

KNX USB Interface Secure – Encryption on IP Communication
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 unauthorized reading of the telegrams.

IP SECURITY

SECURE

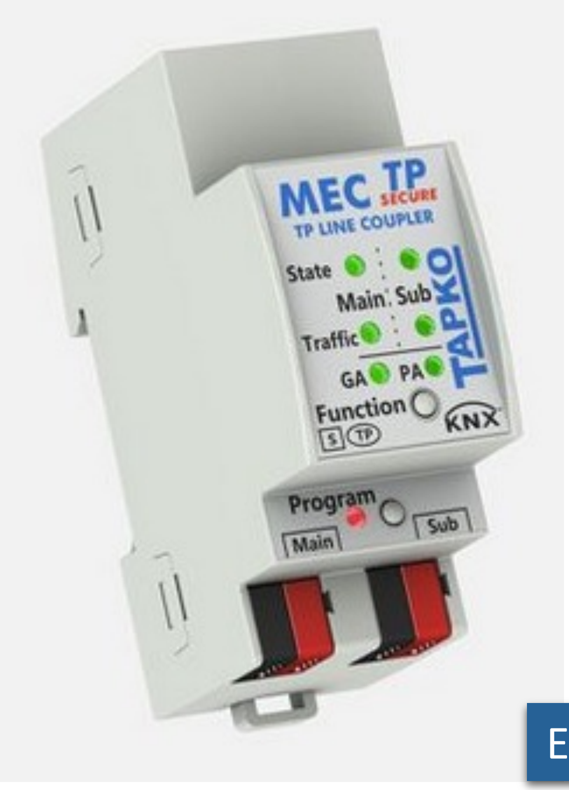
Web front-end

Features

- KNX Secure IP Protocol
- KNX IP Tunneling
- KNX Data Secure
- KNX IP Secure
- Web front-end for Diagnostic and Firmware update
- APDU length 240 Bytes
- Powered by KNX TP
- 4 KNXnet/IP Tunnelling connections
- low power consumption

MECtp-sec - KNX Line/Area Coupler Secure

KNX Line/Area Coupler secure
Used as KNX Line/Area Coupler, MECtp connects a main line and a subline to enable KNX communication between both KNX TP lines. MECtp-Sec supports the "Secure Commissioning" option. When activated, the configuration communication is encrypted by KNX Data Secure.



DATA SECURITY

SECURE

ETS6 Segment Coupler

Features

- various routing filter for group and individual telegrams
- support of long telegrams
- temporary disabling of routing filter via button
- blocking of configuration on upper lines from sub line
- multi colour LEDs show status information
- various ACK and repetition settings
- integrated ACK generator
- ***Prepared for Segment coupler functionality (available with ETS6)***

MECip-sec - KNX IP Router Secure

KNX IP Router secure with routing and tunneling interface
MECip-Sec supports the "Secure Commissioning" option. When activated, the configuration communication is encrypted by KNX Data Secure. Especially for system components, this kind of configuration protection is tremendously important.

Main task of MECip-Sec is protecting the whole KNX IP line from unwanted access. On activation of the "IP Backbone Security" function - only possible with usage of KNX IP Secure Routers- MECip-Sec encrypts the complete communication on KNX IP by KNX IP Secure.

