



Bundesverwaltungsamt

# Leistungsbeschreibung – Allgemeiner Teil

IT-Leistungen zur Unterstützung von Fachaufgaben und Fachverfahren des Bundesverwaltungsamtes

ZIB 21.25 - 0171/24/VV : 1-2

ZIB 21.15 - 0171/24/VV : 3-5

Der zentrale Dienstleister des Bundes

[bundesverwaltungsamt.de](https://bundesverwaltungsamt.de)

## Inhaltsverzeichnis

1.	Einleitung	4
2.	Umfeld und inhaltliche Rahmenbedingungen	5
3.	Übersicht der ausgeschriebenen Lose	7
3.1	Los 1: Beratung Gesamt-Architektur und Entwicklung Softwarestandards	7
3.2	Los 2: Beratung Projekt-, Qualitäts- und Anforderungsmanagement	8
3.3	Los 3 bis 5: Entwicklung und Pflege Fachverfahren	9
3.4	Abgrenzung einzelner Themen/Schnittstellen zwischen den Losen	11
4.	Allgemeine Regelungen	15
4.1	Rahmenbedingungen für Beauftragungen	15
4.2	Arbeitsort, Erfüllungsort	15
4.3	Projektleitung	16
4.4	Vorgehensmodell	17
4.5	Projekthandbuch	18
4.6	Zusammenarbeit	18
4.7	DevOps	19
4.8	Buildmanagement	19
4.9	Technische Anbindung	21
4.10	Informationstechnik der Auftragnehmerin	21
4.11	Sicherheitsvorgaben der BT	22
4.12	Verträge zur Auftragsverarbeitung	22
5.	Softwareprodukte, Frameworks und Bibliotheken	24
6.	Qualitätsmanagement	25
7.	Qualitätssicherung und Testmanagement	27
7.1	Vorgaben für fachlichen Test	27
7.2.	Vorgaben für technischen Test	29
8.	Standards	31

**Hinweis zur geschlechterneutralen Formulierung:**

Aus Gründen der einfacheren Lesbarkeit wird u. U. auf eine geschlechtsspezifische (z. B. Benutzerinnen) bzw. geschlechtsneutrale Differenzierung (z. B. Benutzende) verzichtet. Sämtliche Bezeichnungen gelten dann im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter.

## 1. Einleitung

Das vorliegende Dokument definiert losübergreifende Rahmenbedingungen und Anforderungen an die zu erbringenden Leistungen. Es dient somit in Ergänzung der Regelungen der losspezifischen Rahmenvereinbarungen und Leistungsbeschreibungen sowohl der Erstellung vergleichbarer Angebote als auch der Definition der Rahmenbedingungen und als Vorgabe für die zu erbringenden Leistungen. Bei eventuellen inhaltlichen Abweichungen haben die Aussagen in den losspezifischen Dokumenten (Rahmenvereinbarung bzw. Leistungsbeschreibung) jeweils Vorrang.

Sowohl in diesem Dokument als auch in den losspezifischen Leistungsbeschreibungen werden die Bieter in der Regel als Auftragnehmerin (AN) und die Behörde Bundesverwaltungsamt (BVA) als Bedarfsträgerin (BT) angesprochen. Mit dem Begriff „externer (IT-)Dienstleister“ können auch solche gemeint sein, die nicht unter die Lose 1 bis 5 fallen.

Vorangestellt ist eine kurze Darstellung des Umfelds und der inhaltlichen Rahmenbedingungen, aus denen Anforderungen an BT und AN für die Leistungserbringung resultieren. Es folgt eine kurze Übersicht über die ausgeschriebenen Lose und das Zusammenwirken der verschiedenen AN der Lose sowie grobe Abgrenzungen der Losinhalte.

Im Anschluss folgen die losübergreifend gültigen Leistungsmerkmale und Vorgaben, die zwingend angeboten und eingehalten werden müssen.

## 2. Umfeld und inhaltliche Rahmenbedingungen

Das BVA als zentraler Dienstleister des Bundes nimmt über 150 Fachaufgaben wahr. Die fachliche Aufgabenerledigung macht IT-Einsatz für diese Aufgaben in unterschiedlichsten Formen und Umfängen unverzichtbar. Dieser Bedarf kann sich sowohl auf relativ einfache oder kleine Lösungen als auch auf komplexe Verfahren beziehen.

Die Softwareentwicklung des BVA spielt sich stets im Spannungsfeld zwischen innovativen Technologien und der Wartung von Bestandssystemen ab. Inhaltlich handelt es sich dabei sowohl um Geschäftsanwendungen aus verschiedenen Umfeldern der Fachverfahren des BVA (Banking, Verwaltung, Sozialfonds u. a.) als auch um Registeranwendungen, die mehrheitlich im Umfeld der Öffentlichen Sicherheit eingesetzt werden (Ausländer- und Asylrecht, Waffenrecht etc.). Ein wichtiger Aspekt, der weiter an Bedeutung gewinnt, ist dabei die Vernetzung der Systeme von verschiedenen Behörden des Bundes, Systemen der Europäischen Union und aus der Privatwirtschaft. Die unterschiedlichen Softwaresysteme wurden und werden weitgehend durch unterschiedliche externe Dienstleister entwickelt bzw. weiterentwickelt und gepflegt.

Mit dem Aufgabenportfolio des BVA wächst auch die Softwarelandschaft des BVA. Zusätzlich angefeuert wird dieses Wachstum durch Großprojekte aus dem Bereich der Öffentlichen Sicherheit (u. a. Fluggastdatenspeicherung, Smart Borders) und die Digitalisierung (u. a. Beihilfe, Registermodernisierung). Bedingt durch dieses Wachstum steigt die Anzahl der vorhandenen IT-Anwendungen, der Mitarbeiterinnen und Mitarbeiter der BVA-IT und der beteiligten Dienstleister rapide an. Das BVA unternimmt darum erhebliche Anstrengungen zur ständigen technischen und organisatorischen Konsolidierung der IT.

In technischer Hinsicht verfolgt das BVA eine Strategie der Standardisierung und des Architekturmanagements, um die Anwendungslandschaft trotz ihrer fachlichen Vielfalt und ihrer historisch gewachsenen Heterogenität dauerhaft wirtschaftlich warten und weiterentwickeln zu können. Zu diesem Zweck wurden im BVA die Konstruktions- und Betriebsstandards Register Factory und IsyFact zur einheitlichen Entwicklung von Software und Wiederverwendung von Softwarekomponenten geschaffen. Diese definieren Standards an Technologien, Dokumentation, Softwarebausteinen und Vorgehensweisen, die im BVA Anwendung finden und durch die Projekte weiterentwickelt werden. Heute ist der überwiegende Teil der selbstentwickelten Software des BVA konform zum Technologiestack der Register Factory bzw. IsyFact. Ergänzend zu den Standards für die Individualentwicklung wurde die Digi Factory aufgebaut, um als Rahmenwerk und Baukasten für die standardisierte Digitalisierung zu dienen. Des Weiteren befindet sich die DevOps Factory im Aufbau, die analog zu den Entwicklungsstandards Bausteine, Blaupausen, Methoden, Plattformen und Werkzeuge bereitstellen soll, um die DevOps Plattform und die Umsetzung von DevOps im BVA zu standardisieren.

Aus einem organisatorischen Blickwinkel begegnet das BVA der wachsenden Anzahl von Anwendungen, Projekten und beauftragten Dienstleistenden mit Maßnahmen des Multiprojektmanagements und der Standardisierung von Projektmanagementmethoden. Die hohe Volatilität der Projektanforderungen im politischen Umfeld bedingt aber auch erhebliche Investitionen in den Aufbau von Kapazitäten im Bereich des agilen Projektmanagements.

Der Produktivbetrieb der Anwendung erfolgt nicht bei der BT, sondern extern durch einen IT-Betrieb, in der Regel das Informationstechnikzentrum Bund<sup>1</sup>, im folgenden Betriebsbehörde genannt. Dies hat die AN bei allen Maßnahmen zu berücksichtigen. Die Zusammenarbeit mit der Betriebsbehörde hat in enger Abstimmung mit der BT zu erfolgen.

Priorität hat in allen Phasen der gemeinsamen Zusammenarbeit die Sicherstellung der Lauffähigkeit der bestehenden Verfahren und die termingerechte technische Umsetzung fachlicher bzw. gesetzlicher Anforderungen.

Der zu unterstützende fachliche Themenbereich (Fachorganisation bzw. Fachverfahren) ist in der jeweiligen besonderen Leistungsbeschreibung genannt.

Es ist davon auszugehen, dass die betreffenden IT-Verfahren auch weiterhin eine andauernde fachliche Weiterentwicklung aufgrund von politischen Entscheidungen und neuen gesetzlichen Regelungen erfahren werden. Außerdem findet eine kontinuierliche technische Weiterentwicklung aufgrund von Modernisierungsmaßnahmen oder notwendigen Anpassungen im Rahmen der IT-Konsolidierung Bund oder der Weiterentwicklung der Architekturstandards statt.

---

<sup>1</sup> Weitergehende Informationen siehe auf [itzbund.de](http://itzbund.de).

### **3. Übersicht der ausgeschriebenen Lose**

Zur Bewältigung der Aufgaben insgesamt werden qualifizierte IT-Leistungen externer AN benötigt. Unter Berücksichtigung vergaberechtlicher Vorgaben und der bestehenden Aufstellung der BT ist eine Aufteilung der benötigten Leistungen in fünf Lose erfolgt. Die Lose und die hierin zu erbringenden Leistungen werden im Folgenden grob skizziert. Diese Übersicht soll das Verständnis des Gesamtansatzes zur Aufgabenteilung erleichtern; sie gibt einen Überblick über die von den AN verbindlich zu beachtenden, übergeordneten Anforderungen.

