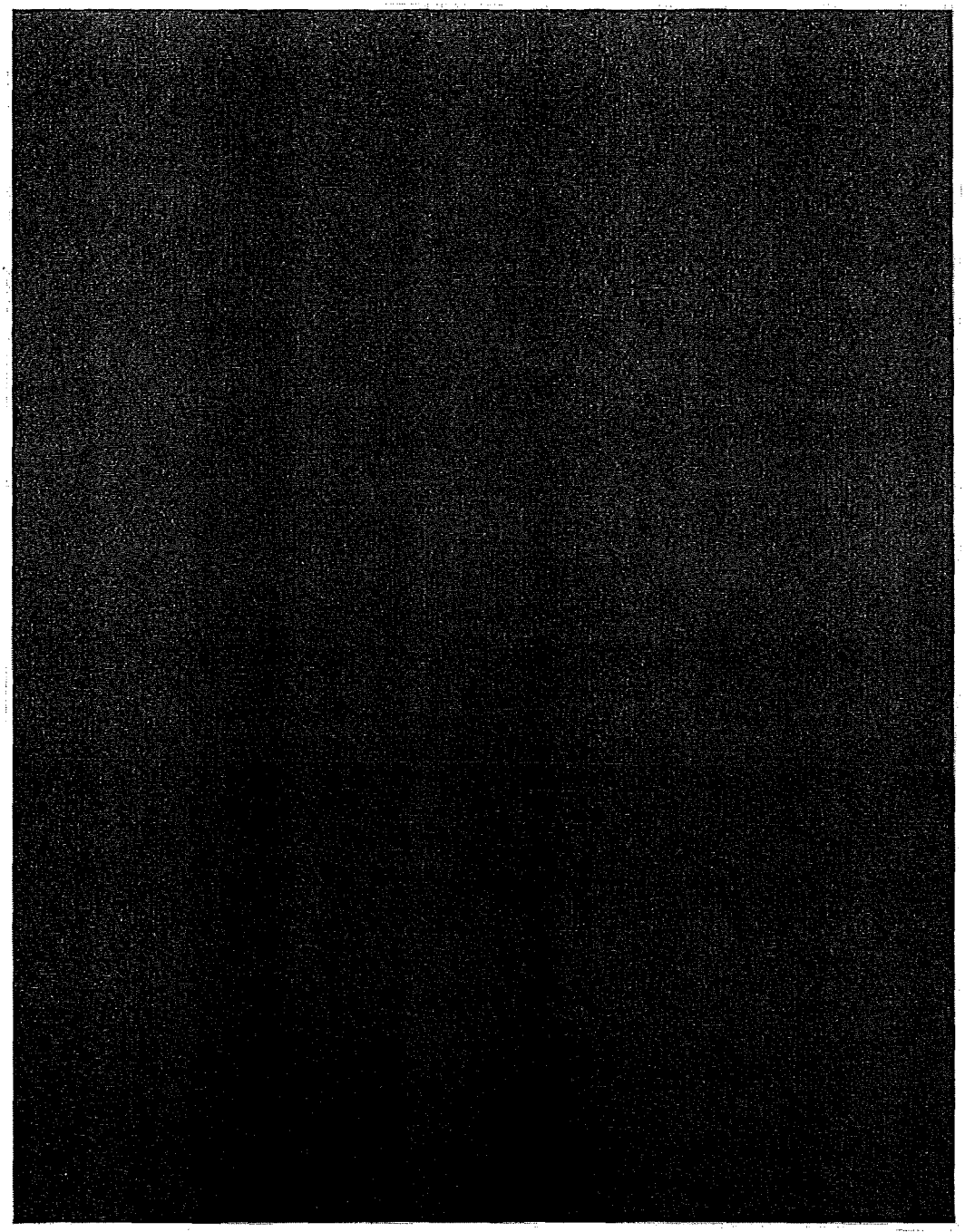
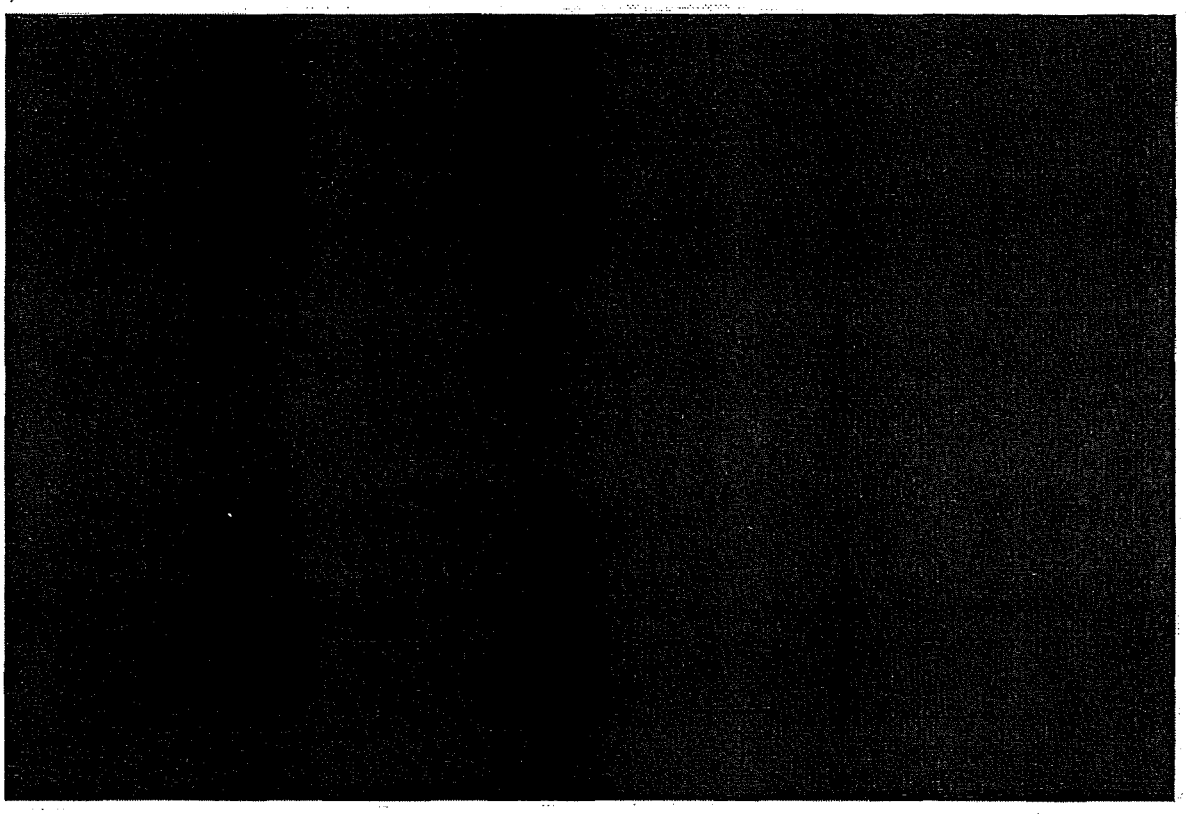


Die [redacted] aus obiger Abbildung zum Beispiel für eine Schnittstellendefinition enthält folgende Bestandteile:

[redacted]



5g)	Beschreiben Sie, wie das von Ihnen gelieferte System eine sichere Kommunikation gemäß Kapitel 2.5.4.B und 2.5.4.C gewährleistet. (nicht länger als 500 Wörter)

Die Justiz setzt für die elektronische Kommunikation aktuell das OSCI-Transportprotokoll in der Version 1.2 ein. Dieses Protokoll definiert die Mechanismen für die Erreichung der geforderten Sicherheitsziele (Vertraulichkeit, Integrität, Authentizität, Nichtabstreitbarkeit, Zurechenbarkeit, Ende-zu-Ende-Verschlüsselung). In dieser Version findet keine Kommunikation zwischen OSCI-Intermediären untereinander statt. Jedem Empfänger ist ein eigener „Heim"-Intermediär zugeordnet, der dessen OSCI-Postfach verwaltet und an den Absender ihre Nachrichten schicken.

[redacted] Daher wird im Weiteren von einer OSCI 1.2 basierten Kommunikation mit der Justiz ausgegangen. Im Rahmen einer späteren Migration müssen die Kommunikationsadapter von OSCI 1.2 auf OSCI 2 umgestellt werden. Da die Software [redacted] bereits beide Standards unterstützt und ein Parallelbetrieb innerhalb einer Serverinfrastruktur möglich ist, ist eine eventuell notwendige Migration auf OSCI 2 zu einem späteren Zeitpunkt gut durchführbar.

Für die Realisierung der Kommunikation zwischen Rechtsanwälten und der Justiz gemäß den Vorgaben des „Elektronisches Gerichts- und Verwaltungspostfach (EGVP)" stellt der Auftragnehmer eine Instanz [redacted] zur Verfügung. Diese Instanz fungiert als „BRAK-Intermediär". Er stellt die erforderlichen Postfächer für die teilnehmenden Rechtsanwälte zur Verfügung und wird entsprechend als Ziel-Intermediär jedes Rechtsanwalts in die S.A.F.E.-Instanz der BRAK eingetragen, so dass Nachrichten der Justiz an Anwälte an die Postfächer dieses Intermediärs gesendet werden. Der Versand von Nachrichten der Anwälte an die Justiz in umgekehrter Richtung erfolgt an die Postfächer der Justiz-Intermediäre. [redacted] So bekommt der Sender einer Nachricht nach der erfolgreichen Einreichung beim Intermediär zunächst eine Bestätigung, die im Nachrichtenjournal vermerkt wird. Um festzustellen, ob ein Empfänger die Nachricht vom Intermediär abgeholt und den Empfang quittiert hat, muss der Sender also den zugehörigen Laufzettel abrufen und prüfen. Entsprechendes gilt umgekehrt für den Empfang von Nachrichten, wobei durch Abrufen der Laufzettelliste (in diesem Fall vom BRAK-Intermediär) ermittelt werden muss, ob neue Nachrichten vorliegen, die dann ggf. abgeholt werden. Jede Änderung des Status einer Nachricht wird im Nachrichtenjournal vermerkt. Im Fall des Scheiterns einer Zustellung wird eine Systemnachricht in dem besonderen Anwaltspostfach des Absenders erzeugt, die in seiner Nachrichtenübersicht erscheint.

Die Umsetzung dieser Aufgaben wird im Detail maßgeblich auch von Performanz-Aspekten bestimmt. Da mit einer großen Zahl von Teilnehmern des Systems gerechnet wird, sollten Laufzettel des BRAK-Intermediärs [redacted]

Da der BRAK-Intermediär mit dem System in einem Vertrauensverhältnis steht und voraussichtlich in derselben Umgebung installiert sein wird, können diese Zugriffe relativ gut optimiert werden. Die Überprüfung des Empfangsstatus einer an die Justiz versand-

ten Nachricht dagegen sollte [redacted]

[redacted]

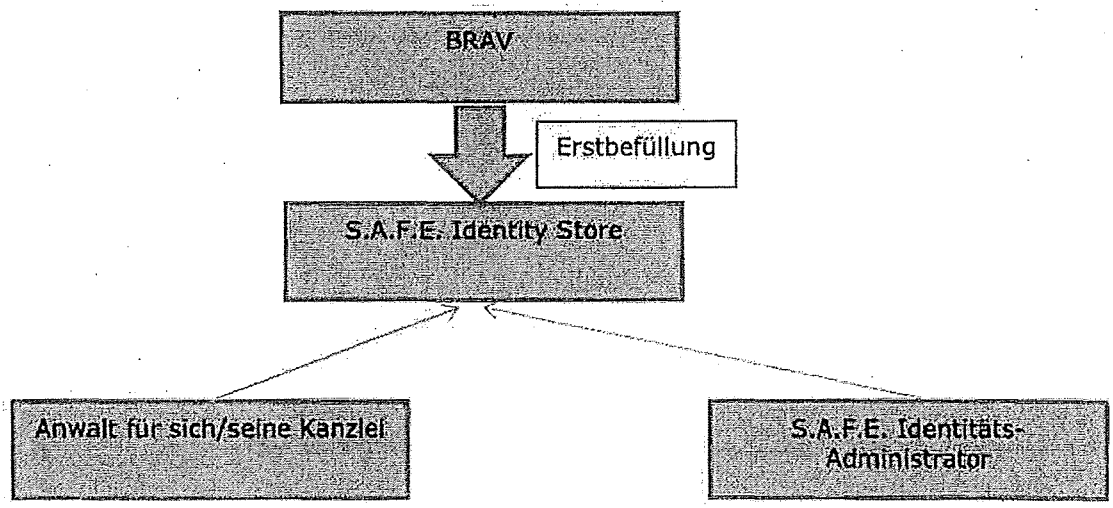
Mit dem [redacted] steht für die Lösung dieser Aufgaben ein Produkt zur Verfügung, für das [redacted]

5h)	Beschreiben Sie, wie das von Ihnen gelieferte System Daten in die S.A.F.E.-Infrastruktur integriert und wie sichergestellt wird, dass Rechtsanwälte von der Justiz gefunden und adressiert werden können. (siehe Kapitel 2.5.5.B) (nicht länger als 500 Wörter)

Nachfolgend beschreibt der Auftragnehmer die Datenintegration sowie das Auffinden und die Adressierung von Rechtsanwälten.

Datenintegration

Über den [redacted] gelangen die Daten für die bei der BRAK verwalteten digitalen Identitäten in deren S.A.F.E.-System. Dabei ist zu unterscheiden zwischen einer „Erstbefüllung" und nachfolgenden Ergänzungen bzw. Änderungen oder Löschungen. Für die Erstbefüllung wird ein Migrationsprogramm erstellt, das die zu einem Stichtag im BRAV vorhandenen Daten zu Anwälten in den neuen Identity Store der BRAK überführt. Diesen Anwälten wird dann eine Webschnittstelle und parallel ein Webservice für evtl. vorhandene Kanzleisoftware bereitgestellt, mit der sie Mitarbeiter mit erlaubten Attributen aufnehmen oder eigene Daten ändern/löschen können. Hierzu sind die Standard-Sicherheitsvorkehrungen des S.A.F.E.-Konzepts (siehe aktuelles Fachkonzept der Justiz) zu beachten. Weiterhin haben Mitarbeiter der Kammern als „Identitätsadministratoren" über ihre Kammersoftware die Möglichkeit, Daten zu Identitäten über ihre Kammersoftware hinzuzufügen bzw. zu bearbeiten. Die Einrichtung von Vertretern z. B. ist alleine ihnen vorbehalten.



Darstellung Datenintegration

Auffinden und Adressierung

Will die Justiz einen Anwalt bzw. eine Kanzlei oder eine Kammer über das EGVP-System adressieren, benötigt sie deren OSCI-Adresse sowie Verschlüsselungszertifikat, damit sie die Nachricht für den Empfänger verschlüsseln und an den richtigen OSCI-Intermediär (in diesem Fall den der BRAK) übermitteln kann.

Hierzu sucht das EGVP der Justiz zunächst im Virtuellen Attribute Service (VAS) von S.A.F.E. nach der im gesamten Verbund eindeutigen S.A.F.E.-ID des gewünschten Empfängers. Der VAS wiederum greift nacheinander auf die Attribute Services (AS) des S.A.F.E.-Systems der Justiz, der BNotK und der BRAK zu, bis er die Identität gefunden hat. Das EGVP erhält vom eigenen S.A.F.E.-System ein (signiertes!) SAML-Token zur Au-

thentifizierung und Autorisierung beim AS der BRAK. Nach dessen positiver Prüfung gibt der AS der BRAK die benötigten Daten zur S.A.F.E.-ID an das anfragende EGVP heraus.

Das oben Beschriebene funktioniert auf folgender Grundlage. Die Prüfung bei der BRAK ist möglich, weil sie eine Vertrauensvereinbarung mit der Justiz zur Föderierung der beiden „Trust Domains" abgeschlossen haben muss. In diesem Zusammenhang müssen auch die Zertifikate für die jeweiligen Signaturen der beiden Systeme in den SAML-Token ausgetauscht werden. Das S.A.F.E. der BRAK verwaltet den enthaltenen öffentlichen Schlüssel der Justiz.

Das EGVP verschlüsselt nun die Nachricht mit dem öffentlichen Schlüssel des Empfängers und sendet sie an den Intermediär der BRAK.

5i)	Beschreiben Sie, wie das von Ihnen gelieferte System Rechtsanwälten ermöglicht, Kommunikationspartner innerhalb der S.A.F.E.-Infrastruktur zu adressieren. (siehe Kapitel 2.5.5.A, B) (nicht länger als 500 Wörter)

Die Integration der S.A.F.E-Domänen der Justiz und der BRAK ermöglicht es, dass Rechtsanwälte von der Justiz adressiert werden können. Der Justiz wird es ebenfalls möglich sein, die Rechtsanwaltskammern zu erreichen.

Der Auftragnehmer wird auf Basis des Software-Produkts [redacted] eine zum S.A.F.E.-Konzept der deutschen Justiz kompatible S.A.F.E.-Domain BRAK erstellen.

Das S.A.F.E.-Konzept beschreibt Schnittstellen Datenformate und Standards zum Aufbau eines Föderierten Identity-Management und Verzeichnisdienst/Attribute-Service (AS). Der AS dient als ein Verzeichnis aller möglichen Kommunikationspartner inklusive notwendiger Kommunikationsparameter und Verschlüsselungszertifikate. Im Rahmen der Föderation können die Identitäten in unterschiedlichen S.A.F.E.-Instanzen hinterlegt sein. Im Kontext der Kommunikation zwischen Anwälten und der Justiz verteilen sich die Identitäten auf mindestens zwei S.A.F.E.-Instanzen (BRAK und Justiz). Eine weitere Instanz befindet sich aktuell bei der Bundesnotarkammer im Aufbau.

Um die komfortable Suche über alle S.A.F.E.-Instanzen zu erlauben, beschreibt das S.A.F.E.-Konzept den Virtuellen Attribut Service. Dieser nimmt Suchanfragen entgegen und leitet diese an die an den VAS angeschlossene S.A.F.E.-Instanzen weiter. Die S.A.F.E-Instanzen stehen hierfür in einer Vertrauensbeziehung untereinander. Die S.A.F.E.-Instanz der BRAK muss dieser Vertrauensinstanz hinzugefügt werden.

Will ein Rechtsanwalt (bzw. Mitarbeiter) einen Kommunikationspartner elektronisch erreichen, nutzt er/sie das im beA-System integrierte Adressbuch. Über dieses Adressbuch ist die Suche nach Kommunikationspartnern innerhalb der S.A.F.E.-Infrastruktur möglich. Dabei werden dem Nutzer die Optionen angeboten

- nur innerhalb der S.A.F.E.-Domain BRAK oder
- über den VAS Kommunikationspartner innerhalb anderer S.A.F.E.-Domänen zu suchen.

Die gefundenen Adressen können in ein lokales Adressbuch und eine Favoritenliste übernommen werden.

Beim Versenden jeder Nachricht werden die Kommunikationsparameter über die S.A.F.E.-Infrastruktur auf Aktualität überprüft.

Für die Erreichbarkeit der Rechtsanwaltskammern durch die Justiz werden im beA-System sogenannte „Organisationspostfächer" vorgesehen. Wie auch die regulären beA-Postfächer für Anwälte haben diese Postfächer einen Postfachbesitzer und entsprechend für die Nutzung freigeschaltete Mitarbeiter der Rechtsanwaltskammern. Organisationspostfächer sind nicht fest mit einem Postfachbesitzer verknüpft, dieser kann ggf. durch eine andere Person ausgetauscht werden.

5j)	Beschreiben Sie, wie Sie das BRAV als führenden Verzeichnisdienst durch die S.A.F.E.-Domain ablösen werden. Gehen Sie hierbei vor allem darauf ein, wie sichergestellt wird, dass das BRAV als Weboberfläche weiterhin für die Suche im Verzeichnis erhalten bleibt. (siehe Kapitel 2.5.5.E) (nicht länger als 500 Wörter)

Der Identity Store im S.A.F.E. BRAK ist in Zukunft der einzige Ort, an dem die Daten zu den Anwälten gespeichert werden. Deshalb wird der Auftragnehmer ein Migrations-Programm erstellen, das zu einem Stichtag sämtliche Daten aus dem aktuellen BRAV ausliest und zu S.A.F.E. migriert. [redacted]

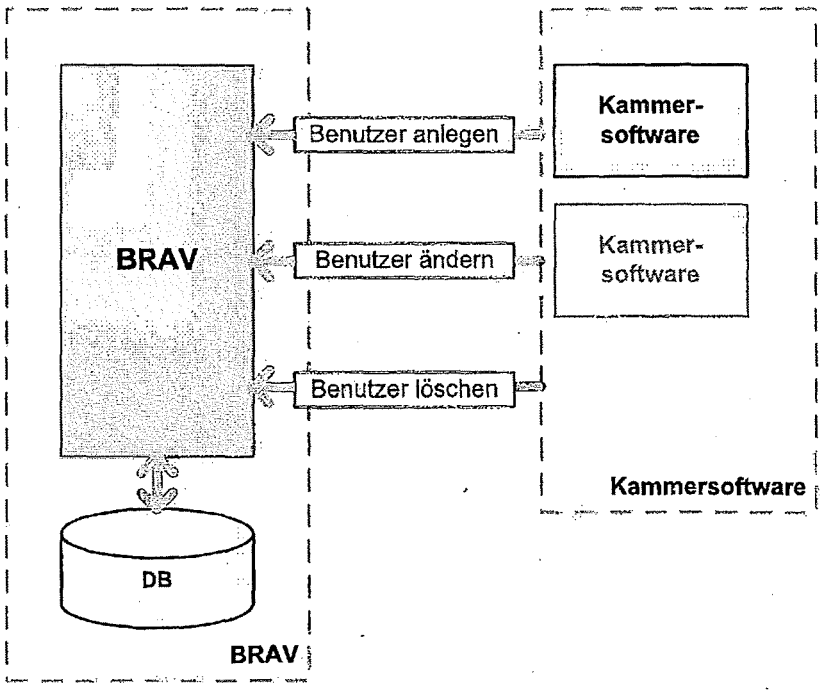
Die Suche nach Anwälten und deren Attributen soll weiterhin über die Oberfläche (Fassade) des BRAV erfolgen. Mit der BRAK ist deshalb beim Feinkonzept abzustimmen, ob alle zugelassenen Nutzer dieser Fassade dieselben Leserechte bzgl. der Anwaltsdaten besitzen. Im einfachsten Fall muss dann nur diese sich am S.A.F.E. der BRAK authentifizieren, um Zugriff auf den Attribute Service (AS) zu erhalten. [redacted]

Auch die Kammersoftware kann fachlogisch auf analoge Weise [redacted] Lediglich die technischen Schnittstellen variieren. Details sind im Rahmen des Feinkonzepts mit den Lieferanten der Kammersoftware und den Kammern abzustimmen.

Die Schnittstelle zur Fassade des BRAV ist ebenfalls abzustimmen. Für Suchen im Verzeichnis der Anwälte, die über die Fassade des BRAV erfolgen, ergeben sich somit keine Änderungen.

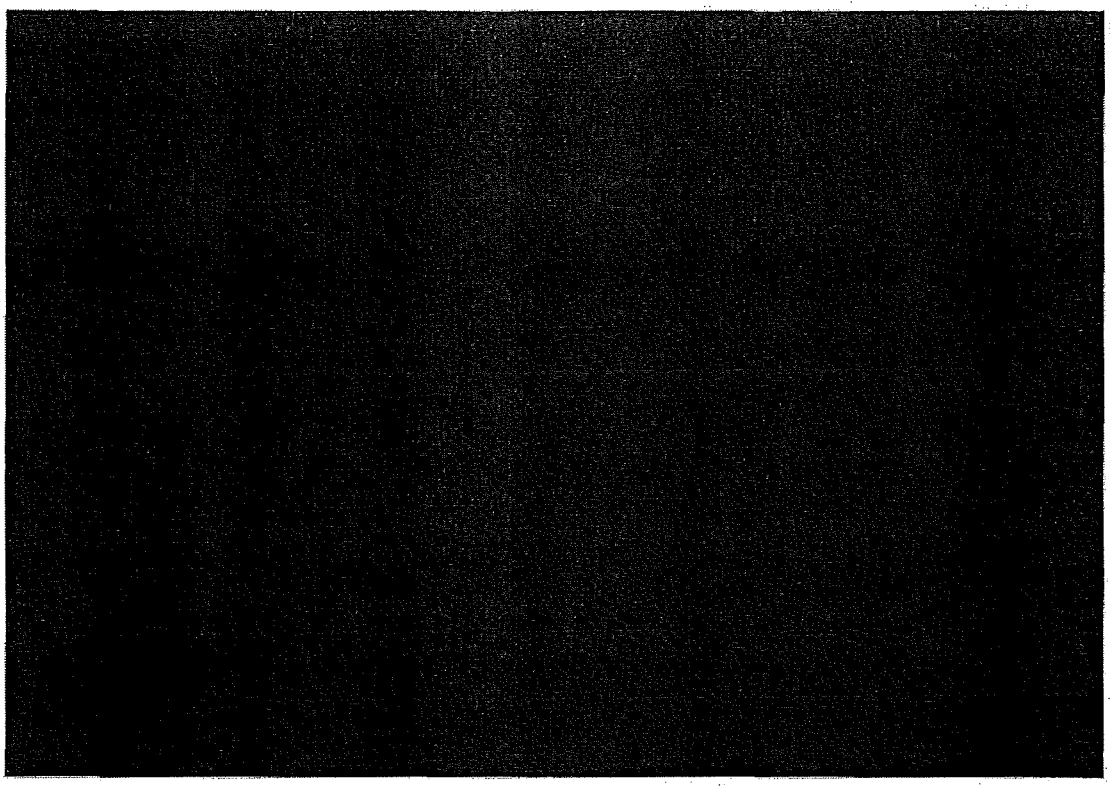
5k)	Beschreiben Sie, wie sie sicherstellen, dass Daten zu Rechtsanwälten, Vertretern, Zustellungsbevollmächtigten und Abwicklern, die über die zwei aktuell im Einsatz befindlichen Kammersoftwareprodukte angelegt, gelöscht oder geändert wurden, in das von Ihnen gelieferte System übergeben werden. Ablaufdarstellungen sind erwünscht. (siehe Kapitel 2.5.5.F) (nicht länger als 500 Wörter)

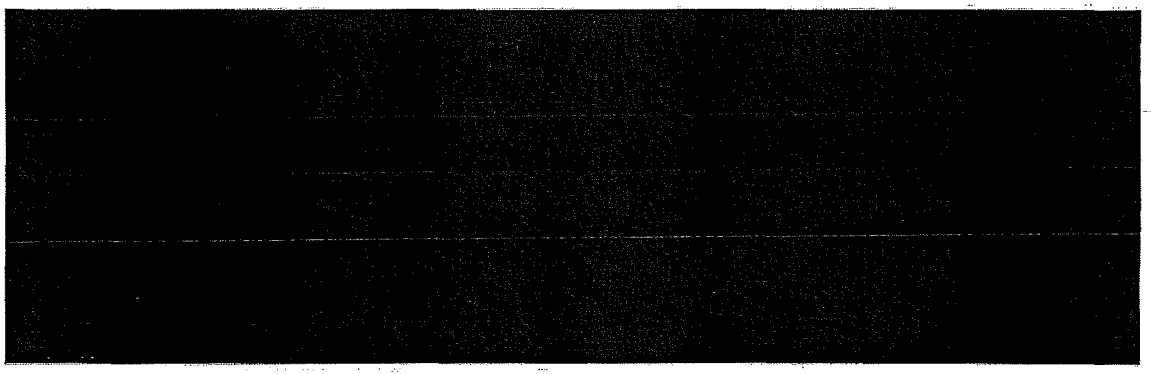
Die beiden aktuell im Einsatz befindlichen Kammersoftwaren besitzen eine Schnittstelle zum BRAV-System. Das BRAV soll durch die S.A.F.E.-Domäne als führendes System abgelöst werden. Änderungen an den Stammdaten oder z. B. Vertretungsregeln, die innerhalb der Kammersoftware durchgeführt werden, müssen sich zukünftig sowohl im Datenbestand der S.A.F.E.-Domäne, als auch in den Postfächern und Berechtigungen widerspiegeln.