IP SECURITY

SECURE

Web front-end

ETS6 Segment Coupler

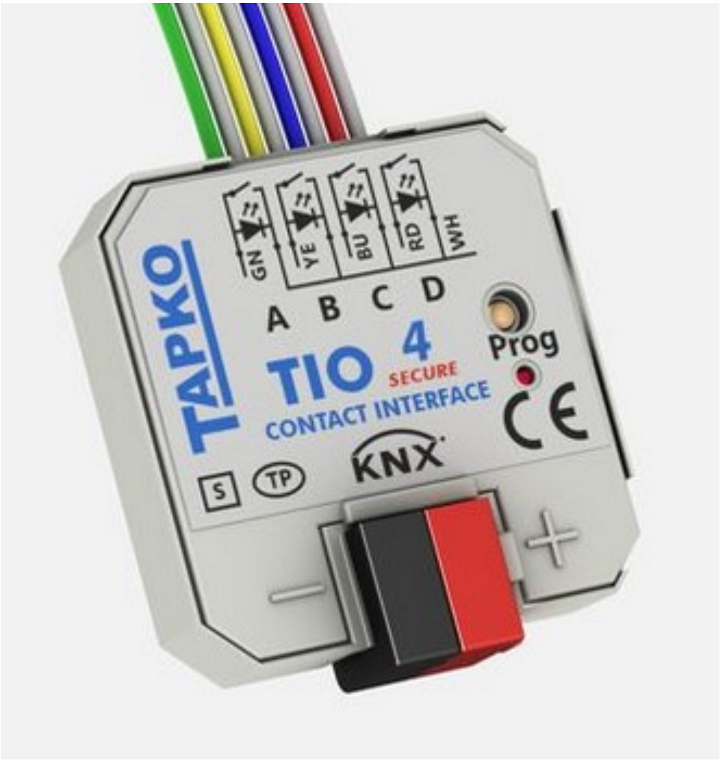
Features

- Secure Commissioning and IP Backbone Security activation
- Secured runtime communication by data encryption
- KNXnet/IP secure Routing
- 4 KNXnet/IP secure Tunnelling connections
- support of long telegrams
- power supply via KNX TP
- low power consumption
- Web front-end for status and diagnostics
- various routing filter for group and individual telegrams
- various ACK and repetition settings
- temporary disabling of routing filter via button
- blocking of configuration on upper lines from sub line
- multi colour LEDs show status information
- integrated ACK generator
- ***Prepared for Segment coupler functionality (available with ETS6)***

TIO4 – KNX Push Button Interface Data Secure

KNX push button interface 4 fold secure with status outputs

TIO4-Sec now also supports KNX Data Secure. The channels of TIO4-sec can be used as output to connect status LEDs.
To drive loads like status LEDs, channels can be operated also as outputs. LED´s brightness and night/day operation can be parametrized. Suitable for sensing potential-free contacts, TIO4-Sec provides the standard input functions for connecting push buttons, conventional switches and contact sensors to KNX.



