Inhalt

Anlage V3

Vorgaben aus der IT Sicht

Allgemeine Vorgaben zu Anwendungen

Integrationsfähigkeit in Portale und Workflows

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 offen legen. 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 akuellen 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 verfügend 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.

Plattform-Konformität

Die Anwendung muss als Software as a Service,

Vorgaben zu Backup & Recovery

Die Anwendung muss die Fähigkeit zu Backup & Recovery besitzen.

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 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)
- manueller Austausch über Cryptshare (https://webft.tk.de)

Anlage V3

Vorgaben aus der IT Sicht

- Austausch über fest definierte S-FTP bzw. FTP-S Server bei externen Partnern.

Für Datentransfers von und zur TK müssen die unterstützten Verfahren genutzt werden.

Im Falle von Austauschverfahren für den Datenaustausch soll als Transportverschlüsselung eines der Protokolle S-FTP oder FTP-S zum Einsatz kommen.

Das gewählte Verfahren ist zwischen TK und AN zu vereinbaren und vom AN zu beschreiben.

Der Austausch von Daten zwischen dem AN und der TK muss über sichere Protokolle (z.B. S-FTP oder gleichwertig) erfolgen, sofern es sich um personenbeziehbare und/oder sensible Daten handelt.

Soweit technisch machbar und wirtschaftlich umsetzbar, sind die Verfahren des Datenaustausches im Gesundheits- und Sozialwesen über Datenannahmestellen (siehe http://www.gkv-datenaustausch.de) zu verwenden.

Für den sicheren Ad-hoc-Datenaustausch muss die durch die TK bereitgestellte Plattform cryptshare genutzt werden.

Alternativ kann die Übertragung von sensiblen Daten auch per S/MIME-verschlüsselter Mail oder über einen sicheren und mit der TK abgestimmten Dienst erfolgen.

Bei Verwendung von S-FTP bzw. FTP-S muss der Auftragnehmer den entsprechenden Server bereitstellen und betreiben.

Wenn ein Datenaustausch regelmäßig vorgesehen ist und eine automatisierte Verarbeitung erfolgen soll, sollen zur Integritäts- und Vollständigkeitskontrolle geeignete Verfahren vom AN unterstützt und eingerichtet werden.

Vorgaben zum Datenschutz

Hosting - Auswertung gesammelter Daten nur mit TK-Auftrag

Der Anbieter darf keine im Rahmen des Hostings gesammelten Daten an Dritte weitergeben oder diese ohne Auftrag auswerten.

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 zur IT-Sicherheit

Benutzerrechte für den Betrieb von Anwendungen

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

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

Eindeutige Authentifizierung

Die Anwendung muss Verfahren für die eindeutige Authentifizierung von Anwendenden besitzen.

Freiheit von Schadsoftware

Alle Bestandteile des Angebots müssen frei von Schadsoftware (Viren, Würmer, Backdoors usw.) sein. Der AN muss dies durch geeignete Maßnahmen sicherstellen. Der AN muss insbesondere sämtliche ausgelieferte Software vor Auslieferung mittels eines marktgängigen und aktuellen Scanners oder mindestens gleichwertiger Technologie prüfen.

Hosting - Administrationsrechte und Funktionstrennung

Der AN muss für alle für die TK bereitgestellten IT-Komponenten (Server, Dienste und Anwendungen) sicherstellen, dass seine Mitarbeiter - insbesondere Systemadministratoren - nur die für die jeweilige Aufgabenerfüllung notwendigen Rechte besitzen. Der AN muss für kritische administrative Prozesse das Vier-Augen-Prinzip umsetzen.

Hosting - Sicherheitsmaßnahmen

Der AN muss alle zumutbaren und geeigneten technischen und organisatorischen Maßnahmen ergreifen, die einen unbefugten und missbräuchlichen Zugriff auf die Anwendungen und/oder Internetseiten, zugehörige Komponenten sowie zugehörige Daten unterbinden. Dies gilt insbesondere für die Abwehr von Bedrohungen, die die Integrität, die Verfügbarkeit und die Vertraulichkeit der Anwendung bzw. des Internetauftritts gefährden oder eine Gefährdung (z.B. durch Exploits, Malicious Software) Dritter (z.B. Besucher eines Internetauftritts) darstellen. Die getroffenen Maßnahmen müssen dabei dem jeweils aktuell gültigen Stand der Technik entsprechen. Ferner müssen bei der Erstellung und Pflege sowie beim Hosting generell Techniken vermieden werden, die bekanntermaßen hohe Sicherheitsrisiken bzw. Sicherheitslücken enthalten, welche nicht durch entsprechende flankierende Maßnahmen geschlossen werden können.

