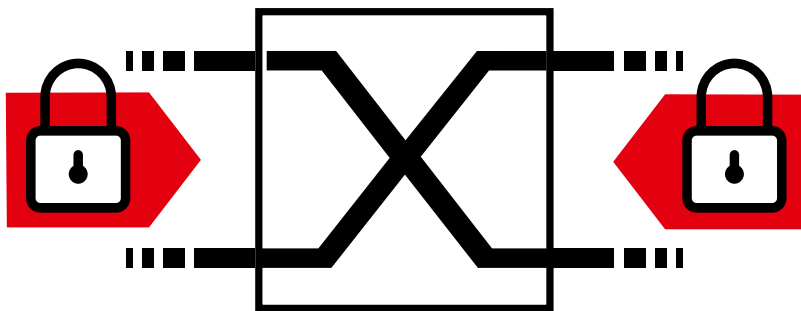


hiXserver

Die Digitalplattform für intelligente Gebäude- sicherheit und -steuerung



hiXserver

Starten Sie mit dem
hiXserver in das digitale
Sicherheitszeitalter!

Digitalplattform hiXserver:

Enorme Vorteile –
höchste Sicherheit für
jede Gebäudeart



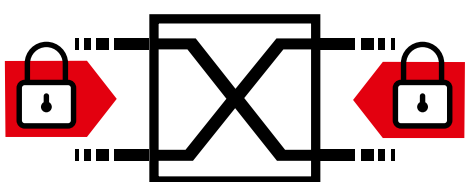
Als erste Digitalplattform ermöglicht hiXserver die vollumfängliche und komfortable Fernservice-Verbindung und Verwaltung zu einer Einbruch- und Gefahrenmeldeanlage von TELENOT, unabhängig von der Netzinfrastruktur, in welcher diese betrieben wird. hiXserver ermöglicht von jedem Ort der Welt die gesicherte, komplette Datenverwaltung und Regelung sämtlicher Zugriffsrechte auf das jeweilige Objekt.

- Änderungen der Parametrierung auf Wunsch Ihres Kunden
- Firmware-Updates
- Fehlersuche und Störungsbeseitigung
- Transponder einlernen
- Service
- Statusabfrage
- u. v. m.

Ebenso ermöglicht die Digitalplattform die sichere, intelligente Steuerung und Bedienung der Einbruch- und Gefahrenmeldeanlagen und smarter Zusatzfunktionen für den Endkunden via Alarmanlagen-App BuildSec 4.0. Über die innovative Digitalplattform hiXserver können Sie und Ihre Kunden mithilfe der Services

- hiXmobile (vgl. Seite 8)
- hiXremote (vgl. Seite 10)
- hiXuser (vgl. Seite 11)

gesichert auf Einbruch- und Gefahrenmeldeanlagen aus dem Hause TELENOT zugreifen. Zudem genießen Sie und Ihre Endkunden enorme Vorteile und Mehrwerte beim Handling und der Administration. Jederzeit und überall. Sie stoßen in eine neue, absolut sichere und zeitsparende Dimension der digitalen Verwaltung und Steuerung Ihrer Objekte vor.



hiXserver



Vorteil 1 ✓

Schnelle und komfortable Einrichtung beim Kunden

Die Digitalplattform hiXserver löst diverse Herausforderungen, die beim Einrichten eines Fernservices oder einer App-Steuerung auftreten können. Themen wie eine öffentliche IP-Adresse, die Portweiterleitung im Router, gesicherte Firmennetze, die Beachtung unterschiedlicher Netzinfrastrukturen (IPv4 / IPv6 – Dual-Stack Lite-Anschlüsse), unterschiedliche Router u. v. m. sind außen vor.

Da die Digitalplattform hiXserver als ein mit dem Netz verbundener Vermittlungsserver agiert, zu dem alle beteiligten Kommunikationspartner eine abgehende Verbindung aufbauen,

✓ **Keine Haftungsprobleme**

✓ **Problemloser Hardwareaustausch**

✓ **Unabhängigkeit von Netzinfrastruktur**

können Sie unabhängig von all diesen sich ständig ändernden Netzparametern agieren. Damit entfallen die aufwendigen Anpassungen und Analysen der Netzinfrastruktur, ebenso eventuelle Anpassungen an der Hardware (Router etc.) und gefährliche Haftungsfragen.

