Freie Hansestadt Bremen
Die Senatorin für Finanzen

Bundesministerium des Innern

Bundesministerium der Finanzen

IT-Planungsrat

SCHÜTZE CONSULTING AG

DAS ARCHITEKTURKONZEPT eRECHNUNG

für die föderale Umsetzung in Deutschland – entwickelt vom Bund und dem Land Bremen

Version 1.0

Kooperationsprojekt Bund-Bremen auf Basis der Arbeit des EG 3: Technische Ausgestaltung XRechnung in Deutschland

Unter Mitwirkung von: BONPAGO

AUTORINNEN UND AUTOREN

Dr. Stefan Werres, Bundesministerium des Innern

Fred Kellermann, Bundesministerium der Finanzen

Tomislav Dedus, Schütze Consulting AG

Martin Rebs, Schütze Consulting AG

Rainer Heldt, Freie Hansestadt Bremen, Senatorin für Finanzen

Dr. Jan C. Thiele, Freie Hansestadt Bremen, Senatorin für Finanzen

Peter Büsing, Freie Hansestadt Bremen, Senatorin für Finanzen

Beate Schulte, Freie Hansestadt Bremen, Koordinierungsstelle für IT-Standards (KoSIT)

Hartmut Scholz, Informationstechnikzentrum Bund (ITZBund)

Nikolai Jaklitsch, Informationstechnikzentrum Bund (ITZBund)

INHALTSVERZEICHNIS

ABBILDUNGSVERZEICHNIS

TABELLENVERZEICHNIS

1 Einleitung

Die EU-Richtlinie 2014/55/EU, die am 26. Mai 2014 in Kraft getreten ist, verpflichtet die öffentlichen Auftraggeber aller föderalen Ebenen, elektronische Rechnungen zu empfangen und zu verarbeiten. Die Verpflichtung ist für zentrale Regierungsstellen bis zum 27. November 2018 und für alle anderen Stellen bis zum 27. November 2019 umzusetzen. Um der Verpflichtung nachzukommen, haben sich der Bund und das Land Bremen auf einen zentralen Rechnungseingang für die Einlieferung von elektronischen Rechnungen verständigt.

Die technologische Umsetzung eines zentralen eRechnungseingangs wird in dem vorliegenden Architekturkonzept beschrieben. Das Dokument ist das Ergebnis einer engen Zusammenarbeit des Bundes und des Landes Bremen. Das hier vorgestellte Konzept kann auch als Vorlage für weitere Länder dienen. Es ist insgesamt als konkretes Architekturmodell für die föderale Umsetzung der eRechnung in Deutschland angelegt. Für die Bundesverwaltung beschreibt das Konzept die mögliche technische Umsetzung eines zentralen Eingangsrechnungsdienstes im Rahmen der IT-Konsolidierung Bund.

1.1 Zielsetzung

1.1.1 Zielsetzung der Umsetzung des zentralen eRechnungseingangs

Die Zielsetzung für die Schaffung eines zentralen eRechnungseingangs adressiert sowohl die Lieferanten und Dienstleister der Verwaltung als Rechnungssender als auch die Verwaltung selbst als Rechnungsempfänger[1].

Für die Rechnungssender soll Klarheit und Verlässlichkeit hinsichtlich der Einlieferungsprozesse und der technischen Anforderungen und damit Investitionsschutz geschaffen werden. Durch die Einrichtung eines zentralen eRechnungseingangs werden verwaltungseinheitliche Einlieferungsschnittstellen angeboten. Im Sinne des "One Stop Governments" gibt es einen Zugangspunkt zur Einlieferung von elektronischen Rechnungen. Dabei soll auf ein benutzerfreundliches Online-Portal aufgesetzt werden, bei dem der Benutzer/Rechnungssender mit maximal 3-Klicks zum Ziel kommen soll. Die Verfolgung einer zentralen Multikanal-Strategie beabsichtigt die Eröffnung von Möglichkeiten zur wirtschaftlichen Umsetzung auf Seiten der Rechnungssender in Abhängigkeit vom Rechnungsvolumen und von der vorhandenen technischen Ausstattung.

Auf Seiten der Verwaltung können durch den zentralen eRechnungseingang gleichartig wiederkehrende Prozesse – wie die Authentifizierung des Senders und die technische Prüfung der Nachricht bzw. Rechnung – an zentraler Stelle gebündelt und technisch gelöst werden. Der Pflegeaufwand wird reduziert und die Verwaltungsmitarbeiter werden nur mit technisch geprüften Rechnungen innerhalb eines digitalen Workflows konfrontiert, wodurch eine Reduktion der Komplexität im Umgang mit elektronischen Rechnungen verfolgt wird.

[1] Werden Personenbezeichnungen in diesem Dokument aus Gründen der besseren Lesbarkeit lediglich in der männlichen oder der weiblichen Form verwendet, so soll diese verkürzte Nennung jedoch das jeweils andere Geschlecht stets mit einschließen.

Folgende Aspekte werden in Rahmen der Umsetzung des zentralen eRechnungseingangs ausdrücklich nicht betrachtet:

- Der zentrale eRechnungseingang fokussiert sich auf die Entgegenahme und Weiterleitung der eingelieferten elektronischen Rechnung. Die Freigabe, Buchung, Zahlung und Archivierung von elektronischen Rechnungen sind nicht Gegenstand des zentralen eRechnungseingangs.
- Die verschiedenen Einlieferungsmöglichkeiten bieten teilweise auch weitere Nutzungsmöglichkeiten, welche im Rahmen der Umsetzung des zentralen eRechnungseingangs nicht weiter betrachtet werden. Hierzu zählen beispielsweise die von De-Mail-Anbietern zur Verfügung gestellten Angebote wie De-Safe (Bereitstellung eines Dokumentensafes) oder De-Ident (Möglichkeit zur Identitätsfeststellung, z. B. zur Registrierung an Online-Shops).

1.1.2 Zielsetzung des vorliegenden Dokuments

Das Architekturkonzept soll als Entscheidungshilfe für die Auswahl von bereits in der Bundesverwaltung bzw. in der Verwaltung des Landes Bremen vorhandenen technischen Komponenten im Kontext der eRechnung dienen. Eine Vergabe soll dabei zugunsten einer konsequenten Nachnutzung bestehender Komponenten obsolet werden.

Das Konzept beleuchtet ausdrücklich nur den bei seiner Erstellung aktuellen technologischen Zustand. Nur die Komponenten, die aktuell vorhanden bzw. geplant sind und für die Ressourcen im späteren Betrieb vorhanden sind, werden für eine Prüfung in Betracht gezogen. Technologische Fortschritte können in nachfolgenden Versionen dieses Dokuments berücksichtigt werden.

Folgende Aspekte werden im vorliegenden Dokument ausdrücklich nicht beleuchtet:

- Das Architekturkonzept stellt kein Pflichtenheft dar. Bindende Anforderungen insbesondere bei der Bereitstellung von Formularen zur Erfassung einer elektronischen Rechnung können nicht aufgestellt werden, da die finale Spezifikation der XRechnung zum aktuellen Zeitpunkt noch nicht verfügbar ist.
- Das Architekturkonzept stellt kein Installations-, Administrations- oder Betriebshandbuch, keine Schnittstellenbeschreibung, kein Sicherheits- oder Infrastrukturkonzept und ebenfalls keinen Implementierungsleitfaden dar. An entsprechenden Stellen des Dokuments wird daher auf weiterführende Literatur bzw. Dokumentationen verwiesen.
- Das Architekturkonzept konzentriert sich auf die konsequente Nachnutzung von vorhandenen Komponenten und die zwingend notwendigen Anforderungen für eine Annahme und Weiterleitung von elektronischen Rechnungen. Darüberhinausgehende Anforderungen, die möglicherweise in späteren Ausbaustufen umgesetzt werden können, werden ausdrücklich nicht erhoben.

1.1.3 Aufbau des Konzepts

Das vorliegende Architekturkonzept stellt den Weg zur technologischen Umsetzung eines zentralen eRechnungseingangs in der Bundesverwaltung vor. Grundsätzlich sollen sowohl von der Bundesverwaltung als auch von der Bremer Verwaltung die gleichen Anforderungen erhoben und über konkrete Anwendungen, Komponenten oder Dienste umgesetzt werden. Ist eine Unterscheidung, z. B. bei der eingesetzten Technologie, zwischen dem Bund und dem Land Bremen nötig, wird in diesem Dokument ausdrücklich darauf hingewiesen.

