



ETS6 Professional

KNX Secure käyttö ETS6:ssa

Periaatteita ja yksityiskohtia

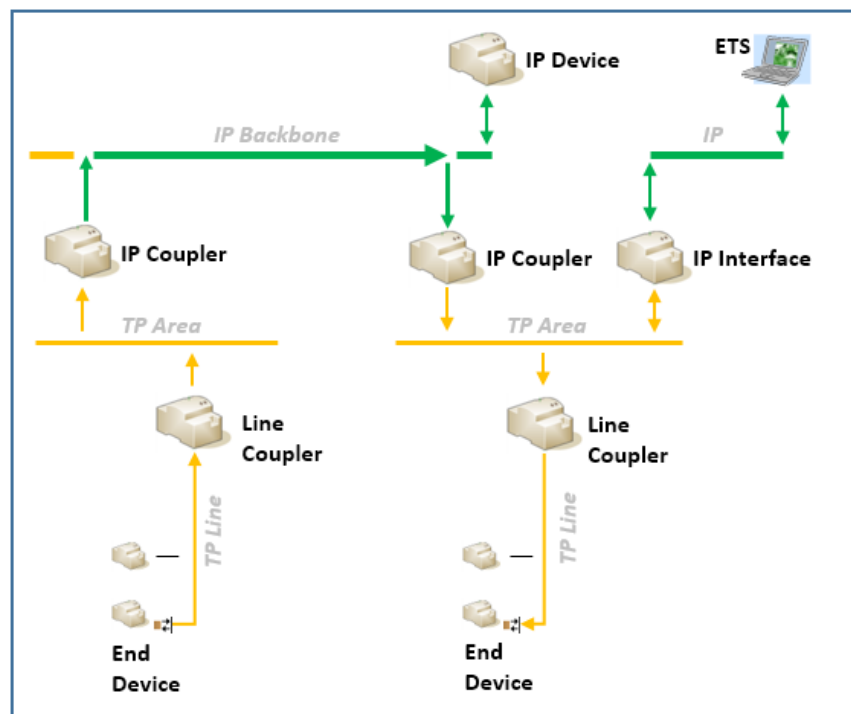
Veijo Piikkilä

Tutor

KNX Finland/TC

KNX IP Secure ja KNX Data Secure

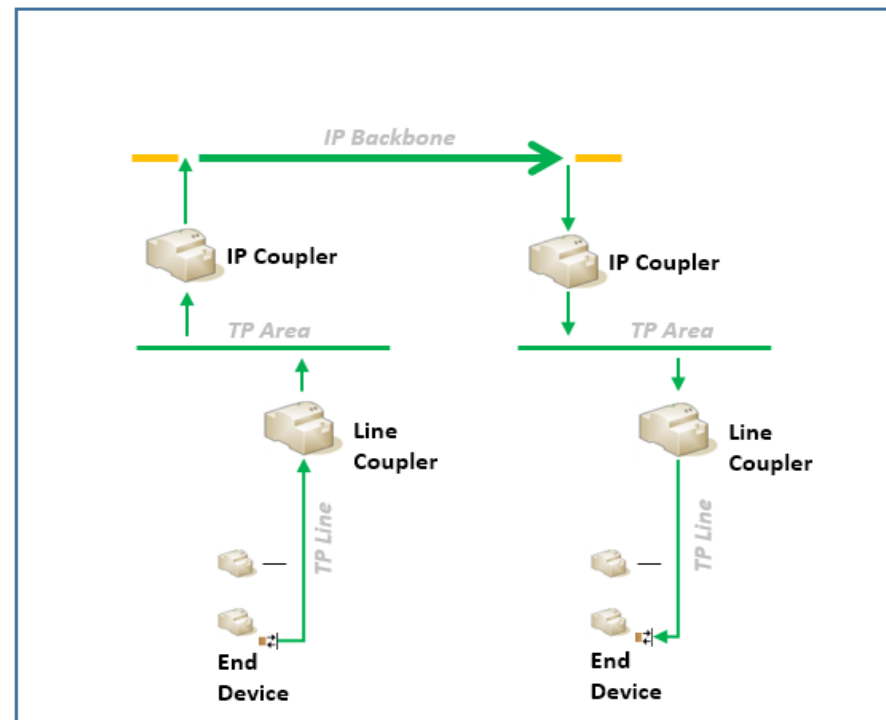
KNX IP Secure



— Tavallinen viestintä
— Turvallinen viestintä

Kaikki kahden (tai useamman) IP-yhdistimen väliset KNX-sanomat on salattu

KNX Data Secure



Tietyn lähettäjän (yksi tai useampi ryhmäobjekti) ryhmäviestintä toiselle ryhmäobjektille on salattu

KNX Turvan faktat



KNX Secure –sovellusalue

KNX Secure kattaa seuraavat KNX-asennuksen sovellusskenaariot:

- Turvattu tiedonsiirto IP:llä
- Turvattu tiedonsiirto päätelaitteiden välillä
- Turvattu tiedonsiirto konfiguroinnin aikana



KNX -turvatut hyökkäysvektorit

KNX Security torjuu tehokkaasti seuraavat uhkaskenaariot tai mahdolliset hyökkäykset KNX-järjestelmään:

- Sanoman toistoa
- Sanoman manipulointi
- Sanoman näkyvyys

KNX Turvan faktat

KNX Secure käyttämiä algoritmeja

KNX Secure käyttää **AES128 CCM**-salausta/todennusta ja elliptistä käyrää Diffie-Hellmanin suojattuun avainten vaihtoon

Advanced Encryption Standard (AES) on yleinen salausalgoritmi (ISO/IEC 18033-3)

- **Lohkon koko:** 128 bit
Avaimen koko: 128 bit, 192 bit tai 256 bit
- **Koostuu:**
 - Tavujen korvaaminen
 - Rivien siirtäminen
 - Sarakkeiden sekoittaminen
 - Kierrosavaimen lisääminen
- Elliptinen käyrä Diffie-Hellman-avainvaihto on maailmanlaajuisesti standardoitu ja laajalti käytetty algoritmi yhteisen salaisen avaimen jakamiseen suojaamattomalla viestintäkanavalla

KNX Turvan faktat

ETS:n KNX-projektien turvallisuus KNX Securella

Jokainen KNX Securea käyttävä ETS-projekti vaatii projektitiedoille korkeampaa "turvallisuustasoa" (projektissa käytettyjen salasanojen näkyvyys estetään) → siksi ETS on suojattava salasanalla

- ETS näyttää tarvittavan salasanan vahvuuden.



