
# KNX Zabezpečení

## Přehled

# Obsah

**Obsah** ..... Chyba! Záložka není definována.

**1 Úvod** ..... Chyba! Záložka není definována.

**2 Zabránění přístupu k síti na různých fyzických médiích KNX....** Chyba! Záložka není definována.

2.1.1 Úvod ..... **Chyba! Záložka není definována.**
2.1.2 Montáž kabelů a přístrojů ..... **Chyba! Záložka není definována.**
2.1.3 Kroucený pár ..... **Chyba! Záložka není definována.**
2.1.4 Powerline ..... 3
2.1.5 Radiofrekvenční ..... **Chyba! Záložka není definována.**
2.1.6 IP ..... 4
2.1.7 Internet ..... 4

**3 Omezení nežádoucí komunikace uvnitř sítě** ..... Chyba! Záložka není definována.

**4 Ochrana komunikace při konfiguraci** ..... Chyba! Záložka není definována.

**5 Ochrana provozní komunikace** ..... **5**

**6 Propojení KNX se zabezpečovacími systémy** ..... **9**

**7 Detekce neautorizovaných přístupů ke sběrnici** ..... **9**

**8 Dodržování nařízení EU GDPR** ..... **10**

**9 Literatura** ..... **10**

# 1 Úvod

Tento dokument slouží jako vodítko jak pro elektroinstalatéry, tak i pro výrobce KNX, aby se seznámili s aktuálními opatřeními, která mohou být učiněna pro zvýšení bezpečnosti instalací KNX

# 2 Zabránění přístupu k síti na různých fyzických médiích KNX

### 2.1.1 Úvod

Vhodná koncepce zabezpečení je založena na zajištění řádné prevence před neoprávněným přístupem. V případě instalace KNX to znamená, že pouze oprávněné osoby (elektroinstalatér, správce, uživatel) mají fyzický přístup k instalaci KNX. Při navrhování a instalaci, pro každé KNX médium, musí být kritické prvky chráněny co možná nejlepším způsobem.

### 2.1.2 Montáž kabelů a přístrojů

- Obecně platí, že zařízení a přístroje musí být řádně připevněny, aby se zabránilo, že by mohly být snadno odstraněny a tím by byl umožněn přístup k instalaci KNX neoprávněným osobám.
- Kryty a rozvaděče obsahující KNX přístroje musí být řádně uzavřeny nebo musí být namontovány v místnostech, do nichž mají přístup pouze oprávněné osoby.
- Ve venkovních prostorách musí být přístroje namontovány v dostatečné výšce (např. meteorologická stanice, snímač větru, snímač pohybu, atd.).
- Ve všech nedostatečně kontrolovaných veřejných prostorách využívat klasické přístroje propojené s binárními vstupy uloženými v chráněných oblastech (např. v rozvaděčích) anebo tlačítková rozhraní skrytá v hlubokých krabicích, což je určitá prevence před nežádoucím přístupem ke sběrnici.
  Pokud možno, využít opatření proti demontážím některých aplikačních modulů (např. mechanické zabezpečení aplikačních modulů šrouby, možnost sejmutí pouze nástroji, nutnost použití nadměrné síly k sejmutí a podobná opatření).

### 2.1.3 Kroucený pár

- Konce kabelů by neměly být viditelné, visící vně na stěnách, ani na výstupech nebo uvnitř budovy.
- Kabel sběrnice ve venkovním prostoru představuje vyšší riziko. Fyzický přístup ke KNX kroucenému páru musí být v tomto případě ještě obtížnější než uvnitř bytu nebo domu.
- Pro dodatečnou ochranu přístrojů instalovaných v místech s omezeným dohledem (venku, v podzemních parkovištích, na WC, atd.) mohou být připojeny k samostatné linii. Aktivací filtrační tabulky v liniové spojce potom může být zabráněno přístupu hackera k celé instalaci.

### 2.1.4 Powerline

- Elektronické filtry by měly být použity k filtrování příchozích i odchozích signálů.

