Netzwerkanforderungen Safe Fire House Brandwarnsystem

Gültig für die PoE-Zentrale, PoE-Repeater und das PoE-Display

Vor Inbetriebnahme der Komponenten die Betriebsanleitung lesen

Diese Anleitung ist Teil des Produktes. Die Nichtbeachtung der Vorgaben dieser Anleitung kann eine Beeinträchtigung der Funktion oder die Beschädigung des Gerätes, anderer Sachwerte sowie Personenschäden zur Folge haben.

- Vor jeder Inbetriebnahme sind die entsprechenden Kapitel dieser Anleitung zu lesen und die enthaltenen Sicherheitshinweise zu beachten.
- Die Anleitung ist an jeden nachfolgenden Benutzer zu übergeben.
- Fragen und Hinweise bitte als Serviceticket stellen. Einen Link dazu finden Sie am Ende dieser Anleitung.

Urheberrecht

Dexa Solutions GmbH
Möhnestraße 2
59519 Möhnesee

1. Einleitung

1.1 Rollenverteilung und Haftung

Die Dexa Solutions GmbH nimmt im Projekt die Rolle des Systemintegrators ein. Wir konzipieren den Lösungsansatz und setzen ihn nach Ihren Vorgaben um. Dabei kommen verschiedene technische Komponenten von namhaften Hard- und Softwareanbietern sowie eigens entwickelte Hard- und Software zum Einsatz. Wir sind nicht Hersteller aller zum Einsatz kommenden Komponenten und übernehmen daher nicht die Produkthaftung der Fremdhersteller, außer für von uns durchgeführte Modifikationen. Diese obliegt weiterhin, genau wie die Gewährleistung und Garantie, dem Hersteller der jeweiligen Komponente. Auf Seiten der Software haften wir in vollem Umfang für die eigens entwickelten Softwareteile, naturgemäß jedoch nicht für die Softwareteile von Drittanbietern.

Unsere Anlage orientiert sich an ausgewählten technischen Anforderungen der VDE 0833-1 (allgemeiner Teil). Es werden teilweise VdS- beziehungsweise EN 54-zertifizierte Rauchmelder eingesetzt, teilweise nicht zertifizierte Rauchsensoren. Die Anlage erfüllt daher ausdrücklich nicht die Anforderungen an bauordnungsrechtlich geforderte Brandmeldeanlagen nach VDE 0833-2/DIN 14675, wie sie insbesondere in Sonderbauten (beispielsweise Schulen, Krankenhäuser, Beherbergungsbetriebe) verlangt werden.

In Fahrzeugen sowie in Gebäuden oder Räumen, für die keine bauordnungsrechtliche Pflicht zur Installation einer Brandmeldeanlage nach VDE 0833-2/DIN 14675 besteht, kann die Anlage eingesetzt werden. Sofern die Integration in ein Brandschutzkonzept erfolgt, kann die Anlage als ergänzende technische Maßnahme zur Verbesserung der Früherkennung und Alarmierung berücksichtigt werden, ohne eine bauordnungsrechtlich geforderte Brandmeldeanlage zu ersetzen.

Als Kunde stellen Sie Teile Ihrer IT-Infrastruktur, zum Beispiel einen Netzwerkanschluss mit Internetzugang, WLAN oder Eingangsschnittstellen zu Alarmsystemen beziehungsweise Gebäudetechnik oder Brandmeldeanlage zur Verfügung. Diese muss am Tag der Inbetriebnahme gemäß der abgesprochenen Anforderungen vorbereitet sein. Für das nachhaltige Funktionieren dieser Infrastruktur tragen Sie als Kunde die Verantwortung. Für ein langfristiges Funktionieren können wir, etwa wenn Sie künftig Änderungen vornehmen, keine Haftung übernehmen.

