

Netzwerkanforderungen Leitstellen-Integration

Netzwerkanforderungen — Anbindung an Leitstellen- / Einsatzleitsysteme

Gültig für die Anbindung der Safe Fire House Brandwarnanlage an Leitstellen- beziehungsweise Einsatzleitsysteme (ELS), beispielsweise iSE COBRA, CKS CELIOS, VivaSecur, IGNIS plus und weitere

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

Die in dieser Anleitung enthaltenen Angaben und Abbildungen entsprechen dem Stand der Auslieferung. Änderungen der Technik, Ausstattung und Form der Geräte gegenüber den Angaben und Abbildungen in dieser Anleitung bleiben der Dexa Solutions GmbH vorbehalten. Diese Anleitung darf weder teilweise noch vollständig vervielfältigt, verbreitet oder verwendet werden. Nur befugten Personen darf diese Anleitung zugänglich gemacht werden.

Diese Anleitung einschließlich aller ihrer Teile ist urheberrechtlich geschützt. Jede Verwendung außerhalb der Grenzen des Urheberrechts ist ohne die Zustimmung der Dexa Solutions GmbH nicht zulässig.

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. Die Anbindung an ein Leitstellen- beziehungsweise Einsatzleitsystem setzt eine entsprechende Schnittstelle sowie deren Freigabe durch den Betreiber der Leitstelle beziehungsweise den Hersteller des Einsatzleitsystems voraus. Wir sind nicht Hersteller der eingesetzten Leitstellen- und Einsatzleitsysteme und übernehmen weder deren Produkthaftung noch die Gewährleistung für deren Schnittstellen. Für die eigens entwickelten Softwareteile haften wir in vollem Umfang, nicht jedoch für Softwareteile von Drittanbietern.

1.2 Hinweise zum Datenschutz

Im Alarmfall werden Alarm- und Standortdaten (Bezeichnung und Anschrift des Standortes, Koordinaten, auslösende Sensorik, Zeitstempel) an das angebundene System übermittelt. Die Übertragung erfolgt

ausschließlich über verschlüsselte, authentifizierte Verbindungen und ausschließlich zum Zweck der Alarmierung und deren Nachweis. Die maßgeblichen Rechtsgrundlagen, Speicherdauern und eingesetzten Auftragsverarbeiter ergeben sich aus den mit Ihnen getroffenen vertraglichen Datenschutzvereinbarungen, insbesondere dem Auftragsverarbeitungsvertrag nach Art. 28 DSGVO.

2. Anbindungswege

Da es keinen einheitlichen, herstellerübergreifenden Standard zur Anbindung an Leitstellen gibt, stehen drei Wege zur Verfügung, mit denen sich in der Regel jedes gängige Einsatzleitsystem anbinden lässt.

Allen Wegen gemeinsam:

- Die Zentrale baut sämtliche Verbindungen **ausschließlich ausgehend auf. Eingehende Portfreigaben oder Portweiterleitungen sind an Ihrem Standort nicht erforderlich.**
- Die Übertragung ist durchgängig TLS-verschlüsselt und authentifiziert.
- Die Rauchmelder und Sensoren kommunizieren per Funk (868 MHz) und stellen keine Anforderung an Ihr Netzwerk.
- Zieladressen, Ports und Zugangsdaten der ELS-seitigen Schnittstelle werden vom Betreiber bereitgestellt und pro Standort festgelegt.

Empfehlung: Für die überwiegende Zahl der Anwendungsfälle ist die Anbindung über das **SMS-Gateway (Abschnitt 2.1)** die wirtschaftlich und technisch sinnvollste Lösung: herstellerunabhängig, kurzfristig umsetzbar, geringe laufende Kosten und mit Echtzeitzustellung sowie Übermittlungsbestätigung nahezu der volle Funktionsumfang einer direkten Schnittstelle — bei deutlich geringerem Einrichtungsaufwand.

2.1 SMS-Gateway (Telekom Vonage API) — empfohlen

Im Alarmfall übergibt der dexa-Alarmdienst die Alarmmeldung über die **Telekom Vonage API** als SMS. Empfänger ist ein **Hardware-SMS-Gateway**, das direkt am Einsatzleitsystem angeschlossen ist und die eingehende SMS in das ELS einspeist. Dieses Gateway empfängt per Mobilfunk (eigene SIM) und ist **entweder bereits vorhanden oder wird durch dexa beigestellt**. Der Weg ist herstellerübergreifend, einfach und kostengünstig und funktioniert mit jedem Einsatzleitsystem.

Ablaufkette:

dexa-Alarmdienst → Telekom Vonage API → (SMS / Mobilfunk) → Hardware-SMS-Gateway am ELS → Einsatzleitsystem

Technischer Ablauf und Nachweis:

- **Versand:** HTTPS-Request des dexa-Alarmdienstes an die Telekom Vonage API; Weiterleitung durch den Gateway in das Mobilfunknetz des Empfängers. Zielrufnummern werden im internationalen Format (E.164, beispielsweise **+49...**) hinterlegt.
- **Echtzeitzustellung:** Die Alarm-SMS wird unmittelbar nach Auslösung übergeben und zugestellt.
- **Übermittlungsbestätigung (Delivery Receipt / DLR):** Der Gateway meldet den Zustellstatus je Nachricht per Callback zurück. Unterschieden werden Zwischenstatus (**accepted** ,

buffered) und Endstatus (**delivered** , **failed** , **rejected** , **expired**); ein Fehlercode (**err-code**) benennt die Ursache bei Nicht-Zustellung. Die Standard-Gültigkeit einer Nachricht beträgt 72 Stunden.