Sollten sich aufgrund neuer Erkenntnisse und Bedrohungen Lücken ergeben, so muss der AN diese unverzüglich der TK anzeigen und sie durch geeignete Maßnahmen beseitigen. Der AN muss die zugehörigen Sicherheitskonzepte fortschreiben und der TK zur Prüfung zur Verfügung stellen. Sofern die Maßnahmen die Verfügbarkeit der für die TK zur Verfügung gestellten Dienste beeinflussen, muss der AN diese mit der TK abstimmen.

Hosting nur mit Sicherheitskonzepten

Der AN muss alle von ihm ergriffenen Sicherheitsmaßnahmen in zugehörigen Sicherheitskonzepten dokumentieren. Vor der Produktivsetzung sowie bei wesentlichen Änderungen muss der AN der TK die Sicherheitskonzepte zur Prüfung zur Verfügung stellen. Die Konzepte müssen mindestens folgende Punkte adressieren:

- Schutz vor Malware

Anlage V3

Vorgaben aus der IT Sicht

- Systemhärtung
- Patch-Management-Prozess
- Verschlüsselung bei Datenübertragungen
- Löschverfahren
- Umgang mit Zugangsdaten und anderen sensiblen Informationen
- Rechtekonzept für Administratoren

Identity und Access Management

Es muss das Microsoft Active Directory oder AzureAD bei der Anmeldung unterstützt werden.

Die Anwendung muss in ein Single Sign On bei der TK integriert werden können.

Zur Authentifizierung soll mindestens eines der folgenden Protokolle unterstützt werden:

- Kerberos
- SAML über Azure AD Enterprise Application (siehe https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/what-is-application-management)
- OAuth2 über Azure AD Enterprise Application (siehe https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/what-is-application-management)

Die Anwendung muss über ein für den Anwendungszweck geeignetes Rollen- und Rechte-Management verfügen, welches sicherstellt, dass auf personenbezogene Daten nur von denjenigen Mitarbeitern zugegriffen werden kann, die den Zugriff für die Erfüllung ihrer Aufgaben benötigen.

Die Rollen des Berechtigungssystems sollen sich aus Mitgliedschaften in AD- bzw. Azure-AD Gruppen ableiten lassen.

Logging

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

Logeinträge müssen maschinell auswertbar sein. Über das Format der Logeinträge muss ab Leistungsbeginn eine vollständige und verständliche Dokumentation geliefert werden.

Sämtliche Logeinträge müssen einen Zeitstempel enthalten. Der Zeitstempel muss auf der Betriebssystemzeit beruhen oder es muss anderweitig sichergestellt werden, 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, müssen entsprechende Aufbereitungsprogramme zur Verfügung gestellt werden.

Logdaten müssen vor unberechtigten Zugriffen geschützt sein.

Meldung von Sicherheitsvorfällen

Der AN muss Sicherheitsvorfälle, die direkt oder indirekt den vom AN für die TK bereitgestellten Dienst betreffen, unverzüglich der TK melden. Die Meldung muss an den jeweils verantwortlichen Ansprechpartner sowie an eine von der TK nach Zuschlag zur Verfügung gestellte E-Mailadresse erfolgen. Reaktionen auf diese Vorfälle müssen gemeinsam abgestimmt werden.

Nutzung von Cookies in Webanwendungen

Attribute und Präfixe müssen entsprechend der Kritikalität der Daten, welche in dem jeweiligen Cookie verarbeitet werden, angemessen gesetzt sein. Die Lifetime von Cookies muss -dem Anwendungszweck entsprechend- möglichst kurz sein. Cookies sollen nicht für die Speicherung von Daten verwendet werden, welche nur auf Clientseite verarbeitet werden.

Stattdessen sollen -sofern im Client verfügbar- die dafür vorgesehenen APIs (z.B. Web Storage API) verwendet werden.

Für Cookies, welche für serverseitiges Tracking von Loginsessions verwendet werden, gelten folgende detaillierte Anforderungen:

- Das Attribut "Expires" darf nicht gesetzt sein.
- Die Attribute "Secure" und "HttpOnly" müssen gesetzt sein.
- Das Attribut "SameSite" soll auf den Wert "Strict" gesetzt sein.
- Das Attribut "Domain" soll nicht gesetzt sein.
- Das Präfix des Cookies soll "__Host-" sein.
- Das Cookie muss bei jedem Authentisierungsvorgang neu gesetzt werden.
- Das Cookie muss bei Logout serverseitig invalidiert werden.