Ausgehend von bereits existierenden Modulen soll ein Architekturmodell empfohlen werden, das auf der IT-Gesamtstruktur des Bundes basiert. Hierfür werden die im Kontext der eRechnung jeweils vorhandenen Module auf eine mögliche Nachnutzung untersucht. Die Überprüfung anhand zuvor erhobener Abnahmekriterien soll dabei zu einer Empfehlung eines konkreten Architekturmodells führen. Sollten sich die untersuchten Module nicht für eine Empfehlung eignen, dienen die Abnahmekriterien bzw. die erarbeiteten Anforderungen als Grundlage für ein Lastenheft und für spätere Vergaben.

Um der Vorgabe der Nachnutzung von vorhandenen Modulen zu entsprechen, ist das Architekturkonzept wie folgt aufgebaut:

In Kapitel 1 wird sowohl die Zielsetzung eines zentralen eRechnungseingangs als auch die Zielsetzung für dieses Dokument dargelegt.

Kapitel 2 beschreibt die bereits vorhandenen Komponenten der Bundesverwaltung bzw. der Bremer Verwaltung, welche möglicherweise die Basisanforderungen eines zentralen eRechnungseingangs erfüllen und im späteren Verlauf des Dokuments anhand von erhobenen Abnahmekriterien für eine Nachnutzung im Kontext eRechnung geprüft werden.

Ein fachlicher SOLL-Entwurf des Rechnungseingangsprozesses wird in Kapitel 3 skizziert. Dort werden SOLL-Prozesse beschrieben, die bei der Einlieferung einer elektronischen Rechnung durchlaufen und deshalb besonders beachtet werden müssen.

Kapitel 4 beschreibt auf Grundlage der bereits vorhandenen Komponenten und des SOLL-Entwurfs die für die Annahme und Weiterleitung von elektronischen Rechnungen zwingend notwendigen fachlichen Anforderungen.

Die für einen zentralen eRechnungseingang notwendigen nicht-funktionalen Anforderungen werden in Kapitel 5 erhoben.

Die auf den funktionalen und nicht-funktionalen Anforderungen basierenden Abnahmekriterien werden in Kapitel 6 erläutert. Dabei gehen neben den zuvor erhobenen Anforderungen ebenso Anforderungen aus Sicht des zukünftigen Betreibers des zentralen eRechnungseingangs in die Kriterien ein.

In Kapitel 7 werden die identifizierten Komponenten anhand der zuvor erstellten Abnahmekriterien auf ihre tatsächliche Eignung zur Nachnutzung geprüft.

In Kapitel 8 wird ein konkretes Architekturmodell unter Nutzung der überprüften Komponenten empfohlen. Dabei werden der gesamte Systemkontext skizziert und die Lösungsbausteine mit ihren Komponenten beschrieben. Das Zusammenspiel wird anhand der Schnittstellen grob aufgezeigt.

2 Vorhandene Module in der Verwaltung im Kontext eRechnung

Dieses Kapitel benennt und skizziert die bereits innerhalb der Verwaltung des Bundes und des Landes Bremen vorhandenen Komponenten, die für eine Nachnutzung innerhalb der Umsetzung eines zentralen eRechnungseingangs in Frage kommen. Hierfür werden zunächst die Ausgangssituation sowie zwingend notwendige grobgranulare Basisfunktionalitäten an einen zentralen eRechnungseingang skizziert und daraus eine abstrakte fachliche Modulsicht abgeleitet. Die konkreten Komponenten, die die geforderten Basisfunktionalitäten möglicherweise erfüllen, werden daraufhin genannt und im weiteren Verlauf des Kapitels beschrieben.

2.1 Ausgangssituation

Die konsequente Nachnutzung bereits vorhandener Komponenten wurde als ein entscheidender Erfolgsfaktor bei der Umsetzung des zentralen eRechnungseingangs für eine möglichst schnelle und kostengünstige erste Umsetzung identifiziert. Aufgrund dessen wurden die IT-Dienstleister der Verwaltung des Bundes und des Landes Bremen nach bereits vorhandenen oder geplanten Komponenten befragt.

2.1.1 Basisfunktionalitäten eines zentralen eRechnungseingangs

Zur Unterstützung einer Vorauswahl der Komponenten wurden die folgenden Basisfunktionalitäten eines zentralen eRechnungseingangs beachtet:

- Möglichkeit zur Registrierung/Authentifikation eines Rechnungssenders: Ein Rechnungssender muss sich an dem zentralen eRechnungseingang registrieren und authentifizieren können.
- Möglichkeit zur Weberfassung/Web-Upload von Rechnungen durch einen Rechnungssender: Kleinen und mittelständischen Unternehmen, die nicht in der Lage sind, elektronische Rechnungen im Standard XRechnung zu erzeugen und digital einzuliefern, soll eine einfache Möglichkeit geboten werden, ihre Rechnungen nebst Anlagen über ein Webformular zu erfassen und abzuschicken.
- Angebot unterschiedlicher Übertragungskanäle für die Rechnungssender: Rechnungssendern sollen unterschiedliche Einlieferungsmöglichkeiten angeboten werden. Konkret soll u. a. eine Maschine-zu-Maschine-Kommunikation über einen Webservice angeboten werden, um eine schnelle und medienbruchfreie Kommunikation zu realisieren.
- Prüfung von elektronischen Rechnungen: Eingelieferte Rechnungen sollen anhand eines konkreten Schemas und anhand von Geschäftsregeln überprüft werden, um beim Sachbearbeiter eingelieferte fehlerhafte Rechnungen signifikant zu mindern.
- Adressierung und Weiterleitung von elektronischen Rechnungen an die Zielbehörde: Die zentral eingelieferten und geprüften Rechnungen sollen an die korrekte rechnungsempfangende Behörde weitergeleitet werden können.

2.1.2 Systemgrenzen

Aus den zuvor genannten Basisfunktionalitäten an einen zentralen eRechnungseingang lassen sich die folgenden Systemgrenzen ableiten. Das System beinhaltet unterschiedliche Einlieferungskanäle, die als Schnittstelle mit dem Rechnungssender dienen. Außerhalb des Systems liegen die verschiedenen Rechnungsfreigabesysteme der Verwaltung. Hierdurch wird eine Datenaustauschschnittstelle mit den externen Rechnungsfreigabesystemen definiert. Die folgende Abbildung zeigt beispielhaft den Systemkontext mit den enthaltenen Systemgrenzen.

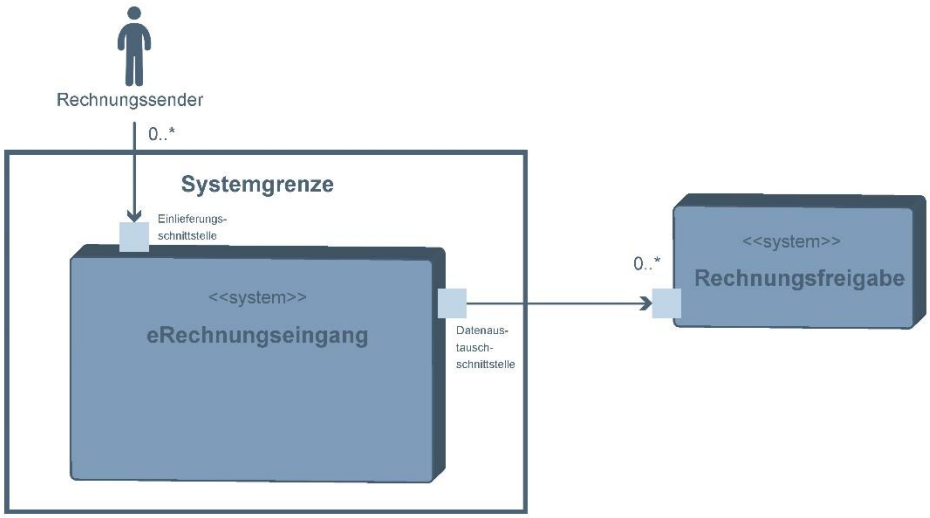

Abbildung 2.1: Systemkontext mit Systemgrenzen

Die fachlichen Module innerhalb der Systemgrenzen werden im folgenden Abschnitt erläutert. Alle Systeme, Komponenten, Dienste usw., welche außerhalb der Systemgrenzen des zentralen eRechnungseingangs liegen, werden im weiteren Verlauf dieses Dokuments nicht betrachtet.