Selbst der Austausch von Hardware (wie dem Router bei einer bereits installierten Einbruch- und Gefahrenmeldeanlage im Objekt selbst) hat für Sie und Ihre Kunden keine Auswirkungen mehr – weder auf den Fernservice noch die gewünschten mobilen Steuerungsfunktionen via der Alarmanlagen-App BuildSec 4.0 (vgl. Seite 8).

Sie müssen keine neuen Routereinstellungen vor Ort beim Kunden vornehmen. Die einzige Voraussetzung dazu ist die Verbindung der Gefahrenmeldeanlage mit dem Router (per LAN oder WLAN) bzw. mit dem Internet.

Vorteil 2 ✓

TLS und AES für eine sichere Ende-zu-Ende-Verschlüsselung

Die Digitalplattform hiXserver nutzt für die Kommunikation die hochsicheren Verschlüsselungen TLS (Transport Layer Security) mit beidseitig zertifikatsbasierter Authentifizierung der Kommunikationspartner und AES (Advanced Encryption Standard) auf zwei voneinander getrennten Kanälen.

Aufbau und Funktionsweise der Fernservice-Verbindung zwischen Software und Gefahrenmeldeanlage über die Digitalplattform erfolgt wie nachfolgend beschrieben.

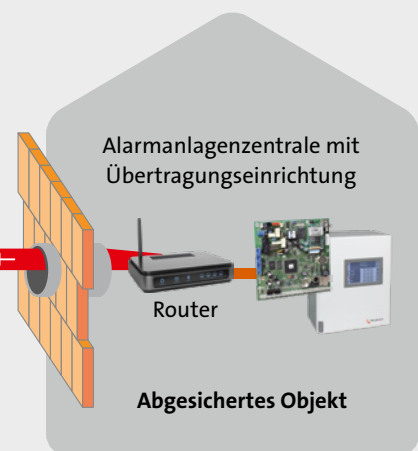
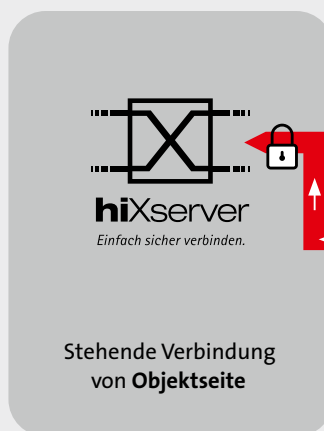
✓ **Kommunikation auf zwei getrennten Kanälen**

✓ **Zertifikatsbasierte Authentifizierung**

✓ **Verbindungsaufbau erst, wenn Authentizität, Vertraulichkeit und Integrität sichergestellt sind**

1

Der Authentifizierungskanal der Gefahrenmeldeanlage ist permanent mit dem hiXserver verbunden.



