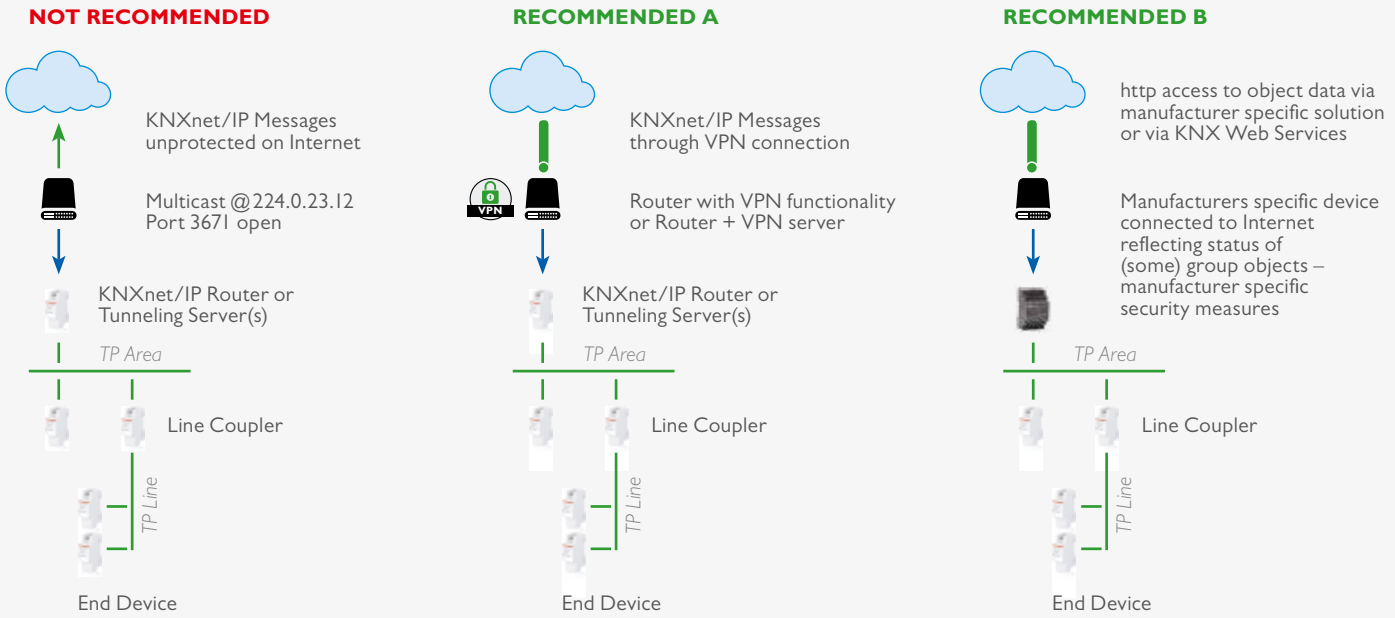
Smart home and building solutions.
Global. Secure. Connected.

KNX SECURE

KNX POSITION PAPER SU SICUREZZA DEI DATI E PRIVACY

Il presente documento è inteso come guida per consentire a installatori e costruttori KNX di apprendere le attuali misure intraprese per aumentare la sicurezza delle installazioni KNX.

IMPEDIRE L'ACCESSO ALLA RETE AI DIVERSI SUPPORTI FISICI KNX



Accesso a reti KNX via Internet

Il concetto di protezione adeguata si basa sulla corretta prevenzione degli accessi non autorizzati. Nel caso di un'installazione KNX, ciò impone che soltanto le persone autorizzate (installatore, manutentore, utente) possano accedere fisicamente all'installazione KNX. Nel corso di progettazione e installazione, si dovranno proteggere al meglio gli elementi essenziali di ogni supporto KNX.

