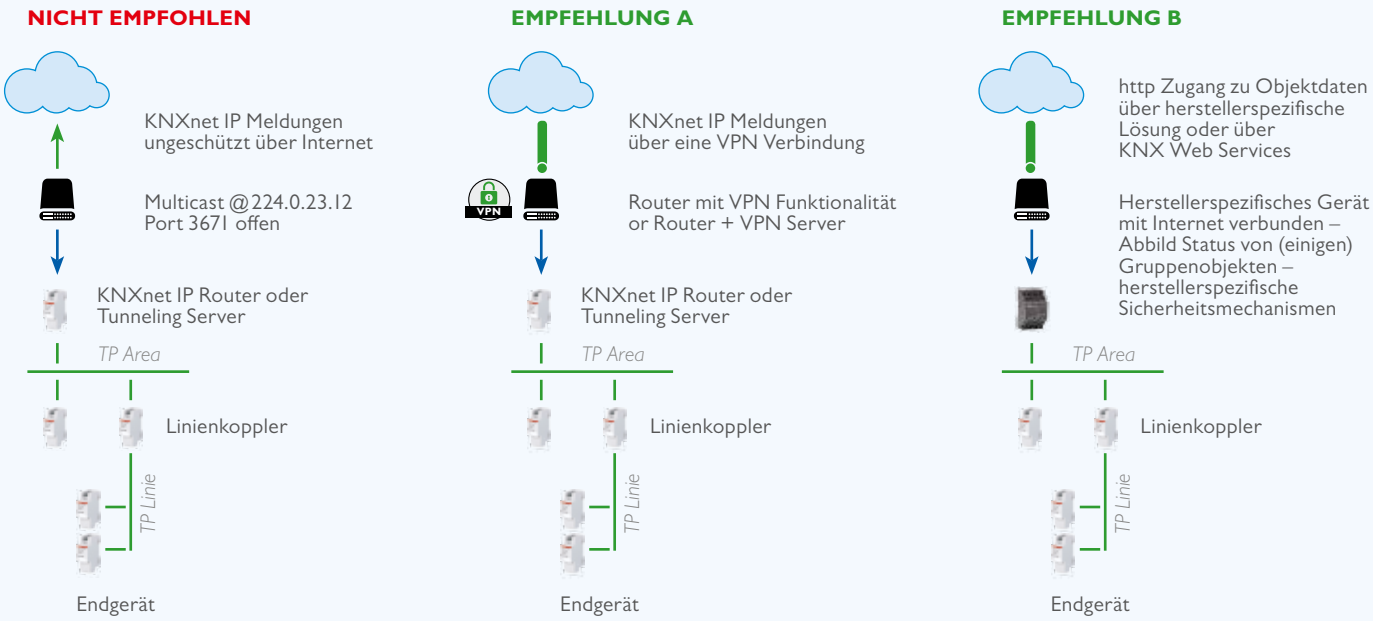
KNX Sicherheit

KNX Positionspapier zu Datensicherheit und Datenschutz

Dieses Papier ist als Leitfaden für Installateure sowie KNX Hersteller gedacht und beschreibt Mechanismen, die verwendet werden können, um die Sicherheit von KNX Anlagen zu verbessern.

1 Verhindern des Zugangs zu den unterschiedlichen KNX Medien



Zugang zu KNX Netzwerken über Internet

1.1 Einführung

Die Basis jedes Schutz-Konzeptes bildet die sorgfältige Abschottung des Systems gegen unberechtigten Zugriff. Im Falle einer KNX Anlage gilt, dass nur befugte Personen (Installateur, Hausmeister, Nutzer) physischen Zugang zur KNX Anlage haben dürfen. Bei der Planung und Installation müssen für jedes KNX-Medium die kritischen Punkte bestmöglich geschützt werden.

1.2 Montage von Leitungen und Geräten

- Allgemein gilt, dass Anwendungen und Geräte fest installiert werden sollten, um zu verhindern, dass diese leicht entfernt werden und dadurch unbefugte Personen Zugang zur KNX Anlage haben.
- Unterverteilungen mit KNX Geräten sollten verschlossen sein, oder sich in Räumen befinden, zu denen nur befugte Personen Zugang haben.
- Im Außenbereich sollten Geräte in ausreichender Höhe installiert werden (z. B. Wetterzentrale, Windsensor, Bewegungsmelder, ...).
- In allen nichtüberwachten öffentlichen Bereichen von Gebäuden sollte die Verwendung von konventionellen Geräten in Verbindung mit geschützt verorteten (z. B. in der Unterverteilung) Binäreingängen oder Tasterschnittstellen in Erwägung gezogen werden – so wird ein Buszugang erschwert.
- Wenn verfügbar, sollten die Diebstahlschutzeinrichtungen der Applikationsmodule verwendet werden (Sicherung durch Schrauben, nur mit Werkzeug entfernbar, hohe Abzugskräfte, ...).