Set Project Password

Andre Berger-GE

A good password should consist of at least eight characters, a least one number, one uppercase letter, one lowercase letter ✓, and have a special character.

New Password

Weak

Confirm Password



Set Project Password

Andre Berger-GE

A good password should consist of at least eight characters ✓, at least one number, one uppercase letter, one lowercase letter ✓, and have a special character.

New Password

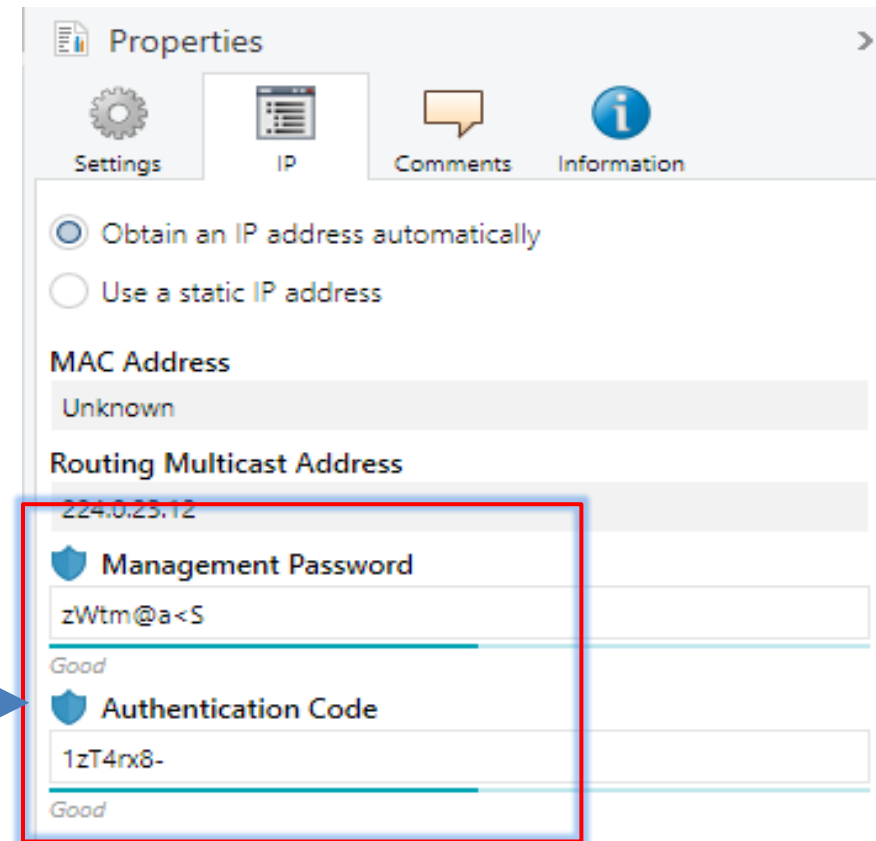
Very good

Confirm Password

KNX Turvan faktat

ETS:n KNX -projektien turvallisuus KNX Securella

- Jokaisella ETS -projektissa turvallisesti käytetyllä KNX Secure-laitteella on myös yksilölliset salasanat.
- Myös tässä ETS näyttää salasanan vahvuuden oikealla tavalla.
- KNX Secure-tuotteet voidaan tuoda tavalliseen tapaan. Ne on helppo tunnistaa sinisestä ”suojakilvestä”.

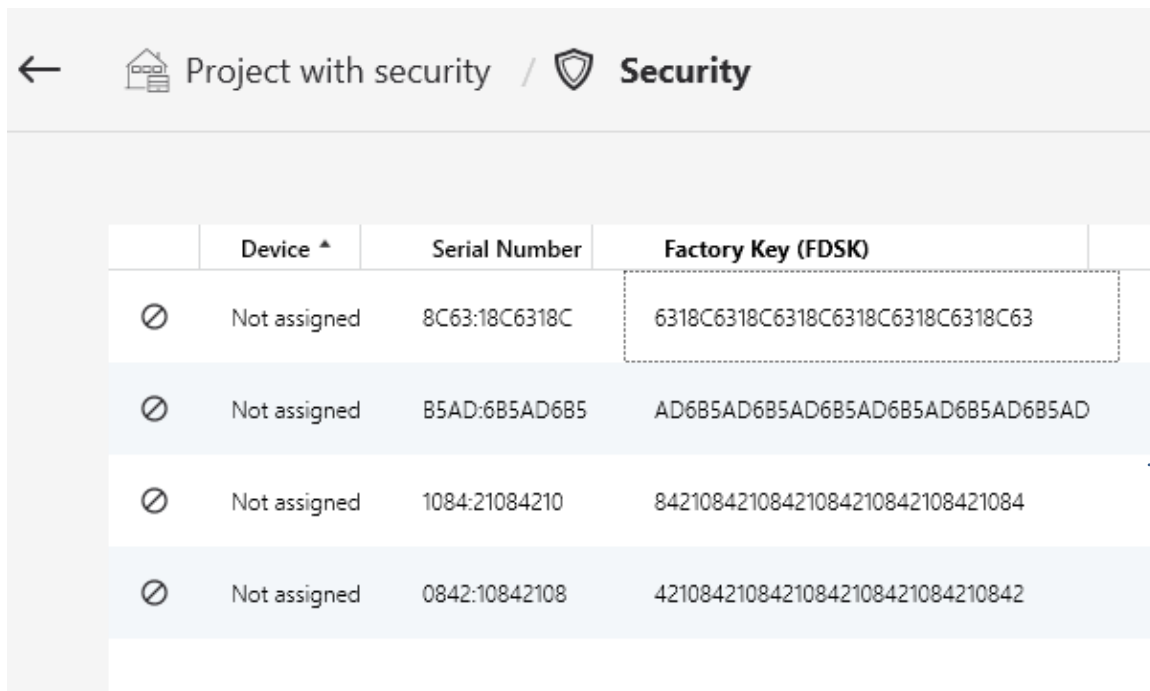


KNX Turvan faktat

Avaimet ETS KNX-projektissa, jossa on KNX Secure

Kun käytetään laitteiden KNX Secure -ominaisuuksia, yksittäinen laite ja/tai IP-runkoverkkoavain on säilytettävä ”turvattua” viestintää varten.

ETS tallentaa ja ylläpitää näitä avaimia turvallisesti, vaikka projekteja viedään.



The screenshot shows the 'Security' section of the ETS software. It features a table with four columns: 'Device', 'Serial Number', and 'Factory Key (FDSK)'. The first column contains a circular icon with a diagonal line. The table lists four entries, all marked as 'Not assigned'. The first entry's 'Factory Key (FDSK)' is highlighted with a dashed blue box, and a callout points to it with the text 'Laitteen (yksilölliset) Avaimet'.