Installazione di cavo e dispositivi

- In generale, applicazioni e dispositivi saranno fissati adeguatamente in modo da evitare che siano rimossi con facilità, consentendo così alle persone non autorizzate di accedere a un'installazione KNX.
- Enclosure e quadri di distribuzione contenenti dispositivi KNX dovranno essere chiusi correttamente o montati in stanze a cui possano accedere soltanto le persone autorizzate.
- Nelle aree esterne, i dispositivi saranno montati ad altezze sufficienti (ad es. stazione meteo, sensore del vento, rilevatore di movimento, ...).
- Nelle aree pubbliche non adeguatamente sorvegliate, si dovrà prevedere l'impiego di dispositivi convenzionali connessi a ingressi binari montati in aree protette (ad es. nei quadri di distribuzione) o interfacce a pulsante, per prevenire l'accesso al bus.
- Utilizzare, se disponibili, le misure antifurto previste da alcuni moduli applicativi (ad es. protezione dei dispositivi con viti, rimovibili unicamente con attrezzi, resistenza elevata alla trazione, ...).

Doppino

- Le estremità dei cavi non dovranno essere visibili, pendere dalla parete all'interno o all'esterno dell'edificio.
- I cavi del bus nelle aree esterne rappresentano un rischio maggiore. In questo caso, l'accesso fisico al doppino KNX dovrà risultare ancora più difficoltoso rispetto a un'abitazione/un immobile.

- Per maggiore protezione, i dispositivi installati nelle aree a sorveglianza limitata (esterno, parcheggio sotterraneo, toilette, ecc.) possono essere connessi a una linea supplementare. Attivando la tabella filtro negli accoppiatori di linea, in conformità alla clausola 2, è possibile prevenire l'accesso di un hacker all'intera installazione.

Powerline

- Utilizzare filtri elettronici per filtrare segnali in entrata e in uscita.

Frequenza

- Poiché la frequenza radio è aperta, non è possibile adottare misure di protezione fisica per prevenire l'accesso. Per questo, è necessario adottare altre misure indicate alle clausole da 2 a 5 (e in particolare quelle riportate alla clausola 4).

IP

- L'automazione degli edifici dovrà essere eseguita su LAN e WLAN dedicate con hardware proprio (router, switch, ecc.).
- Indipendentemente dal tipo di installazione KNX, si dovranno osservare comunque i consueti meccanismi di protezione per le reti IP. Questi possono comprendere:
  - Filtri MAC
  - Codifica di reti wireless abbinata a password forti (cambio della password predefinita, WPA 2 o superiore) e relativa protezione da persone non autorizzate.
  - Cambio di SSID predefinito (SSID è il nome con cui un punto di accesso wireless è visibile sulla rete, in prevalenza costruttore e tipo di prodotto). Gli SSID predefiniti possono puntare a produrre particolari punti deboli dei punti di accesso in uso e sono per questo particolarmente vulnerabili agli hacker. Il punto di accesso può essere inoltre impostato in modo da evitare la segnalazione (trasmissione periodica dell'SSID, tra gli altri).
- Per IP multicast KNX, si dovrà utilizzare un altro indirizzo IP come predefinito (224.0.23.12). È possibile concordare un indirizzo idoneo con l'amministratore di rete.
- Gli specialisti di rete IT saranno coinvolti in progetti di ampio respiro con connessione a KNXnet/IP: in questo modo la configurazione di rete può essere ancora ottimizzata (gestione switch, LAN virtuale, punti di accesso con IEEE 802.X, ecc.) ed è possibile implementare altri meccanismi di protezione come filtraggio e-mail e anti-virus.