Manche Alarmsysteme, wie zum Beispiel Alamos, werden lokal durch den Kunden gehostet. Hier trägt dieser die Verantwortung für das Funktionieren der bereitgestellten Schnittstelle. Andere Systeme, wie zum Beispiel DIVERA 24/7, sind Cloud-basiert. Hier wird die Schnittstelle direkt vom Hersteller betrieben. Wir können für den Fall, dass dieser Änderungen vornimmt und dadurch Funktionseinschränkungen auftreten, keine Haftung übernehmen. Unsere Systeme sind aber darauf ausgelegt, in diesem unwahrscheinlichen Fall nachträglich mit nur geringem Aufwand, beispielsweise per Fernwartung, angepasst zu werden. Die Zusage zur Anbindung von individuellen und wunschgemäßen Schnittstellen, die durch uns noch nicht entwickelt sind, erfolgt unverbindlich und im Rahmen der Verhältnismäßigkeit. Dies gilt ebenso für den Einsatz von besonderen Hardwarekomponenten.

Damit die Zusammenarbeit gelingt und der Verbau der Innenraumüberwachungssysteme zu einem nachweislichen Erfolg wird, endet jede Inbetriebnahme mit einem umfangreichen Funktionstest, der dokumentiert wird. Darüber hinaus kann jeder Melder beziehungsweise Sensor zu jeder Zeit eigenständig getestet und somit die Funktionssicherheit überprüft werden. Den Einsatzkräften wird dies ausdrücklich als Probealarm angezeigt, sodass es nicht zu Missverständnissen kommt.

Sofern der Anschluss an eine vorhandene Brandmeldeanlage gewünscht ist, wird dieser in der Regel durch das Schalten eines potenzialfreien Eingangskontaktes realisiert. Dieser muss Ihrerseits, beziehungsweise durch den Servicetechniker der Wartungsfirma der Brandmeldeanlage, bereitgestellt werden. In der Nähe des Kontaktes muss in fünf Metern Abstand eine 230-V-Steckdose vorhanden sein. Für den Anschluss unseres Schaltaktors an Ihre Brandmeldeanlage gelten die gültigen Aufschaltbedingungen Ihrer zuständigen Brandschutzbehörde. Diese geben in der Regel vor, dass Sie nur nach DIN 14675 beziehungsweise EN 54 zertifizierte Komponenten, also Teile anderer Brandmeldeanlagen, anschließen dürfen. Naturgemäß ist dies bei unserem System nicht der Fall, da es für die Überwachung von Innenräumen der Fahrzeuge kein technisches Regelwerk gibt. In den allermeisten Fällen lässt sich ein Anschluss unseres Systems an Ihre BMA aber trotzdem realisieren, da fast alle behördlichen Aufschaltbedingungen eine Öffnungsklausel haben, die besagt, dass die zuständige Behörde im Rahmen ihrer Genehmigung von den vorangestellten Anforderungen abweichen kann. Sie müssen daher, sofern Ihre Brandmeldeanlage bei einer Feuerwehr-Leitstelle aufgeschaltet ist, vor der Inbetriebnahme eine entsprechende Genehmigung einholen. Die Verantwortung hierfür liegt beim Auftraggeber.

1.2 Hinweise zum Datenschutz

Bitte beachten Sie die folgenden Informationen bezüglich des Datenschutzes in Verbindung mit der Fernwartungsfunktion sowie unseres Online-Service-Logbuchs, die in unserem System enthalten ist:

1. Zweck der Fernwartung: Die Fernwartungsfunktion ermöglicht es unserem technischen Support-Team, auf Ihr System zuzugreifen, um Wartungs- und Supportdienste zu erbringen, Updates durchzuführen und

Probleme zu diagnostizieren und zu beheben. Dies geschieht auf freiwilliger Basis. Die Fernwartungsfunktion ist standardmäßig immer aktiv. Wünschen Sie dies nicht, müssen Sie uns darauf schriftlich hinweisen.

2. Datenschutz und Sicherheit: Wir nehmen den Schutz Ihrer Daten ernst und ergreifen angemessene technische und organisatorische Maßnahmen nach Art. 32 DSGVO, um sicherzustellen, dass Ihre Daten während der Fernwartung sicher und geschützt bleiben. Jeglicher Zugriff auf Ihr System erfolgt unter Einhaltung geltender Datenschutzgesetze und unserer IT-Sicherheitsregeln. Der Fernwartungszugriff erfolgt ausschließlich über verschlüsselte, mehrfach authentifizierte Verbindungen.