1.3 Twisted Pair

- Die Leitungsenden des KNX Twisted Pair Kabels sollte nicht sichtbar sein oder aus der Wand herausstehen, weder innerhalb noch außerhalb des Gebäudes.
- Busleitungen im Außenbereich stellen ein erhöhtes Risiko dar. Der physische Zugang zum KNX Twisted Pair Kabel sollte hier besonders erschwert werden.

- Geräte, die in begrenzt geschützten Bereichen verbaut sind (Außenbereich, Tiefgarage, WC, etc.), können als zusätzlicher Schutz als eigene Linie ausgeführt werden. Durch Aktivierung der Filtertabelle im Linienkoppler gemäß Punkt 2 wird verhindert, dass ein Angreifer Zugriff auf die gesamte Anlage erlangen kann.

1.4 Powerline

- Elektronische Bandsperrfilter sollten zur Abgrenzung eintreffender und ausgehender Signale eingesetzt werden.

1.5 Funk

- Da Funk ein offenes Medium ist, können physische Schutzmechanismen den Zugang zum Medium nicht verhindern. Aus diesem Grund müssen die Maßnahmen ergriffen werden, die in den Punkten 2 bis 4 (und ins Besondere des Punkts 3) dieses Dokumentes aufgeführt sind.

1.6 IP

- Für die Gebäudeautomation sollte ein getrenntes LAN oder WLAN Netzwerk mit eigener Hardware (Router, Switches etc.) verwendet werden.
- Unabhängig von der KNX Anlage sind unbedingt die üblichen Sicherheitsmechanismen für IP-Netzwerke anzuwenden. Diese sind beispielsweise:
  - MAC-Filter
  - Verschlüsselung von Drahtlosnetzwerken bei Verwendung starker Passwörter (unbedingte Änderung des voreingestellten Passwortes – WPA2 oder höher) und Schutz dieser vor unbefugten Personen.
  - Änderung der voreingestellten SSID (SSID ist der Name, unter dem ein drahtloser Access Point sichtbar ist, meistens Hersteller und Typbezeichnung). Voreingestellte SSIDs können auf bekannte produktspezifische Schwächen der jeweiligen eingesetzten Access Points hinweisen und werden deswegen bevorzugt von Hackern angegriffen. Zusätzlich kann der Access Point so eingestellt werden, dass das sogenannte Beaconing (periodische Übermittlung u. a. der SSID) unterbunden wird.
- Für die Verwendung von KNX IP Multicast sollte eine andere als die voreingestellte IP-Adresse (voreingestellt: 224.0.23.12) verwendet werden. Eine geeignete Adresse kann mit dem Administrator des IP-Netzwerks abgesprochen werden.
- Für größere Projekte mit KNXnet IP Anbindung, sollten IT Netzwerkspezialisten herangezogen werden: auf diese Weise kann die Netzwerkkonfiguration weiter optimiert (Managed Switches, Virtual LAN, Access Points mit IEEE 802.1X, etc.) bzw. weitere Schutzmaßnahmen wie E-Mail Filter und Anti-Viren-Schutz implementiert werden.