Internet

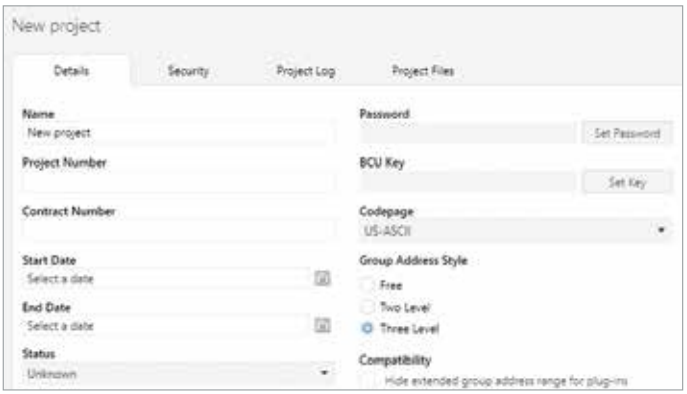
- KNXnet/IP Routing e KNXnet/IP Tunnelling non sono concepiti per l'uso su Internet. Per questo, non è consigliabile aprire le porte dei router a internet, in quanto si renderebbe visibile la comunicazione KNX su internet.
  - L'installazione della (W)LAN dovrà essere protetta tramite firewall.
  - Qualora non sia necessario un accesso esterno all'installazione, il gateway predefinito può essere azzerato, bloccando così qualsiasi comunicazione con internet.
- L'eventuale accesso a un'installazione via internet può essere realizzato come segue:
  - garantire accesso all'installazione KNX tramite connessioni VPN: ciò richiede tuttavia un router che supporti la funzionalità del server VPN o un server con funzionalità VPN.
  - Una delle soluzioni specifiche e dedicate del costruttore disponibili sul mercato e le visualizzazioni (ad es. consentendo l'accesso ad http).
  - KNX ha specificato in un'estensione dello standard KNX una soluzione KNX standardizzata per accedere alle installazioni KNX su internet tramite servizi web.

LIMITAZIONE DI COMUNICAZIONE INDESIDERATA ALL'INTERNO DELLA RETE

- Gli indirizzi individuali dei dispositivi saranno adeguatamente assegnati in base alla topologia e i router configurati in modo da non trasmettere messaggi con indirizzi sorgente non adatti. In questo modo, si limita la comunicazione indesiderata a una sola linea.
- Si dovrà bloccare la comunicazione point-to-point ed eventualmente quella in broadcasting attraverso i router. In questo modo, si limita nuovamente la riconfigurazione a una sola linea.
- Gli accoppiatori saranno configurati in modo da utilizzare attivamente le tabelle filtro senza superare gli indirizzi di gruppo non utilizzati in una determinata linea. In caso contrario, la comunicazione inserita in una linea specifica rischia di diffondersi senza controllo all'intera installazione KNX.

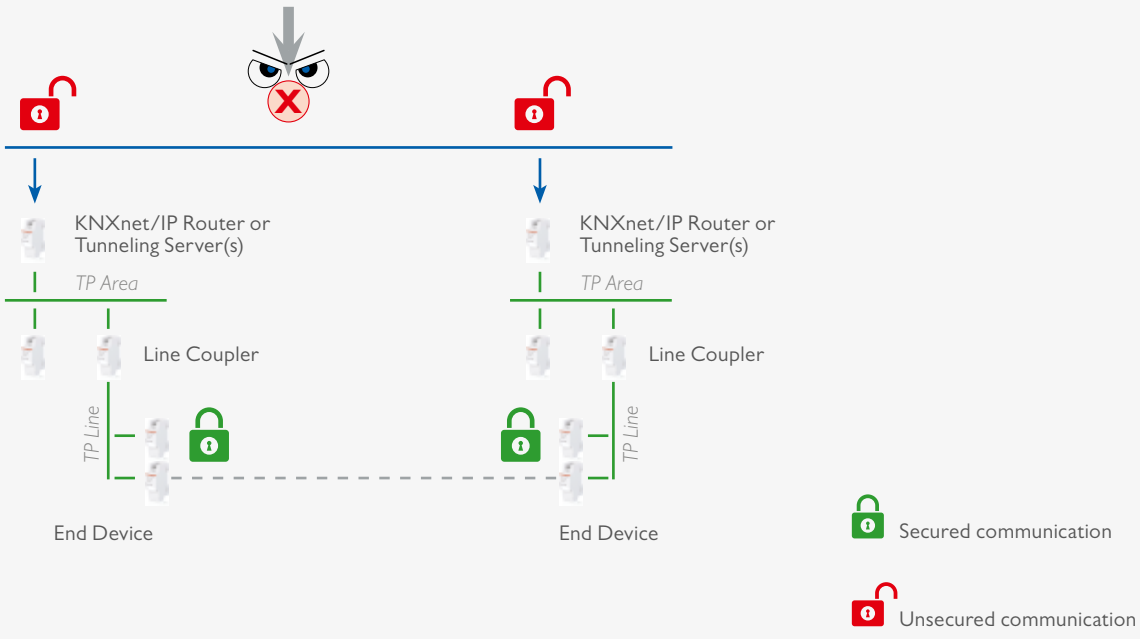
PROTEZIONE DELLA COMUNICAZIONE DI CONFIGURAZIONE