Device ^	Serial Number	Factory Key (FDSK)
Not assigned	8C63:18C6318C	6318C6318C6318C6318C6318C6318C63
Not assigned	B5AD:6B5AD6B5	AD6B5AD6B5AD6B5AD6B5AD6B5AD6B5AD
Not assigned	1084:21084210	84210842108421084210842108421084
Not assigned	0842:10842108	42108421084210842108421084210842

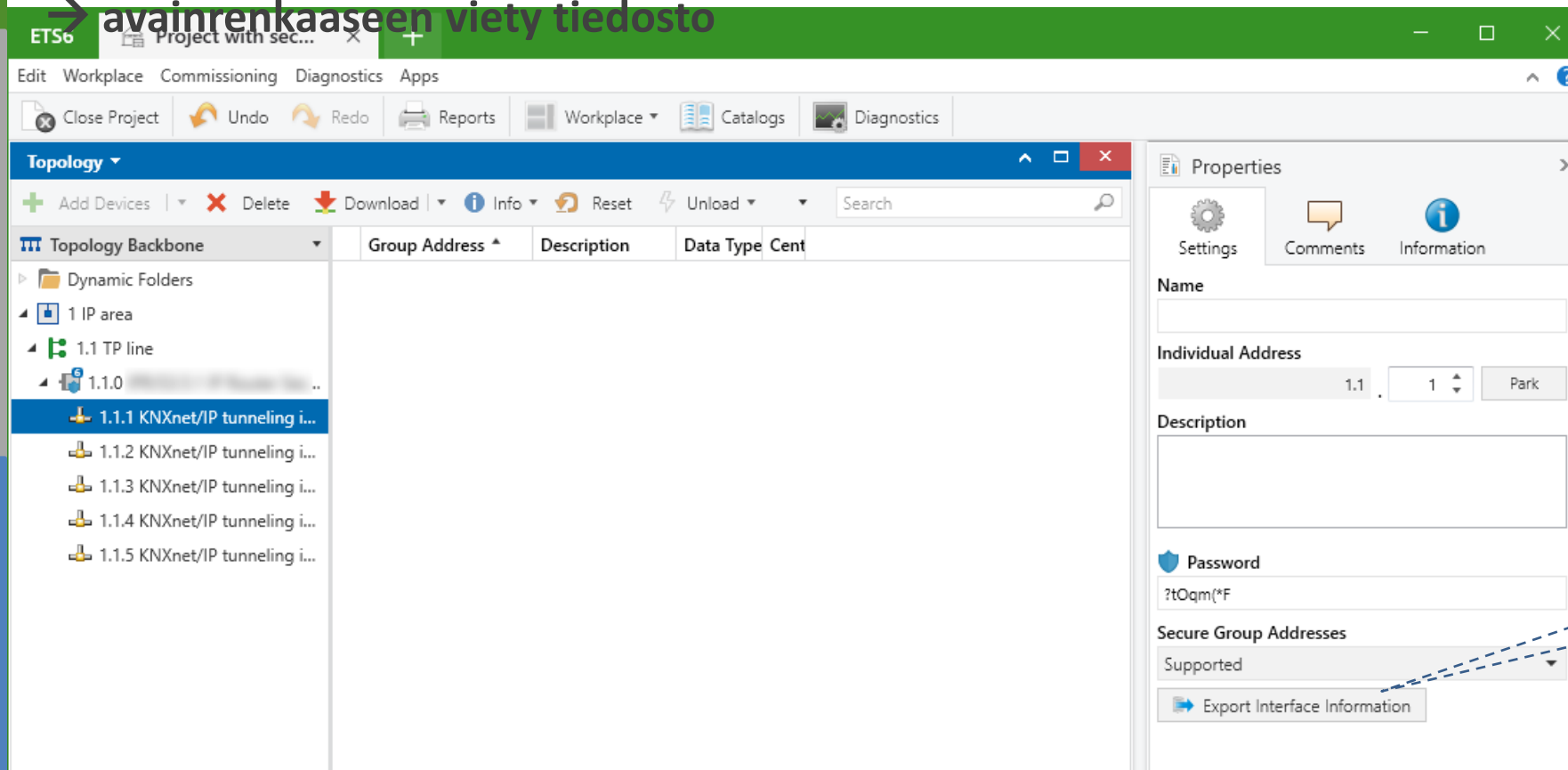
Laitteen (yksilölliset)
Avaimet

KNX Turvan faktat

Avaimet ETS KNX -projektissa KNX Securen kanssa

KNX (Secure)-asennuksen valvonta → luvallisesta käytöstä (esim. ulkoinen visualisointi tai diagnostiikka) on päästävä käsiksi ETS -projektissa käytettyihin avaimiin (turvatulla tavalla)

