

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
Plattform-Konformität	3
Remote-Management von Serverkomponenten	3
Vorgaben für Installationsverfahren	4
Vorgaben zu Backup & Recovery	4
Vorgaben zur Netzwerkkommunikation	4
Vorgaben zur Virtualisierbarkeit	4
Vorgaben zu Clients	5
Allgemeine Vorgaben für Clients	5
Vorgaben zum Datenschutz	5
Keine Datenübermittlung an Dritte	5
Vorgaben zur Ergonomie	5
Barrierefreiheit für interne Anwendungen	5
Vorgaben zur IT-Sicherheit	5
Authentifizierungsverfahren mit geheimem Wissen als Faktor	5
Benutzerrechte für den Betrieb von Anwendungen	6
Eindeutige Authentifizierung	6
Freiheit von Schadsoftware	6
Identity und Access Management	6
Logging	7
Nutzung von Cookies in Webanwendungen	7
Patch- und Release-Management (allgemeine Vorgaben)	7
Patch Management Prozess bei Betrieb in der TK	8
Speicherung von Passwörtern	8
Transport Layer Security (TLS)	8
Transportverschlüsselung nicht-öffentlicher Daten	8
Überprüfung von Eingaben	8
Wahl von Verschlüsselungsverfahren und Cipher-Suites	8
Sicherheitsrelevante Zufallswerte	8
Zugriff auf das Active Directory per LDAP	9
Vorgaben zu Webclients	9
Lauffähigkeit auf aktuellen Browsern	9
Vorgaben für Webclients (allgemein)	9

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

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.

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 (z. B. Scriptmethoden zum Wegschreiben von wichtigen Anwendungsdaten).

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.

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 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 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 IT-Sicherheit

Authentifizierungsverfahren mit geheimem Wissen als Faktor

Sofern die Anwendung eine eigene Authentifizierungskomponente implementiert und bei der Authentifizierung geheimes Wissen als Faktor verwendet, gelten nachfolgende Anforderungen.

- Die Authentifizierungskomponente begrenzt die Anzahl von Fehlversuchen. Dies kann z.B. dadurch erreicht werden, dass ein Konto nach 10 Fehlversuchen gesperrt und nach 15 Minuten automatisch wieder entsperrt wird.
- Die Authentifizierungskomponente verhindert die Auswahl von trivialen Geheimnissen durch Anwendende. Dies kann z.B. durch Erzeugung des Geheimnisses mittels eines technischen Prozesses erreicht werden.
- Sofern die Authentifizierungskomponente nicht anfällig ist für offline Angriffe (z.B. Smart Cards) und das Geheimnis durch einen technischen Prozess zufällig erzeugt wird, beträgt die Entropie des Geheimnisses mindestens $\log_2(10^6)$. Dies kann z.B. mittels einer 6-stelligen numerischen PIN erreicht werden.
- Sofern die Authentifizierungskomponente nicht anfällig ist für offline Angriffe (z.B. Smart Cards) und das Geheimnis durch Anwendende selbst wählbar ist, so wird erzwungen, dass es mindestens 8-stellig ist und aus Buchstaben und mindestens

einer weiteren Zeichenklasse (Sonderzeichen oder Ziffern) besteht. Dies kann z.B. durch eine alphanumerische PIN erreicht werden.

- Sofern die Authentifizierungskomponente anfällig ist für offline Angriffe, so ist das Geheimnis mindestens 12-stellig. Sofern eine Maximallänge definiert ist, so beträgt diese mindestens 64 Stellen. Führende und abschließende Leerzeichen werden bei der Eingabe verhindert. Dies dient der Vermeidung von Eingabefehlern. Leerzeichen innerhalb des Geheimnisses dürfen erlaubt sein. Alle Zeichen der Klassen Großbuchstabe, Kleinbuchstabe, Ziffer und druckbare Sonderzeichen sind durch Anwendende verwendbar. Die Verwendung von mindestens zwei der angegebenen Klassen wird erzwungen. Bei reduziertem Zeichensatz wird die Mindestlänge des Geheimnisses so erhöht, dass die Anzahl der Möglichkeiten äquivalent ist. Die Ausführung von offline Angriffen auf Geheimnisse wird mittels geeigneter Verfahren (bspw. Verwendung von Passworthashingverfahren wie PBKDF2 oder Argon2) wirksam erschwert.
- Sofern aus dem Geheimnis direkt kryptographisches Material abgeleitet wird, so beträgt seine Entropie mindestens 2^{100} .
- Bei einem Passwortwechsel wird das aktuelle Passwort abgefragt. Es ist nicht als neues Passwort wählbar.