ETS consente di definire la password specifica di un progetto tramite la quale è possibile bloccare i dispositivi per evitare l'accesso non autorizzato. Ciò impedisce che la configurazione dell'installazione possa essere letta o modificata da persone non autorizzate.



Protezione della comunicazione di configurazione in ETS

PROTEZIONE DELLA COMUNICAZIONE RUNTIME



Protezione della comunicazione run time KNX su rete IP con KNXnet IP Security

- Oltre alle misure citate sopra, la comunicazione runtime KNX può essere protetta tramite
  - KNX Data Secure e
  - i meccanismi KNX IP Secure specificati
- KNX Data Secure assicura che, indipendentemente dal supporto KNX, i messaggi selezionati inviati da dispositivi KNX possano essere autenticati e/o codificati, per garantire che siano stati definiti i meccanismi KNX IP Secure anche qualora tale comunicazione non fosse protetta e le reti fossero connesse a IP. Ciò garantisce che i messaggi di routing o tunnelling IP KNX non possano essere registrati o manipolati su IP. I meccanismi KNX IP Secure garantiscono l'aggiunta di un wrapper di sicurezza attorno al traffico dati KNXnet/IP completo.
- I meccanismi KNX Data Secure e KNX IP Secure garantiscono che i dispositivi possano stabilire un canale di comunicazione protetto, garantendo così:
  - Integrità dei dati, cioè impedire che un aggressore prenda il

controllo inserendo frame manipolati. In KNX, ciò è garantito allegando un codice di autenticazione a ogni messaggio: this appended code allows verification that the message has not be modified and that it effectively originates from the trusted communication partner. il codice allegato consente di verificare che il messaggio non sia stato modificato e che abbia realmente origine dal partner di comunicazione di fiducia.