3. Datenerhebung und -verarbeitung: Während der Fernwartung sowie im Rahmen des zentralen Service-Logbuchs werden technische Informationen, Fehlerprotokolle sowie Standort- und Anlagendaten (Bezeichnung des Standortes, Anschrift der Anlage, technische Kennwerte) verarbeitet. Namen, Privatanschriften oder Telefonnummern natürlicher Personen werden hierbei nicht erhoben. Für den Versand von Serviceberichten und Test-Meldungen sowie gegebenenfalls Alarm-Meldungen werden die E-Mail-Adressen der jeweiligen Empfänger verarbeitet; hierbei handelt es sich um personenbezogene Daten, deren Verarbeitung nach den Vorgaben der Datenschutz-Grundverordnung (DSGVO) erfolgt. Der E-Mail-Versand erfolgt über einen Auftragsverarbeiter mit Datenverarbeitung in der Europäischen Union auf Grundlage eines Auftragsverarbeitungsvertrags nach Art. 28 DSGVO. Die vorgenannten Daten werden ausschließlich für Support-, Überwachungs- und Produktverbesserungszwecke verwendet und nicht an sonstige Dritte weitergegeben, es sei denn, dies ist gesetzlich vorgeschrieben oder wird von Ihnen autorisiert.

4. Zentrales Service-Logbuch: Zusätzlich zu den oben genannten Informationen möchten wir darauf hinweisen, dass Anlagendaten in ein zentrales Service-Logbuch geschrieben werden. Diese Daten dienen der Überwachung und Optimierung der Systemleistung und -zuverlässigkeit und werden gemäß den geltenden Datenschutzbestimmungen verarbeitet.

5. Weitere Informationen und Ihre Rechte: Die vorstehend beschriebene Verarbeitung im Rahmen von Fernwartung und Service-Logbuch erfolgt in Übereinstimmung mit der Datenschutz-Grundverordnung (DSGVO). Die für Ihr System maßgeblichen Rechtsgrundlagen, Speicherdauern und eingesetzten Auftragsverarbeiter sowie Ihre Betroffenenrechte (unter anderem Auskunft, Berichtigung, Löschung, Einschränkung und Widerspruch) ergeben sich aus den mit Ihnen getroffenen vertraglichen Datenschutzvereinbarungen, insbesondere dem Auftragsverarbeitungsvertrag nach Art. 28 DSGVO. Bei Fragen zum Datenschutz wenden Sie sich bitte an unseren Ansprechpartner für den Datenschutz über die am Ende dieser Anleitung genannten Kontaktdaten.

---

2. Hinweis zur Verbindung

Die Zentrale und der Repeater müssen sich im gleichen Netzwerksegment befinden und über einen Internetzugang verfügen.

Die Rauchmelder und Sensoren kommunizieren per Funk (868 MHz) mit Zentrale und Repeater und stellen keine Anforderung an Ihr Netzwerk.

2.1 Netzwerkanforderungen für Einzelstandort

- **Anschluss:** RJ45 mit PoE
- **PoE-Protokoll:** 802.3af (PoE) / 802.3at (PoE+)
- **Übertragungsrate:** 10/100/1000 Mbps

2.2 Zusätzliche Netzwerkanforderungen für Multistandort

Wenn das System standortübergreifend eingesetzt werden soll, bedarf es einer Vernetzung der Standorte im selben Netzwerk. Dies kann über VPN-Systeme wie WireGuard, ZeroTier, IPSec o. ä. erfolgen. Alternativ auch über ein VXLAN / VLAN. Hierfür sind folgende Anforderungen zwingend erforderlich:

- **Netzwerktyp:** Die Kommunikation zwischen den Standorten erfolgt über Multicast. Die genutzte Multicast-Gruppe 224.0.0.120 liegt im link-lokalen Bereich (224.0.0.0/24) und wird nicht geroutet. Eine standortübergreifende Kopplung muss daher als **Layer-2-Verbindung (Bridge über das VPN)** ausgeführt werden; ein reines Layer-3-Routing der Multicast-Pakete ist für diese Gruppe nicht möglich.
- **Kommunikationsart:** Multicast
- **Architektur:** Am besten gleicher IP-Adressbereich, gleiches Subnetz.