#### **3.1 Los 1: Beratung Gesamt-Architektur und Entwicklung Softwarestandards**

Das zentrale Architekturmanagement der BT soll im Rahmen von Los 1 weiter ausgebaut und die übergreifende Architekturarbeit organisiert und optimiert werden. Dabei soll die ausgeschriebene Beratung alle Fachthemen der BT betrachten.

Die BT steht hinsichtlich der Architektur und des Standards- und Innovationsmanagement vor großen Herausforderungen. Die Unterstützung der BT mit Fokus auf eine zukunftsfähige Weiterentwicklung der Standardisierung, der Softwareentwicklungsstandards und der Digitalisierungsstandards erfolgt durch die AN in Los 1. Dabei sollen auch innovative Technologien aus Projekten identifiziert und in die Standards sinnvoll integriert werden.

Des Weiteren erfolgt die Weiterentwicklung der DevOps Factory und die methodische Beratung zu Build und Deployment ebenfalls durch die AN in Los 1.

Die Entwicklung/Gestaltung/Durchsetzung und kontinuierliche Pflege einer Enterprise-Architektur für das BVA ist eine übergreifende Aufgabenstellung für die BT. Die Harmonisierung der gesamten Anwendungslandschaft des BVA unter Berücksichtigung (und soweit möglich Mitgestaltung) der Rahmenbedingungen (wie Architekturmanagement des Bundes) ist eine herausfordernde Aufgabe. Es gilt außerdem die BT dabei zu unterstützen, im Hinblick auf den Einsatz von Künstlicher Intelligenz (KI) Kompetenzen aufzubauen. Diese Aufgabenstellungen für die BT bedürfen einer entsprechend qualifizierten externen Unterstützung durch die AN von Los 1.

Die AN von Los 1 hat neben der Architekturberatung auch Softwareentwicklungsleistungen im Rahmen der Weiterentwicklung und Pflege von und Neuentwicklungen für die IsyFact/Register Factory/Digi Factory zu leisten und ausnahmsweise die Rolle des Product Owners für die Standards zu erfüllen.

Darüber hinaus wird operative Unterstützung im Bereich des Build und Deployment durch die AN von Los 1 benötigt.

### **3.2 Los 2: Beratung Projekt-, Qualitäts- und Anforderungsmanagement**

Die Unterstützung der BT zur Qualitätssicherung insgesamt sowie weiterer primär den Fachbereichen in den Projekten zugeordneten Aufgaben wird durch die AN von Los 2 erfolgen. Ganz wesentlich ist dabei, die fachliche Analyse und Definition der fachlichen Anforderungen separat von den Dienstleistern für Entwicklung und Pflege (s. u.) zu unterstützen, da ansonsten Interessenskonflikte die Ergebnisse der Anforderungsanalyse beeinflussen könnten. Auch die Unterstützung im Bereich der Qualitätssicherung, die nicht vollumfänglich von der BT selbst geleistet werden kann, durch einen anderen Dienstleister als den, der die Software-Entwicklung und -Pflege umsetzt, ist sowohl unter fachlichen als auch unter wirtschaftlichen Gesichtspunkten sinnvoll. Die AN Los 2 führt die Qualitätssicherung auf Basis ihrer Kenntnisse der Anforderungen durch und lässt die Ergebnisse der Qualitätssicherung wiederum ins Anforderungsmanagement einfließen.

Für den Schwerpunkt der Leistungen ist der jeweilige Fachbereich der BT der unmittelbare Leistungsempfänger für diese Fachdomänen- bzw. Fachverfahrens- bzw. Fachprojekt-spezifischen Leistungen. Eine enge Zusammenarbeit ist aber auch mit dem IT-Bereich der BT notwendig, um die Erreichung der Zielsetzungen insgesamt sicherzustellen, z. B. durch Durchführung technischer Tests im Rahmen der Qualitätssicherung und mittels Fokus auf eine weitestgehend vollständige Testautomatisierung in Hinblick auf eine zukünftige Integration der Tests in CI/CD-Pipelines sowie die Berücksichtigung von DevOps-Konzepten. Nach Möglichkeit sollen synthetische Testdaten eingesetzt werden. Die BT wird dabei unterstützt, entsprechende Testdatengeneratoren für laufende oder künftige Verfahren zu entwickeln. So soll das Ziel erreicht werden, nur noch in Ausnahmefällen Echtdaten für Tests einzusetzen.

Die Unterstützung der Fachbereiche der BT durch die AN soll nicht eng auf die oben genannten Themen eingeschränkt werden, z. B. können auch Beratungsleistungen zum methodischen Vorgehen und Definition entsprechender Prozesse, zu den fachlichen Serviceleistungen für die Endkunden und deren Ausgestaltung, zum Projektmanagement im fachlichen Verantwortungsbereich oder auch die Durchführung von Projektmanagement-Office-Tätigkeiten beauftragt werden (z. B. Projektassistenz-Aufgaben). Dies beinhaltet auch Coachingmaßnahmen zu fachlichen Prozessen, Methoden und Werkzeugeinsatz. Zudem ist innerhalb der IT-Bereiche eine Unterstützung in den verschiedenen Aufgabenbereichen der Komponentenverantwortlichen vorgesehen (Thema: Wartung und Betrieb; bspw. durch das Betreuen der Anwendungskomponenten in der BVA-Systemlandschaft).

Grundsätzlich sind ganz unterschiedliche Fachaufgaben und Fachverfahren von der AN dieses Loses zu unterstützen – in parallelen Projekten, mit internen und externen Stakeholdern. Diese können unabhängig voneinander sein oder es können auch enge fachliche Abhängigkeiten bestehen.



Die AN von Los 2 hat als komplexe Projektmanagement-Aufgabe auch die Koordination des Zusammenspiels der verschiedenen weiteren Dienstleister unter Berücksichtigung derer ggf. divergierenden Interessen zu leisten.

### 3.3 Los 3 bis 5: Entwicklung und Pflege Fachverfahren

Die Entwicklung neuer Fachverfahren und die Realisierung notwendiger Änderungen bestehender Fachverfahren sowie alle weiteren benötigten Leistungen im Kontext der Realisierungen (z. B. 3-rd Level Support) sind Leistungsgegenstand dieser drei Lose und werden an verschiedene AN vergeben. Die Domänen und deren Aufteilung für diese Lose richten sich nach der folgenden Übersicht:

Fachdomäne/Fachverfahren (aktueller Status Quo)	Los	Schutzbedarf <sup>2</sup>
Registerportal (nur die reine Portalfunktion (=„Klammer“ um die über das Portal verfügbaren Funktionalitäten))	3	normal
Register Ausländerwesen <ul style="list-style-type: none"> <li>• Ausländerzentralregister inkl. Visadatei</li> <li>• AZR-Mitteilungen</li> <li>• AZR- Scanstelle</li> <li>• SIRENE</li> <li>• Schengener Informationssystem</li> <li>• Flüchtlingsverfahren inkl. Konsultation und/oder Information der beteiligten Behörden aus Bund/Land Kommune</li> <li>• Verfügungstextanwendung: Einfügen der ausländerrechtlichen Entscheidungsdokumente in die Historie der Sachverhalte</li> <li>• Informationssystem Urkunden</li> <li>• EMA Elektronische Anbindung der Meldebehörden</li> <li>• C730</li> </ul>	3	hoch bis sehr hoch
Beteiligungs- und Konsultationsverfahren <ul style="list-style-type: none"> <li>• Beteiligungsverfahren Ausländerbehörden/Sicherheitsbehörden</li> <li>• Beteiligungsverfahren Bundesagentur für Arbeit</li> <li>• Visa-Konsultationsverfahren</li> <li>• Asylkonsultationsverfahren</li> </ul>	3	sehr hoch
Visa-Angelegenheiten (national und europäisch) <ul style="list-style-type: none"> <li>• Visumverfahren</li> <li>• Zugriff Visumsbehörden</li> <li>• Nationale Kopfstelle</li> </ul>	3	hoch bis sehr hoch
Grenzen <ul style="list-style-type: none"> <li>• EU-Integration</li> <li>• Border Control Middleware</li> <li>• Zugriff Strafverfolgungsbehörden</li> </ul>	3	hoch bis sehr hoch

<sup>2</sup> Entsprechend der Klassifizierung des IT-Grundschutzes.