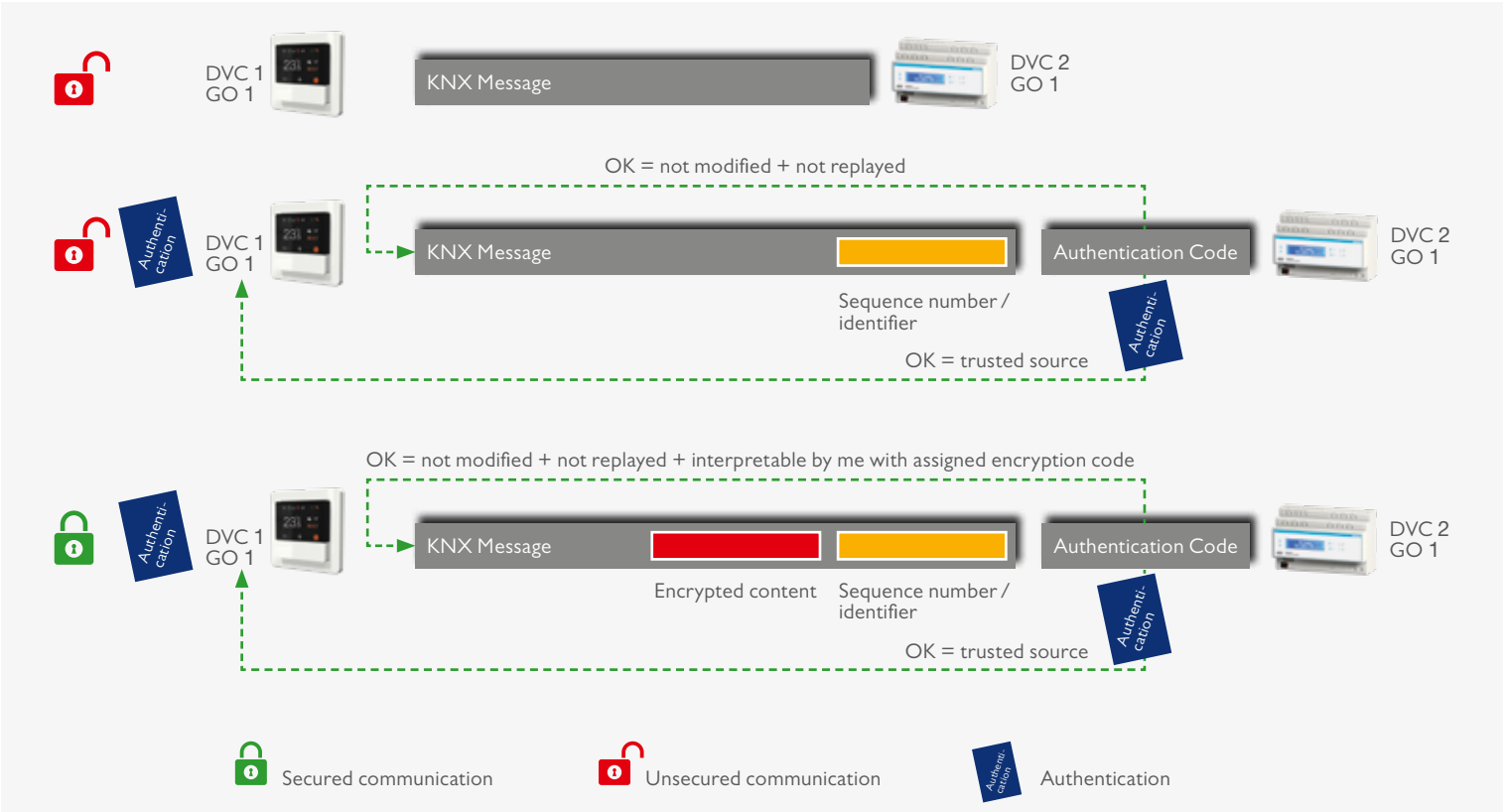
- Freshness, cioè impedire che un aggressore registri i frame e li riproduca in seguito senza manipolarne il contenuto. In KNX Data Secure ciò è garantito da una sequenza di numeri e in KNX IP Secure da un identificativo in sequenza.
- Riservatezza, cioè codificare il traffico in rete in modo che un aggressore abbia la percezione minima dei dati trasmessi realmente. Quando si autorizza la codifica del traffico di rete KNX, i dispositivi KNX garantiscono almeno la codifica in conformità agli algoritmi AES-128 CCM insieme a un codice simmetrico.

Un codice simmetrico indica l'utilizzo dello stesso codice da parte del mittente per proteggere un messaggio in uscita (autenticazione + riservatezza!) nonché da parte del(i) destinatari(o) per verificare la ricezione di tale messaggio.
I dispositivi KNX Data Secure utilizzano un formato telegramma KNX più lungo per trasmettere dati autenticati e codificati. Ciò non compromette in alcun modo la velocità di reazione dei dispositivi. Per KNX Data Secure, i dispositivi sono protetti come segue:

