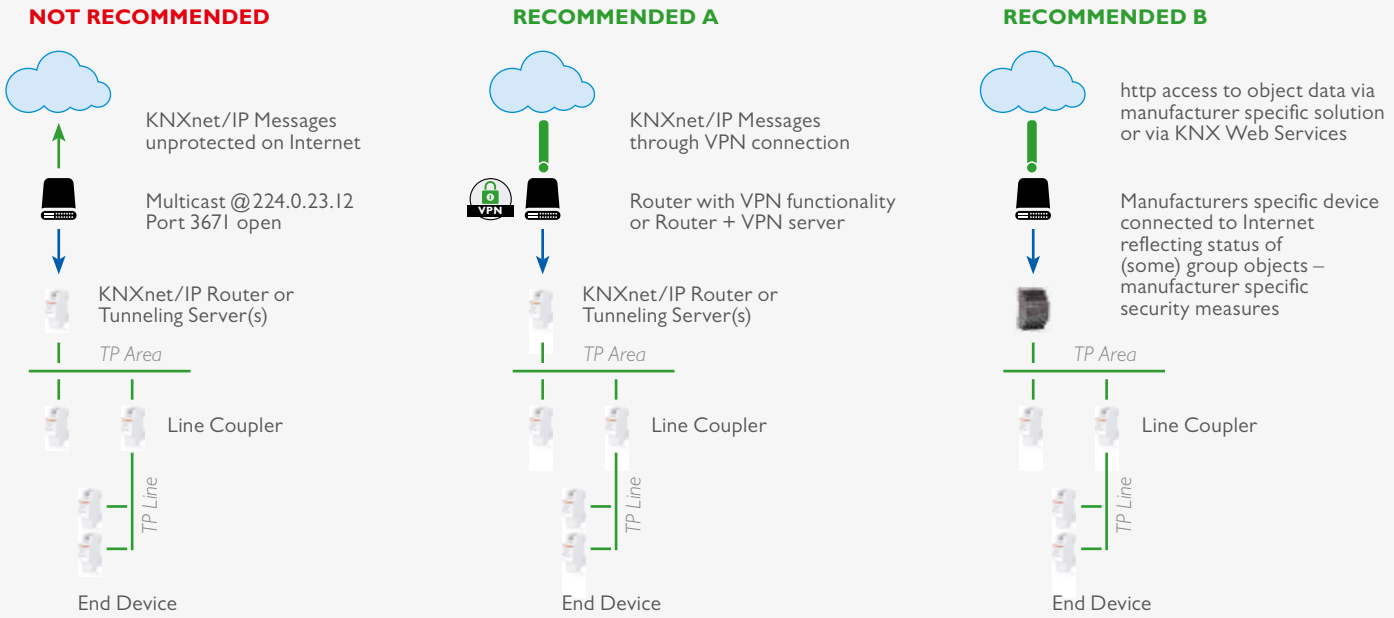
Smart home and building solutions.
Global. Secure. Connected.

KNX SECURE

NOTE DE SYNTHÈSE KNX SUR LA SÉCURITÉ ET LA CONFIDENTIALITÉ DES DONNÉES

Ce document destiné à servir de guide aux installateurs comme aux fabricants KNX présente les mesures courantes qui peuvent être prises pour renforcer la sécurité des installations KNX.

EMPÊCHER L'ACCÈS AUX DIFFÉRENTS MÉDIAS PHYSIQUES KNX PAR LE RÉSEAU



Accéder aux réseaux KNX par Internet

Un concept pertinent en matière de sécurité consiste en la prévention appropriée de tout accès non autorisé. Dans le cas d'une installation KNX, cela implique que seules les personnes autorisées (l'installateur, le gardien, l'utilisateur) peuvent accéder physiquement à l'installation KNX. Lors de la conception et de l'installation, pour chaque média KNX, les éléments critiques doivent être protégés de la meilleure manière possible.

