Lingg & Janke

KNX Secure
Grundlagen

Lingg & Janke OHG, Zeppelinstraße 30, D-78315 Radolfzell, Germany
Tel. +49 (0) 77 32 / 9 45 57 50 info@lingg-janke.de www.lingg-janke.de Fax +49 (0) 77 32 / 9 45 57 99

1 Einführung

1.1 Vorwort

Sehr geehrte Kundin,
sehr geehrter Kunde,

in der KNX Welt hat ein neues Zeitalter begonnen, das Zeitalter der digitalen Verschlüsselung.

Wir, die Fa. Lingg & Janke, wollen Sie in dieses Zeitalter begleiten und Sie bei Ihren KNX Projekten mit unseren Produkten, die dem neuen KNX Secure Standard entsprechen, unterstützen.

1.2 Was ist KNX Secure?

KNX Secure ist die konsequente Weiterentwicklung des KNX Standards. Wurden bisher alle Daten auf dem KNX Bus offen und für jeden, der Zugriff auf diesen KNX Bus hat, mitlesbar und manipulierbar übertragen, so ist dies mit KNX Secure nicht mehr möglich.

Damit zieht die Datensicherheit und der Schutz der Privatsphäre auch in die moderne Elektroinstallation ein.

Im KNX Standard wird KNX Secure in KNX IP Security und KNX Data Security unterteilt.

KNX IP Security wird dann verwendet, wenn KNX Telegramme über KNX IP Linien- oder Bereichskoppler sowie KNX IP Gateways übertragen werden.
Bei allen anderen KNX Busteilnehmern wird KNX Data Security verwendet, so z. B. bei "normalen" KNX Geräten, die an der verdrillten Zweidraht-Leitung hängen. KNX Data Security wird also von fast allen Lingg & Janke KNX Produkten verwendet.

1.3 Wie funktioniert KNX Data Security?

KNX Telegramme bestehen im Wesentlichen aus zwei Teilen:

Einem Adress- und Steuerteil (Quelladresse, Zieladresse und Telegrammtyp) und einem Datenteil (Schaltwert, Temperaturwert oder Geräteparameter etc.).

Lingg & Janke OHG, Zeppelinstraße 30, D-78315 Radolfzell, Germany
Tel. +49 (0) 77 32 / 9 45 57 50 info@lingg-janke.de www.lingg-janke.de Fax +49 (0) 77 32 / 9 45 57 99

Verschlüsselt wird bei KNX Data Security nur der Datenteil. Dies hat den Vorteil, dass mit Hilfe der Quell- und Zieladresse das Telegramm über Linien- und Bereichskoppler vom Sender zum Empfänger geleitet werden kann, ohne dass jeweils eine Ent- bzw. Verschlüsselung in den Kopplern notwendig ist.

In einer Zweidraht KNX Installation können also herkömmliche Programmierschnittstellen (USB und IP) sowie herkömmliche Linien- / Bereichskoppler verwendet werden. Sie müssen jedoch lange Telegramme (Long Frames) verarbeiten können. Der Datenteil eines verschlüsselten KNX Telegramms ist etwas länger als der Datenteil eines herkömmlichen KNX Telegramms.

Damit ein verschlüsseltes KNX Telegramm (z. B. Jalousie auf) nicht einfach durch seine Wiederholung erneut zur Ausführung gebracht werden kann, enthält der Datenteil bei jeder Aussendung des Telegramms eine neue Nummer. Diese Sequenz-Nummer wird zwar unverschlüsselt übertragen, geht aber in die Verschlüsselung der Daten mit ein. Ist eine Sequenz-Nummer bei einem Empfänger bereits bekannt, so wird ein Telegramm mit dieser Sequenz-Nummer nicht mehr akzeptiert und damit nicht zur Ausführung gebracht. Neben dem Dateninhalt wird auch die Datenwiederholung abgesichert.

1.4 Was ist bei sicherer Inbetriebnahme zu beachten?

Da jeder Dateninhalt in einem KNX Secure Telegramm verschlüsselt sein kann, ist auch eine sichere Inbetriebnahme der einzelnen KNX Secure Geräte durch die ETS® möglich.