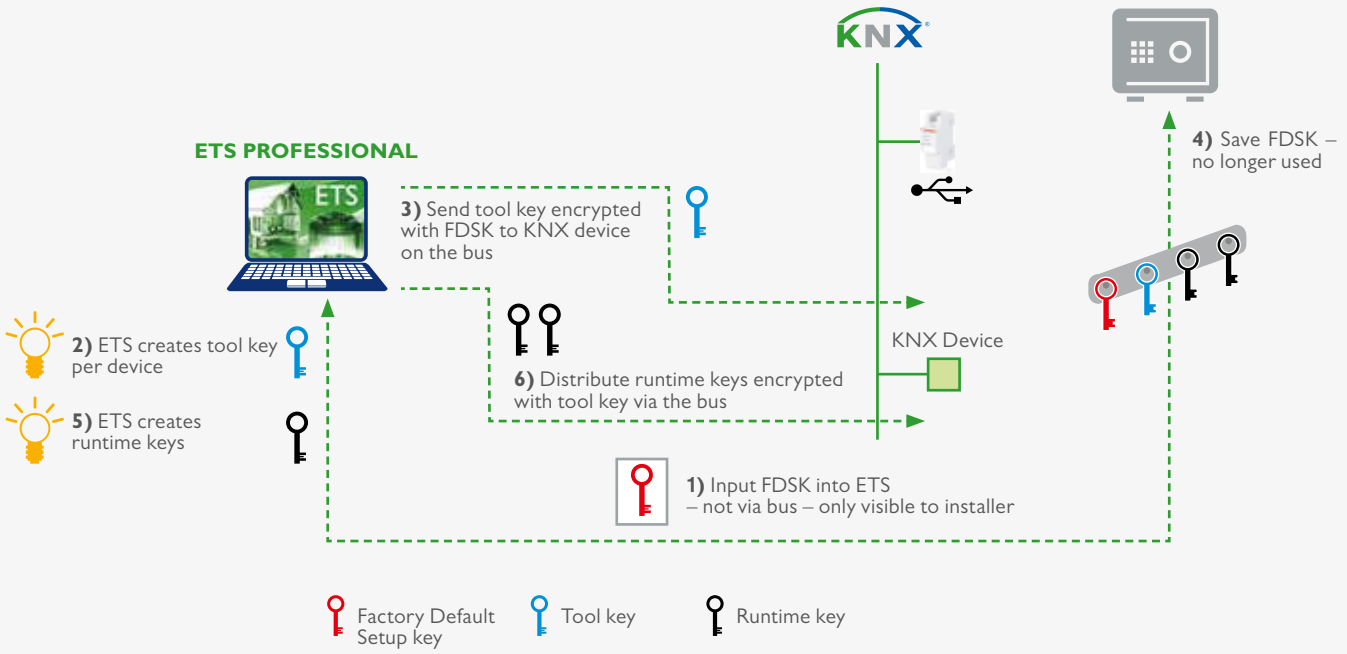
- Un dispositivo è spedito con un Factory Device Set up Key (FDSK) unico.
- L'installatore entra in questo FDSK nello strumento di configurazione ETS (quest'azione non si effettua in alcun caso tramite bus).
- Lo strumento di configurazione crea un codice strumento specifico del dispositivo.
- Tramite il bus, ETS invia al dispositivo da configurare il proprio codice strumento, codificando e autenticando comunque il messaggio con l'FDSK inserito in precedenza. Lo strumento e il codice FDSK non sono mai trasmessi in plain text sul bus.
- Da quel momento, il dispositivo accetta soltanto il codice strumento per ulteriore configurazione con ETS. FDSK non è più utilizzato durante la successiva comunicazione, tranne nel caso in cui il dispositivo sia ripristinato alle impostazioni di fabbrica, dopodiché tutti i dati protetti nel dispositivo saranno cancellati.
- ETS crea codici runtime (in quantità necessaria) per la comunicazione di gruppo che deve essere protetta.
- Tramite il bus, ETS invia al dispositivo da configurare questi codici runtime, codificando e autenticando comunque i messaggi con il codice strumento. I codici runtime non sono mai trasmessi in plain text sul bus.

Per KNX IP Secure, si stabilisce una connessione sicura (Tunnelling o Device Management) come segue:

- Client e server creano una singola coppia di codici pubblico/privato, riferita a una codifica asimmetrica.
- Il client invia il proprio codice pubblico al server come plain text.