Abgleich Prozess heute

Die Realisierung wird in Form [redacted] erfolgen. Dieser [redacted]





Das System legt automatisch neue beA-Postfächer für hinzugefügte Rechtsanwälte an. Sollten neu Bestellte/Benannte noch über kein persönliches Postfach verfügen, wird auch dieses automatisch auf der Basis der Daten aus der S.A.F.E.-Meldung (Webservice-Aufruf) angelegt.

Wird ein Rechtsanwalt innerhalb der Kammersoftware gelöscht, deaktiviert das System das entsprechende Postfach.

5l)	Beschreiben Sie, wie die Autorisierung und Authentifizierung der Benutzer im System erfolgen soll. (siehe Kapitel 2.5.5.H) (nicht länger als 500 Wörter)

Authentifizierung

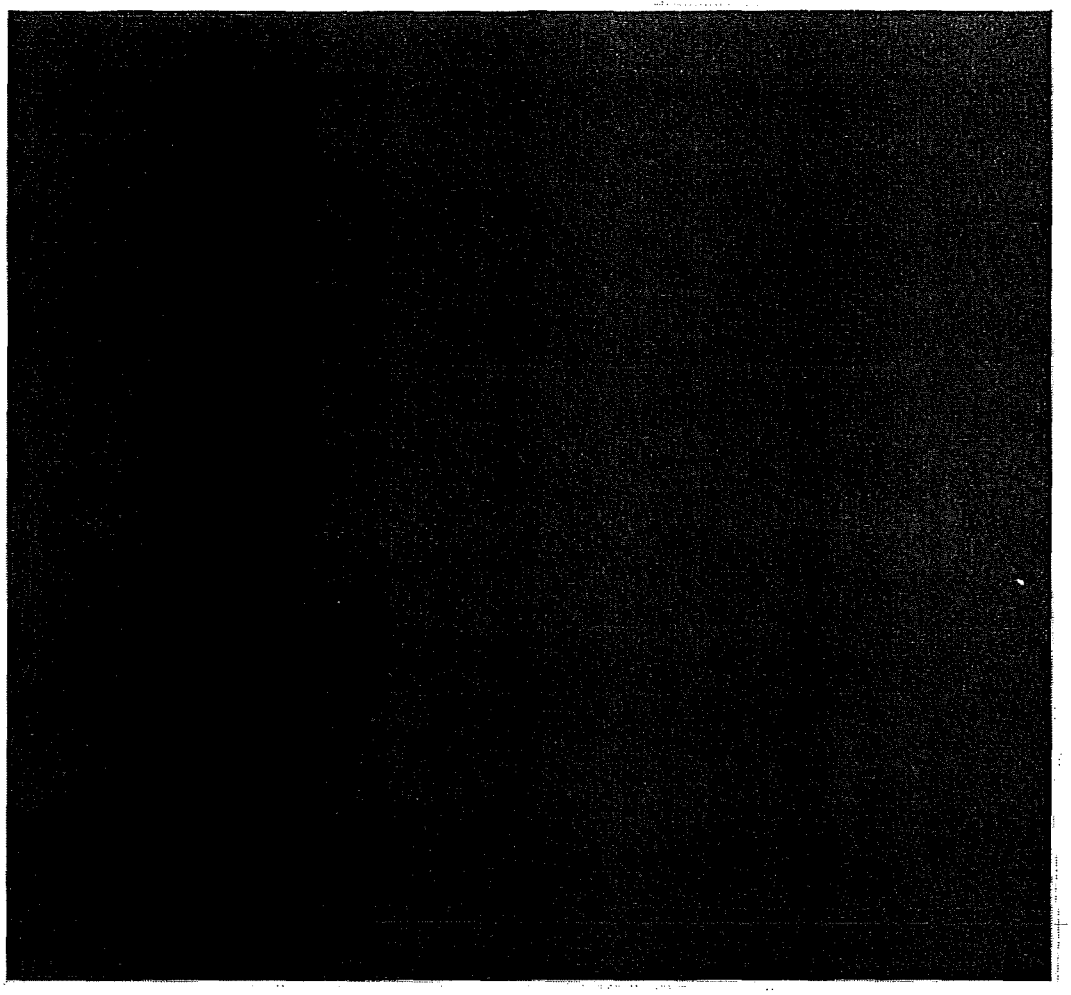
Für die Authentifizierung kommt das Produkt [redacted] zum Einsatz. Dieses unterstützt folgende Authentifizierungsverfahren:

- einfache Authentifizierung durch Benutzername und Passwort
- zertifikatsbasierte Authentifizierung mit Hilfe von Schlüsseldateien (p12 / pfx-Dateien) und PIN
- zertifikatsbasierte Authentifizierung mit Hilfe von Signaturkarten
- Authentifizierung durch den neuen Personalausweis
- Authentifizierung durch von anderen S.A.F.E.-Instanzen ausgestellten SAML-Token
- weitere je nach Bedarf über zusätzliche Konnektoren

[redacted] wird von der Webanwendung des besonderen Anwaltspostfachs über [redacted] angesprochen.

[redacted]

Für eine einfache Nutzername/Passwort- Authentifizierung [redacted]



[redacted] Externe Systeme wie Kanzleisoftware-Clients müssen ihre Nutzer auf demselben Wege authentifizieren.

Authentifizierungen mit Hilfe von Zertifikaten bzw. Privatschlüsseldateien, Signaturkarten oder dem neuen Personalausweis laufen nach demselben Prinzip ab. [redacted]

Somit können alle im Zusammenhang mit dem besonderen elektronischen Anwaltspostfach derzeit in Betracht kommenden Authentifizierungsvarianten abgebildet werden. Ergänzungen sind durch die Architektur von [redacted] später leicht möglich.

Autorisierung

Nach der Authentifizierung durch die beschriebenen Mechanismen übernimmt die beA-Anwendung die Autorisierung des Benutzers im System. Hierzu werden die über den SAML-Response gelieferten Informationen ausgewertet. Zusätzlich werden die für den angemeldeten Benutzer hinterlegten Rollen- und Rechteinformationen ausgewertet.

Die Rechten für einen Benutzer werden einerseits fest über die Rolle vergeben, können andererseits auch über die Administration um weitere Rechte ergänzt werden. Rechte beziehen sich immer auf ein Postfach, hat ein Benutzer Zugriff auf mehrere Postfächer, müssen seine Rechte pro Postfach entsprechend vergeben werden.

Zuständig für die Ergänzung der Rechte auf unterschiedliche Postfächer im beA-System sind die Systemverwalter, welche die unterschiedlichen Benutzertypen administrieren können.

Darüber hinaus können z. B. Rechte auf ein Postfach über eine dezentrale Administration von einem Postfachbesitzer für seine administrierten Mitarbeiter vergeben werden.

6)	Fassen Sie die wesentlichen Eckpunkte Ihrer Lösung für den Anforderungsbereich „Informationssicherheit" kurz (nicht länger als 500 Wörter) zusammen.

Die konzipierte Lösung berücksichtigt die besonderen Anforderungen des Aufraggebers an die Sicherheitsziele Vertraulichkeit, Integrität, Authentizität, Nichtabstreitbarkeit, Zurechenbarkeit und Identifizierung durch den Architekturentwurf und die gewählten Rahmenbedingungen für die Implementierung. Ein stabiles Reaktionsverhalten des Systems bei hoher Belastung sowie die Minimierung des Datenverlustes bei kritischen Störungen sind weitere Design-Kriterien.

Besonders hervorzuheben ist in diesem Zusammenhang die Verfügbarkeit der Hardware Security Module als zentrale Komponente für die Schlüsselverwaltung der Postfächer. Durch die besondere Architektur unterstützen die angebotenen HSMs Funktionalitäten, wie [redacted] Um den besonderen Anforderungen des beA gerecht zu werden, sind in dem Angebot vier HSMs enthalten, die in verteilten Sicherheitsbereichen eingesetzt werden sollen. Damit ist ein Höchstmaß an Sicherheit und Verfügbarkeit gegeben.

Die MTBF (mean time between failures) für einen einzelnen HSM beträgt [redacted] Stunden. Der in diesem Angebot zugrundeliegende Servicelevel für die HSMs ist der höchste Support-Level, „Geschäftskritisch". MTTR in der folgenden Tabelle steht für mittlere Wiederherstellungszeit (Mean Time to Repair, MTTR).

[redacted]

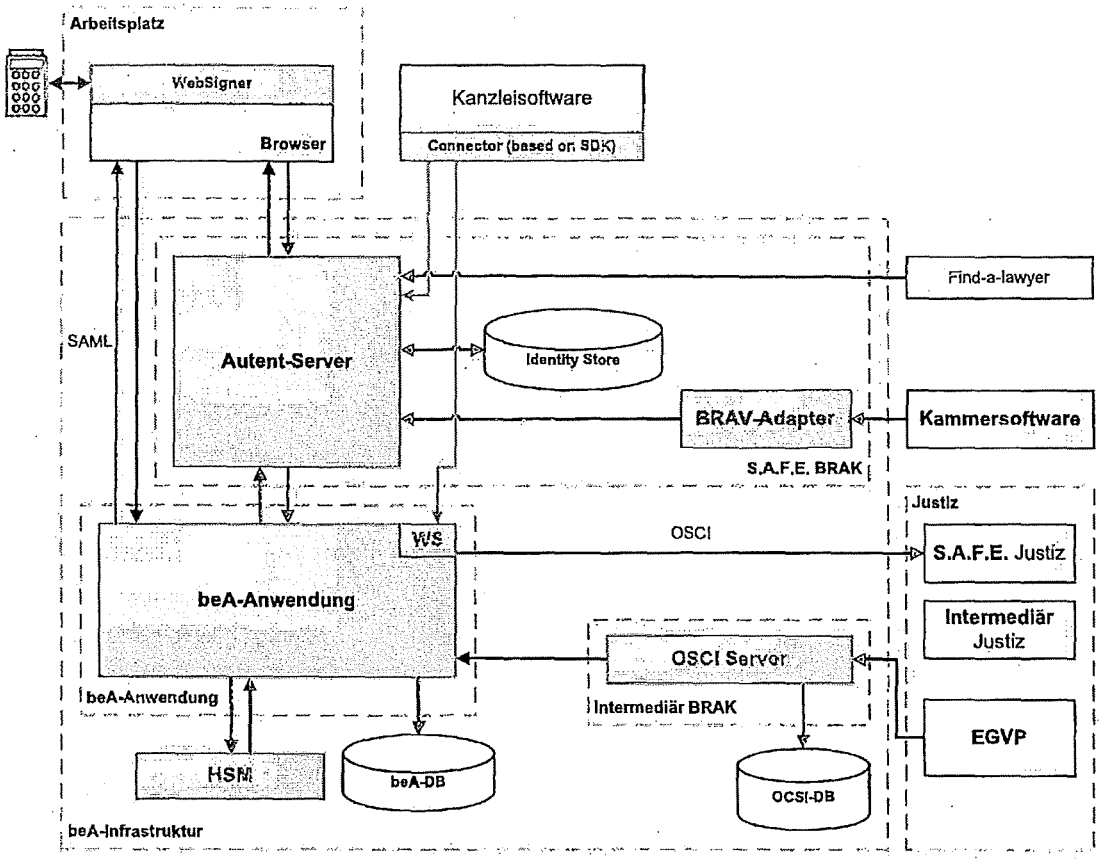


Abbildung Lösung Informationssicherheit

Die Vertraulichkeit der Informationen wird durch die Ende-zu-Ende-Verschlüsselung von Inhalts- und Nutzdaten während des Transportes und der Speicherung gewährleistet. Als Verschlüsselungsalgorithmus kommt AES mit einer Schlüssellänge von mindestens 256 Bit zum Einsatz. Die beA-Datenbank ist das Herzstück der Anwendung für die Speicherung von Inhalts- und Nutzdaten. Als Datenbank kommt [redacted] zum Einsatz. Über die Aufgabentrennung bei der Datenbankverwaltung und -nutzung in Verbindung mit der Verschlüsselung einzelner Tabellen und Tablespaces wird ein unberechtigter Zugriff bzw. eine unberechtigte Kenntnisnahme von Inhalten verhindert.

Die Integrität sowohl der Inhaltsdaten als auch der Nutzdaten bei der Speicherung und Übertragung wird durch das Anbringen von persönlichen als auch technischen Signaturen bei der Erstellung der Daten überprüfbar gemacht. Die angebotene Lösung berücksichtigt sowohl den Integritätsschutz mittels einer qualifizierten elektronischen Signatur z. B. beim Versand einer Nachricht als auch mittels technischer Signaturen.

Die Überprüfung der Integrität der Journale gegenüber Manipulationen sowohl durch die Benutzer als auch durch die Systemverwalter wird durch das Anbringen von technischen Signaturen u.a. in Form von Zeitstempeln gewährleistet. Die Zeitstempel werden über die [redacted] bezogen. Die Erstellung der Zeitstempel erfolgt entweder durch das [redacted] selbst (fortgeschrittene Zeitstempel). Oder sie muss bei qualifizierten Zeitstempeln durch Dienstanbieter erfolgen. Im [redacted] können qualifizierte Zeitstempel von allen Dienstanbietern konfiguriert werden. Bei der Einbindung von externen Dienstanbietern können ggf. entsprechende Betriebskosten entstehen.

Die Prüfung der Authentizität eines Benutzers erfolgt bei der Anmeldung an der beA-Infrastruktur in mehreren Stufen. Clientseitig erfolgt eine Zweifaktor-Authentisierung

mittels User-Zertifikat (Soft-PSE), Smartcard oder Personalausweis gegenüber der beA-Anwendung. Daraufhin wird mittels SAML-Token eine Autorisierung am Autent-Server der S.A.F.E. BRAK eingeleitet. Ist die Autorisierung erfolgreich, so erhält der Benutzer über die Rechteverwaltung der beA-Anwendung die der hinterlegten Rolle zugewiesenen Rechte.

Die Rechteverwaltung in der beA-Anwendung folgt einem hierarchischen Modell mit Vererbungsregeln und Gültigkeitszeiträumen. Dabei gelten Rechte für einen Benutzer in einer Rolle nur so lange, wie die Rechte des übergeordneten Benutzers gelten, welcher die Rechte vergeben hat.

Bezogen auf die Nichtabstreitbarkeit sowohl in Bezug auf die Autorenschaft einer Nachricht als auch auf den Kommunikationsvorgang wird das System so konzipiert, dass Aktivitäten der Nutzer mit Nutzer-ID, Datum und Uhrzeit für das Anlegen, Bearbeiten, Löschen, Exportieren, Drucken sowie das Versenden und den Empfang von Nachrichten in entsprechenden Journalen protokolliert werden. Für die Aktivitäten von Systemverwaltern (Anwendungsadministratoren) werden gesonderte Logdaten erhoben, die die Aktivitäten über den gesamten Zeitraum der Anmeldung protokollieren.

Bezogen auf die Zurechenbarkeit in den Bereichen Zugriffskontrolle, Beweissicherung bzw. Protokollierung sowie zeitliche Bestimmtheit wird das System so ausgelegt, dass Aktivitäten von Benutzern grundsätzlich mit ihren Metadaten protokolliert werden. Versuche von Benutzern, auf Daten zuzugreifen, auf die sie keine Berechtigungen haben, oder Daten unberechtigterweise zu manipulieren [redacted]

Der Auftragnehmer beachtet uneingeschränkt alle zur Erbringung der mit dem Auftraggeber vereinbarten Dienstleistungen relevanten Vorschriften des Bundesdatenschutzgesetzes.

6a)	Beschreiben Sie, wie das von Ihnen gelieferte System die Erfüllung der in 2.6.1.A, B beschriebenen Sicherheitsziele sicherstellt. (bis zu 1.000 Wörtern)

Das gelieferte System erfüllt die in 2.6.1.A, B beschriebenen Sicherheitsziele wie folgt:

- Die **Vertraulichkeit** sowohl von Inhaltsdaten als auch von Nutzungsdaten wird durch die Verschlüsselung der jeweiligen Daten mittels symmetrischen Schlüssels AES 256 Bit erreicht.
  - Inhalts- und Nutzungsdaten werden grundsätzlich auf Datenbankebene gespeichert. Als Datenbank kommt [redacted] zum Einsatz.

    [redacted]

    Inhaltsdaten, die der Anforderung einer Ende-zu-Ende Verschlüsselung unterliegen, sind zusätzlich durch einen symmetrischen Transportschlüssel vom Absender bis zum berechtigten Empfänger geschützt. Der symmetrische Transportschlüssel wird mittels asymmetrischer Verschlüsselung mit dem öffentlichen Schlüssel des Postfaches bzw. des berechtigten Empfängers auf dem Transportweg geschützt.
  - Der Verbindungsaufbau eines Web-Clients bzw. einer Kanzleisoftware zur beA-Infrastruktur erfolgt mittels [redacted] entsprechend den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik[9] (BSI). Beim Verbindungsaufbau wird der symmetrische AES-Schlüssel ausgehandelt.
  - Die Kommunikation zu den Drittsystemen wie Kanzleisoftware, Kammersoftware oder Find A Lawyer wird [redacted] abgesichert (s. o.). Die Anbindung an die Justiz (EGVP) verwendet die im OSCI 1.2-Transportprotokoll festgelegten Verschlüsselungsalgorithmen (zzt. AES-256/512 in Verbindung mit RSA, Schlüssellänge mind. 2048 Bit). OSCI verwendet das Prinzip des doppelten Umschlags, bei dem die Inhaltsdaten doppelt, die Nutzungsdaten einfach verschlüsselt übertragen werden.
- Die **Integrität** sowohl der Inhaltsdaten als auch der Nutzungsdaten bei der Speicherung und Übertragung wird durch das Anbringen von persönlichen als auch technischen Signaturen bei der Erstellung der Daten überprüfbar gemacht werden. Die angebotene Lösung berücksichtigt sowohl den Integritätsschutz mittels einer qualifizierten elektronischen Signatur z. B. beim Versand einer Nachricht als auch mittels technischer Signaturen. Beim Export von Nachrichten und Anhängen werden diese auf vorhandene Signaturen geprüft. Diese bleiben beim Export erhalten. Nachrichten und Anhänge ohne vorhandene Signaturen werden mit einer technischen Signatur der beA-Anwendung versehen.

[9] Mindeststandard des BSI nach § 8 Abs. 1 Satz 1 BSIG für den Einsatz des SSL/TLS-Protokolls in der Bundesverwaltung

Die konkreten Ausprägungen der Nutzung der technischen Signaturen werden in der Feinspezifikation festgelegt.

Die Überprüfung der Integrität der Journale gegenüber Manipulationen [redacted] Bei der Einbindung von externen Dienstanbietern können ggf. entsprechende Betriebskosten entstehen.

- Die Prüfung der **Authentizität** eines Benutzers erfolgt bei der Anmeldung an der beA-Infrastruktur in mehreren Stufen. Clientseitig erfolgt eine Zwei-Faktor-Authentifizierung mittels Smartcard oder Personalausweis (zukünftig) gegenüber der beA-Anwendung. Daraufhin wird mittels SAML-Token eine Authentifizierung am Auth-Server der S.A.F.E. BRAK eingeleitet. Ist die Authentifizierung erfolgreich, so erhält der Benutzer über die Rechteverwaltung der beA-Anwendung die der hinterlegten Rolle zugewiesenen Rechte.

  Sowohl Inhalts- als auch Nutzungsdaten, welche von einem berechtigten Benutzer erstellt bzw. verändert wurden, werden im Postfach mit einem Attribut gekennzeichnet, welches auf den berechtigten Benutzer verweist, der diese Daten erstellt oder zuletzt verändert hat. Die Historie jeder Nachricht wird in einem Nachrichtenjournal dokumentiert werden. Beim Versand von Inhalts- bzw. Nutzungsdaten werden diese, falls erforderlich, mit einer qualifizierten elektronischen Signatur bzw. einer technischen Signatur des Systems versehen, welche die Authentizität der Daten gegenüber dem Empfänger der Nachricht belegt.

- Das System muss die **Nichtabstreitbarkeit** sowohl in Bezug auf die Autorenschaft einer Nachricht als auch auf den Kommunikationsvorgang gewährleisten

  Das System protokolliert die Aktivitäten der Nutzer mit Nutzer-ID und Datum/Uhrzeit für das Anlegen, Bearbeiten, Löschen, Exportieren, Drucken sowie das Versenden und den Empfang von Nachrichten in entsprechenden Journalen. Die Journale werden mit einer technischen Signatur zum Schutz der Integrität der Inhaltsdaten versehen. Für die Aktivitäten von Anwendungsadministratoren werden gesonderte Logdaten erhoben, die die Aktivitäten über den gesamten Zeitraum der Anmeldung protokollieren. Das Logging von Aktivitäten von Systemadministratoren ist in Abhängigkeit von der Infrastruktur im Sicherheitskonzept des Betreibers festzulegen.

  Die Aufbewahrungsfrist dieser technischen Journale ist im Sicherheitskonzept festzulegen.

- Das System muss die **Zurechenbarkeit** in den Bereichen Zugriffskontrolle, Beweissicherung bzw. Protokollierung sowie zeitliche Bestimmtheit sicherstellen.

  Das System ist so ausgelegt, dass Aktivitäten von Benutzern grundsätzlich mit ihren Metadaten protokolliert werden. [redacted] Die konkrete Ausprägung solcher Systemevents ist in der Feinspezifikation zu definieren.

- Das System stellt sicher, dass jeder Benutzer eindeutig als eine natürliche Person identifiziert werden kann.

  Voraussetzung für eine Erstanmeldung (Registrierung) eines Postfachbesitzers sind gültige persönliche Daten, mit denen die Registrierungsinformationen übermittelt werden können (E-Mail-Adresse oder Postadresse). Außerdem benötigt der Benutzer für die erfolgreiche vollständige Registrierung ein gültiges Verschlüsselungszertifikat, ein gültiges Authentifizierungszertifikat und ein gültiges qualifiziertes Signaturzertifi-

kat, bei dem die Eigenschaft als Berufsträger in das Signaturzertifikat aufgenommen wurde.

Bei der Registrierung werden die Anmeldedaten mit dem qualifizierten Signaturschlüssel des potentiellen Postfachbesitzers signiert. Die Gültigkeit der Signatur und die Übereinstimmung der persönlichen Daten des Postfachbesitzers im Zertifikat mit den Antragsdaten ist hinreichender Beweis für den eindeutigen Nachweis als eine natürliche Person. Für die Nutzung des Postfaches muss sich der Postfachinhaber immer mit dem im System bei der Registrierung hinterlegten Authentifizierungsmerkmal anmelden.

Für die Erstanmeldung eines weiteren Benutzers ist die Registrierung des Benutzers durch einen bereits registrierten Postfachbesitzer/Benutzer erforderlich. Dem neuen Benutzer wird durch den Registrierungsprozess ein Link und ein Einmalpasswort zur Verfügung gestellt (siehe 3 a). Mit diesen Informationen ist der neue Benutzer in der Lage, die Erstanmeldung durchzuführen und die erforderlichen persönlichen Daten (siehe Antwort zur Frage 6c) zu hinterlegen. Für die Nutzung des Postfaches muss sich der Benutzer immer mit dem im System bei der Registrierung hinterlegten Authentifizierungsmerkmal anmelden.

Sind die clientseitigen Voraussetzungen zur Nutzung des neuen Personalausweises gegeben (Hardware, Software, Freischaltung der Authentifizierungsfunktion), kann dieser zur eindeutigen Identifizierung eines Benutzers genutzt werden. Sowohl für Kanzleisoftware als auch für den Webbrowser hat die Governikus KG Bausteine entwickelt und vom BSI zertifizieren lassen, die hierfür geeignet sind und genutzt werden sollen.