### 2.1.5 Radiofrekvenční

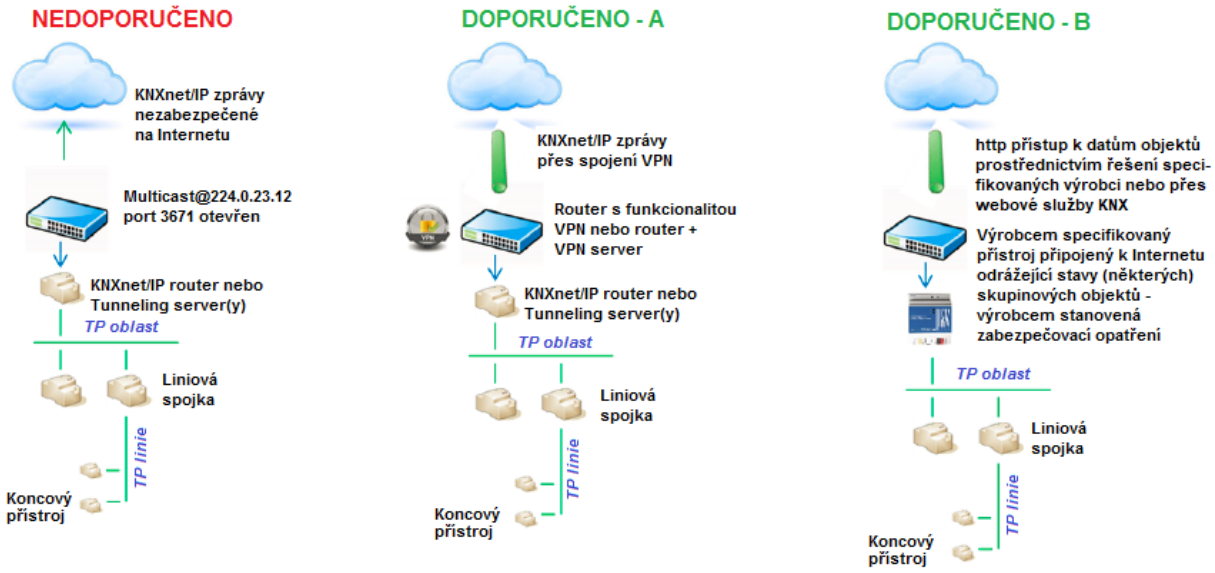
- Jelikož radiofrekvenční přenos je otevřené médium, nelze přijmout opatření *fyzické* ochrany pro zabránění přístupu. Proto je zapotřebí přijmout jiná opatření, která jsou uvedena v článcích 3 až 6 (a zejména ta která jsou uvedena v článku 5).

### 2.1.6 IP

- Automatizace budov by měla běžet přes vyhrazený LAN a WLAN s vlastním hardwarem (routery, přepínače, atd.).
- Bez ohledu na typ instalace KNX, musí se v každém případě dodržovat obvyklé ochranné mechanismy pro IP sítě. Ty mohou zahrnovat:
  - MAC filtry
  - Šifrování bezdrátových sítí ve spojení se silnými hesly (změna výchozího hesla – WPA2 nebo vyšší) a ochrana proti neoprávněným osobám.
  - Změna výchozí SSID (SSID je název, pod kterým je bezdrátový přístupový bod viditelný v síti, většinou výrobce a typ výrobku). Výchozí SSID může poukázat na s výrobkem spojené slabiny použitých přístupových bodů, čímž tak mohou být zvláště citlivé na hackery). Přístupový bod může být kromě toho nastaven tak, že je zabráněno periodickému přenosu mezi jiné SSID.
- Pro KNX IP multicast musí být použita jiná IP adresa jako výchozí (224.0.23.12). Vhodnou adresu lze dohodnout se správcem sítě.
- IT síťoví specialisté se budou podílet na větších projektech s připojením ke KNXnet / IP: takto bude možné optimalizovat konfiguraci sítě (řiditelné přepínače, VLAN, přístupové body podle IEEE802.X atd.) a mohou být využity další mechanismy na ochranu jako filtrování e-mailů a antivirus.

### 2.1.7 Internet

- KNXnet / IP routing a KNXnet/ IP tunneling nejsou určeny k použití prostřednictvím internetu. Proto není vhodné otevřít porty routerů k internetu a tím KNX komunikaci učinit viditelnou přes internet.
  - Instalace (W) LAN musí být chráněna firewallem.
  - Není-li nutný jakýkoli externí přístup k instalaci, výchozí rozhraní může být nastaveno na hodnotu 0 a takto zablokovat veškerou komunikaci s internetem.
- Přeje-li si někdo realizovat přístup k instalaci přes internet, pak to může být uskutečněno následujícím způsobem:
  - Zajištění přístupu k instalaci KNX prostřednictvím připojení VPN: To však vyžaduje router, který podporuje funkce serveru VPN nebo přímo server s funkcemi VPN.
  - Některá z jednoúčelových řešení specializovaných výrobců, která jsou na trhu a vizualizace (např. umožnění přístupu http).
  - V KNX bylo specifikováno rozšíření standardu KNX o standardní řešení KNX s přístupem k instalacím KNX přes internet prostřednictvím webových služeb.



