KNX Association cvba
De Kleetlaan 5 bus 11
B-1831 Brussels-Diegem
Belgium

Tel.: +32 (0) 2 775 85 90
Fax: +32 (0) 2 675 50 28

info@knx.org
www.knx.org

Press Release

KNX Secure – Secured KNX Communication

KNX IP Secure and KNX Data Secure provide secured access to KNX Installations.

BRUSSELS / FRANKFURT, 14th of March 2016: They exist – the hackers – who intrude in building technology. Jesters switch on the lights at the neighbor's and boast of it. However, criminal energy and related know-how can cause immense damage. Therefore KNX Security is a red-hot subject. Already up to now KNX complies with the security requirements, as long as installers of Home and Building Control take care of the recommended protective measures against manipulations. Yet, new media like LAN and WLAN with internet access, wireless operation concepts and applications in sensible areas increase the risk of damage by unwanted intruders. According to these but also to other requirements KNX has developed new security concepts: KNX Data Secure and KNX IP Secure. Both of them are based on worldwide established security protocols and can be integrated seamlessly into existing KNX systems.

The possibility to remotely control KNX installations via the internet and/or via the wireless network WLAN requires additional protective measures. Due to the access to devices and media exists the risk of manipulation of the data traffic. Thus it is necessary to protect the transmitted information on each medium (KNX TP, PL, RF, IP) against modification or logging telegrams and repeating them in a manipulating way from outside. The remote access to a KNX bus system via the internet should be secured in such a way, that the operation and the configuration of bus devices can only be done by verifiable authorized persons. It is an effective protective mechanism against manipulation if bus devices can only communicate with each other when they recognize themselves a part of the bus system. According to these and other requirements KNX has developed new security concepts: KNX Data Secure and KNX IP Secure. Both use mechanisms which are e.g. used for the secure data transmission between electricity meters and utility companies.

Encrypted Telegrams

If data have to be sent via the internet the connection between the sending and receiving network can be protected by a virtual private network (VPN). Yet, this does not ensure, that the sender is authorized to configure the bus system or to exchange data with it. Here KNX IP Secure offers additional security by extending the KNX IP protocol in such a way that the transmitted data are completely encrypted. This can be realized even in existing installations with little effort.

If data have to be transmitted via KNX only locally, it is sufficient to protect the data by an extension of the bus protocol. The specified protection mechanism KNX Data Secure authentifies and/or encrypts selected KNX telegrams independent of the medium. The keys are allocated to the devices resp. to the objects via ETS. As in one KNX system secured and unsecured applications are possible, it is not necessary to secure all devices. Also existing system components have not to be replaced. Such the effort is kept low and the investment in the KNX bus technology is ensured.

Security Protocol worldwide established
In future the newly specified protection mechanisms KNX Data Secure and KNX IP Secure will allow the creation of secured communication channels between KNX participants. Thus the infiltration of manipulated messages in order get control of the system can be inhibited. For this purpose each message is equipped with an authentification code. The automatic allocation of sequence numbers resp. the sequence identification prevents from the attempt to log data and to re-transmit it later on for sabotage purposes. Finally the encryption of the data traffic makes the KNX installation almost invulnerable. The procedure is based on worldwide established security protocols.

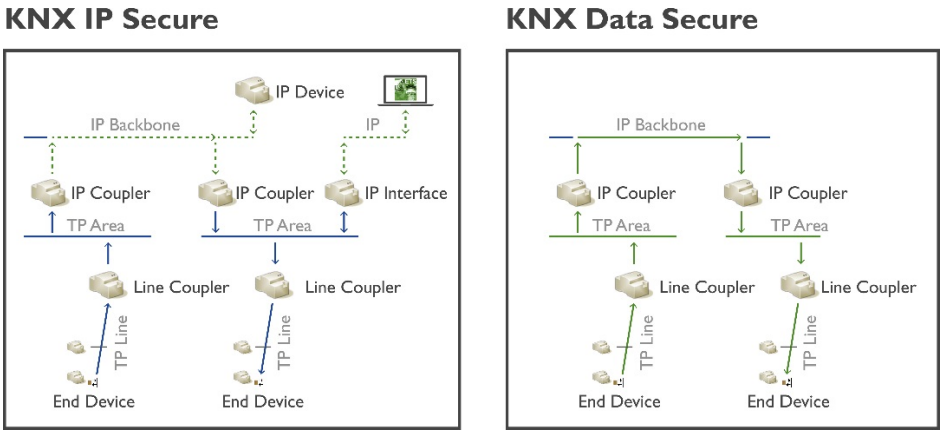
Introduction with ETS 5.5
Last but not least planners, installers and system integrators have to pay attention, that hackers do not have any chances. They have to become familiar with the protection measures and to apply them. While handing over the system as well as by periodic verification of the running system the envisaged security level can be ensured. The new security functions, especially for the access via the internet, can be applied to existing systems by using interfaces with the new KNX security mechanisms. KNX IP Secure and KNX Data Secure will be supported by the new ETS 5.5 planning and commissioning software.

Futher information:
Further information on the subject KNX security can be found on our website under Download -> Marketing -> Flyer (http://www.knx.org/knx-en/downloads/index.php)

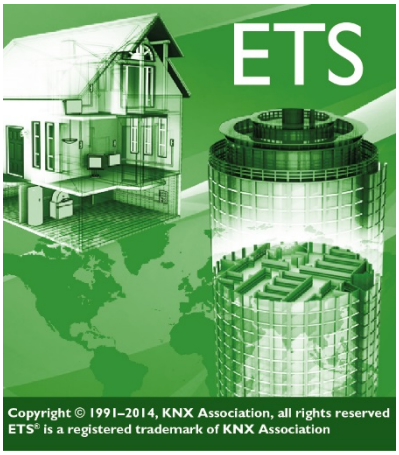
- KNX Security Checklist
- KNX Security Position paper

The complementary webinar „KNX Security“ informs you currently on the required protection measures for your KNX installation. Registration under:

http://www.knx.org/knx-de/schulung/knxeacademy/webinars/index.php



Pic. 1: KNX IP Secure for secured KNX transmission between buildings
KNX Data Secure secured KNX transmission within the building



Pic. 2: KNX IP Secure and KNX Data Secure are available with the ETS 5.5.

About KNX
KNX Association is the creator and owner of the **KNX** technology – the worldwide STANDARD for all applications in home and building control, ranging from lighting and blind control to various security systems, heating, ventilation, air conditioning, monitoring, alarming, water control, energy management, smart metering as well as household appliances, audio/video and many more. **KNX** provides a single, manufacturer independent design and commissioning tool (ETS), with a complete set of supported communication media (TP, PL, RF and IP) as well as a complete set of supported configuration modes (system and easy mode). **KNX** is approved as a European (CENELEC EN 50090 and CEN EN 13321-1) and an International standard (ISO/IEC 14543-3). This standard is based upon 25 years of experience in the market. Over 400 member companies worldwide from different application domains have more than 7000 KNX certified product groups in their catalogues. The **KNX** Association has partnership agreements with almost 50,000 installer companies in more than 138 countries.

www.knx.org

For more information / material please contact: heinz.lux@knx.org

Pictures can be downloaded at: www.knx.org/news-press/press-room