6b)	Beschreiben Sie, wie und mit welchen möglichen Authentifizierungsmitteln (Kapitel 2.6.2.A) sich ein Benutzer im von Ihnen gelieferten System authentifiziert und unter welchen Bedingungen er nicht mehr als authentifiziert angesehen wird (Kapitel 2.6.2.E), sodass die in Kapitel 2.6.1.A beschriebenen Sicherheitsziele eingehalten werden. Berücksichtigen sie bei Ihren Ausführungen sowohl die Nutzung über die Webanwendung als auch über eine Kanzleisoftware. (nicht länger als 500 Wörter)

Bevor der Benutzer auf ein beA-Postfach zugreifen kann, muss er sich bei der Anmeldung am System authentifizieren. Es werden unterschiedliche Authentifizierungsmittel unterstützt, wie es in [redacted] und S.A.F.E. üblich ist. Je nach Anwendungsumfeld können also unterschiedliche hohe Sicherheitsniveaus möglich sein. In S.A.F.E. wird standardmäßig gespeichert, mit welchem Niveau authentifiziert (und mit welchem registriert) wurde. Implementiert werden neben einem Kennwort Authentifizierungszertifikate (in Software oder mittels Signaturkarte) sowie der neue Personalausweis, was sich im [redacted] bewährt hat. Das Authentifizierungsmittel muss bei der Anmeldung/Registrierung dem Benutzer zugeordnet werden. Dies wird auch für die BRAK so realisiert.

Die geforderte Zwei-Faktor-Authentifizierung kombiniert in der Regel Besitz und Wissen (siehe auch http://de.wikipedia.org/wiki/Authentifikation), d. h. etwa den Besitz eines Privatschlüssels oder Ausweises mit dem Wissen der PIN, die zum Zugriff auf den Schlüssel erforderlich ist. Dies ist im Autent realisiert und wird so angeboten. Die Kombination von „zwei Wissen" (z. B. Kennwort und Sicherheitsfrage) ist möglich, wird aber nicht empfohlen.

Auf jeden Fall wird die geforderte Verschlüsselung zwischen Benutzer-Client und System so implementiert.

Hinweis: Die Authentifizierung über Signaturkarte oder Personalausweis erfordert die Ansprache des jeweiligen Kartenlesers direkt vom Benutzer-Client aus. Sowohl für als auch für den Webbrowser hat die [redacted] entwickelt und vom BSI zertifizieren lassen, die hierfür geeignet sind und genutzt werden sollen.

Technisch erfolgt die Authentifizierung des Benutzers im System durch die Mechanismen des SAML-Protokolls (Secure Authentication Markup Language), das in dem Produkt [redacted] umgesetzt ist. Da die Abläufe in der SAML-Spezifikation standardisiert sind, können auch Drittsoftwareanbieter (Kanzlei-, Kammersoftware) die Anmeldung ihrer Nutzer auf diesem Wege implementieren. Die gesamte Kommunikation – sowohl im Rahmen der Authentisierung als auch in der anschließenden Sitzung – wird über TLS unter Verwendung von Algorithmen und Schlüssellängen gemäß den jeweils aktuellen Empfehlungen des BSI abgesichert.

Nach einer erfolgreichen Authentifizierung wird zwischen Client und Server eine HTTP-Session eröffnet. Diese Session hat ein konfigurierbares Timeout, nach dem diese im Fall von Inaktivität beendet wird, so dass eine erneute Authentifizierung erforderlich wird. Eine bewusste Abmeldung eines Nutzers ist genauso über Browser oder Kanzleisoftware möglich, inkl. Bestätigung.

Bringt der Nutzer eine qualifizierte Signatur an einer Nachricht an, so muss er sich durch die Eingabe der Signaturkarten-PIN authentifizieren.

6c)	Skizzieren Sie, wie das erste Anmelden eines Benutzers im von Ihnen gelieferten System erfolgen wird. (siehe Kapitel 2.6.2.C) (nicht länger als 500 Wörter)

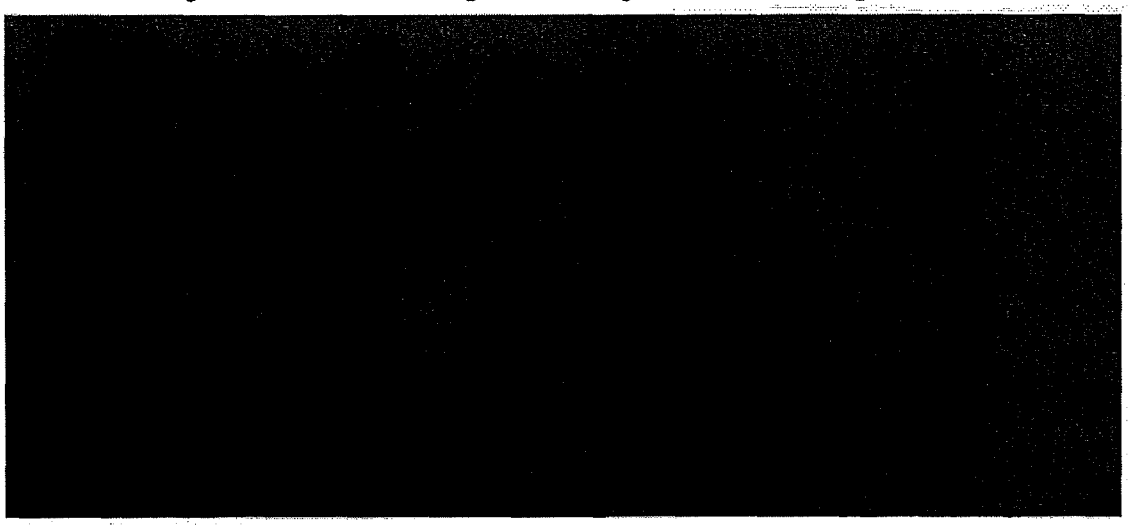
Ein Benutzerkonto bzw. ein Postfach befindet sich nach dem Anlegen im Zustand „vorbereitet aktiv". In diesem Zustand sind der öffentliche und der private Schlüssel des Postfaches generiert und der öffentliche Schlüssel mit dem zugehörigen Zertifikat in der S.A.F.E. BRAK hinterlegt. Damit sind die Voraussetzungen erfüllt, dass bei Postfächern der Zugang von Nachrichten möglich ist.

Das System setzt das Benutzerkonto bzw. das Postfach in den Zustand „vollständig aktiv", wenn die Rolle Postfachbesitzer mit einer berechtigten natürlichen Person verknüpft ist und diese berechtigte natürliche Person die Erstanmeldung erfolgreich durchgeführt hat.

Nach der Erstanmeldung (Registrierung) des Postfachbesitzers/Benutzers über die webbasierte Administrationsoberfläche der beA-Anwendung ist der Zugang zum beA-Postfach über Schnittstellen zum Web-Client, Kanzleisoftware, etc. möglich.

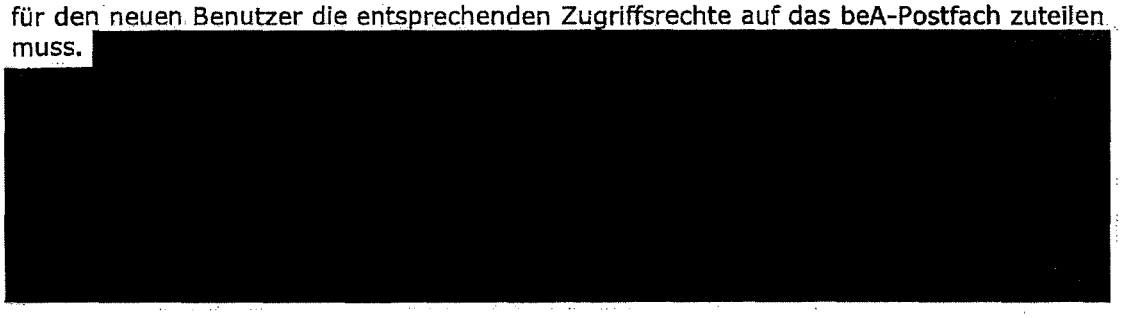
Erstanmeldung eines Postfachbesitzers

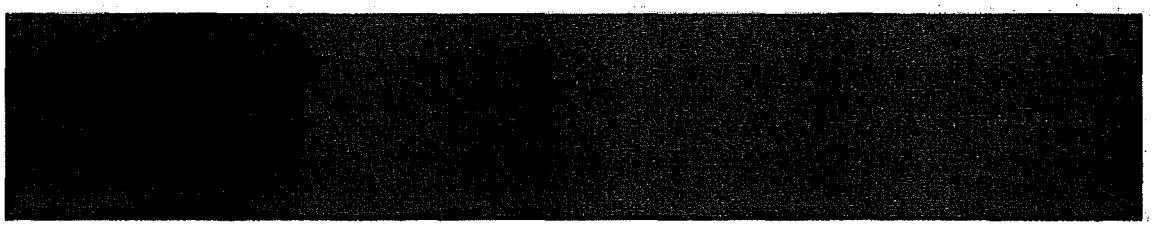
Voraussetzung für eine Erstanmeldung eines Postfachbesitzers sind gültige persönliche Daten (E-Mail-Adresse oder Postadresse), sowie ein gültiges Verschlüsselungszertifikat, ein gültiges Authentifizierungszertifikat und ein gültiges qualifiziertes Signaturzertifikat, bei dem die Eigenschaft als Berufsträger in das Signaturzertifikat aufgenommen wurde.



Erstanmeldung eines Benutzers

Der Postfachbesitzer oder ein anderer berechtigter Nutzer richtet einen neuen Benutzer über die Administrationsoberfläche der beA-Anwendung im Web-Browser ein, wobei er für den neuen Benutzer die entsprechenden Zugriffsrechte auf das beA-Postfach zuteilen muss.





6d)	Beschreiben Sie, wie das von Ihnen gelieferte System sicherstellt, dass Mitarbeiter von Vertretern der Zugriff auf das Postfach eines vertretenen Rechtsanwalts entzogen wird, wenn der Vertreter seine Rechte verliert. (siehe Kapitel 2.6.3.C) (nicht länger als 500 Wörter)

Die Rechteverwaltung in der beA-Anwendung folgt einem hierarchischen Modell mit Vererbungsregeln und Gültigkeitszeiträumen. Dabei gelten Rechte für einen Benutzer in einer Rolle nur so lange, wie die Rechte des übergeordneten Benutzers gelten, welcher die Rechte vergeben hat.

Werden die Rechte eines Vertreters auf ein Postfach entzogen, oder ist das Datum des Endes der Vertretung überschritten, wird in der Rechtverwaltung die Zuordnung des Vertreters auf das Vertretungspostfach gelöscht.

Damit erlöschen gleichzeitig alle von dem Vertreter abhängigen Rechte weiterer Benutzer auf das Vertretungspostfach. Diese Rechte werden ebenfalls gelöscht.

Die Vergabe und der Entzug der Rechte auf ein Postfach werden in den Systemprotokollen protokolliert.

Die Prüfung eines Rechtes auf Zugang zu einem Postfach und deren Inhalte erfolgt immer zum Zeitpunkt des Zugangs bzw. Zugriffs auf ein Objekt und entspricht dem Modell einer Positivliste. Objekte in diesem Sinn sind Postfächer, Ordner, beA-Nachrichten oder Inhalte von beA-Nachrichten.

6e)	Beschreiben Sie, wie ein nachweisbar manipulationsfreier und geheimer Nachrichtentransport von Ihrem gelieferten System gewährleistet wird und alle Sicherheitsziele bezüglich des Nachrichtentransportes gemäß Kapitel 2.6.1.A eingehalten werden. Gehen Sie dabei insbesondere auf die Situation ab 01.01.2018 ein. (siehe Kapitel 2.6.4.A - D) (bis zu 1.000 Wörtern)

Die geforderten Sicherheitsziele werden durch die etablierten kryptographischen Methoden der elektronischen Signatur und symmetrischer bzw. asymmetrischer Verschlüsselungen realisiert.

Die **Kommunikation zwischen Webanwendung und Server** wird über TLS-Protokoll V1.2 unter Anwendung von Perfect Forward Secrecy [10] abgesichert.

Das System bietet eine **Ende-zu-Ende-Sicherheit**. Die zu übermittelnden Nachrichten werden bereits auf dem Rechner des Erstellers verschlüsselt. Die Entschlüsselung der Nachrichten erfolgt grundsätzlich erst auf dem Rechner des Empfängers. Die Nachrichteninhalte liegen auf dem Weg vom Ersteller der Nachricht zum Empfänger zu keinem Zeitpunkt im Klartext vor. Nachrichteninhalte in diesem Zusammenhang sind alle Bestandteile der Nachricht mit dem Schutzbedarf der Vertraulichkeit wie die Nachricht selbst, der Betreff der Nachricht sowie Anhänge der Nachricht, falls vorhanden.

Anwendung findet eine Hybrid-Verschlüsselung der Daten als Kombination von RSA und AES-256/AES-512.

Eine Besonderheit ist die geforderte Möglichkeit des Zugriffs von Vertretern/Mitarbeitern auf die Nachrichten im Postfach. Da die Entschlüsselung der Nachrichten erst auf dem System des Nutzers erfolgen darf, müssen alle potentiellen Leser der Nachrichten in der Lage sein, die Nachrichten zu entschlüsseln.

Im EGVP-System wird nicht zwischen den OSCI-Rollen Empfänger und Leser unterschieden. Die EGVP-Nachrichten sind genau einmal verschlüsselt mit dem Schlüssel des Empfängerpostfachs, unabhängig von der Zugriffsberechtigung. Zur Lösung des Problems im beA schlägt der Auftragnehmer folgendes vor:

- **Umschlüsselung unter Nutzung eines Hardware Security Moduls (HSM)**

  Entsprechend dem oben genannten Hybrid-Verfahren wird die Nachricht symmetrisch verschlüsselt und dieser Schlüssel mit dem öffentlichen Schlüssel des beA-Postfachs (Empfänger) für den Transport verschlüsselt. Zum Zeitpunkt des Zugriffs eines berechtigten Nutzers auf die verschlüsselte Nachricht im Postfach erfolgt innerhalb des HSM eine Umschlüsselung dieses Schlüssels. Dabei bleiben die Inhaltsdaten zu jedem Zeitpunkt im Postfach verschlüsselt.

  Der private Schlüssel des Postfaches ist nicht als Nutzdaten exportierbar.

  Durch das HSM werden die Berechtigungen zur Umschlüsselung der symmetrischen Schlüssel zum Zeitpunkt des Auftrages unter Anwendung von kryptografischen Methoden (Signaturen)geprüft.

  Eine adäquate Lösung ist in Österreich durch cyberDOC, einem Joint Venture der österreichischen Notariatskammer mit dem Auftragnehmer realisiert.

  Die Betreffzeilen der Nachrichten werden mittels HSM für jedes Postfach individuell umgeschlüsselt, so dass eine performante Suche über Inhalte der Betreffzeilen durch den Benutzer möglich ist.

[10] Mindeststandard des BSI nach § 8 Abs. 1 Satz 1 BSIG für den Einsatz des SSL/TLS-Protokolls in der Bundesverwaltung

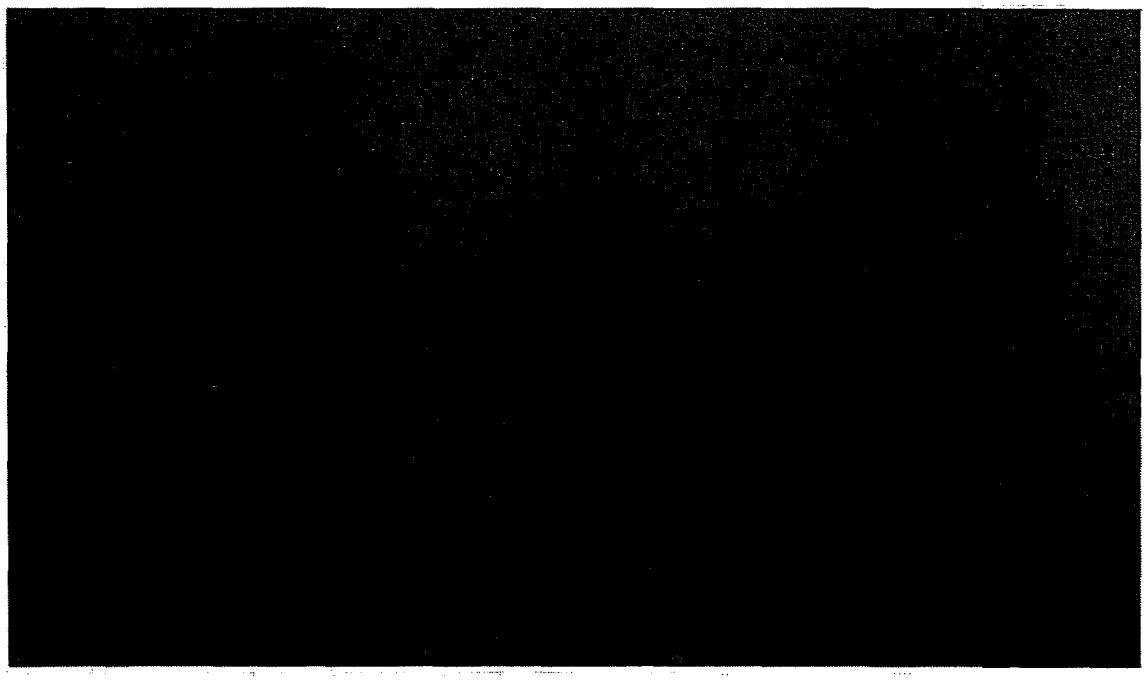
Mittels **elektronischer Signaturen** werden die Nachrichten gegen unbemerkte Manipulation geschützt (Integrität). Durch die Signaturzertifikate ist der Autor eindeutig identifizierbar, so dass Authentizität und Nichtabstreitbarkeit gewährleistet sind. Der Zusammenhang zwischen Zertifikaten und Personen wird durch die Einträge in den S.A.F.E.-Verzeichnissen oder durch den Einsatz der qualifizierten elektronischen Signatur sichergestellt.

Das **OSCI-Transportprotokoll** definiert die Mechanismen, mit denen die Sicherheitsziele in der Kommunikation mit der Justiz erfüllt werden. Dabei werden OSCI-Nachrichten in beA-Nachrichten konvertiert bzw. umgekehrt.

Die **Authentifizierung** der Clientbenutzer erfolgt über eine Zwei-Faktor-Authentifizierung, den Besitz einer Privatschlüsseldatei, einer Signaturkarte / eines Personalausweises und dem Wissen der dazugehörigen PIN. Der Authentifizierungsvorgang selbst wird gestützt auf das SAML-Protokoll von [redacted] durchgeführt. Mit der Unterstützung des neuen Personalausweises ist diese ab dem 01.01.2018 erforderliche Form der Authentifizierung abgedeckt.

Eine besondere Herausforderung sind **manipulationssichere Systemsignaturen**, die z. B. für noch nicht signierte Nachrichtenentwürfe/Bestandteile, Journale oder exportierte Nachrichten gefordert werden. Diese sollen gegen Manipulationen durch die Systemadministratoren geschützt werden.. Die Kontrolle des Administrationszugriffs ist durch organisatorische Sicherheitsmaßnahmen abzufedern (Vieraugenprinzipien, geteilte Passworte, etc.). Durch das Anbringen von elektronischen Zeitstempeln werden nachträgliche Eingriffe erheblich erschwert. Bei Journaleinträgen werden jeweils die Hashwerte über die vorangegangenen Einträge mit signiert, so dass eine lückenlos nachvollziehbare Kette über die Einträge gebildet werden kann.

Eine weitere Besonderheit für die Anbringung von Systemsignaturen beim Export von Nachrichten ergibt sich aus der Anforderung der Ende-zu-Ende-Verschlüsselung. Um den Anforderungen der Leistungsbeschreibung Kap. 2.2.4 A gerecht zu werden, erfolgt der Nachrichtenexport in folgenden Stufen:



Ab dem 01.01.2018 kann laut Gesetz die Authentifizierung des Absenders durch den **neuen Personalausweis** die Signatur als Nachweis der Urheberschaft einer Nachricht ersetzen. Das beA-Postfach signiert in diesem Fall einen Nachrichtentransportvermerk, in dem die erfolgreiche Authentifizierung des Absenders bestätigt wird. Dieser Transportvermerk wird dem Sender- und dem Empfängerpostfach hinzugefügt. Er enthält die Signatur der Nachricht, die vom Empfänger geprüft werden kann. Das System bestätigt mit seiner Signatur, dass Nachricht und Signatur innerhalb einer erfolgreich authetierten Sitzung von dem Sender eingereicht wurde.

Zur Absicherung der Kommunikation von Komponenten des Gesamtsystems untereinander werden [redacted] werden deren Sicherheitsmechanismen verwendet.

6f)	Beschreiben Sie, wie Sie sicherstellen, dass die zur Erstellung des Systems durch Sie beauftragten Personen die Aspekte Bundesdatenschutzgesetzes wie in Kapitel 2.6.5 beschrieben einhalten. (nicht länger als 500 Wörter)

Der Auftragnehmer beachtet uneingeschränkt alle zur Erbringung der mit dem Auftraggeber vereinbarten Dienstleistungen relevanten Vorschriften des Bundesdatenschutzgesetzes.

Der Auftragnehmer verfügt über eine DIS-Organisation (Datenschutz und Informationssicherheit), die alle Mitarbeiter zu DIS-Themen regelmäßig sensibilisiert, verbindliche DIS-Vorgaben veröffentlicht und die DIS-Umsetzung kontrolliert.

Der von der Geschäftsführung bestellte Datenschutzbeauftragte nimmt seine Aufgaben gem. §§ 4f, 4g BDSG (Bundesdatenschutzgesetz) wahr. Diese Aussagen gelten für den Unterauftragnehmer Governikus KG analog.

Alle für die Erbringung der Dienstleistungen eingesetzten Mitarbeiter sind schriftlich auf das Datengeheimnis gem. §5 BDSG verpflichtet. Diese Verpflichtung ist bei internen Mitarbeitern Teil der Personalakte und besteht über das Vertragsverhältnis hinaus.

Zur Sicherstellung der Einhaltung der Aspekte des BDSG setzt der Auftragnehmer die technischen und organisatorischen Maßnahmen wie in Anlage zu §9 BDSG beschrieben um. Dies dient dazu, den Auftraggeber in die Lage zu versetzen, seinen gesetzlichen Verpflichtungen gemäß BDSG nachzukommen.

Sämtliche Daten des Auftraggebers werden ausschließlich in Deutschland gespeichert.

Der Auftragnehmer wickelt seine Leistungen auf Grundlage eines Sicherheitsmanagements ab. Dieses beinhaltet unter anderem schriftlich dokumentierte Richtlinien und Leitfäden zum IT- / Rechenzentrumsbetrieb. Sie bauen auf gesetzlichen Regelungen sowie auf intern bewährten Regelungen auf. Die eingesetzten Sicherheitsverfahren werden laufend überprüft.

Die Richtlinien sind auch für beauftragte Subunternehmer verbindlich. Weisungen des Auftraggebers wird der Auftragnehmer unverändert an Subunternehmer weitergeben.

Atos IT Solutions and Services GmbH ist nach DIN EN ISO 9001:2008 und ISO/ IEC 27001 von Ernst & Young CertifyPoint B.V. zertifiziert.

6g)	Beschreiben Sie, wie Sie ein stabiles Reaktionsverhalten des von Ihnen gelieferten Systems auch bei hoher Belastung durch eine hohe Anzahl aktiver Benutzer und der Übertragung sehr großer Nachrichten realisieren werden. (siehe Kapitel 2.6.6.A) (bis zu 1.000 Wörtern)

Für ein stabiles Reaktionsverhalten des beA-Systems sollten zumindest diejenigen Teilsysteme, welche die Hauptlast in Bezug auf die Benutzer und übertragende Daten bewerkstelligen, skalierbar ausgelegt werden.

Die Teilsysteme sind:

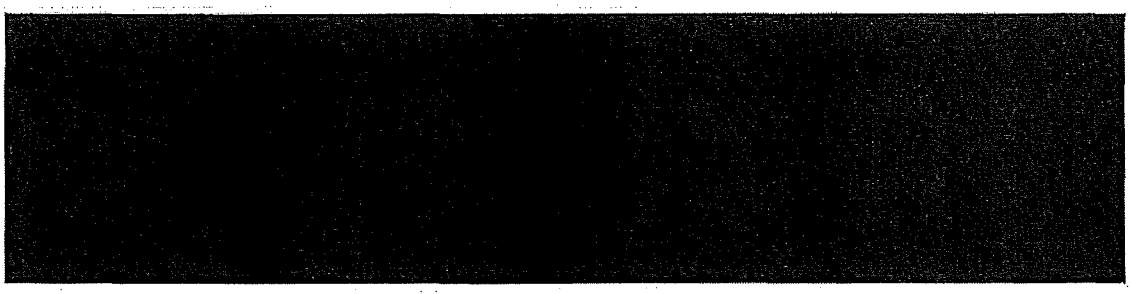
- [redacted] – Authentifizierung und Stammdatensystem für Identitäten
- **OSCI** Server – für die Kommunikation mit der Justiz
- **beA-Anwendung** – fachliche Anwendung.

Diese Teilsysteme können durch die verwendete Softwarearchitektur auf einer auf Hochverfügbarkeit ausgelegten Systemarchitektur installiert werden. Im Folgenden wird eine beispielhafte Topologie für diesen Anwendungsfall skizziert.

[redacted]

Alle Benutzeranfragen werden über einen [redacted] geleitet.

[redacted]



Um ein stabiles Reaktionsverhalten sicherzustellen, werden frühestmöglich Lasttests durchgeführt, um potentielle Performanzprobleme frühzeitig zu erkennen.

Außerdem ist für die konkrete Dimensionierung der Hardware ein möglichst realistisches Nutzungsprofil der Anwendung zu erstellen. Hier ist insbesondere die Anzahl der gleichzeitigen Benutzer und die durchschnittliche Größe der zu übertragenden Daten wichtig, um neben der Dimensionierung der Hardware auch die benötigte Netzwerkanbindung der Anwendung abschätzen zu können.