Objektseite

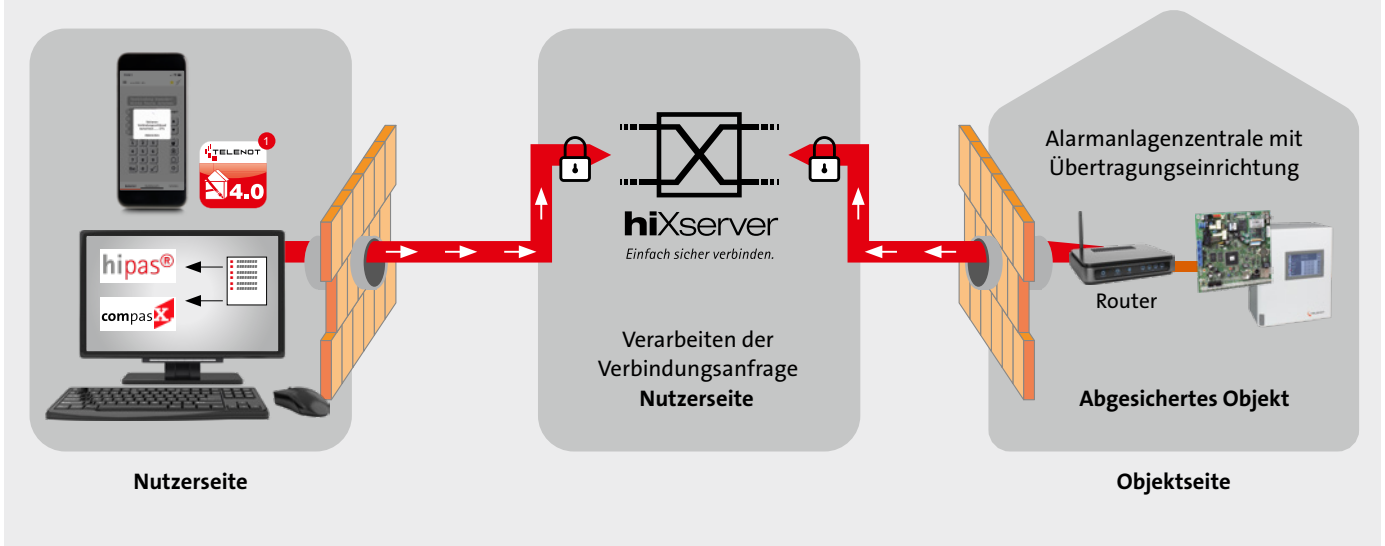


TELENOT-Management-Protokoll (TLS-Verschlüsselung)

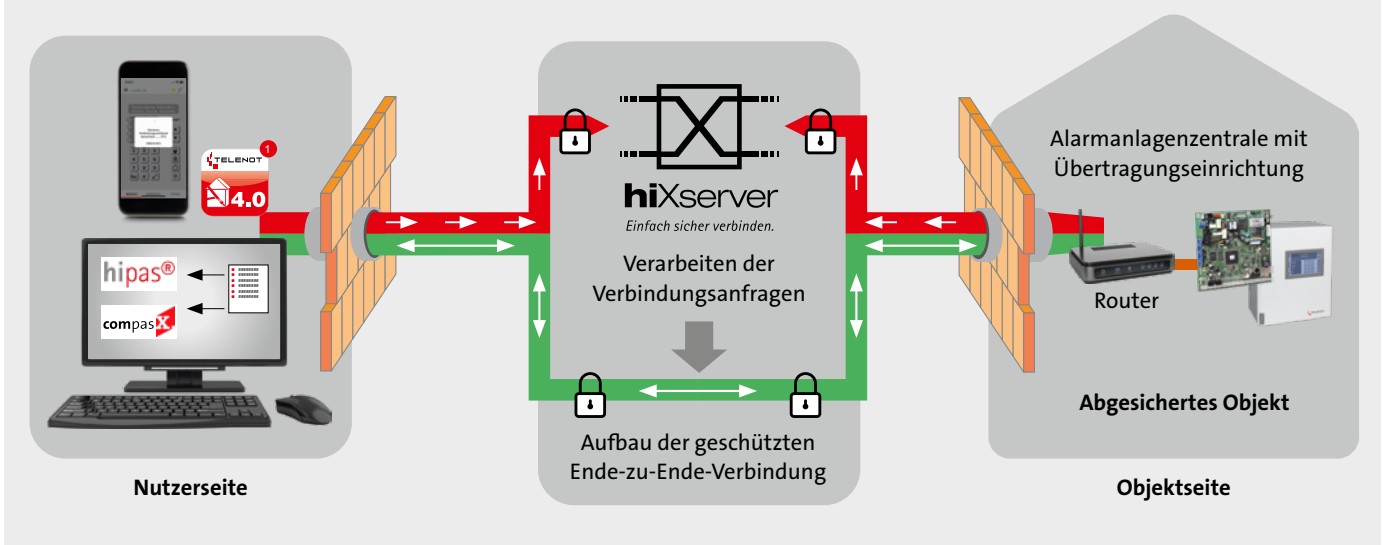


Verschlüsselte Ende-zu-Ende-Kommunikation im VdS-Protokoll (AES-Verschlüsselung)