Die Multicast-Gruppe, über die kommuniziert wird, ist 224.0.0.120. Es ist sinnvoll, den gesamten Multicast-(udp)-Verkehr zwischen den Repeatern und der Zentrale zu erlauben. Zusätzlich werden hierfür die Ports 9292 (tcp), 43439 (tcp) und 43438 (udp) genutzt. Die gesamte Kommunikation läuft im VPN-Netzwerk ab. Freigaben in das Internet sind für die Verbindung zwischen Zentrale und Repeater nicht notwendig, außer Sie nutzen ZeroTier als Relay-Dienst.

Der Multicast-Verkehr kann über folgenden Befehl (Linux) eingesehen werden:

```
tcpdump -i eth0 -n 'udp and dst 224.0.0.120'
```

Bitte eth0 gegebenenfalls durch das verwendete Interface ersetzen.

Achten Sie bei der Gestaltung der Netzwerkarchitektur in Ihren VPN-Routern oder Firewalls auf sauberes Bridging der Interfaces, sodass keine Loops entstehen. Multicast-Pakete gehen „wild" über alle Interfaces, je nach Routing und Bridging. Lassen sich Loops nicht vermeiden, aktivieren Sie Beschränkungen wie beispielsweise das Spanning Tree Protocol (STP) und Multicast-Begrenzungen (beispielsweise bei ZeroTier).

Falls Sie Fragen zur Umsetzung haben, sprechen Sie uns an. Gerne bieten wir Ihnen die Vernetzung Ihrer Standorte als zusätzliche Leistung in einem Vorprojekt an.

2.3 Einsatz hinter einer Firewall

Beim Betrieb der PoE-Zentrale hinter einer Firewall ist zu beachten, dass die Endpunkte gemäß folgender Tabelle sowie die genannten Ports erreichbar sind. Es wird hier anhand von DIVERA 24/7 lediglich ein Beispiel für eine Alarmschnittstelle gegeben. Für die Erreichbarkeit weiterer Alarmdienste und Schnittstellen sind die Dokumentationen der jeweiligen Anbieter zu konsultieren. Bitte sprechen Sie uns an, falls Sie Unterstützung benötigen.

Bitte stellen Sie sicher, dass alle genannten Ziele, Ports und Protokolle in Ihrer Firewall freigegeben sind, um eine reibungslose Funktionalität der PoE-Zentrale und angeschlossener Geräte zu gewährleisten.

Unser System benötigt keine eingehenden Portfreigaben oder Portweiterleitungen aus dem Internet! Alle Verbindungen ins Internet werden ausschließlich von der Anlage aus aufgebaut.

Die Verbindungen sind nachfolgend in drei Blöcke gegliedert: Verbindungen innerhalb Ihres Netzes, Verbindungen zu Servern der dexa group und Verbindungen zu weiteren Zielen.

Block 1 — Lokales Netz

Diese Verbindungen verlassen Ihr Netzwerk nicht. Eine Freigabe ist nur erforderlich, wenn Sie innerhalb Ihres Netzes filtern, beispielsweise zwischen VLANs. Die Kommunikation erfolgt in beide Richtungen zur Zentrale.

Verbindung	Protokoll/Port	Ziel	Zweck
PoE-Zentrale ? PoE-Repeater	Multicast (udp/43438), tcp/9292, tcp/43439	local network	Kommunikation zwischen Zentrale und Repeatern
PoE-Display ? PoE-Zentrale	HTTP (tcp/80)	local network	Lokale Kommunikation mit dem Frontend
PoE-Zentrale ? DNS-Server	udp/53, tcp/53	interner DNS-Server (local network)	DNS-Namensauflösung

Block 2 — dexa-Server (feste IP-Adressen, zertifiziertes Rechenzentrum in Deutschland)

Sämtliche nachfolgenden Ziele sind Server der dexa group mit festen IP-Adressen. Die Freigabe von Namensräumen mit Platzhalter (Wildcard) ist nicht erforderlich. Alle Verbindungen werden ausschließlich **ausgehend** von der Anlage aufgebaut. Angaben zum Rechenzentrum und seinen Zertifizierungen finden Sie in Abschnitt 2.4.