Die Skalierbarkeit einer Lösung ist nicht ausschließlich von der verwendeten Infrastruktur abhängig. Die Wahl der Lösungsarchitektur und die Beachtung von [redacted] beeinflussen die Skalierbarkeit einer Lösung ebenfalls in hohem Maße. Die Lösungsarchitektur ist so ausgelegt, dass sie [redacted] ist.

Herausforderungen

Im konkreten Fall der beA-Anwendung besteht eine Herausforderung darin, dass unter Umständen viele Benutzer gleichzeitig große Nachrichten auf den Server übertragen.

Hier ist besonders darauf zu achten, dass während des Uploads nicht die gesamte Nachricht in den Arbeitsspeicher des Servers geladen wird, da sonst abhängig von der Nachrichtengröße sehr viel Arbeitsspeicher pro aktivem Benutzer auf dem Server belegt wird. Um dieses Problem zu umgehen, sollten die Daten [redacted] Das genaue Verhalten wird im Umsetzungskonzept definiert.

Die minimale Dauer eines Uploads ist auch durch die Upload Bandbreite des Clients festgelegt. Gerade bei kleineren Kanzleien muss davon ausgegangen werden, dass bei Nutzung eines normalen DSL Anschlusses nur geringe Upload Bandbreiten (< 1Mbit/sec) zur Verfügung stehen. Dies führt dazu, dass ein Upload längere Zeit dauern kann (100MB bei 1Mbit/sec ungefähr 14 Min.). Diese langen Upload-Zeiten erschweren es, die Daten direkt in die Datenbank zu streamen, da hierzu sehr lange Transaktionen auf der Datenbank benötigt würden. Aus diesem Grund empfehlen wir, die [redacted] Das genaue Verhalten wird im Umsetzungskonzept definiert.

[redacted] macht es außerdem leichter, einen Upload, der z. B. durch Verbindungsprobleme beim Client abgebrochen wurde, an derselben Stelle wieder aufzunehmen, was sowohl die Last auf dem Server verringert, als auch die Akzeptanz beim Client erhöht.

6h)	Beschreiben Sie, wie das von Ihnen gelieferte System den Datenverlust auch bei kritischen Störungen minimiert und es dem Benutzer ermöglicht die Bearbeitung einer Nachricht zu unterbrechen um sie zu einem späteren Zeitpunkt wieder aufnehmen zu können. (siehe Kapitel 2.6.6.B) (nicht länger als 500 Wörter)

Für die Verwaltung der Nachrichten wird eine relationale Datenbank eingerichtet. Je nach Zustand der Nachricht wird diese in unterschiedliche „Verzeichnisse" gespeichert:

- **Entwurf** – Nachrichten, die sich in Bearbeitung befinden, aber noch nicht versendet wurden.
- **Eingang** – alle empfangenen Nachrichten. Ungelesene Nachrichten werden hervorgehoben.
- **Ausgang** – alle Nachrichten, die gerade versendet werden, von denen aber noch keine Empfangsbekenntnis angekommen ist.
- **Gesendet** – für Nachrichten, die versandt und empfangsbestätigt wurden.
- **Papierkorb** – Nachrichten, die zwar als gelöscht gelten, aber wieder durch den Anwender reaktiviert werden können.
- **Weitere Verzeichnisse des Anwenders**

Die gespeicherte Nachricht besteht aus

- den Nachrichtenparametern/ Metadaten,
- steuernden, organisatorischen und technischen Merkmalen,
- Verwaltungsattributen,
- Strukturdaten,
- den Anhängen inklusive externen Signaturdateien,
- und dem Nachrichtenjournal.

Kritische Textparameter der Nachricht sowie alle Anhänge werden verschlüsselt gespeichert, so dass nur der Autor diese wieder öffnen kann. Ein Administrator mit Zugriff auf die Nachrichtendatenbank ist nicht in der Lage, diese zu öffnen, da er nicht im Besitz des privaten Schlüssels des Autors der Nachricht ist.

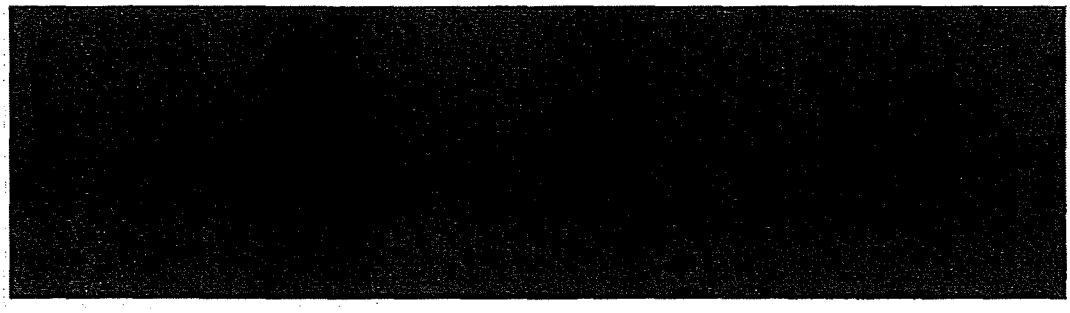
Vor dem Versand wird die Nachricht aus der Datenbank in die vorgegebene XML-Nachrichtenstruktur generiert. Beim Empfang einer Nachricht im XML-Format wird diese validiert, geparst und dann in die Datenbank geschrieben.

Speichern von neuen bearbeiteten Nachrichten

Für die Erstellung neuer Nachrichten und die Weiterbearbeitung von Entwürfen wird ein Dialog erstellt, in dem alle erforderlichen Parameter angegeben und Anhänge zugewiesen werden können. Während der Bearbeitungszeit werden die Nachrichtenparameter in einer eigenen Speicherstruktur des beA-Clients gehalten. Diese Nachricht wird bei Betätigung des „Speichern"-Buttons im Dialog des Clients validiert und im Erfolgsfall verschlüsselt an den Server gesendet. Dort wird sie nach einer weiteren Validierung in die beA-Datenbank in das Verzeichnis „Entwurf" abgelegt. Die somit abgelegte Nachricht kann zu jeder Zeit wieder geladen und weiterverarbeitet werden. Im Fehlerfall werden die Validierungsfehler im Clientdialog angezeigt. Damit wird vermieden, dass inkonsistente und fehlerhafte Daten gespeichert werden.

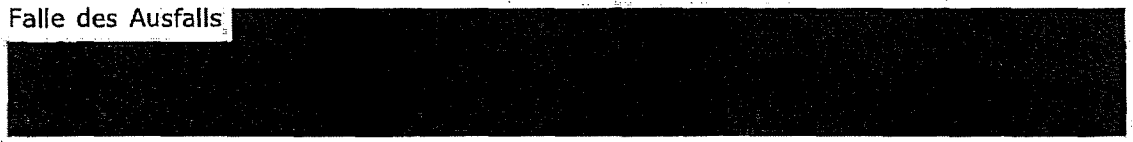
Eine gespeicherte Nachricht kann zu jeder Zeit wieder geöffnet und nachbearbeitet oder versendet werden.

Folgende Maßnahmen führen zu einer möglichst schnellen Speicherung der Daten:



Skalierbarkeit und Ausfallsicherheit der Lösung

Die beA- und Datenbankserver werden in einem [redacted] betrieben, so dass im Falle des Ausfalls



Die beA-Datenbank ist die zentrale Stelle für die Ablage der Nachrichten. Ein Ausfall dieser Datenbank stört das gesamte Kommunikationssystem. Deswegen ist es notwendig auch hier eine ausfallsichere Lösung vorzusehen, um einen Datenverlust im Falle von Storage-Problemen zu vermeiden.

7)	Fassen Sie die wesentlichen Eckpunkte Ihrer Lösung für den Anforderungsbereich „Dokumentation" kurz (nicht länger als 500 Wörter) zusammen.

Der Bereich Dokumentation setzt sich aus den Eckpunkten Dokumentation und Anwenderhilfe zusammen.

Dokumentation

Das Vorgehen bei der Erstellung und Gliederung von Dokumenten ist beim Auftragnehmer durch ein weltweit verbindliches Standardverfahren festgelegt und im Atos Integrated Management System (AIMS) beschrieben.

Anwenderhilfe

Eng in Verbindung mit der Dokumentation ist die Anwenderhilfe zu sehen. Diese hat sich durch die Einflüsse des Web 2.0 Trends sowie des Social Networkings weg vom gedruckten Text im Sinne einer Dokumentation hin zu Online-Hilfe in Form eines Wikis entwickelt.

Grundlegend ist ein Wiki-System - eine Software, die es den Nutzern ermöglicht

- Beiträge zu verfassen,
- zu editieren,
- zu korrigieren und
- zu löschen.

Einzelne Seiten im Wiki können mit Hilfe von Hyperlinks miteinander in Verbindung gebracht werden. Dabei werden Wikis unter anderem in folgenden Einsatzbereichen eingesetzt:

- Online-Hilfen
- Handbücher
- FAQs
- Change Logs
- Schulungsunterlagen
- Glossare.

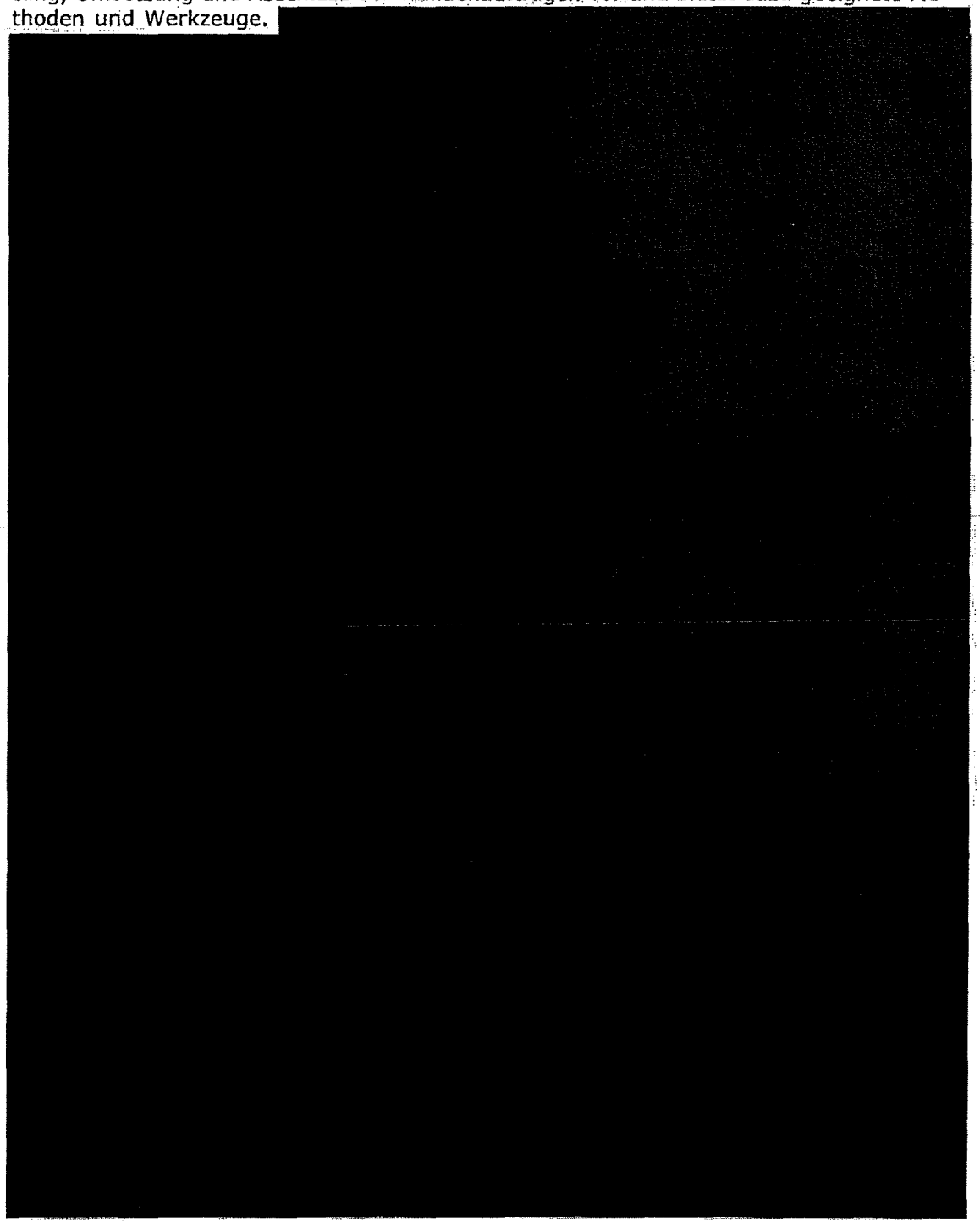
Die Anbindung einer Wiki-Online Hilfe erfolgt über Links innerhalb der Webanwendung. Ein wesentlicher Vorteil ist die Entkopplung der Webanwendung von dem Hilfe-System.

Dies ermöglicht die Pflege der Online-Hilfe unabhängig von der Installation einer neuen Version und erweitert den klassischen Ansatz um Web2.0 Funktionalitäten.

Kontextbezogene Hilfen werden bei Webanwendungen in der Regel über Tooltipps realisiert. Für einzelne Felder in den Dialogen kann hierbei ein Hilfetext und ein weiterführender Link hinterlegt werden. Die Hilfetexte werden eingeblendet, wenn der Benutzer mit dem Mauszeiger über das Hilfe-Icon fährt.

7a)	Erläutern Sie Ihre Vorgehensweise zur Erstellung der im Kapitel 2.7.1.A geforderten Dokumentationen. Gehen Sie dabei auch auf Abhängigkeiten zu weiteren Projektmeilensteinen ein. (nicht länger als 500 Wörter)

Die Vorgehensweise zur Erstellung der geforderten Dokumente leitet sich aus dem Prozessmodell für Kundenaufträge ab. Das beim Auftragnehmer weltweit eingesetzte Prozessmodell „Global Delivery Platform" (GDP) gibt verbindlich das Vorgehen bei Einleitung, Umsetzung und Abschluss von Kundenaufträgen vor und bietet dazu geeignete Methoden und Werkzeuge.



7b)	Skizzieren Sie exemplarisch die Gliederung der technischen Systemdokumentation. Beachten Sie dabei die in Kapitel 2.7.1.C angeforderten Inhalte zur Systemdokumentation. Erläutern Sie dabei, wie Sie sicherstellen, dass zum Verständnis keine Kenntnisse einer Programmiersprache benötigt werden. (nicht länger als 500 Wörter)

Die technische Systemdokumentation beinhaltet die Beschreibung der technischen Lösung, der Randbedingungen und der Entscheidungen, die dazu geführt haben. Diese muss so verfasst werden, dass auch ein technisch weniger versierter Leser diese verstehen kann. Dabei muss folgendes beachtet werden:

- Die Beschreibung muss auch für komplexe technische Themen klar und leicht verständlich gestaltet werden, mit vielen Abbildungen und Querverweisen zur Verdeutlichung der Texte.
- Programmiercode-Schnipsel können zur Verdeutlichung der Texte beigefügt werden, dürfen aber nicht das einzige Beschreibungsmittel sein.
- Die Beschreibung muss in den Kontext der Gesamtdokumentation des Systems passen. Dies bedeutet, dass
  - eine gemeinsame Begrifflichkeit (Glossar), die für das gesamte Projekt erstellt wird, auch in den technischen Dokumenten Verwendung finden muss.
  - quasi ein „roter Faden" zu anderen Dokumenten wie z. B. der Anwenderdokumentation, dem Betriebshandbuch und dem Sicherheitskonzept gesponnen wird.

Für die Erststellung der technischen Systemdokumentation ist ein Umfang von ca. 100 Seiten vorgesehen.

Hier ist folgender Aufbau vorgesehen, bzw. folgende Fragen werden beantwortet:

1) Einleitung
   a) Zweck des Dokumentes
   b) Leseanleitungen und Hinweise zu Gestaltungsmerkmalen
2) Aufgabenstellung und Ziele
   a) Grund für den Aufbau eines neuen Systems
   b) Zielgruppen und Stakeholder
3) Voraussetzungen und Randbedingungen
   a) Anforderungen und Randbedingungen
   b) Voraussetzungen und Annahmen
   c) Organisatorische und gesetzliche Entscheidungen
4) Beschreibung der Lösungsstrategie und wichtiger Architekturentscheidungen
   a) Generelle Beschreibung der Architektur des neuen Systems
      i) Paradigmen (Vorgehensweisen)
      ii) Subsysteme/Teilsysteme
      iii) Eingesetzte Technologie-Stacks
   b) Globale Architekturentscheidungen

5) Systemaufbau (der programmtechnischen Lösung)
   a) Subsysteme
      i) Fachsystem beA
      ii) S.A.F.E.-konformes Sicherheitssystem (S.A.F.E., OSCI-Infrastruktur (Intermediär)
      iii) Import- und Exportmodule
   b) Fachliche und technische Dekomposition des Systems in Subsysteme und Komponenten und deren Zuordnung zu logischen Architektur-Layern
   c) Physikalische Layer des Systems
   d) Sicherung der Skalierbarkeit und Ausfallsicherheit
6) Eingesetzte Technologien und Produkte
7) Beschreibung des Systemkontextes
   a) Systemkontext mit allen Applikationen und Komponenten/Diensten und deren Schnittstellen
   b) Anzubindende Applikationen (Beispiele: Kammersoftware, Kanzleisoftware)
      i) Informationsfluss an den Schnittstellen
      ii) Eingesetzte Technologie, Methoden und Parameter
      iii) Sicherheitsmaßnahmen an der Schnittstelle (Authentifizierung/Single Sign On, Autorisierung, Vertraulichkeit, Datenintegrität, usw.)
   c) Beschreibung der anzubindenden fachlichen und technischen Komponenten (Beispiele: Abrechnungssystem, BRAV-Adapter, Intermediär, Identity Provider, Attribute Service)
      i) Beschreibung der Abläufe und des Informationsflusses
      ii) Beschreibung der Schnittstelle(n)
      iii) Sicherheitsmaßnahmen an der Schnittstelle
   d) Beschreibung der anzubindenden technischen und Infrastruktur-Komponenten wie Datenbanken oder E-Mailverfahren
8) Beschreibung der typischen Muster und technischen Abläufe im System
   Beispiele:
   a) Was passiert im System bei der Erstellung und Versand einer Nachricht an die Justiz mit Empfangsbekenntnis?
   b) Wie werden empfangene Nachrichten zugestellt?
   c) Wie funktioniert eine Anmeldung mittels S.A.F.E.-Identity Provider?
9) Absicherung des Systems, Umsetzung der Maßnahmen aus der Schutzbedarfsanalyse
   a) Verwendete Authentifizierungs- und Autorisierungsverfahren, Zusammenspiel mit der S.A.F.E.-konformen Sicherheitsinfrastruktur

b) Beschreibung des Single Sign On (SSO)-Verfahrens, Zusammenspiel mit der S.A.F.E.-konformen Sicherheitsinfrastruktur

c) Umsetzung von Vertraulichkeit, Datenintegrität und Nichtabstreitbarkeit im Gesamtablauf

d) Transportverschlüsselung

10) Beschreibung der Konfigurations- und Administrationsmöglichkeiten

a) Konfigurationsdatensenken (Dateien, Datenbanktabellen)

b) Administrationsseiten

c) Import- und Exportmöglichkeiten

11) Logging und Monitoring

12) Umsetzung nichtfunktionaler Anforderungen.
Beispiele:

a) Benutzerfreundlichkeit und Barrierefreiheit

b) Session-Handling an der GUI

c) Maßnahmen zur Verbesserung der Performance

d) Maßnahmen zur Ausfallsicherheit

13) Technisches Glossar

14) Literaturverzeichnis.

7c)	Skizzieren Sie exemplarisch die Gliederung der Betriebsdokumentation. Beachten Sie dabei die in Kapitel 2.7.1.D angeforderten Inhalte zur Betriebsdokumentation. (nicht länger als 500 Wörter)

Die Betriebsdokumentation wird in drei getrennten Handbüchern erläutert:

Installations- und Administrationshandbuch der Fachapplikation beA

1) Einleitung
2) Beschreibung der Systemarchitektur
3) Beschreibung der Deployment-Archive/Artefakte (Applikationen und Komponenten)
4) Beschreibung der eingesetzten Standardsoftware Governikus
5) Beschreibung der Vorkonfiguration (Dateien und Parameterwerte, die mit der Installation voreingestellt werden)
6) Beschreibung der Installationsprozeduren und deren Konfiguration
7) Beschreibung der PKI[12] (benötigte Schlüssel und Zertifikate)
8) Einrichten der Datenbanktabellen, Generierung von Initialdaten
9) Beschreibung des Systemstarts, der Anmeldung, des Shutdowns und der Abmeldung
10) Beschreibung der Möglichkeiten für die Überprüfung der Korrektheit der Installation
11) Beschreibung der Deinstallation des Gesamtsystems oder einzelner Komponenten
12) Beschreibung des Exports und Imports von Konfigurationsdaten der Applikation, z. B. durch den Export der Konfigurationsdaten aus der Datenbank.

Betriebshandbuch

1) Einleitung
2) Kurzbeschreibung der Systemarchitektur
   a) Systemkomponenten und deren Verteilung im System (System-Topologie)
   b) Schnittstellen zu anderen Systemen und zu Infrastrukturkomponenten
   c) Sicherheitsdomänen
3) Beschreibung der Anforderungen an Hardware
   a) Server, Nennung der Produkte und deren Ausbau
   b) Eingesetzte Datenspeicher
4) Beschreibung der Netzwerktopologie
   a) Netzwerkdomänen

[12] Public Key Infrastructure

b) Kapazitäten, Netzbandbreiten

c) IP-Adressen und Portnummern und deren Mapping auf Namen (DNS)

d) Network-Appliances (Load Balancer, Firewalls, Router, usw.), Nennung der Produkte und deren Ausbau

5) Beschreibung der Softwareprodukte, die zum Einsatz kommen

a) Betriebssysteme

b) Applikationsserver, Webserver

c) [redacted]-Komponenten ([redacted], etc.)

d) Datenbanksoftware

6) Initiale Installation und Konfiguration der

a) Betriebssysteme

b) Applikationsserver und Webserver

i) Installation der Administrations- und Managed Server sowie deren Konfiguration

ii) Clusterkonfigurationen und Skalierung, Festlegung von Indikatoren und Grenzwerten

iii) Logging-Konfiguration

iv) Konfiguration der Ausfallsicherheit (über Watchdogprozesse oder Node Manager)

v) Automatische Prozeduren für die Installation und Konfiguration

vi) Möglichkeiten des Exports und Imports von Konfigurationen z. B. mit Mitteln der Plattform oder durch Scripting

c) Sicherheitsinfrastruktur laut S.A.F.E.

i) Installation und Konfiguration des Identity Providers und Security Token Services

ii) Installation und Konfiguration des Access Management und der Identity Federation

d) Network Appliances

e) Datenbankserver und Datenbanken

i) Datenbankzugriffe (Ressourcen) für die Clients

ii) Datenbankserver, Cluster

iii) Prozeduren für die initiale Einrichtung von Tabellen, Table Spaces usw.

iv) Export- und Importprozeduren

v) Spiegelung zwischen Instanzen

7) Backup und Recovery, Desaster Recovery

a) Vorgaben für das Backup und Recovery für Datenbanken: manuell und durch zeitgesteuerte Prozeduren (als Cron Jobs)

b) Vorgaben für das Backup und Recovery für Server (komplett oder nur Konfigurationsfiles): manuell und durch zeitgesteuerte Prozeduren

c) Desaster Recovery

8) Monitoring und Fehlerdiagnose durch

a) Auswertung und Konfiguration der Logging-Informationen

b) Nutzung und Konfiguration von SNMP-Traps für spezielle Ereignisse wie Ressourcenengpässe (z. B. bei der Skalierung, Dateisystem)

c) Monitoring der Web Services durch Aufrufen von Heart Beat-Funktionen

d) Business Activity Monitoring (falls Geschäftsprozesse genutzt werden)

9) Bekannte Probleme und deren Lösung

a) Bekannte und gelöste Problemstellungen

b) Frequently Asked Questions (FAQs) für häufige Aufgaben

c) Systemeinstellungen für die Diagnose und das Tracing/ Debbugging

10) Festlegung von Betriebszeiten und personellen Zuständigkeiten

a) Benutzer- und Rollenkonzept

b) Betriebszeiten/ Ansprechpartner bei Problemen.

Administrationshandbuch

1) Serverstart-Parameter
2) Benutzer- und Rollenkonzept
3) SSL/HTTPS-Konfiguration
4) Sicherheitskonfiguration
5) Load Balancing- und Cluster-Konfiguration
6) Logging.

7d)	Beschreiben Sie, wie Sie die Betriebsdokumentation gestalten, sodass das von Ihnen gelieferte System auf der Basis dieser Dokumentation vollständig durch Betreiber installiert und betrieben werden kann. (siehe Kapitel 2.7.1.D) (nicht länger als 500 Wörter)

Die Betriebsdokumentation ist so aufzubereiten, dass auch ein neuer Systembetreiber das System soweit versteht, dass er dieses selbständig installieren, konfigurieren, administrieren und betreiben kann. Des Weiteren muss aus der Betriebsdokumentation auch ersichtlich sein, wie das Gesamtsystem oder Teile davon außer Betrieb gesetzt werden können.

Da eine gute Betriebsdokumentation sehr umfangreich sein kann, wird empfohlen, diese in mehrere „Handbücher" aufzuteilen. Dies ermöglicht eine einfachere Pflege und Weiterentwicklung auch durch mehrere Autoren und ein schnelleres Auffinden von gesuchten Informationen. Des Weiteren kann jedes der hier aufgeführten Handbücher einer zuständigen Person oder Rolle zugeordnet werden.

1) Installations- und Administrationshandbuch der Fachapplikation beA – zeigt wie
   - paketiert (Aufteilung in Deployment-Archive),
   - installiert (Deployment der Archive auf die Server, Installation von Zusatzsoftware),
   - konfiguriert (Erläuterungen zu den Konfigurationsdateien und deren Parameter),
   - technisch administriert (Erläuterungen der technischen Administrationsoberfläche von beA)
   - und kurz auf Funktionsfähigkeit getestet wird.