2.1.3 Fachliche Modulübersicht

Die folgende Abbildung gibt einen groben Überblick über die fachlichen Module innerhalb der Systemgrenzen des zentralen eRechnungseingangs, welche sich aus den zuvor genannten Basisfunktionalitäten zusammensetzen.

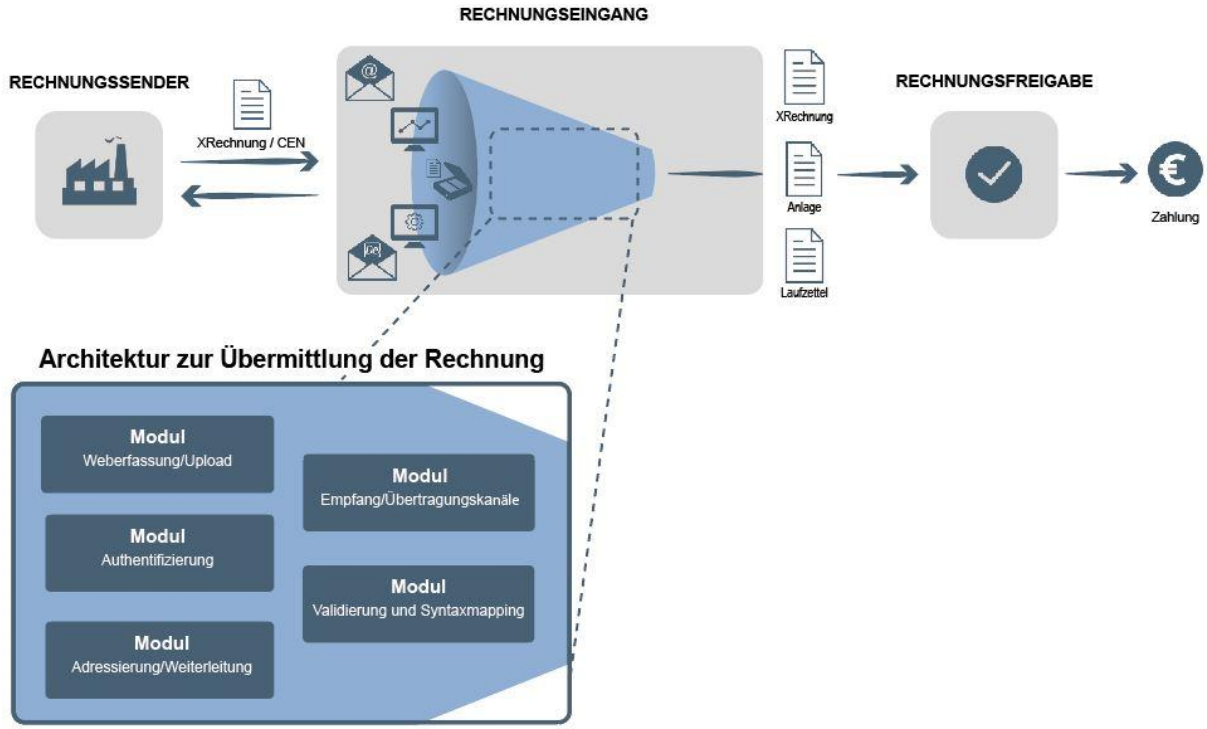

Abbildung 2.2: Fachliche Modulübersicht des zentralen eRechnungseingangs

Ein Rechnungssender liefert seine elektronische Rechnung über ein Webformular oder einen anderen angebotenen Übertragungskanal an den zentralen Rechnungseingang. Für eine erfolgreiche Lieferung muss sich der Rechnungssender vorher registriert/authentifiziert haben. Die eRechnung wird daraufhin validiert und durch eine eindeutige Adressierung jeweils an ein nachgelagertes System zur Rechnungsbearbeitung und -freigabe übermittelt. In dem jeweiligen Freigabesystem wird die eRechnung freigegeben und die Zahlung angewiesen.

Die elektronische Rechnung im Format XRechnung und die fachlichen Module werden nachfolgend kurz erläutert.

2.1.3.a XRechnung

Der Rechnungssender kann eine eRechnung in Form von sogenannten Nachrichten gemäß des jeweils gültigen Standards XRechnung auf unterschiedliche Weise an den Rechnungseingang übermitteln. Eine vollständige eRechnung setzt sich dabei aus dem Rechnungsdokument im XML-Format, allen vorhandenen rechnungsbegründenden Anlagen (z. B. Arbeitsnachweise) und einem elektronischen Laufzettel (z. B. Prüfberichte zur eRechnung) zusammen.

Für weitergehende Informationen sei an dieser Stelle an die finale Spezifikation der XRechnung verwiesen. Im weiteren Verlauf dieses Dokuments werden die Begriffe elektronische Rechnung, eRechnung und XRechnung synonym verwendet. Gemeint ist stets eine elektronische Rechnung im Format XRechnung.

2.1.3.b Weberfassung/Upload

Über eine Weberfassung kann ein Rechnungssender eine XRechnung über ein angebotenes Webformular manuell erfassen. Des Weiteren kann ein Rechnungssender eine XRechnung über einen Datei-Upload manuell hochladen.

2.1.3.c Übertragungskanäle

Über die folgenden Übertragungskanäle kann ein Rechnungssender eine XRechnung an einen zentralen eRechnungseingang übermitteln:

- per Webservice
- per De-Mail
- per E-Mail

Auch der Scan und die Umwandlung einer Papierrechnung in eine elektronische Rechnung wären als Einlieferungsweg denkbar. Hierbei könnte es zukünftig sowohl eine zentrale als auch viele dezentrale, kleinere Scanlösungen geben, die ein ersetzendes Scannen realisieren. Hiermit wird eine beweiswertige digitale Übersetzung der Rechnung realisiert, welche das Original in Papierform elektronisch ersetzt. Dieser Übertragungskanal, seine konkrete Ausgestaltung und Kommunikationswege werden im weiteren Verlauf des Dokuments nicht betrachtet. Die Untersuchung, ob ein zentraler Scandienst etabliert wird oder dezentrale Lösungen möglich sind, wird im Rahmen der Gemeinsamen IT des Bundes erfolgen.

2.1.3.d Authentifizierung

Nur einem zuvor registrierten/authentifizierten Rechnungssender stehen die Weberfassung und die weiteren Übertragungskanäle für die Einlieferung einer XRechnung offen.

2.1.3.e Validierung

Die übertragene eRechnung wird an zentraler Stelle anhand eines Schemas validiert und einer Schematronprüfung, welche die Geschäftsregeln des Standards XRechnung überprüft, unterzogen.

2.1.3.f Adressierung/Weiterleitung

Die eingelieferte XRechnung wird anhand eines eindeutigen Kriteriums dem jeweils nachgelagerten Freigabesystem der rechnungsempfangenden Behörde zur Verfügung gestellt. Dieses Kriterium kann eine verpflichtende Auftragskennnummer sein.

2.1.4 Identifizierte Komponenten zur Nachnutzung

Die nachfolgend genannten bereits genutzten oder geplanten Komponenten innerhalb der Verwaltung des Bundes wurden vom ITZBund identifiziert:

- das sich in der Umsetzung befindende Verwaltungsportal mit dem Servicekonto des Bundes für die Registrierung und Authentifizierung
- als Alternative zum Servicekonto des Bundes Governikus Autent für die Registrierung und Authentifizierung
- das Formular Management System des Bundes für die Weberfassung
- der Governikus MultiMessenger für die Realisierung unterschiedlicher Übertragungskanäle
- der WebSphere Process Server für die Adressierung/Weiterleitung der elektronischen Rechnungen (Dieser könnte ebenso für eine übergeordnete infrastrukturelle Orchestrierung der Komponenten genutzt werden.)

Für die Prüfung einer elektronischen Rechnung konnte weder in der Verwaltung des Bundes noch in der Verwaltung des Landes Bremen eine Komponente für eine konkrete Nachnutzung gefunden werden. Eine Eigenentwicklung, welche die Funktionalität zur Prüfung von elektronischen Rechnungen realisiert, erscheint nötig und sinnvoll. Diese könnte nach Einbringung in den IT-Planungsrat zentral nachgenutzt werden.

2.2 Formular Management System (Bund)

2.2.1 Kernfunktionalität

Das Formular Management System der Firma Lucom bietet die Möglichkeit unterschiedlichste Formulare webbasiert zu erfassen. Neben der reinen Formularerfassung können auch komplexere Workflowstrukturen abgebildet werden. Die erfassten Formulare können validiert und in eine Vielzahl von Datenformaten transformiert werden. Zudem können Drittsystemen die Inhalte über verschiedene bereits implementierte Schnittstellen zur Verfügung gestellt werden.