Installation de câbles et d'appareils

- En général, les applications et les appareils doivent être correctement fixés pour éviter qu'il soit possible de les retirer facilement, ce qui permettrait à des personnes non autorisées d'accéder à une installation KNX.
- Les armoires et les tableaux de distribution contenant des appareils KNX doivent être correctement fermés ou montés dans des salles accessibles uniquement aux personnes autorisées.
- En extérieur, les appareils doivent être montés à une hauteur suffisante (par exemple : station météorologique, anémomètre, détecteur de mouvements, etc.).
- Dans tous les lieux publics qui ne sont pas suffisamment surveillés, il doit être envisagé de recourir à des appareils conventionnels combinés à des entrées binaires montées dans des endroits protégés (par exemple dans des tableaux de distribution) ou des interfaces à bouton-poussoir, pour empêcher ainsi l'accès au bus.
- Le cas échéant, les mesures de protection antivol prévues par certains modules d'application doivent être utilisées (par exemple : sécurisation des appareils par des vis, retrait possible uniquement au moyen d'outils, haute résistance à l'arrachement, etc.).

Paires torsadées

- Les extrémités des câbles ne doivent pas être visibles en dépassant de l'extérieur ou l'intérieur du mur du bâtiment.
- Un câble de bus en extérieur présente un risque supérieur. L'accès physique à un câble KNX à paires torsadées, dans ce cas, doit être rendu encore plus difficile que depuis la maison / le bâtiment même.

- Pour une protection supplémentaire, les appareils installés dans des endroits dont la surveillance est limitée (extérieur, parking souterrain, toilettes, etc.) peuvent être connectés à une ligne supplémentaire. En activant une table de filtrage dans des coupleurs de ligne conformément à la clause 2, il est possible d'empêcher un pirate d'accéder à l'installation entière.

Courant porteur

- Des filtres électroniques doivent être utilisés pour filtrer les signaux entrants et sortants.

Fréquence

- La radiofréquence étant un média ouvert, il n'est pas possible de prendre de mesures de protection physique pour empêcher l'accès. Pour cela, d'autres mesures doivent être prises, énoncées aux clauses 2 à 5 (en particulier, celles énumérées à la clause 4).

IP

- L'automatisation des bâtiments doit fonctionner sur un LAN et un WLAN dédiés disposant de leur propre matériel (routeurs, commutateurs, etc.).
- Indépendamment du type d'installation KNX, chacun doit, en tout état de cause, observer les mécanismes de protection habituels pour les réseaux IP, qui peuvent être les suivants :
  - Filtres MAC.
  - Cryptage des réseaux sans fil combiné à des mots de passe forts (modification du mot de passe par défaut – WPA2 ou supérieur) et leur protection contre l'accès à des personnes non autorisées.
  - Modification du SSID par défaut (le SSID est le nom sous lequel un point d'accès sans fil est visible sur le réseau ; généralement le fabricant et le type de produit). Les SSID par défaut peuvent indiquer les faiblesses spécifiques des produits aux points d'accès utilisés et, en ce sens, sont particulièrement vulnérables au piratage). Le point d'accès peut, de plus, être paramétré de sorte à empêcher le balisage (transmission périodique du SSID entre autres).
  - Pour la communication IP KNX multidiffusion, une autre adresse IP telle que l'adresse par défaut (224.0.23.12) doit être utilisée. Il peut être convenu d'une adresse appropriée avec l'administrateur réseau.
- Des spécialistes en réseaux informatiques doivent être impliqués dans les projets d'envergure comportant une connexion à KNXnet/IP : ainsi, il est toujours possible d'optimiser la configuration du réseau (commutateurs administrés, LAN virtuel, points d'accès avec IEEE 802.X, etc.) et d'autres mécanismes de protection tels qu'un filtrage des e-mails et des antivirus peuvent être mis en œuvre.