<ul style="list-style-type: none"> <li>• Linkauflösung</li> <li>• ETIAS Zentralstellen</li> <li>• Zugriff Migrationsbehörden</li> <li>• Datenqualitätsinstanz/Querschnittskomponenten</li> </ul>		
Personalausweis und Elektronischer Identitätsnachweis <ul style="list-style-type: none"> <li>• Elektronischer Identitätsnachweis – Vergabestelle für Berechtigungszertifikate</li> <li>• Globaler Sperrdienst</li> </ul>	3	normal bis hoch
Passagierdatenregister (PNR) <ul style="list-style-type: none"> <li>• PNR-Portal, PNR-Querschnittssysteme und Accessmanagern</li> <li>• Datenannahme und Speicherung, Sanktionierung von Luftfahrtunternehmen</li> <li>• PNR-Register</li> <li>• Abgleiche und Suchverfahren</li> <li>• Vorgangsverwaltung</li> <li>• Datenanalyse und Reporting</li> </ul>	4	hoch bis sehr hoch
Datenabgleichverfahren (Geheimhaltungsstufe, eingebunden u.a. in das Visaverfahren und diverser Verfahren von Sicherheitsbehörden)	5	sehr hoch
Waffenregister mit weiteren Ausbaustufen wie Verbindung zu den Herstellern	5	hoch
Waffenrechtliche Erlaubnisse	5	hoch
Staatsangehörigkeit <ul style="list-style-type: none"> <li>• Verfahren Staatsangehörigkeiten (FASTA-STA)</li> <li>• Entscheidungen in Staatsangehörigkeitsangelegenheiten (ESTA)</li> <li>• Staatsangehörigkeitsdatei-Fundstellenverzeichnis (FAStA-STADA)</li> <li>• Anwendung Staatsangehörigkeiten (ASTA)</li> </ul>	5	normal bis hoch
Spätaussiedler <ul style="list-style-type: none"> <li>• Spätaussiedleraufnahmeverfahren (AAV)</li> </ul>	5	normal bis hoch

Aufgrund der primär fachlich orientierten Aufteilung sind die Tätigkeitsbereiche der verschiedenen AN für die Entwicklung im jeweiligen Los prinzipiell unterschiedlich. Die Rahmenvereinbarung und Leistungsbeschreibung dieser drei Lose sind weitgehend identisch – mit Ausnahme der AN-spezifischen Daten (z. B. Ansprechpartner, Tagessätze) und der zugeordneten fachlichen Bereiche. Grundsätzlich sind in jedem der drei Lose ganz unterschiedliche fachliche Themen von der AN dieses Loses zu unterstützen. Diese können unabhängig voneinander sein, oder es können auch enge fachliche Abhängigkeiten bestehen.

Der IT-Bereich der BT ist der primäre Leistungsempfänger für diese Verfahrens- bzw. Projektspezifischen Leistungen mit eher technischem Schwerpunkt. Eine enge Zusammenarbeit ist darüber hinaus mit dem fachlichen Auftraggeber, den Fachabteilungen der BT, notwendig, um die Umsetzung von zielführenden gemeinsam verstandenen fachlichen Anforderungen und fachlichen Zielarchitekturen abzusichern. Diese Zusammenarbeit gestaltet sich überwiegend agil, teilweise noch klassisch nach dem V-Modell XT Bund.

### 3.4 Abgrenzung einzelner Themen/Schnittstellen zwischen den Losen

Teils beinhalten die verschiedenen Lose Aufgaben mit gleichen Bezeichnungen. Inhaltlich erfolgt die Abgrenzung zwischen den Losen über den jeweiligen Schwerpunkt. Dies wird an den wichtigsten Beispielen erläutert:

- **Architektur:**
  - Alle Aspekte verfahrensübergreifender Fragestellungen (fachlich und technisch) sind dem Los 1 zugeordnet. In Zusammenarbeit mit der AN von Los 1 wird die BT ihre Gesamtzielsetzung einer tragfähigen konsolidierten Gesamtarchitektur verfolgen. Dazu sind auch Entwürfe der AN zu Los 3 bis 5 ebenso wie Entwürfe aus anderen Bereichen der BT (von anderen Dienstleistern oder intern erstellt) gemeinsam mit der BT vor Umsetzung zu prüfen und zu bewerten bzw. Vorgaben für deren Leistungen zu definieren.
  - Alle Aspekte einer verfahrensspezifischen fachlichen und technischen Architektur sind den Losen 3 bis 5 zugeordnet (je nach Zuordnung des jeweiligen Verfahrens zu den Losen). Die BT wird die Architekturentwürfe der AN der Lose 3 bis 5 entsprechend prüfen, ggf. unterstützt durch die AN Los 1. Abweichungen in der Architektur von den Vorgaben bedürfen der expliziten Zustimmung der BT.
- **Projektmanagement:** Jede AN leistet das Projektmanagement für ihre Gesamtleistungen, die sie für die BT erbringt.
  - Jede AN leistet das Projektmanagement für ihre Leistungen in jedem ihrer Einzelprojekte. Aufgrund der Vielzahl zu unterstützender Fachverfahren in jedem Los unterstützt die AN ggf. parallel unterschiedliche Projektaktivitäten.
  - Die AN Los 2 leistet für die BT die Projektmanagement-Aufgaben zur Sicherstellung übergreifender Zielsetzungen, z. B. bei der Koordinierung der AN der Lose 1 sowie 3 bis 5 – inkl. ggf. Review und Bewertung von Projektplänen der AN und deren Abgleich bei Beteiligung mehrerer AN.
  - Die AN Los 2 unterstützt die BT bei Projektmanagement-Aufgaben in Verantwortung der Fachbereiche, z. B. durch Führung eines Projektmanagement-Office für die fachlichen Projektabläufe.
  - Die AN Lose 1 und 3 bis 5 leisten für die BT die Projektmanagement-Aufgaben in Verantwortung der IT-Bereiche, z. B. durch Durchführung aller benötigten Disziplinen des Projektmanagement (z. B. Risikomanagement) für das durch sie umzusetzende Einzelprojekt unter dem jeweiligen Einzelauftrag gemäß der Rahmenvereinbarung.
- **Test:**

- Die AN Lose 1 sowie 3 bis 5 führen alle notwendigen Tests (fachlich und technisch) in dem in der Rahmenvereinbarung oder den besonderen Leistungsbeschreibungen für die Lose 1 sowie 3 bis 5 definierten Verfahren zur Abnahme vor Auslieferung der Softwarelösung an die BT durch, um die erforderliche Qualität ihrer Lieferung sicherzustellen. Der Automatisierungsgrad der Integrationstests, mit dem Ziel eines hohen Reifespektrums, soll nach den üblichen handwerklichen Standards (ISTQB) erfolgen. Zu den notwendigen Tests gehören auch Sicherheitstests. Die technische Abnahme in Los 1 soll weitgehend durch Los 1 automatisiert werden.
- Die AN Los 2 übernimmt für die BT Aufgaben bei der fachlichen und technischen Prüfung der von der AN Lose 3 bis 5 gelieferten Softwarelösungen, insbesondere durch Durchführung entsprechender, möglichst automatisierter, Tests.
- Die AN Los 2 übernimmt für den IT-Bereich der BT Aufgaben bei der technischen Funktionsprüfung der von der AN Lose 1 sowie 3 bis 5 gelieferten Softwarelösungen, insbesondere durch Durchführung entsprechender Tests. Für die Auslieferungen soll eine weitgehend automatisierte technische Abnahme realisiert werden. Los 2 ist hier im Rahmen des Qualitätsmanagements dafür zuständig, kontinuierlich zu evaluieren, ob die automatisierte Testabdeckung ausreichend ist.
- Die AN Los 2 führt Tests für die BT auf Testumgebungen der BT durch. Wenn eine direkte Anbindung an die Build-Infrastruktur der BT realisiert werden kann, so konfigurieren die AN der Lose 1 sowie 3 bis 5 per GitOps die Pipelines für die Befüllung der Testumgebung und die Ausführung der Tests in der Testumgebung. Die AN Lose 1 sowie 3 bis 5 stellen auf Anforderung der BT Testumgebungen zur Verfügung. Dies kann bedeuten, dass die AN Los 2 die Testdurchführung auf Testumgebungen durchführt, die die AN Lose 1 sowie 3 bis 5 bereitstellen.
- Die Bereitschaft der verschiedenen AN zum Austausch von Testdaten und Testfällen untereinander wird erwartet (z. B. zur Wiederverwendung oder Nachstellung von Fehlersituationen).
- Register Factory/IsyFact/Digi Factory:
  - Grundsätzlich ist die konzeptionelle Weiterentwicklung der Register Factory/IsyFact/Digi Factory durch die AN Los 1 vorgesehen. Dies schließt jedoch nicht aus, dass auch als Teil der weiteren Leistungen Konzepte mit fachlichem Schwerpunkt (Los 2) oder im Rahmen der Entwicklung und Pflege (Lose 3 bis 5) Beiträge zu Register Factory/IsyFact/Digi Factory zu liefern sind, wenn dies in der konkreten Themenstellung angemessen und sinnvoll ist.

- Die Realisierung der Entwicklungsleistungen für die Register Factory/Isyfact/Digi Factory ist durch die AN Los 1 vorgesehen. Es können jedoch nach Absprache von den Losen 3-5 Zulieferungen erstellt werden, die durch Los 1 zu integrieren sind.
- Querschnittsanwendungen:

Im Rahmen der Softwareentwicklung ist zu unterscheiden zwischen der Entwicklung konkreter Fachverfahren und der Entwicklung von Querschnittsanwendungen (QAs). Querschnittsanwendungen werden in der Regel von mehreren Fachverfahren genutzt und können (je nach Abstraktionsgrad der Funktionalität) in einer oder mehreren Anwendungslandschaften betrieben werden. Pro Querschnittsanwendung kann es folglich viele verschiedene nutzende Verfahren geben, die in unterschiedlichen fachlichen Domänen verortet sind. Daher werden für die QA-Entwicklung die zwei folgenden übergreifenden Rollen definiert, anhand derer die Aufgaben im Kontext der QA-Entwicklung pro Los verteilt werden können.

