

Vorgaben aus IT-Sicht

Inhalt

Allgemeine Vorgaben zu Anwendungen	3
Integrationsfähigkeit in Portale und Workflows	3
Qualitätssicherung	3
Vorgaben für den Betrieb	3
Antwortzeit	3
Appliances nur mit Wartung durch den Anbieter	3
Herstellersupport	4
Plattform-Konformität	4
Remote-Management von Serverkomponenten	4
Vorgaben für Installationsverfahren	4
Vorgaben zu Backup & Recovery	5
Vorgaben zur Netzwerkkommunikation	5
Vorgaben zur Virtualisierbarkeit	5
Wartungsarbeiten und Störungsbeseitigung	5
Vorgaben zu Clients	5
Allgemeine Vorgaben für Clients	5
Vorgaben für Windows-Apps	5
Vorgaben zum Datenaustausch	6
Verfahren für den Austausch von Dateien	6
Vorgaben zur Datenhaltung	6
Auswahl der Datenbank	6
Vorgaben zu dezentraler Datenhaltung	6
Nutzung von Stored Procedures in Datenbanken	7
Vorgaben zum Datenschutz	7
Hosting - Auswertung gesammelter Daten nur mit TK-Auftrag	7
Keine Datenübermittlung an Dritte	7
Vorgaben zur Ergonomie	7
Barrierefreiheit für interne Anwendungen	7
Vorgaben zur Verfügbarkeit	7
Erweiterte Anforderungen an die Verfügbarkeit	7
Vorgaben zu Webclients	8
Lauffähigkeit auf aktuellen Browsern	8
Vorgaben für Webclients (allgemein)	8

Allgemeine Vorgaben zu Anwendungen

Integrationsfähigkeit in Portale und Workflows

Alle Funktionen der Anwendung sind über eine API und/oder eine URL aufrufbar.

Qualitätssicherung

Der AN unterzieht den Content, die Funktionalitäten und die Anwendungen einer inhaltlichen und technischen, nachhaltigen Qualitätssicherung (QS). Folgende Maßnahmen werden durch den AN im Rahmen der QS mindestens eingesetzt:

- Tests inkl. Dokumentation der Testfälle und -ergebnisse
- Statische und dynamische Verfahren zum Aufspüren von Schwachstellen in eigenentwickeltem Code
- Verfahren zur Erkennung von Schwachstellen in verwendeten Drittanbieterkomponenten
- Überprüfen von Code-Qualitätsstandards in eigenentwickeltem Code
- Change-Management inkl. Freigabeverfahren
- Problem-Management inkl. Lösungen und Maßnahmen zur künftigen Prävention

Der AN legt im Rahmen der Auftragsdurchführung das Verfahren zur QS gegenüber der TK offen. Bei festgestellten Mängeln kann die TK Nachbesserung verlangen.

Vorgaben für den Betrieb

Antwortzeit

Die Anwendung beantwortet 95% aller Anfragen in weniger als 2 Sekunden.

Für Anwendungen, die in der TK betrieben und genutzt werden, zählt dabei die End-2-End-Antwortzeit am Client. Es kann dabei davon ausgegangen werden, dass alle Clients mindestens über ein WAN mit 4 MBit/s angebunden sind. Die aktuellen Hard- und Software-Spezifikationen eines TK-Referenzclients können auf Anfrage entsprechend bereitgestellt werden.

Für Anwendungen, bei denen die Antwort über das Internet ausgeliefert wird, kann seitens TK mit einem für die Anwendung zur Verfügung stehenden/zugesicherten Bandbreitendurchsatz von 5 MBit/s gerechnet werden, bei einer Latenz von max. 100ms.

Auf Basis dieser Kennzahlen muss die Anwendung für die geforderten Transaktionen die entsprechende Antwortzeiten einhalten.

Appliances nur mit Wartung durch den Anbieter

Der Auftragnehmer führt sämtliche Wartungsarbeiten aller zum Lieferumfang gehörenden Komponenten der Appliance entweder selbst durch oder lässt sie durch den Hersteller/Lieferanten durchführen. Dies gilt insbesondere für Sicherheitsupdates und Behebung von Fehlkonfigurationen.