Benutzerrechte für den Betrieb von Anwendungen

Die Anwendung wird nur mit den betrieblich notwendigen Rechten betrieben. Dies bedeutet u.a.:

- Die Anwendung wird ohne administrative Rechte im Active Directory betrieben. (Keine Verwendung des Domänenadministrators oder Enterpriseadministrators, keine Mitgliedschaft in den entsprechenden Domain-Gruppen)
- Die Anwendung wird ohne administrative Rechte auf dem jeweiligen Endgerät betrieben. (Keine Verwendung von root, Administrator oder SYSTEM, keine Mitgliedschaft in den entsprechenden lokalen Gruppen)

Eindeutige Authentifizierung

Die Anwendung besitzt Verfahren für die eindeutige Authentifizierung von Anwendenden. Bei Anwendungen, die sich an TK-Mitarbeitende richten, entsprechen die Benutzernamen dem bei der TK verwendeten Schema. Das Schema wird dem Auftragnehmer durch die TK auf Anforderung bereitgestellt.

Freiheit von Schadsoftware

Alle Bestandteile des Angebots sind frei von Schadsoftware (Viren, Würmer, Backdoors usw.). Der AN stellt dies durch geeignete Maßnahmen sicher. Der AN prüft insbesondere sämtliche ausgelieferte Software vor Auslieferung mittels marktgängiger und aktueller Scanner oder mindestens gleichwertiger Technologie.

Identity und Access Management

Die Anwendung ist in ein Single Sign On bei der TK integrierbar. Es wird das Microsoft Active Directory oder Entra ID bei der Anmeldung unterstützt.

Zur Authentifizierung wird mindestens eines der folgenden Protokolle unterstützt:

- OpenID/OAuth2 über Microsoft Entra ID Enterprise Application (siehe <https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/what-is-application-management>)
- SAML über Microsoft Entra ID Enterprise Application (siehe <https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/what-is-application-management>)
- Kerberos über Microsoft Active Directory. Dies ist jedoch NICHT zulässig für Anwendungen, die über eine HTTP-Schnittstelle angesprochen werden. In diesem

Fall unterstützt die Anwendung mindestens eines der beiden anderen genannten Protokolle.

Die Anwendung verfügt über ein für den Anwendungszweck geeignetes Rollen- und Rechte-Management. Dieses stellt insbesondere sicher, dass:

- Die Rechte für administrative Tätigkeiten von den Rechten zur regulären Nutzung getrennt sind.
- Auf von der Anwendung verarbeitete Daten nur von denjenigen Mitarbeitern zugegriffen werden kann, die den Zugriff für die Erfüllung ihrer Aufgaben benötigen.

Logging

Zugriffe auf sensible oder sozialversicherungsrechtliche Daten sowie administrative Zugriffe und das Starten von Batch-Prozessen werden mittels Logging protokolliert.

Für das Logging wird die Logging-Facility des Betriebssystems verwendet (Linux Syslog, Windows Eventlog) oder die Logeinträge werden in Dateien oder Datenbanken gespeichert.

Logeinträge sind maschinell auswertbar. Über Format und Inhalt der Logeinträge wird ab Leistungsbeginn eine vollständige und verständliche Dokumentation geliefert.

Sämtliche Logeinträge enthalten einen Zeitstempel. Der Zeitstempel beruht auf der Betriebssystemzeit oder es wird anderweitig sichergestellt, dass die Abweichung zu einer offiziellen Zeitquelle (z. B. einem NTP-Server) weniger als 3 Sekunden beträgt.

Sofern die Logeinträge nicht in von Menschen lesbarer und verständlicher Form für Revisionszwecke vorliegen, werden entsprechende Aufbereitungsprogramme zur Verfügung gestellt.

Logdaten sind vor unberechtigten Schreib- und Lesezugriffen geschützt.

Eine Anbindung an ein SIEM-System (Security Information and Event Management) ist möglich.

Nutzung von Cookies in Webanwendungen

Cookies, welche für serverseitiges Tracking von Loginsessions verwendet werden, erfüllen folgende Anforderungen

- Das Attribut "Expires" ist nicht gesetzt.
- Die Attribute "Secure" und "HttpOnly" sind beide gesetzt.
- Das Cookie wird bei jedem Authentisierungsvorgang neu gesetzt.
- Das Cookie wird bei Logout serverseitig invalidiert.