- 2** Bei Bedarf verbindet sich die Nutzerseite über den Authentifizierungskanal mit dem hiXserver. Dies wird mittels des Verschlüsselungsprotokolls TLS realisiert, das die Aspekte „Vertraulichkeit“, „Authentizität“ und „Integrität“ sicherstellt. Die Überprüfung beider Seiten findet über die beidseitige zertifikatsbasierte Authentifizierung statt unter dem Motto „Wir kennen uns.“




- 3** Ist diese Überprüfung positiv, erfolgt die Kommunikation separat über einen zweiten AES-verschlüsselten Kanal. Für die sichere, geschützte Ende-zu-Ende-Verbindung wird jedes Mal ein neuer, einmaliger AES-Schlüssel erzeugt unter dem Motto „Wir kennen uns und kommunizieren sicher (verschlüsselt)“.



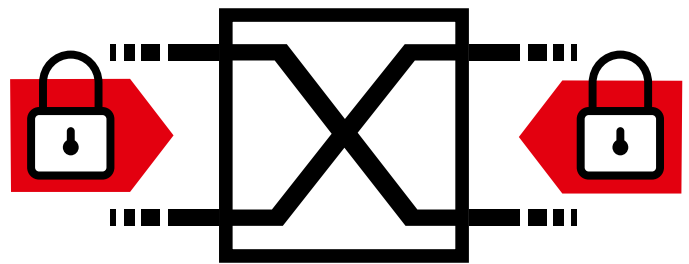
TLS und AES über zwei getrennte Kanäle.

Kanal 1: TLS stellt Vertraulichkeit, Authentizität und Integrität sicher  „Wir kennen uns!“

Kanal 2: AES stellt verschlüsselte Kommunikation her  „Wir kommunizieren sicher!“

Vorteil 3 ✓

Keine sicherheitsrelevanten Daten auf dem hiXserver



hiXserver

Bei üblichen IoT-Lösungen (Internet of Things) werden auch sicherheitsrelevante Systemzustände auf Servern abgelegt, dort über mobile Endgeräte gesteuert und mit der Anlage synchronisiert. Damit wird neben den unvermeidbaren Kommunikationswegen ein weiteres Angriffsziel geboten – der Server.

Durch Manipulation der dort abgelegten Daten kann die Anlage vor Ort direkt beeinflusst werden – im schlimmsten Fall lässt sich eine Einbruch- und Gefahrenmeldeanlage unscharf schalten. Selbst wenn es nur möglich ist, die auf dem Server abgelegten Anlagendaten zu lesen, gibt dies direkte Einblicke in das Nutzerprofil (z. B. wann das Haus verlassen wird), was wiederum zu Sicherheitsrisiken führt.

Nicht so bei der Digitalplattform hiXserver. Aus Sicherheitsgründen besitzt sie zu keiner Zeit sensible Informationen über den Zustand der Einbruch- und Gefahrenmeldeanlage wie z. B. den Scharfschaltzustand oder Einblick in den Ereignisspeicher.

Sämtliche Anlagen- und Objektinformationen werden vollständig anonym zwischen den Endgeräten ausgetauscht.

✓ Keine
Einblicke ins Nutzerprofil

✓ Keine
Datenmanipulation von
außen

✓ Anonymer
Informationsaustausch über
Endgeräte

Vorteil 4 ✓

Höchste Zugriffs-
sicherheit und
Datentransparenz

Welcher Ihrer Mitarbeiter hat Zugriff auf welche Einbruchmeldeanlage? Welcher Monteur hat wann eine Fernservice-Verbindung aufgebaut? Welche Zugriffsrechte weisen Sie welchem Mitarbeiter zu und – falls ein Mitarbeiter aus Ihrem Unternehmen ausscheidet – wie können Sie dessen Zugriffsrechte schnell sperren? Welche Objekte haben Sie in der Verwaltung und im Service?

