



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



KNX Secure Solutions

KNX Secure offers maximum protection



400+ certified KNX Secure devices already and counting!

KNX Secure Solutions 2022- Services to change the world

The growing demand for IoT devices, such as smart radiator-valves or smart speakers, which react to your voice, and external services from providers, such as facility managers and security companies, have made their way into the world of smart homes and smart buildings.

But digitalisation and the growing networking also constitute an increased risk of hacking attempts, cyberattacks and unauthorised manipulation. The challenge therefore is to allow the homeowner to integrate the newest devices and services, whilst taking appropriate and imperative protective measures, especially for critical functions within each facility. An approach that covers all levels simultaneously is essential for comprehensively protecting against internal and external attacks.

The importance of security for the integration of external services

Service providers have created a new market, which extends the functionality of each home or building. It is a setup that is external to a KNX system, that generally involves human or AI intervention as a result of data received from the KNX system. For example, an external carer could be alerted to a problem with a vulnerable person thanks to KNX sensors and alarms within the home and could then take remedial action. By including external services, we open a whole new world, which will tremendously contribute to comfort and safety for the users. At the same time, we make ourselves more vulnerable as we integrate external elements to our KNX installation. Creating a door for hackers to tamper with a KNX installation requires the highest level of protection, which KNX Secure offers. Thanks to KNX IP Secure, no hacker will be able to tamper with the KNX installation from outside, whereas from inside, KNX Data Secure does the rest to protect the installation from tampering from the inside.

KNX Secure offers maximum protection

Home and building automation with KNX natively offer security on multiple levels. With the rising demand for stronger security features, the KNX Technology was extended by KNX Secure, the industry leading security mechanisms in the world of smart homes and smart buildings. KNX Secure 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) 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.

KNX Secure with services in action - Use-cases

Especially when it comes to an application in the real world, the importance of security is put in a special focus, emphasising the need for an impenetrable installation. The following examples will showcase the integration of external services with KNX Secure in action.

1

The KNX Smart Home with KNX Secure

Especially when it comes to an application in the real world, the importance of security is put in a special focus, emphasising the need for an impenetrable installation. The following examples will showcase the integration of external services with KNX Secure in action.

Task

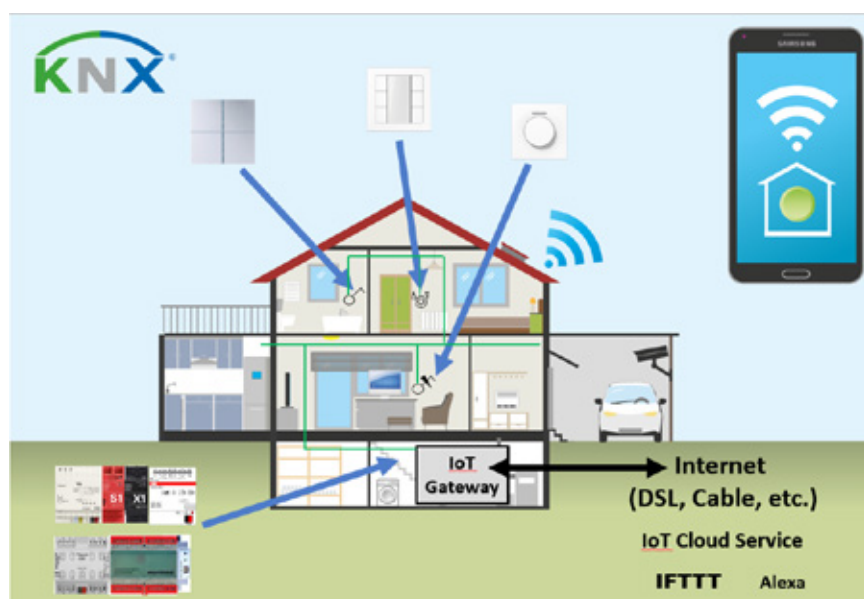
Smart homes offer a variety of solutions for the home owner, which do not only contribute to a higher sophistication, but foremost elevate the home' level of comfort. Combined with KNX Secure, the KNX smart home is the perfect solution for everyone. The panel by Matthias Weber impressively shows the full potential, by directly addressing new comers in the field.

Solution

The panel features a classic KNX installation with REG distribution, operating devices and simulated consumers. A multi-actuator controls light and drivers, as well as an universal dimmer, blind actuator and the visualisation. The highlight is the integration of typical functions from the IoT world and KNX Secure.