2) Betriebshandbuch – beschreibt
   - den Aufbau der Infrastruktur (Netze, Server, Firewalls, Loadbalancer usw.) sowie die hierfür eingesetzten Hardware- und Softwareprodukte,
   - die Installation und Konfiguration der Betriebssysteme,
   - die Installation und Konfiguration der Applikationsserver und Network Appliances,
   - die Installation und Konfiguration der Datenbanken,
   - die Konfiguration der Schnittstellen,
   - die Installations- und Konfigurationsprozeduren (z. B. mittels JMX oder WLST),
   - die Prozeduren, die für den Betrieb des Gesamtsystems erforderlich sind (Backup, Recovery, Desaster Recovery, Cron-Jobs, Logging-Konfiguration, SNMP13-Nachrichten),

[13] Simple Network Management Protocol

- die Maßnahmen zur Skalierung und Ausfallsicherheit (Clusterkonfiguration, Prozessüberwachung usw.),
- die Maßnahmen zur Lösung von typischen Problemen,
- die Vorgaben zu Betriebszeiten, Wartungszeiten und
- die personellen Zuständigkeiten für diverse Arbeiten.

3) Administrationshandbuch - beschreibt mittels Hardcopies themenweise die Einstellungen in den Serveradministrationsseiten
Beispiele:
   - Sicherheitskonfiguration (Benutzer und Gruppen, Single Sign On usw.)
   - Load Balancing Konfiguration
   - Serverstart-Parameter
   - Logging.

Gestaltungsmöglichkeiten der Betriebsdokumentation

Die Betriebsdokumentation wird als Wiki erstellt. Das ausgesuchte Wiki sollte einen PDF-Export für Kapitel mit Unterkapiteln besitzen, so dass bei Bedarf auch Teile der Betriebsdokumentation (Beispiel: Betriebshandbuch) als PDF exportiert und ausgedruckt werden können.

Die Nutzung eines Wiki für die Erstellung dieser Dokumentation bringt viele Vorteile:

- Möglichkeit der zeitnahen Pflege der Inhalte durch mehrere Personen
- Verlinkung der Inhalte untereinander und mit anderen Informationsquellen
- Gute Suchfunktionen
- Zugriffsmöglichkeiten von überall
- Automatische Historisierung der Änderungen
- Verknüpfung der Beschreibung mit Diskussionsforen
- Nutzung von Schlagwörtern für das Auffinden von Seiten
- Umfangreiche Darstellungsmöglichkeiten.

Notwendige Qualitätsmerkmale der Betriebsdokumentationsgestaltung

- Verständliche und benutzerfreundliche Gestaltung der Betriebsdokumentation durch:
  - Klare und eindeutige Beschreibung der Aufgaben mit konkreten Beispielen
  - Hinterlegung von Bildern und Diagrammen, die das Ganze verdeutlichen
  - Hinterlegung von Querverweisen auf interne und externe Quellen
  - Beschreibung des Gesamtkontextes, in dem eine Aufgabe stattfindet
  - Nennung und Beschreibung von Automatisierungsprozeduren

- Schnelle Auffindbarkeit von Informationen durch die Nutzung von :
  - Suchfunktionen
  - Indizes und Schlagwörtern
  - Inhalts-, Tabellen- und Abbildungsverzeichnissen
  - Onlinebereitstellung von Dokumenten auf einem Dokumentenserver mit Verlinkung im Wiki.
- Fehlerfreies und effizientes Arbeiten mit der Betriebsdokumentation durch Hinterlegung von:
  - Checklisten für komplexe Vorgänge
  - Prozeduren für die Umsetzung komplexer Aufgaben (z. B. Einspielung einer Konfiguration)
  - Problemlösungen für bereits bekannte Problemstellungen
  - FAQs (frequently asked questions) für häufig auftretende Aufgaben
  - Systemeinstellungen für die Diagnose und das Tracing/ Debugging.

7e)	Skizzieren Sie exemplarisch die Gliederung des Sicherheitskonzepts. Beachten Sie dabei die in Kapitel 2.7.1.E angeforderten Inhalte zum Sicherheitskonzept. (nicht länger als 500 Wörter)

Das Sicherheitskonzept gliedert sich in folgende Kapitel:

Schutzbedarfsanalysen

Der Auftragnehmer wird den Schutzbedarf der angebotenen Services und Anwendungen feststellen und dokumentieren. Dazu werden in einem ersten Schritt die Objekte bzw. Prozesse identifiziert. Dann werden die Elemente einem Schutzbedarf (niedrig, mittel hoch) sowie einem Schutzziel (Vertraulichkeit, Integrität, Verfügbarkeit) zugeordnet. Es wird eine Schadensbewertung bei Verletzung der Ziele vorgenommen. Der Schutzbedarf der Services und Anwendungen wird bestimmt, indem der Schutzbedarf der Anwendungen nach dem Maximum-Prinzip auf die relevanten Komponenten übertragen wird. Das Maximum-Prinzip besagt, dass – sofern mehrere Objekte oder Prozesse eine Komponente nutzen – das Objekt oder der Prozess mit dem höchsten Schutzbedarf die Schutzbedarfseinstufung bestimmt.

Bedrohungs- und Schwachstellenanalyse

Für die in der Schutzbedarfsanalyse beschriebenen Services und Anwendungen wird eine Bedrohungs- und Schwachstellenanalyse durchgeführt. Dazu wird pro Objekt eine Bedrohungsmatrix erstellt, die den Ursachen einer Bedrohung die Auswirkung zuordnet. Zusätzlich findet eine Zuordnung von den in der Schutzbedarfsanalyse festgestellten Schutzzielen zu den Bedrohungen statt.

In einem weiteren Schritt werden Schwachstellen und falls Personen (im Gegensatz zu Außenwirkung oder Elementarereignis) beteiligt sind, deren Motiv erfasst.

Die Kombination aus Bedrohungen, Schwachstellen und ggfs. Angreifern ergeben die Angriffsszenarien und -potenziale, die nach Kritikalität bewertet werden.

Sicherheitsanalyse

Für die Services und Anwendungen wird eine Sicherheitsanalyse erstellt. In diese Analyse werden die Angriffsszenarien, die das Ergebnis der Bedrohungs- und Schwachstellenanalyse sind, den getroffenen Sicherheitsmaßnahmen gegenübergestellt. Anhand dieser Kombination wird entschieden, ob das Objekt bzw. der Prozess als sicher gegenüber den Angriffen zu erachten ist. Ist dies nicht der Fall, so muss eine Risikoanalyse durchgeführt werden.

Risikoanalyse

In der Risikoanalyse werden in Zusammenarbeit mit dem Auftraggeber für die Objekte und Prozesse, die in der Sicherheitsanalyse als unsicher erkannt wurden, das Restrisiko bewertet, akzeptiert und ggfs. weitere Sicherheitsmaßnahmen z. B. in Form von Richtlinien gefordert.

In die Risikobewertung fließen die Schadenshöhe, die Eintrittswahrscheinlichkeit sowie die Kosten für zusätzliche Maßnahmen ein. Ziel ist es, die Eintrittswahrscheinlichkeit und/oder die Schadenshöhe zu vermindern. Ist der „return of security investment (ROSI)" negativ, ist zu erwägen, ob das Risiko akzeptiert wird.

Zur Risikobegrenzung dienen u. a. Richtlinien zur Zugriffskontrolle, zur Löschung von Daten sowie zum Patchmanagement. Mitarbeiter werden in Belangen des Secure Codings geschult.

Sicherheitsvorfälle

Um dem Risiko von Vorfällen zu begegnen, werden die Systeme zyklisch auf Schwachstellen getestet. Dies beinhaltet auch fehlende Patches. Die Systeme des Auftragnehmers sind mit einem aktuellen Virenschutz versehen.

Ferner wird ein Monitoringkonzept zur Überwachung der Systeme des Auftragnehmers erstellt (z. B. der Zugriffskontrolle). Es werden Notfallpläne erstellt, die u. a. Ansprechpartner und Eskalationswege enthalten.

Der Auftragnehmer unterhält eine Organisation zu Datenschutz und Informationssicherheit, die die Einhaltung der Regelungen und Richtlinien überwacht.

Für Behandlung schwerwiegender Sicherheitsvorfälle steht dem Auftragnehmer ein CSIRT (Computer Security Incident Response Team) zur Verfügung, das u. a. forensische Analysen durchführen kann.

Die Behandlung von Sicherheitsvorfällen wird in einer Richtlinie geregelt.

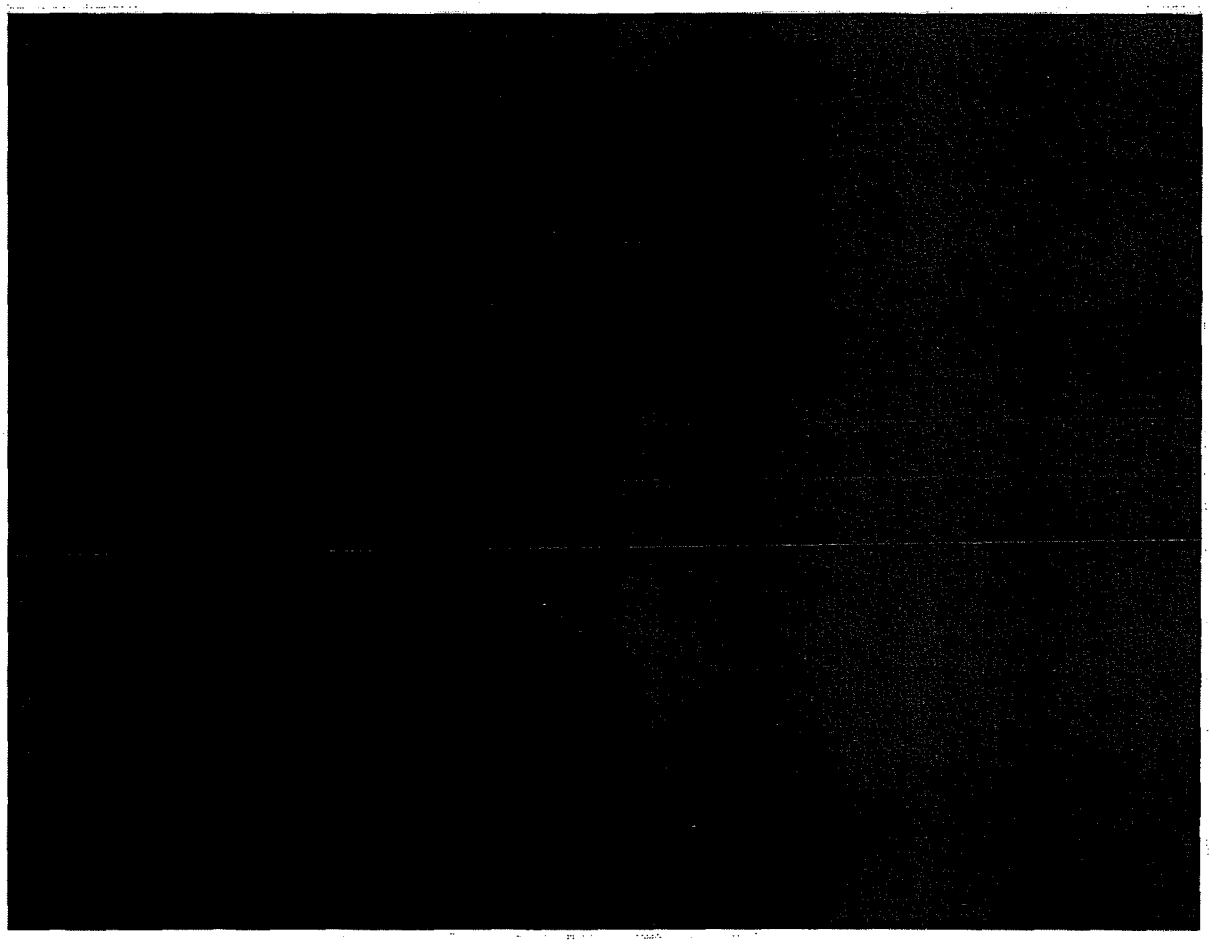
7f)	Beschreiben Sie den Aufbau und die Funktionsweise der Online-Hilfe Ihres gelieferten Systems. (siehe Kapitel 2.7.2.) (nicht länger als 500 Wörter)

Online -Hilfe (Wiki)

Die gesamten detaillierten Hilfetexte für die beA-Anwendung werden im Rahmen der Umsetzung des Projektes in einem Wiki-System (Annahme MediaWiki) zusammengeführt.

Grundsätzlich ist im Rahmen der Konzeptionsphase eine Entscheidung über das eingesetze Wiki-System zu treffen. Hierbei sind neben den Anforderungen an die Online-Hilfe auch ggf. bereits vorhandene Wiki-Systeme beim Auftraggeber zu berücksichtigen.

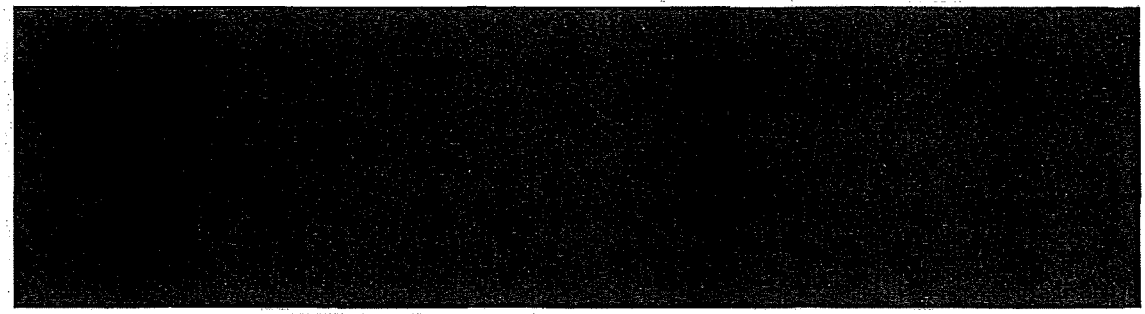
Das ausgewählte Wiki-System kann dann einfach an die Design-Richtlinien des Auftraggebers angepasst werden.



Funktionsweise in der beA-Anwendung

Die Online-Hilfe befindet sich außerhalb der eigentlichen beA-Anwendung und kann jederzeit über einen entsprechenden Link in der Kontextnavigation aufgerufen werden. Außerdem kann die Volltextsuche im externen Hilfesystem (Wiki) auf ein Suchfeld aus der Anwendung heraus aufgerufen werden.

Die Ergebnisseite im externen Hilfesystem zu den eingegebenen Suchbegriffen öffnet sich dann in einem externen Fenster.

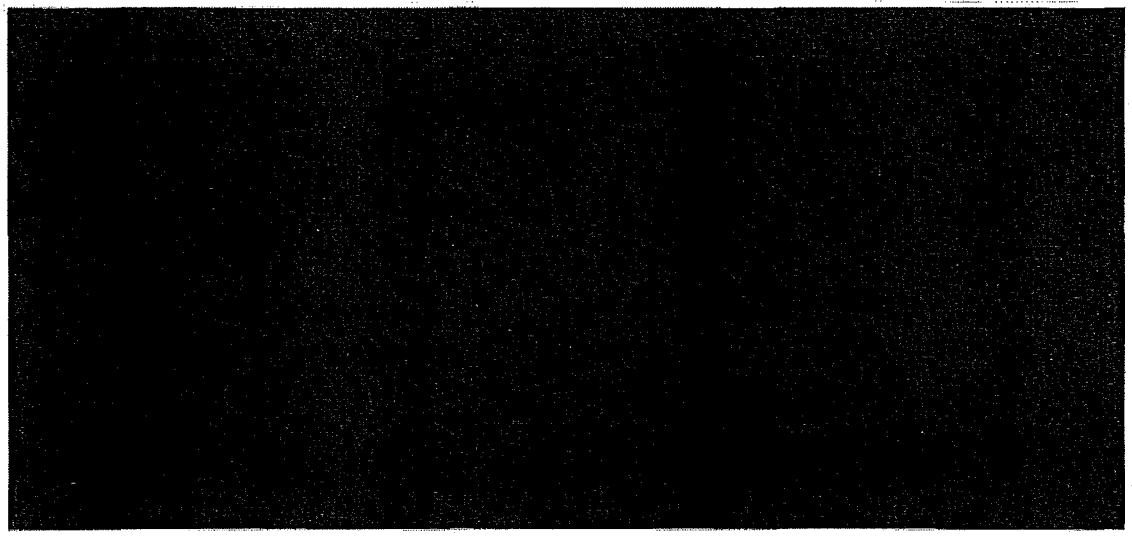


Der Aufbau der Online-Hilfe orientiert sich stark an den in der beA-Anwendung verfügbaren Funktionen und Dialogen. Hier findet der Benutzer detaillierte Beschreibungen zur Funktionsweise der einzelnen Dialoge, zusammen mit Lösungen und Hinweisen für Fragen, welche bei der Nutzung der Anwendung häufig auftreten.

Die Online-Hilfe wird mit der Weiterentwicklung des Systems und auftretenden Supportfällen stetig weitergeschrieben. Änderungen werden dem Auftraggeber zur Freigabe vorgelegt.

Kontextbezogene Hilfe

Für einzelne Felder in den Dialogen der beA-Anwendung können ein Hilfetext und ein weiterführender Link hinterlegt werden. Die Hilfetexte werden eingeblendet, wenn der Benutzer mit dem Mauszeiger über das Hilfe-Icon hinter dem Feld fährt.



Klickt der Benutzer auf das Icon wird der hinterlegte weiterführende Link zu dem Feld aufgerufen und in einem neuen Fenster angezeigt. In der Regel führt der Link zu einer Sprungmarke innerhalb der Anwendungshilfeseiten, welche die Anwenderhilfe zum aktuellen Dialog enthält.

Umfang und Inhalte der Anwenderdokumentation

Anwenderhilfe und Anwenderdokumentation stellen den gleichen Inhalt bereit. Zu jedem Dialog wird eine Übersichtsbeschreibung, sowie eine Detailbeschreibung zu den einzelnen Feldern und Schaltflächen erstellt. Die Anwenderhilfe wird für ca. 20 Dialoge erstellt,

die im Mittel ca. 10 Felder und 5 Schaltflächen beinhalten. Die Anwenderdokumentation besteht aus genau den Inhalten der Anwenderhilfe.

7g)	Beschreiben Sie, wie die von Ihnen gelieferte Online-Hilfe durch den Auftraggeber bearbeitet und fortgeschrieben werden kann. (siehe Kapitel 2.7.2.A) (nicht länger als 500 Wörter)

Für die Bearbeitung der unterschiedlichen Hilfetexte und Hilfeartikel bietet die beA-Anwendung einerseits Administrationsoberflächen für die Pflege kontextbezogener Hilfetexte (MouseOver-Texte für die Hilfe Icons). Andererseits kann die Online-Hilfe im Wiki durch Redakteure gepflegt werden.

Online-Hilfe (Wiki)

Für die Online-Hilfe der beA-Anwendung eignet sich ein Wiki besonders gut, weil die Anforderungen an die Hilfe abgedeckt werden können. Die Darstellung und Formatierung von Hilfedaten in einem Wiki folgt einem im Internet weit verbreiteten Standard.

Bestimmte Grundfunktionalitäten die bereits in unterschiedlichen Wikis integriert sind, können für den Aufbau der Online-Hilfe genutzt werden.

- **Versionsverwaltung**

  Eine integrierte Versionsverwaltung versetzt die Online-Hilfe Redakteure in die Lage, Änderungen an den einzelnen Wiki-Artikeln zu versionieren und so Änderungen besser verfolgen zu können. Außerdem können über die Versionsverwaltung später Releases der Online-Hilfe für die einzelnen Systeme gesteuert werden.

- **Volltextsuche**

  Eine Volltextsuche für die Inhalte der Online-Hilfe kann über eine integrierte Suchfunktion etabliert werden. Über eine entsprechende Integration in der beA-Anwendung (in der Kontext-Navigation) kann der Start einer solchen Suche auch aus der beA-Anwendung initiiert werden.

- **Gestaltung / Anpassbarkeit**

  Ein Wiki bietet die Möglichkeit, umfangreiche standardisierte Methoden für die Gestaltung (z. B. Baumstruktur) zu nutzen. Das Erscheinungsbild des Wiki kann frei für den Anwendungsfall der beA-Anwendung angepasst werden. Für die strukturierte und einheitliche Erstellung der Online-Hilfe Seiten wird eine Designrichtlinie erstellt. Für die einfache Umsetzung durch die einzelnen Redakteure sollten dann Beispielseiten ins Wiki integriert werden.

- **Benutzerverwaltung**

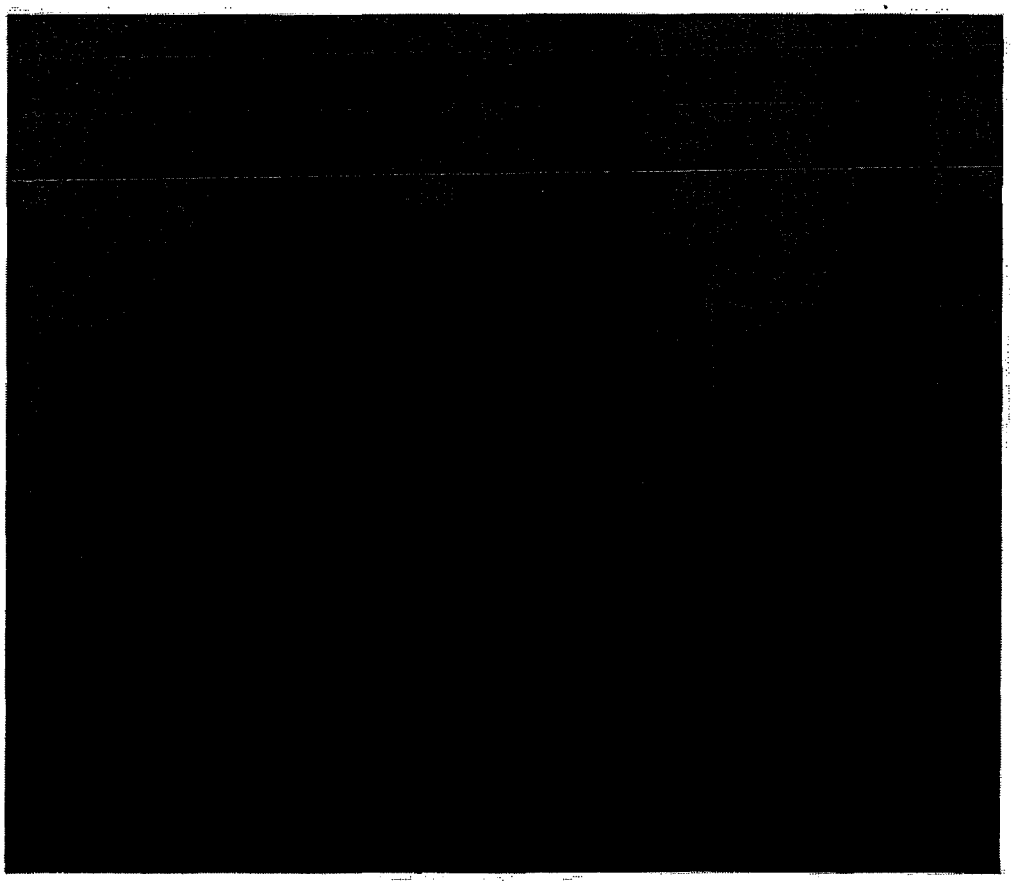
  Der Redaktionsprozess der Online-Hilfe der beA-Anwendung kann über die integrierte Benutzerverwaltung gesteuert und abgesichert werden.

- **Export von Inhalten**

  Inhalte können aus einem Wiki System ggf. in PDF-Format exportiert werden.

Kontextbezogene Hilfe

Die Pflege der Texte für die kontextbezogene Hilfe kann über die Administration in der beA-Anwendung durch entsprechend berechtigte Personen vorgenommen werden. Die Pflegetexte werden in der Datenbank gespeichert und sind somit direkt nach der Speicherung durch den Administrator in den Dialogen der beA-Anwendung verfügbar.



Über einen Auswahldialog kann der richtige Schlüssel für die Pflege der Hilfe-Parameter ausgewählt und markiert werden. Für den gewählten Schlüssel können dann die Hilfe-Parameter wie der Link in die Online-Hilfe und der Hilfetext angepasst und gespeichert werden.

8)	Fassen Sie die wesentlichen Eckpunkte Ihrer Lösung für den Anforderungsbereich „Einweisung" kurz (nicht länger als 500 Wörter) zusammen.

Die beiden wesentlichen Elemente für die Einweisung der Mitarbeiter des Betreibers in die beA-Anwendung sind das Einweisungskonzept und die Einweisung. Die eigentliche Einweisung wird in der Testumgebung des Auftragnehmers erfolgen.

Der Auftragnehmer wird ein Einweisungskonzept erstellen. Dieses Einweisungskonzept ist an den Vorgaben des Auftraggebers aus der Leistungsbeschreibung ausgerichtet, es enthält die folgenden Punkte:

- Zielgruppe und Zielsetzung
- Einweisungsvoraussetzungen und -inhalte, benötigte technische Ausstattung
- Einweisungsdauer und maximale Teilnehmerzahl.

Das Einweisungskonzept legt Zielgruppe und -setzung fest. Zielgruppe sind die Mitarbeiter des Betreibers, die für den sicheren Betrieb der beA-Anwendung zuständig sind. Ziel ist es, die Mitarbeiter in die Lage zu versetzen, den Betrieb der beA-Anwendung gemäß den hohen Anforderungen des Auftraggebers an die Verfügbarkeit durchzuführen. Das Einweisungskonzept wird einen Umfang von ca. 20 Seiten haben. Zur Einweisung der Systemverwalter werden drei zweitägige Workshops geplant.

Für die Benennung und die erforderliche fachliche Qualifikation der Mitarbeiter, die den Betrieb der beA-Anwendung durchführen sollen, ist der Betreiber verantwortlich. Eine Überprüfung durch den Aufraggeber erscheint sinnvoll.

