SOFTWARE WHITEPAPER · AUSGABE 1.0

Digitale Feuerwehrverwaltung als sichere Plattform

Architektur, Mandantentrennung, Datenmodell, Sicherheitsprinzipien und Betriebsmodell von IGNIS 2AB – entwickelt für kommunale Feuerwehrstrukturen und nachvollziehbare Verwaltungsabläufe.

Executive Summary

IGNIS 2AB bündelt Personal, Ausbildung, Einsätze, Fahrzeuge, Geräte, Lager, Organisation, Dokumente und ausgewählte Finanzprozesse in einer webbasierten Plattform. Das System bildet eine Hauptfeuerwehr mit untergeordneten Ortsfeuerwehren ab, ohne lokale Verantwortungsbereiche aufzulösen.

Die Architektur kombiniert eine mandantenfähige Symfony-Anwendung, PostgreSQL, private Dateispeicherung, rollen- und feuerwehrbezogene Autorisierung sowie einen getrennten Lizenzdienst. Entwicklung, Demo und Produktion sind organisatorisch und technisch getrennt.

1. Ausgangslage und Zielbild

Feuerwehrverwaltungen arbeiten häufig mit heterogenen Fachanwendungen, Tabellen, Papierakten und lokalen Ablagen. Dadurch entstehen Medienbrüche, doppelte Pflege, uneinheitliche Berechtigungen und geringe Transparenz über Qualifikationen, Einsatzbereitschaft und Technik.

IGNIS 2AB verfolgt ein modulares Zielbild: Eine gemeinsame Datenbasis, eindeutige Organisationskennungen, feingranulare Rechte, prüfbare Lebenszyklen und standardisierte Exporte – bei weiterhin klarer Trennung der einzelnen Feuerwehren.

2. Technische Architektur

Anwendung

Symfony 7.4, PHP 8.2+, Twig, serverseitige Validierung und Security-Komponenten.

Datenbank

PostgreSQL mit fachlichen Schemas, UUIDs und zusätzlicher Mandantentrennung.

Betrieb

Containerisierter Betrieb mit Nginx, reproduzierbaren Deployments und Healthchecks.

Dateien

Private Upload-Ablage außerhalb des öffentlichen Webroots, UUID-Dateinamen und Prüfsummen.

E-Mail

Authentifizierter SMTP-Versand mit TLS für Verifizierung, Berichte und Benachrichtigungen.

Lizenzierung

Separater anwendungsunabhängiger Dienst auf license.2ab.it mit signierter API.

3. Organisations- und Mandantenmodell

Jede Kundenorganisation besitzt eine unveränderliche Org-ID. Haupt- und Ortsfeuerwehren erhalten Site-IDs; jede bereitgestellte Instanz besitzt eine Installations-ID. Diese UUID-basierten Kennungen verhindern namensbasierte Mehrdeutigkeiten und bilden zugleich die Grundlage für Schnittstellen und Lizenzierung.

Fachdaten werden einem Mandanten und – soweit fachlich erforderlich – einer Feuerwehr zugeordnet. Ortsfeuerwehren sehen und bearbeiten grundsätzlich ihre eigenen Daten. Zentrale Rollen erhalten nur die ausdrücklich vorgesehenen organisationsübergreifenden Lese- oder Verwaltungsrechte.

Die Anwendung kombiniert Repository-Filter, Berechtigungsprüfungen und Datenbankmechanismen. Die aktive Feuerwehr ist ein expliziter Benutzerkontext, keine bloße Oberflächenfilterung.

4. Fachmodule

Personal

Stammdaten, Dienstgrade, Funktionen, Gruppen, Qualifikationen, Dokumente und Organigramme.

Ausbildung

Kataloge, Buchungen, Prüfung, Genehmigung, Ablehnung und personenbezogene Ausbildungsakte.

Einsatz

Einsätze, Beteiligte, Fahrzeuge, Geräte, Material, Zeitlinie, Berichte und Bescheinigungen.

Technik

Fahrzeuge, Beladung, Geräte, Funktechnik, Prüfungen, Wartung und Lifecycle-Ereignisse.

Lager

Artikel, Bestände, Eingänge, Ausgaben, Inventur und Bestellungen.

Organisation

Feuerwehrstruktur, Benutzerzuordnung, Logos, Lizenzen und Importwerkzeuge.

Finanzen

Ausgewählte Prozesse wie arbeitgeberbezogener Verdienstausfall mit geschütztem Zugriff.

Dokumente

Einheitliche Verknüpfung mit Personen, Fahrzeugen, Geräten und Einsätzen.

5. Sicherheitsarchitektur

Identität und Zugriff

Individuelle Benutzerkonten, Passwort-Hashing, Login-Drosselung, CSRF-Schutz, sichere Sessions und Zwei-Faktor-Authentisierung schützen den Zugang. Privilegierte Rollen sollen 2FA verpflichtend verwenden.

Autorisierung

Rollen, Mandantenmitgliedschaft, aktive Feuerwehr und objektspezifische Voter werden gemeinsam ausgewertet. Nicht berechtigte Objekte können absichtlich als nicht vorhanden erscheinen, um Informationslecks zu vermeiden.