2.2.2 Beschreibung des Systems

2.2.2.a Kurzbeschreibung

Das Formular Management System (FMS) ist ein durch Java SE realisiertes System, welches einen formulargebundenen Austausch in Webanwendungen unterstützt. Die Formulare werden durch Standard-Webtechnologien umgesetzt. Das FMS basiert auf dem Produkt Lucom Interaction Platform (LIP) der Firma Lucom und bietet fertige Funktionalitäten zur Realisierung eines Online-Formulars.

Die Formulare sind der Hauptbestandteil des FMS. Sie werden Nutzern im Browser angezeigt und unterstützen diesen beim Ausfüllen. Die Eingabefelder können teilweise bereits vorausgefüllt werden. Bei der Eingabe der Daten im Browser durch den Benutzer können einzelne Felder validiert und Fehler unmittelbar als Fehlermeldung zurückgegeben werden. Die Umsetzung der Validierung erfolgt zum einen durch die technische Vorgabe von Formaten, zum anderen durch serverseitige fachliche oder technische Validierung aufgrund von festgelegten Regeln.

Sowohl beim Erfassen des Formulars als auch bei der Weiterleitung gibt es mehrere mögliche Formate, die vom FMS unterstützt werden. Die typischen Formate sind PDF, XML und CSV. Die eingegebenen Formulardaten werden in einer vorgegebenen XML-Struktur weitergegeben, welche alternativ auch als Anhang zur Weiterleitung hochgeladen werden kann.

Webservice-Schnittstellen sind im FMS integriert. Diese Schnittstellen können sowohl beim Eingang der Daten ins FMS als auch beim Ausgang der Daten an nachgelagerte Systeme genutzt werden. Das FMS ist für die Darstellung im Browser konzipiert und kann in bestehende Portale eingebunden werden.

Für detaillierte Informationen sei an dieser Stelle an die Referenzarchitektur FMS des ITZBund verwiesen (http://www.formular-management-system.de/SharedDocs/Publikationen/DE/Referenzarchitektur_FMS.html?nn=64794).

2.2.2.b Formularbereitstellung

Die Bereitstellung von Formularen ist der Hauptbestandteil des FMS. Formulare werden den Nutzern im Browser zum Ausfüllen angezeigt und unterstützen diesen beim Ausfüllen. Die Eingabefelder können auch vorbelegt werden. Die Formularinhalte werden dem Empfänger in einem strukturierten Format zur Weiterverarbeitung zur Verfügung gestellt.

Es besteht die Möglichkeit, Dateien an ein Formular anzuhängen. Dem Benutzer wird ein Upload-Bereich zur Verfügung gestellt. Die erlaubten Formate, die Anzahl der Anhänge sowie die Gesamtgröße des Formulars inkl. aller Anlagen können eingeschränkt werden.

Werden Dateien hochgeladen, können diese durch den Nutzer auch wieder heruntergeladen werden. Sie werden binär in der Datenbank gespeichert.

Das Speichern eines Zwischenstands wird mittels eines lokalen Downloads ermöglicht. Der Benutzer füllt das Formular nur teilweise aus, lädt den Zwischenstand herunter, speichert die Datei lokal auf seinem Gerät und kann sie zu einem späteren Zeitpunkt wieder in das FMS hochladen.

2.2.2.c Validierung

Bereits bei der Eingabe der Daten im Browser durch den Benutzer können einzelne Felder validiert werden. Zum einen durch die technische Vorgabe von Formaten, zum anderen durch serverseitige fachliche oder technische Validierung aufgrund von festgelegten Regeln.

2.2.2.d Webservices

Webservice-Schnittstellen sind im FMS integriert. Diese Schnittstellen können sowohl beim Eingang der Daten ins FMS als auch beim Ausgang der Daten an nachgelagerte Systeme genutzt werden.

Die Anbindung an Drittsysteme erfolgt über Konnektoren. Bisher sind ca. 15 Konnektoren von Lucom umgesetzt worden und können genutzt werden.

2.2.2.e Digitale Formate

Sowohl bei Eingang des Formulars als auch bei Ausgang gibt es mehrere mögliche Formate, die von FMS unterstützt werden. Die typischen Formate sind PDF, XML und CSV. Die eingegebenen Formulardaten werden in einer vorgegebenen XML-Struktur weitergegeben, welche alternativ auch als Anhang zur Weiterleitung hochgeladen werden kann.

2.2.2.f Mapping

Das Mapping im FMS wird mittels XSLT für große Datenstrukturen bzw. über Java-Script mit XML-Fragmenten für kleine Strukturen umgesetzt.

2.2.2.g Performance

Sollte ein Applikationsserver für die Menge der Anfragen nicht ausreichen, kann ein Cluster eingerichtet werden. Über einen vorgeschalteten Loadbalancer können die Anfragen verteilt werden.

2.2.2.h Portale

Das FMS ist für die Darstellung im Browser konzipiert und kann in bestehende Portale eingebunden werden. Sowohl die Einbettung des Formulars in eine Portal-Seite als auch die Präsentation in einem neuen Fenster sind möglich.

2.2.2.i Fachverfahren

Die Formulardaten werden vom FMS entgegen genommen, validiert und ggf. gespeichert. Anschließend werden sie an dahinterliegende Systeme weitergereicht. Das FMS bietet unterschiedliche Möglichkeiten der Anbindung an, z. B. per Webservice. Die XML-Strukturen werden dabei an einen Service weitergegeben, der das Routing zum adressierten Fachverfahren übernimmt.

2.2.2.j Verzeichnisdienste

Für den Anmeldeprozess können Verzeichnisdienste angebunden werden. Diese übernehmen die Registrierung, Identifikationsbestätigung, Rechtevergabe und die Autorisierung der Formularnutzung.

2.2.3 Zu prüfende Funktionalität im Kontext eRechnung (Bund)

Das FMS ist die Formular-Management-Komponente des Bundes und dort für alle IT-Verfahren eine Basiskomponente. Eine Bundeslizenz liegt vor, sodass alle Bundesbehörden das FMS nutzen können.

Im Kontext der eRechnung (Bund) könnte das FMS bei der manuellen Erfassung einer Rechnung durch die Rechnungssender über ein webbasiertes Formular zum Einsatz kommen. Ebenso wird der Upload von strukturierten Datenformaten (z. B. XRechnung) über das Web unterstützt.

2.2.3.a Manuelle Weberfassung von Rechnungen

Kleinen und mittelständischen Unternehmen, die nicht die Möglichkeit haben, ihre Rechnungen in einem strukturierten Datenformat zu erstellen und digital zu liefern, soll der zentrale eRechnungseingang die Möglichkeit geben, Rechnungen über ein webbasiertes Formular zu erfassen und weiterzuleiten – mit allen dazugehörigen Anlagen. Die Unternehmen sollen bei der Eingabe, wie in modernen Systemen üblich, möglichst durch den Erfassungsprozess geführt und über Validierungen unterstützt werden. Dies beschreibt die Kernfunktionalität, die vom FMS zur Verfügung gestellt wird.

2.2.3.b Webupload von elektronischen Rechnungen

Kleinen und mittelständischen Unternehmen, die zwar in der Lage sind, Rechnungen in einem strukturierten Datenformat zu erstellen, deren Rechnungsaufkommen allerdings gering ist, soll der zentrale Rechnungseingang die Möglichkeit bieten, ihre elektronischen Rechnungen über ein Web-Upload hochzuladen. Diese Funktionalität wird ebenso durch das FMS unterstützt.

2.2.4 Fazit

Die Kernfunktionalität des FMS besteht in der Bereitstellung von Formularen und der Unterstützung des Nutzers bei der Eingabe. Das FMS ist eine Basiskomponente des Bundes und wird bereits in anderen Verfahren produktiv eingesetzt. Da es die geforderten Funktionalitäten bereitstellt, wird es gegen die Abnahmekriterien des zentralen Rechnungseingangs im weiteren Verlauf des Dokuments geprüft.

2.3 Verwaltungsportal (Bund)

2.3.1 Kernfunktionalität

Das Verwaltungsportal des Bundes soll eine zentrale Anlaufstelle für alle Bürger und Unternehmen in Deutschland sein, um den Zugriff auf weitere Portale (z. B. Länderportale) oder Dienste (z. B. eRechnung) zur Verfügung zu stellen. Hierbei wird eine **Drei-Klick-Strategie** verfolgt, d. h., die gesuchte Information bzw. der gesuchte Dienst soll innerhalb von drei Klicks aufgefunden werden.