The panel clearly shows the required devices for a KNX installation and how the functions are put into practice. With simple solutions for switching and dimming of lighting, room temperature control and blind control, the outcome is not

only the understanding of a KNX installation's basics, but also the limitless potential of KNX through scene control with dimming value, blind position and room temperature. The installation's sophistication is underlined by the servers Gira X1 and Gira S1, which allow the usage of KNX Secure as well as the connection to the world of IP. Not only is the highest level of security guaranteed but additional solutions, such as geofencing can easily be implemented through IFTTT, which uses the position data of the smartphone to automatically trigger actions when leaving or returning to the home. On top of that, the smartphone, respectively the tablet can be used for controlling and visualisation of functions. The HOOC gateway serves as an alternative IoT gateway for a secure connection between the KNX installation and the Internet. KNX provides users with a reliable home automation system with high investment security. The solution highlights that basic functions can be easily extended for more comfort and complemented with IT as well as the highest available security standards for smart homes and smart buildings.



KNX Certified Devices	Devices for (external) Service	Apps and Gateways
ABB: Universal dimming actuator UD/S 2.300.2 Basalte: SENTIDO KNX 200-02 / V3.1 ISE: SMART CONNECT KNX Remote Access Jung: 6-Fold push button sensor, Rotary sensor DS 4092 TS Theben: Power supply 640mA T Zennio: Multi function actuator MAXinBOX 8 v3	Hooc: Fernzugriff via GSM IFTTT: IoT Service	Gira: Gira S1, Gira X1

2

Ambient Assisted Living with KNX Offline Voice Control

Task

Smart homes of today allow the users to have all building functions under control. This becomes not only an additional benefit to the house but a necessity for occupants with disabilities. With the solution by Katja Schuster from company EAB Elektroanlagenbau GmbH Rhein/Main and Marco Koyné from company Koyné System Elektronik, KNX demonstrates its potential, when it comes to add unique features to your home to facilitate the needs of people with need for assistance.

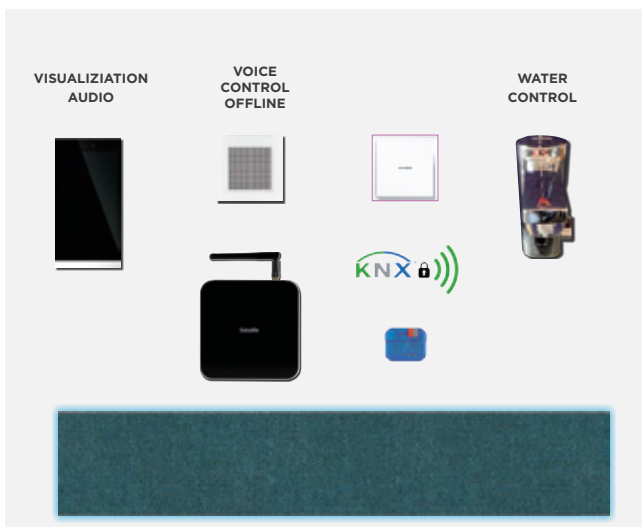
Solution / Implementation / Benefits

Highlighted by a touch panel, which allows to control the entire real estate, the comfort of the smart home surfaces immediately. Lighting, shutters, HVAC and all other solutions can be controlled from a single room with the touch of a finger. To further address the needs of impaired users, water supply can be controlled through the same system. Enhanced energy efficiency comes with a smart home installation, but brought to the next level thanks to visualisation, which stores the consumption data and present it to the home user. Because energy savings start with the consumer. Not only due to the growing demand, but also to further facilitate the need of comfort for reasons of convenience but

also for assisted living requirements, the presented solution integrates a full functioning voice control. Key here is the offline support of the voice control, which provides multiple benefits. Not only is the smart home protected from any kind of network failure, which can result in threatening situations, but the unique voice control also guarantees the highest possible privacy by keeping all information inside the house. The voice control is supported by state-of-the-art devices such as Amazon's Alexa or Google Assistant.

The special feature of the solution in regards of assisted living, which again reflects the suitability of KNX for people with disabilities, is the sanitary and temperature monitoring, realising a hygienic disinfection against legionella. This does not only represent an additional layer of assisted living solution, it also shows once again the limitless is created by connecting to KNX.

The whole presentation is topped off with the use of KNX Data Secure, which encrypts the entire communication in the house, making it physically as well as virtually impenetrable. Thanks to KNX IP Secure, remote access can be established, allowing to make modifications by only authorised users, hence allowing the highest level of comfort according to individual requirements.