Der Auftragnehmer führt entweder vor Auslieferung der Appliance spätestens aber im Rahmen der Inbetriebnahme die vom Hersteller empfohlenen Härtingsmaßnahmen durch. Dies beinhaltet insbesondere:

- Änderung von Standardpasswörtern, Standardschlüsseln
- Soweit möglich Deinstallation nicht benötigter Softwarebestandteile. Falls Deinstallation nicht möglich, soweit möglich Deaktivierung nicht benötigter Funktionen. Falls Deaktivierung nicht möglich, soweit möglich Beschränkung der Zugriffe.

- Installation der zum Auslieferungszeitpunkt jeweils aktuellen Softwarestände.

Herstellersupport

Der AN leistet Support mit garantierten Responsetimes. Die Responsetime in dem Fall, dass die Anwendung nicht zur Verfügung steht, beträgt 4 Stunden im Zeitraum 24/7.

Plattform-Konformität

Die Anwendung wird als Software as a Service oder als Appliance ausgeliefert oder sie ist auf einer im RZ der TK betriebenen und nachfolgend aufgelisteten Plattform lauffähig.

- JBoss EAP 7 und Apache 2.4 auf Linux
- Windows Server zum Angebotszeitpunkt aktuelles Major-Release im Long Term Servicing Channel (LTSC) und Vorgängerversion (auch im LTSC)
- Red Hat Enterprise Linux, zum Angebotszeitpunkt aktuelles Major-Release und Vorgängerversion
- Red Hat OpenShift 4.x (aktuelles Minor-Release)
- Open Virtual Appliance auf VMware ESX 8.0
- SAP Netweaver 7.5

Remote-Management von Serverkomponenten

Die Serverkomponente der Anwendung kann remote administriert und konfiguriert werden.

Der serverseitige Teil der Anwendung ist komplett ohne interaktive Eingaben über die Kommandozeile zu starten, zu stoppen und der Status abzufragen. Entsprechende Skripte oder Konfigurationsdateien für die vorgesehene Plattform werden mitgeliefert (z. B. Unit-Files, Deployment-Konfigurationen).

Ein Monitoring aller Serverprozesse von einem zentralen Punkt ist möglich.

Von der Anwendung erzeugte Logdaten können an ein zentrales Log Management System weitergeleitet werden.

Vorgaben für Installationsverfahren

Sofern die Anwendung für Installation auf Nutzerendgeräten vorgesehen ist, erfolgt die Installation silent also ohne Interaktion mit den Nutzenden.

Die Installationspfade sind frei definierbar, Umgebungsvariablen werden unterstützt.

Der Ablageort von benutzerspezifischen Dateien ist frei konfigurierbar (z.B. kein Zwang zum Roamingprofil oder UE-V (User Experience Virtualization)).

Die Installationsroutine kann vorhandene ältere Installationen der Anwendung erkennen und deinstallieren.

Die AN liefert je nach Plattform eines der folgenden Paketformate:

Plattform	Paketformat	Installationstool
Windows	MSI oder Setup	Windows Installer
JBoss	war oder ear	-
Redhat Linux	rpm	yum/dnf
VMware	OVA	-

OpenShift	Docker Image	-
-----------	--------------	---

Vorgaben zu Backup & Recovery

Die Anwendung besitzt die Fähigkeit zu Backup & Recovery.

Entweder: Das Backup und Recovery der Anwendung ist mit der bei der TK eingesetzten Datensicherungslösung VEEAM möglich. Oder: Der AN liefert einen alternativen Weg für Backup und Recovery der Anwendung.

Die Anwendung behindert ein Backup von Datenbanken und des Filesystems nicht.

Vorgaben zur Netzwerkkommunikation

Alle verwendeten Netzwerk-Kommunikationsprotokolle sind gemäß den jeweils gültigen RFCs implementiert. Die Anwendung ist integrierbar in Netzwerken, in denen IPv4-Netzwerk-Adress-Translation eingesetzt wird. Die Netzwerk-Kommunikation des Produktes ist zwischen per Firewallsystemen getrennten Netzwerkbereichen möglich.