2.3.2 Kurzbeschreibung

Das Verwaltungsportal des Bundes soll im Laufe des Jahres 2017 in Produktion gehen. Technische Details sind zu diesem Zeitpunkt noch nicht bekannt.

2.3.3 Zu prüfende Funktionalität im Kontext eRechnung (Bund)

Das Webformular für die manuelle Erfassung einer eRechnung muss innerhalb einer Webanwendung, z. B. ein Portal, technisch zur Verfügung gestellt werden. Diesen Rahmen kann das Verwaltungsportal des Bundes bereitstellen.

2.3.4 Fazit

Das Verwaltungsportal des Bundes wird als Rahmen für die Weberfassung und den Web-Upload von elektronischen Rechnungen genutzt. Die Umsetzung der konkreten Funktionalitäten der Weberfassung und des Web-Uploads müssen allerdings von anderen Komponenten erbracht werden. Das Verwaltungsportal dient dabei als Hülle und als ein zentraler Webzugriffspunkt.

2.4 Servicekonto

2.4.1 Kernfunktionalität

Das Servicekonto bietet Funktionen zur sicheren Identifizierung von Bürgern und Unternehmen für Online-Anwendungen im Zusammenhang mit dem Verwaltungsportal und daran angeschlossenen Diensten. Die zentral verwaltete Nutzeridentität kann zur Registrierung/Authentifizierung für unterschiedliche Anwendungen und Dienste genutzt werden, sodass eine einmalige Registrierung ausreicht und kein wiederholtes Registrierungsverfahren durchlaufen werden muss.

2.4.2 Kurzbeschreibung

Das Servicekonto des Bundes soll im Laufe des Jahres 2017 in Produktion gehen. Technische Details sind zu diesem Zeitpunkt noch nicht bekannt.

2.4.3 Zu prüfende Funktionalität im Kontext eRechnung (Bund)

2.4.3.a Registrierung

Der zentrale eRechnungseingang soll den Rechnungssendern die Möglichkeit bieten, sich zu registrieren und nach erfolgreicher Registrierung über verschiedene Übertragungskanäle elektronische Rechnungen an die Bundesverwaltung digital zu verschicken. Das umzusetzende Servicekonto soll Nutzern (Unternehmen

und Bürgern) eine einmalige Registrierung und die Nutzung von daran angeschlossenen Diensten ermöglichen. Der zentrale eRechnungseingang kann dabei so konzipiert werden, dass dieser als Dienst zur Verfügung steht.

2.4.3.b Authentifizierung

Der Rechnungssender muss sich vor der Erfassung einer Rechnung über ein Webformular zuerst am System authentifiziert haben. Der Anschluss an das Servicekonto kann diese Authentifizierung umsetzen und könnte daneben auch ein sogenanntes Single Sign-On, d. h. eine Einmalanmeldung, zur Verfügung stellen. Der Rechnungssender kann damit ohne erneute Anmeldung auch andere an das Servicekonto angeschlossene Dienste nutzen.

2.4.4 Fazit

Das Servicekonto des Bundes wird für die Registrierung und Authentifizierung am zentralen eRechnungseingang vorgesehen. Da innerhalb des Zeitraums der Erstellung dieses Dokuments keine technischen Details bekannt waren und eine nicht rechtzeitige Umsetzung des Servicekontos als signifikantes Projektrisiko angesehen wird, ist der mögliche Einsatz einer alternativen Lösung als Übergangslösung vorzusehen. Die Komponente Governikus Autent realisiert als Kernfunktionalität die Registrierung und Authentifizierung von Nutzern und kann damit ebenso einer Prüfung als Teil des zentralen eRechnungseingangs unterzogen werden.

2.5 WebSphere Process Server (Bund)

2.5.1 Kernfunktionalität

Der WebSphere Process Server der Firma IBM dient primär zur Implementierung einer Service Oriented Architecture (SOA). Er bietet die Möglichkeit, unterschiedlichste Dienste bzw. Services miteinander zu orchestrieren. Hierfür werden Nachrichten transaktional angenommen und je nach Anwendungsfall an eine mögliche Vielzahl von angeschlossenen Adressaten weitergereicht. Durch die Orchestrierung der verschiedenen Dienste können auch komplexe Geschäftsprozesse und Workflows abgebildet werden.

2.5.2 Beschreibung des Systems

2.5.2.a Kurzbeschreibung

Der IBM WebSphere Process Server gehört zu einer Java-basierten Middleware Plattform nach SOA-Prinzipien und basiert auf dem WebSphere Application Server.

SOA basiert auf dem Prinzip, Funktionalitäten als Services anzubieten, welche über Schnittstellen aufgerufen werden. Als zentraler Nachrichtenempfänger können Nachrichten an unterschiedliche Systeme weitergeleitet werden. Die Daten kommen per Webservice zum WPS, welcher die Zieladresse des nachgelagerten Systems, an die diese Daten weitergegeben werden sollen, anhand der XML-Struktur ermittelt.

Die Architektur basiert auf offenen Standards wie Java, Java Enterprise Edition (JSP, EJB, JMS, JDBC), Webservices etc.

Mit dem WebSphere Process Server können Prozess- und Orchestrierungslogiken umgesetzt werden, also die Ausführung von modellierten Geschäftsprozessen. Dazu gehören z. B. die Entgegennahme von Nachrichten, das Auswerten und Weiterleiten an nachgelagerte Systeme anhand einer Entscheidungstabelle.

Zur Umsetzung wird die Business Process Execution Language (BPEL) genutzt, die Geschäftsprozesse auf Basis von XML beschreibt. BPEL eignet sich für die Integration verschiedener Systeme, die durch einen hohen Automatisierungsgrad und komplexe Transaktionssemantik gekennzeichnet sind. Einmal implementiert, laufen diese BPEL-Prozesse, beispielsweise zur Datenübertragung, automatisch und können auch nach dem konkreten Durchlauf detailliert nachvollzogen werden. Änderungen im Mapping können an zentraler Stelle angepasst und neu eingespielt werden.

Für detaillierte Informationen sei an dieser Stelle auf den Hersteller IBM verwiesen (https://www-01.ibm.com/software/integration/wps/).

2.5.2.b Einordnung

Der WebSphere Process Server ist eine konkrete Ausprägung des WebSphere Application Servers, der die Einbindung des BPEL-Moduls unterstützt.

Der WebSphere Application Server ist ein JEE Applikations Server, der JEE-basierte Anwendungen ausführen kann.

Der WebSphere Process Server ist ein Applikations Server, der daneben auch BPEL Prozesse ausführen kann. Hierfür sind spezielle Installationen, Lizenzen und Ressourcen notwendig. Diese sind im ITZBund bereits vorhanden und können bei Bedarf erweitert werden.

2.5.2.c Einsatzgebiet

Der WPS ist für Prozess- und Orchestrierungslogik entwickelt worden. Mit ihm können zuvor modellierte Geschäftsprozesse in einer heterogenen IT-Landschaft ausführbar gemacht werden. Webservices bieten einen standardisierten, plattformunabhängigen Zugriff auf unterschiedliche Systemfunktionalitäten. Die Entgegennahme von Nachrichten, die Auswertung und individuelle Weiterleitung anhand einer Entscheidungstabelle sind Kernkompetenzen des Process Servers.

Als Beschreibungssprache wird dabei die Business Process Execution Language (BPEL) verwendet. BPEL beschreibt Geschäftsprozesse auf Basis von XML. Die einzelnen Aktivitäten sind durch Webservices implementiert. BPEL eignet sich besonders für die Integration verschiedener Systeme, die durch einen hohen Automatisierungsgrad und komplexe Transaktionssemantik gekennzeichnet sind.

2.5.2.d Business Process Rules Manager

Der Business Process Rules Manager ist ein webbasiertes Werkzeug, das die Suche und Anpassung von Werten für Geschäftsregeln unterstützt. Dieses ist im WPS integriert und kann bei Bedarf nachinstalliert werden (falls es nicht bereits bei der Erstinstallation ausgewählt wurde).

