

Vorgaben aus IT-Sicht: Managed File Transfer

25-08734

Inhalt

Vorgaben aus IT-Sicht: Managed File Transfer	1
Allgemeine Vorgaben zu Anwendungen	3
Integrationsfähigkeit in Portale und Workflows	3
Qualitätssicherung	3
Vorgaben für den Betrieb	3
Antwortzeit	3
Herstellersupport	3
Plattform-Konformität	4
Remote-Management von Serverkomponenten	4
Vorgaben für Installationsverfahren	4
Vorgaben zu Backup & Recovery	4
Vorgaben zur Netzwirkommunikation	5
Vorgaben zur Virtualisierbarkeit	5
Wartungsarbeiten und Störungsbeseitigung	5
Vorgaben zu Clients	5
Allgemeine Vorgaben für Clients	5
Vorgaben zur Datenhaltung	5
Auswahl der Datenbank	5
Gebot zentraler Datenhaltung	6
Nutzung von Stored Procedures in Datenbanken	6
Vorgaben zum Datenschutz	6
Keine Datenübermittlung an Dritte	6
Vorgaben zur Ergonomie	6
Barrierefreiheit für externe Anwendungen	6
Barrierefreiheit für interne Anwendungen	6
Vorgaben zu Webclients	6
Lauffähigkeit auf aktuellen Browsern	6

Allgemeine Vorgaben zu Anwendungen

Integrationsfähigkeit in Portale und Workflows

Alle wesentlichen Funktionen der Anwendung müssen über eine API und/oder eine URL aufrufbar sein. Eine API soll als REST-API mit der Unterstützung von standardisierten Sicherheits-Mechanismen zur Autorisierung ausgestaltet sein. Ein Aufruf per URL soll über Standardbrowser mit standardisierten Sicherheitsmechanismen möglich sein. Die API soll klar und eindeutig nach OpenAPI Standard dokumentiert sein.

Der Aufruf von Funktionen für extern übergebene Schlüsselwerte (z. B. eine Versichertennummer oder eine Prozess-ID) soll möglich sein.

Die Anwendung soll in TK-eigene Prozesse integriert werden können. Dazu soll sie folgende Funktionalitäten bereitstellen:

- Überwachung von Statusänderungen in der Anwendung mit Möglichkeit der Weiterleitung an einen Event-Bus
- Verwaltung einer TK-Prozess-ID als Ordnungsbegriff

Qualitätssicherung

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

- Tests inkl. Dokumentation der Testfälle und -ergebnisse
- Überprüfen von Qualitätsstandards
- Change-Management inkl. Freigabeverfahren
- Problem-Management inkl. Lösungen und Maßnahmen zur künftigen Prävention

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

Vorgaben für den Betrieb

Antwortzeit

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

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 gerechnet werden, bei einer Latenz von max. 100ms.

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

Die Performancedaten (Antwortzeit, Durchsatz, Fehleranzahl) aller wesentlichen Funktionen/Transaktionen der Anwendung sollen in ein Berichtswesen auf Basis Grafana / InfluxDB integriert werden können, deshalb müssen entsprechende Metriken seitens der Anwendung über offene Schnittstellen bereitgestellt werden können.

Herstellersupport

Der AN hat Support mit garantierten Responsetimes zu leisten gemäß Anlage V2 Leistungsbeschreibung, Kapitel 6.3 Supportlevel der MFT-Lösung inkl. „Premium Support und TAM“

Die Integration in die ITSM-Prozesse der TK soll für Second- und Third-Level-Support Ticket-basiert automatisierbar sein. Tickets, die beim AN zur Bearbeitung liegen, sollen durch zuständige TK-Mitarbeiter einsehbar sein.

Plattform-Konformität

Die Anwendung muss auf einer der folgenden, im RZ der TK betriebenen Plattformen lauffähig sein.

- Red Hat Enterprise Linux 8.x (aktuelles Minor-Release)
- Red Hat Enterprise Linux 9.x (aktuelles Minor-Release) mit aktiviertem SELinux
- Red Hat OpenShift 4.x (aktuelles Minor-Release)

Remote-Management von Serverkomponenten

Die Serverkomponente der Anwendung muss remote administriert und konfiguriert werden können.

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

Ein Monitoring aller Serverprozesse von einem zentralen Punkt muss möglich sein.

Das Logging muss über die von der Plattform vorgegebene Logging Facility erfolgen.

Vorgaben für Installationsverfahren

Anwendungen sollen ohne Benutzerinteraktion (silent) installierbar sein.

Installationen auf Clients müssen silent erfolgen können.

Die Installationspfade müssen frei definierbar sein und Umgebungsvariablen unterstützen.

Der Ablageort von benutzerspezifischen Dateien muss frei konfiguriert werden können (z.B. kein Zwang zum Roamingprofil oder UE-V (User Experience Virtualization)).

Die Installationsroutine muss vorhandene ältere Installationen der Anwendung erkennen und deinstallieren können.