Verbindung	Protokoll/Port	Ziel	Zweck
PoE-Zentrale ? dexa-Vermittler	HTTPS (tcp/443)	**auth.dexa.gmbh** (188.64.56.101, IPv6 2a00:6140:100:1d::1)	Zwei Aufgaben über dieselbe Adresse: Koordination der Fernwartungsverbindung und Multifaktor-Anmeldung an der Bedienoberfläche
PoE-Zentrale ? Fernwartungs-Relay	HTTPS (tcp/443), STUN (udp/3478), Relay (udp/40000)	**derp.dexa.gmbh** (185.64.114.155, IPv6 2a00:6140:127:41::1)	Verschlüsselter Relay-Weg der Fernwartung, wenn keine direkte Verbindung möglich ist
PoE-Zentrale ? Service-Plattform	HTTPS (tcp/443)	**hooks.dexa.gmbh** (188.64.62.196, IPv6 2a00:6140:112:16::1)	Überwachung der Komponenten und Schnittstellen (Statusmeldungen)
PoE-Zentrale ? Stammdaten-Schnittstelle	HTTPS (tcp/443)	**api.dexa.gmbh** (188.64.62.196, IPv6 2a00:6140:112:16::1)	Abruf und Pflege der Standort-, Fahrzeug- und Komponentendaten
PoE-Zentrale ? Mailserver	SMTP (tcp/465, implizites TLS)	**smtp.dexa.gmbh** (188.64.62.196, IPv6 2a00:6140:112:16::1)	Versand von Statusmails
PoE-Zentrale ? Zeitserver	NTP (udp/123)	**ntp.dexa.gmbh** (188.64.62.196, IPv6 2a00:6140:112:16::1)	Synchronisation von Datum und Uhrzeit

Zusammenfassung der freizugebenden Adressen (Block 2)

Adresse	IPv6	benötigte Ports (ausgehend)
188.64.56.101	2a00:6140:100:1d::1	tcp/443
185.64.114.155	2a00:6140:127:41::1	tcp/443, udp/3478, udp/40000
188.64.62.196	2a00:6140:112:16::1	tcp/443, tcp/465, udp/123

Hinweis zu Sicherungen und Service-Logbuch: Die Übertragung der Anlagensicherungen und der Service-Logbuch-Einträge erfolgt ausschließlich über die verschlüsselte Fernwartungsverbindung. Dafür ist **keine** gesonderte Freigabe erforderlich; insbesondere werden weder FTP noch SFTP zu unseren Servern benötigt.

> **Hinweis bei sporadischen Verbindungsabbrüchen (feste IP statt Hostname): Filtert Ihre Firewall anhand von Hostnamen (FQDN-Objekten), kann es trotz eingetragener Freigabe zu wiederkehrenden, kurzen Verbindungsabbrüchen kommen. Grund ist, dass solche Regeln eine einmal aufgelöste IP zwischenspeichern und nach einer Adressänderung blockieren, bis sie neu auflösen. Da die dexa-Ziele feste IP-Adressen haben, empfehlen wir, diese direkt als IP-Regel einzutragen statt als Hostname. Bestehen die Abbrüche fort, kann es zusätzlich helfen, `controlplane.tailscale.com` als Hostname-Objekt freizugeben — dies ist optional.**

Block 3 — Weitere Ziele

Diese Ziele werden **nicht** von der dexa group betrieben. Auch hier werden alle Verbindungen ausschließlich ausgehend von der Anlage aufgebaut. **Bei aktuellem Softwarestand ist keines dieser Ziele zwingend** — siehe die Hinweise unten.