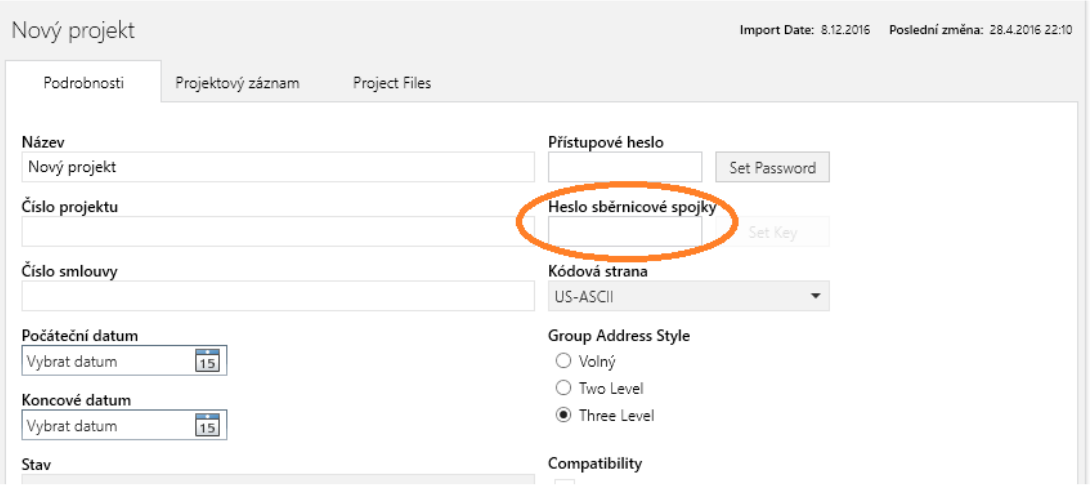

Obr. 1: Přístup k sítím KNX přes Internet

# 3 Omezení nežádoucí komunikace uvnitř sítě

- Individuální adresy přístrojů musí být řádně přiřazeny v souladu s topologií a routery musí být nakonfigurovány tak, aby nemohly předávat zprávy s neodpovídajícími zdrojovými adresami. Takto lze nežádoucí komunikaci omezit na jednu linii.
- Je potřebné zablokovat komunikaci typu Point-to-Point a případnou nefiltrovanou komunikaci přes routery. Tímto způsobem může být rekonfigurace opět omezena na jedinou linii. Spojky musí být nakonfigurovány tak, aby měly aktivní filtrační tabulky a nepřenášely skupinové adresy nepoužívané v příslušných liniích. Pokud by tomu tak nebylo, nežádoucí komunikace v jedné linii by nesla riziko nekontrolovaného šíření zpráv po celé instalaci KNX.