- **Der Maintainer einer QA**

Jede QA hat genau einen Maintainer, der die folgenden Aufgaben und Verantwortungen innehat:

- Hauptverantwortung für die Pflege der QA; dies umfasst
  - Koordination der Weiterentwicklung und Pflege der QA
  - Durchführung von regelmäßigen Technologie-Updates
  - Durchführung von Sicherheitsupdates (bei CVE-Funden o.ä.)
- Anpassung von Schnittstellen zu (externen) Drittsystemen
- Integration von Zulieferungen
- Definition von Qualitätsanforderungen für die Integration

Rahmenbedingungen:

Jede QA hat immer nur einen Maintainer. Dieser ist für die Minimalpflege und die Koordination der inhaltlichen Weiterentwicklung zuständig.

Die Zuordnung des Maintainers einer QA zu den Losen 1, 3, 4 oder 5 richtet sich nach der Nähe zu dem im Schwerpunkt einschlägigen Fachverfahren (vgl. dazu Kapitel 3.3).

- **Der Zulieferer einer QA**

Jede AN eines Entwicklungsloses (= Lose 1 und 3 bis 5) kann Zulieferer für die fachlichen Anforderungen für eine QA sein:

- Zulieferungen erfolgen per Pull-Request an den Maintainer (dieser muss integrieren)
- Abstimmung mit anderen Zulieferungen und dem Maintainer

Rahmenbedingungen

Die AN der Lose 1 und 3 bis 5 können Zulieferer für eine QA sein. Dies gilt auch für den Maintainer. Die Zulieferer müssen sich untereinander und mit dem Maintainer bzgl. der Entwicklungstätigkeiten abstimmen.

**Die zugrundeliegenden Zielsetzungen der dargestellten Losbildung lassen sich nur mit einer Loslimitierung erreichen: die Lose 1 bis 5 müssen daher von verschiedenen AN bearbeitet werden.**

Die BT arbeitet mit unterschiedlichen externen Dienstleistern und anderen Behörden zusammen. Die Bereitschaft der AN zur vertrauensvollen Zusammenarbeit mit diesen Partnern der BT ist unverzichtbar.

## **4. Allgemeine Regelungen**

### **4.1 Rahmenbedingungen für Beauftragungen**

Die BT geht von einem kontinuierlichen Bedarf insbesondere an Werk- und Dienstleistungen für die IT-Systeme einschließlich der oben genannten Fachverfahren aus, kann eine entsprechende kontinuierliche Beauftragung aber nicht garantieren. Der Bedarf wird voraussichtlich nicht gleichverteilt sein, sondern immer wieder Spitzen aufweisen, ggf. auch Unterbrechungen.

Aufgrund möglicher Änderungen während des Projektverlaufs, insbesondere der rechtlichen und aufgabenorientierten Rahmenbedingungen, können sich Prioritätenänderungen und Umplanungen ergeben. Beispiele hierfür sind geänderte Vorgaben aufgrund (neuer) gesetzlicher Vorgaben und/oder Termine vor dem Hintergrund der Jährlichkeit des Haushalts.

Die AN sind verpflichtet, sich an die Einhaltung der TLP-Richtlinie des BVA und des TLP-Merkblatts des BSI zu halten. Sie muss darüber hinaus zusichern, dass sie vor einer zulässigen Weitergabe der Informationen zu Unterauftragnehmerinnen, die jeweilige Firmenleitung über die TLP-Vorgaben informiert, damit diese geeignete Sensibilisierungsmaßnahmen veranlassen kann.

Für jegliche schriftliche Kommunikation innerhalb des Bundesverwaltungsamtes und im Namen des BVA sowie bei der Erstellung von Dokumenten sind die Vorgaben des Bundesministerium für Inneres zur Anwendung der gendersensiblen Sprache zu beachten.

### **4.2 Arbeitsort, Erfüllungsort**

Erfüllungsort (Ort, an dem die Leistung bereitgestellt wird) ist grundsätzlich der Dienstsitz der BT, also Köln. Die AN entwickelt die Software in der Regel nicht bei der BT und nicht in oder auf deren Infrastruktur.

Zudem können Bereitstellungen und Arbeiten auch in Liegenschaften in Hamm oder in Berlin erforderlich sein. Wird die Anwesenheit von Beschäftigten der AN im Einzelfall auch an anderen Standorten, z. B. anderer Behörden (z. B. BMI in Berlin) oder bei Veranstaltungen durch die BT für erforderlich erachtet, gilt auch dieser Ort als Arbeitsort. Losübergreifend wird eine Reisetätigkeit in Höhe von ca. 5 % erwartet.

Der konkrete Arbeitsort für jede Leistung wird vom Projektleitenden der BT vorgegeben. Diese Vorgabe bezieht sich ausschließlich auf die zu erbringende Leistung; sie beinhaltet keine Weisung über die Festlegung der einzusetzenden Beschäftigten und keine Weisung an den jeweiligen Beschäftigten der AN.

Die AN gewährleistet im Rahmen der Leistungserbringung, dass sie alle Vorgaben des Handbuchs zum Geheimschutz in der Wirtschaft sowie der VSA einhält.

Mit Zustimmung sowohl der AN als auch der BT kann im Einzelauftrag projektbezogen vereinbart werden, dass Beschäftigte der AN auch außerhalb der Betriebsstätte(n) der AN arbeiten dürfen („mobiles Arbeiten“). Voraussetzung hierfür ist, dass die internen Vorgaben der AN, die auf Verlangen gegenüber der BT nachzuweisen sind, ein solches mobiles Arbeiten zulassen.

Dabei gelten folgende Vorgaben für die Verwendung von BT-eigener Hardware außerhalb der Liegenschaften der BT:

- In den Räumlichkeiten des beauftragten Unternehmens. Befindet sich das Unternehmen im EU-Ausland, ist die Arbeit mit BT-eigener Hardware nur dann zulässig, wenn ein Geheim-  
schutzabkommen zwischen der BRD und dem jeweiligen Einsatzland des Fremdpersonals vor-  
liegt.
- In Telearbeit/aus dem Home-Office, sofern sich der häusliche Arbeitsplatz innerhalb der Bun-  
desrepublik Deutschland befindet.
- Ortsungebunden („mobiles Arbeiten“ z. B. im Zug oder im Hotel) innerhalb der Bundesrepublik  
Deutschland.
- Aufwände und Kosten zur Einrichtung dieser Umgebungen werden nicht separat vergütet.
- Die BT ist berechtigt, in den Niederlassungen die Konformität der Arbeitsweisen nach ISO/IEC  
27001 und ISO 25010 zu prüfen oder durch Beauftragte prüfen zu lassen.

#### **4.3 Projektleitung**

Jede AN benennt eine Gesamt-Projektleitung als für die Gesamtleistungen der AN verantwortliche An-  
sprechperson sowie eine Vertretung. Die Gesamt-Projektleitung der AN steuert die Aktivitäten der AN  
in enger Abstimmung mit den Ansprechpersonen der BT für die jeweilige Rahmenvereinbarung.

Ein regelmäßiger Jour fixe der Gesamt-Projektleitung der AN mit den jeweiligen Projektverantwortli-  
chen der BT ist Bestandteil der Projektleitungs-Aufgabe (in der Regel 14-tägig, bei Bedarf muss auch  
ein anderer Rhythmus möglich sein). Der Jour fixe erfolgt in der Regel via Videokonferenz in einem  
hierfür von der BT bereitgestellten Videokonferenzsystem, ausnahmsweise auf Anforderung der BT als  
Präsenztermin in einer Liegenschaft der BT.

Ein Großteil der von BT und AN zu bewältigenden Aufgabenstellungen wird in Form von Einzel-/Teil-  
Projekten bearbeitet werden. Für jedes Einzel-/Teil-Projekt benennen BT und AN entsprechende Ein-  
zel-/Teil-Projektleiter/innen. Diese stimmen sich weitest möglich direkt zu allen Fragen ihres Einzel-  
/Teil-Projektes ab und berichten an die jeweiligen Gesamt-Projektleitenden. Die Benennung von Ein-  
zel-/Teil-Projektleiter/innen durch die BT lässt die Verantwortlichkeit des AN für die Erbringung der  
Gesamtleistungen unberührt.



## 4.4 Vorgehensmodell

Die BT setzt unterschiedliche Vorgehensmodelle ein:

- a) Hybride Modelle, die das Vorgehensmodell des Bundes (V-Modell XT Bund, derzeit Version 2.4) mit Elementen aus der agilen Welt vereinen, insbesondere nach Scrum;
- b) Vollumfänglich agil; oder
- c) Vorgehensmodell des Bundes (V-Modell XT Bund, derzeit Version 2.4); darin sind vollumfänglich agile Methoden integriert.<sup>3</sup>

Im Zusammenspiel mit internen Abteilungen und anderen Behörden sowie anderen Dienstleistern hat es sich in der Praxis als zielführend herausgestellt, sogenannte hybride Vorgehensmodelle zu implementieren, die die Vorteile beider Welten vereinen. Das sind insbesondere aus dem V-Modell XT Bund die systematische und detaillierte Beschreibung von Anforderungen, das einheitliche Vorgehen in der Qualitätssicherung nach dem ISTQB Standard, sowie Planungssicherheit für alle beteiligten Organisationen. Aus der agilen Welt hat sich bewährt: der Umgang mit unvollständigen oder sich häufig ändernden Anforderungen, der Entwicklungsfortschritt in kleinen Inkrementen, die Verstärkung der internen Kommunikation durch regelmäßige Sprintreviews und Retrospektiven unter Einbeziehung der operativen Ebenen. Die AN muss in der Lage sein, diese Gratwanderung zielführend durchzuführen und sich aktiv und den Teamgedanken fördernd darin einzubringen, ohne dabei ihre Gesamtverantwortlichkeit für die zu erbringenden Leistungen aus dem Auge zu verlieren.