Internet

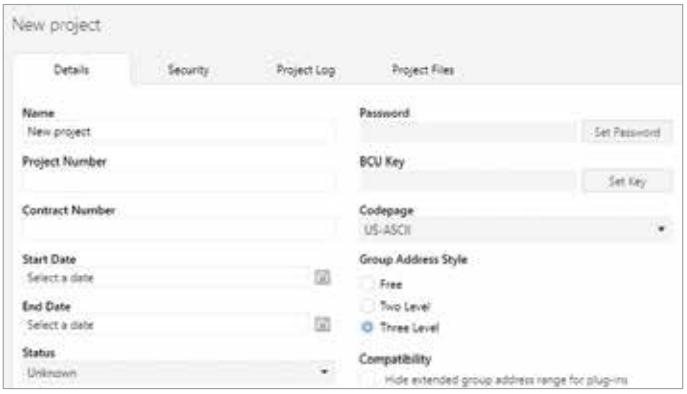
- Le routage KNXnet/IP et la tunnellisation KNXnet/IP ne sont pas conçus pour être utilisés sur Internet. Pour cette raison, il n'est pas conseillé d'ouvrir les ports des routeurs vers Internet, ce qui rendrait la communication KNX visible sur Internet.
  - L'installation (W)LAN doit être protégée au moyen d'un pare-feu.
  - Si aucun accès externe à l'installation n'est nécessaire, la passerelle par défaut peut être configurée à 0, ce qui a pour effet de bloquer toute communication vers Internet.
- Si l'on souhaite rendre possible l'accès à une installation via Internet, cela peut être réalisé comme suit :
  - Établir l'accès à l'installation KNX par des connexions VPN: cela nécessite cependant un routeur assurant la fonctionnalité de serveur VPN ou un serveur doté de la fonctionnalité VPN.
  - Toute solution de fabricant dédiée spécifique disponible sur le marché et visualisation (permettant par exemple un accès http).
  - KNX a spécifié, dans une extension de la norme KNX, une solution standardisée pour accéder aux installations KNX par Internet via des services en ligne.

LIMITER LES COMMUNICATIONS INDÉSIRABLES AU SEIN DU RÉSEAU

- L'adresse individuelle des appareils doit être attribuée de manière appropriée conformément à la topologie et les routeurs doivent être configurés de manière à ne pas transmettre de message d'une adresse source inappropriée. Ainsi, les communications indésirables peuvent être limitées à une ligne unique.
- La communication point à point et, si possible, en diffusion générale via les routeurs, doit être bloquée. Ainsi, la reconfiguration peut encore être limitée à une ligne unique.
- Les coupleurs doivent être configurés de sorte à utiliser les tables de filtrage activement et ne pas transmettre des adresses de groupe qui ne sont pas utilisées sur une ligne spécifique. Sinon, la communication insérée sur une ligne spécifique risque de se diffuser de manière incontrôlée sur toute l'installation KNX.

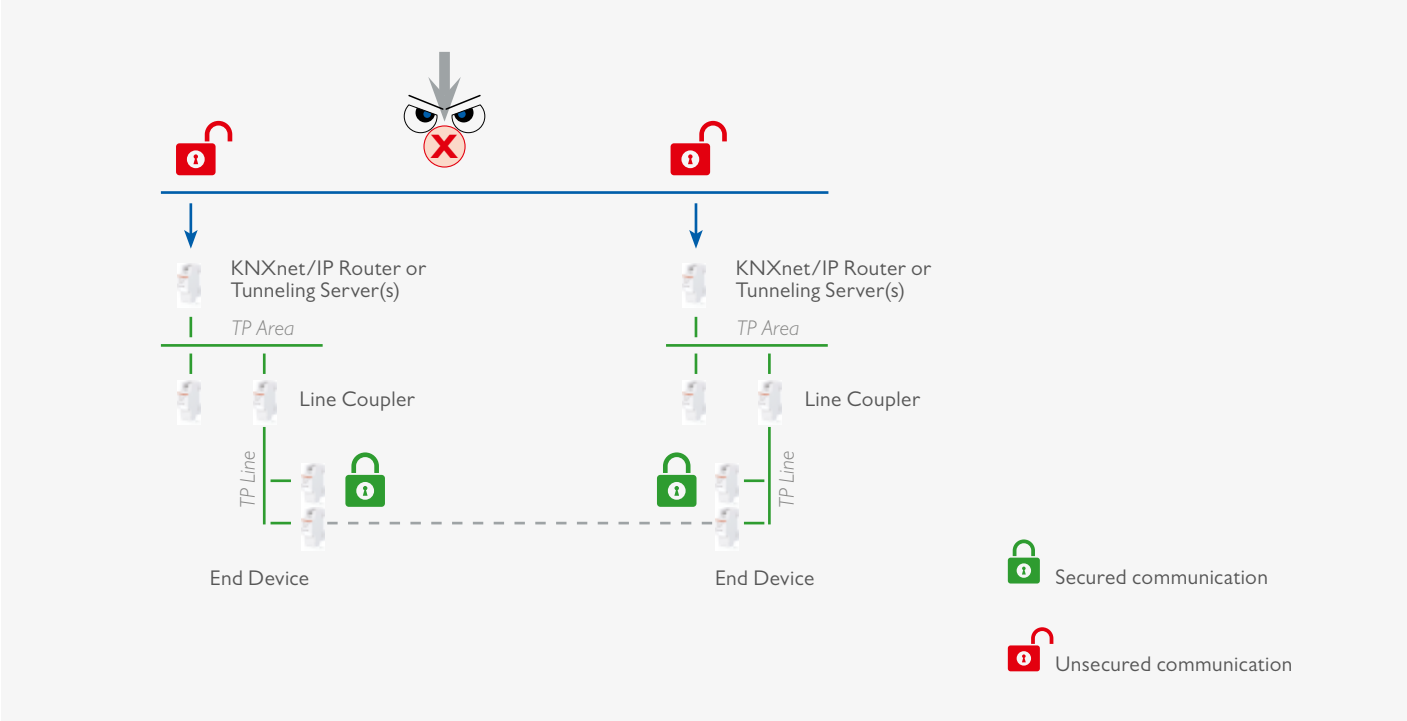
PROTÉGER LA CONFIGURATION DES COMMUNICATIONS