- **Nachweisführung:** Versandzeitpunkt, Zielrufnummer, Nachrichten-Kennung und Zustellstatus werden zentral im dexa-System erfasst und revisionssicher dokumentiert.

Netzwerkanforderung:

Verbindung	Protokoll/Port	Ziel
dexa-Alarmdienst ? Telekom Vonage API	HTTPS (tcp/443), ausgehend	API-Endpunkt der Telekom Vonage API
Telekom Vonage API ? zentrale dexa-Gegenstelle	HTTPS (tcp/443)	dexa-Rückmelde-Endpunkt (DLR-Webhook)

Versand und Entgegennahme der Zustellbestätigung erfolgen zentral über den dexa-Alarmdienst. Das Hardware-SMS-Gateway am Einsatzleitsystem empfängt per Mobilfunk und benötigt keine Anbindung an Ihr Netzwerk. **An Ihrem Standort ist hierfür keine Freigabe und keine Portweiterleitung erforderlich.**

2.2 Direkte Schnittstelle des Einsatzleitsystems (WDX3)

WDX3 ist eine standardisierte Leitstellenschnittstelle (bereitgestellt durch das ELS iSE COBRA). Alarm- und Statusdaten werden über einen **WDX3-Server** ausgetauscht, der durch den Hersteller (iSE, auch als Cloud-Server) oder durch die Leitstelle selbst betrieben wird. Über die Schnittstelle können — je nach Freigabe bidirektional — Einsatzdaten, Einsatzmittel inklusive FMS-Status und Standort, Lagemeldungen sowie Rückmeldungen ausgetauscht werden. Die Übertragung ist fehlertolerant und wiederholt fehlgeschlagene Übermittlungen automatisch.

Technische Voraussetzungen:

- **Transport:** TLS über TCP zum WDX3-Server.
- **Authentifizierung:** Client-Zertifikat mit privatem Schlüssel (mTLS). Zertifikat, Schlüssel, Serveradresse und Port werden vom Betreiber der Schnittstelle (iSE beziehungsweise Leitstelle) bereitgestellt. Zertifikat und privater Schlüssel müssen zueinander passen.
- **Beschaffung/Kosten:** Die WDX3-Schnittstelle wird **einmalig pro Leitstelle** beim Hersteller beauftragt, beschafft und eingerichtet; dies ist mit entsprechendem zeitlichem und finanziellem Aufwand aufseiten der Leitstelle verbunden. Die anschließend angebotenen Organisationen verursachen für die Schnittstellennutzung in der Regel keine weiteren Kosten. Die Freigabe des anzubindenden Systems erfolgt durch den Hersteller auf Anforderung der Leitstelle.

Netzwerkanforderung:

Verbindung	Protokoll/Port	Ziel
dexa-Alarmdienst ? WDX3-Server	TLS über TCP, Port projektspezifisch (Vorgabe des Betreibers)	WDX3-Server des Einsatzleitsystems

2.3 Eigene REST-API des Einsatzleitsystems

Stellt das Einsatzleitsystem eine eigene REST-Schnittstelle bereit, übergibt die Anlage die Alarmdaten direkt an den API-Endpunkt des ELS. Die Übertragung folgt der dexa-Spezifikation „**API-Anforderungen für Alarmierungen**“. Dieser Weg ermöglicht eine tiefgreifende, individuell zugeschnittene Integration

(beispielsweise bidirektionaler Abgleich von Rückmeldungen und Fahrzeugstatus, Übergabe zusätzlicher Objekt- und Datenfelder, angepasste Alarmierungslogik).

Technische Eckdaten (dexa-Alarmierungs-API):

Parameter	Wert
Transport	HTTPS, TLS 1.2 oder höher
Content-Type	application/json; charset=UTF-8
Authentifizierung	Bearer Token (min. 32 Zeichen), verschlüsselt auf der Zentrale hinterlegt
Erstalarm	POST /api/v1/alarms
Nachmeldung (Broadcast)	PUT /api/v1/alarms/{alarmId}
Statusabruf inklusive Rückmeldungen	GET /api/v1/alarms/{alarmId}
Rate Limit	60 Requests/Minute; bei HTTP 429 Retry-After beachten
Idempotenz	über Feld externalId ; SFH-seitige Retry-Strategie (5 s / 10 s / 30 s)
Optional	IP-Whitelisting der SFH-Gegenstelle beim ELS

Netzwerkanforderung:

Verbindung	Protokoll/Port	Ziel
dexa-Alarmdienst ? ELS-REST-API	HTTPS (tcp/443), ausgehend	REST-Endpunkt des Einsatzleitsystems

Die vollständige Feld-, Fehler- und Response-Spezifikation ist in der Knowledge Base unter „API-Anforderungen für Alarmierungen“ hinterlegt.

3. Weitere Informationen und Technische Daten

- Spezifikation der REST-Schnittstelle: „API-Anforderungen für Alarmierungen“ in unserer Knowledge Base.
- 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