Geschäftsregeln werden als IF-THEN-Regelset definiert, bei denen IF die Bedingung und THEN die Aktion der Regel darstellt. Diese können auch zur Laufzeit angepasst werden. Ein mögliches Einsatzgebiet wäre das Routing von Daten an nachgelagerte Systeme. Das Regelwerk ist über einen Browser einsehbar. In dieser Übersichtstabelle kann ein Admin jederzeit einen Überblick über z. B. angeschlossene Drittsysteme (denkbar wären hier z. B. Rechnungsfreigabesysteme von Behörden) bekommen und das Regelwerk bei Bedarf erweitern. Gespeicherte Änderungen am Regelwerk werden von dem Prozess, welcher auf die Entscheidungstabelle zugreift, direkt ohne Neuinstallation bzw. Neustart eingebunden. Fehlt dem Prozess die entsprechend notwendige Entscheidungszeile, bricht er mit einer Fehlermeldung ab.

2.5.2.e Merkmale des IBM WebSphere Process Server

Auf dem WPS werden sowohl kurzlaufende als auch langlaufende Prozesse ausgeführt. Langlaufende Prozesse beinhalten zumeist Human Tasks, also manuelle Aufgaben. Außerdem wird auf dem WPS die Verwaltung der Prozessanwendungen sichergestellt, wozu ein Mechanismus zur Versionierung und die Migration von Prozessen gehören. Es kann jederzeit auf eine neue oder alte Service-Version gewechselt werden, sofern die Schnittstellendefinition kompatibel ist.

Für eine transaktionssichere Kommunikation mit anderen Systemen nutzt der WPS den WebSphere Enterprise Service Bus. Dieser ist vordergründig für das Routing verantwortlich und nutzt dazu Standardprotokolle und Adapter. Der WPS stellt diese Funktionalitäten als Service für externe Systeme bereit.

Mechanismen für Clustering, Fail-Over, Transaktionsmonitoring, Security oder Caching werden ebenso vom Server bereitgestellt. Zusätzliche Produkte werden hierfür nicht benötigt.

2.5.2.f Kommunikation

Für die Drittanwendungen können Warteschlangen (JMS-Queues) zur Verfügung gestellt werden. Der WebSphere Application Server realisiert diese auf Basis des Service Integration Bus. Der Service Integration Bus stellt hochverfügbare und skalierbare Queues zur Verfügung, welche zur Datenspeicherung an eine Datenbank angeschlossen sind.

Die Kopplung zwischen Systemen erfolgt nicht direkt über entfernte JMS Verbindungen, sondern über einen „Store-And-Forward"- Ansatz: Die Anwendung liefert die Nachricht zuerst an einen lokalen QueueManager ab und dieser transferiert sie anschließend zur entfernten Queue. Dies hat den Vorteil, dass die Kommunikation auch dann fehlerfrei umgesetzt wird, wenn das Zielsystem oder das Netzwerk nicht verfügbar sind.

Eine Kommunikation über Webservices ist ebenso umsetzbar.

2.5.2.g Datenbanken Topologie

Es wird zwischen einer Verwaltungsdatenbank für den Process Server und einer Anwendungsdatenbank für die Nutzdaten aus der jeweiligen Anwendung unterschieden.

Im ITZBund werden sowohl DB2 von IBM als auch Oracle eingesetzt. Beide Datenbanksysteme werden von WebSphere für die Verwaltungsdatenbank und Anwendungsdatenbank unterstützt.

2.5.3 Zu prüfende Funktionalität im Kontext eRechnung (Bund)

Der WebSphere Process Server wird bereits im ITZBund produktiv betrieben. Vor Ort existiert ein tiefes Wissen über die Implementierung und Anpassung der Logik zur Orchestrierung von unterschiedlichen Diensten.

Im Kontext eRechnung (Bund) könnte der WebSphere Process Server zur Adressierung und Weiterleitung von elektronischen Rechnungen an die konkreten Freigabesysteme der einzelnen Behörden dienen. Ebenso erscheint die Software für den Einsatz zur Orchestrierung von verschiedenen Diensten des zentralen eRechnungseingangs (z. B. von der Annahme zur Prüfung bis zur Weiterleitung) geeignet.

2.5.3.a Adressierung

Nachdem der zentrale eRechnungseingang die elektronische Rechnung angenommen und technisch geprüft hat, muss diese an die korrekte Zielbehörde bzw. das Rechnungsfreigabesystem der Zielbehörde weitergeleitet werden. Hierfür könnte anhand eines eindeutigen Kriteriums innerhalb der elektronischen Rechnung entschieden werden, welche Behörde den korrekten Empfänger darstellt. Dies deckt sich mit der beschriebenen Funktionalität des WebSphere Process Servers, da dies einen Funktionsausschnitt der Orchestrierung verschiedener Services darstellt.

2.5.3.b Orchestrierung

Softwaresysteme können in unterschiedliche fachliche Komponenten unterteilt werden, die jeweils eine fachliche Aufgabe zur Verfügung stellen. Der zentrale eRechnungseingang könnte u. a. in die Annahme, Prüfung und Adressierung/Weiterleitung unterteilt werden. Für die korrekte Verbindung der fachlichen Komponenten und damit für die Umsetzung des gesamten Geschäftsprozesses mit allen benötigten Prozessschritten wird eine Orchestrierung der Komponenten bzw. Services benötigt. Der WebSphere Process Server dient zur Implementierung einer SOA und stellt damit die Umsetzung einer Orchestrierung von unterschiedlichen Diensten dar.

2.5.4 Fazit

Die Kernfunktionalität des WebSphere Process Servers besteht in der Bereitstellung und Umsetzung der Logik zur Orchestrierung (und damit auch Adressierung bzw. Weiterleitung von Nachrichten) unterschiedlichster Services, Komponenten, Anwendungen usw. und kann gegen Anforderungen des zentralen eRechnungseingangs im Hinblick auf die Adressierung und Orchestrierung geprüft werden. Ebenso wird er im ITZBund eingesetzt und die damit verbundenen Umsetzungen und Anpassungen von Orchestrierungslogiken werden bereits vor Ort erbracht. Daher wird der WebSphere Process Server im Verlauf des Dokuments anhand der Abnahmekriterien für einen Einsatz innerhalb des zentralen eRechnungseingangs (Bund) bewertet.

2.6 KoGIs/SIX CMS (Bremen)

2.6.1 Kernfunktionalität

Das KoGIs-Baukastensystem realisiert die Erstellung einer vollständigen Struktur und inhaltlichen Pflege von Internet- und Intranetauftritten. Hierfür werden Muster mit unterschiedlichen Layoutvorlagen und grundlegende Funktionen zur Verfügung gestellt. Darüber hinaus werden weitere Zusatzmodule angeboten, die wahlweise verwendet werden können.

Die Funktionen sind technisch vollständig barrierefrei gestaltet und entsprechen dem vorgeschriebenen bremischen Design der Verwaltung.

2.6.2 Beschreibung des Systems

2.6.2.a Kurzbeschreibung

Das KoGIs Baukastensystem (KoGIs - das Kompetenzzentrum für die Gestaltung der Informationssysteme bei der Senatorin für Finanzen) wird verpflichtend seit dem Jahr 2006 für die Erstellung und Pflege der Internet- und Intranetauftritte der Bremischen Verwaltung genutzt. Darüber hinaus wird der Baukasten freiwillig bei Eigenbetrieben und Gesellschaften eingesetzt.

Die Basismodule ermöglichen ein einheitliches vorgeschriebenes bremisches Design und basieren auf dem Content Management System (CMS) der Firma Six Offene Systeme GmbH (http://www.six.de/).

2.6.2.b Grundfunktionen

Administration der Benutzerverwaltung: Unterscheidung in Redakteure, Chefredakteure, Entwickler, Redakteure mit Zugriff auf Zusatzmodule

Aufbau der Struktur des Internet- und Intranetauftritts: Kopf, Navigation, Inhaltsbereich, Fußnavigation

Gestaltungselemente für die Pflege aller Strukturelemente: Kopf, Navigation, Inhaltsbereich, Fußnavigation

2.6.2.c Zusatzfunktionen

Das System kann um zusätzliche Funktionalitäten erweitert werden. Dies wird in Form von Modulen realisiert. Es existiert eine Vielzahl von Modulen, z. B. ein **Formularbaukasten**:

Das Zusatzmodul Formularbaukasten erstellt Formulare mit allen gängigen Formularfeldtypen und bietet die Möglichkeit, wahlweise die Formulardaten im CMS von KoGIs zu speichern oder per E-Mail zu versenden. Das verwendete Framework ist Symfony. Die Funktionen wurden mit XHTML in der SixCMS-eigenen Scriptsprache entwickelt. Detaillierte Informationen über die Zusatzmodule in Form von Handbüchern können unter http://www.kogis.bremen.de/handbuecher abgerufen werden.