Vorgaben zur Virtualisierbarkeit

Die Anwendung ist auf einem virtuellen Server unter VMware vSphere ab Version 9.0 lauffähig.

Wartungsarbeiten und Störungsbeseitigung

In Abstimmung mit der TK können Wartungsarbeiten und die Bearbeitung von Störungsmeldungen im direkten Remote Zugriff auf die installierten Server ermöglicht werden. Der Auftragnehmer verpflichtet sich, diese Arbeiten unter Einhaltung der geltenden Datenschutzanforderungen zu leisten. Ein Zutritt der Auftragnehmer zu einem RZ der TK ist nur in Begleitung und mit vorheriger Anmeldung beim Operating möglich, kann aber auch außerhalb der normalen Arbeitszeiten gewährt werden.

Vorgaben zu Clients

Allgemeine Vorgaben für Clients

Die Anwendung reagiert auf die Eigenschaften des jeweils benutzten Endgerätes und unterstützt eine geräteoptimierte Darstellung, die gute Lesbarkeit und einfache Navigation mit einem Minimum an Verschieben und Blättern ermöglicht (Responsive Design).

Die Validierung von Eingaben erfolgt immer serverseitig und ggf. **ergänzend** clientseitig (z.B. durch JavaScript).

Vorgaben für Windows-Apps

Die Anwendung ist ohne Zugriffe auf Wechselmedien (CD, DVD, Diskette, USB-Stick etc.) lauffähig.

Die Anwendung ist unter dem Betriebssystem Windows 11 Enterprise 64 Bit in einem User-Kontext ohne Administrator-Rechte lauffähig.

Die Installation der Software kann in einen Maschinen- und User-Teil geteilt werden.

Die Anwendung unterstützt eine Bildschirm-Auflösung von mind. 1920x1080 und skaliert für höhere Auflösungen.

Die Anwendung ist auf einem x64-basierten PC mit einem Prozessor mit 2 GHz und 8 GB Hauptspeicher lauffähig.

Die Anwendung kann mit den folgenden Client-Anwendungen auf einem System koexistieren:

- Microsoft M365Apps Enterprise X64
- Firefox
- Edge
- Google Chrome
- SAP-GUI Version 770
- MS System Center Defender
- Java Virtual Machine (Oracle) 1.8.x
- Java Virtual Machine (OpenJDK) 11
- Netskope Client
- MS Defender for Endpoint

Vorgaben zum Datenaustausch

Verfahren für den Austausch von Dateien

Die TK unterstützt für den Austausch mit externen Stellen folgende Verfahren:

- Automatisierte Austauschverfahren für den Datenaustausch im Gesundheitswesen (s. "Gemeinsame Grundsätze Technik", https://www.gkv-datenaustausch.de/technische_standards_1/technische_standards.jsp)
- Austausch über fest definierte S-FTP bzw. FTP-S Server bei externen Partnern.
- S/MIME-gesicherte E-Mails
- Manueller Austausch über Cryptshare (<https://webft.tk.de>)

Für Datentransfers von und zur TK müssen die unterstützten Verfahren genutzt werden. Das gewählte Verfahren ist zwischen TK und AN zu vereinbaren und vom AN zu beschreiben. Soweit technisch machbar und wirtschaftlich umsetzbar, sind die Verfahren des Datenaustausches im Gesundheits- und Sozialwesen über Datenannahmestellen (siehe <https://www.gkv-datenaustausch.de>) bevorzugt zu verwenden.

Bei Verwendung von S-FTP bzw. FTP-S stellt der Auftragnehmer den entsprechenden Server bereit und betreibt diesen.