Die Anwendung muss je nach Plattform in folgendem Paketformat geliefert werden:

Plattform	Paketformat	Installationstool
Redhat Linux	rpm	yum/dnf
VMware	OVA	-

Vorgaben zu Backup & Recovery

Die Anwendung muss die Fähigkeit zu Backup & Recovery besitzen.

Sofern die Anwendung im RZ der TK betrieben wird, soll das Sichern und das Wiederherstellen der Anwendung durch die bestehende Datensicherungslösung der Firma Veeam möglich sein.

Die Anwendung soll das Online-Backup der Datenbank und die Sicherung der Filesysteme nicht behindern.

Sofern die obigen Soll-Bedingungen nicht eingehalten werden, müssen alternative Sicherungs- und Wiederherstellungsmethoden aufgezeigt werden (z. B. Scriptmethoden zum Wegschreiben von wichtigen Anwendungsdaten).

Vorgaben zur Netzwerkkommunikation

Alle verwendeten Netzwerk-Kommunikationsprotokolle müssen gemäß den jeweils gültigen RFCs implementiert sein.

Das Produkt muss in Netzwerken, in denen IPv4-Netzwerk-Adress-Translation eingesetzt wird, integrierbar sein.

Die Netzwerk-Kommunikation des Produktes muss zwischen per Firewallsystemen getrennten Netzwerkbereichen möglich sein.

Vorgaben zur Virtualisierbarkeit

Die Anwendung soll auf einem virtuellen Server unter VMware vSphere ab Version 6.7 lauffähig sein.

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 muss auf die Eigenschaften des jeweils benutzten Endgerätes reagieren können und eine geräteoptimierte Darstellung unterstützen, die gute Lesbarkeit und einfache Navigation mit einem Minimum an Verschieben und Blättern ermöglicht (Responsive Design).

Eine clientseitige Validierung von Eingaben (z. B. mit JavaScript) darf nur ergänzend zu einer serverseitigen Validierung vorgenommen werden.

Vorgaben zur Datenhaltung

Auswahl der Datenbank

Die Software muss eines der folgenden Datenbanksysteme unterstützen:

- 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
- PostgreSQL, die Version muss einer der beiden höchsten derzeit verfügbaren RTM-Versionen entsprechen.

Anwendungen müssen mit den Standard-Technologien zu Hochverfügbarkeit (HA) / Disaster Recovery (DR) der jeweiligen Datenbank verträglich sein.

Die Verbindungen zwischen Client und Server müssen die Vorgaben zur Netzwerkkommunikation sowie zur Transport Layer Security (TLS) einhalten.

Die oben genannten Datenbanksysteme müssen nicht unterstützt werden, wenn

- ein aufwandsloser Betrieb im Sinne einer SaaS-, einer Appliance- oder einer Container-Lösung sichergestellt ist
- und ggf. absehbare Anforderungen zur Anbindung an ein Data Ware House oder einen Data Lake anderweitig (z.B. über APIs) abgedeckt sind

Gebot zentraler Datenhaltung

Die Anwendung soll Daten zentral speichern. Eine dezentrale Speicherung auf Endgeräten soll nicht erfolgen. Sofern es eine Herstellerempfehlung gibt, Daten aus Performancegründen dezentral vorzuhalten, so müssen geeignete Verfahren zur Datensicherung und zum Schutz der Daten angegeben werden.

Nutzung von Stored Procedures in Datenbanken

Wenn Stored Procedures auf einer von der TK betriebenen Datenbank eingesetzt werden, dann müssen diese in einer vom Datenbankhersteller vorgegebenen Sprache geschrieben sein und müssen ohne die Verwendung von externen Bibliotheken in der Datenbank lauffähig sein. Die Verwendung muss detailliert beschrieben sein.

Vorgaben zum Datenschutz

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 externe Anwendungen

Anwendungen, die für die Benutzung durch TK-Kunden oder die Allgemeinheit gedacht sind, müssen die BITV 2.0 einhalten.

Barrierefreiheit für interne Anwendungen

Das User Interface muss barrierefrei sein. Es muss mindestens unterstützen:

- 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 zu Webclients

Lauffähigkeit auf aktuellen Browsern

Die vom AN bereitgestellte Anwendung bzw. die bereitgestellten Internetseiten müssen von folgenden Browsern vollständig und korrekt dargestellt werden:

- Chrome, Firefox, Edge, Safari: es sind alle Versionen zu unterstützen, deren Nutzung 5% in Deutschland in Bezug auf den jeweiligen Browser überschreitet

Die Anwendung bzw. die Internetseiten sind vom AN fortlaufend mit den zu unterstützenden Browsern zu testen.

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 muss die Unterstützung der in der aktualisierten Liste genannten Browser binnen vier Wochen sicherstellen, sofern die neu hinzugekommenen Browser vergleichbar kompatibel mit der aktuellen HTML Spezifikation des W3C sind.