# 4 Ochrana komunikace při konfiguraci

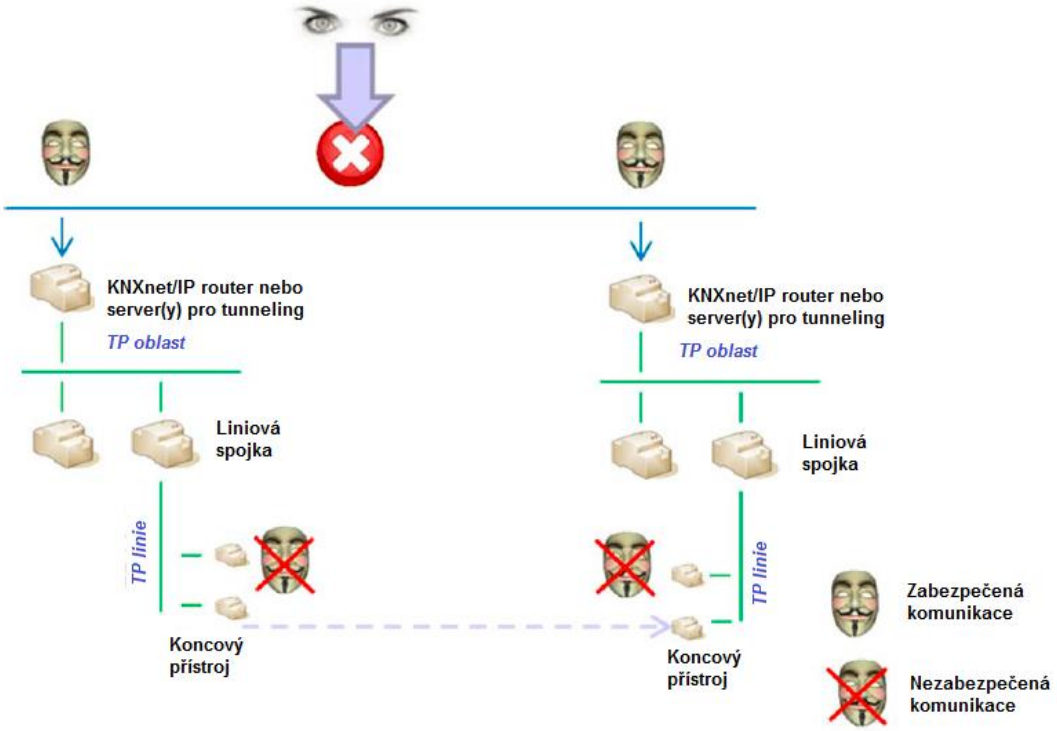
- ETS umožňuje definovat heslo pro konkrétní projekt, jehož prostřednictvím lze uzamknout přístroje před neoprávněným přístupem. Tím se zabrání, aby konfiguraci instalace bylo možné číst nebo měnit neoprávněnými osobami.




Obr. 2: Ochrana před konfigurační komunikací v ETS

# 5 Ochrana provozní komunikace

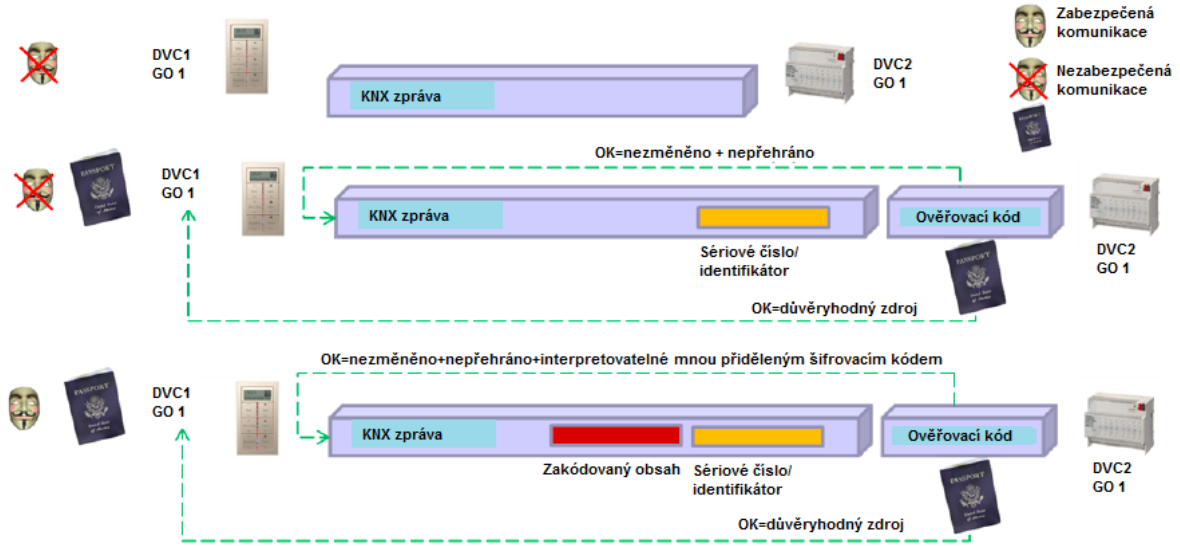
- Následně k předchozím opatřením, lze KNX provozní komunikace chránit využitím
  - Zabezpečením KNX dat
  - Mechanismy KNX IP Secure
- KNX Data Secure zajišťuje, že bez ohledu na přenosové KNX médium, vybrané zprávy odesílané KNX přístroji mohou být ověřovány anebo také šifrovány.
  Aby bylo zajištěno, že i v případě, kdy by taková komunikace nebyla zajištěna a takové sítě by byly propojeny s IP, byly definovány výše zmíněné mechanismy KNX IP Secure.
  Takto je zajištěno, že KNX IP tunneling nebo routing zpráv nelze zaznamenávat ani s nimi manipulovat na IP. KNX IP Secure mechanismus zajistí přidání bezpečnostní obálky ke kompletnímu datovému provozu KNXnet / IP.