Um jedoch von Anfang an sicher, d.h. mit verschlüsselten Telegrammen, auf ein KNX Gerät zugreifen zu können, benötigt die ETS® einen ersten Geräteschlüssel, den so genannten Fabrikschlüssel (FDSK, Factory Default Setup Key).

Dieser Fabrikschlüssel wird in Form eines QR-Codes von Lingg & Janke zu jedem KNX Secure Gerät mitgeliefert. Im betreffenden Gerät ist der Fabrikschlüssel ebenfalls gespeichert.

Vor der Inbetriebnahme wird für jedes Gerät der QR-Code in die ETS® eingelesen. Im QR-Code ist auch noch die Seriennummer des Gerätes enthalten, so dass die ETS® weiß, zu welchem Gerät welcher Schlüssel gehört. Bei der Geräteparametrierung durch die ETS® wird durch Drücken der Programmiertaste die Seriennummer des betreffenden Gerätes abgefragt. Dadurch kann die ETS® den richtigen Fabrikschlüssel zuordnen und ab sofort mit dem Gerät verschlüsselt kommunizieren.

Lingg & Janke OHG, Zeppelinstraße 30, D-78315 Radolfzell, Germany
Tel. +49 (0) 77 32 / 9 45 57 50 info@lingg-janke.de www.lingg-janke.de Fax +49 (0) 77 32 / 9 45 57 99

Um die Sicherheit noch weiter zu steigern wird von der ETS® jetzt ein neuer Geräteschlüssel automatisch erzeugt. Dieser wird unter Verwendung des Fabrikschlüssels in das zu parametrierende Gerät übertragen. Der neue ETS® Schlüssel wird als "Tool Key" bezeichnet und gilt sofort nach der Übertragung. Er ist nur der ETS® bzw. dem ETS® Projekt für die betreffende KNX Installation bekannt. Mit dem Fabrikschlüssel kann danach nicht mehr auf das Gerät zugegriffen werden.

1.5 Wie werden Daten verschlüsselt?

In der weiteren Parametrierung wird jeder Gruppenadresse, die an das KNX Gerät vergeben wurde, von der ETS® ein weiterer, neuer Gruppenschlüssel automatisch zugeordnet und in das Gerät geladen. D. h. wenn ein KNX Gerät mit dreißig unterschiedlichen Gruppenadressen parametriert wird, dann werden auch dreißig zugeordnete Gruppenschlüssel in das Gerät überspielt. Jedes Telegramm, das eine andere Gruppenadresse enthält, wird auch mit einem anderen Gruppenschlüssel verschlüsselt. Dies erhöht die Sicherheit nochmals enorm. Einen Generalschlüssel gibt es bei KNX Secure nicht. Jedes Gerät hat einen eigenen ETS® Schlüssel und jede Gruppenadresse hat einen eigenen Gruppenschlüssel.

1.6 Wie wird Projektsicherheit erzeugt?

Doch dem noch nicht genug. Die ETS® vergibt auch an jedes zu parametrierende KNX Gerät eine eigene Sequenz-Nummer. Und die ETS® teilt allen in einer Installation (in einem ETS® Projekt) beteiligten Geräten mit, wer mit welcher Physikalischen Adresse mit wem kommuniziert bzw. kommunizieren darf. Die Geräte in einer Installation (in einem ETS® Projekt) bilden also eine geschlossene Gruppe. Daher muss eine Installation immer zwingend mit nur einem ETS® Projekt in Betrieb genommen werden. Ein neu hinzugefügtes Gerät kann mit den Geräten in einer Gruppe nicht sofort kommunizieren. Hinzugefügte Geräte bedingen die Neuparametrierung aller bisherigen Geräte, mit denen sie kommunizieren wollen. Dies erhöht die Sicherheit auf ein Maximum.

Ohne das ETS® Projekt für eine betreffende KNX Installation kann an dieser Installation praktisch nichts verändert werden. Wer das ETS® Projekt hat, hat die uneingeschränkte Projekthoheit. Das garantiert Eigentümern und Projekterstellern, dass unerlaubte Veränderungen, die zu Fehlern führen können, nicht möglich sind. Bei sicherer Inbetriebnahme erzwingt die ETS® auch ein Projekt-Passwort. Geht das Passwort verloren, ist das ETS® Projekt nicht mehr verwendbar und die KNX Installation kann nicht mehr verändert werden.