Überwiegend kommen in den Projekten der BT agile Vorgehensweisen basierend auf Scrum und Kanban zum Tragen. Die Vorgehensweise und Prozesse sind dabei so auszugestalten, dass Konformität zum V-Modell XT Bund (derzeit Version 2.4) gewahrt wird. Die Implementierung dieser Vorgehensweisen erfolgt unter Berücksichtigung der Werte des agilen Manifests in enger Abstimmung mit der BT und bezieht andere AN mit ein. Die AN muss in der Lage sein, durch entsprechenden Nachweis von Schulungs- und Trainingsmaßnahmen ihrer Mitarbeiter/innen agil vorzugehen und gleichzeitig hohe Qualitätsstandards einzuhalten, in dem sie agile Disziplin wahrt.

Das V-Modell XT Bund (derzeit Version 2.4) ist ein generischer Vorgehensstandard, der für ein konkretes Projekt angepasst und konkretisiert werden muss. Vervollständigt wird dies durch BVA-spezifische Ergänzungen im Rahmen von Register Factory/IsyFact und fachbereichsspezifische Standards.

Die AN nimmt in Zusammenarbeit mit der BT spätestens zu Beginn eines Teil-/Einzelprojekts ein zweckmäßiges Tailoring auf der Grundlage des V-Modell XT Bund vor. Die Ausrichtung des in den

---

<sup>3</sup> **Fehler! Linkreferenz ungültig.** [https://www.cio.bund.de/Webs/CIO/DE/digitaler-wandel/Achitekturen\\_und\\_Standards/V\\_modell\\_xt/V\\_modell\\_xt\\_bund/v\\_modell\\_xt\\_bund-node.html](https://www.cio.bund.de/Webs/CIO/DE/digitaler-wandel/Achitekturen_und_Standards/V_modell_xt/V_modell_xt_bund/v_modell_xt_bund-node.html).

Dokumenten von IsyFact (Anlage IsyFact\_RegisterFactory\_2025) beschriebenen Vorgehens ist zu beachten. Die AN verwendet gegebenenfalls zusätzlich weitere geeignete Vorgehensmodelle bzw. Elemente daraus.

#### **4.5 Projekthandbuch**

Die AN muss, wenn von der BT gefordert, zu Gesamtprojekt-Beginn ein Projekthandbuch erstellen; dies gilt für alle Lose. Das Projekthandbuch beinhaltet eine Kurzbeschreibung des Projekts, den grundlegenden Projektdurchführungsplan, die notwendige und vereinbarte Unterstützung der BT sowie Organisation und Vorgaben für die Planung und Durchführung des Projekts und die anstehenden Aufgaben. Bei einem hybriden Vorgehen ist die Integration von agilen und „klassischen“ Vorgehen (V-Modell XT Bund, derzeit Version 2.4) im Projekthandbuch entsprechend zu dokumentieren.

Das Projekthandbuch ist im Projektverlauf nach Abstimmung mit der BT anzupassen und von der AN fortzuschreiben. Die Inhalte sind für die Projektdurchführung maßgeblich zu berücksichtigen.

Sämtliche Dokumente im Projekt (Arbeitspapiere, Berichte) müssen vollständig in deutscher Sprache verfasst sein und in editierbarer Form der BT in einem marktüblichen, elektronischen Format zur Verfügung gestellt werden. Das konkrete Dateiformat (z. B. Microsoft Office Version) ist mit der BT einvernehmlich abzustimmen.

#### **4.6 Zusammenarbeit**

Die BT legt Wert auf eine Vorgehensweise, die auf möglichst enger Zusammenarbeit von internen und externen Beschäftigten beruht und auch die Vermittlung bzw. den Austausch des fachlichen und technischen Know-hows zum Ziel hat. Dies ist deshalb als wesentlicher Bestandteil in die Vorgehensplanung einzubeziehen.

Deshalb wird von allen Beschäftigten der AN eine enge Zusammenarbeit mit den Beschäftigten der BT erwartet, sowohl aus dem IT-Bereich als auch aus den Fachbereichen.

In der folgenden groben Skizzierung des Vorgehens bei der Softwareentwicklung und -weiterentwicklung und Pflege sind auch interne Aspekte der BT berücksichtigt, um den zukünftigen AN einen ersten Eindruck von den Prozessen zu vermitteln, in die sie eingebunden sein werden:

Der Bereich „Softwareentwicklung und Projektmanagement“ der BT arbeitet eng mit dem fachlichen BT, den Fachabteilungen der BT, zusammen. Gemeinsam werden die fachlichen Anforderungen ermittelt, analysiert, strukturiert und qualitätsgesichert. Je nach Projekt und Erfahrung arbeiten externe IT-Dienstleistende bereits in dieser Phase an der Aufgabe mit, um eine frühe Einbindung und ein gemeinsames Verständnis zu erreichen. Vertragstechnisch werden hierfür in der Regel Arbeitspakete nach Aufwand mit definierter Obergrenze vereinbart.

Sichtbare Merkmale der praktizierten Projektsteuerung durch die BT sind z. B. formalisierte Steuerungsgremiumssitzungen zwischen Fachabteilung, Softwareentwicklung, Betriebsbehörde und externen IT-Dienstleistenden, formalisiertes Problem- und Changemanagement über (soweit vorhanden) Werkzeuge der BT sowie bedarfsabhängige Abstimmungen zwischen externen IT-Dienstleistenden und der Softwareentwicklung der BT über vertragliche Inhalte.

#### **4.7 DevOps**

Die BT hat als Ziel die Einführung interdisziplinärer Teams nach Vorbild des sog. DevOps-Gedanken. DevOps beschreibt Prozesse und Software-Werkzeuge, die eine effektivere und effizientere Zusammenarbeit der Bereiche Softwareentwicklung (Dev), Systemadministratoren (Ops), sowie Qualitätssicherung und des Anforderungsmanagements ermöglichen. Hierbei legt die BT fest, ob einzelne Systeme, Verfahren oder ganze Anwendungslandschaften in solchen Teams bearbeitet werden.

Die AN hat mit Fokus auf das jeweilige Los die Mitwirkung in diesen Teams bestmöglich zu unterstützen und zu operationalisieren. Die BT kann in Zusammenarbeit mit der AN Beratung für die Weiterentwicklung der genannten Prozesse und eingesetzten Werkzeuge in Anspruch nehmen. Die AN kann der BT konkrete Vorschläge unter gegenseitiger Mitwirkung für weiter zu entwickelnde Prozesse vorlegen. Die Entscheidungshoheit liegt bei der BT.

#### **4.8 Buildmanagement**

Die AN ist dazu verpflichtet, regelmäßig die entwickelten Programm-Sourcen im GitLab der Zentralen Softwareentwicklung-Service-Infrastruktur (ZSSI) bereitzustellen. Außerdem ist die AN für die Konfiguration und Sicherstellung der Lauffähigkeit der CI-Pipelines zuständig. Die CI-Pipelines sind nach den Vorgaben und Möglichkeiten der BT und der Referenzarchitektur für einheitliche Build und Deployment Pipelines (BDPRA), zu entwickeln.

Ein Deployment darf im Rahmen der Pipeline nur erfolgen, wenn für die erstellte Software und ihre Abhängigkeiten die, durch die BT vorgegebenen, Freigabekriterien erfüllt sind. (Beispiel: Abbruch des automatischen Builds bei kritischen Schwachstellenfunden im Rahmen der Sicherheitstests.)

Es sind abhängig von den Vorgaben mehrere Stages für Builds, Tests und Deployments einzurichten, die folgende Substages beinhalten können:

- Build der Software und Signierung der Artefakte
- Erstellung von SBOMs
- Ausführung von Unit-Tests
- Prüfung der statischen Code-Qualität:
- Prüfung auf Einhaltung der Softwarearchitekturvorgaben
  - Ermittlung der Test-Coverage

- Erkennung von Secrets
  - Durchführung statischer Sicherheitstests (Static Application Security Testing)
  - Prüfung der Dependencies auf bekannte Sicherheitslücken (CVEs)
- Bereitstellung der Artefakte im Artifactory
- Automatisierte Aktualisierung von Dependencies
- Durchführung von Integrations-, Akzeptanz- und Performance-Tests
- Deployment der Software und Datenbanken in Test- und Produktionsumgebungen

Die Tools, die innerhalb der CI-Pipelines verwendet werden müssen, werden von der BT vorgegeben.

Bei der Erstellung der CI-Pipelines sind folgende Qualitätsziele zu beachten.