KOYNE
SYSTEM ELEKTRONIK

KNX Certified Devices

Enertex:

KNX LED dimming sequencer 20A/5x with KNX Data Secure

ISE:

SMART CONNECT KNX Remote Access

Jung:

Flush-mounted actuator single-fold 23001 1S U with KNX Data Secure

Lingg und Janke:

Push Button 2-fold flush mounted with KNX Data Secure

Devices for (external) Service

Franke-Aquarotte:

ECC control with water tap

Basalte:

Elli Touchpanel

Apps and Gateways

Gira:

Gira S1 for secured remote access

ProKNX:

ARAGON-Offline Voice Control

3

Services for distributed Facilities – KNX Secure Inside

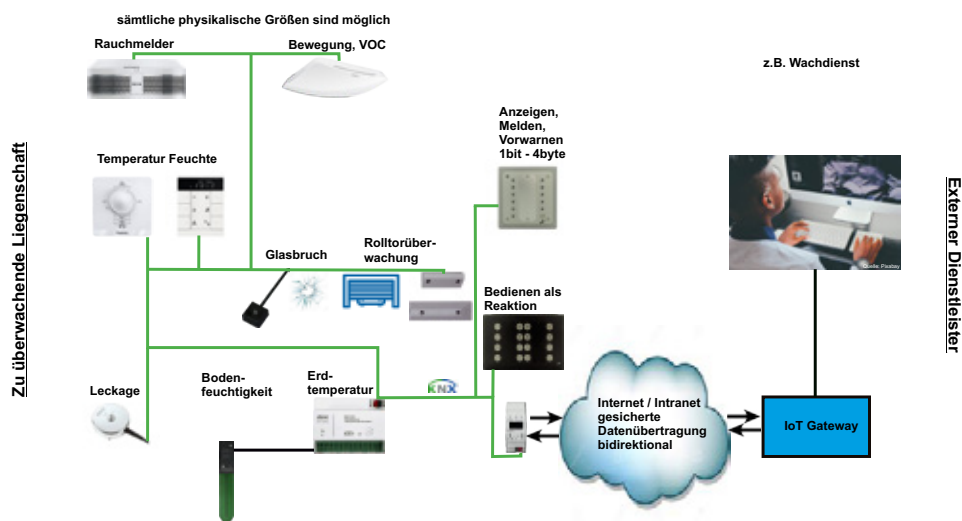
Task

With the growing importance of smart energy management, buildings are more and more required to communicate its statuses amongst one another to guarantee the best possible usage of renewable resources for all KNX controlled functions in the building. The more facilities are connected, the higher the requirements for external facility managers, who can check the conditions of the KNX installation, without actually having a KNX installation at their place of work. Needless to say that also for the integration of remote facility services, a cybersecurity protection is crucial to guarantee that the facility manager can see the real-time status. The solution by Mr. Dirk Müller from GePro Gesellschaft für Prozesstechnik mbH impressively shows how distributed facilities can easily be managed by external facility managers through a secured IP communication.

Solution / Implementation / Benefits

The solution displays the recording of physical values such as temperature (°C), air quality (VOC), carbon dioxide (CO₂) and humidity as well as the monitoring of the security technology such as smoke detectors, leakage and glass breakage sensors, earth leakage circuit-breakers and motion detectors. If critical states are achieved or alarms are triggered, they are routed to a service provider. The network is in the public domain and exposed possibly exposed to unauthorised tampering. The connection between the properties and the service provider is therefore protected via KNX IP Secure router.

A KNX control and alarm panel on site indicates critical variables both optically as well as acoustically and switching operations can be carried out directly in the installation via a KNX control panel. The whole KNX installation is protected by KNX Secure, implemented in two IP Secure routers by different manufacturers as well as by the usage of KNX Data Secure within the buildings. The service provider, who does not have its own KNX installation can exchange data securely, via integration of services. This occurs for example using a PC and visualisation, with tablets and smartphone. It is possible to not only monitor and process physical variables as well as convert critical values into fault signals, but central functions for lighting, roller blinds, ventilation etc. can also be triggered. Thanks to KNX, the managing of distributed facilities through external service providers can seamlessly be integrated. This allows the monitoring of properties situated in different locations by only one central service provider. The whole communication, from inside the building all the way from outside the building is secured with KNX Data Secure, which prevents unauthorised penetration within the building, as well as KNX IP Secure, which encrypts the IP telegram once it leaves the building to communicate with other facilities, respectively with the facility manager. Due to the direct connectivity between the external facility manager with the buildings, quick reactions to technical errors, faults and alarms can be guaranteed, thanks to the remote operation possibilities of selected central functions.