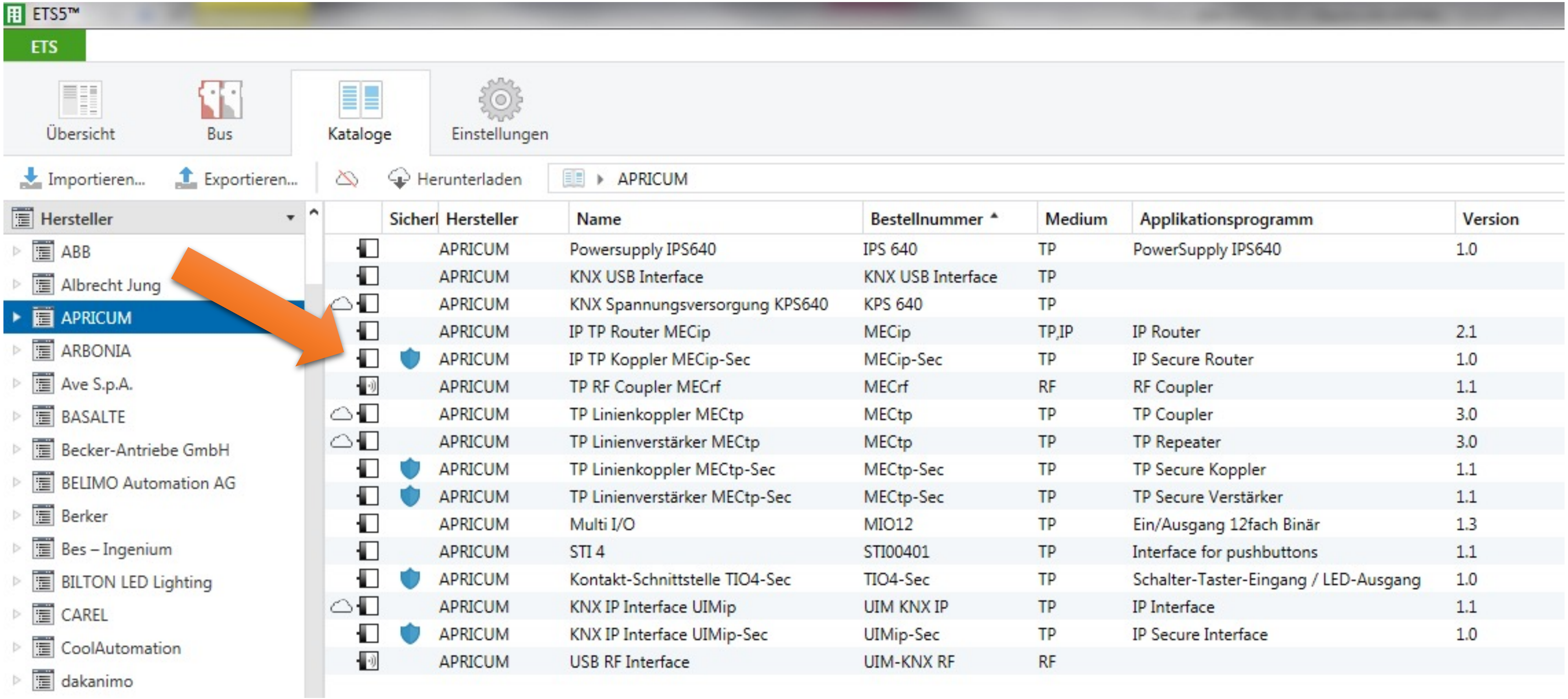
DATA SECURITY

SECURE

Features

- Small dimensions
- connect classic push-buttons
- Suitable for flush mounting
- Detection of short and long push
- independent configuration of each channel
- 4 Channel Pushbutton Interface
- 1 or 2 Button Shutter / Dimming operation
- various input functionality (switch, dimming, counter, …)
- Inputs can be configured as dimmable outputs to drive status LEDs

KNX Secure Applications



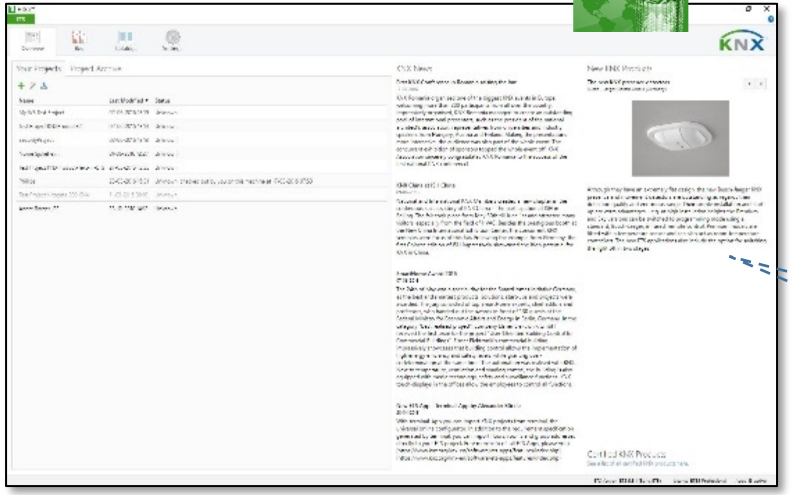
Hersteller

- ABB
- Albrecht Jung
- APRICUM
- ARBONIA
- Ave S.p.A.
- BASALTE
- Becker-Antriebe GmbH
- BELIMO Automation AG
- Berker
- Bes – Ingenium
- BILTON LED Lighting
- CAREL
- CoolAutomation
- dakanimo