Transport und API

Öffentliche Verbindungen verwenden TLS. APIs sind ausnahmslos tokenpflichtig. Lizenzprüfungen werden mit HMAC-SHA256, Zeitstempel und Nonce gegen Manipulation und Replay geschützt; Antworten sind ebenfalls signiert.

Infrastruktur

Host-Firewall, Fail2ban, schlüsselbasierter SSH-Zugang, getrennte Konten, Sicherheitsheader und kontrollierte Deployments ergänzen die Anwendungskontrollen.

6. Daten- und Dokumentenmodell

UUIDs dienen als stabile technische Primärschlüssel. Fachliche Kennungen wie Personalnummern bleiben davon getrennt. Lebenszyklusmodelle dokumentieren Prüfungen, Wartungen, Ausgaben, Rückgaben, Aussonderungen, Eintritte, Austritte, Beförderungen und Funktionswechsel.

Uploads werden privat abgelegt, mit internen Dateinamen und SHA-256-Prüfsummen versehen und über kontrollierte Downloadrouten ausgeliefert. Dokumentverknüpfungen erlauben fachbezogene Ablage ohne öffentliche Dateipfade.

Besonders schutzbedürftige Informationen, etwa Tauglichkeit oder Verdienstausfall, benötigen eingeschränkte Rollen, Auditierung und festgelegte Löschfristen.

7. Migration und Integration

Der Import aus alternativen Systemen verarbeitet bereitgestellte Sicherungen in einem kontrollierten Ablauf aus Upload, technischer Prüfung, Vorschau und ausdrücklich freigegebenem Import. Quell-IDs, Prüfsummen, Zielobjekte und Warnungen werden protokolliert.

Importe erzeugen keine stillschweigende fachliche Wahrheit: Zuordnungen, Dubletten, Nummernkreise und Organisationsstrukturen müssen fachlich geprüft und abgenommen werden. Ein strukturierter Export unterstützt Datenportabilität und Vertragsende.

Öffentliche Fach-APIs werden erst nach Versionierung, Rechtekonzept, Datenminimierung und dokumentierter Freigabe aktiviert. Die aktuelle API-Dokumentation beschreibt ausschließlich die bereits vorhandene Lizenz- und Provisionierungs-API.

8. Lizenz- und Betriebsmodell

Eine Mandantenlizenz deckt die zentrale Hauptfeuerwehr ab. Ortsfeuerwehren werden als eigenständig lizenzierbare Stationen unter der Organisation geführt. Der Lizenzserver speichert nur notwendige Organisations- und Installationsmetadaten und keine Feuerwehrpersonaldaten.

Aktive und Trial-Lizenzen liefern Schreibzugriff; abgelaufene, gesperrte, widerrufene oder nicht lizenzierte Einheiten werden in den Lesemodus versetzt. Lizenzstatus wird regelmäßig geprüft und kann innerhalb einer begrenzten Offline-Grace sicher zwischengespeichert werden.

9. Entwicklung, Qualität und Betrieb

Der Entwicklungsserver ist die Single Source of Truth. Änderungen werden versioniert, getestet und zunächst in einer Demo-Umgebung geprüft. Die Produktion wird bewusst und mit Datenbanksicherung, Migrationsprüfung, Rollbackplan und Funktionscheck aktualisiert.

Healthchecks, Anwendungs- und Systemprotokolle, Speicher- und RAID-Überwachung sowie Backup- und Restore-Verfahren unterstützen den Betrieb. Buildkennungen unterscheiden Entwicklung, Demo und Produktion.

Tests konzentrieren sich neben Fachlogik besonders auf Berechtigungen, Mandantentrennung, Organisationswechsel, Importkonsistenz, Lizenzverhalten und sicherheitskritische Abläufe.

10. Datenschutz und Governance

Kommunen beziehungsweise Kunden bleiben für ihre Fachdaten verantwortlich; 2AB verarbeitet sie im Rahmen eines Vertrags nach Art. 28 DSGVO. Verarbeitungsanlage, TOM, Unterauftragnehmerliste und Weisungsformular konkretisieren die Verantwortlichkeiten.

Datenschutz durch Technikgestaltung umfasst Datenminimierung, private Speicherung, Berechtigungstrennung, Protokollierung, Export-, Berichtigungs- und Löschprozesse sowie getrennte Entwicklungsdaten. Löschfristen werden je Datenkategorie verbindlich beschlossen und technisch umgesetzt.

Eine Datenschutz-Folgenabschätzung, das Verzeichnis der Verarbeitungstätigkeiten und die Abnahme durch Datenschutzbeauftragte gehören zur organisatorischen Produktionsfreigabe.

11. Abgrenzung und Weiterentwicklung

IGNIS 2AB unterstützt Verwaltungs- und Dokumentationsprozesse, ersetzt jedoch keine Einsatzleitung, medizinische Beurteilung, rechtliche Prüfung oder gesetzlich vorgeschriebene Fachentscheidung.

Die Plattform wird modular weiterentwickelt. Künftige Schwerpunkte sind standardisierte Fach-APIs, weitergehende Datenschutzautomatisierung, Malwareprüfung von Uploads, verschärfte Content-Security-Policy, Ausbau automatisierter Sicherheitsprüfungen und zusätzliche Integrationen.