Zugriffskontrolle, Verbindungslog und Verbindungsübersicht

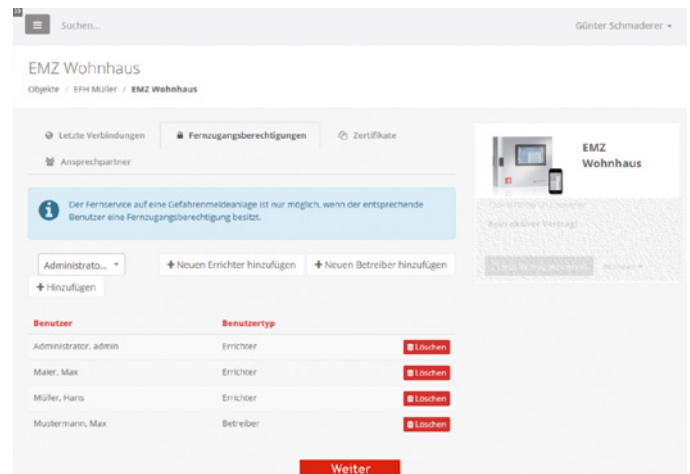
Die Digitalplattform hiXserver erleichtert Ihnen die Verwaltung der Zugriffsrechte Ihrer Mitarbeiter auf die Einbruch- und Gefahrenmeldeanlagen. Per Mausklick können Sie als Administrator über die Digitalplattform Ihre Techniker/Nutzer freischalten oder sperren. Bei einem Mitarbeiterwechsel können diese Rechte einfach und sicher angepasst werden.

Zudem werden die ausgeführten Fernservice-Verbindungen für die Dauer von acht Wochen protokolliert und können auf der Digitalplattform hiXserver entweder speziell für eine bestimmte Gefahrenmeldeanlage oder global für alle von Ihnen betreuten Gefahrenmeldeanlagen eingesehen werden.

✓ **Einfache Verwaltung
der Zugriffsrechte per
Mausklick**

✓ **Protokollierung und
Transparenz
der Verbindungen**

✓ **Datensicherheit
durch 2-Faktor-
Authentifizierung**



2-Faktor-Authentifizierung auf der Digitalplattform hiXserver

Um den hiXserver optimal vor Missbrauch zu schützen, wird er mit einer 2-Faktor-Authentifizierung abgesichert. Es kann dabei wahlweise

- jeder Login auf dem hiXserver oder
- einzelne sicherheitskritische Aktionen wie z. B. das Setzen von Berechtigungen

mit einem zweiten Faktor abgesichert werden. Die Zustellung des zweiten Faktors erfolgt in Form einer sechsstelligen Zahl per SMS auf die beim jeweiligen Nutzer hinterlegte Handynummer.

Höchste Datentransparenz für alle betreuten Anlagen

Alle aktuell mit dem hiXserver verbundenen Gefahrenmeldeanlagen werden in einer Übersicht dargestellt, um z. B. im Bedarfsfall von Support-Anfragen jederzeit Auskunft über den Zustand einer Gefahrenmeldeanlage geben zu können. Damit bietet Ihnen die Digitalplattform höchste Datentransparenz über verrichtete Arbeiten und liefert Ihnen zugleich einen Überblick über den aktuellen Stand aller der von Ihnen betreuten Anlagen.

hiXmobile

Zuverlässig und
sicher mobil
kommunizieren



Der Dienst hiXmobile der Digitalplattform hiXserver garantiert die schnelle Einrichtung der Alarmanlagen-App BuildSec 4.0 und die absolut sichere Kommunikation über zwei verschlüsselte getrennte Wege zwischen mobilem Endgerät und Einbruch- und Gefahrenmelderzentrale.

Mittels der Digitalplattform hiXserver entfallen aufwendige Programmierarbeiten am vor Ort installierten Router ebenso wie die Beachtung der vorhandenen Netzinfrastruktur. **Sie sparen bei jeder Installation wertvolle Zeit und Geld.**

Die Alarmanlagen-App ist über die Digitalplattform hiXserver mit der Einbruch- und Gefahrenmeldeanlage über eine sichere Ende-zu-Ende-Verschlüsselung verbunden. Sämtliche Daten der Anlage sowie alle Steuerungsbefehle, die über die BuildSec 4.0 ausgeführt werden, sind über alle Stationen hinweg bei jeder Kommunikation mit einem neuen einmaligen Schlüssel sicher Ende-zu-Ende verschlüsselt. Auch diese Kommunikation erfolgt auf zwei voneinander getrennten Kanälen mittels TLS- und AES-Verschlüsselung (vgl. S. 4/5).