→ avainrenkaaseen viety tiedosto



**Avainrenkaan vienti
koko asennuksesta
(XML-tiedosto)**

**Yksilöllisen avainrenkaan
vienti vain tätä
tunnelointiliitintää varten**

KNX Secure tyypit

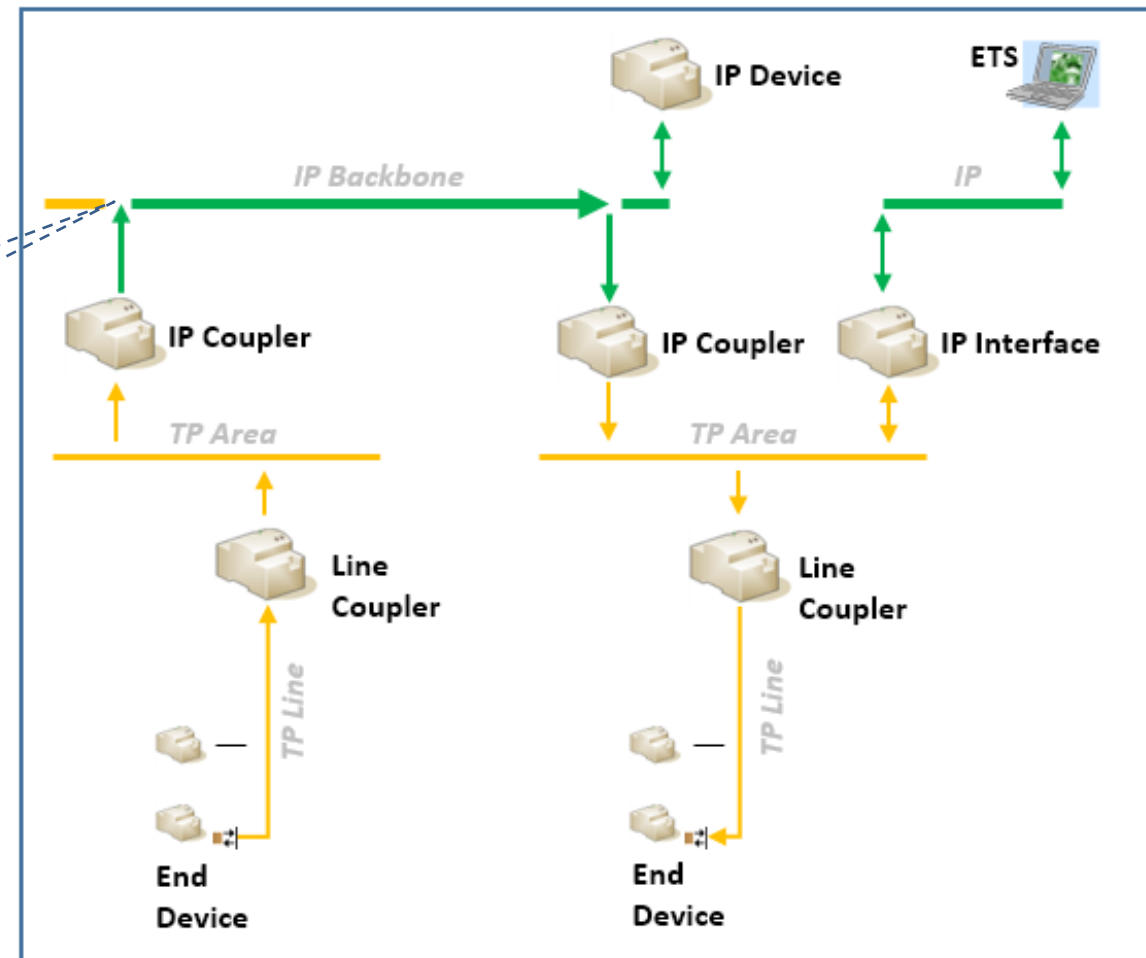
KNX-turvatyypit

KNX IP Secure, tekniikka

KNX IP Secure turvaa koko KNXnet/IP -kehyksen.

Kaikki kahden (tai useamman) IP-yhdistimen väliset KNX-sanomat ovat **TURVALLISIA**

- Tavallinen viestintä
- Turvallinen viestintä



KNX-turvatyypit

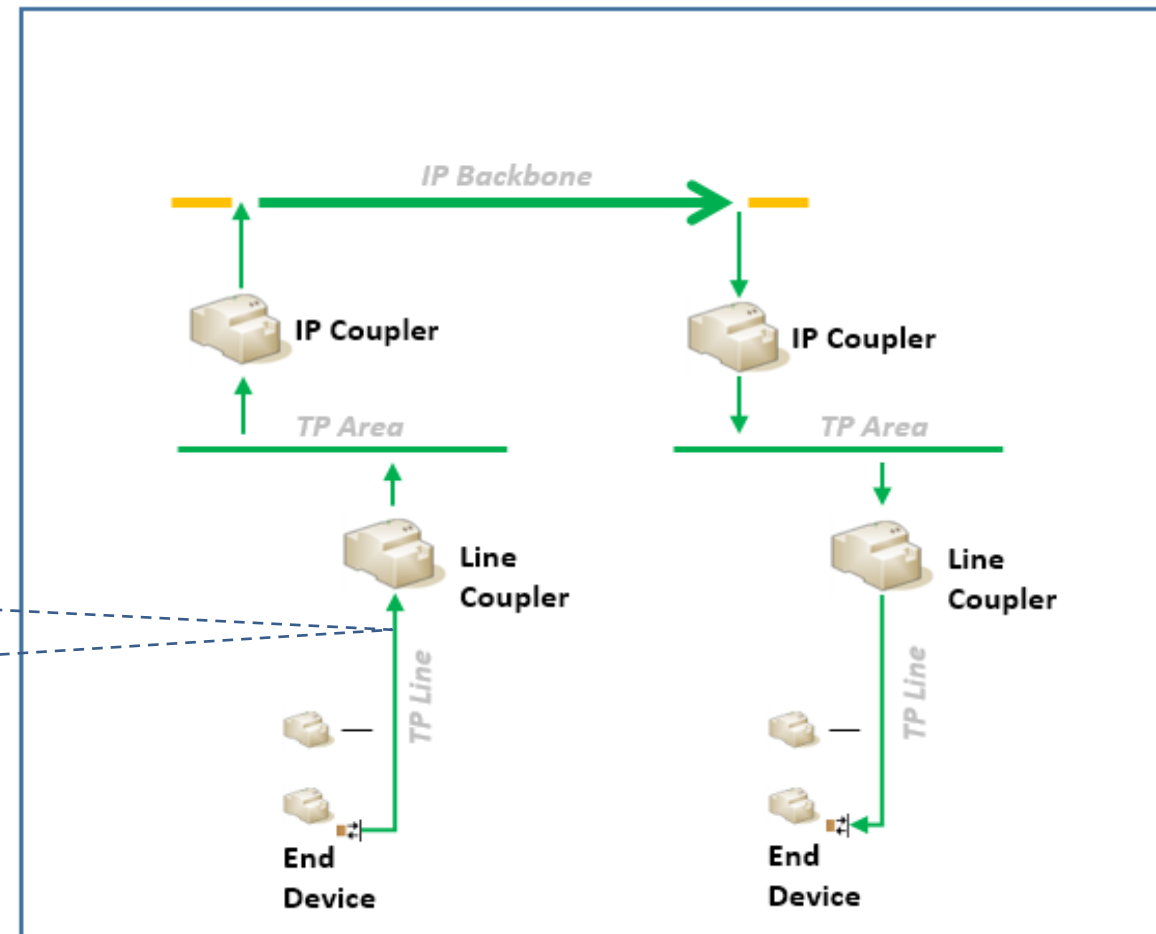
KNX Data Secure, tekniikka

KNX Data Secure turvaa vain APCI*:n ja hyötykuorman

Tietyn lähettäjän (yhden tai useamman ryhmäobjektin) ryhmäviestintä toiselle ryhmäobjektille on **TURVALLISTA**