1.7 Internet

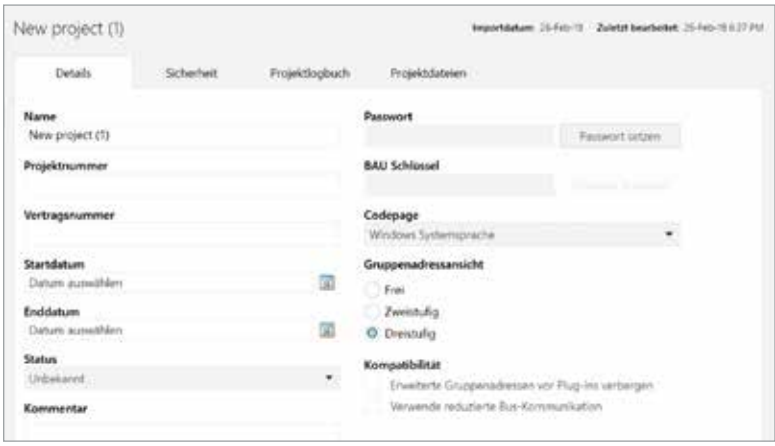
- KNXnet/IP Routing und KNXnet/IP Tunneling sind nicht für die Verwendung im Internet vorgesehen. Aus diesem Grund dürfen keine Ports von Routern Richtung Internet geöffnet werden: dies verhindert, dass die KNX Kommunikation im Internet sichtbar wird.
  - Die (W)LAN Anlage sollte über eine entsprechende Firewall geschützt werden.
  - Wird kein externer Zugriff auf die Anlage benötigt, können in KNXnet/IP Routern die Einstellungen für das Default-Gateway auf 0 gesetzt werden. Dadurch ist eine Kommunikation ins Internet unterbunden.
- Wenn auf eine Anlage aus dem Internet heraus zugegriffen werden soll, sollte dies wie folgt realisiert werden:
  - Zugang zu KNX Installationen über VPN Verbindungen: dies setzt jedoch einen Router mit VPN Server Funktionalität voraus oder einen Server mit VPN Funktion.
  - Verwendung einer der am Markt verfügbaren herstellerspezifischen Lösungen oder Visualisierungen (z. B. mit Zugang über http).
  - KNX hat eine Ergänzung zum KNX Standard zur Festlegung eines standardisierten Zugangs zu KNX Installationen über Internet und via Web Services spezifiziert.

2. Ungewollte Kommunikation im Netzwerk reduzieren

- Die physikalischen Adressen der Geräte sollten entsprechend der Topologie zugewiesen werden. Die Router sollten so konfiguriert werden, dass keine Meldungen mit inkorrekter Quelladresse weitergeleitet werden. Auf dieser Weise kann ungewollte Kommunikation auf eine einzige Linie begrenzt werden.
- Punkt-zu-Punkt und wenn möglich Broadcast Kommunikation über Router hinweg sollte blockiert werden. Auf dieser Weise wird Re-Konfiguration auf eine einzige Linie begrenzt.
- Die Koppler sollten so konfiguriert werden, dass Filtertabellen aktiv sind. So blockiert der Koppler Gruppenadressen, die kein Gerät in der Linie betreffen, wodurch verhindert wird, dass ein fremdes eingeschleustes Gerät Zugriff auf die gesamte KNX Anlage erlangen würde.

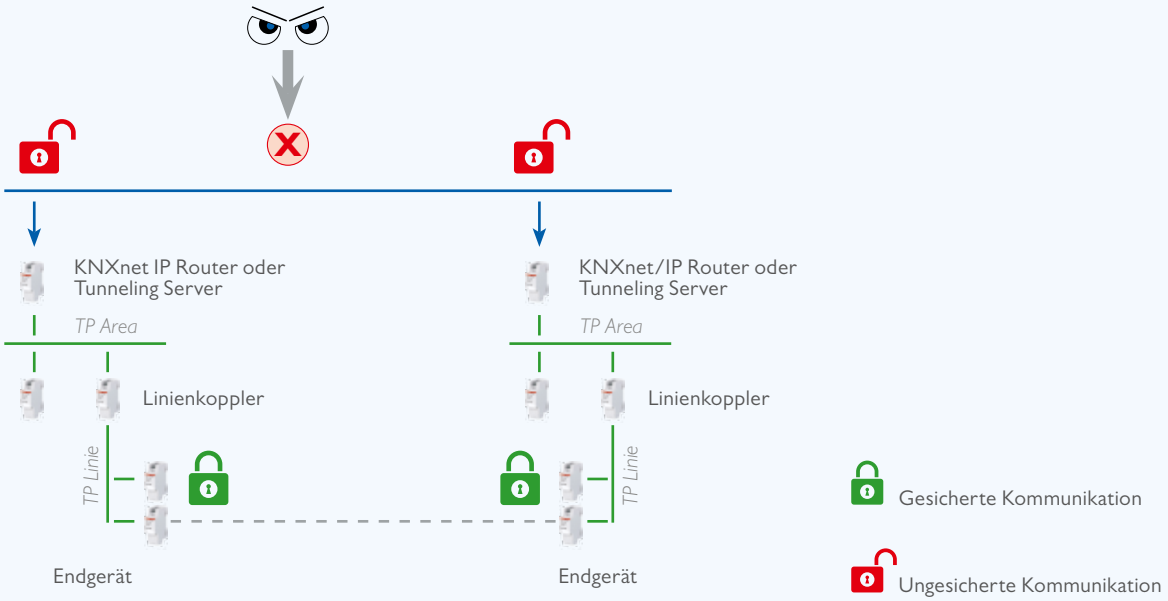
3. Konfigurationskommunikation schützen

Die ETS erlaubt ein projektspezifisches Passwort festzulegen, das Geräte gegen unerlaub-ten Zugang schützt. Der Passwortschutz verhindert, dass die Konfigurationsdaten durch unautorisierte Personen gelesen oder geändert werden.