ETS permet de définir un mot de passe de projet spécifique au moyen duquel il est possible de verrouiller les appareils contre l'accès non autorisé. Cela empêche toute personne non autorisée de consulter ou de modifier la configuration de l'installation.



Protéger la configuration des communications dans ETS

PROTÉGER LA COMMUNICATION D'EXÉCUTION



Protéger la communication d'exécution KNX sur un réseau IP avec KNXnet IP Security

- En plus des mesures précédemment mentionnées, la communication d'exécution KNX peut être protégée par les mécanismes
  - KNX Data Secure et
  - KNX IP Secure spécifiés.
- KNX Data Secure garantit qu'indépendamment du média KNX sélectionné, les messages envoyés par des appareils KNX peuvent être authentifiés et/ou cryptés. Afin de garantir cela même dans le cas où cette communication ne serait pas sécurisée et que ces réseaux seraient connectés à l'IP, les mécanismes KNX IP Secure ont été définis en conséquence. Ainsi, l'impossibilité d'enregistrer ou de manipuler sur IP la tunnellisation KNX IP ou le routage des messages est assurée. Les mécanismes KNX IP Secure veillent à ce qu'un enveloppeur de sécurité soit ajouté autour du trafic de données KNXnet/IP complet.
- Les mécanismes KNX Data Secure et KNX IP Secure garantissent que les appareils peuvent établir un canal de communication sécurisé, assurant ainsi :

- L'intégrité des données, en empêchant tout pirate de prendre le contrôle en introduisant des trames manipulées. Pour ce faire, un code d'authentification est annexé à chaque message dans KNX : ce code annexé permet de vérifier que le message n'a pas été modifié et qu'il provient effectivement du partenaire de communication fiable.
- La fraîcheur, en empêchant tout pirate d'enregistrer des trames et de les exécuter de nouveau plus tard sans manipuler le contenu. Pour ce faire, un numéro de séquence est attribué dans KNX Data Secure, et un identifiant de séquence dans KNX IP Secure.
- La confidentialité, c'est-à-dire le cryptage du trafic du réseau pour garantir qu'un pirate aie la vision la plus restreinte possible sur les données effectivement transmises. Lors de l'autorisation du cryptage du trafic réseau KNX, l'appareil KNX assure au moins le cryptage conformément aux algorithmes AES-128 CCM avec une clé symétrique.