Das bedeutet: Sie richten einmalig für Ihre Kunden die BuildSec 4.0 ein. Spätestens an dieser Stelle wird Ihrem Kunden deutlich, mit welchen Sicherheitsstandards die App und damit auch die gesamte Digitalplattform hiXserver ausgestattet ist. Auch ein Wechsel des mobilen Endgerätes ist in einfachster Art und Weise möglich.

Unter dem Motto: „Meine Firma oder mein Eigenheim gehört mir!“ hat nur der jeweilige Nutzer Zugriff. Sprachassistenten, IP-Kameras und andere vergleichbare Services bleiben außen vor.

Die Alarmanlagen-App BuildSec 4.0 selbst ist eine Anwendersoftware für Smartphones, Tablets und Windows-Computer zur Bedienung und Darstellung von Betriebszuständen der TELENOT-Gefahrenmelderzentralen complex 200H/400H, hiplex 8400H und compact easy. Welches Objekt auch immer gegen

- **Einbruch,**
- **Brandgefahren,**
- **technische Störungen oder den Zutritt unberechtigter Personen**

geschützt werden soll: Mit der BuildSec 4.0 weiß Ihr Kunde immer, ob wirklich alles in Ordnung ist.

Die BuildSec 4.0 bietet zusätzlich umfangreiche Schalt- und Steuerfunktionen für Smart-Home-Anwendungen, wie z. B. Garagentor auf/zu, Außenlicht an/aus oder Jalousien auf/ab.



Dank der Digitalplattform hiXserver findet die Kommunikation über mobile Endgeräte zur Einbruch- und Gefahrenmeldeanlage jederzeit sicher und zuverlässig statt.

Ihre Kunden können sich die Alarmanlagen-App BuildSec 4.0 für alle mobilen Endgeräte für Windows, Android oder iOS in den entsprechenden App-Stores herunterladen.

Die App-Funktionalität und damit ihre Nutzung ist von der Freischaltung der Gefahrenmelderzentrale bzw. der Übertragungseinrichtung abhängig. Die Freischaltung der BuildSec 4.0 wiederum kann bei der TELENOT ELECTRONIC GMBH von Ihnen als Fachbetrieb erworben werden und ist dann schnell mit allen vorgenannten Vorteilen beim Kunden einrichtbar.