- **Reproduzierbarkeit** – Artefakte, die innerhalb der Pipeline erzeugt werden, sollen reproduzierbar sein. Das heißt, bei erneuter (späterer) Ausführung der Pipeline werden die gleichen Artefakte erzeugt. Reproduzierbarkeit ermöglicht es jedem zu verifizieren, dass ein Artefakt auf entsprechende Weise aus dem gegebenen Source Code erzeugt wurde.
- **Schnelligkeit** – Die Pipeline soll in angemessener Geschwindigkeit durchlaufen, so dass kein Prozess, wie Code Integrationen, Tests oder Deployment, aufgrund langer Wartezeiten unterbrochen oder verzögert wird und eine schnelle Auslieferung von neuen Features und insbesondere wichtigen Patches ermöglicht wird.
- **Automatisierung** – Die Pipeline soll einen hohen Grad an Automatisierung besitzen und möglichst viele automatisierbare Tätigkeiten übernehmen, um Kapazitäten zu sparen und den Entwicklungs- und Auslieferungsprozess zu beschleunigen.
- **Zuverlässigkeit** – Die Pipeline sollte möglichst durchgehend verfügbar sein, verlässlich funktionieren und die erwarteten Ergebnisse und Artefakte liefern.
- **Sicherheit** – Die Pipeline soll die Supply Chain Security der Projekte sicherstellen. Bei den verwendeten Tools wird ein Minimalprinzip bei Berechtigungen, Credentials, etc. angewendet. Erzeugte Artefakte besitzen Signatures und es werden weitere Maßnahmen getätigt, um die Nachvollziehbarkeit zur Herkunft und Builds von Artefakten herzustellen und jegliche Manipulationen zu unterbinden, bzw. zu erkennen.
- **Benachrichtigungen** – Sowohl bei erfolgreichen Abschlüssen als auch bei Fehlschlägen einzelner Schritte der Pipeline sollen alle dafür relevanten Benutzer und Systeme über effiziente Kanäle informiert werden. Die Benachrichtigungen sollen verständlich sein und relevante Ergebnisse zusammenfassen. Es soll sichergestellt werden, dass die Benachrichtigungen keine kritischen oder sicherheitsrelevanten Informationen enthalten.

- **Dokumentation** – Der Umfang und die Funktionen der Pipeline, bzw. der einzelnen Bestandteile dieser werden umfassend sowie verständlich dokumentiert. Konfigurationsoptionen, erforderliche und optionale Eingaben, sowie eingehende und ausgehende Artefakte werden erläutert. Abhängigkeiten zu anderen Systemen oder Teilen der Pipeline sowie weitere Anforderungen werden angegeben.

#### 4.9 Technische Anbindung

Die BT stellt für ihre Softwareentwicklungsaufgaben eine Zentrale Softwareentwicklung-Service-Infrastruktur (ZSSI) bereit.

Diese Infrastruktur wird von der AN zu nutzen sein, um Projektinhalte (z. B. Tickets, Dokumente, Sourcen) zentral abzulegen und auszutauschen. Die wesentlichen Produkte sind

- JIRA als Issue-Tracker (auch für Unterstützung des Anforderungs-, Test- und Fehlermanagements, Configuration-Management, Qualitäts-Management);
- Confluence;
- Git/GitLab als Sourcecode-Versionsverwaltung und als Continuous-Integration-Server;
- Alfresco als Dokumenten-Management-System mit Versionskontrolle; und
- Artifactory als Artefakt-Repository.

Verbindliche Termine für die Bereitstellung des kompletten Serviceumfangs können derzeit nicht zugesagt werden. Die Produkte JIRA, Confluence, GitLab, Alfresco und Artifactory stehen bereits zur Verfügung.

Es ist im Rahmen der Leistungserbringung erforderlich, bei der AN eine geeignete Infrastruktur nach Maßgabe der für IT-Sicherheit zuständigen Stelle der BT einzurichten und zu betreiben, die der AN einen Remote-Zugriff (z. B. zum Repository-Zugriff, zum sicheren Austausch von Dokumenten) ermöglicht.

Stand 2025: Der Zugang zur ZSSI ist nicht über das Internet möglich. Zur Anbindung an die ZSSI wird der AN von der BT eine VPN-Appliance zur Verfügung gestellt. Es darf keine Netzkoppelung zwischen dem privaten Netz der Appliance und dem Firmennetz der AN oder dem Internet hergestellt werden. Die Appliance wird von der BT oder einer von ihr beauftragten Behörde betrieben. Gegebenenfalls kann von diesem Vorgehen für privilegierte Accounts abgewichen werden, was mit weiteren Einschränkungen bzgl. der Hardware verbunden sein kann. Es gilt die Informationssicherheitsrichtlinie zur Fremdfirmeneinwahl, die im Auszug anhängt (ISR Fremdfirmeneinwahl).

#### 4.10 Informationstechnik der Auftragnehmerin

Grundsätzlich obliegt es der AN, die eigenen Beschäftigten mit jeglicher Informationstechnik auszustatten, die zur Erfüllung der Leistungen aus dieser Rahmenvereinbarung erforderlich ist. Die AN

sichert die eigene, betriebliche Informationstechnik der Beschäftigten nach Stand der Technik ab (s. Anlage „Technologische Übersicht“).

Sofern die Beschäftigten der AN im Rahmen der Leistungserbringung für die BT Dokumente bzw. Verschlusssachen mit dem Geheimhaltungsgrad VS-NfD verarbeiten müssen, stellt die BT diesen Beschäftigten einen IT-Arbeitsplatz bzw. Endgeräte für die Sichere Inter-Netzwerk-Architektur (kurz „**SINA**“ und „**SINA Endgeräte**“) zur Verfügung. Die Beschäftigten der AN müssen SINA Endgeräte an den Liegenschaften des ITZBund entgegennehmen, an denen das ITZBund die SINA Ausgabe im Einzelfall vorsieht. Die SINA Endgeräte werden mit Microsoft Office, Visio und bei Bedarf mit einer vom BSI zugelassenen Software zur Ver- und Entschlüsselung von E-Mails und Dateien ausgestattet (derzeit GnuPG VS-Desktop). Darüber hinaus erhält die AN von der BT Zugriff auf Plattformen und Programme, die zur Auftragserfüllung erforderlich sind. Im Ausland dürfen keine SINA Endgeräte für mobiles Arbeiten verwendet werden.

Die Verarbeitung von Dokumenten bzw. Verschlusssachen mit Geheimhaltungsgrad VS-NfD auf eigener, betrieblicher Informationstechnik der AN ist nur mit ausdrücklicher, vorheriger schriftlicher Genehmigung der BT zulässig. Sofern die AN aufgrund Genehmigung eigene Informationstechnik einsetzt, muss die AN dafür Sorge tragen, dass die an die Informationstechnik zu stellenden Anforderungen des Handbuches zum Geheimschutz in der Wirtschaft sowie der VSA erfüllt sind. Für die Veranlassung von Ermächtigungen der Beschäftigten bis zur Geheimhaltungsstufe „Geheim“ (Ü2) ist die AN verantwortlich. Soweit erforderlich, muss die AN in der Informationstechnik vom BSI zugelassene IT-Sicherheitsprodukte zum Einsatz bringen und für alle notwendigen Freigaben sorgen.

#### **4.11 Sicherheitsvorgaben der BT**

Neben allgemeinen Sicherheitsvorgaben aus dem IT-Grundschutzkompendium des BSI zur Nutzung von Hard- und Softwareprodukten der BT (z. B. Umgang mit BT-Hardware, Passwort-Policies) sind die Informationssicherheitsrichtlinien Fremdpersonal, Fremdfirmeneinwahl und Softwareentwicklung für die AN verbindlich einzuhalten.

Ausnahmsweise ist es möglich, dass die BT im Rahmen der Beauftragung Daten mit dem Schutzbedarf „sehr hoch“ an die AN zur Bearbeitung übergibt. Die technisch-organisatorischen Maßnahmen müssen sich demnach auf den Schutzbedarf „sehr hoch“ beziehen.

#### **4.12 Verträge zur Auftragsverarbeitung**

Die meisten beim BVA verwendeten und entwickelten IT-Systeme verarbeiten personenbezogene Daten, die den jeweils anwendbaren gesetzlichen Bestimmungen zum Datenschutz unterliegen. Im Einzelfall ist nicht auszuschließen, dass die AN Kenntnis von personenbezogenen Daten erlangt oder diese

zur Erbringung der Leistungen im Auftrag der BT verarbeitet. Dies kann beispielsweise bei Sicherheitstests in Produktionsumgebungen oder Revisionen bzw. Audits vorkommen.

Um solche Situationen von Anfang an rechtlich abzusichern, ist hierfür nach den Maßgaben der Datenschutzgrundverordnung der EU, Verordnung (EU) 2016/679 (DSGVO), dem Bundesdatenschutzgesetz (BDSG) sowie allen weiteren anwendbaren Vorschriften zum Datenschutz eine Auftragsverarbeitung zwischen der BT und der AN zu vereinbaren. Eine Mustervereinbarung für eine solche Vereinbarung befindet sich in den Anlagen zur Ausschreibung, einmal gemäß DSGVO (Anlage Mustervereinbarung zur Auftragsverarbeitung nach DSGVO) und einmal gemäß BDSG (Anlage Mustervereinbarung zur Auftragsverarbeitung nach BDSG), und wird nach Abschluss der Rahmenvereinbarung zwischen BT und AN abgeschlossen, soweit für die unter einem Einzelauftrag/mehreren Einzelaufträgen erbrachten Leistungen erforderlich. Die der Ausschreibung anliegenden Muster sind bindend und im Rahmen der Aufnahme der Zusammenarbeit als Anlage zur Rahmenvereinbarung auszufüllen und von beiden Seiten zu unterzeichnen.

- In der Vereinbarung selbst sind insbesondere die ggf. betroffenen Datenarten und -kategorien zu dokumentieren.
- Im Anhang „Technisch-organisatorische Maßnahmen“ (TOM) der Vereinbarung sind spezifisch für die jeweilige Situation alle notwendigen Regelungen (Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, usw.) vorgegeben und entsprechend umzusetzen. Diese technisch-organisatorischen Maßnahmen müssen vor der Zuschlagserteilung und vor der Datenverarbeitung vorhanden sein.

Der Abschluss von angemessenen Vereinbarungen zur Auftragsverarbeitung ist gesetzlich vorgeschrieben und daher unverzichtbar (Art. 28 Absatz 3 DSGVO, § 62 Absatz 4 BDSG).