- Tavallinen viestintä
- Turvallinen viestintä

***APCI**; Application Layer **P**rotocol **C**ontrol **I**nformation



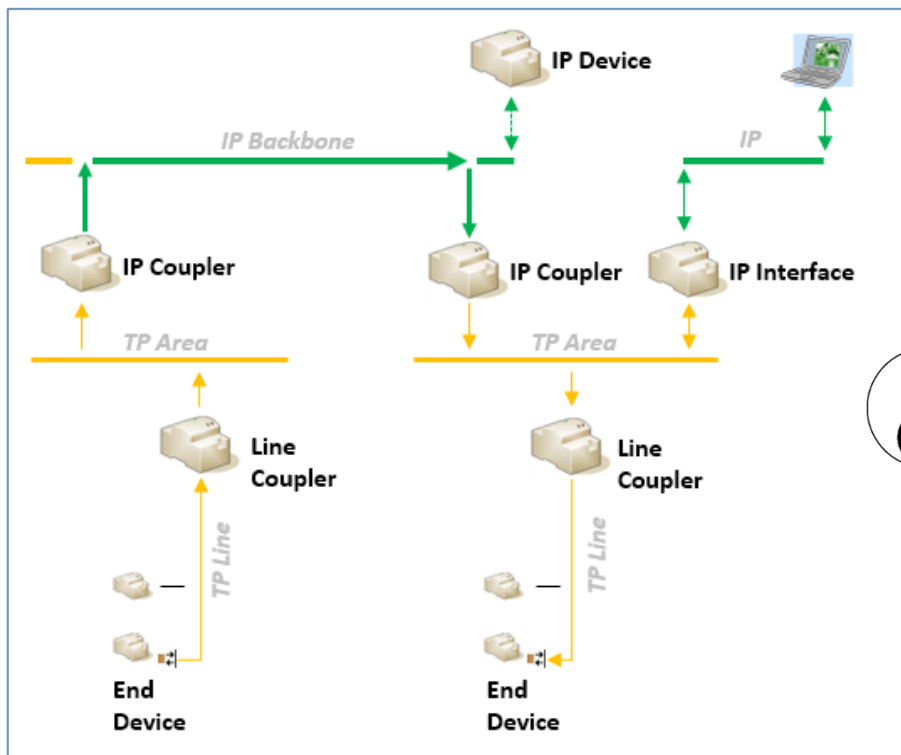
KNX-suojaustyypit

KNX Secure, Yhdistelmä

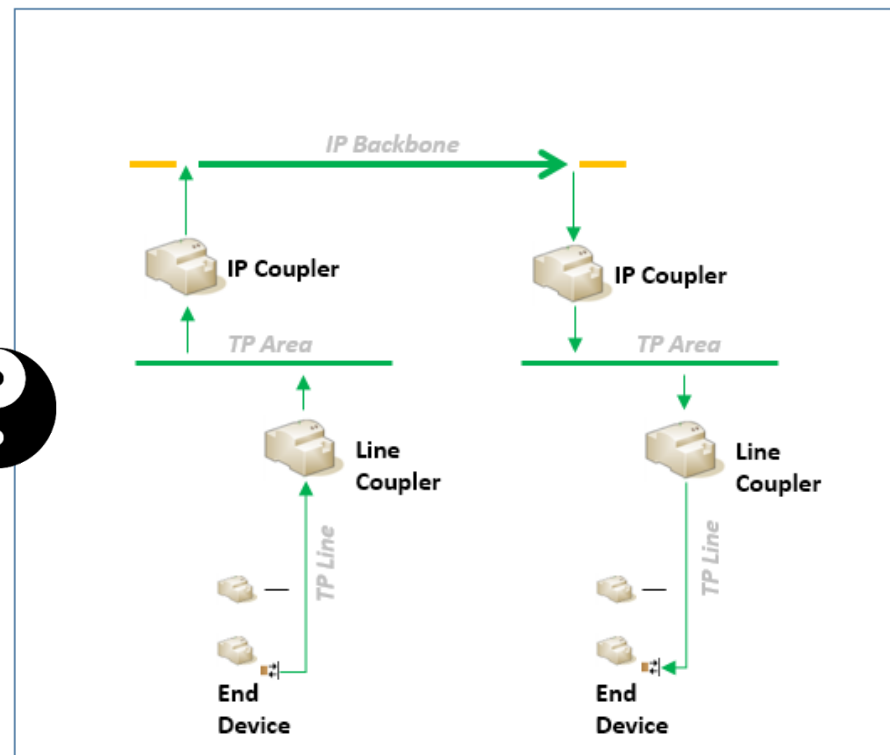
KNX IP Secure ja KNX Data Secure voidaan yhdistää ETS -projektiin/asennukseen.

ETS hoitaa avainten hallinnan/jakelun, luo ”turvatut linkit” ja lataa nämä linkit KNX Secure-laitteisiin riippumatta KNX Secure-tyypeistä.

KNX IP Secure



KNX Data Secure



- Tavallinen viestintä
- Turvallinen viestintä

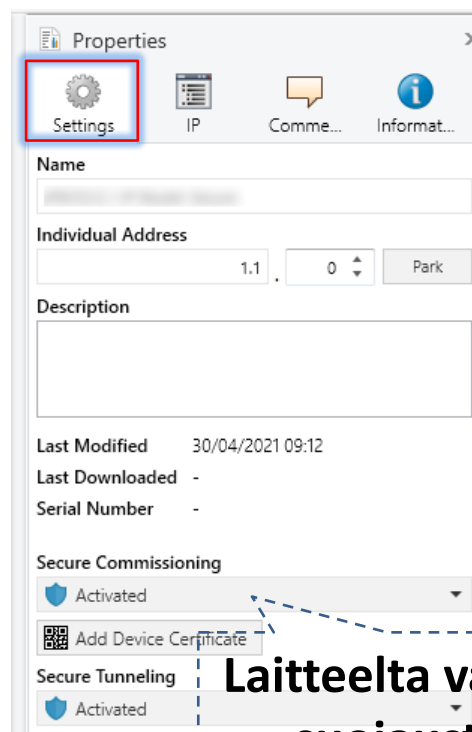
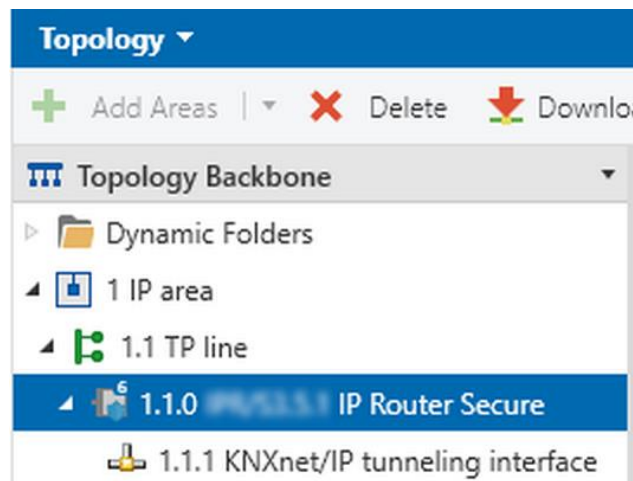
KNX Secure ETS6:ssa