Die Inhalte der Einweisung orientieren sich an den folgenden Punkten:

- Grundverständnis der Lösung
- Erläuterung der technischen Systemdokumentation
- Einweisung in die Installationsdokumentation
- Erläuterung der Installationsaufgaben und -rahmenbedingungen.

Der Auftragnehmer wird für das Einweisungskonzept eine Untergliederung vornehmen, die von den fachlichen Inhalten an dieser Stelle abgeleitet ist. Zu den einzelnen Punkten wird angegeben, welche zentralen Punkte die Mitarbeiter des Betreibers verstanden haben müssen. Deren Beherrschung wird im abschließenden praktischen Test überprüft.

Die oben genannten Inhalte der Einweisung gliedern die eigentliche praktische Einweisung. Ziel ist es, die technischen und fachlichen Aspekte des gesamten gelieferten Systems und die notwendige Infrastruktur verständlich zu machen sowie die Kenntnisse zu vermitteln, die deren sichere Beherrschung ermöglichen.

Zum Grundverständnis der Lösung gehören die Systemarchitektur, die internen und externen Schnittstellen sowie alle Bausteine und Infrastrukturkomponenten. Im Rahmen der Systemdokumentation werden die Mitarbeiter auf besondere Anforderungen und Risiken für den Betrieb der Lösung hingewiesen. Eine Checkliste für die Installation der Lösung innerhalb der konkreten Infrastruktur und unter den Rahmenbedingungen des Betreibers wird erstellt. Weitere Schwerpunkte bilden der Datenschutz sowie die Installation und der Betrieb des Hardware Security Modules (HSM). Der Auftragnehmer gibt Hinweise darauf, wie die hohen Anforderungen an Ausfallsicherheit und Performanz zu gewährleisten sind.

Zum Abschluss der Einweisung erfolgt eine praktische Installation des beA-Systems in der Testumgebung des Auftragnehmers. Dabei erfolgt eine Überprüfung des Erfolgs der Einweisung.

8a)	Bitte beschreiben Sie die Eckpunkte der Einweisung des Dienstleisters des Betriebs (Betrieb des von Ihnen gelieferten Systems). Bitte beachten Sie dabei die im Kapitel 2.8.C aufgeführten Bestandteile der Schulung. (nicht länger als 500 Wörter)

Vor der Inbetriebnahme der durch den Auftragnehmer gelieferten Lösung durch den Betreiber wird der Auftragnehmer eine Einweisung in die technischen und fachlichen Aspekte des gesamten gelieferten Systems und die notwendige Infrastruktur durchführen. Diese Einweisung erfolgt in den Räumen des Auftragnehmers. Sie ist an den genannten Anforderungen ausgerichtet.

Grundverständnis der Lösung

Im Rahmen dieser Einweisung wird dem Betreiber eine genaue Kenntnis aller Bausteine und benötigten Infrastrukturkomponenten vermittelt. Beginnend mit der Erläuterung und grafischen Darstellung der Systemarchitektur und der internen und externen Schnittstellen, wird der Betreiber schrittweise an die Gesamtlösung herangeführt. Die Einweisung konzentriert sich dabei nicht nur auf die technischen Aspekte der Komponenten und Schnittstellen, sondern ordnet diese auch in den jeweiligen fachlichen Kontext ein, um dem Betreiber ein genaues Bild des Zusammenwirkens der einzelnen Bestandteile der Lösung zu vermitteln. Ein Schwerpunkt der Einweisung wird auf den Sicherheitsanforderungen der Schnittstellen und dabei insbesondere auf den externen Schnittstellen liegen.

Erläuterung technische Systemdokumentation, Einweisung in Installationsdokumentation

Anhand der Systemdokumentation und Installationsdokumentation wird auf besondere Anforderungen und Risiken für den Betrieb der Lösung hingewiesen. Mit dem Betreiber wird eine Checkliste für die Installation der Lösung innerhalb der konkreten Infrastruktur und unter den Rahmenbedingungen des Betreibers erarbeitet. Zu den Rahmenbedingungen des Betreibers, die an dieser Stelle auf die Anforderungen des gelieferten Systems abgestimmt werden müssen, gehört insbesondere der organisatorische und technische Aufbau der Netztopologie. Die Komponenten des gelieferten Systems müssen den entsprechenden Sicherheitszonen des Netzes des Betreibers zugeordnet und eventuell weitere Infrastrukturkomponenten (Paketfilter, etc.) ergänzt werden.

Ein Fokus bei der Einweisung des Betreibers wird die Thematik der Vertraulichkeit der Daten und der daraus entstehenden besonderen Anforderungen für den Betrieb sein. Die Einweisung wird das Thema des Datenschutzes und der technischen Aspekte der Verschlüsselung beinhalten, um dem Betreiber ein gutes Verständnis für die Funktion des Systems zu geben und ihn für die IT-Sicherheit und den Datenschutz zusätzlich zu sensibilisieren. Die besonderen Anforderungen an den sicheren und verschlüsselten Betrieb der Datenbanken zum Schutz der Konfigurationsdaten und Metadaten vor Einsichtnahme durch Administratoren wird ebenfalls Gegenstand der Einweisung in das System.

Ein weiterer wichtiger Punkt der Einweisung wird die Installation und der Betrieb des Hardware Security Modules (HSM) sein. Hier werden dem Betreiber die notwendigen organisatorischen sowie technischen Aspekte für den sicheren und datenschutzkonformen Betrieb des HSMs vermittelt.

An das System werden hohe Anforderungen bezüglich Ausfallsicherheit und Performanz gestellt. Der Auftragnehmer wird dem Betreiber die Anforderungen und Möglichkeiten für den verteilten Betrieb der Lösung zur Realisierung von Lastverteilung und zur Erhöhung der Ausfallsicherheit anhand der technischen Systemdokumentation und Installationsdokumentation ausführlich darlegen.

Ein weiterer Punkt der Einweisung wird sich mit der Überwachung des Systems im laufenden Betrieb befassen. Der Auftragnehmer stellt die Schnittstellen zur Einbindung des

Systems in vorhandene Monitoring-Lösungen vor und erläutert die unterschiedlichen Log-Dateien, die die Überwachung des Systems und die Fehleranalyse unterstützen.

Erläuterung der Installationsaufgaben und -rahmenbedingungen

Die umfangreiche theoretische Einweisung in das System wird durch eine praktische Installation des Systems in einer Testumgebung ergänzt. Anhand dieses Beispielsystems werden dem Betreiber praktische Beispiele für die Überwachung des Systems und die Analyse der Logdateien gegeben.

8b)	Skizzieren Sie exemplarisch die Gliederung des Einweisungskonzeptes. Beachten Sie dabei die in Kapitel 2.8.A angeforderten Inhalte zum Einweisungskonzept. (nicht länger als 500 Wörter)

Der Auftragnehmer wird die Mitarbeiter des Betreibers in die Grundlagen und Verfahren des Betriebs für die beA-Anwendung einweisen. Dafür erstellt der Auftragnehmer ein Einweisungskonzept.

Zielgruppe und Zielsetzung

Die Zielgruppe sind die für den Betrieb der beA-Anwendung verantwortlichen Mitarbeiter des Betreibers. Sie müssen mit der Einweisung in die Lage versetzt werden, den Betrieb der beA-Anwendung gemäß den hohen Anforderungen des Auftraggebers an die Verfügbarkeit durchzuführen.

In dem Teil des Einweisungskonzepts zu diesen Punkten wird die Zielsetzung weiter im Detail definiert. Für das Erreichen der Zielsetzung werden bewertbare Kriterien aufgestellt. Zum Beispiel kann dies sein, die Mitarbeiter führen die unter 8a beschriebene praktische Installation durch und es werden spezifische Parameter vorgegeben, deren Einhaltung geprüft wird. Ggf. kann eine Vertiefung der Einweisung erfolgen, sofern die Ziele nicht umgehend zu erreichen sind.

Einweisungsvoraussetzungen und –inhalte, benötigte technische Ausstattung

Die Einweisung erfolgt in der Testumgebung des Auftragnehmers. Die technischen Voraussetzungen zur Durchführung der Einweisung sind damit gegeben. Für die fachliche Eignung der zu schulenden Mitarbeiter ist der Betreiber der beA-Anwendung verantwortlich. Der Auftragnehmer wird für die Einweisungsunterlagen spezifizieren und dokumentieren, welche Kenntnisse für den reibungslosen 24/7 Betrieb der beA-Anwendung erforderlich sind. Der Betreiber hat sicherzustellen, dass die Mitarbeiter, die er zur Einweisung entsendet, die notwendigen fachlichen IT-Kenntnisse haben, um den Betrieb durchzuführen. Ggf. kann der Auftraggeber vom Betreiber entsprechende Nachweise einholen. Dies kann auf der Basis der vom Auftragnehmer erstellten Liste erfolgen.

Die Inhalte für das Einweisungskonzept setzen sich aus den folgenden Themenfeldern zusammen:

- Grundverständnis der Lösung
- Erläuterung der technischen Systemdokumentation
- Einweisung in die Installationsdokumentation
- Erläuterung der Installationsaufgaben und -rahmenbedingungen.

Zu jedem dieser Gliederungspunkte wird der Auftragnehmer für das Einweisungskonzept eine Untergliederung vornehmen, die von den fachlichen Inhalten an dieser Stelle abgeleitet ist. Die zentralen Punkte, die von den Mitarbeitern des Betreibers verstanden sein müssen, werden besonders hervorgehoben. Sie sind in den abschließenden praktischen Übungen Teil der Kriterien zur Beurteilung des Erfolgs der Einweisung.

Einweisungsdauer und maximale Teilnehmerzahl

Die erforderliche Einweisungsdauer wird vom Auftragnehmer am Ende der Entwicklung der beA-Anwendung abgeschätzt. Dies erfolgt anhand der erstellten Einzelpunkte zu den oben angeführten Themenfeldern. Für jeden Bereich in diesen Themenfeldern schätzt der verantwortliche Projektmitarbeiter des Auftragnehmers ab, wie lange es dauern wird, die

Kenntnisse an die Mitarbeiter des Betreibers zu vermitteln. Auf dieser Basis erstellt der Auftragnehmer einen Zeitplan für die Einweisung.

Die maximale Teilnehmerzahl hängt von der Kapazität der Testumgebung des Auftragnehmers ab. Entscheidend wird sein, ob die Anzahl der Mitarbeiter des Betreibers, die dieser in die beA-Anwendung einweisen lassen will, die verfügbare Kapazität der Testumgebung überschreitet. In diesem Fall kann es erforderlich sein, mehr als einen Termin für die Einweisung durchzuführen. Die Teilnehmerzahl erhebt der Auftragnehmer im Rahmen der Erstellung des Einweisungskonzepts.

9)	Fassen Sie die wesentlichen Eckpunkte Ihrer Lösung für den Anforderungsbereich „Maßnahmen zur Inbetriebnahme" kurz (nicht länger als 500 Wörter) zusammen.

Die Maßnahmen zur Inbetriebnahme werden im Umsetzungsfeinkonzept detailliert beschrieben und mit dem Auftraggeber sowie weiteren erforderlichen Parteien (z. B. dem Betriebs-Dienstleister) abgestimmt.

Dabei werden folgende Leistungen durch den Auftragnehmer erbracht:

1) Qualitätssicherung
   - Übergreifende Konzeption der Tests (2.9.1 E)
   - Planung der Tests (2.9.1 A, 2.9.1 E)
   - Spezifikation der Testszenarien (2.9.1 B)
   - Durchführung der Tests (2.9.1 C)
   - Durchführung spezieller Ausfalltests (2.9.2 C)
   - Auswertung der Tests (2.9.1 D)
   - Bereitstellung von Planung, Testspezifikationen und Durchführungsergebnissen (2.9.1 G).

2) Übergang in den Betrieb
   - Benennung eines zentralen Ansprechpartners des Auftragnehmers und von Vertretern für die Unterstützung der Inbetriebnahme (2.1 J)
   - Bereitstellung der Systemanforderungen (Software- und Hardwarekomponenten) (2.9.2 A)
   - Bereitstellung einer betriebsbereiten Installation (2.9.2 B)
   - Einweisung des Betriebs-Dienstleisters in technische und fachliche Aspekte zum Betrieb des neuen Systems (2.8 C)
   - Unterstützung des Betriebs-Dienstleisters bei der Inbetriebnahme des Produktiv-Systems (2.9.2 D).

Qualitätssicherung

Innerhalb der übergreifenden Qualitätssicherung wird ein erfahrener Testmanager des Auftragnehmers die Konzeption und Koordination aller Aktivitäten verantworten. Er hat langjährige Erfahrung in vergleichbaren Projekten und ist ISTQB-Advanced Level zertifiziert für die Rolle Testmanager.

Im Fokus für den Testmanager liegt die optimale Abstimmung der unterschiedlichen Testphasen und Testmethodiken aufeinander. Basierend auf dem zum Einsatz kommenden industrialisierten Testprozess und erprobter Best Practices aus vergleichbaren Projekten werden alle Qualitätssicherungs-Maßnahmen derart gestaltet, dass ein dem Projektvorgehen entsprechendes und effizientes Testen möglich ist.

Die für Testdesign, Testdurchführung und Reporting verantwortlichen Testexperten des Auftragnehmers [redacted]

Schlüsselelemente der geplanten Tests stellen die technischen Überprüfungen bzgl. Lastverhalten und Ausfallsicherheit sowie die Einbindung von ausgewählten Benutzern in die Pilottestphasen dar. Diese Aspekte werden in den Fragen 9e und 9h im Detail betrachtet.

Übergang in den Betrieb

Der Übergang in den Betrieb wird durch Spezialisten des Auftragnehmers aus den Bereichen Entwicklung, Systembetrieb und Test gemäß den Anforderungen des Auftraggebers unterstützt. Schlüsselelemente hier werden die Begleitung des Betreibers bei den technischen Tests sowie die Prüfung der bereitgestellten Dokumentationen (Systemarchitektur, Sicherungskonzepte etc.) für den Betreiber sein.

Neben der Einbeziehung von Auftraggeber und Betreiber sowie der Bereitstellung aller relevanten Dokumente und Testergebnisse für den Systembetrieb wird sich der Auftragnehmer aktiv an den Phasen der technischen Inbetriebnahme sowie der operativen Live-Setzung beteiligen.

9a)	Beschreiben Sie Ihr Vorgehen bei der Definition, Durchführung und Dokumentation von Testfällen. (siehe Kapitel 2.9.1.B, C) (nicht länger als 500 Wörter)

Die Aktivitäten zur Definition, Durchführung und Dokumentation von Testfällen gehören zu den Standardschritten im Rahmen des eingesetzten und standardisierten Testprozesses. Jede einzelne Testphase und jeder einzelne Integrationstestzyklus wird gemäß Standardtestprozess in aufeinander aufbauenden Prozessschritten organisiert:

Standardtestprozess

Definition von Testfällen

Bei der Definition von Testfällen (Testspezifikation) kommen verschiedene Methoden aus Testanalyse und -design zum Einsatz, um im Ergebnis ein den Testzielen einer spezifischen Testphase entsprechenden Testfall im Testmanagement-Tool dokumentieren zu können.

Die in diesem Schritt erstellen Testfälle enthalten mindestens folgende Informationen:

[redacted]

Basis für die Herangehensweise der Testspezialisten an die Testspezifikation sind:

[redacted]

Messgröße für den Umfang der Testspezifikation ist die Testabdeckung. Sichtbar gemacht wird diese Testabdeckung über das Testmanagement-Tool (z. B. [redacted]), in dem Anforderungen und Testszenarien abgelegt und miteinander verknüpft werden. Der Auftragnehmer wird im Rahmen der Testfalldefinition für die geplanten Testphasen eine 100%-Testabdeckung aller Anforderungen realisieren.

Darüber hinaus werden durch die Methode des [redacted] Anforderungen mit hoher Kritikalität sichtbar gemacht - davon werden Testumfang bzw. Testtiefe abgeleitet.

[redacted]

[redacted]

Durchführung von Testfällen

Basis der Testdurchführung ist

[redacted]

[redacted]

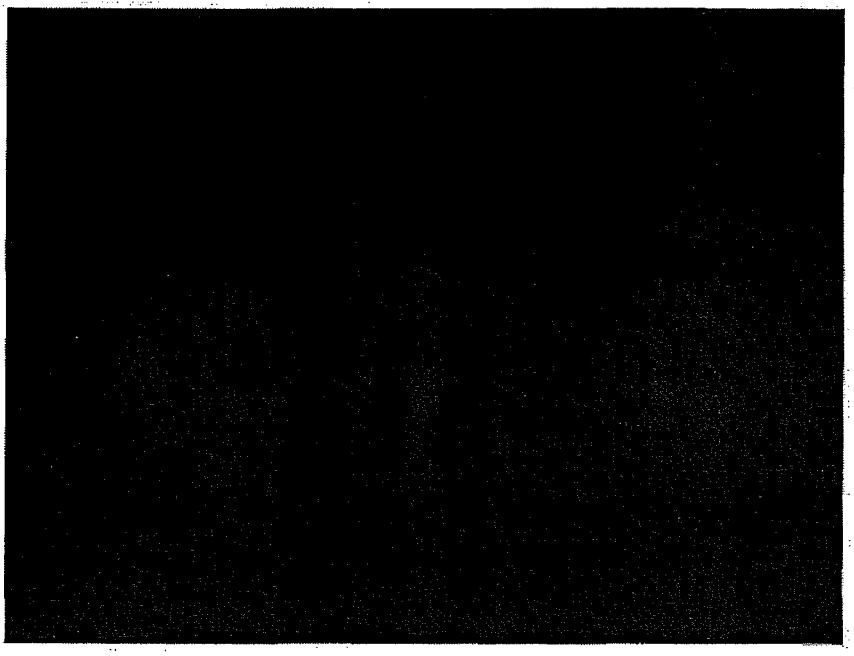
[redacted]

Dokumentation von Testfällen

[redacted]

Die Testfälle können zu jedem Zeitpunkt komplett und in verschiedenen Formaten (MS Word, MS Excel, HTML) aus dem System extrahiert und bereitgestellt werden. Solche

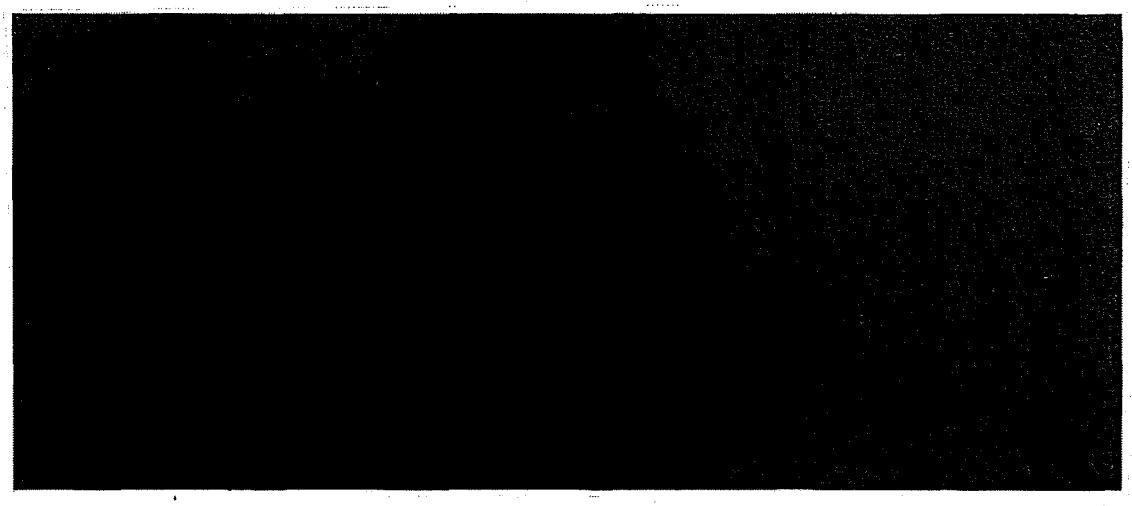
Extrakte sind für die Reviewphase mit dem Auftraggeber sowie zur Veröffentlichung der Testspezifikation vorgesehen.



9b)	Beschreiben Sie Ihr Vorgehen und den Umfang der von Ihnen vorgesehenen Smoketests, Whitebox-Tests, Blackbox-Tests, Integrations- und Lasttests für das von Ihnen gelieferte System. (siehe Kapitel 2.9.1.C) (nicht länger als 500 Wörter)

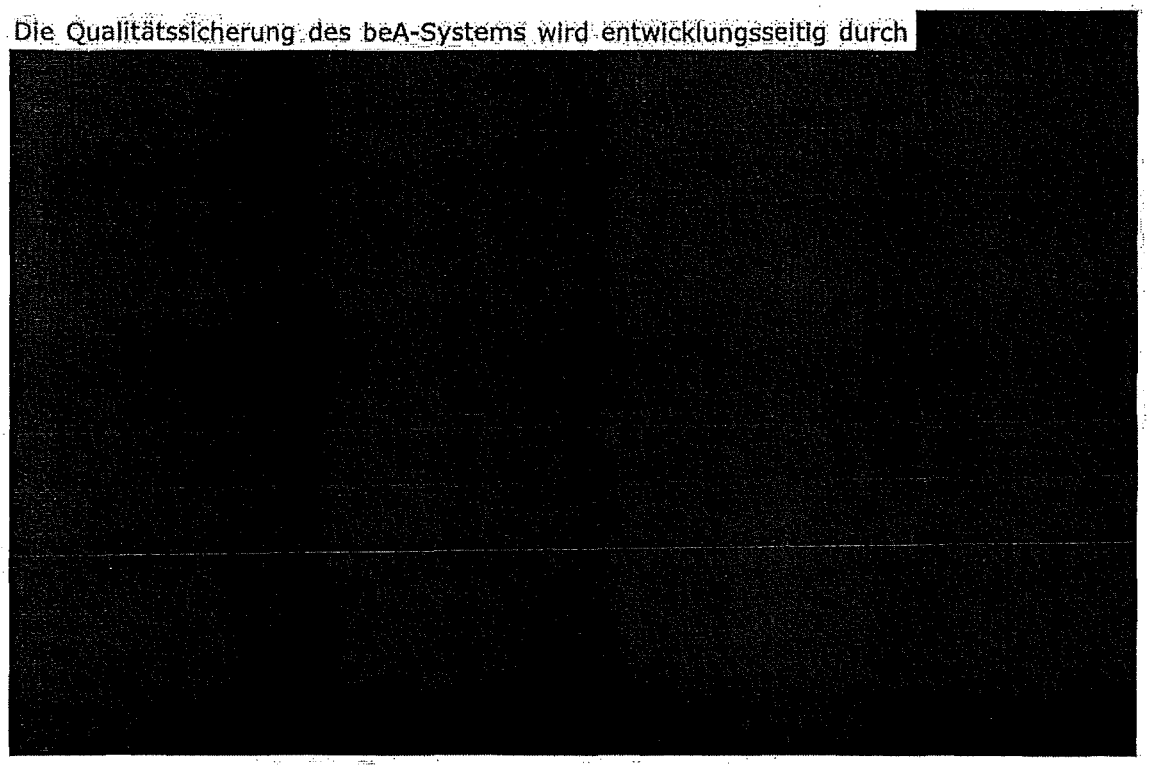
Die geplanten Tests werden im Rahmen verschiedener Testphasen durchgeführt (siehe dazu auch Frage 1a). In jeder Phase wird eine bestimmte Zielsetzung verfolgt:

Die Zielsetzung der gewählten Testphasen bestimmt die im Rahmen der Testphase zum Einsatz kommenden Testmethoden und -typen. Die folgende Matrix zeigt die einzelnen Testphasen und die im Rahmen der Testphase eingesetzten **Testmethoden**, welche definieren, wie bzw. auf welcher Basis ein Test durchgeführt wird:



Die pro Testphase zu verwendenden **Testtypen** definieren, welches Qualitätsmerkmal einer Software im Detail untersucht wird:

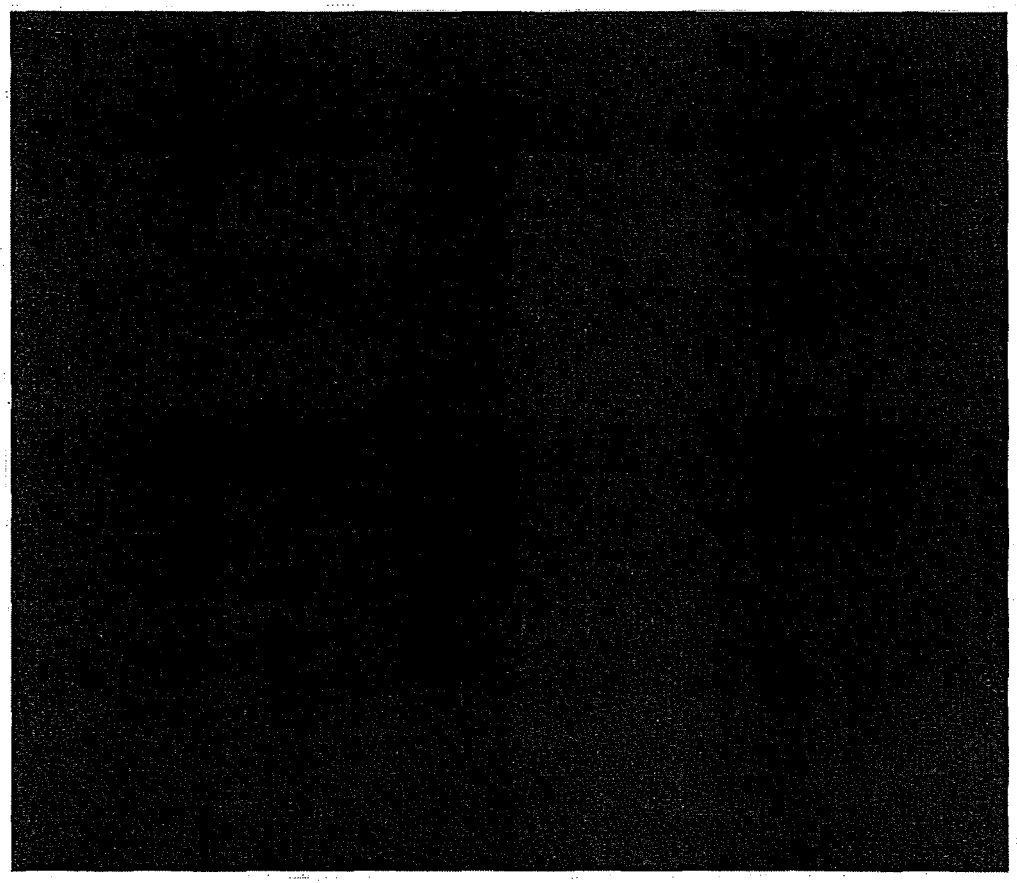
Die Qualitätssicherung des beA-Systems wird entwicklungsseitig durch



9c)	Beschreiben Sie Ihr Standard-Vorgehen zur Fehlerbehebung. (siehe Kapitel 2.9.1.C und 2.9.1.E) (nicht länger als 500 Wörter)

Das Fehlermanagement im Projekt beA wird Tool-basiert realisiert, um Informationsverluste zu verhindern und schnelle Reaktionszeiten bei der Fehlerbehebung zu ermöglichen. Der Auftragnehmer setzt u. a. das Tool [redacted] ein, das eine Kollaborationsplattform für Tester und Entwicklern umfasst.