Obr. 3: Ochrana KNX provozní komunikace na síti IP s využitím KNXnet IP Secure

- KNX Data Security a KNX IP Secure mechanismy zajišťují, aby:
  přístroje mohly vytvořit zabezpečený komunikační kanál a tím zajistit:
  - *Integrita dat,* tj. zabránění tomu, aby útočník získal kontrolu vložením manipulovaných rámců. V KNX je to zajištěno připojením **ověřovacího** kódu ke každé zprávě: tento připojený kód umožňuje ověření, že zpráva nebyla změněna a že pochází od důvěryhodného komunikačního partnera.
  - *Aktuálnost*, tj. zabránění útočníkovi nahrávání rámců a jejich pozdějšího přehrávání bez manipulace s obsahem. V KNX Data Security je toto zajištěno sekvenčním číslem a v KNX IP Secure identifikátorem sekvence.
  - *Důvěryhodnost*, tj. šifrování komunikace po síti k zajištění toho, že útočník má co nejmenší možný pohled na skutečně přenášená data. Při povolení **šifrování** KNX síťového provozu přístroje KNX zajistí šifrování alespoň podle algoritmů AES-128 CCM spolu se symetrickým klíčem.

Symetrickým klíčem rozumíme, že stejný klíč používá odesílatel k ochraně odchozí zprávy (ověření + důvěryhodnost!), jakož i v přijímači(ích) k ověření při příjmu této zprávy.

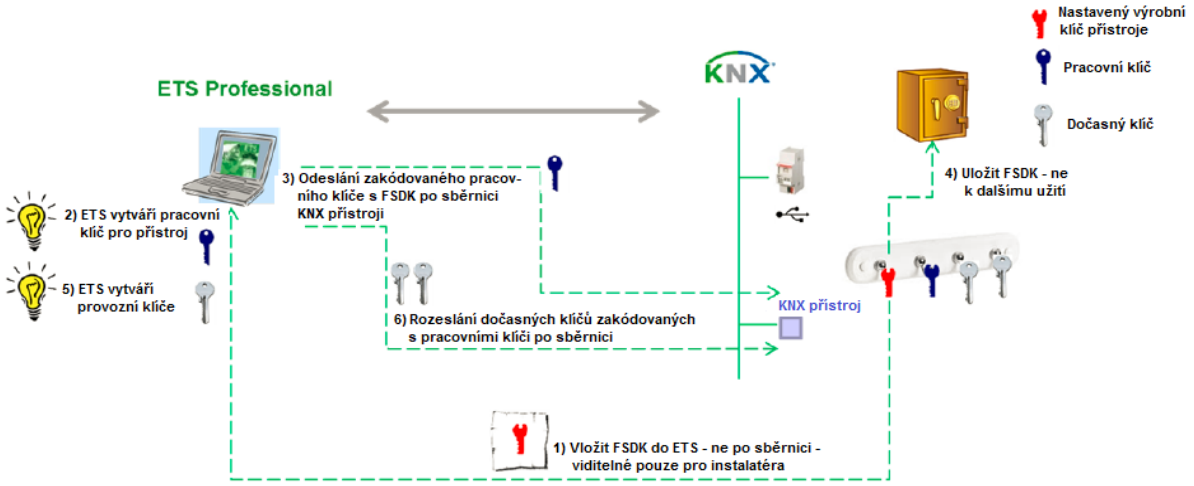



Obr. 4: Přehled mechanismů KNX Data Security

Přístroje KNX Data Secure používají při přenosu ověřených a šifrovaných dat delší formát telegramu KNX. To nemá vliv na reakční rychlost přístrojů.