2.6.2.d Technische Angaben

Beschreibung	Name	Version
Content Management System	SixCMS	9.0.5p3
Datenbank	MariaDB	10.0.23
Programmiersprache	PHP	7.0.3
Web-Server	Apache	2.4.18
Betriebssystem	Linux	4.4.0
Distribution	Ubuntu	16.04 LTS
PDF Erzeugung	PDFlib	9.0.6
PHP Framework	Symfony	2

Tabelle 2.1: KoGIs – Technische Angaben

2.6.3 Zu prüfende Funktionalität im Kontext eRechnung (Bremen)

Im Kontext der eRechnung (Bund) könnte das KoGIs Baukastensystem bei der manuellen Erfassung einer Rechnung durch die Rechnungssender über ein webbasiertes Formular zum Einsatz kommen. Ebenso wird der Upload von strukturierten Datenformaten (z. B. einer elektronischen Rechnung) über das Web unterstützt.

2.6.3.a Manuelle Weberfassung von Rechnungen

Kleinen und mittelständischen Unternehmen, die nicht die Möglichkeit haben, ihre Rechnungen in einem strukturierten Datenformat zu erstellen und digital zu liefern, soll der zentrale eRechnungseingang die Möglichkeit bieten, Rechnungen über ein webbasiertes Formular zu erfassen und weiterzuleiten. Durch den Einsatz des Zusatzmoduls Formularbaukasten des KoGIs Baukastensystems können Rechnungssendern webbasierte Formulare für die Erfassung zur Verfügung gestellt werden.

2.6.3.b Web-Upload von elektronischen Rechnungen

Kleinen und mittelständischen Unternehmen, die zwar in der Lage sind, Rechnungen in einem strukturierten Datenformat zu erstellen, deren Rechnungsaufkommen allerdings gering ist, soll der zentrale Rechnungseingang die Möglichkeit geben, ihre elektronischen Rechnungen über ein Web-Upload hochzuladen. Ein Datei-Upload von elektronischen Rechnungen und rechnungsbegründenden Anlagen kann über das KoGIs CMS realisiert werden.

2.6.4 Fazit

Eine manuelle Erfassung und ein Datei-Upload von elektronischen Rechnungen können mit dem KoGIs Baukastensystem umgesetzt werden. Es wird im Land Bremen für die Erstellung und die Pflege von Internet- und Intranetauftritten genutzt. Das System wird im weiteren Verlauf des Dokuments anhand der Abnahmekriterien für den Einsatz im Land Bremen geprüft.

2.7 Governikus MultiMessenger (Bund/Bremen)

2.7.1 Kernfunktionalität

Der Governikus MultiMessenger (GMM) ist eine Multikanal-Kommunikationsplattform, die alle in der öffentlichen Verwaltung relevanten Nachrichten-Transportkanäle und zukünftig auch alle europäischen elektronischen Einschreib-Zustelldienste technisch-juristisch verarbeiten kann.

Jede vom GMM entgegengenommene elektronische Nachricht wird vereinheitlicht, geprüft und protokolliert sowie im gewünschten Format an das jeweils zuvor definierte interne System bzw. an den relevanten externen Empfänger weitergeleitet.

2.7.2 Beschreibung des Systems

2.7.2.a Kurzbeschreibung

Der Governikus MultiMessenger nimmt wie eine zentrale Poststelle sämtliche elektronischen Nachrichten aus den unterschiedlichen Quellen entgegen und leitet diese nach Ablauf der Prüfroutinen an ein Zielsystem.

Nachdem der GMM die Nachrichten aus dem Quellsystem entgegengenommen hat, wird das Format vereinheitlicht und die zentrale Ver- und Entschlüsselung sowie Überprüfung der qualifiziert elektronischen Signaturen der Nachrichten sowie der mitgesendeten Anhänge auf Gültigkeit nach SigG veranlasst. Für die Zertifikatsprüfungen greift der GMM auf die Anwendung Governikus des IT-Planungsrates zu. Damit ist auch die Verifikation europäischer Signaturen und Zeitstempel gewährleistet.

Alle wichtigen Informationen und Prüfergebnisse werden in einem Laufzettel protokolliert, der der jeweiligen Nachricht zugeordnet und im Poststellenbuch vermerkt ist. Eine lückenlose Nachweisbarkeit ist somit gewährleistet. Über die konfigurierbaren Quittungsnachrichten bestätigt der GMM dem Absender einer Nachricht deren Prüfung und Weiterleitung.

Anders als bei Postfächern, in denen Nachrichten für spätere Zugriffe vorgehalten werden, übergibt der GMM aktiv Nachrichten an ein Zielsystem (Push-Mechanismus). Quell- und Zielsysteme, Prüfroutinen, Laufzettel und weitere Einstellungen werden über virtuelle Postfächer (VPF) gesteuert.

2.7.2.b Kommunikationswege

Die nachfolgende Tabelle beschreibt die unterschiedlichen Nachrichtentypen, in welche der Governikus MultiMessenger Nachrichten kategorisiert.

Nachrichtentyp	Beschreibung
Inbound Nachrichten	Der GMM empfängt über die unterschiedlichen externen Eingangskanäle alle eingehenden elektronischen Nachrichtenformate wie E-Mails, De-Mails, EGVP/OSCI-Nachrichten, Nachrichten aus Web-Portalen, E-Postbriefe und zukünftig eDelivery. Die Nachrichten werden geprüft und intern in das jeweils gewünschte Zielsystem zur Vorgangsbearbeitung weitergeleitet. Als Zielsystem können flexibel Fachverfahren, DMS- oder eAkten-Systeme sowie das intern verwendete E-Mail-System angebunden werden. Die eindeutige Zuordnung der internen Empfänger wird dabei über virtuelle Postfächer festgelegt.
Outbound Nachrichten	Des Weiteren werden die ausgehenden elektronischen Nachrichten, die direkt intern aus einem angebundenen Fachverfahren, eAkten-System oder aber von einem internen E-Mail-Server versendet werden, vom GMM entgegengenommen und nach Ablauf der Prüfroutinen an das gewünschte Kommunikationssystem des externen Empfängers weitergeleitet. Dabei wird eine explizite Zugangseröffnung durch den externen Kommunikationspartner unterstützt. Möchte der Nutzer also lediglich per De-Mail kontaktiert werden, sorgt der

Nachrichtentyp	Beschreibung
	GMM dafür, dass er die Nachricht auch per De-Mail erhält. Die Identitäten der externen Empfänger werden im internen Identitäten-Speicher verwaltet.
Interne Nachrichten	Interne Nachrichten sind von einem Virtuellen Postfach (VPF) oder einem zugeordneten Sachbearbeiter abgesendete Nachrichten, die an eine externe Adresse eines VPF des GMM adressiert werden. Diese Nachrichten verlassen nicht die Instanz des GMM und werden direkt weitergeleitet. Optional besteht die Möglichkeit, auch diese Nachrichten über das äußere Transportsystem, wie z. B. den De-Mail Provider, zu routen.

Tabelle 2.2: Governikus MultiMessenger – Nachrichtentypen

2.7.2.c Virenprüfung

Nachrichten können bei Bedarf über eine angeschlossene Antivirus-Lösung auf Schadsoftware geprüft werden.

2.7.2.d Schnittstellen

Alle Schnittstellen des GMM sind an offenen nationalen und internationalen Standards ausgerichtet, wie beispielsweise SPML, SMTP oder XTA2.

- Durch die Verwendung des offenen SPML Webservice-Standards ist der GMM zu anderen Identitätsspeichern (z.B. Servicekonten, Lokalen Systemen mit LDAP Schnittstelle etc.) kompatibel. Beispielsweise kann der GMM an den Autent-Server der Anwendung Governikus des IT-Planungsrates angebunden werden. Governikus Autent ermöglicht ein umfassendes Identitätsmanagement, unterstützt den fachverfahrensseitigen Aufruf eines geforderten Vertrauensniveaus und bietet gemäß TR 03107-1 Authentisierungsmethoden an.
- Über die SMTP-Schnittstelle kann das vorhandene Mailsystem, beispielsweise Microsoft Exchange oder Lotus Domino, angeschlossen werden.
- Über die SOAP-basierte XTA2-Schnittstelle kann der GMM in sicheren Netzen Nachrichten mit Webportalen, Fachverfahren oder DMS-Systemen austauschen.
- Der GMM besitzt eine generische Schnittstelle zur Anbindung beliebiger Antivirus-Dienste.
- Zur frühzeitigen Beweiswertsicherung können eingehende Nachrichten über die TR-ESOR-konforme Schnittstelle unmittelbar nach Eingang zusätzlich an ein Langzeitspeichersystem bzw. DMS-Systems übergeben werden. Über die Referenzierung des Archiv-Datenpaketes in der weitergeleiteten Nachricht können nachgelagerte Vorgangsbearbeitungssysteme eine Verknüpfung zum Archiv aufbauen, um beispielsweise fachliche Verknüpfungen zu schaffen.