Panoramica dei meccanismi KNX Data Secure

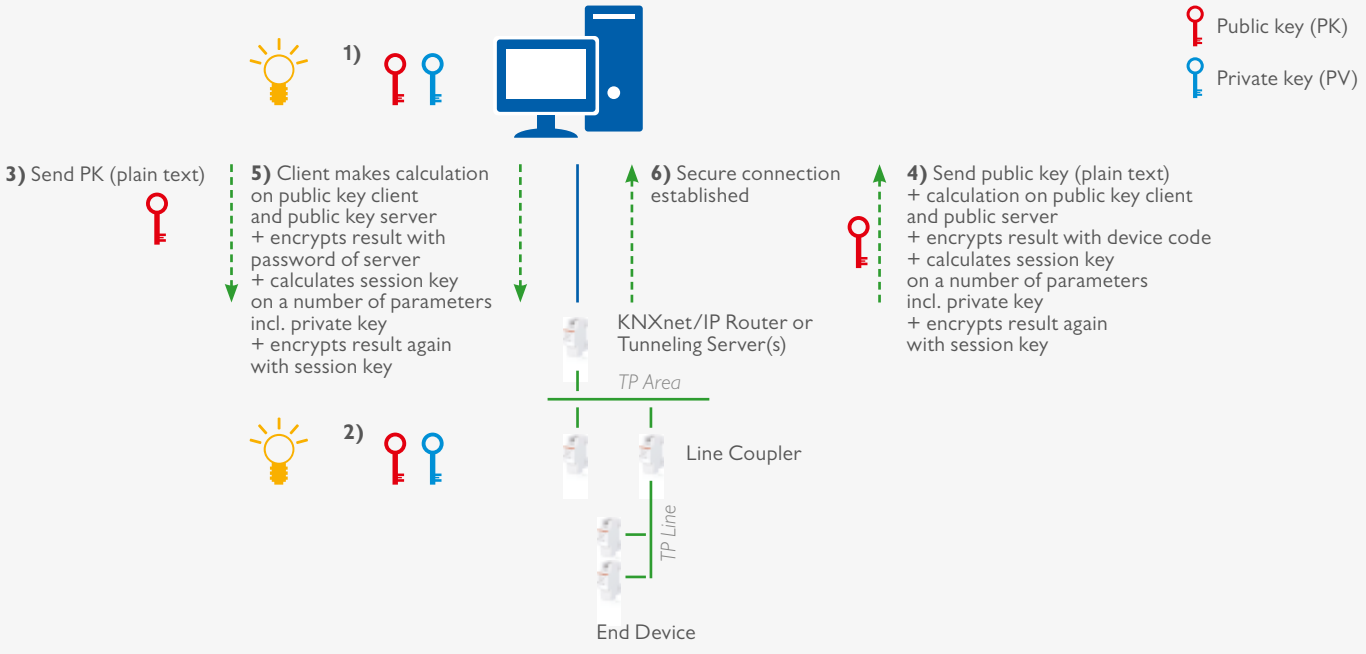


Procedura di protezione di dispositivi KNX

- Il server risponde con il proprio codice pubblico in plain text, allegato al risultato del calcolo: calcola il valore XOR del codice pubblico del server con il codice pubblico del client, lo codifica con il codice del dispositivo e lo autentica sul client, quindi lo codifica una seconda volta con il
- codice sessione calcolato.
- Il codice di autenticazione dispositivo è assegnato tramite ETS durante la configurazione o il codice strumento. Il codice di autenticazione dispositivo deve essere fornito all'operatore della visualizzazione che intende stabilire una connessione sicura con il relativo server.
- Il client esegue la stessa operazione XOR, ma l'autorizza codificandola innanzitutto con una delle password del server e di nuovo, una seconda volta, con il codice sessione. Si osservi che l'algoritmo di codifica utilizzato (Diffie Hellmann) garantisce che il codice sessione di client e server sia identico. La password del server deve essere fornita all'operatore della visualizzazione che intende stabilire una connessione sicura con il relativo server.