Der Fehlermanagement-Prozess wird durch den Testverantwortlichen in Abstimmung mit Auftragnehmer und Entwicklung definiert und freigegeben.



Mehrere Testzyklen im Projekt begründen den Bedarf eines kontinuierlichen Fehlermanagements mit Beginn der ersten Testaktivitäten bis zur operativen Live-Setzung.

Alle Aktivitäten steuert und verantwortet ein Fehlermanager. Diese Rolle wird durch den Testmanager übernommen. Er ist im Projekt zentral verantwortlich für

- die Definition des Fehlerprozesses,
- die Definition der Fehlerklassen,
- das Aufsetzen des Fehlermanagement-Tools,
- eine angemessene Erfassung aller Auffälligkeiten/ Fehler während der Testdurchführungen,
- eine zeitnahe Bearbeitung durch die Entwicklung des Auftragnehmers und/ oder Fachexperten des Auftraggebers,
- das regelmäßige Reporting ausgewählter KPIs (u. a. Anzahl offener Fehler),

- die Organisation von regelmäßigen Abstimmungsrunden zwischen Auftraggeber, Test und Entwicklung und
- ein zeitnahes Retesten der Fehlerbehebungen.

Im Folgenden wird der generische Fehlerprozess mit Schlüsselaktivitäten beschrieben:

- **Fehler dokumentieren**
  Während der Testdurchführung dokumentiert der verantwortliche Testspezialist alle festgestellten Abweichungen zum erwarteten Verhalten im Fehlermanagement-Tool. Neben der detaillierten Beschreibung zur Reproduktion des Fehlerverhaltens und der Beschreibung des erwarteten Verhaltens ordnet der Testspezialist jedem Fehler auch eine Fehlerklasse zu. Die **Fehlerklassen** dienen dazu, die Dringlichkeit von Korrekturmaßnahmen unter Berücksichtigung des Schweregrades eines Fehlers transparent zu machen. Dabei definiert der Testspezialist den Schweregrad u. a. anhand folgender Kriterien:
  - Umfang nicht nutzbarer Funktionalitäten
  - Wichtigkeit der betroffenen Funktionalitäten aus Anwendersicht
  - Testszenarien, die aufgrund des Fehlerverhaltens blockiert sind.

  Während der auftraggeberseitigen Tests unterstützt der Auftragnehmer bei der Fehlererfassung. Zudem wird ausgewählten Vertretern des Auftraggebers der Zugriff auf das Fehlererfassungs-Tool ermöglicht, um neue Fehler zu dokumentieren und den Bearbeitungsstand von vorhandenen Fehlern zu prüfen.

- **Fehler analysieren & Fehlerfix liefern**
  Das Entwicklerteam erhält direkt nach Zuordnung im Fehlertool eine Mitteilung über einen neu erfassten Fehler. In Abhängigkeit von der Priorität (=Fehlerklasse) ergibt sich die Reaktionszeit. Bei schweren Fehlern ist ein zeitnahes Feedback in Richtung Fehlerersteller und eine Behebung innerhalb von 24h erforderlich. Sonderlieferungen (Installations-Downtime) solcher Fehlerbehebungen auf die Testumgebungen erfolgen in Abstimmung mit dem Umgebungsverantwortlichen aus dem Testteam.

  Weniger kritische Fehler werden paketiert und im Rahmen von Regellieferungen (z. B. 1x wöchentlich) innerhalb einer Testphase zum Retest bereitgestellt.

  Die Programmierung und damit auch die Fehlerbehebung innerhalb der Entwicklung erfolgt testgetrieben. In der Regel wird die Entwicklung zunächst versuchen, den Fehler durch einen automatisierbaren Test nachzustellen und erst in einem zweiten Schritt den eigentlichen Fehler beheben.

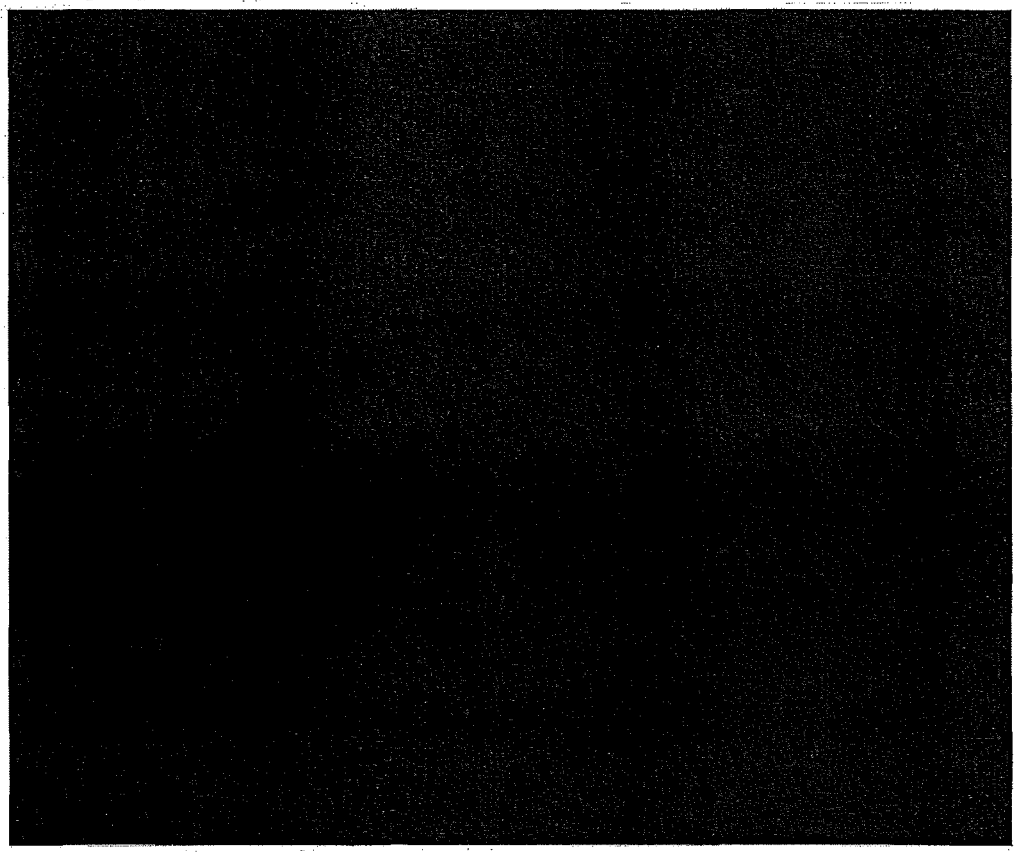
Vor Auslieferung eines Fehlerfixes durchläuft die Software die Entwicklertests, die pro Fehler um eine Prüfung zur behobenen Fehlersituation erweitert werden. Diese Unit-Tests werden bei jeder Folgelieferung mit ausgeführt und verhindern das erneute Auftreten eines Fehlers mit gleicher Ursache.

- **Fehler retesten & Fehler schließen**
  Innerhalb einer Testphase sollen alle in dieser Phase gefundenen Fehler durch die Entwicklung behoben und durch das Testteam erneut getestet werden. Zwischen den Testzyklen der Teilintegration sollen, nach Abstimmung mit Auftraggeber und Entwicklung, ausgesuchte Fehler weitergegeben werden können, um hier die Effizienz von laufenden Tests und laufender Entwicklung zu sichern.

  Fehlerfixlieferungen gelangen ausschließlich durch vollständige Lieferungen (Softwarepaket & Releasenotes) auf das Testsystem. Dabei enthalten die Releasenotes jeweils die neuen Softwareversionen sowie die Beschreibung, welche Fehler mit der Lieferung behoben wurden. Bei allen Lieferungen, die auch der Auf-

traggeber erhält, werden die Releasenotes um Kurzinformationen zu jeder Fehlerbehebung erweitert (Auszug aus dem Fehlermanagement-Tool HP ALM). Das Testteam des Auftragnehmers erhält diese Informationen direkt aus dem Fehlermanagement-Tool.

Im Rahmen der Retests führt der Testspezialist das bei der Fehleridentifikation durchgeführte Testszenario erneut durch. Die aktuellen Ergebnisse werden im Testszenario dokumentiert, der Fehlerstatus im Fehlermanagement-Tool angepasst. Bei erfolgreichem Retest wird ein Fehler geschlossen. Im Negativfall, der ebenfalls im Fehlerprozess zu definieren ist, wird der Fehler erneut der Entwicklung zugewiesen.



9d)	Beschreiben Sie, Ihr Vorgehen zur Auswertung der Tests. (siehe Kapitel 2.9.1.D) (nicht länger als 500 Wörter)

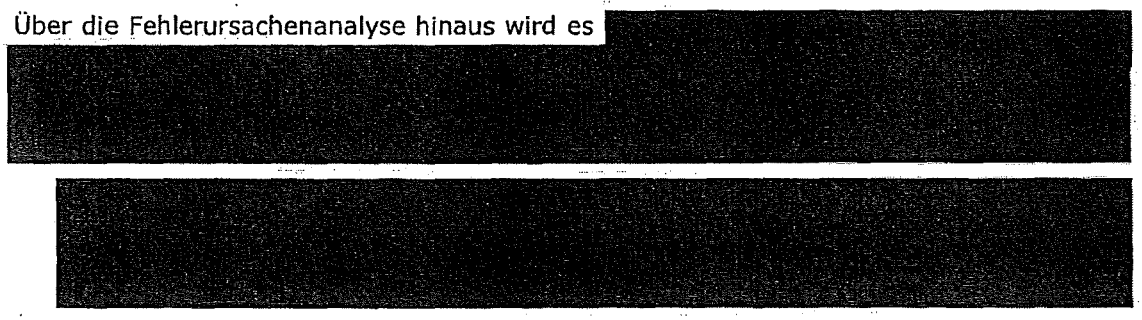
Im Rahmen der geplanten Testdurchführungen (siehe dazu auch Frage 1a) werden durch die Testspezialisten vordefinierte Testszenarien durchlaufen. [redacted]

Nach Analyse der Fehlerursache wird die Entwicklung, wenn dadurch eine Effizienzsteigerung für das Gesamtprojekt zu erwarten ist, den Entwicklungsprozess und / oder die entwicklerseitigen Tests anpassen/ optimieren. Zur künftigen Fehlervermeidung bzw. Verbesserung der Entwicklertests stehen u. a. folgende Möglichkeiten zur Verfügung:

[redacted]

Da die unterschiedlichen Testphasen sich durch unterschiedliche Methoden und Zielsetzungen auszeichnen, ergibt sich jedoch nicht aus jedem Fehler ein Optimierungsbedarf für das Entwicklungsvorgehen.

Über die Fehlerursachenanalyse hinaus wird es

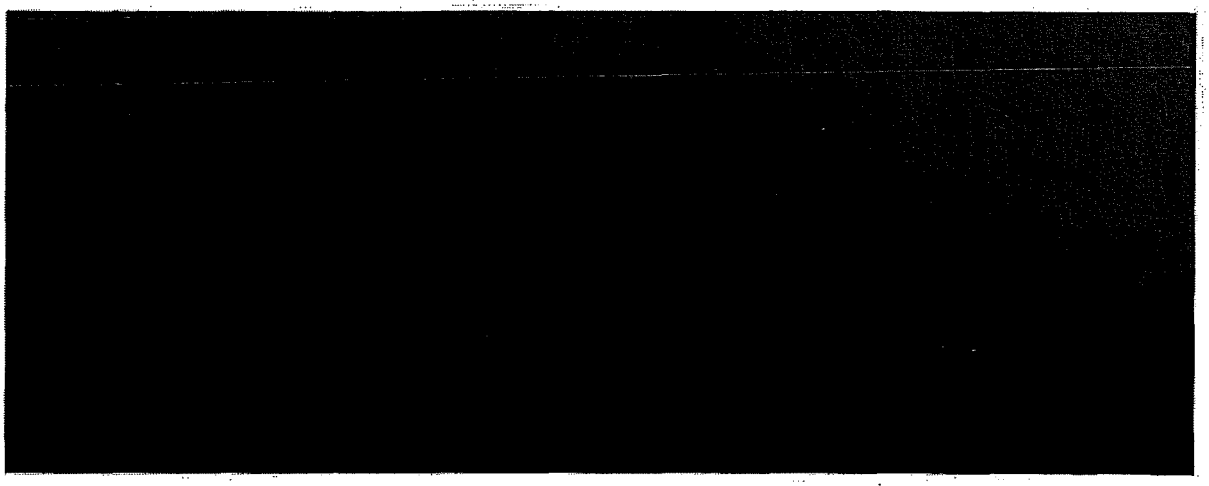


9e)	Beschreiben Sie, wie Sie die Pilottests zu den Oberflächen sowie die Tests mit den Kanzleien und der Justiz planen und welche Auswirkungen diese auf den Gesamtprojektplan haben. (siehe Kapitel 2.9.1.E) (nicht länger als 500 Wörter)

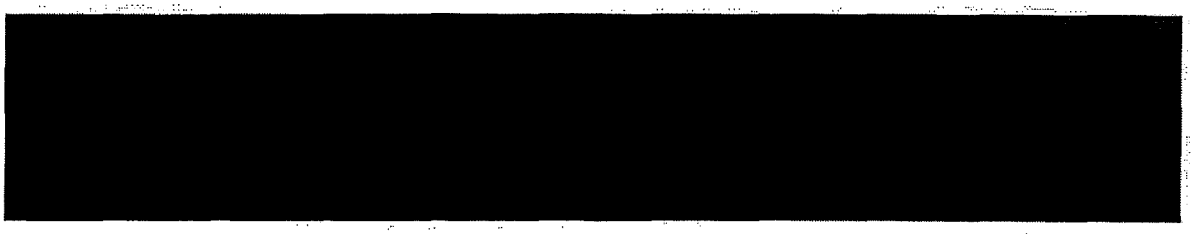
Im Rahmen der übergreifenden Qualitätssicherung sind auch Tests mit späteren Systemnutzern geplant. Ziel ist es, eine Prüf- und Feedback-Möglichkeit für den Auftraggeber vor Abnahme des Systems zu ermöglichen. Zu diesen geplanten Tests zählen:

- Pilottest zu Oberflächen
- funktionaler Test mit Test-Kanzleien
- Integrationstest mit Justiz.

Diese Tests werden auf der Integrationstestumgebung mit einem definierten und vorher durch den Auftragnehmer qualitätsgesicherten Softwarestand stattfinden.



Pilottest Oberflächen



[redacted]

Schnittstelle zur Justiz

[redacted]

Die Testexperten des Auftragnehmers werden die Pilottestphase mit der Justiz vorbereiten und begleiten, u. a.:

[redacted]

Tests mit den Kanzleien

[redacted]

[redacted]

Im Rahmen dieser Tests sollen:

[redacted]

geprüft werden.

Die Tests der ausgewählten Kanzleien werden [redacted]

Die Fehler werden in Abhängigkeit der Störungspriorität, gemäß den Anforderungen des Auftraggebers in der Leistungsbeschreibung behoben.

9f)	Beschreiben Sie, mit welchen Maßnahmen Sie eine betriebsbereite Installation unter den in 2.9.2.B aufgeführten Bedingungen vollumfänglich sicherstellen werden. (nicht länger als 500 Wörter)

Der Auftragnehmer stellt das System betriebsbereit dem Auftraggeber bzw. Betreiber zur Verfügung. Dazu zählen die folgenden Aktivitäten:

- Das System wurde durch den Auftragnehmer mit allen Funktionalitäten, Schnittstellen und der Webanwendung und gemäß den Anforderungen an die Informationssicherheit entwickelt.
- Das System ist in Übereinstimmung mit den Anforderungen durch den Auftragnehmer dokumentiert.
- Das System wurde durch den Auftragnehmer entsprechend der Testkonzeption als ‚bereit zur Abnahme' getestet.
- Sämtliche für den Betrieb notwendigen Konfigurationen sind dokumentiert.
- Das System ist auf einem Test- und Integrationssystem des Auftragnehmers installiert und konfiguriert. Die Test- und Integrationsumgebung umfasst alle Komponenten des vom Auftragnehmer gelieferten Systems und ist entsprechend der Installationsdokumentation eingerichtet.
- Das Projekt wird durch professionelles Projekt- und Qualitätsmanagement geplant, gesteuert und überwacht.

9g)	Beschreiben Sie, mit welchen Maßnahmen Sie den Dienstleister des Betriebs des von Ihnen gelieferten Systems vor und im Zeitraum der Inbetriebnahme unterstützen werden. (siehe Kapitel 2.9.2.A, D) (nicht länger als 500 Wörter)

Der Auftragnehmer unterstützt den Dienstleister des Betriebs mit folgenden Aktivitäten:

Informationen über Software- und Hardwarekomponenten

Der Auftragnehmer berät den Dienstleister des Betriebs im Rahmen von drei Architektur-Workshops zur notwendigen Serverinfrastruktur, dem notwendigen Betriebssystem, der Datenbank sowie Web- und Applikationsserver, auch bzgl. Sicherheit und Hochverfügbarkeit. Darüber hinaus erarbeitet der Auftragnehmer einen Vorschlag zur Dimensionierung der Hardware-Infrastruktur für den Dienstleister.

Unterstützung bei der Inbetriebnahme

Im Rahmen der ersten Inbetriebnahme des neuen Systems unterstützt der Auftragnehmer den Betreiber initial durch [redacted] um unmittelbar die Einrichtung und Konfiguration auf die vom Betreiber gestellte Infrastruktur zu unterstützen.

Unterstützung bei Integrationstests und Lasttests des Betreibers

Die durch den Betreiber auf der produktionsnahen oder Produktivumgebung geplanten Tests werden durch Testspezialisten des Auftragnehmers begleitet.

Es wird davon ausgegangen, dass diese Tests nach Abschluss der Gesamtintegrationstests des Auftragnehmers und parallel zu den Abnahmetests durch den Auftraggeber stattfinden.

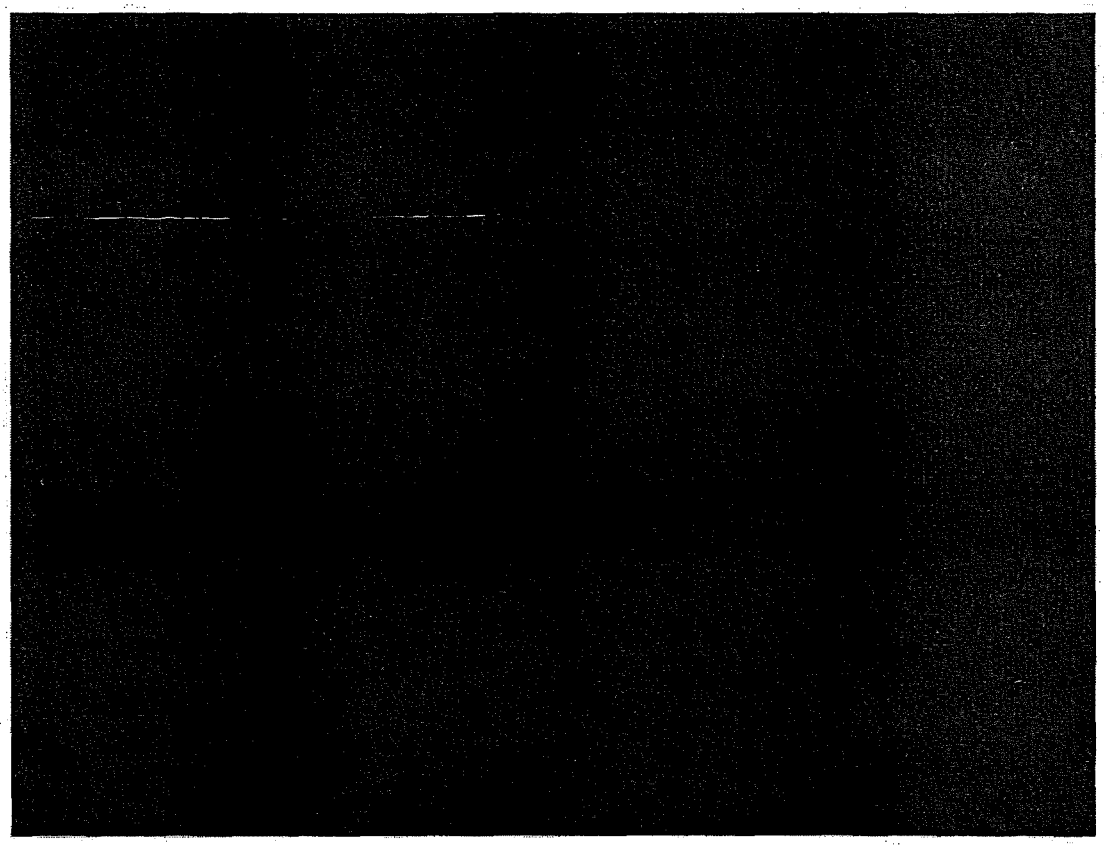
Die Testspezialisten des Auftragnehmers unterstützen den Betreiber in dieser Phase bei folgenden Themen:

[redacted]

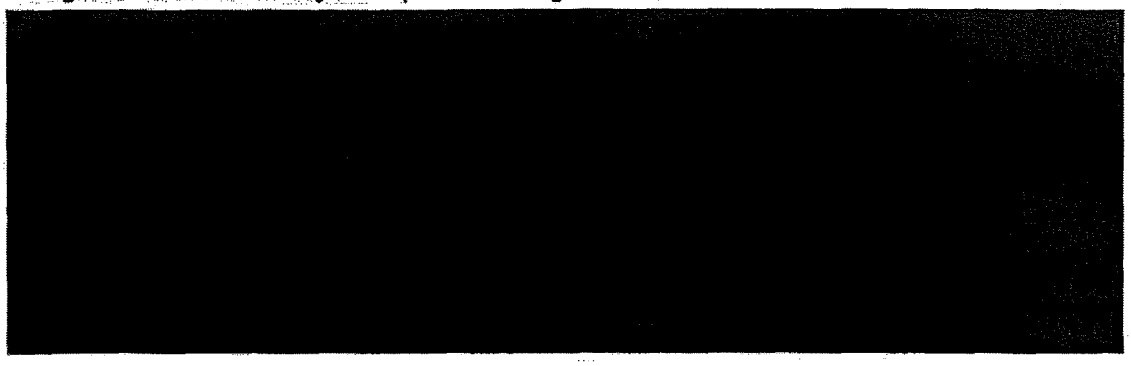
9h)	Skizzieren Sie, welche Tests Sie für den Prüfung der Ausfallsicherheit und zur Wiederherstellung des Regelbetriebs durchführen werden. (siehe Kapitel 2.9.2.C) (nicht länger als 500 Wörter)

Die Tests zu Ausfallsicherheit, Verfügbarkeit, Systemwiederherstellung und Wiederanlauf sind Teil der durch den Auftragnehmer geplanten Phase der technischen Tests. Sie gliedern sich in die Phasen der übergreifenden Gesamtqualitätssicherung und werden im Umsetzungsfeinkonzept detailliert beschrieben.

Orientiert an der Systemarchitektur und der Norm für Qualitätsmerkmale (ISO/IEC 9126) werden die Testszenarien ausgewählt.



Folgende Tests werden je Komponente vorgesehen:



Dieses Vorgehen wird im Rahmen der Finalisierung der Systemarchitektur und durch eine technische Schwachstellenanalyse während der Konzeptionsphase des Projekts überprüft, ggf. angepasst.

Alle Ausfalltests setzen auf den ebenfalls in der Phase der technischen Tests geplanten Lasttests auf. [redacted]

Ausfalltest Verfügbarkeit

Architekturkonzepte zur Realisierung einer hohen Verfügbarkeit wie [redacted] stehen im Fokus für die beA-Systemkomponenten, für die solche Konzepte bestehen, siehe Tabelle oben.

Über ein geeignetes Last- und Ausfallszenario wird geprüft, ob einzelne Komponenten der Hochverfügbarkeits-Architektur ausfallen können und wie sich dies auf bestehende und/oder neu gestartete Systemprozesse auswirkt.

Betrachtet werden folgende Aspekte:

[redacted]

Ausfall und Wiederanlauf Software-Komponente

Die Wiederanlauftests überprüfen, ob das System korrekt wieder anläuft, wenn eine Applikation oder eine Komponente nach einem Ausfall neu gestartet wird.

Über geeignete Monitoring-Mechanismen wird die Dauer der Downtime sowie das Verhalten im Fehlerfall und beim Wiederanlauf untersucht.

Backup & Restore

Im Rahmen von Systemausfällen oder -störungen kann es ggf. zu einem inkonsistenten Stand bei Daten oder Konfiguration kommen. Im Testszenario wird der letzte konsistente Stand wiederhergestellt, z. B.