KNX Certified Devices

ABB:
IP-Router secure IPR/S

Elsner:
Leckagesensor Leak KNX 70315

Enertex:
KNX-IP-Router secure

Jung:
Secure PB 1fold LS CD; 10911ST,
2-fold 10921 ST,
Power supply 160mA 20160 REG

GePro:
Alarmtableau MAT, KNX4, KNX-Tableau 16

Devices for (external) Service

GePro:
Alarmtableau MAT, KNX4, KNX-Tableau 16

Meanwell:
Power supply 1280 mA with surveillance
and diagnose

Steinel:
True Presence Multisensor KNX

Theben:
AMUN 716 SKNX 7169230
Power supply 160mA 20160 REG

Weinzierl:
KNX IO 511.1 secure

Gira:
Smoke Alarm Dual Q with KNX-Modul 233602+234300

4

Energy Management and Charging Services – KNX Secure Inside

Task

Mobile charging stations for batteries as part of a smart home are large consumers and demand an intelligent management of the charging currents. To realise this, the smart homes is required to react through flexible energy and charging management. Furthermore, the integration of third-party systems and devices through KNX gateways is required as well as the visualisation of the electrical consumption, the generated energy, the capacity of the battery station, the charging state, the range of an electric vehicle and corresponding statistics of external IoT services. To prevent any kind of intrusion by burglars or car-jackers, an impenetrable security of the installation from within and outside is the highest requirement. These energy management, charging and security challenges are the focus of the example by Peter Sperlich from the Swiss company Smart Building Design GmbH.

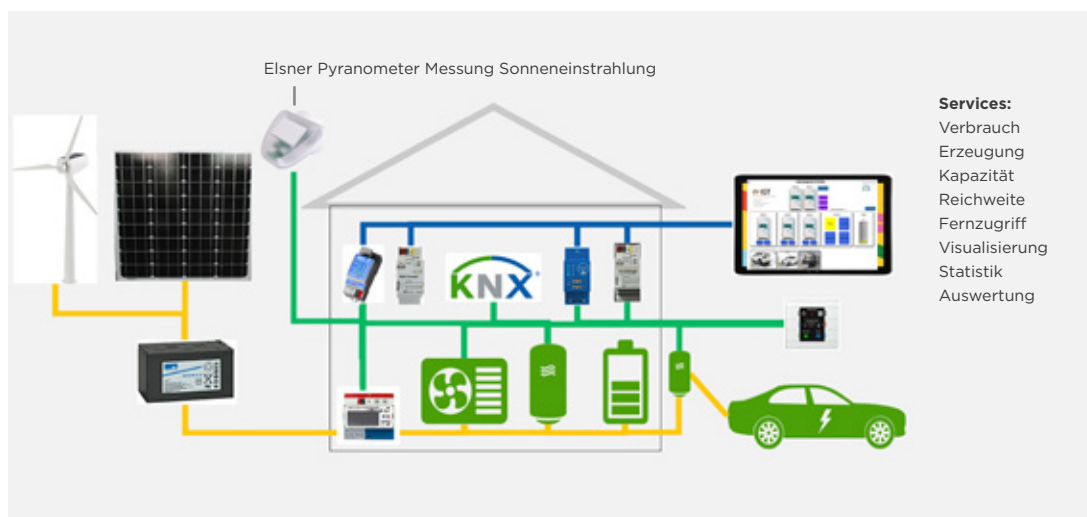
Solution / Implementation / Benefit

The current generation of the energy self-sufficient home is carried via photovoltaics and wind energy. The energy is also stored. The current power consumption in the house is dynamically adapted to the charging state of the energy store and the solar radiation. A KNX electricity meter records the current total consumption. The use of a KNX IP Secure router guarantees the securely encrypted data communication on the IP network between KNX-TP and the visualisation. The energy store is linked to KNX via a gateway and transmits the current charging state and further values. The remote access module enables secure VPN access, which

adds a further layer of security to the installation. An additional gateway secures the data exchange with the charging pole, which signals with red or green light “charged” or “not charged”. This demonstrates the functionality of the complete system. It can be shown using an iPad or iPhone and influenced at the touch of a button. Using adaptive calculation, it is possible to optimise the use of the electrical energy and the charging response of the energy store dependent on the weather forecast of the next 3-5 days.

The data transfer between the individual decentralised systems is carried out with KNX TP and IP. The protection of the installation against unauthorised tampering is realised through KNX Data and KNX IP Secure as well as a VPN connection. The visualisation shows the current data of the decentralised KNX devices as well as external systems. Depending on whether there is sufficient energy available in the battery, it is charged if required or individual systems are switched in order of priority.