Vorgaben zur Datenhaltung

Auswahl der Datenbank

Die Anwendung unterstützt eines der folgenden Datenbanksysteme:

- Oracle EE in der aktuellen LTS (Longterm Support) Version (vg. Oracle Doc ID 742060.1), ausschließlich auf Oracle Exadata Systemen mit Code-Page (Character Set) AL32UTF8
- Microsoft SQL-Server Enterprise for Windows, die Version muss einer der beiden höchsten derzeit im Microsoft Support verfügbaren RTM Versionen entsprechen
- SAP HANA - Für Anwendungen, die auf der Plattform SAP eingesetzt werden, zwingend erforderlich

Die Anwendung ist mit den Standard-Technologien zu Hochverfügbarkeit (HA) / Disaster Recovery (DR) der jeweiligen Datenbank verträglich.

Die Verbindungen zwischen Anwendung als Client und RDBMS als Server halten die Vorgaben zur Netzwerkkommunikation sowie zu Transport Layer Security (TLS) ein.

Vorgaben zu dezentraler Datenhaltung

Sofern Daten bspw. aus Performancegründen dezentral gespeichert werden, so werden Verfahren zur Datensicherung und zum Schutz der Vertraulichkeit und Integrität angegeben und umgesetzt.

Nutzung von Stored Procedures in Datenbanken

Sofern Stored Procedures auf einer von der TK betriebenen Datenbank eingesetzt werden, sind diese in einer vom Datenbankhersteller vorgegebenen Sprache geschrieben und sind ohne die Verwendung von externen Bibliotheken in der Datenbank lauffähig. Die Verwendung ist detailliert beschrieben.

Vorgaben zum Datenschutz

Hosting - Auswertung gesammelter Daten nur mit TK-Auftrag

Der Auftragnehmer gibt keine im Rahmen des Betriebes gesammelten personenbezogenen Daten an Dritte weiter oder wertet diese ohne Auftrag aus.

Keine Datenübermittlung an Dritte

Personenbezogene Daten gem. Art. 4 Nr. 1 DSGVO sowie Sozialdaten gem. § 67 Abs. 2 SGB X dürfen nicht an Dritte gem. Art. 4 Nr. 10 DSGVO übermittelt werden, sofern sich dies nicht explizit aus dem Vertrag oder einer gesetzlichen Verpflichtung nach deutschem oder europäischem Recht ergibt.

Vorgaben zur Ergonomie

Barrierefreiheit für interne Anwendungen

Das User Interface ist barrierefrei. Es unterstützt mindestens:

- Vollständige Tastaturbedienbarkeit
- Unterstützung von Screenreadern und Braille-Zeilen
- Alternativtexte für Bilder
- Bedienbarkeit auch bei Einsatz eines Skalierungsfaktors von 250% gegenüber der von der Berufsgenossenschaft empfohlenen Schriftgröße (Zeichenhöhe für Großbuchstaben in mm = Sehabstand in mm / 155; entsprechend 20-22 Bogenminuten Sehwinkel).
- Bedienbarkeit bei Einsatz der durch das Betriebssystem bereitgestellten Mittel zur erleichterten Bedienung (insbesondere die Nutzung der vom Betriebssystem vorgegebenen Standards, damit individuell angepasste Farbschemata verwendet werden können).

Vorgaben zur Verfügbarkeit

Erweiterte Anforderungen an die Verfügbarkeit

Für die Überprüfung der Einhaltung des Service Level Agreements (SLA) hinsichtlich der Transaktionszeiten stellt der AN der TK mind. eine entsprechende offene Schnittstelle (API) bereit, über die Antwortzeit- und Verfügbarkeitsmetriken in Intervallen von maximal 15 Minuten maschinenlesbar abgerufen werden können. Folgende Verfahren stehen dabei alternativ zur Verfügung:

- Die Anwendung bietet einen HTTPS Metricendpoint (z.B. nach Prometheus-Standard bzw. OpenTelemetry Spezifikationen) und liefert darüber detailliert Performancemetriken zu den ausgeführten Transaktionen.
- Die Anwendung bzw. eine eigene Monitoringagentenkomponente unterstützt nativ die Weiterleitung von ihren eigenen Performancedaten an einen InfluxDB kompatiblen Endpoint.
- Sofern es sich um netzwerknahe Services (z. B. Printspool) handelt, ist zusätzlich möglich: Die Anwendung bietet eine SNMP Schnittstelle, welche Abfragen via SNMP (v3) zulässt, um Performancemetriken der Anwendung aktiv auszulesen.

