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

KNX SECURE CHECKLIST

CHECKLIST PER MAGGIORE SICUREZZA E PRIVACY NELLE INSTALLAZIONI KNX

1. Le seguenti misure sono state considerate durante l'installazione?

Dispositivi e applicazioni sono montati in modo fisso? È stato verificato che i dispositivi siano adeguatamente protetti dallo smontaggio (ad es. adozione di misure di protezione antifurto)?	☐
È garantito che le persone non autorizzate abbiamo accesso limitato ai quadri di distribuzione con installazioni KNX montate (ad es. sempre chiusi o posizionati in stanze chiuse)?	☐
È difficile accedere ai dispositivi nelle aree esterne? (ad es. montati ad altezza sufficiente)?	☐
In caso l'installazione KNX possa essere azionata da zone (di edifici) pubbliche e non sorvegliate, è stato previsto l'utilizzo di input binari (montati nei quadri di distribuzione) o interfacce a pulsante?	☐
I pannelli KNX Touch sono protetti da password (utente, gruppo o modalità ospite)?	☐

2. Si utilizza il doppino come mezzo di comunicazione?

I cavi sono protetti da accessi non autorizzati all'interno o all'esterno dell'abitazione o dell'edificio?	☐
In caso di utilizzo del doppino in zone che richiedono misure di protezione supplementari, sono state adottate le misure indicate al punto 6?	☐

3. Powerline è utilizzato come mezzo di comunicazione?

I filtri di arresto banda sono stati installati?	☐
Se si utilizza Powerline anche all'esterno dell'edificio, sono state adottate le stesse misure per l'accoppiatore di rete indicate al punto 6?	☐

4. IP è utilizzato come mezzo di comunicazione?

Le impostazioni di rete sono state documentate e fornite al proprietario dell'immobile o all'amministratore LAN?	☐
Switch e router sono stati impostati in modo che soltanto gli indirizzi MAC conosciuti possano accedere al mezzo di comunicazione?	☐
Per la comunicazione KNX, si utilizza una rete LAN o WLAN separata con hardware proprio?	☐
L'accesso alle reti IP (KNX) è limitato alle persone autorizzate tramite nomi utenti idonei e password forti?	☐
Per la comunicazione IP Multicast KNX, si dovrà utilizzare un altro indirizzo IP come indirizzo predefinito (solitamente 224.0.23.12). Questo indirizzo IP multicast è stato modificato?	☐
L'SSID predefinito del punto di accesso wireless è stato modificato? È stata disattivata la trasmissione periodica dell'SSID dopo l'installazione?	☐
Le porte dei router per KNX sono state chiuse a internet e il gateway predefinito del router KNXnet/IP utilizzato azzerato? L'installazione della (W)LAN è stata protetta da un firewall adeguato? Se è necessario l'accesso a internet per un'installazione KNX, verificare le possibilità da implementare: 1. Stabilire una connessione VPN all'Internet Router 2. Utilizzare KNX Object Server specifici del costruttore	☐

5. La frequenza radio è utilizzata come mezzo di comunicazione?

Sono state adottate le stesse misure per l'accoppiatore di rete indicate al punto 6?	☐
Ogni dominio RF ha un indirizzo di dominio diverso?	☐

6. Sono stati usati gli accoppiatori nell'installazione?

I singoli indirizzi dei dispositivi sono stati assegnati in base alla loro posizione nella topologia?	☐
Si prevede tramite l'impostazione di parametri corretti negli accoppiatori che indirizzi sorgente errati non siano inoltrati al di fuori della linea?	☐
La comunicazione in broadcasting e point-to-point attraverso l'accoppiatore è stata bloccata?	☐
Le tabelle filtro sono state caricate correttamente e le impostazioni effettuate in modo che gli accoppiatori considerino le tabelle filtro?	☐
Sono state adottate le misure indicate al punto 7 per gli accoppiatori?	☐

7. È stata bloccata la riconfigurazione dei dispositivi?

In caso contrario inserire un BCU key1 nel progetto ETS.	☐

8. Si utilizzano dispositivi KNX Secure[2]?

Per proteggere le comunicazioni di gruppo, utilizzare l'autenticazione prevista e il meccanismo di codifica del dispositivo. ☐

9. Si sospetta un accesso non autorizzato al bus?

Registrare il traffico dei telegrammi e analizzarlo. Nel caso dei dispositivi KNX Secure, consultare il Registro degli errori.
Documentare il tempo e gli effetti osservati (cosa accade, cosa non accade, perché e quando).
Disabilitare la connessione internet del sistema KNX e verificare se gli effetti scompaiono o meno.
Contattare la hotline del costruttore: gli effetti o i problemi di sicurezza sono noti al costruttore, gli aggiornamento sono disponibili? ☐

Leggere il PID_Device_Control[3] dei dispositivi e verificare se i medesimi eseguono l'invio con lo stesso indirizzo individuale. ☐

Leggere il PID_Device_Control[3] dei dispositivi e verificare se i medesimi eseguono nuovamente il download dopo la configurazione. ☐

10. È stata bloccata la riconfigurazione dei dispositivi?

Il collegamento di KNX agli impianti di sicurezza è stato realizzato in uno dei seguenti modi?
1. Tramite gateway o dispositivi KNX certificati da assicurazioni nazionali contro le perdite?
2. Tramite contatti potenzialmente liberi (input binari, interfacce con pulsanti, ...)?
3. Tramite i gateway o le interfacce previste (RS232, ...): è stato verificato che la comunicazione KNX non possa attivare funzioni rilevanti per la sicurezza nella parte dell'impianto dedicata alla sicurezza stessa? ☐

11. Misure di sicurezza generali

ETS è aggiornato?
1. Il PC, su cui è installato ETS, è sicuro (scansione virus aggiornata, ultimo aggiornamento del sistema operativo)? Si raccomanda di utilizzare un dispositivo dedicato per progettazione e messa in servizio di KNX.
2. Durante l'installazione, evitare di collegare altri dispositivi di memorizzazione dati non affidabili al PC (USB, disco fisso esterno, ...). ☐
3. Plug-in e app ETS saranno preferibilmente installate prima dell'installazione
4. Eseguire il backup del file di progetto dopo l'installazione (teoricamente su una chiavetta USB protetta,da conservare in sicurezza) e cancellare il progetto dal PC.

Il firmware del dispositivo utilizzato è aggiornato? ☐

12. Ulteriori misure relative alla privacy (GDPR)

Installatore e cliente dovranno sottoscrivere una dichiarazione sulla privacy. ☐

Al fine di adempiere ai regolamenti del GDPR, l'installatore dovrà fornire una copia del file di progetto ETS al cliente. ☐

[2] Disponibile da ETS 5.5 in avanti / [3] Non supportato su tutti i dispositivi