KNX Secure ETS6:ssa

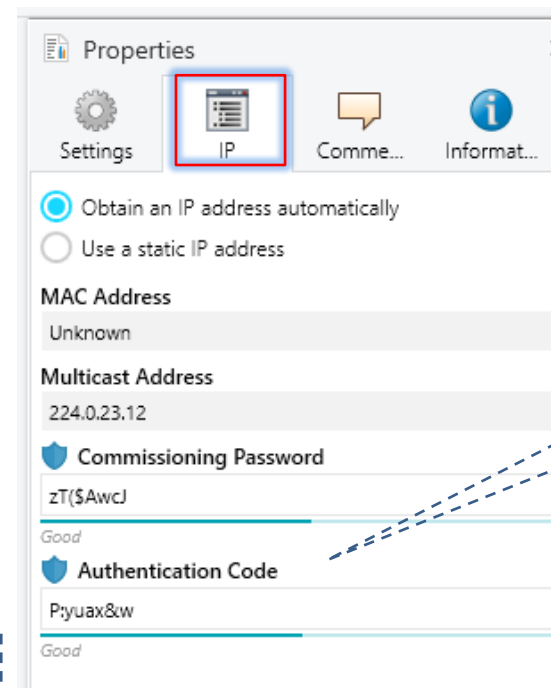
KNX IP Secure, IP-laitteet

KNX-turvattu IP-laitteiden taso (esim. Runkoverkossa) on osa **laitteen** ominaisuuksia.

- Mahdolliset tasot ovat **aktivoitu/deaktivoitu**.
- Tämän tason ja runkoverkon välillä on riippuvuuksia (esim. tarve asettaa taso aktivoiduiksi tällaisille laitteille, kun runkoverkko on suojattu)



Laitteelta vaadittu
suojaustaso



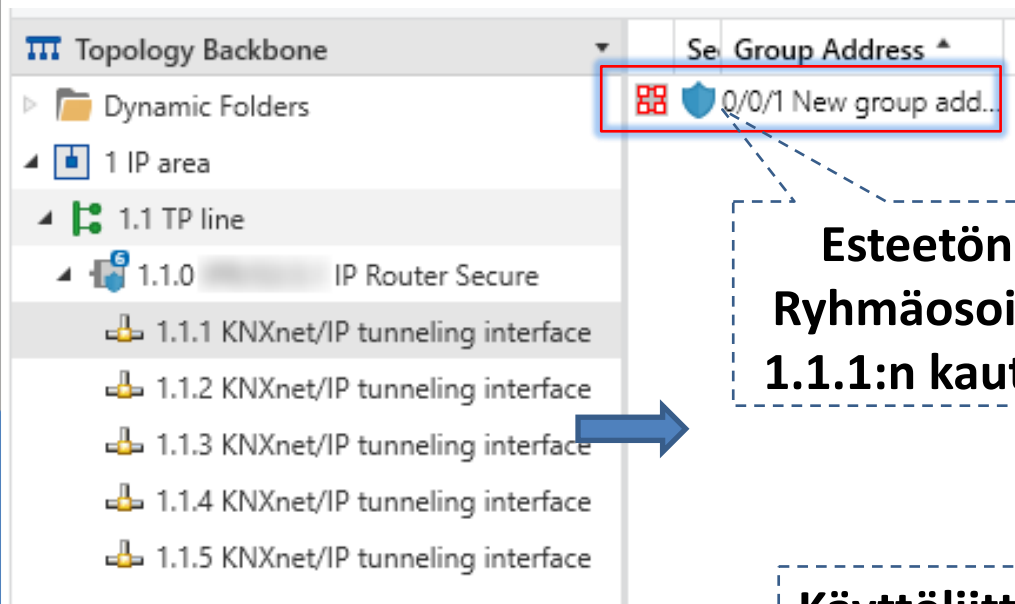
Laittehallinnan
salasanat

KNX Suojaus ETS6:ssa

KNX IP Secure, IP –rajapinnat

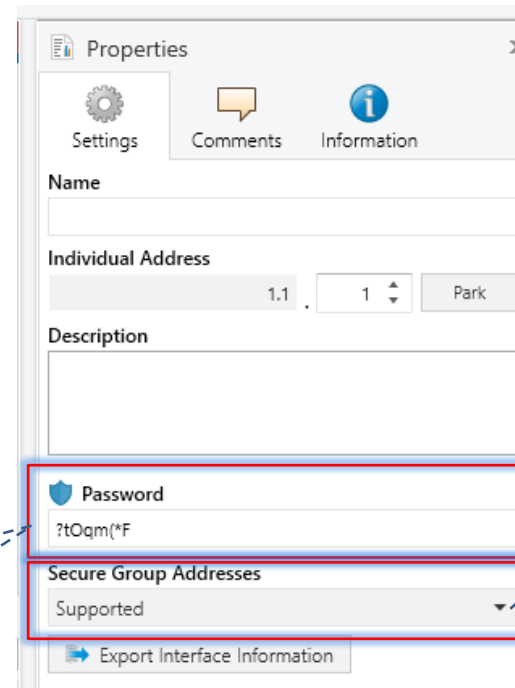
KNX -suojattu IP-rajapintojen taso on (myös) osa **laitteen** ominaisuuksia.

- Ulkoiseen (visualisointiin) pääsyä varten (ylimääräisten) tunnelointiliitännöiden kautta tarvitaan rajapinnan salasana ja rajapinnalle nimenomaisesti määritetty ryhmäosoite