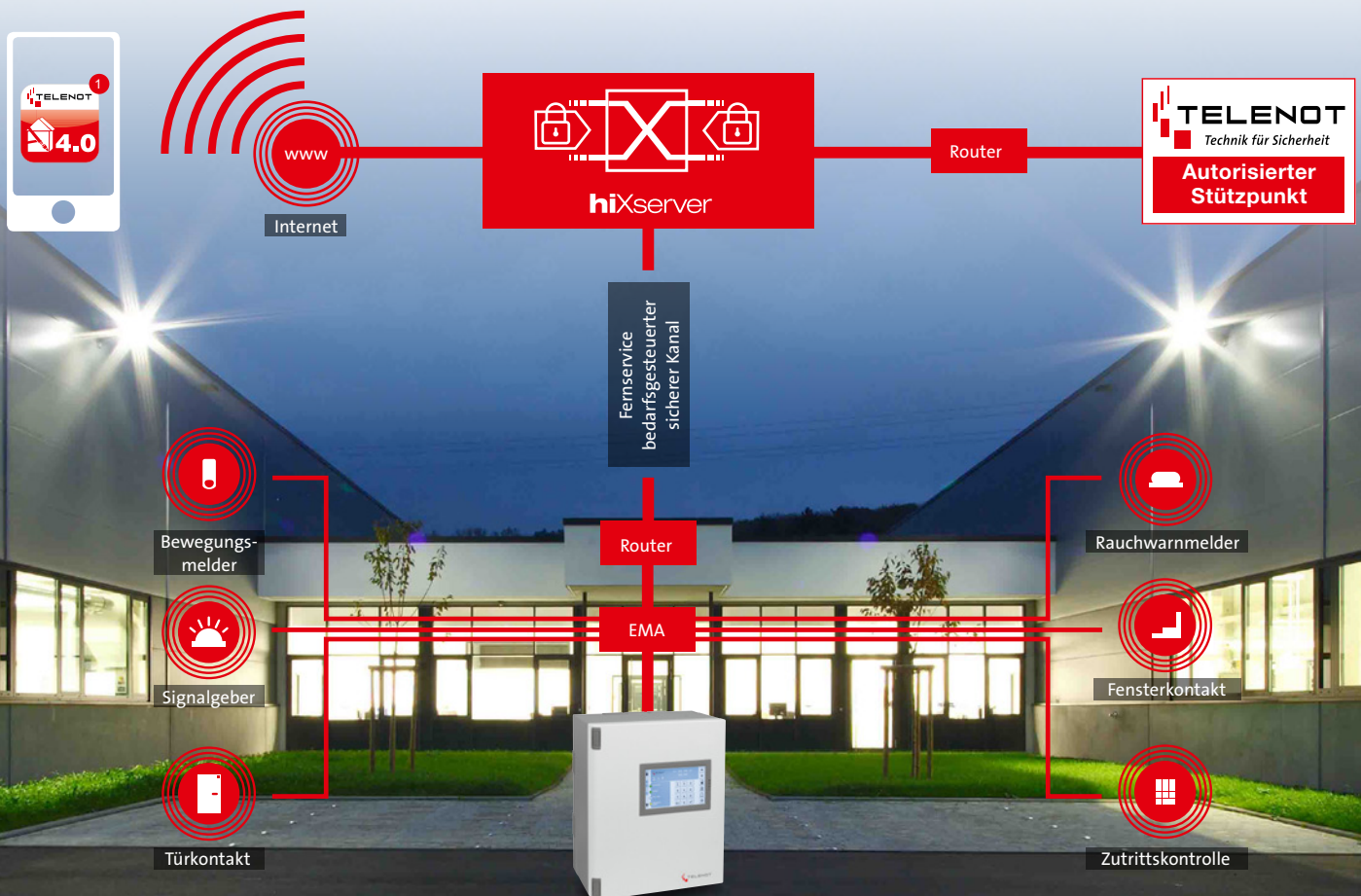
hiXremote

Ihr Werkzeug für
sicheren und
komfortablen
Fernservice

Mit dem Werkzeug hiXremote bietet Ihnen die Digitalplattform hiXserver eine sichere Fernservice-Verbindung für das komplette Einbruch- und Gefahrenmeldesystem von TELENOT.

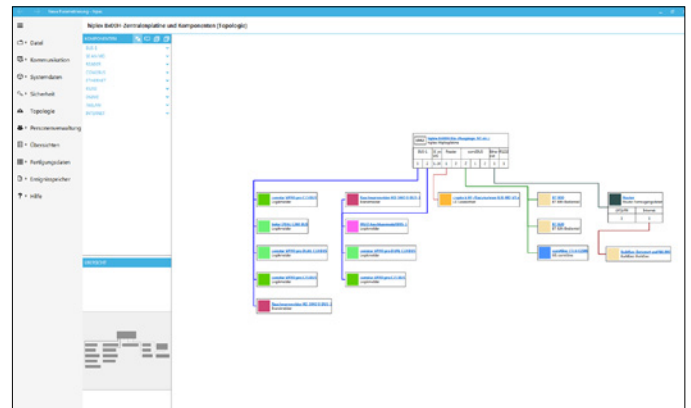
Dies ermöglicht es Ihnen, unter Beachtung höchster Sicherheitsstandards, schnell und einfach Störungen zu beseitigen und neue Anforderungen seitens des Kunden zu erfüllen. Nachdem der über zwei getrennte Wege verschlüsselte Verbindungsaufbau steht, können nachfolgende Fernservicefunktionen mittels der Parametriersoftware compasX bzw. hipas realisiert werden.