V KNX Data Secure jsou přístroje chráněny následujícím způsobem:

- Přístroj se dodává s jedinečným nastaveným výrobním klíčem přístroje (FDSK).
- Instalatér vkládá tento FDSK do konfiguračního nástroje ETS (tuto akci ale v žádném případě nelze uskutečnit po sběrnici)).
- Konfigurační nástroj vytváří pro přístroj specifický pracovní klíč.
- ETS po sběrnici odešle přístroji, který má být konfigurován tento pracovní klíč, avšak s využitím šifrování a ověření zprávy s předem zadanou FDSK. Ani nástroj ani klíč FDSK nejsou nikdy obsaženy v přenášeném prostém textu na sběrnici.
- Přístroj od tohoto okamžiku přijme pouze pracovní klíč pro další konfiguraci s ETS. FDSK se při následné komunikaci již nepoužívá, pokud přístroj není resetován do výchozího výrobního stavu.
- ETS vytváří dočasné klíče (kolik jich je zapotřebí) pro skupinovou komunikaci, kterou je nutné zabezpečit.
- Přístroji, který má být konfigurován odesílá ETS o sběrnici tyto dočasné klíče, ovšemže při využití šifrování a ověřování zpráv pracovním klíčem. Dočasné klíče nejsou nikdy přenášeny po sběrnici ve formátu prostého textu.



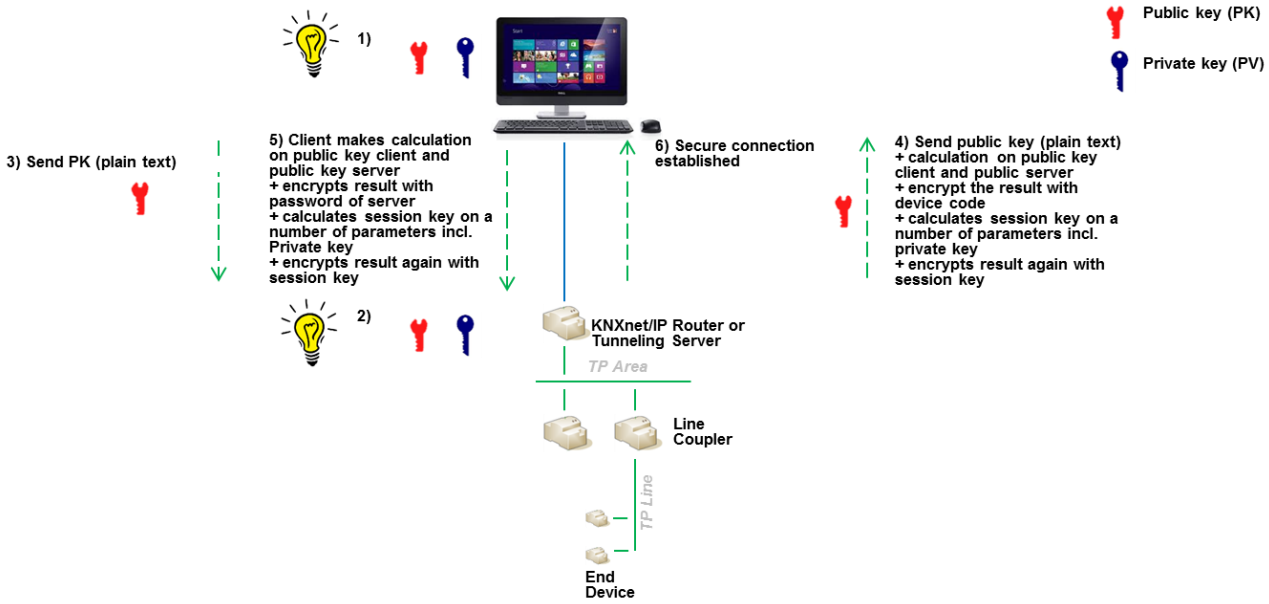

Obr. 5: Proces zabezpečení KNX přístrojů

Pro KNX IP Secure, zabezpečené připojení (Tunneling nebo Device Management) je stanoveno následujícím způsobem:

- Jak klient, tak i server vytvoří individuální veřejný / soukromý pár klíčů. To se označuje jako asymetrické šifrování.
- Klient pošle svůj veřejný klíč na server jako prostý text.
- Server odpoví s veřejným klíčem v prostém textu, který je přiložen k výsledku následujícího výpočtu: vypočtená hodnota XOR serveru veřejného klíče pomocí veřejného klíče klienta, zašifruje se kódem přístroje pro ověření klienta a zašifruje se podruhé s vypočteným klíčem relace.