Lingg & Janke OHG, Zeppelinstraße 30, D-78315 Radolfzell, Germany
Tel. +49 (0) 77 32 / 9 45 57 50 info@lingg-janke.de www.lingg-janke.de Fax +49 (0) 77 32 / 9 45 57 99

Die KNX Produkte selbst können jedoch wiederverwendet werden. Nach einem "Rücksetzen auf Auslieferungszustand (Factory Reset)" können die Geräte wieder neu programmiert werden. Alle bisherigen Schlüssel, Gruppenadressen etc. werden jedoch gelöscht, so dass das Gerät nicht mehr zur bisherigen Installation gehört.

1.7 Können KNX Secure Geräte mit bisherigen KNX Geräten kommunizieren?

Sichere Inbetriebnahme und sichere, verschlüsselte Kommunikation sind jedoch nicht zwingend vorgeschrieben. Für jedes KNX Secure Gerät kann vor der Parametrierung entschieden werden, ob das Gerät sicher, d. h. verschlüsselt, oder unsicher, d. h. unverschlüsselt, in Betrieb genommen werden soll. Bei Lingg & Janke können alle KNX Secure Geräte, für die es eine bisherige, ungesicherte ETS® Applikation gibt, auch mit dieser bisherigen Applikation in Betrieb genommen werden. Die KNX Secure Geräte verhalten sich dann wie herkömmliche KNX Geräte. Im Auslieferungszustand sind alle Lingg & Janke Geräte im ungesicherten Modus.

Ebenso kann für jede Gruppenadresse bzw. für jedes daraus entstehende Gruppentelegramm festgelegt werden, ob verschlüsselt oder unverschlüsselt übertragen werden soll. So können auch ältere KNX Geräte, die KNX Secure noch nicht unterstützen, mit neuen KNX Secure Geräten kommunizieren. Ein Mischbetrieb zwischen alt und neu ist problemlos möglich.

Wird jedoch sichere Kommunikation gewünscht, so muss auch sichere Inbetriebnahme verwendet werden. Sonst könnten im unsicheren Modus alle Gruppenschlüssel ausgelesen werden und eine sichere Übertragung wäre nicht gewährleistet.

Soweit eine kurze Einführung in KNX Secure.

In der Praxis merken Sie von all diesen technischen Neuheiten nur, dass Sie sie einschalten oder ausschalten können. Der Rest geschieht in den Geräten automatisch.

Viel Erfolg mit den neuen KNX Secure Geräten von Lingg & Janke wünscht Ihnen

Ihr Peter Janke

Lingg & Janke OHG, Zeppelinstraße 30, D-78315 Radolfzell, Germany
Tel. +49 (0) 77 32 / 9 45 57 50 info@lingg-janke.de www.lingg-janke.de Fax +49 (0) 77 32 / 9 45 57 99

1.8 Häufig gestellte Fragen (FAQs)

Muss ein KNX Secure Gerät sicher in Betrieb genommen werden?
NEIN
Das Gerät wird immer im unsicheren Modus ausgeliefert. In der ETS® kann sichere Inbetriebnahme aktiviert oder deaktiviert werden.

Müssen Gruppentelegramme bei KNX Secure Geräten immer verschlüsselt übertragen werden?
NEIN
Für jede Gruppenadresse und jedes daraus entstehende Gruppentelegramm kann in der ETS® festgelegt werden, ob verschlüsselte oder unverschlüsselte, herkömmliche Übertragung gewünscht wird. Dazu wird in den Einstellungen die Sicherheit entweder ein- oder ausgeschaltet. Wird "Automatisch" ausgewählt, entscheidet die ETS® selbst, ob Sicherheit möglich ist oder nicht. Sicherheit ist dann möglich, wenn alle beteiligten Geräte KNX Secure unterstützen und sicher in Betrieb genommen werden.

Können ältere KNX Geräte mit neueren KNX Secure Geräten kommunizieren?
JA
Bei den betreffenden Gruppenadressen muss die Sicherheit ausgeschaltet werden.

