

Hur uppnår jag hög datasäkerhet i mitt fastighetsautomationssystem?

Johan Hollsten ABB

Marie Holmberg Schneider Electric



Arrangeras av Voltimum.se – portalen för elproffs

Agenda

- Inledning
- Säkra installationer
- KNX Secure
- Ansvarsfördelning
- Summering/frågor

Definition datasäkerhet

1. Sekretess: förhindrande av obehörigt avslöjande av information
2. Integritet: förhindrande av obehörig eller oavsiktlig förändring av information
3. Tillgänglighet: förhindrande av obehörigt undanhållande av information
4. Spårbarhet: att vissa eller alla aktiviteter i ett system ska kunna härledas till en användare

Exempel datasäkerhet

- Datasäkerhet över webben
 - Brandvägg och VPN
 - Kryptering
 - HTTP VS HTTPS
 - Krypterad trafik med hjälp av TLS (SSL)
 - Ökar kraven på proxy-servrar och antivirusprogram
 - 5% av alla domäner

Riskbedömning

- Varje fastighet måste analyseras
 - Potentiella risker och dess sannolikhet
 - Säkerhet (passage, el, brand, drift etc.)
 - Datarelaterade (ex. närvaro och förlust av information)
 - Ekonomiska
 - Komfort
 - Varumärke/publicitet
 - Konsekvenser

		Sannolikhet				
		5	4	3	2	1
Konsekvens	5	25	20	15	10	5
	4	20	16	12	8	4
	3	15	12	9	6	3
	2	10	8	6	4	2
	1	5	4	3	2	1

KNX-system

Störst säkerhetsrisk finns ...

- ... med KNX i större byggnader
- ... i byggnader med känslig verksamhet
- ... i byggnader med funktioner för dörrkontroll, larmsystem
- ... där KNX är kopplat mot kameror, andra system
- ... mm

Hur har detta hanterats?

Fysiska barriärer

- Håll bussen otillgänglig för obehöriga:
 - Montera apparater för att försvåra demontering
 - I offentliga miljöer kan strömbrytare ihop med binäringång i central användas
 - Placera yttre apparater på positioner och höjder som är svåra att nå
 - Minimera åtkomst till centraler och teknikrum till endast behöriga
 - Skydda kabeländar och kabelförläggning så gott det går

Digitala barriärer

- Använd filtertabeller
- Minimera antalet gruppadresser mellan linjer

KNX Secure

- KNX Association har lanserat en säker lösning för kommunikation inom KNX-system.
- KNX Secure uppfyller krav enligt krypteringsstandard AES128 (ISO/IEC 18033-3). Alla tillverkare följer samma standard (EN 50090-4-3).
- Detta ger högsta möjliga säkerhet för byggnadsautomation inom nuvarande teknologi.

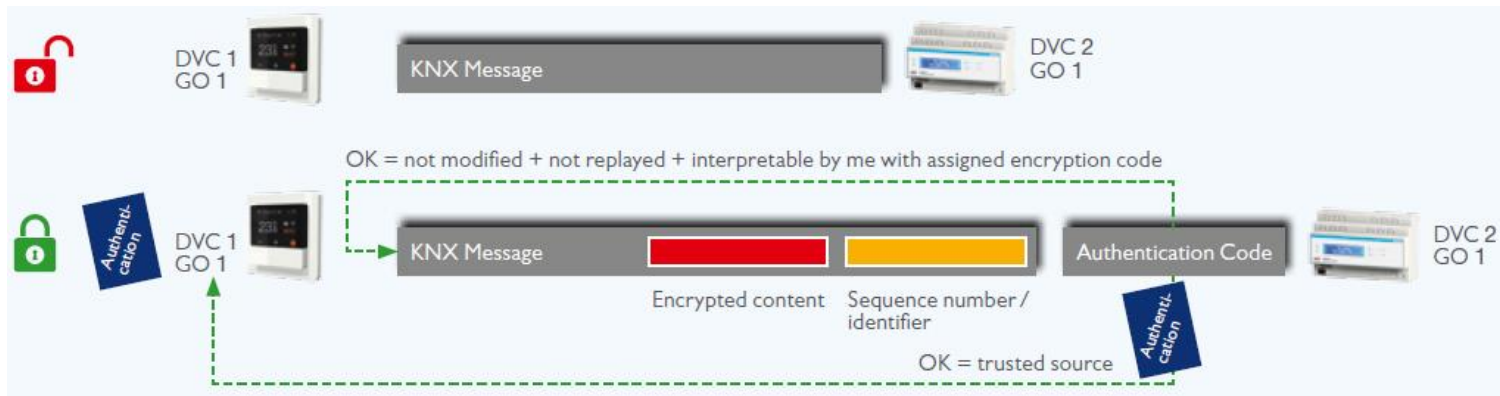
Skydd på två nivåer:

- KNX Data Secure – säkrar kommunikationen inom installationen med kryptering
- KNX IP Secure – lägger till kryptering för all KNX-trafik över IP



KNX Data Secure

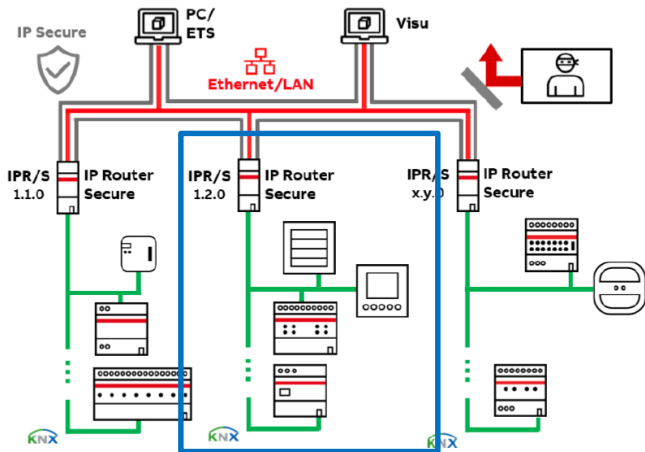
KNX Data Secure skyddar kommunikationen mellan apparater.



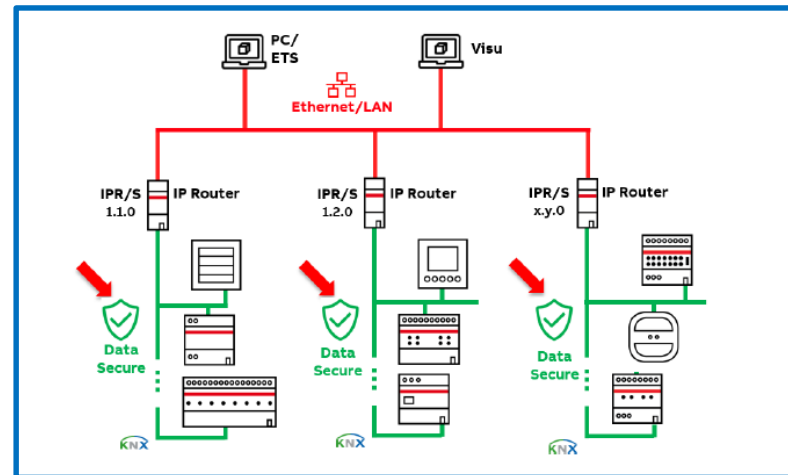
Säkerheten byggs upp med nycklar genererade av ETS och sekvensnummer.

KNX IP Secure

- KNX IP Secure skyddar kommunikationen över IP
- Packar in KNX-data med hjälp av kryptering
- Bilda säkra "zoner"



KNX IP Secure



KNX Data Secure

Öka säkerheten i steg

Steg 0: Skapa fysiska och digitala barriärer genom smart installation och integration

Steg 1: Säkra IP-kommunikationen i din anläggning med “KNX IP Secure”

- Använd routers, gränssnitt och andra IP enheter som stödjer KNX IP Secure

Steg 2: Använd produkter som stödjer “KNX Data Secure”

Vem gör vad?

Leverantör

- Efterleva senaste säkerhetsstandard och produktstandard samt tillhandahålla uppdatering
- Tillhandahålla checklistor och utbildningar
- Support

Systemintegratör/projektör/installatören

- Riskanalys
- Säkerhetstänk vid planering, installation och drift

Fastighetsägare/fastighetsskötare

- Hantering av behörighet och åtkomst till system (lösenord, krypteringsnycklar, ETS-filer m.m)
- Utbilda sin personal i generell IT-säkerhet
- Anläggningskännedom



Summaring

- Fastighetsautomation kan göras säker med rätt val av produkter, installation och drift
- Hitta balans mellan säkerhet, ekonomi och användarvänlighet
- Hela byggnadens livscykel måste tas i beaktande
- Integratörer och installatörer med rätt kunskap kommer efterfrågas
- För mer information om KNX Secure: <https://knxsecure.knx.org>

Frågor?



Arrangeras av Voltimum.se – portalen för elproffs