Die AN stellt sicher, dass zum Zeitpunkt der Aufnahme der Datenverarbeitung die von dem BT geforderten Maßnahmen umgesetzt sind.

## 5. Softwareprodukte, Frameworks und Bibliotheken

Basistechnologie für die Entwicklung ist die Programmiersprache „JAVA“. Realisierungen haben gemäß den JAVA-Programmierkonventionen zu erfolgen.

Einzusetzende Softwareprodukte, Frameworks und Bibliotheken müssen der Register Factory/Isy-Fact/DevOps Factory in der jeweils aktuellen Fassung entsprechen.<sup>4</sup> Abweichungen hiervon bedürfen einer Ausnahmegenehmigung des Standardsboard (ein BVA-internes Architekturgremium)<sup>5</sup>.

Die einzusetzenden Produktversionen werden im Einzelfall von der BT festgelegt und können im Projektverlauf natürlich auch (ggf. kurzfristig) aktualisiert werden.

Der Einsatz von Tools, die auf der Basis Künstlicher Intelligenz (KI) funktionieren und arbeiten und dadurch Workflows vereinfachen, wird angestrebt und insbesondere im Bereich der Softwareentwicklung gewünscht. Eine Nutzung in einer on premise Umgebung ist wünschenswert. Soweit ein Hosting in einer Cloud-Umgebung erfolgt, ist die Einhaltung des C5:2020 Kriterienkataloges und der C5 Kriterien in der aktuellen Fassung zwingend erforderlich.

Ein Hosting in einer Cloud-Umgebung darf nur nach Abstimmung und vorheriger, ausdrücklicher und schriftlicher Zustimmung des BT erfolgen. Die jeweils intern geltenden Vorgaben beim BT werden bei der Entscheidung berücksichtigt. Zudem darf der zugrundeliegende Sourcecode nicht im Sinne der Verschlusssachenanweisung eingestuft sein (vgl. dazu § 2 VSA) und es dürfen keine Echtdaten verwendet werden. Zur Verhinderung von Urheberrechtsverletzungen und zur Gewährleistung der Einräumung der ausschließlichen Rechte an die BT sind entsprechende Schutzmaßnahmen zu treffen. Die Nutzung von Tools, die auf KI-Systeme i.S.d. § 3 Nr. 1 Verordnung über künstliche Intelligenz zugreifen oder selbst ganz oder teilweise aus einem solchen KI-System bestehen, muss bei der Leistungserbringung unter einem Los vorher mit der/dem Informationssicherheitsbeauftragten, dem IT-Vertragsmanagement und dem fachlichen Bedarfsträger aus dem IT-Bereich abgestimmt sein. Im Einzelauftrag ist eine Aufwandsschätzung für die Leistung unter Einbindung derartiger KI-Tools und ohne vorzunehmen.

Die Einrichtung und Pflege von Entwicklungs- und Testumgebungen beim AN ist ausschließlich von den AN der Lose 1 und 3 bis 5 zu leisten.

---

<sup>4</sup> [https://www.bva.bund.de/DE/Das-BVA/Aufgaben/I/Informationstechnik/RegisterFactory/Technologie/technologie\\_rf\\_node.html](https://www.bva.bund.de/DE/Das-BVA/Aufgaben/I/Informationstechnik/RegisterFactory/Technologie/technologie_rf_node.html), sowie: <https://isyfact.github.io/isyfact-standards-doku/current/einstieg/einstieg.html>.

<sup>5</sup> Ausnahme: Die angegebenen Werkzeuge zur Programmierung sind Empfehlungen.



## 6. Qualitätsmanagement

Die AN jedes Loses ist bezüglich der von ihr zu erbringenden Leistungen zu einem qualifizierten Qualitätsmanagement verpflichtet.

Die AN führt mit von der eigenen Projektorganisation unabhängigem Personal für alle Leistungen folgende Aufgaben durch:

- Interne Qualitätssicherung
- Internes Risikomanagement
- Internes Projektcontrolling
- Parallele Instanz für das Eskalationsmanagement

Sämtliche Maßnahmen zur Qualitätsplanung und Qualitätssicherung müssen zwischen der AN und der BT abgestimmt werden.

Die BT legt großen Wert auf eine umfassende und für sie transparente Qualitätssicherung. Dazu gewährt die AN der BT Einsicht in ihr internes Qualitätsmanagement und stellt der BT auf Anfrage alle internen Prüfdokumente (Prüfspezifikationen, Prüfprotokolle, Behebungshinweise, Nachprüfungsprotokolle) und vorliegende Qualitätsmanagementartefakte zur Verfügung. Die Einsicht erfolgt nach Wahl der BT per Videokonferenz/geteiltem Bildschirm, vor Ort bei der AN und/oder durch Überlassung/Übersendung von Dokumenten und/oder Kopien.

Die AN stellt ein QS-Handbuch mit folgenden Inhalten zur Verfügung:

- Qualitätsziele
- Maßnahmen zur Erreichung der QS-Ziele (skalierte Teststrategie)
- Verwendung von Richtlinien und Normen
- Rollen und Aufgabenverteilung
- Testkonzept (inkl. Testfälle)
- Prüfmethoden
- Prüfgegenstände
- Kritikalität
- Prüfkriterien
- Prüfumgebung

Grundsätzlich sind qualitätssichernde Maßnahmen durch die AN für alle Objekte innerhalb eines IT-Projektes durchzuführen (z. B. Systemspezifikation, Betriebshandbuch, Schulungsdokumente, usw.).

Die konkreten Maßnahmen sind am Typ des Prüfgegenstandes auszurichten.

Grundsätzlich ist ein ganzheitlicher Ansatz mit konstruktiven (fehlervermeidenden) als auch analytischen (fehleraufdeckenden), qualitätssichernden Maßnahmen zur Sicherstellung von

Softwarequalitätsmerkmalen nach ISO 25010 umzusetzen. Unter analytischen Maßnahmen wird das Testmanagement, die Testspezifikation, sowie die Testdurchführung und -auswertung insbesondere im Rahmen der Abnahme von (Teil-) Systemen verstanden.

## 7. Qualitätssicherung und Testmanagement

Die folgenden Vorgaben und Anforderungen gelten primär für die AN der Lose 2 bis 5. Die AN Los 2, 3 bzw. 4 bzw. 5 sind verantwortlich für diese Aufgaben vor der Lieferung an die BT. Die AN Los 2 unterstützt die BT zusätzlich bei deren Aufgaben zur Sicherstellung der Qualität der gelieferten Produkte.

### 7.1 Vorgaben für fachlichen Test

Für jeden spezifizierten Anwendungsfall bzw. dessen Prüfkriterien muss mindestens ein Testfall definiert werden und möglichst entsprechende Testdatensätze automatisiert erzeugt werden. Besteht der Anwendungsfall aus mehr als einem Hauptszenario, sind ebenfalls für die Alternativ-Szenarien Testfälle zu erstellen. Sollten sich innerhalb eines Anwendungsfalls durch Variation der Eingangszustände für einen Testfall unterschiedliche Ausgangszustände ergeben, so sind in diesem Fall entsprechend weitere Testfälle zu generieren. Bei dem Entwurf der Testfälle sind geeignete Testentwurfsverfahren wie z. B. Äquivalenzklassenbildung anzuwenden und zu dokumentieren. Der grundsätzliche Aufbau eines Testfalls orientiert sich dabei an folgender Vorlage (IEEE 829-2008 ff), kann aber durch die AN nach vorheriger Zustimmung mit der BT verfeinert werden:

- Verweis auf die Anforderung, den Anwendungsfall (Use Case)/Datenmodell
- Szenario
- Eingangszustand
- Durchgeführte Aktion
- Erwartetes Ergebnis (Soll)
- Tatsächliches Ergebnis/Ausgangszustand (Ist)

Die AN muss Testkataloge und -fälle erstellen und in den Testwerkzeugen so umsetzen, dass diese auch für eine automatisierte Testdurchführung mit einem Testframework und für Regressionstests wiederverwendbar sind.

Bei Bedarf des Fachbereichs der BT ist ein geeignetes Testwerkzeug mit der BT auszuwählen und anzupassen.

In der Regel sind sämtliche Testfälle und deren Ergebnisse an die BT zu liefern (auf Anforderung der BT als XML-Dateien).

Die an die BT ausgelieferten Testfälle sind auf die Anforderungen zu referenzieren.

Dies umfasst alle:

- funktionalen Anforderungen,
- nicht-funktionalen Anforderungen,
- folgende Parameter sind in der Regel je Anforderung zu pflegen:

- Verweise auf die fachliche Dokumentation der Anforderung (z. B. das Lastenheft oder Artefakte wie EPIC und/oder User Story bei agilem Vorgehen (inkl. detaillierter Angabe der Fundstelle))
  - Verweise zwischen Anforderungen, System- und Schnittstellenspezifikation (inkl. Angabe Anwendungsfall, Kapitel im Detail)
  - die Versionierung der Anforderungen
  - Verweise zwischen Anforderungen und Testfällen
  - Verweise zwischen Anforderungen und Systementwurf
- Optional sind die Parameter:
  - Risikostatus
  - Prioritäten
  - Abhängigkeiten der Anforderungen untereinander
  - Kosten der Änderung je Anforderungsgruppe

Eine Spezifizierung in dem von der BT gestellten Tickettool wird bevorzugt, ist aber zu vereinbaren.