Konfigurationskommunikation in der ETS schützen

4. Laufzeitkommunikation schützen

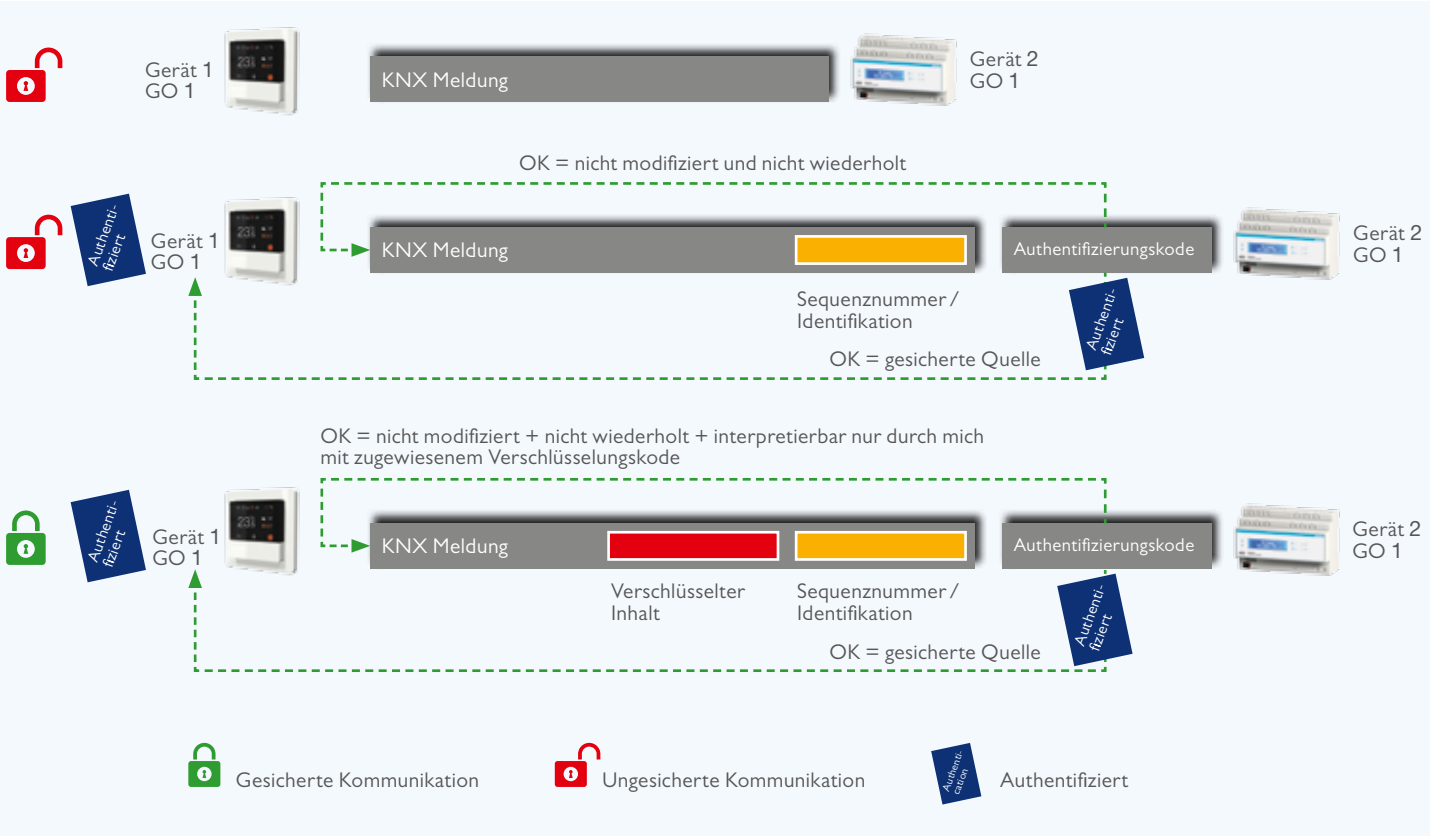


Schützen von KNX Laufzeitkommunikation in einem IP Netzwerk mittels KNXnet IP Secure