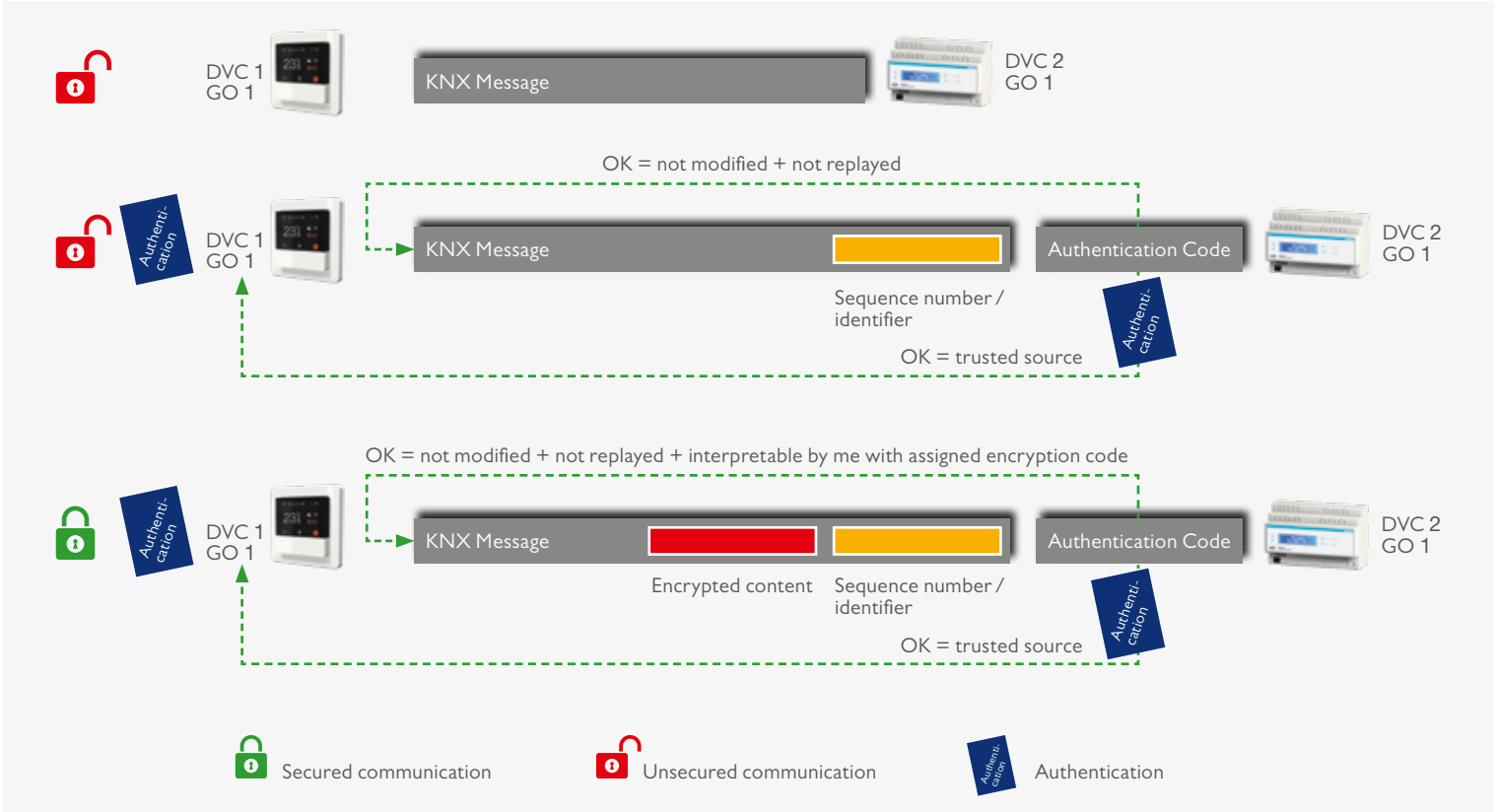
Une clé symétrique signifie qu'une même clé est utilisée par l'expéditeur pour protéger un message sortant (authentification + confidentialité !) et par le(s) destinataire(s) pour vérification lors de la réception du message.