- Fernparametrierung einer Übertragungseinrichtung comXline
- Firmware-Update einer Übertragungseinrichtung comXline
- Fernparametrierung einer Einbruch- und Gefahrenmelderzentrale complex 200/400H, hiplax 8400H und compact easy
- Fehlersuche und Störungsbeseitigung
- Transponder einlernen
- Service
- Statusabfrage



hiXuser

Sichere Bedien-
funktionen direkt
für den Betreiber



Die Digitalplattform hiXserver bietet mit dem Werkzeug hiXuser eine sichere Fernservice-Verbindung, um dem Betreiber, Wachdienst oder Kunden zahlreiche Funktionen wie

- Personen- und Transponderverwaltung,
- Anzeige des Ereignisspeichers oder Fernbedienung

mittels der Software compasX-User bzw. hipas-User zu ermöglichen.

Um die Services hiXmobile, hiXremote und hiXuser nutzen zu können, ist der Kauf von hiX-Lizenzpaketen notwendig. Diese können Sie über den TELENOT Smart Services-Shop unter www.telenotsmartservices.com erwerben.

Die hiX-Lizenzpakete im Überblick:

Wir bieten Ihnen die drei Tools **hiXremote**, **hiXmobile** und **hiXuser** für die vollumfängliche und komfortable Fernservice-Verbindung und Verwaltung einer TELENOT Einbruch- und Gefahrenmeldeanlage gebündelt in verschiedenen Lizenzpaketen an, die Sie individuell, abgestimmt auf die Anzahl Ihrer Objekte, bestellen können. Fragen Sie uns gerne:

Lizenz-Paket	Lizenz-Paket	Lizenz-Paket	Lizenz-Paket
hiX1	hiX10	hiX50	hiX100/100mobile
hiXmobile: 1 Lizenz hiXremote: 1 Lizenz hiXuser: 1 Lizenz	hiXmobile: 10 Lizenzen hiXremote: 10 Lizenzen hiXuser: 10 Lizenzen	hiXmobile: 50 Lizenzen hiXremote: 50 Lizenzen hiXuser: 50 Lizenzen	hiXmobile: 100 Lizenzen hiXremote: 100 Lizenzen hiXuser: 100 Lizenzen

Nutzen Sie die Digitalplattform hiXserver der TELENOT Smart Services GmbH für die absolut geschützte, kostensparende und einfache Fernservice-Verbindung zu all Ihren Kundenobjekten.

**Starten Sie gemeinsam mit TELENOT Smart Services
in das digitale Sicherheitszeitalter.
Weitere Informationen unter www.telenotsmartservices.com**

In nur drei Schritten zur intelligenten Gebäudesicherheit und -steuerung



Einmalig registrieren unter
www.telenotsmartservices.com



Ein für Ihren Kundenstamm
passendes Lizenzpaket bequem
im Online-Shop kaufen.



Freischaltung und Zuweisung
der einzelnen Lizenzen pro Gefahren-
meldeanlage auf dem hiXserver.

Der Vertrieb der Produkte hiXserver (hiXmobile, hiXremote und hiXuser) erfolgt im Namen und auf Rechnung der
TELENOT Smart Services GmbH, Wiesentalstraße 60, 73434 Aalen.

Sie haben Fragen oder wünschen weitere Informationen?
Kontaktieren Sie uns.

Stammsitz

Kontakt Deutschland:

TELENOT ELECTRONIC
GMBH

Wiesentalstraße 60
73434 Aalen
GERMANY

Telefon +49 7361 946-400

info@telenot.de

Kontakt International:

TELENOT ELECTRONIC
GMBH

Wiesentalstraße 60
73434 Aalen
GERMANY

Telefon +49 7361 946-4990

info@telenot.com

Kontakt Österreich:

TELENOT ELECTRONIC
Vertriebs-Ges.m.b.H.

Josef-Haas-Straße 3
4655 Vorchdorf
AUSTRIA

Telefon +43 7614 8258-0
Telefax +43 7614 8258-11

info@telenot.at

Kontakt Schweiz:

TELENOT ELECTRONIC AG

Bahnhofstrasse 41
5600 Lenzburg
SWITZERLAND

Telefon +41 52 544 17 22

info@telenot.ch

Kontakt Luxemburg:

marco zenner s.à r.l.
Offizieller Distributor
TELENOT

2b, Zone Industrielle Zare Est
4385 Ehlerange
LUXEMBOURG

Telefon +352 44 15 44-1

telenot@zenner.lu
www.zenner.lu