Patch- und Release-Management (allgemeine Vorgaben)

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

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

Die TK muss vom AN selbstständig und ohne Aufforderung über neue Releasestände und Patches informiert werden, idealerweise per E-Mail.

Patch Management Prozess bei gehosteten Anwendungen

Der AN muss über einen Patch-Management-Prozess gewährleisten, dass alle von ihm eingesetzten Systeme, Systemkomponenten und Entwicklungswerkzeuge jeweils auf einem aktuellen Versionsstand und insbesondere frei von Schwachstellen sind. Der AN muss sicherstellen, dass je nach Risiko für die Anwendung (bewertet durch den AN) Sicherheitspatches - innerhalb von 1-18 Arbeitstagen nach Veröffentlichung des Patches eingespielt sind. Darüber hinaus muss der AN für eine angemessene Härtung der Systeme sorgen.

Prüfrechte der TK

Die TK ist berechtigt, sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim AN getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Darüber hinaus hat die TK das Recht, die Sicherheit der beteiligten Systeme und Prozesse im Rahmen von Assessments zu überprüfen. Insbesondere stimmt der AN zu, dass die TK bzw. ein von Ihr beauftragter Prüfer nach Vorankündigung eigene Penetrationstests durchführen darf.

Speicherung von Kennwörtern

Eine Speicherung von Kennwörtern im Klartext darf nicht erfolgen. Kennwörter müssen mittels Kennworthashingalgorithmen wie PBKDF2 oder Argon2 oder vergleichbar sicheren Verfahren geschützt werden.

Transport Layer Security (TLS)

Der AN muss sich bei der Wahl von TLS-Version(en) und der einzusetzenden Cipher-Suites an die Empfehlungen der jeweils aktuellen Fassung der Technischen Richtlinie "Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 2 – Verwendung von Transport Layer Security (TLS))" des BSI halten. Dabei ist sicher zu stellen, dass alle Kommunikationsteilnehmer mindestens eine der angebotenen Cipher-Suites unterstützen.

Anlage V3

Vorgaben aus der IT Sicht

Der AN muss die von ihm gewählte Konfiguration mindestens jährlich gegen die Vorgaben des BSI abgleichen und bei Bedarf anpassen.

Transportverschlüsselung nicht-öffentlicher Daten

Nicht-öffentliche Daten müssen verschlüsselt übertragen werden. Hierfür soll TLS (Transport Layer Security) verwendet werden.

Transportverschlüsselung von Zugangsdaten

Werden Zugangsdaten zur Authentifizierung verwendet, so müssen diese verschlüsselt übertragen werden.

Überprüfung von Eingaben

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

Vorgaben zur Datenlöschung

Bei der Außerbetriebnahme einer Appliance, bei Austausch von Hardware-Komponenten sowie bei der Beendigung eines Vertrages und vor der Wiederverwendung von Speichermedien durch andere Kunden des AN, müssen alle permanent speichernden Datenträger sicher vernichtet oder sicher gelöscht werden. Eine Weitergabe oder Rückgabe an Dritte, ausgenommen zur professionellen Löschung bzw. Vernichtung, darf nicht stattfinden. Der AN muss über die erfolgte Vernichtung/Löschung ein Protokoll anfertigen, aus dem hervorgeht, wann und mittels welchen Verfahrens die Datenträger vernichtet/gelöscht wurden. Der AN muss der TK das Protokoll zur Verfügung stellen.

Für Datenträger mit folgenden Kriterien muss eine Vernichtung erfolgen. Löschen ist unzulässig:

- Nicht-öffentliche Daten oder Daten mit unbekannter Klassifizierung sind unverschlüsselt/schwach verschlüsselt auf Datenträger gespeichert
- Datenträger ist defekt
- Daten der VSK "C4 – Streng geheim" sind auf Datenträger gespeichert
- USB-Sticks, Speicherkarten

Eine Vernichtung muss gemäß folgender Vorgaben oder gleich-/höherwertiger Verfahren erfolgen:

- Festplatten (HDD): DIN 66399-2, mindestens Stufe H-3
- Solid State Disks (SSD): DIN 66399-2, mindestens Stufe E-3
- Für die Vernichtung von Hybridfestplatten (SSHD), USB-Sticks und Speicherkarten gelten dieselben Anforderungen wie bei Solid State Disks

Bei allen funktionsfähigen, verschlüsselten magnetischen Datenträgern kann eine elektronische sichere Löschung durchgeführt werden. Dabei muss die Löschung auf dem gesamten Datenträger nach einem der nachfolgenden Löschverfahren erfolgen:

1. Löschfunktion des Laufwerks (ATA "Secure Erase")
2. DoD 5220.22-M (E) bzw. gleich-/höherwertig
3. Löschfunktion des Laufwerks (ATA "Secure Erase")

Anlage V3

Vorgaben aus der IT Sicht

Bei allen funktionsfähigen, verschlüsselten halbleiterbasierten Datenträgern kann eine elektronische sichere Löschung durchgeführt werden. Dabei muss die Löschung auf dem gesamten Datenträger nach einem der nachfolgenden Löschverfahren erfolgen:

- Verfahren 1:
  - Löschfunktion des Mediums (ATA-"Secure-Erase")
  - Überschreiben des gesamten Speichers
  - Löschfunktion des Mediums (ATA-"Secure-Erase")
- oder Verfahren 2:
  - Löschen des Schlüssels für die Festplattenverschlüsselung im TPM-Chip
  - Überschreiben des gesamten Speichers
  - Löschen des Schlüssels für die Festplattenverschlüsselung im TPM-Chip

Wahl von Verschlüsselungsverfahren und Cipher-Suites

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

Zufallszahlen

Sollen Zufallszahlen in einer Anwendung verwendet werden, so müssen diese – dem Anwendungszweck entsprechend – hinreichend zufällig sein. Als Informationsquelle für zulässige Zufallszahlengeneratoren kann das Kapitel 9 "Zufallszahlengeneratoren" der aktuellen Technischen Richtlinie TR-02102-120 des BSI dienen.

Vorgaben zur Verfügbarkeit

Basisanforderungen zur Verfügbarkeit

Der AN legt die von ihm bereitgestellten Dienste und Anwendungen hochverfügbar aus. Die geschuldete Verfügbarkeit in der definierten Betriebszeit ergibt sich aus Nr. 9.4 a. des Vertrags sowie Ziffer 8.3 der EVB-IT Cloud-AGB. >

Sofern das Internet verwendet wird, stellt der AN eine leistungsfähige und redundante Anbindung an den Internet-Backbone sicher.

Bei geplanten Änderungen an Systemen und Anwendungen, die zu einer Abweichung von den vereinbarten Betriebszeiten führen oder führen können, muss der AN die TK mit einem Vorlauf von einer Woche informieren. Dies kann schriftlich oder per E-Mail an den vereinbarten Ansprechpartner der TK erfolgen.

Der AN richtet seine Backup- und Recovery-Verfahren so ein, dass nach einer Störung der Dienst innerhalb von 7 Tagen wieder zur Verfügung steht. In jedem Fall darf nach einem Wiederanlauf nur ein Datenverlust des Transaktionsvolumens von maximal24 Stunden auftreten.

Der AN muss das Operating der TK nach Feststellung eines Fehlers und bei Beeinträchtigung des Dienstes unverzüglich per Telefon oder E-Mail informieren. Er gibt dabei die Art der Störung und die voraussichtliche Zeitdauer der Beeinträchtigung bzw. des Ausfalls an. Nach Beseitigung der Störung gibt der AN eine Entwarnung per Telefon oder E-Mail an das Operating der TK.

Vorgaben aus der IT Sicht

Die maximale Ausfallzeit - auch bei Hardware-Defekten - beträgt 7 Tage.

Erweiterte Anforderungen an die Verfügbarkeit

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 Fax oder Brief 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.

Vorgaben für Webclients (allgemein)

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

- Andere clientseitige Scriptsprachen als JavaScript sind in keinem Fall zu verwenden.
- Framesets dürfen nicht eingesetzt werden.
- 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 müssen entsprechend der aktuellen W3C-Konvention syntaktisch richtig sein.
- Flash-Animationen und andere Plugins dürfen nicht eingesetzt werden.

Die Anwendung muss die Kommunikation mit einem WEB-Proxy grundsätzlich unterstützen. Darüber hinaus entsprechen die verwendeten Technologien und Protokolle den üblichen Internetstandards gemäß Request for Comments (RFC).