Verbindung	Protokoll/Port	Ziel	Zweck
PoE-Zentrale ? direkte Peer-Verbindung (verschlüsselter Transporttunnel)	WireGuard (udp/41641)	direkte Verbindung zum Wartungsplatz (wechselnde Adresse, ausgehend)	Fernwartung über den direkten, verschlüsselten Tunnel (optional; ohne diese Freigabe läuft die Fernwartung über den Relay)
PoE-Zentrale ? Internet-Erreichbarkeit (nur älterer Softwarestand)	ICMP (Echo/Ping)	`8.8.8.8` (Google LLC)	Konnektivitätsprüfung (WatchDog)
PoE-Zentrale ? Alarmierungsschnittstellen (Beispiel)	HTTPS (tcp/443)	`app.divera247.com` (Beispiel, DIVERA 24/7 GmbH)	Alarmierung
	HTTP/HTTPS, lokal (Port gemäß Ihrer Installation)	localhost beziehungsweise local network	Beispiel Alamos (lokal beim Kunden gehostet)

Hinweis zur IT-Sicherheit: Alle externen Schnittstellen werden ausschließlich verschlüsselt und mit entsprechend sicherer Authentifizierung (Token, MFA oder Zertifikat) angesprochen.

Hinweis zur Service-Plattform: `hooks.dexa.gmbh` ist der von der dexa group betriebene Meldeweg für Statusmeldungen mit festen Adressen (188.64.62.196, IPv6 2a00:6140:112:16::1). Er nimmt ausschließlich die Statusmeldungen der Anlage entgegen und leitet sie an unser zentrales Service-Logbuch weiter.

Hinweis zur Stammdaten-Schnittstelle: `api.dexa.gmbh` ist der von der dexa group betriebene Zugang zu den Stammdaten Ihrer Anlage (Standort, Fahrzeuge, Komponenten, Service-Logbuch) mit festen Adressen (188.64.62.196, IPv6 2a00:6140:112:16::1). Die Zentrale weist sich dabei mit einem eigenen, anlagenbezogenen Zugangsmerkmal aus; Zugangsdaten zu Diensten Dritter werden auf der Anlage nicht

gespeichert. Der Zugang ist auf die Daten Ihrer Anlage beschraenkt und kann einzeln gesperrt werden.

Hinweis zum Service-Connector: Die Fernwartung benötigt eine Koordinationsstelle, die den Verbindungsaufbau zwischen Anlage und Wartungsplatz vermittelt. Ab Softwarestand SFH 2.4 spricht die Anlage hierfür ausschließlich den dexa-Vermittler unter der festen Adresse 188.64.56.101 (tcp/443, ausgehend) an. Die Freigabe eines Namensraums mit Platzhalter ist nicht erforderlich. Sofern Ihre Firewall Verbindungen nicht anhand der Zieladresse, sondern anhand des im Verbindungsaufbau übermittelten Servernamens filtert, ist zusätzlich der Name **controlplane.tailscale.com** zuzulassen; die Verbindung wird dabei dennoch ausschließlich zur oben genannten dexa-Adresse aufgebaut. Bei Anlagen mit älterem Softwarestand tritt an die Stelle des Vermittlers der Adressbereich **192.200.0.0/24** (tcp/443, ausgehend).

Hinweis zur Internet-Erreichbarkeit: Bei aktuellem Softwarestand prüft die Zentrale ihre Internetverbindung gegen den dexa-Vermittler (188.64.56.101, tcp/443) — dafür ist keine zusätzliche Freigabe erforderlich. Bei älterem Softwarestand erfolgt die Prüfung per ICMP-Echo (Ping) an **8.8.8.8**; sollte ausgehender ICMP-Verkehr in Ihrer Firewall nicht zulässig sein, stellen wir die Prüfung per Fernwartung auf den dexa-Vermittler um. Bitte sprechen Sie uns in diesem Fall an.

Hinweis zum Zeitserver: **ntp.dexa.gmbh** ist der von der dexa group betriebene Zeitdienst mit festen Adressen (188.64.62.196, IPv6 2a00:6140:112:16::1). Für die Synchronisation genügt ausgehender NTP-Verkehr (udp/123) zu diesem Ziel; eingehende Freigaben sind nicht erforderlich. In Netzen ohne externe DNS-Auflösung kann die IP-Adresse direkt hinterlegt werden.