- Neben den oben aufgelisteten Maßnahmen, kann die KNX Laufzeitkommunikation über die folgenden spezifizierten Mechanismen geschützt werden:
  - KNX Data Secure und
  - KNX IP Secure
- KNX Data Security stellt sicher, dass unabhängig vom KNX Medium ausgewählte durch KNX Geräte ausgesendete Meldungen authentifiziert und/oder verschlüsselt werden. KNX IP Secure erlaubt, dass durch KNX Geräte ausgesendete Meldungen in IP-Netzen authentifiziert und verschlüsselt werden. Auf diese Weise ist sichergestellt, dass KNX Tunneling oder Routing Meldungen auf IP nicht mitgelesen oder manipuliert werden können. Die KNX IP Secure Mechanismen sind eine zusätzliche Sicherheitshülle, die den kompletten KNXnet IP Datenverkehr schützt.
- Die KNX Data Security und KNX IP Secure Mechanismen ermöglichen, dass Geräte einen gesicherten Kommunikationskanal aufbauen können, wobei folgendes sichergestellt wird:

- Datenintegrität, d. h. verhindern, dass ein Angreifer Kontrolle über die Anlage be-kommt, indem er manipulierte Meldungen einspeist. Bei KNX wird dies erreicht, indem ein Authentifikationscode jeder Meldung angehängt wird: dieser Code erlaubt es zu verifizieren, dass eine Meldung nicht verändert wurde und dass sie auch vom richtigen Kommunikationspartner stammt.
- Freshness, d. h. verhindern, dass Meldungen aufgezeichnet und zu einem späteren Zeitpunkt wieder abgespielt werden, ohne den Inhalt zu manipulieren. Bei KNX Data Secure wird dies über eine Sequenznummer und bei KNX IP Secure über eine Sequenzidentifikation sichergestellt.
- Vertraulichkeit, d. h. der Netzwerkverkehr wird verschlüsselt, sodass ein Angreifer den geringstmöglichen Einblick in die versendeten Daten hat. Zur Verschlüsselung von KNX Netzwerkverkehr lassen KNX Geräte eine Verschlüsselung gemäß AES-128 CCM Algorithmen mittels eines symmetrischen Schlüssels zu.

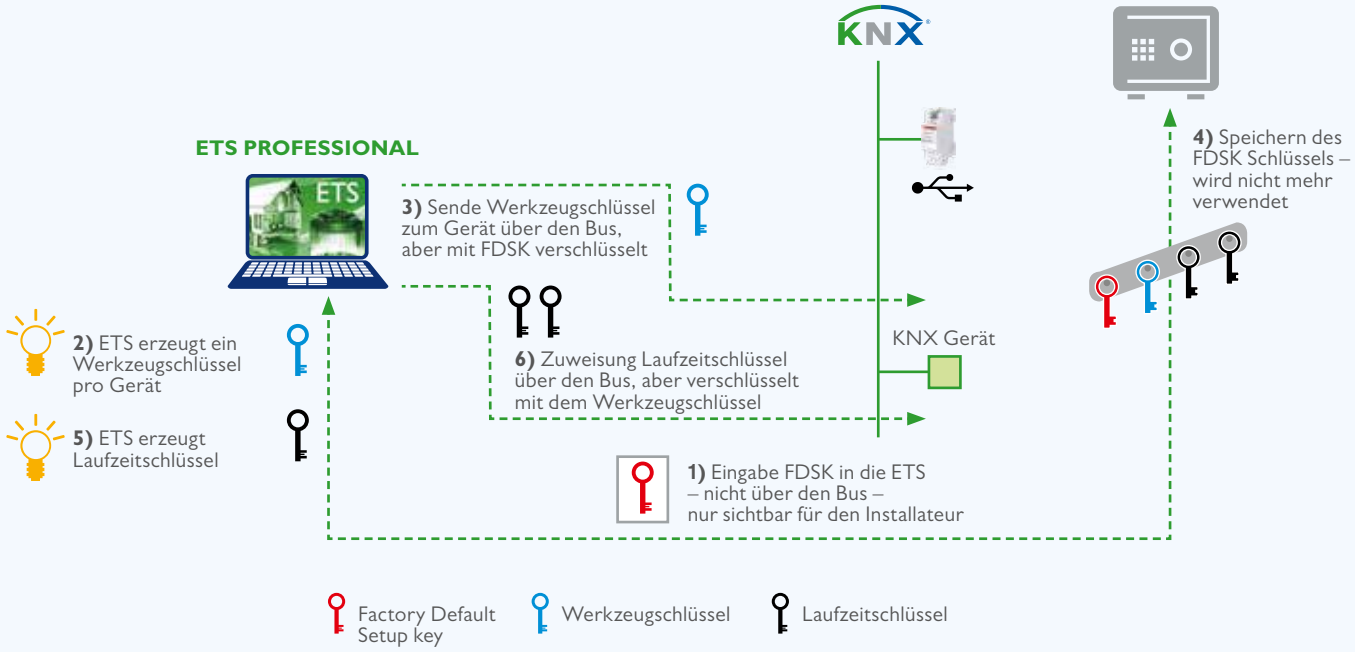
Ein symmetrischer Schlüssel bedeutet, dass der gleiche Schlüssel sowohl durch den Sender für die Verschlüsselung ausgehender Meldungen (Authentifizierung und Vertraulichkeit!) als durch den/die Empfänger zur Verifikation und Entschlüsselung der empfangenen Meldungen verwendet wird.