Les appareils KNX Data Secure utilisent un format de télégramme KNX plus long lors de la transmission des données authentifiées et cryptées. Cela n'a aucun effet sur la vitesse de réaction des appareils. Pour KNX Data Secure, les appareils sont protégés de la manière suivante :

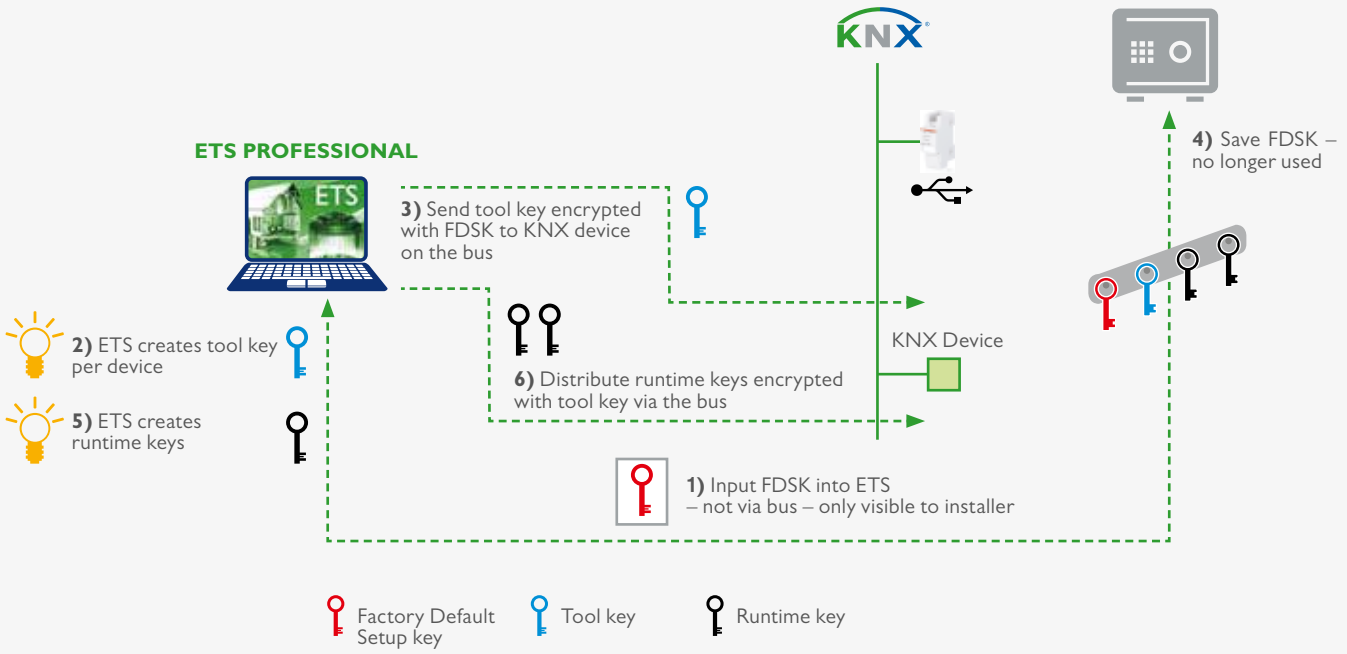
- Un appareil est expédié avec une clé de configuration d'appareil départ usine (FDSK).
- L'installateur saisit cette FDSK dans l'outil de configuration ETS (cette action n'est en aucun cas effectuée via le bus).
- L'outil de configuration crée une clé Tool Key propre à l'appareil.
- Via le bus, l'ETS envoie à l'appareil à configurer sa clé Tool Key, en cryptant et en authentifiant toutefois ce message avec la FDSK saisie précédemment. Ni la clé Tool Key ni la FDSK ne sont transmises à aucun moment en texte clair sur le bus.
- Désormais, l'appareil accepte uniquement la clé Tool Key aux fins d'une configuration ultérieure avec l'ETS. La FDSK n'est plus utilisée pour la communication ultérieure, sauf si l'appareil est réinitialisé départ usine, après quoi toutes les données sécurisées dans l'appareil seront effacées.
- L'ETS crée des clés d'exécution (autant que nécessaire) pour la communication de groupe devant être sécurisée.
- Via le bus, ETS envoie à l'appareil à configurer ces clés d'exécution, en cryptant et en authentifiant toutefois ces messages avec la clé Tool Key. Les clés d'exécution ne sont jamais transmises en texte clair sur le bus.