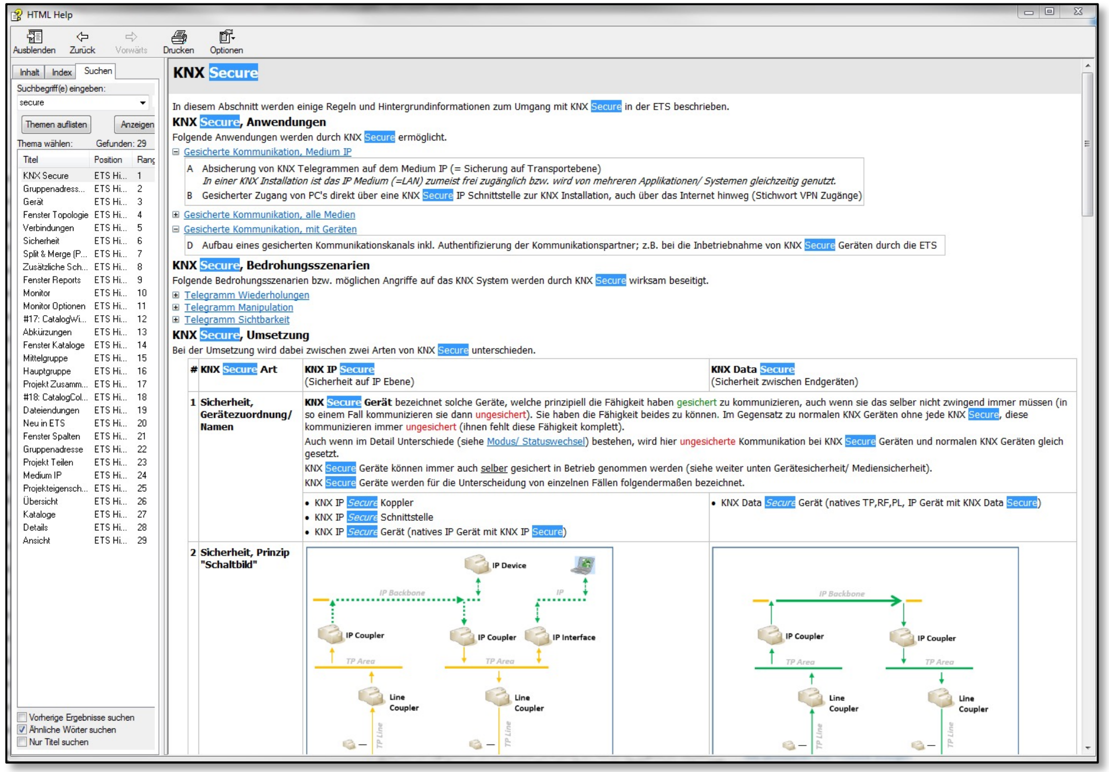
	Sicherl	Hersteller	Name	Bestellnummer	Medium	Applikationsprogramm	Version
		APRICUM	Powersupply IPS640	IPS 640	TP	PowerSupply IPS640	1.0
		APRICUM	KNX USB Interface	KNX USB Interface	TP		
☁		APRICUM	KNX Spannungsversorgung KPS640	KPS 640	TP		
		APRICUM	IP TP Router MECip	MECip	TP,IP	IP Router	2.1
	🛡	APRICUM	IP TP Koppler MECip-Sec	MECip-Sec	TP	IP Secure Router	1.0
		APRICUM	TP RF Coupler MECrf	MECrf	RF	RF Coupler	1.1
☁		APRICUM	TP Linienkoppler MECtp	MECtp	TP	TP Coupler	3.0
☁		APRICUM	TP Linienverstärker MECtp	MECtp	TP	TP Repeater	3.0
	🛡	APRICUM	TP Linienkoppler MECtp-Sec	MECtp-Sec	TP	TP Secure Koppler	1.1
	🛡	APRICUM	TP Linienverstärker MECtp-Sec	MECtp-Sec	TP	TP Secure Verstärker	1.1
		APRICUM	Multi I/O	MIO12	TP	Ein/Ausgang 12fach Binär	1.3
		APRICUM	STI 4	STI00401	TP	Interface for pushbuttons	1.1
	🛡	APRICUM	Kontakt-Schnittstelle TIO4-Sec	TIO4-Sec	TP	Schalter-Taster-Eingang / LED-Ausgang	1.0
☁		APRICUM	KNX IP Interface UIMip	UIM KNX IP	TP	IP Interface	1.1
	🛡	APRICUM	KNX IP Interface UIMip-Sec	UIMip-Sec	TP	IP Secure Interface	1.0
		APRICUM	USB RF Interface	UIM-KNX RF	RF		

KNX Secure Information: Helpfile ETS5 (Press F1)

ETS Professional



Press F1



Suchbegriff(e) eingeben: secure

Thema wählen: Gefunden: 29

Titel	Position	Rang
KNX Secure	ETS Hi...	1
Gruppenadress...	ETS Hi...	2
Gerät	ETS Hi...	3
Fenster Topologie	ETS Hi...	4
Verbindungen	ETS Hi...	5
Sicherheit	ETS Hi...	6
Split & Merge (P...	ETS Hi...	7
Zusätzliche Sch...	ETS Hi...	8
Fenster Reports	ETS Hi...	9
Monitor	ETS Hi...	10
Monitor Optionen	ETS Hi...	11
#17: CatalogWi...	ETS Hi...	12
Abkürzungen	ETS Hi...	13
Fenster Kataloge	ETS Hi...	14
Mittelgruppe	ETS Hi...	15
Hauptgruppe	ETS Hi...	16
Projekt Zusamm...	ETS Hi...	17
#18: CatalogCol...	ETS Hi...	18
Dateiendungen	ETS Hi...	19
Neu in ETS	ETS Hi...	20
Fenster Spalten	ETS Hi...	21
Gruppenadresse	ETS Hi...	22
Projekt Teilen	ETS Hi...	23
Medium IP	ETS Hi...	24
Projekteigensch...	ETS Hi...	25
Übersicht	ETS Hi...	26
Kataloge	ETS Hi...	27
Details	ETS Hi...	28
Ansicht	ETS Hi...	29