Patch- und Release-Management (allgemeine Vorgaben)

Die Anwendung wird regelmäßig weiterentwickelt und an neue Anforderungen angepasst. Sicherheitsrelevante Patches auf Plattform- und Datenbankebene werden spätestens 2 Wochen nach deren genereller Verfügbarkeit unterstützt. Service Packs und neue Maintenance Level auf Plattform- und Datenbankebene werden spätestens 3 Monate nach der generellen Verfügbarkeit unterstützt. Neue Releases auf Plattform- und Datenbankebene werden spätestens 12 Monate nach deren genereller Verfügbarkeit unterstützt.

Sofern Anwendungskomponenten auf Windows-Clientsystemen vorgesehen sind, unterstützen diese neue Windows-Funktionsupdates innerhalb von 6 Monaten nach genereller Verfügbarkeit.

Der AN informiert die TK selbstständig und ohne Aufforderung über neue Releasestände und Patches, idealerweise per E-Mail.

Patch Management Prozess bei Betrieb in der TK

Bei Bekanntwerden von Schwachstellen in von der Anwendung verwendeten Bibliotheken und Komponenten stellt der AN sicher, dass je nach Risiko für die Anwendung (bewertet durch den AN) die jeweilige Bibliothek/Komponente innerhalb von 1-18 Arbeitstagen aktualisiert wird. Sicherheitsrelevante Updates, Patches und/oder Anleitungen werden der TK unverzüglich zur Verfügung gestellt.

Sofern das Patchmanagement durch den AN durchgeführt wird, installiert der AN sicherheitsrelevante Patches spätestens 2 Wochen nach allgemeiner Verfügbarkeit. Ebenso ist dann der Betrieb aller für das Patchmanagement notwendigen Komponenten (Hardware, Lizenzen) durch den Auftragnehmer zu leisten.

Der AN stellt der TK auf Anfrage nach einer konkreten Bibliothek oder Komponente innerhalb von 2 Arbeitstagen Informationen bereit, ob und in welcher Version diese in der gelieferten Anwendung verwendet wird.

Speicherung von Passwörtern

Sofern die Anwendung eine Authentifizierungskomponente enthält, die auf Passwörtern basiert, werden die Passwörter niemals im Klartext gespeichert. Gespeicherte Passwörter sind mittels Passworthashingverfahren wie PBKDF2 oder Argon2 oder vergleichbar sicheren Verfahren geschützt.

Transport Layer Security (TLS)

Der AN hält sich bei der Wahl von TLS-Version(en) und der eingesetzten Cipher-Suites an die Empfehlungen der jeweils aktuellen Fassung der Technischen Richtlinie BSI TR-02102-2 *"Kryptographische Verfahren: Verwendung von Transport Layer Security (TLS)"* des BSI. Der Auftragnehmer stellt sicher, dass alle Kommunikationsteilnehmer mindestens eine der zulässigen Cipher-Suites unterstützen. Der AN gleicht die von ihm gewählte Konfiguration mindestens jährlich gegen die Vorgaben des BSI ab. Bei Abweichungen passt der AN die Konfiguration an, um Konformität mit der o.a. Richtlinie herzustellen.

Transportverschlüsselung nicht-öffentlicher Daten

Nicht-öffentliche Daten werden immer verschlüsselt übertragen.

Überprüfung von Eingaben

Die Anwendung bzw. die vom AN für die TK bereitgestellten Dienste prüfen alle Eingaben vor der Verarbeitung, um bspw. Buffer-Overflows und Injection-Angriffe auszuschließen.

Wahl von Verschlüsselungsverfahren und Cipher-Suites

Sofern in der Software Verschlüsselungsalgorithmen eingesetzt werden, sind diese zur aktuellen Fassung "BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen" konform. Sofern Verschlüsselungsalgorithmen im direkten Umfeld von qualifizierten elektronischen Signaturen nach dem bundesdeutschen Signaturgesetz eingesetzt werden, richten sie sich nach den Veröffentlichungen der Bundesnetzagentur im Bundesanzeiger. Verschlüsselungsverfahren werden vor Ablauf des laut der o.a. genannten Vorschriften zulässigen Verwendungsdatums durch aktuelle Verfahren ersetzt werden.

Sicherheitsrelevante Zufallswerte

Sollen sicherheitsrelevante Zufallswerte (z.B. Session-IDs, kryptographisches Material, Initial-PINs) in einer Anwendung verwendet werden, so müssen diese hinreichend zufällig sein. Die dafür verwendeten Zufallsgeneratoren müssen den Vorgaben aus Kapitel "Zufallszahlengeneratoren" der aktuellen Technischen Richtlinie BSI TR-02102-1 des BSI entsprechen.

Zugriff auf das Active Directory per LDAP

Zugriffe auf das Active Directory per LDAP erfolgen weder anonym noch mit Gast-Identität.

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.