Pour KNX IP Secure, une connexion sécurisée (tunnellisation ou gestion d'appareil) est établie de la manière suivante :

- Le client comme le serveur créent une paire individuelle de clés publique/privée. Cela s'appelle le cryptage asymétrique.
- Le client envoie sa clé publique au serveur en texte clair.
- Le serveur répond avec sa clé publique en texte clair, affectée du résultat du calcul suivant : il calcule la valeur XOR de sa clé publique de serveur, crypte cela avec la clé publique du client, crypte cela avec le code de l'appareil pour s'authentifier lui-même auprès du client, et crypte cela une deuxième fois avec la clé de session calculée.



Vue d'ensemble des mécanismes KNX Data Secure



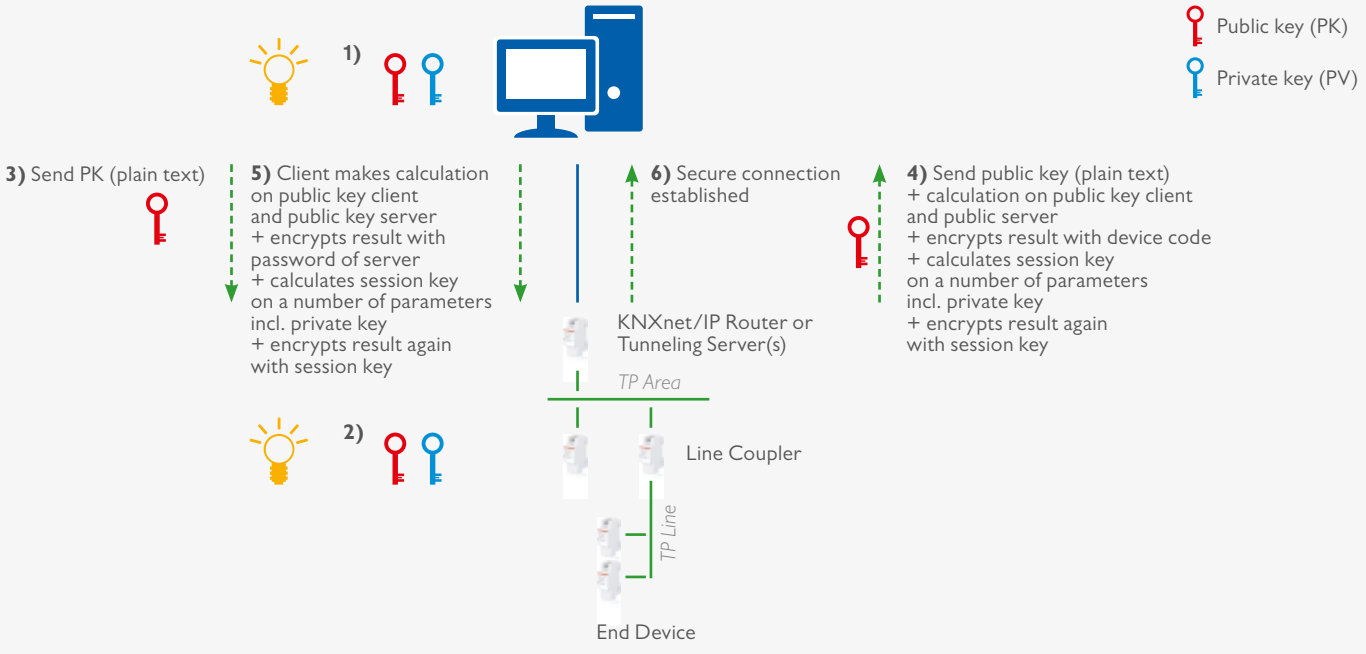
Procédure de sécurisation des appareils KNX

Le code d'authentification de l'appareil est soit attribué par l'ETS lors de la configuration, soit par la clé Tool Key. Ce code d'authentification d'appareil doit être fourni à l'opérateur de visualisation qui souhaite établir une connexion sécurisée avec le serveur correspondant.