☐ Vorherige Ergebnisse suchen
☑ Ähnliche Wörter suchen
☐ Nur Titel suchen

KNX Secure

In diesem Abschnitt werden einige Regeln und Hintergrundinformationen zum Umgang mit KNX Secure in der ETS beschrieben.

KNX Secure, Anwendungen

Folgende Anwendungen werden durch KNX Secure ermöglicht.

⊟ Gesicherte Kommunikation, Medium IP

A Absicherung von KNX Telegrammen auf dem Medium IP (= Sicherung auf Transportebene)
In einer KNX Installation ist das IP Medium (=LAN) zumeist frei zugänglich bzw. wird von mehreren Applikationen/ Systemen gleichzeitig genutzt.

B Gesicherter Zugang von PC's direkt über eine KNX Secure IP Schnittstelle zur KNX Installation, auch über das Internet hinweg (Stichwort VPN Zugänge)

⊞ Gesicherte Kommunikation, alle Medien

⊟ Gesicherte Kommunikation, mit Geräten

D Aufbau eines gesicherten Kommunikationskanals inkl. Authentifizierung der Kommunikationspartner; z.B. bei die Inbetriebnahme von KNX Secure Geräten durch die ETS

KNX Secure, Bedrohungsszenarien

Folgende Bedrohungsszenarien bzw. möglichen Angriffe auf das KNX System werden durch KNX Secure wirksam beseitigt.

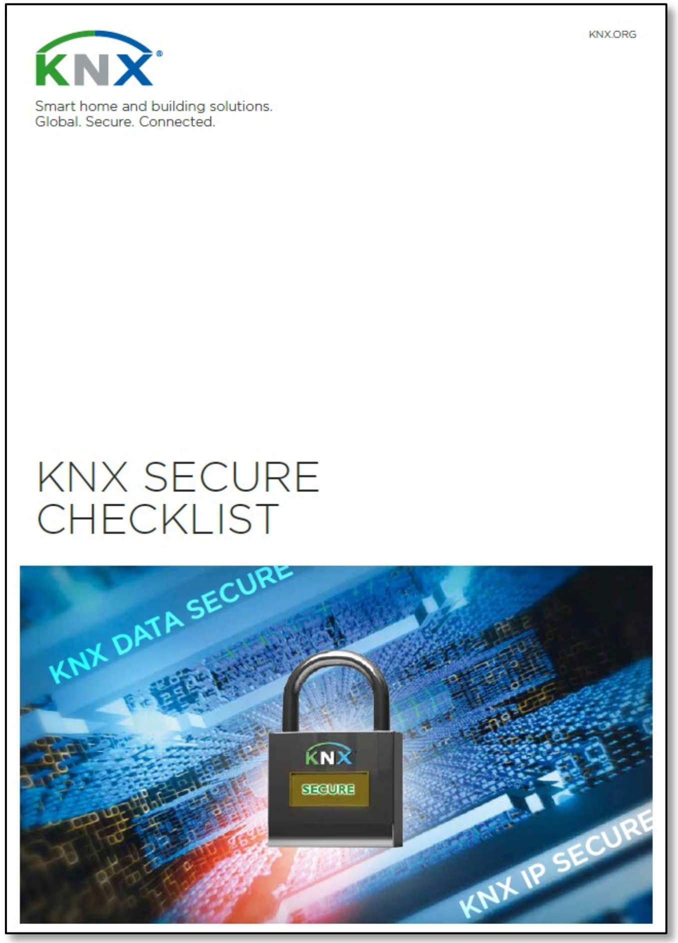
⊞ Telegramm Wiederholungen
⊞ Telegramm Manipulation
⊞ Telegramm Sichtbarkeit

KNX Secure, Umsetzung

Bei der Umsetzung wird dabei zwischen zwei Arten von KNX Secure unterschieden.