Zur Überprüfung der Erreichbarkeit des Service stellt der AN einen Referenzdienst bereit. Der Referenzdienst simuliert das Verhalten des bereitgestellten Dienstes und muss ein sicherer Indikator für die Verfügbarkeit und Performance aller beteiligten Komponenten sein. Die Details zur Nutzung des Referenzdienstes im Rahmen des Monitorings werden zwischen TK und AN abgestimmt.

Ein Dienst gilt in einem Abfrage-Referenzintervall als nicht verfügbar, wenn entweder der Dienst nicht erreicht werden kann oder in diesem und den beiden vorhergehenden Referenzintervallen die vereinbarten Antwortzeiten nicht eingehalten wurden.

Die Anwendung muss ein automatisches Umschalten beim Schwenken von benutzten Server- und Netzwerk-Ressourcen unterstützen, ohne dass dazu manuelle Eingriffe nötig sind.

Der Auftragnehmer hat ein funktionierendes Business Continuity Management, mind. in Anlehnung des BSI-Standards 200-4 oder der ISO 22301 BCMS, bei sich etabliert.

Vorgaben zu Webclients

Lauffähigkeit auf aktuellen Browsern

Die vom AN bereitgestellte Anwendung bzw. die bereitgestellten Internetseiten werden von folgenden Browsern vollständig und korrekt dargestellt und sind vollständig funktionsfähig: Google Chrome, Mozilla Firefox, Microsoft Edge, Apple Safari.

Von jedem Browser werden diejenigen Versionen unterstützt, welche von dem jeweiligen Hersteller innerhalb den letzten 24 Monaten veröffentlicht wurden. Dies gilt fortlaufend über die komplette Vertragslaufzeit. Der AN testet die Anwendung bzw. die Internetseiten mit den zu unterstützenden Browsern.

Die TK kann die Liste der zu unterstützenden Browser aktualisieren, z.B. um die Entwicklungen des Marktes zu berücksichtigen. Sie zeigt dem AN die Aktualisierung schriftlich per E-Mail oder über ein Ticketsystem (falls vorhanden) an. Der AN stellt die Unterstützung der in der aktualisierten Liste genannten Browser binnen vier Wochen sicher, sofern die neu hinzugekommenen Browser vergleichbar kompatibel mit der aktuellen HTML Spezifikation des W3C sind.

Vorgaben für Webclients (allgemein)

Für die Internetseiten und -anwendungen gelten nachstehende Anforderungen und Pflichten zu den verwendeten Sprachen und Gestaltungstechniken:

- Als clientseitige Scriptsprache wird nur JavaScript eingesetzt.
- Flash-Animationen und andere Plugins werden nicht eingesetzt.
- Framesets werden nicht eingesetzt.
- Die Anwendung unterstützt die Kommunikation mit einem WEB-Proxy grundsätzlich unterstützen. Darüber hinaus entsprechen die verwendeten Technologien und Protokolle den üblichen Internetstandards gemäß Request for Comments (RFC).
- Der AN setzt konsequent Cascading Style Sheets ein und gewährleistet damit die Trennung von Inhalt und Darstellung - unter Einhaltung des Corporate Design der TK.
- Die vom AN eingesetzten Stylesheets sind entsprechend der aktuellen W3C-Konvention syntaktisch korrekt.
- Der AN hat dabei die zum Zeitpunkt der Entwicklung die aktuellste Version der UI Library zu verwenden und
- Auf explizite Anweisung des AG ist die verwendete Version der UI Library innerhalb von 4 Wochen auf einen genannten Stand zu aktualisieren. Es steht dem AN frei

selbständig aktuellere Versionen der UI Library zu verwenden, sowie diese im Laufe des Vertragsverhältnisses vom AG veröffentlicht werden.