- Le client réalise la même opération XOR, mais s'autorise lui-même en la cryptant d'abord avec l'un des mots de passe du serveur puis une deuxième fois avec la clé de session. Il convient de noter que l'algorithme de cryptage utilisé (Diffie Hellmann) garantit que les clés de session du client et du serveur sont identiques. Les mots de passe du serveur doivent être fournis à l'opérateur de visualisation qui souhaite établir une connexion sécurisée avec le serveur correspondant.

Concernant les mesures décrites ci-dessus pour protéger la communication d'exécution, il convient de noter que :

- Des appareils KNX Data Secure peuvent être utilisés sans aucun problème avec des appareils KNX « classiques ». Cela implique que les données KNX et IP Secure peuvent être mises en œuvre à titre de mesure de sécurité supplémentaire.
- Si un installateur choisit d'utiliser un appareil KNX IP Secure dans une zone IP, tous les coupleurs IP et les éventuels appareils KNX IP de cette zone doivent être du type KNX IP Secure.
- Si un installateur, à la demande du client, a utilisé un appareil KNX Secure pour une fonction afin de sécuriser la communication d'exécution, chaque partenaire de communication de cet appareil doit également prendre en charge KNX Secure pour la fonction associée. En d'autres termes, un objet de



Paramétrer une connexion KNX IP Secure

communication d'un appareil KNX Secure ne peut pas être associé une fois à une adresse de groupe sécurisée et une fois à une adresse de groupe en texte clair.

Il est possible de distinguer les appareils compatibles KNX Data et IP Secure des appareils KNX « classiques » grâce au signe « X » qui figure sur leur étiquette.

KNX IP Secure et KNX Data Secure sont pris en charge par les versions d'ETS 5.5 et supérieures. L'ETS permet de configurer de nouveaux appareils KNX Secure et il permet également de remplacer des appareils KNX Secure défectueux.

COUPLAGE DE KNX AUX SYSTÈMES DE SÉCURITÉ

Le couplage de KNX à des applications telles que des systèmes anti-effraction, coupe-feu ou d'ouverture de portes est possible au moyen :

- d'appareils ou d'interfaces KNX dûment certifiés par les assurances de dommages locales ;
- de contacts libres (entrées binaires, interfaces à bouton-poussoir, etc.) ;
- d'interfaces (RS232, etc.) ou de passerelles appropriées : si tel est le cas, il doit être veillé à ce que la communication KNX ne soit pas en mesure de déclencher de fonctions relatives à la sécurité dans la partie sécurité de l'installation.

DÉTECTION D'ACCÈS NON AUTORISÉ AU BUS

Bien entendu, il est possible de surveiller le bus et de tracer le trafic inhabituel.

Les appareils KNX Secure gardent trace des intrusions dans des journaux de failles de sécurité : ainsi, il est possible à tout moment de vérifier si l'installation KNX a subi des attaques de sécurité.

Certains types d'appareils peuvent détecter si un autre appareil envoie des télégrammes avec leur adresse individuelle. Cela n'est pas signalé spontanément sur le réseau, mais il est possible de le lire dans PID_DEVICE_CONTROL.

Une mise en œuvre très récente peut déjà afficher le PID_DOWNLOAD_COUNTER.

La comparaison de la valeur lue (périodiquement) avec une valeur de référence indique des changements de configuration des appareils.

CONFORMITÉ AUX DISPOSITIONS DU RGPD

RGPD est l'abréviation de Règlement général sur la protection des données (voir https://ec.europa.eu/info/law/law-topic/data-protection_fr).

Cette réglementation vise à harmoniser la législation relative à la protection des données dans toute l'Europe.

Afin de répondre aux obligations du RGPD, l'installateur doit remettre une copie du fichier de projet ETS au client.

L'installateur et le client doivent signer une déclaration relative à la protection des données.

Les données générées par des appareils KNX doivent être utilisées uniquement aux fins de la commande à distance de l'appareil par le client (via une application), à des fins de diagnostic et pour le développement ultérieur des produits. Elles ne peuvent pas être utilisées à des fins de publicité ciblée.

Dokumentation

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

v11-21


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


Join us
www.knx.org