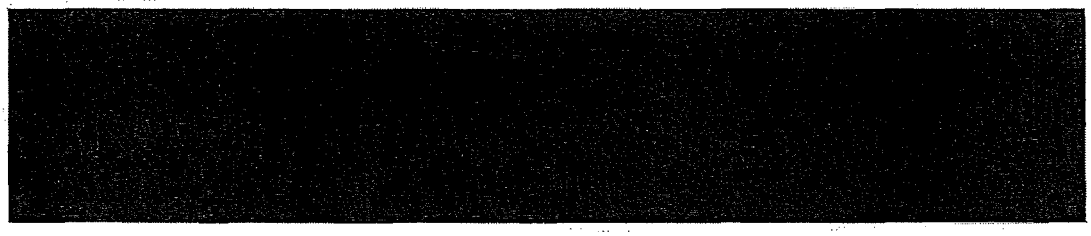
[redacted]

K-Ausfall und Wiederanlauf Hardware

Der K-Ausfall bezeichnet ein Katastrophenszenario, in dem eine komplette Hardware oder sogar ein gesamtes Rechenzentrum ausfallen.

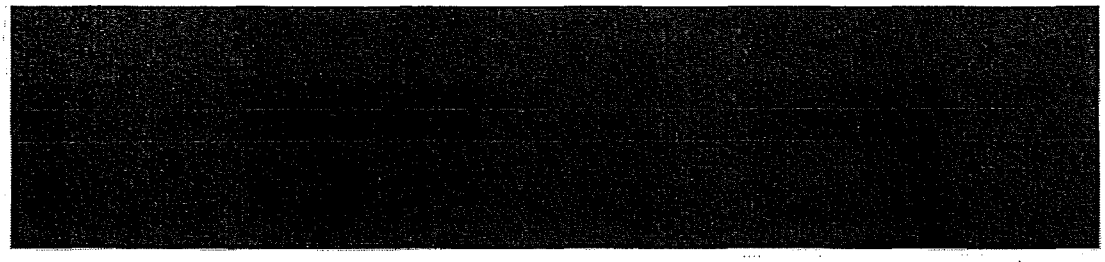
Im Rahmen der beA-Tests werden alle Komponenten, die auf einer dedizierten Hardware laufen, einem Ausfalltest unterzogen werden.

Im Fokus der Tests stehen:



Rahmenbedingungen

Folgende Punkte sind für die technischen Tests von Bedeutung und in der Konzeptionsphase zwischen Auftraggeber, Betreiber und Auftragnehmer abzustimmen:



10)	Fassen Sie die wesentlichen Eckpunkte Ihrer Lösung für den Anforderungsbereich „Softwarepflege und Wartung" kurz (nicht länger als 500 Wörter) zusammen.

Der Bereich Softwarepflege und Wartung hat die Aspekte Release-Planung, Third-Level-Support; Change und Service Requests sowie Problembehandlung im Third-Level-Support.

In der Release-Planung sind zwei Zeiträume zu unterscheiden. Für die ersten sechs Monate hat der Auftraggeber die folgende Frequenz vorgegeben: Für die Fehlerbehebung sind wöchentliche, für die Funktionserweiterung monatliche Releases zu liefern. Für die Zeit ab dem siebten Monat schlägt der Auftragnehmer vor, für die Fehlerbehebung einmal im Monat und für die Funktionserweiterung alle sechs Monate neue Releases vorzusehen. Third-Level-Fehler sind nach den dafür explizit vorgesehenen Zeiten und Releasezyklen zu beheben und einzuspielen.

Für jedes Release geht der Auftragnehmer nach dem gleichen, intern als Standard definierten Verfahren vor. [redacted]

Für die Behebung von Störungen innerhalb der vereinbarten Reaktions- und Fehlerbehebungszeiten bietet der Auftragnehmer den Service aus seinem Global Delivery Center. [redacted]

Change Requests und offene Punkte sind nach festgelegten Prozessen zu bearbeiten. Offene Punkte werden zwischen Auftraggeber und Auftragnehmer nach Möglichkeit auf unterer Ebene geklärt. Ist das nicht erfolgreich, dann wird das Änderungsverfahren nach EVB-IT benutzt. Dieses ist in jedem Fall einzusetzen, wenn es um Change Requests im Sinn von neuen Anforderungen des Auftraggebers geht. Nach Erhalt des Change Requests analysiert der Auftragnehmer die zeitlichen Folgen, Kosten und weitere Konsequenzen des Änderungsverlangens. Innerhalb eines zu vereinbarenden Zeitrahmens (z. B. 10 Arbeitstage) legt er dem Auftraggeber die Bewertung vor. Die Entscheidung über die Umsetzung fällt der beA-Lenkungsausschuss.

Anforderungen für einen Service und die Problembehandlung sind nach dem betroffenen Teil des beA-Systems und Schwere zu klassifizieren. Dabei sind Service Requests Anforderungen, die sich auf die Wartung und Behebung von Störungen beziehen, die eine niedrige Priorität aufgrund geringer Auswirkungen haben. Fehler in der Software oder Störungen des Systems mit geringen bis mittleren Auswirkungen haben mittlere Priorität. Die Behebung auf der Ebene der unteren und mittleren Priorität erfolgt im Rahmen des normalen Releasezyklus für Fehler. Die höchste Priorität haben Störungen des Betriebs, die über den Third-Level-Support gemeldet sind. Hier erfolgt die Bearbeitung auf der Grundlage der Vorgaben aus der Leistungsbeschreibung.

10a)	Beschreiben Sie Ihr Standard-Vorgehen bei der Release-Planung und deren Aktualisierung. (siehe Kapitel 2.10.1) (nicht länger als 500 Wörter)

Im Rahmen der Softwarepflege des Systems sind vom Auftragnehmer regelmäßig Releases bereitzustellen. Das Release-Management wird in der Phase der Inbetriebnahme aufgebaut. Der Zyklus für die Bereitstellung der Releases wird während der ersten sechs Betriebsmonate kurz getaktet sein. Für die Fehlerbehebung sind wöchentliche, für die Funktionserweiterung monatliche Releases zu liefern.

Für die Betriebszeit nach den ersten sechs Monaten sind die Zyklen für die Releases mit dem Auftraggeber zu vereinbaren. Der Auftragnehmer schlägt vor, für die Fehlerbehebung einmal im Monat und für die Funktionserweiterung alle sechs Monate neue Releases vorzusehen. Third-Level-Fehler sind nach den dafür vorgesehenen Zeiten und Releasezyklen zu beheben und einzuspielen.

Der Auftragnehmer wird neue Releases durch sein Entwicklerteam für die beA-Anwendung umsetzen.
für die Softwaretests v[redacted]

Dieser Prämisse soll auch die Definition der Inhalte eines Release folgen.

Zusammen bildet sich so der Releasezyklus.

[redacted]

Ein Release mit Funktionserweiterung sollte erst in den Betrieb überführt werden, wenn die Akzeptanz und der Nutzen der Lösung für den praktischen Einsatz überprüft sind. Zumindest sollte das Release in einer produktionsnahen Systemumgebung einer Anzahl von ausgewählten Benutzern zur Erprobung dauerhaft verfügbar gemacht werden.

10b)	Beschreiben Sie, wie Sie den Third-Level-Support für die Behebung von Störungen innerhalb der vereinbarten Reaktions- und Fehlerbehebungszeiten gewährleisten werden. (siehe Kapitel 2.10.2.C) (nicht länger als 500 Wörter)

Der Auftragnehmer bietet einen Third-Level-Support für das entwickelte beA-System und die darin enthaltenen Komponenten.

Der Third-Level-Support des Auftragnehmers übernimmt dabei Problemmeldungen, die durch den First- und Second-Level-Support des Auftraggebers bzw. Betreibers nicht gelöst werden können. Die Übergabe des Tickets von dem Betreiber in Richtung Auftragnehmer erfolgt durch [redacted]

Bei Eintreffen einer Problemmeldung lokalisiert der zuständige Support-Mitarbeiter die Problemursache und sorgt für eine Problemlösung.

Der 24x7-Third-Level-Support des Auftragnehmers wird als deutschsprachiger Support durch Mitarbeiter im [redacted]

Die Mitarbeiter im vorgesehenen [redacted] vor Beginn des Support-Vertrages durch die Applikationsentwickler intensiv geschult.

Um darüber hinaus eine unmittelbare und schnelle Lösungsfindung zu ermöglichen, [redacted]

Die Mitarbeiter des Third-Level-Supports arbeiten dabei eng mit dem Betreiber des beA-Systems zusammen, [redacted]

In dem Third-Level-Support enthalten sind:

[redacted]

Nicht enthalten im Third-Level-Support sind die Wartung und Pflege der beA-Software, die separat unter einer eigenen Preisposition angeboten sind.

10c)	Beschreiben Sie Ihr Vorgehen für die von Ihnen vorgesehenen Maßnahmen zur Umsetzung von Changes, Service-Requests und die Problembehandlung als Third-Level-Support im Betrieb des von Ihnen gelieferten Systems. (siehe Kapitel 2.10.2.B, C) (nicht länger als 500 Wörter)

Change Requests

In einem Projekt der Größenordnung des beA sind erfahrungsgemäß Änderungen (Changes) unvermeidbar, denn es ist nicht möglich, jedes Detail im Voraus zu planen. Treten offene Punkte auf, sind die nach einem zu vereinbarenden Verfahren zu klären. Hier ist zu unterscheiden zwischen offenen Punkten, die auf zuvor nicht bekannte Tatsachen oder nicht erkannte Folgewirkungen zurückgehen. Des Weiteren können vom Auftraggeber völlig neue Anforderungen gestellt werden, die z. B. auf Verordnungen des BMJ für die Umsetzung des ERV zurückgehen.

Offene Punkte werden zunächst bis zur Ebene der Projektleiter zu klären versucht. Dafür wird der Auftragnehmer zu Projektbeginn ein entsprechendes Formular erstellen, in dem die offenen Punkte klassifiziert werden. Eine Einordnung der potenziellen Risiken und Konsequenzen, die sich aus dem offenen Punkt ergeben, erfolgt.

Anforderungen, die sich aus der Klärung offener Punkte ergeben oder die vom Auftraggeber im Projektverlauf neu eingebracht werden, werden vom Auftragnehmer als Change Request (Änderungsantrag) behandelt. Das Änderungsverfahren gemäß EVB-IT mit dem entsprechenden Formular bildet hierzu die formale Grundlage.

Entsprechend den Vorgaben des Formulars „Änderungsverfahren" beschreibt der Auftraggeber, welche Änderungen des Leistungsumfangs er verlangt. Der Auftragnehmer nimmt eine Prüfung vor. Terminliche Konsequenzen, Aufwände, ggfs. erforderliche Beschaffungen von Hard-Software, oder der Einsatz von zusätzlichen Experten werden bewertet. Der Auftragnehmer legt dem Auftraggeber auf der Ebene des Projektausschusses die Bewertung innerhalb eines definierten Zeitraums (z. B. 10 Arbeitstage) vor. Die Entscheidung über die Umsetzung des Änderungsantrages obliegt dem Lenkungsausschuss.

Service Requests, Problembehandlung

Anforderungen für einen Service und die Problembehandlung sind nach ihrer Art zu klassifizieren. Entscheidend dafür ist, auf welchen Teil des beA-Systems sie sich beziehen. Weiterhin sind sie nach der Schwere (Severity) zu klassifizieren.

[redacted]

11)	Fassen Sie die wesentlichen Eckpunkte Ihrer Lösung für den Anforderungsbereich „Erweiterungen" kurz (nicht länger als 500 Wörter) zusammen.

Die Erweiterbarkeit von Applikation ist eine strategische Anforderung an moderne IT-Lösungen, die der Auftragnehmer in allen Projekten als Basisanforderung berücksichtigt.

Architekturqualität

Voraussetzung für ein hohes Maß an Investitionsschutz und Zukunftssicherheit ist eine Lösungsarchitektur, die allen Anforderungen unternehmenskritischer Anwendungen gerecht wird. Die beA-Lösungsarchitektur nutzt konsequent [redacted] Dies ermöglicht die Anbindung neuer Präsentations-Schichten z. B. mobile Endgeräte, bei denen aber zusätzlich noch die spezifischen Anforderungen berücksichtigt werden müssen (z. B. für die Umsetzung der Authentifizierung). Für die korrekte und sichere Ausführung fachlicher Funktionen verwendet die beA-Lösung [redacted]

Flexibilität

In einer immer komplexeren Geschäfts- und Arbeitswelt stellt die schnelle, flexible Abwicklung aller Geschäftsprozesse einen entscheidenden Erfolgsfaktor dar. Geschäftsprozesse und -modelle ändern sich schnell. Anwendungen müssen deshalb in ihrer Architektur so konzipiert werden, dass sie mit wenig Aufwand schnell änderbar, erweiterbar und anpassungsfähig sind. Die beA-Lösung nutzt die [redacted]

Offene Standards

[redacted]

Integrationsfähigkeit

Die Integration bestehender Anwendungen und Systeme ermöglicht den Investitionsschutz durch weitere Nutzung bestehender IT-Systeme sowie zukünftig geplanter neuer Systeme. Die Integration bestehender Anwendungen und Systeme ist ein zentrales Leistungsmerkmal der beA-Lösungsarchitektur. Die Anbindung von weiteren Kommunikationspartnern ist über die verwendete Lösungsarchitektur möglich und wird auch schon in der beA-Lösung z. B. für die Kanzleisoftware verwendet.

Eingesetzte Methoden

[redacted]

Einfache Übergabe in Betrieb

Die notwendigen Aufwände sind maßgeblich von der richtigen Methode im Entwicklungsprozess und damit dem erzielten Automatisierungsgrad des Bereitstellungs-Prozesses (Deployment) abhängig. Dieses wird vom Auftragnehmer berücksichtigt.

11a)	Beschreiben Sie, welche Methoden Sie einsetzen werden, um die Änderbarkeit/Erweiterbarkeit des von Ihnen gelieferten Systems zu ermöglichen. Gehen Sie hierbei vor allem auf die Bereiche Analysierbarkeit, Modifizierbarkeit, Stabilität und Prüfbarkeit ein. (siehe Kapitel 2.11.1) (nicht länger als 500 Wörter)

Die Begriffe Analysierbarkeit, Modifizierbarkeit, Stabilität und Prüfbarkeit sind zentrale Aspekte unseres Qualitätsmanagement in IT-Projekten. Ziel des Qualitätsmanagements ist es dabei, die Erstellung von Software-Produkten/Lösungen qualitativ zu verbessern und die Messung von Qualität zu operationalisieren. Dazu dienen verschiedene Qualitätsmodelle [redacted]

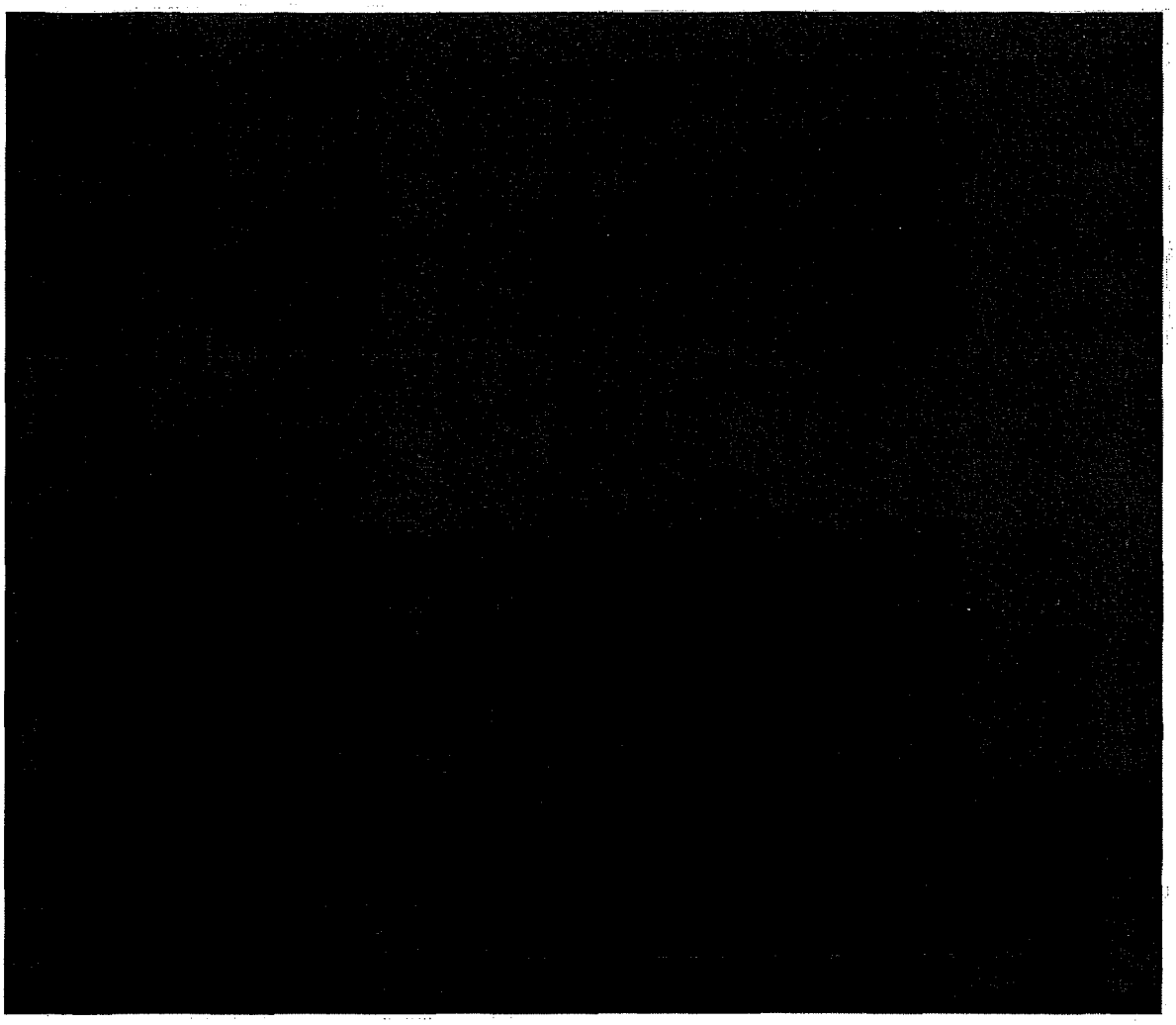
Um diese Anforderungen in einem IT-Projekt kontinuierlich zu adressieren und zu prüfen, werden sie über das gesamte Projekt analysiert und gemonitort.

Das Qualitätsmanagement in IT-Projekten ist beim Auftragnehmer ein kontinuierlicher Prozess [redacted] Hierbei sind zusätzlich zu den oben genannten Themen die folgenden Aspekte wichtig für die Softwarequalität unserer Lösung:

[redacted]

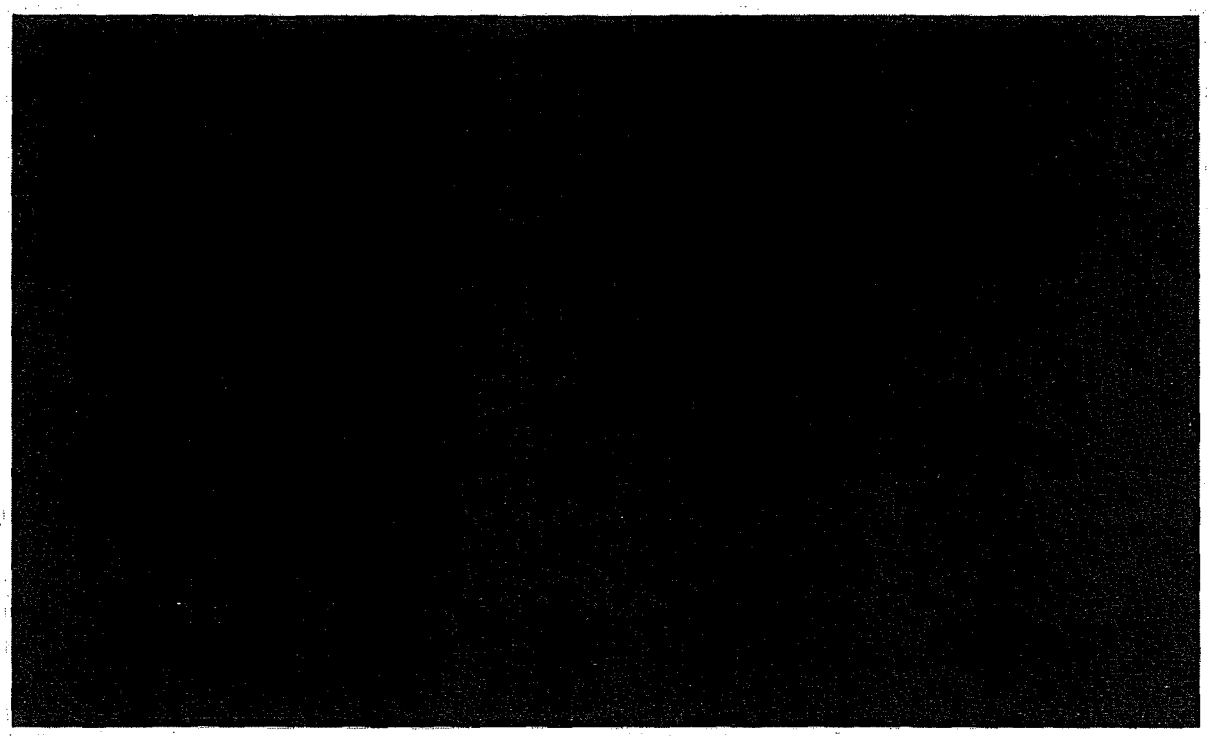
Beim Auftragnehmer wird die Methode [redacted] für die Softwareentwicklung eingesetzt.

[redacted]



Unit-Tests

Im Rahmen des Entwicklungsprozesses werden Unit-Tests zur Überprüfung der Basisfunktionen des Quellcodes erstellt.

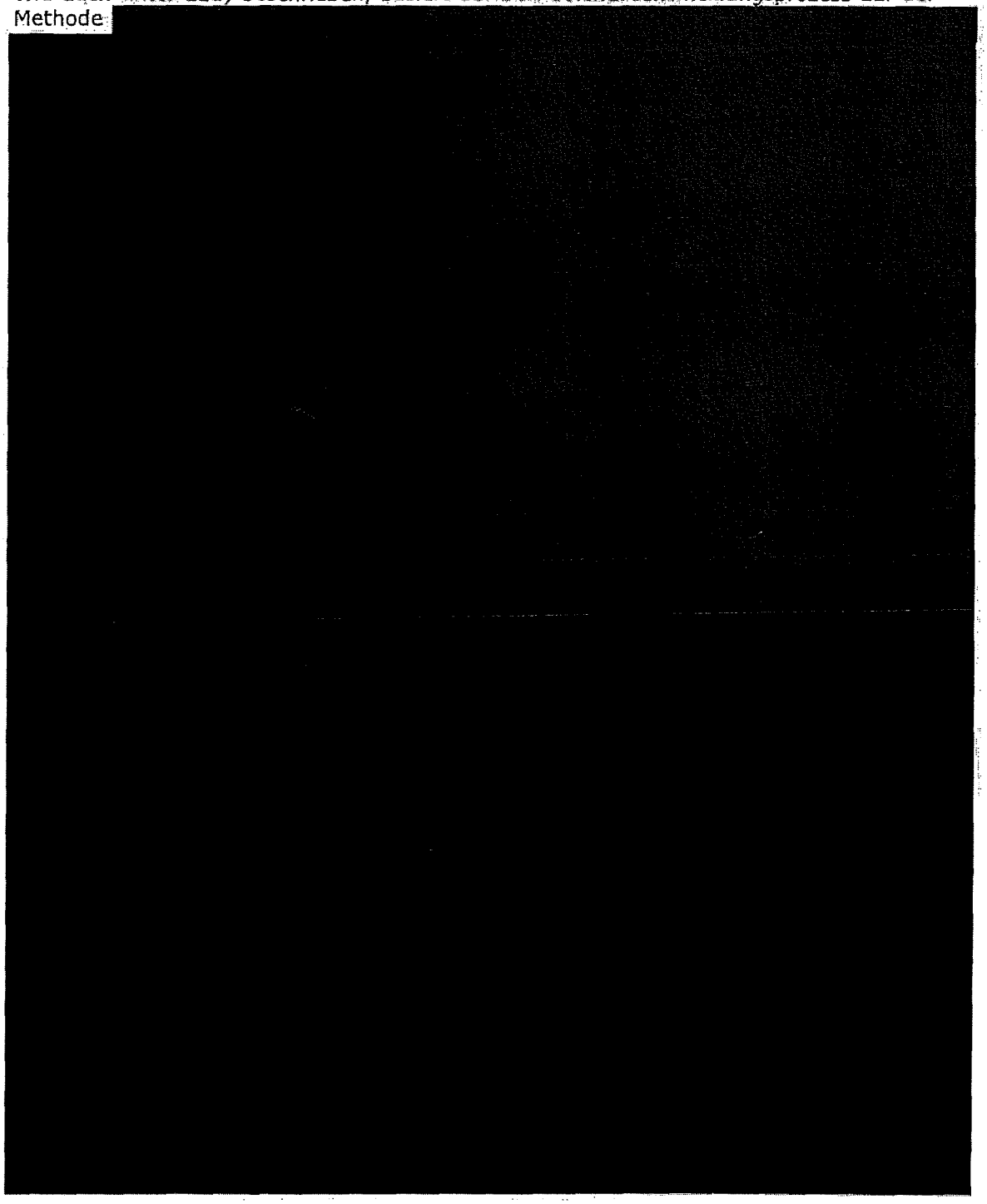


11b)	Beschreiben Sie, wie sie sicherstellen, dass im Betrieb des neuen Systems eine Übergabe in ein neues Umfeld mit geringem Aufwand möglich ist. (siehe Kapitel 2.11.1) (nicht länger als 500 Wörter)

Für die Übergabe in ein neues Umfeld sind zwei Aspekte wichtig.

Aspekt 1: Die richtige Methode für den Entwicklungsprozess

Wie auch unter 11a) beschrieben, basiert der beA-Softwareentwicklungsprozess auf der Methode



Aspekt 2: Einsatz von Standards