The display of the consumption data shows users how much electrical energy they can save and where they can be cost-effective. Furthermore, the display of energy store data indicates the current charging states, allowing users to take appropriate decisions. Thanks to the simple integration of external services, the installation is not only limited to one technology, but can easily and securely integrate any kind of solution using KNX IP Secure interfaces. To add a further level of protection, the whole communication is additionally secured through VPN hardware as well as KNX Data Secure devices



KNX Certified Devices	Devices for (external) Service	Apps and Gateways
<p>Apricum d.o.o: MECip Secure KNX IP Secure router</p> <p>Elsner Elektronik: KNX pyranometer</p> <p>Lingg & Janke: KNX Secure flush mount push button 4fold</p>	<p>Alexander Maier: Eisbaer Visualisation Server</p> <p>Hooc AG: VPN Module Connect H LT M</p> <p>Lingg & Janke: REG meter EMU</p>	<p>ise: Connect module for E3DC energy store as well as e-charge module for charging pole</p>

5

Tenant Electricity Billing for Alternative Energies

Task

One of the major advantages of smart metering is the transmission of consumption data to the energy provider for an exact billing procedure. However, especially when various alternative sources, such as photovoltaic, wind, water, etc. are used, the metering of the consumed, respectively generated electricity, can turn out to over-complicate the whole topic, turning the advantage to a disadvantage. On top of that, as consumption data is classified as critical data, unauthorised access must be prevented at any cost.

Thanks to KNX, the cost of enjoying the benefits of smart meters in combination with the highest available security is very straightforward, as the panel by Andreas Berg, from the Swiss-based company InnoEnergy GmbH is showcasing

Solution / Implementation / Benefits

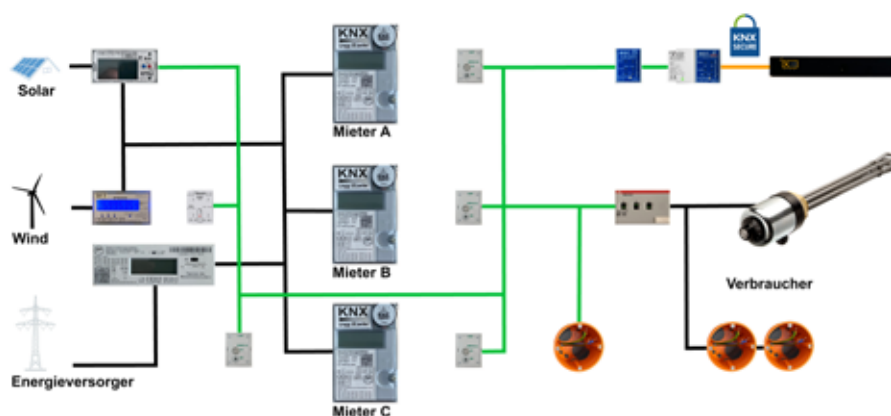
The panel addresses tenants of rentals as well as property owners, who do not only create liveable spaces, but foremost smart homes of the highest standards. Each apartment unit is equipped with various lines, consisting of KNX Data Secure

and non-secure devices. The connection to the visualisation is realised through a KNX IP Secure.

Highlight is not only the availability of KNX in each unit, but foremost the including of various renewable energy sources and their according metering as well as the control of surplus energy. Thanks to KNX Secure, the data can be transmitted according to the highest security standards, guaranteeing the prevention of any unauthorised access.

Furthermore, KNX allows the extracting, analysing and transmitting of data from various meters, unifying the world of smart meters for the greatest reliability and comfort of the home users.

Altogether, the solution by Andreas Berg impressively shows that KNX can be used for the greater good of multiple tenants, especially when it comes to the integration and metering of renewable energy sources, and especially the secured transmission of data within the KNX installation, thanks to KNX Data Secure and outside via KNX IP Secure.



KNX Certified Devices

ABB:
SE/S 3.16.1 (3-Fach Energie-Schaltaktor)

Apricum:
MEC IP Secure (IP-Secure-Koppler)
MEC PS (TP Line Koppler mit 640 mA PS)

Lingg & Janke:
Sens2-Q mit IR-Kopf (Gateway IR-Zähler)
Energy Meter Standard 3/5 KNX (3-Phasen Stromzähler)

Tense:
ZPS 160M PS (160 mA PS)

Devices for (external) Service

EMH metering:
eHZ-PW8E2AUL0HQ10
eBZD-W2EV-0L-HL0-000001-G50/Q2
Grid-Meter

InnoEnergy:
X2B Visualisation Server

Apps and Gateways

Lingg & Janke:
Sens2-Q mit IR-Kopf (Gateway IR-Zähler)
ZRX-KCI4S0 (Gateway 4 * S0-Zähler)



Join us
www.knx.org