Können sicher in Betrieb genommene KNX Secure Geräte nachträglich umparametriert werden?
JA
Es muss ein "Zurücksetzen auf Herstellungszustand (Factory Reset)" durchgeführt werden.
Folgende Schritte sind durchzuführen: Busklemme abziehen / Programmiertaste drücken und gedrückt halten / Bus anstecken / Programmier-LED leuchtet auf / Programmiertaste loslassen / Warten bis Programmier-LED aus geht (ca. 5 Sek.) / Gerät ist im Auslieferungszustand.

Ist für die sichere Inbetriebnahme ein Zusatzaufwand notwendig?
JA
Der Zusatzaufwand ist jedoch gering.
Es müssen alle QR-Codes der verwendeten Produkte in die ETS® eingelesen werden. Dies geschieht über die eingebaute Kamera im Laptop oder über eine mit dem Laptop verbundene USB Kamera.
Die Inbetriebnahmezeit pro Gerät steigt etwas an. Bei Lingg & Janke Geräten beträgt diese Zusatzzeit ca. 10 - 20 Sek. Im unsicheren Modus werden ca. 30 Sek. für den Download benötigt. D. h. die Gesamtzeit für sichere Inbetriebnahme pro Gerät beträgt ca. 40 - 50 Sek.

Lingg & Janke OHG, Zeppelinstraße 30, D-78315 Radolfzell, Germany
Tel. +49 (0) 77 32 / 9 45 57 50 info@lingg-janke.de www.lingg-janke.de Fax +49 (0) 77 32 / 9 45 57 99

Ist eine KNX Secure Installation schwieriger in der Wartung?
NEIN
Voraussetzung ist jedoch, dass das betreffende ETS® Projekt zur Verfügung steht.
Ist das ETS® Projekt geöffnet, können alle Telegramme in der ETS® unverschlüsselt dargestellt und aufgezeichnet werden. Es besteht praktisch kein Unterschied zu einer herkömmlichen KNX Installation.

Können die Schlüssel aus einem ETS® Projekt exportiert werden?
JA
Es kann eine XML Datei mit allen in diesem Projekt verwendeten Schlüsseln erstellt werden. Diese "Schlüsselbund"-Datei muss mit einem Passwort gesichert werden.

Gibt es eine KNX Secure Visualisierung?
JA
Lingg & Janke vertreibt eine passende KNX Visualisierung, die den KNX Secure Standard unterstützt. Die notwendigen Schlüssel werden mit Hilfe der "Schlüsselbund"-Datei übertragen.

Soll man KNX Secure nur auf Kundenanforderungen anwenden?
NEIN
Ein verschlüsseltes KNX Projekt bietet auch dem Installateur / Systemintegrator einen optimalen Projektschutz vor unerlaubten Eingriffen.

Reicht in einer KNX Installation KNX IP Security als Schutz aus?
NEIN
KNX IP Security bietet nur einen Schutz auf dem IP-Netzwerk. Auf dem restlichen KNX Bus sind alle Telegramme ungeschützt.
Umgekehrt ist das anders. Wird KNX Data Security verwendet, dann sind alle Telegramme auf dem KNX Bus geschützt, also auch die, die über das IP-Netzwerk laufen.

Kann eine KNX Secure Installation, für die das betreffende ETS® Projekt nicht mehr vorhanden ist, geändert werden?
NEIN
Ohne das betreffende ETS® Projekt, in dem alle Schlüssel vorhanden sind, können weder Geräte umparametriert werden, noch können weitere Geräte hinzugefügt werden. Gäbe es hier eine Möglichkeit, wäre die Installation nicht geschützt.
Die einzige Möglichkeit ist dann, alle Geräte in den Auslieferungszustand zurückzusetzen und neu zu beginnen.

Lingg & Janke OHG, Zeppelinstraße 30, D-78315 Radolfzell, Germany
Tel. +49 (0) 77 32 / 9 45 57 50 info@lingg-janke.de www.lingg-janke.de Fax +49 (0) 77 32 / 9 45 57 99

1.9 Notizen

Lingg & Janke OHG, Zeppelinstraße 30, D-78315 Radolfzell, Germany
Tel. +49 (0) 77 32 / 9 45 57 50 info@lingg-janke.de www.lingg-janke.de Fax +49 (0) 77 32 / 9 45 57 99