Per quanto concerne le misure di protezione della comunicazione runtime descritte sopra, si dovrà osservare che:

- Si possono utilizzare i dispositivi KNX Data Secure senza alcun problema accanto ai dispositivi KNX "classici". Ciò implica che si possono implementare i dati KNX e IP Secure come misura di sicurezza supplementare.
- Se un installatore sceglie di utilizzare un dispositivo KNX IP Secure in una dorsale IP, tutti gli accoppiatori IP e qualsiasi dispositivo KNX IP in tale backbone devono essere di tipo KNX IP Secure.



Impostazione di connessione KNX IP Secure

- Se l'installatore – su richiesta di un cliente - ha utilizzato per una funzione un dispositivo sicuro KNX per proteggere la comunicazione runtime, anche ogni partner della comunicazione di tale dispositivo deve supportare KNX Secure per la funzione collegata. In altre parole, l'oggetto di comunicazione di un KNX Secure Device non può essere collegato una volta a un indirizzo di gruppo protetto e una volta a un indirizzo di gruppo plain.

I dispositivi che supportano KNX Data e IP secure si distinguono dai dispositivi KNX "classici" per il segno "X" riportato sull'etichetta del prodotto.
KNX IP Secure e KNX Data Secure sono supportati da ETS 5.5 in avanti. ETS consente di configurare nuovi dispositivi KNX Secure e di sostituire quelli difettosi.

ACCOPPIAMENTO DI KNX A SISTEMI DI SICUREZZA

L'accoppiamento di KNX ad applicazioni come sistemi antifurto/antincendio/apertura porte può essere effettuato tramite:

- dispositivi o interfacce KNX con apposita certificazione dell'assicurazione locale contro le perdite;
- contatti potenzialmente liberi (ingressi binari, interfacce con pulsanti, ...);
- interfacce (RS232, ...) o gateways idonei: in questo caso, si dovrà garantire che la comunicazione KNX non possa attivare funzioni di sicurezza rilevanti nella parte dell'impianto dedicata alla sicurezza stessa.

RILEVAZIONE DI ACCESSO BUS NON AUTORIZZATO

Ovviamente, il bus potrà essere monitorato, tracciando il traffico insolito.
I dispositivi KNX Secure tracciano le violazioni nei log degli errori di sicurezza: in questo modo, è possibile controllare in qualsiasi momento se l'installazione KNX ha subito attacchi alla sicurezza.
Alcuni tipi di dispositivi possono rilevare se un altro dispositivo invia telegrammi con il loro indirizzo individuale. Ciò non viene evidenziato in automatico dalla rete, ma si può leggere in PID_DEVICE_CONTROL.
Un'implementazione molto recente può già mostrare il PID_DOWNLOAD_COUNTER.
Confrontando il valore di lettura (periodica) con un valore di riferimento, il segnale nella configurazione del dispositivo cambierà.

CONFORMITÀ AL REGOLAMENTO GDPR DELL'UE

GDPR è l'abbreviazione di General Data Protection Regulation [Regolamento generale per la protezione dei dati] (vedere https://ec.europa.eu/info/law/law-topic/data-protection_it), il cui scopo è armonizzare le leggi sulla protezione dei dati in tutta Europa.
Al fine di conformarsi al regolamento GDPR, l'installatore dovrà fornire una copia del file di progetto ETS al cliente. Installatore e cliente dovranno sottoscrivere una dichiarazione sulla privacy.
I dati generati dai dispositivi KNX possono soltanto essere utilizzati a fini di controllo remoto del dispositivo da parte del cliente (tramite app), a fini diagnostici e di ulteriore sviluppo del prodotto. Non possono essere utilizzati per pubblicità personalizzata.

Bibliografia

[1] AN 158 KNX Data Security
[2] AN 159 KNX IP Secure
[3] Volume 3/8/x KNXnet/IP Specifications

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