Übersicht der KNX Data Security Mechanismen

KNX Data Secure Geräte verwenden für die Übertragung der authentifizierten und verschlüsselten Daten ein längeres KNX Telegrammformat. Dies hat jedoch keine Auswirkungen auf die Reaktionsgeschwindigkeit der Geräte. Bei KNX Data Security werden Geräte auf folgende Art und Weise geschützt:

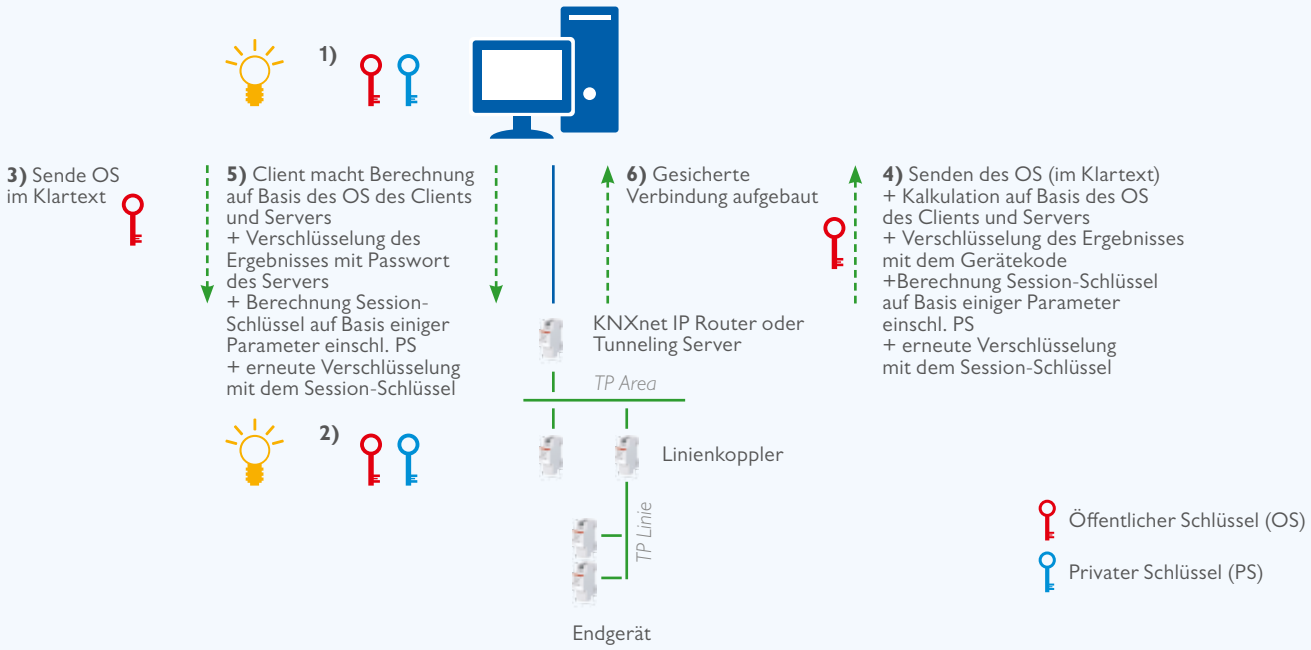
- Ein Gerät wird mit einer gerätespezifischen „Factory Device Set up Key (FDSK)“ ausgeliefert.
- Der Installateur gibt diesen Schlüssel in das Konfigurationswerkzeug (ETS) ein (dieser Vorgang erfolgt nicht über den Bus).
- Das Konfigurationswerkzeug erzeugt einen gerätespezifischen Werkzeugschlüssel.
- Über den Bus sendet die ETS den Werkzeugschlüssel zum Gerät, das konfiguriert werden soll. Die Übertragung wird mit dem ursprünglichen und vorher eingegebenen FDSK-Schlüssel verschlüsselt und authentifiziert. Weder der Werkzeug- noch der FDSK Schlüssel werden im Klartext über den Bus gesendet.
- Das Gerät akzeptiert nach der vorherigen Aktion nur noch den Werkzeugschlüssel für weitere Kommunikation mit der ETS. Der FDSK-Schlüssel wird für die weitere Kommunikation nicht mehr verwendet, es sei, das Gerät wird in den Auslieferzustand zurückgesetzt: dabei werden alle eingestellten sicherheitsrelevanten Daten gelöscht.
- Die ETS erzeugt so viele Laufzeitschlüssel wie für die Gruppenkommunikation, die man schützen möchte, benötigt werden.
- Über den Bus sendet die ETS die Laufzeitschlüssel zum Gerät, das konfiguriert werden soll. Die Übertragung erfolgt indem sie über den Werkzeugschlüssel verschlüsselt und authentifiziert wird. Die Laufzeitschlüssel werden nie im Klartext über den Bus gesendet.