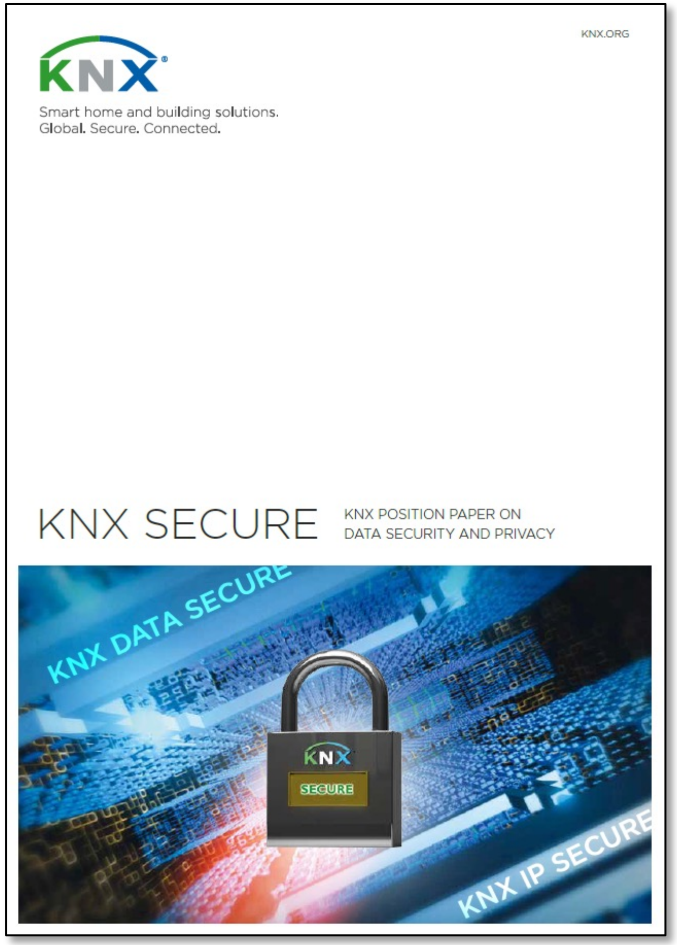
#	KNX Secure Art	KNX IP Secure (Sicherheit auf IP Ebene)	KNX Data Secure (Sicherheit zwischen Endgeräten)
1	Sicherheit, Gerätezuordnung/ Namen	**KNX Secure Gerät** bezeichnet solche Geräte, welche prinzipiell die Fähigkeit haben gesichert zu kommunizieren, auch wenn sie das selber nicht zwingend immer müssen (in so einem Fall kommunizieren sie dann ungesichert). Sie haben die Fähigkeit beides zu können. Im Gegensatz zu normalen KNX Geräten ohne jede KNX Secure, diese kommunizieren immer ungesichert (ihnen fehlt diese Fähigkeit komplett). Auch wenn im Detail Unterschiede (siehe Modus/ Statuswechsel) bestehen, wird hier ungesicherte Kommunikation bei KNX Secure Geräten und normalen KNX Geräten gleich gesetzt. KNX Secure Geräte können immer auch selber gesichert in Betrieb genommen werden (siehe weiter unten Gerätesicherheit/ Mediensicherheit). KNX Secure Geräte werden für die Unterscheidung von einzelnen Fällen folgendermaßen bezeichnet.	
		• KNX IP Secure Koppler • KNX IP Secure Schnittstelle • KNX IP Secure Gerät (natives IP Gerät mit KNX IP Secure)	• KNX Data Secure Gerät (natives TP,RF,PL, IP Gerät mit KNX Data Secure)
2	Sicherheit, Prinzip "Schaltbild"		

KNX Secure Information: Helpful Information


KNX.ORG

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

KNX SECURE
CHECKLIST


KNX.ORG

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

KNX SECURE

KNX POSITION PAPER ON
DATA SECURITY AND PRIVACY

Downloads & Informations

TAPKO TECH NEWS 2020 (english) 2 MB
TAPKO TECH NEWS 2020 (chinese) 2 MB
TAPKO Brochure (german) 4 MB
TAPKO Brochure (english) 4 MB
TAPKO Brochure (chinese) 4 MB

Website Link - https://www.tapko.de/brochures

Watch our film on the core topic OEM

TAPKO
TECHNOLOGIES GMBH

Thank you for your attention.

Questions ?

Peter Sperlich
peter.sperlich@tapko.de
Phone: +49 160 9550 1452