Es wird ein schrittweises Testvorgehen entsprechend V-Modell XT Bund (derzeit Version 2.4) erwartet, das nicht nur die neu entwickelten bzw. geänderten Software-Komponenten umfasst, sondern die Funktionalität auch Ende-zu-Ende entlang der Geschäftsprozessunterstützung nachweist. In agilen Vorgehensweisen führt dies zur Wiederholung bzw. Erweiterung von fachlichen Abnahmetests aus den Entwicklungsinkrementen (Sprints) hin zum Test des integrierten Systems.

Fachliche Tests finden auf verschiedenen Teststufen statt:

- Akzeptanztests durch die BT anhand von Prototypen oder GUI-Entwürfen zu einem möglichst frühen Zeitpunkt tragen zur Absicherung des Lösungsansatzes bei. Die AN stellt diese der BT daher zur Verfügung.
- Die AN führt auch Tests hinsichtlich Barrierefreiheit (z. B. BITV-Test) durch und dokumentiert die Ergebnisse.
- Es sind Unittests (Modultests) als funktionale Tests auf Basis von QS-gesicherten Komponentenspezifikationen vorzusehen.
- Entsprechendes gilt für Komponentenintegrationstests, die technisch wie Unittests realisiert werden.
- Funktionale Systemtests (d. h. aus Sicht des Endanwenders) bilden die umfangreichste Teststufe: sämtliche funktionale Anforderungen werden systematisch abgeleitet und als Testbasis verwaltet. Dabei ist die Realisierung der Verfolgbarkeit (Traceability) zwischen Anforderung und entstandenen Testfällen zwingend vorzusehen, um die Testabdeckung messen und eine Auswirkungsanalyse nach fachlichen Änderungen durchführen zu können.

- Letzte Teststufe sind Systemintegrationstests (High-Level-Test) auf Basis von Geschäftsprozess- bzw. Workflowmodellen, um das korrekte Interagieren der Applikationen durchgängig zu testen.

Maßnahmen zur Qualitätssicherung sind somit auch verfahrensübergreifend durchzuführen. Inhaltliche Änderungen in einem Verfahren können relevante Auswirkungen für andere Verfahren bedeuten. Diese Abhängigkeiten sind beginnend bei der Definition von Änderungsanforderungen (Change Requests) zu bewerten und im Rahmen der Tests zu prüfen.

Beispiele für solche Abhängigkeiten:

- Änderungen an technischen Schnittstellen sind hinsichtlich der Abhängigkeiten anderer Nachbarsysteme zu prüfen, z. B. bei Änderung von Feldlängen, Pflichtattributen, Kennungen etc.
- Änderungen der Prüfredeln für (interne) Anfrage- oder Meldungsschnittstellen sind gegen das Anfrage-/Meldeverhalten der verbundenen Verfahren zu prüfen. Änderungen an Suchalgorithmen oder -bewertungen können zu Ergebnismengen führen, die für die anfragenden Verfahren zu unbefriedigenden Verarbeitungsergebnissen führen (z. B. fehlende Nachvollziehbarkeit von Treffern, zu kleine oder zu große Treffermengen).

Die AN stellt sich der angesprochenen Problematik durch ein konsequentes zielgerichtetes verfahrensübergreifendes Qualitätsmanagement.

## **7.2. Vorgaben für technischen Test**

Es müssen Last- und Performancetests durchgeführt und dokumentiert werden. Diese sind auf einer produktionsnahen Testumgebung (Pre-Produktionsumgebung) bei der BT möglichst unter Einsatz von Generatoren für die Erzeugung von Testdatensätzen durchzuführen.

Es müssen Fehlertoleranztests (Ausfalltests) durchgeführt werden, aus denen hervorgeht, ob das System im Fehler- oder Störfall in einem konsistenten Zustand gehalten wird, bei Abbruch bzw. dem Rücksetzen von Transaktionen eine entsprechende Fehlermeldung erfolgt sowie Ereignis und Art der Systemreaktion protokolliert werden. Die im Fehlertoleranztest zu prüfenden Ereignisse (Stromausfall, Verbindungsabbruch, Bedienungsfehler, Import fehlerhafter Daten, Ressourcenerschöpfung usw.), das Vorgehen im Test und das erwartete Systemverhalten (z. B. Verlagerung auf Spiegelsystem oder geordnetes Herunterfahren) werden zwischen der AN und der BT abgestimmt und in der Testspezifikation niedergelegt.

Im Rahmen des Fehlertoleranztestes muss geprüft werden, ob nach dem Störfallereignis eine Rückführung des Systems in den Normalzustand gemäß den Anleitungen aus dem Betriebshandbuch möglich ist.

Die AN führt auch Tests hinsichtlich IT-Sicherheit (z. B. Penetrationstest) durch und dokumentiert die Ergebnisse.

Für jegliche Form von Web-Applikationen (Webseiten, Web-Anwendungen, Webservices), sowohl auf Client- als auch auf Server-Seite, sind die Tests gemäß OWASP-Standard (Open Web Application Security Project) in der jeweils aktuellen Version durchzuführen. Für Nicht-Web-Applikationen ist nach OSSTMM (Open Source Security Testing Methodology Manual) vorzugehen.

Zugehörige Vorgaben des BSI zum Vorgehen und der Dokumentation der Ergebnisse in aktueller Version sind zu befolgen.<sup>6</sup>

Sofern die Tests auf Umgebungen der AN bzw. unter Einbeziehung von Geräten der AN durchgeführt werden, sind die darauf einzusetzenden Tools (z. B. Nessus Vulnerability Scanner, Acunetix Web Vulnerability Scanner oder Metasploit-Framework) auf eigene Kosten von der AN zu beschaffen.

---

<sup>6</sup> [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Pentest\\_Webcheck/Leitfaden\\_Penetrationstest.html](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Pentest_Webcheck/Leitfaden_Penetrationstest.html),  
[https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Dienstleistungen/ISPentest\\_ISWebcheck/ispentest\\_iswebcheck\\_node.html](https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Dienstleistungen/ISPentest_ISWebcheck/ispentest_iswebcheck_node.html).

## 8. Standards

Folgende Standards, Dokumente und Bausteine müssen bei der Leistungserbringung beachtet werden:

- BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS)
- BSI-Standard 200-2: IT-Grundschutz-Methodik
- BSI-Leitfaden zur Basis-Absicherung nach IT-Grundschutz
- BSI-Standard 200-3: Risikoanalyse auf der Basis von IT-Grundschutz
- BSI-Bausteine der Ebenen APP, CON, DER, IND, INF, ISMS, NET, OPS, ORP, SYS und alle Standard-Bausteine, die innerhalb der Vertragslaufzeit durch das BSI neu veröffentlicht werden.
- BSI Mindeststandard zur Nutzung externer Cloud-Dienste
- C5:2020 Kriterienkatalog in der bei Bekanntgabe der Vergabeunterlagen aktuellen Fassung

Darüber hinaus gelten für alle Arbeiten auch weitere De-facto Standards und andere öffentliche Dokumente.

Die folgenden Dokumente sind in ihrer jeweils aktuellen Fassung bei der Erteilung von Einzelaufträgen zu beachten. Da sie öffentlich zugänglich sind, werden sie nicht im Rahmen der Vergabeunterlagen explizit bereitgestellt.

- IT-Vorgaben für die Bundesverwaltung (in der jeweils aktuellen Fassung) (<http://www.cio.bund.de>)
  - Vorgehensmodell des Bundes (V-Modell XT Bund, derzeit Version 2.4)
  - Architekturrichtlinie für die IT des Bundes
  - Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (Barrierefreie-Informationstechnik-Verordnung - BITV 2.0))
  - XÖV-Standards (z. B. XAusländer, XMeld, XInneres)
  - Sichere Szenarien für Kommunikationsprozesse im Bereich hoheitlicher Dokumente (BSI TR-03132)
  - OSCI-Standards (<http://www1.osci.de>)
- BSI Grundschutz (in der jeweils aktuellen Fassung) (<http://www.bsi.bund.de>)
  - BSI Grundschutz-Kataloge (IT-Grundschutz „Alt“)
  - BSI Grundschutz-Kompodium (IT-Grundschutz „Neu“)
- Normen (in der jeweils aktuellen Fassung)
  - ISO 9000 ff
  - ISO 20000
  - ISO 25000 ff
  - ISO 27000 ff

- ISO 29119
  - ISO 42010
  - IEEE 730-2014
- OGC IT Infrastructure (ITIL) v3
- ISACA Control Objectives for IT and related Technologies (COBIT) v4.1
- ISTQB International Software Testing Qualifications Board
- IsyFact-Standard, (<https://github.com/isyfact>, [isyfact.github.io](https://isyfact.github.io))
- World Wide Web Consortium (W3C), (<http://w3.org>)
- Die De-facto Standards des World Wide Web Consortiums (W3C) (z. B. für HTML, CSS, XML, XSL, SOAP, WSDL, etc.) sind als verbindlicher Bestandteil anzusehen – insbesondere wird verwiesen auf:
  - Web Content Accessibility Guidelines v2 (WCAG)
- Organization for the Advancement of Structured Information Standards (OA-SIS), (<http://oa-sis-open.org>);
- SUN: Java Code Conventions (<http://java.sun.com>), (<http://www.oracle.com/technetwork/work/java>)
- Stabile Projekte der Open Web Application Security Project (OWASP), (<http://www.owasp.org>), z. B. OWASP Top Ten.
- Technische Richtlinien des BSI
  - [BSI TR-03121 Technical Guideline Biometrics for Public Sector Applications](#)
  - [BSI TR-03135 Machine Authentication of MRTDs for Public Sector Applications](#)
  - [BSI TR-03183-2 \(Software Bill of Materials\)](#)