Hinweis zum Fernwartungs-Relay: Kommt zwischen der Zentrale und dem Wartungsplatz keine direkte Verbindung zustande, läuft die Fernwartung verschlüsselt über den von der dexa group selbst betriebenen Relay **derp.dexa.gmbh**. Dieser steht in einem Rechenzentrum in Deutschland. Der Relay kann die übertragenen Inhalte technisch nicht mitlesen — die Verschlüsselung besteht Ende-zu-Ende zwischen den beteiligten Geräten. Der Relay stellt auf derselben Adresse zwei Wege bereit: den Relay-Dienst über tcp/443 und udp/3478 sowie einen dedizierten Weiterleitungsdienst über udp/40000, über den die Fernwartungsverbindung unabhängig vom Standort des Wartungsplatzes stabil zustande kommt. Bitte geben Sie alle drei Ports frei. Ist **derp.dexa.gmbh** aus Ihrem Netz nicht freigegeben, weicht die Fernwartung ersatzweise auf die Relay-Infrastruktur des Herstellers aus (***.tailscale.com**, tcp/443 und udp/3478). Für einen Betrieb ausschließlich über den deutschen Relay geben Sie bitte **derp.dexa.gmbh** frei. Die Angaben zum Service-Connector bleiben in beiden Fällen erforderlich: Über diesen wird die Verbindung koordiniert, der Relay übernimmt ausschließlich den Transport.

Hinweis zur Authentifizierung: Die Anmeldung an der Bedienoberfläche der Zentrale erfolgt mit Multifaktor-Authentifizierung über den dexa-Anmeldedienst **auth.dexa.gmbh** mit fester Adresse. Ist dieses Ziel aus Ihrem Netz nicht erreichbar, ist keine Anmeldung an der Bedienoberfläche möglich. Der Alarm- und Meldebetrieb der Anlage ist davon nicht betroffen und läuft unabhängig von dieser Verbindung weiter.

2.4 Rechenzentrum

Sämtliche in Block 2 genannten Server der dexa group werden bei der **Centron GmbH** in Deutschland betrieben. Die Verarbeitung Ihrer Anlagendaten findet damit ausschließlich innerhalb der Bundesrepublik Deutschland und des Geltungsbereichs der Datenschutz-Grundverordnung statt; ein Drittlandtransfer findet nicht statt.

Das Rechenzentrum verfügt über folgende Zertifizierungen und Testate:

Zertifizierung	Bedeutung
ISO 27001	Standard für Informationssicherheitsmanagementsysteme (ISMS) – zum Teil auch nach BSI IT-Grundschutz umgesetzt
ISO 9001	Nachweis für ein effektives Qualitätsmanagement
ISO 14001	Zertifizierung für ein nachhaltiges Umweltmanagement
BSI C5:2020 (Typ 1)	Testierte Cloud-Sicherheit für compliance-orientierte Services
German Cloud	Auszeichnung vom Cloud EcoSystem e. V. für datenschutzkonforme Cloud-Lösungen

Die Angaben beziehen sich auf den Betreiber des Rechenzentrums. Bei Fragen zu Nachweisen, Auditberichten oder zur Einbindung in Ihr eigenes Sicherheitskonzept sprechen Sie uns bitte an.

3. Weitere Informationen und Technische Daten

- Weitere Informationen finden Sie in unserer Knowledge Base: https://docs.dexa.gmbh/books/faq

4. Kontaktdaten und Serviceticket

- Ein Serviceticket können Sie durch Scannen des QR-Codes auf Ihrer PoE-Zentrale/PoE-Repeater erstellen.
- Alternativ finden Sie unser Ticketsystem auch hier: https://dexa.gmbh/serviceticket

Dexa Solutions GmbH
Möhnestraße 2
59519 Möhnesee

Telefon: +49 2924 496 937-0
E-Mail: info@dexa.gmbh