**Esteetön
Ryhmäosoite
1.1.1:n kautta**

**Käyttöliittymän
salasana 1.1.1:llä**



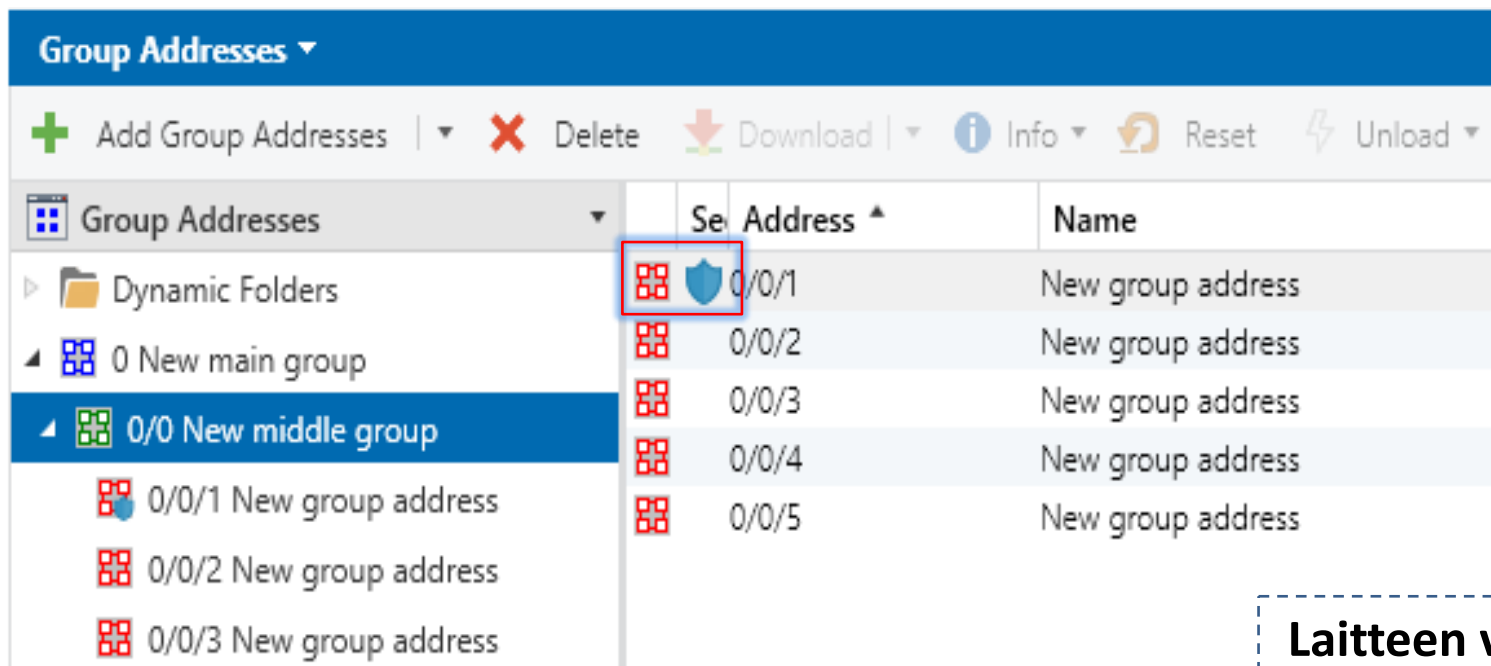
**Määritä, tukeeko tätä
tunnelointiliittymää
käyttävä ohjelmisto
turvattuja Ryhmäosoitteita**

KNX Suojaus ETS6:ssa

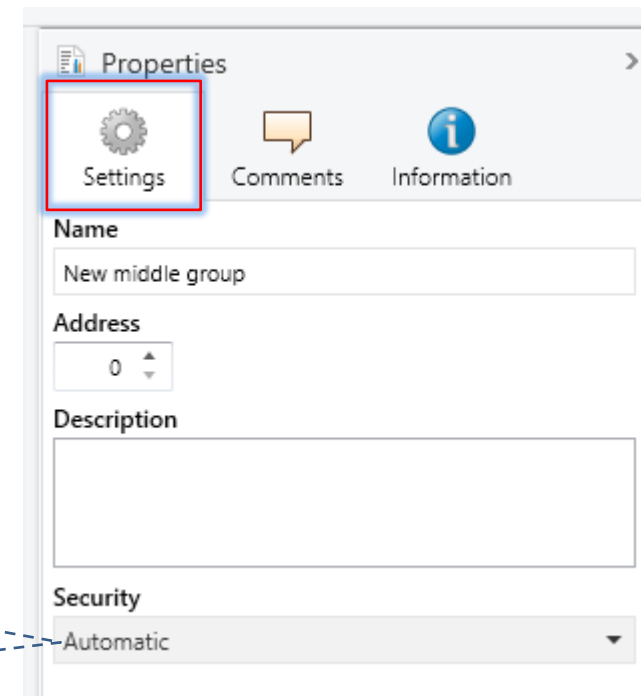
KNX Data Secure, Ryhmäosoitteet

Ryhmäosoitteen KNX-turvataso on osa **ryhmäosoitteen** ominaisuuksia.

- Mahdolliset tasot ovat **Päällä/Pois/Automaattinen**.
- Tämän tason ja ryhmäobjekteille osoitettujen ryhmäosoitteiden välillä on riippuvuuksia (esim. tarve ladata tällaisia laitteita myös turvattuna, kun ryhmäosoite on turvattu)



	Se	Address	Name
Dynamic Folders			
0 New main group			
0/0 New middle group			
0/0/1 New group address	Shield	0/0/1	New group address
0/0/2 New group address		0/0/2	New group address
0/0/3 New group address		0/0/3	New group address
0/0/4 New group address		0/0/4	New group address
0/0/5 New group address		0/0/5	New group address