  Ověřovací kód přístroje je buď přiřazen z ETS během konfigurace, nebo je to pracovní klíč. Tento ověřovací kód přístroje musí být poskytnut provozovateli vizualizace, která má být bezpečně propojena s příslušným serverem.
- Klient uskuteční stejnou operaci XOR, ale ověřuje se sám šifrováním, a to nejprve s jedním z hesel serveru a ještě podruhé s klíčem relace.
  Je třeba poznamenat, že použitý šifrovací algoritmus (Diffie Hellmann) zajišťuje, aby klíč relace klienta a serveru byly shodné.

  Hesla serveru musí být poskytována provozovateli vizualizace, když chce navázat bezpečné spojení s příslušným serverem.




Obr. 6: Nastavení KNX IP Secure spojení

Pokud jde o výše popsaná opatření k ochraně probíhající komunikace, je potřebné poznamenat, že:

- KNX Secure přístroje lze používat bez jakýchkoli problémů společně s “klasickými” KNX přístroji. To znamená, že KNX Data a IP Secure lze využít jako dodatečné bezpečnostní opatření.
- Pokud se instalatér rozhodne pro použití přístrojů KNX IP Secure v IP páteřní linii, musí být všechny IP spojky v této páteřní linii typu KNX IP Secure.
- Pokud instalatér - na přání zákazníka - má použít k funkci KNX Secure přístroj pro zabezpečení probíhající komunikace, musí každý komunikační partner tohoto přístroje také podporovat funkci KNX Secure pro propojenou funkci. Jinými slovy, komunikační objekt přístroje KNX Secure nemůže být současně propojen se zabezpečenou skupinovou adresou i s nezabezpečenou skupinovou adresou.

Přístroje, které podporují KNX Data a IP Secure, lze odlišit od "klasických" přístrojů KNX, protože na štítku produktu je zobrazen symbol "X".

KNX IP Secure a KNX Data Secure jsou podporovány od ETS 5.5 výše. ETS umožňuje konfigurovat nové KNX Secure přístroje a také dovoluje výměnu chybných přístrojů KNX Secure.

# 6 Propojení KNX se zabezpečovacími systémy

Připojení KNX k takovým aplikacím, jakými jsou zabezpečovací systémy proti vloupání / požární ochrana / vstupní dveřní systémy, lze zajistit:

- KNX přístroji nebo rozhraními s příslušnou certifikací místních pojišťoven;
- bezpotenciálovými kontakty (binárními vstupy, tlačítkovými rozhraními apod.);
- odpovídajícími rozhraními (jako RS232) nebo hradly: v takovémto případě musí být zajištěno, aby KNX komunikace nespustila příslušné funkce zabezpečení v zabezpečovací části instalace.

# 7 Detekce neautorizovaných přístupů ke sběrnici

- Je samozřejmé, že sběrnici lze monitorovat a tak vysledovat neobvyklý provoz.

- Přístroje KNX Secure uchovávají přehled o cestách průniků v protokolech o chybách zabezpečení: takto je možné kdykoli zkontrolovat, zda instalace KNX byla předmětem bezpečnostních útoků.
- Některé typy přístrojů mohou detekovat, zda jiný přístroj nevysílá telegramy s jejich individuální adresou. To není samovolně oznámeno v síti, ale lze to načíst z PID_DEVICE_CONTROL.
- Právě nedávná implementace se může projevit již v PID_DOWNLOAD_COUNTER. Porovnáním čtení hodnoty (periodického) s referenční hodnotou bude signalizována změna v konfiguraci přístroje.

# 8 Dodržování nařízení EU GDPR

- GDPR je zkratkou pro General Data Protection Regulation (viz http://www.eugdpr.org/). Cílem nařízení je harmonizace zákonů na ochranu údajů v celé Evropě.
- Pro splnění nařízení GDPR, instalatér má zákazníkovi předat soubor s projektem z ETS. Instalační technik a zákazník také podepíší prohlášení o ochraně údajů.
- Data, která jsou generována KNX přístroji, mohou být používána pouze pro účely dálkového ovládání přístrojů zákazníkem (prostřednictvím App), pro diagnostické účely a pro další vývoj produktu. Nemohou být použita pro personalizovanou publicitu.

# 9 Literatura

[1] AN 158 KNX Data Security

[2] AN 159 KNX IP Secure

[3] Svazek 3/8/x KNXnet/IP Specifikací