Verfahren zur Verschlüsselung von KNX Geräten

Bei KNX IP Secure, wird eine gesicherte Verbindung (Tunneling oder Gerätemanagement) auf folgende Art und Weise aufgebaut:

- Sowohl Client als auch Server erzeugen eine Kombination eines individuellen öffentlichen/privaten Schlüssels. Dies wird als asymmetrische Verschlüsselung bezeichnet.
- Der Client sendet dem Server seinen öffentlichen Schlüssel im Klartext.
- Der Server antwortet mit seinem öffentlichen Schlüssel im Klartext und hängt das Ergebnis der folgenden Berechnung an: er berechnet den XOR Wert seines öffentlichen Schlüssels, verschlüsselt dies mit dem Gerätecode (um sich gegenüber dem Client zu authentifizieren) und verschlüsselt dies ein zweites Mal mit dem berechneten Session-Schlüssel.
  Der Geräte-Authentifikationsschlüssel wird entweder durch die ETS während der Konfiguration zugewiesen oder ist der Werkzeugschlüssel. Möchte eine Visualisierung eine gesicherte Verbindung mit dem jeweiligen Server herstellen, so muss ihr der Geräteauthentifikationsschlüssel zur Verfügung gestellt werden.
- Der Client führt die gleiche XOR Operation durch aber autorisiert sich indem er erstens mit dem Passwort des Servers und zweitens mit dem Session-Schlüssel verschlüsselt.
  Bei dem Vorgang ist zu beachten, dass der verwendete Verschlüsselungsalgorithmus (Diffie Hellmann) sicherstellt, dass der Session-Schlüssel des Clients und des Servers identisch sind.
  Möchte eine Visualisierung eine gesicherte Verbindung mit dem jeweiligen Server herstellen, so müssen ihr die Passwörter des Servers zur Verfügung gestellt werden.



Aufbau einer KNX IP Secure Verbindung

In Zusammenhang mit den oben beschriebenen Maßnahmen zum Schütz der Laufzeitkommunikation ist zu beachten, dass:

- KNX Data Secure Geräte problemlos in einer Anlage neben üblichen Geräten eingesetzt werden können. Das bedeutet konkret, dass KNX Data und IP Security als zusätzliche Maßnahme ergriffen werden können.
- Wenn jedoch der Installateur in einem IP Backbone ein KNX IP Secure Gerät einsetzt, alle anderen eingesetzten IP-Koppler und KNX IP Geräte ebenfalls IP Secure Geräte sein müssen.
- Wenn jedoch der Installateur (auf Wunsch des Kunden) für eine Funktion eines KNX Secure Gerätes die Laufzeitkommunikation geschützt hat, jede Kommunikationspartner dieses Gerätes für die verknüpfte Funktion ebenfalls KNX Secure unterstützen muss. Mit anderen Worten, ein Kommunikationsobjekt eines KNX Secure Gerätes kann nicht einmal mit einer geschützten KNX Gruppenadresse und einmal mit einer nicht-geschützten KNX Gruppenadresse verbunden sein.