Properties

Settings Comments Information

Name
New middle group

Address
0

Description

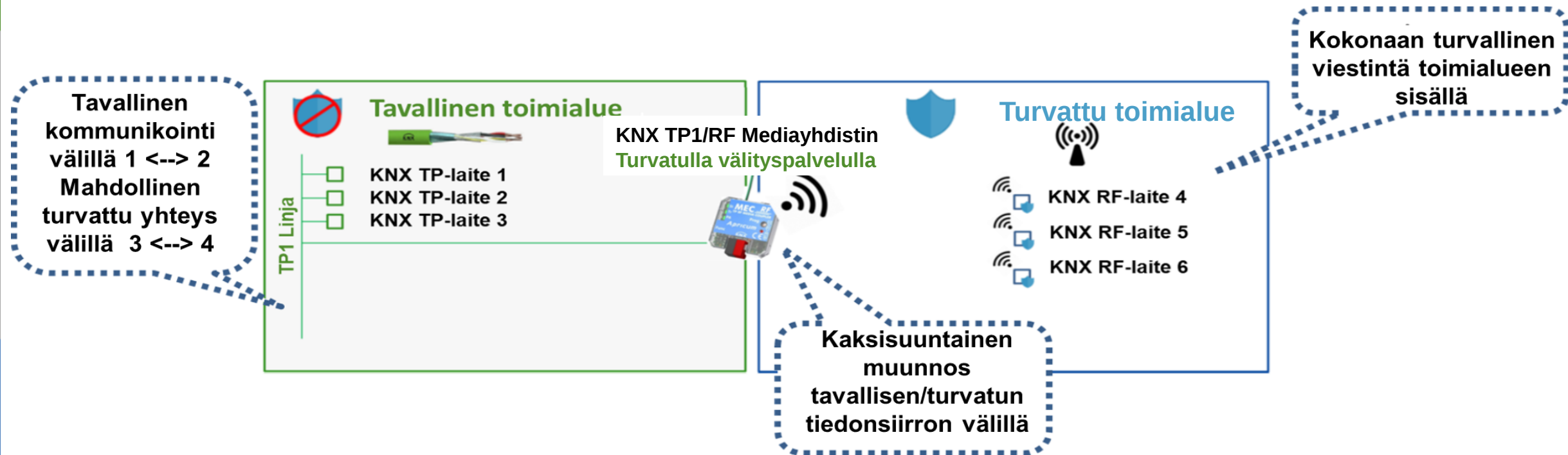
Security
Automatic

Laitteen vaadittu
turvataso

KNX Turvattu Välityspalvelin ETS6:ssa

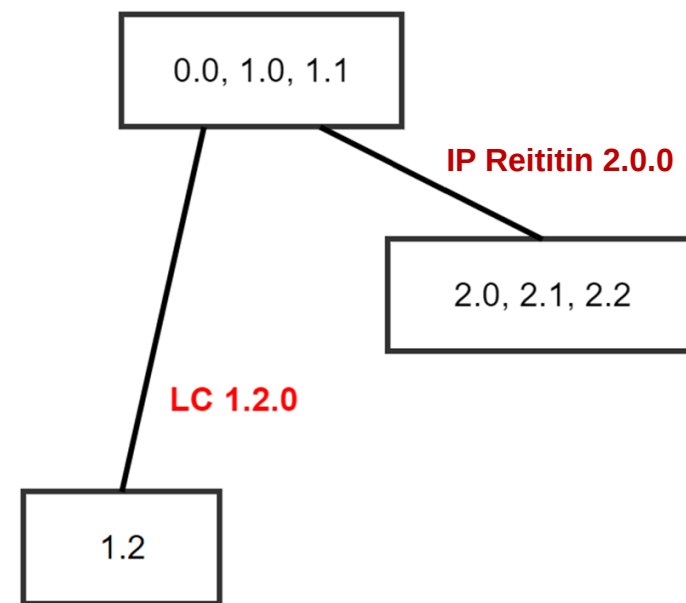
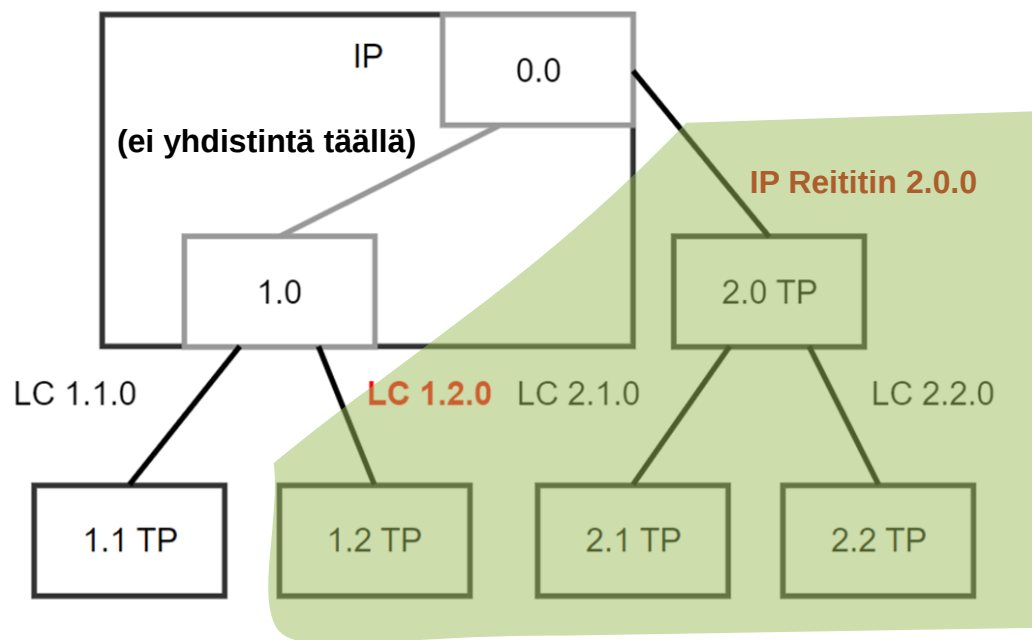
KNX:n Turvattu Välityspalvelin ETS6:ssa

ETS6 Professional tukee KNX Turvattua Välityspalvelinta (Secure Proxy)



KNX:n Suojattu Välityspalvelin ETS6:ssa

- **ETS6** pystyy selviytymään useista turva-alueista (ETS5 vain yhdestä), joiden suojaussäännöt ovat samat kuin ETS5:ssä
- **ETS6** voi selviytyä tietoturva-alueen rajoista



KNX:n Suojattu Välityspalvelin ETS6:ssa

Ryhmäviestinnän turvaaminen – päätelmät

Päätelmä 1: Tietoturva-alueen sisällä tietyn ryhmäosoitteen käyttäminen on joko turvattua tai aivan tavallista.

Päätelmä 2: Asennuksessa on yksi avain ryhmää kohti.

Päätelmä 3: ETS tukee vain A+C, ei A:ta. (A = todennus, C = luottamuksellisuus)

Group Addresses ▾			
+ Add Group Addresses ▾ X Delete Download ▾ i Info ▾ ↺ Reset ⚡ Unload ▾ Print			
Group Addresses ▾	Security	Address ^	Name
▸ Dynamic Folders	🔒	0/0/1	Switching
▾ 0 New main group	🔒	0/0/2	Status
▾ 0/0 New middle group	🔒	0/0/3	Central Switch
🔒 0/0/1 Switching			
🔒 0/0/2 Status			
🔒 0/0/3 Central Switch			
Group Addresses			
<no interface selected> 1.1 TP line			

Group Addresses ▾		
+ Add Group Addresses ▾ X Delete Download ▾ i Info ▾ ↺ Reset ⚡ Unload ▾ Print		
Group Addresses ▾	Se	Object ^
▸ Dynamic Folders		
▾ 0 New main group		
▾ 0/0 New middle group		
🔒 0/0/1 Switching	🔒	1: Channel C1 - Switch object
🔒 0/0/2 Status		
🔒 0/0/3 Central Switch		
		36: Channel 1: Switching - Output
		1.1 SU 1 RF
		1.3.1 Remo KNX RF



Kysyttävää?

Lähteet

- Vassilios Lourdas, KNX Association
- KNX Association materiaali