Geräte, die KNX Data und IP Secure unterstützen, sind daran zu erkennen, dass auf dem Produktetikett ein ‚X' angebracht ist.

KNX IP Secure sowie KNX Data Secure werden ab ETS5.5 unterstützt. Die ETS lässt nicht nur zu, neue KNX Secure Geräte zu konfigurieren, sondern auch defekte Geräte auszutauschen.

5. Kopplung KNX mit Sicherheitsanlagen

Wenn eine KNX Anlage mit solchen Anwendungen wie Einbruchmelde-, Brandmelde- oder Türöffnersystemen gekoppelt wird, kann dies auf folgende Weise realisiert werden:

- über VdS approbierte KNX Geräte oder Schnittstellen;
- über potentialfreie Kontakte (Binäreingänge, Tasterschnittstellen, ...);
- über entsprechende Schnittstellen (RS232, ...) oder Gateways: in diesem Fall sollte sichergestellt werden, dass die KNX Kommunikation keine sicherheitsrelevanten Funktionen im Fremdsystem auslösen kann.

6. Unautorisierte Buszugriff detektieren

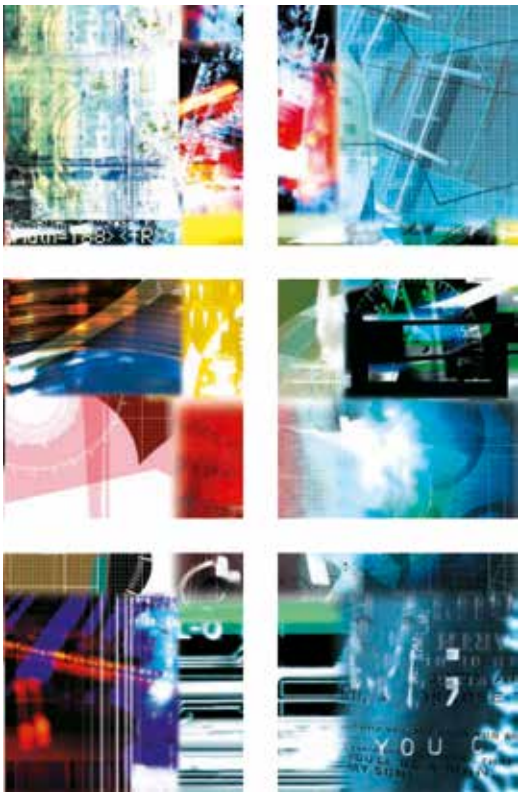
- Selbstverständlich kann der Bus jederzeit überwacht werden und ungewöhnlicher Verkehr aufgezeichnet werden.
- KNX Secure Geräte führen sogenannte Security Failure Logs : dadurch kann jederzeit erkannt werden, ob es Security Angriffe auf die KNX Anlage gab.
- Manche Geräte können feststellen, wenn andere Geräte Telegramme mit der eigenen physikalischen Adresse senden. Dies wird nicht auf den Bus gesendet, kann aber über den PID_Device_Control ausgelesen werden.
- Neue Implementierungen verfügen möglicherweise über den PID_Download_Counter. Wenn der Wert (zyklisch) ausgelesen und mit einem Referenzwert verglichen wird, kann aus dieser Information eine Änderung in der Gerätekonfiguration abgeleitet werden.

7. Erfüllung der EU GDPR Richtlinie

- GDPR steht für General Data Protection Regulation (siehe www.eugdpr.org). Die Richtlinie beabsichtigt die Harmonisierung von Datenschutzgesetzen in ganz Europa.
- Zur Erfüllung der GDPR Richtlinie ist vom Installateur die ETS-Projektdatei dem Kunden zu übergeben. Der Installateur und Kunde sollen gemeinsam eine Datenschutzerklärung unterschreiben.
- Von KNX Geräten gelieferte Daten dürfen nur für den Zweck der Remote-Steuerung durch den Nutzer (App), für Wartungszwecke und für die Produktentwicklung eingesetzt werden. Sie dürfen ausdrücklich nicht für personalisierte Werbung verwendet werden.

Literature

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



www.knx.org