2.7.3 Zu prüfende Funktionalität im Kontext eRechnung

2.7.3.a Bereitstellung von verschiedenen Übertragungskanälen für die Einlieferung von elektronischen Rechnungen

Dem Rechnungssender sollen verschiedene Übertragungskanäle zur Einlieferung einer elektronischen Rechnung zur Verfügung gestellt werden. Neben der Erfassung bzw. dem Datei-Upload über ein Webformular sollen auch die Übertragung per Webservice, De-Mail und E-Mail ermöglicht werden. Die Einlieferung von Nachrichten über unterschiedliche Übertragungskanäle stellt die Kernfunktionalität des Governikus MultiMessenger dar und kann somit realisiert werden.

2.7.4 Fazit

Der Governikus MultiMessenger unterstützt die Einlieferung von Nachrichten (und Anhängen) über unterschiedliche Übertragungskanäle und erfüllt damit eine Basisanforderung an den zentralen eRechnungseingang. Im weiteren Verlauf des Dokuments wird die Komponente gegen die Abnahmekriterien des Gesamtsystems geprüft.

2.8 Governikus Autent (Bund/Bremen)

Das Servicekonto des Bundes gilt als gesetzte Komponente für die Registrierung und Authentifizierung von Rechnungssendern für die Umsetzung innerhalb des Bundes. Sollte diese nicht rechtzeitig realisiert werden, könnte der Governikus Autent als mögliche Übergangslösung eingesetzt werden.

Davon unberührt kann der Governikus Autent zur Umsetzung für die Registrierung und Authentifizierung im Land Bremen genutzt werden.

2.8.1 Kernfunktionalität

Governikus Autent stellt Server- und Client-Komponenten zur Verfügung, um eine Authentisierung mittels elektronischer Identitäten sicherzustellen.

Je nach gefordertem Sicherheits- und Vertrauensniveau eines konkreten Kommunikationsszenarios kann Governikus Autent sowohl mit der Online-Ausweisfunktion des Personalausweises bzw. elektronischen Aufenthaltstitels umgehen, als auch zertifikatsbasierte oder Benutzername / Passwort basierte Authentisierungen vornehmen.

2.8.2 Beschreibung des Systems

2.8.2.a Allgemeines

Neben dem sicheren Transport von vertraulichen Daten muss eine Authentisierung der Kommunikationsteilnehmer in Abhängigkeit vom konkret geforderten Vertrauensniveau ermöglicht werden. Für ein umfassendes Identitätsmanagement, auch unter den Gesichtspunkten SingleSign-On und Interoperabilität, steht mit der Anwendung Governikus Autent ein Funktionsbaustein für den Aufbau sicherer und föderierter Kommunikationsinfrastrukturen zur Verfügung. Die in der TR 03107-1 definierten Vertrauensniveuas können bedient werden. Außerdem ermöglicht Governikus Autent zur Umsetzung der eIDAS-Verordnung den Umgang mit europäischen Identitäten.

2.8.2.b Logische Systemübersicht

Für den ganzheitlichen Umgang mit elektronischen Identitäten, also dem sicheren Identifizieren und Verwalten der Kommunikationspartner, dem Zulassen berechtigter und der Verhinderung unberechtigter Zugriffe auf Inhalte und Dienstleistungen stehen folgende drei Module/Komponenten zur Verfügung, die unter der Anwendung Governikus Autent zusammengefasst sind:

Governikus Autent Server:

Als zentrale Serverkomponente ist der der Governikus Autent Server für den Authentisierungsvorgang von digitalen Identitäten verantwortlich, d.h. ein Zugriff auf den dahinterstehenden Identitätsspeicher erfolgt stets via Governikus Autent Server. Hierfür stehen eine Vielzahl an standardisierten Schnittstellen wie SPML, Rest(SCIM), SAML und WebServices zur Verfügung. Es werden die gängigen Authentisierungsverfahren Username/Password, Zertifikate bzw. Token unterstützt. Darüber hinaus wird die Online-Ausweisfunktion (eID-Funktion) des nPA/eAT unterstützt. Im Rahmen des durch die CEF geförderten Projektes TREATS (TRans-European AuThentication Services), das die Governikus KG als Konsortialführer leitet, wird der Autent-Server dahingehend erweitert, auch entsprechend notifizierte europäische Identifikationsmittel zu unterstützen.

Governikus Autent ID Connect:

Governikus Autent ID Connect ist ein Erweiterungsmodul zum Governikus Autent Server. Es stellt als zentrales Modul für das Identitätsmanagement für Servicekonten und Portalverbünde die Interoperabilität zu anderen Servicekonten im Portalverbund sicher. Hierfür wird die für die Wahrung der Schriftform notwendige Funktion der Protokollierung bereitgestellt.

Mit Autent ID Connect wird eine vereinfachte Anbindung von fachlichen Szenarien an den Governikus Autent Server als auch zur Anbindung an ein sogenanntes Berechtigungszertifikat im Falle einer eID Nutzung (nPA/eID) ermöglicht.

Governikus Autent Frontend:

Mit Governikus Autent Frontend wird die Oberfläche zur Benutzerverwaltung zur Verfügung gestellt. Dies sind Funktionen für registrierte Benutzer/Identitäten (bspw. Selbstverwaltung der eigenen Daten, E-Mail-Verifikation) und Funktionen für sogenannten Identitätsadministratoren. Die Identitätsadmins haben so die

Möglichkeit, Benutzer/Identitäten freizuschalten oder Daten zu ändern bzw. zu ergänzen, gemäß dem dahinterliegenden Rechte-/Rollenkonzept. Die grafischen Oberflächen sind konfigurativ anpassbar.

2.8.2.c Unterstützung von interoperablen Servicekonten

Interoperable Servicekonten stellen eine Erweiterung der Servicekonten dar. Das Konzept hierfür wird durch die PG eID-Strategie entwickelt.

In dem Pilotprojektes zu interoperablen Servicekonten, das im Rahmen der PG eID-Strategie im Auftrag des IT-Planungsrates mit den Ländern Bayern und Nordrhein-Westfalen durchgeführt wird, wird das Servicekonto.NRW auf Basis von Governikus Autent als zentrale Single Sign-On Lösung realisiert.

2.8.2.d Unterstützung unterschiedlicher Vertrauensniveaus bzw. Level of Assurance

In der Technischen Richtlinie Nr. 3107-1 Version 1.1 des Bundesamtes für Sicherheit in der Informationstechnik (BSI), die sich mit Elektronischen Identitäten und Vertrauensdiensten im E-Government beschäftigt, werden u. a. grundlegende Kriterien für sogenannte Vertrauensniveaus festgelegt, analog zu der Definition von „Level of Assurance" (LoA) im EU-Kontext in der eIDAS-Durchführungsverordnung (EU2015/1502). Die Vertrauensniveaus bewerten die Qualität und Vertrauenswürdigkeit von Mechanismen anhand verschiedener technischer und organisatorischer Faktoren, z. B. der Sicherheit der Authentisierung, der Güte der Registrierung und der Möglichkeit zum zeitnahen Sperren bzw. zum Rückruf eines verwendeten Authentisierungsverfahrens.

Die Vertrauensniveaus werden in der o. g. Technischen Richtlinie in die drei Kategorien „normal", „substantiell" und „hoch" unterteilt, die analogen Level of Assurance der eIDAS Verordnung heißen „low", „substantial" und „high". Governikus Autent unterstützt den fachverfahrensseitigen Aufruf eines geforderten Vertrauensniveaus und bietet Authentisierungsmethoden an, die mindestens dem gewünschten Level of Assurance entsprechen.

2.8.3 Zu prüfende Funktionalität im Kontext eRechnung (Bund/Bremen)

Als Bestandteil der Anwendung Governikus des IT-Planungsrates kann Governikus Autent sowohl vom Bund als auch von den Ländern ohne weitere Lizenzkosten abgerufen werden.

Im Kontext der eRechnung können über den Governikus Autent sowohl die Registrierung als auch die Authentifizierung realisiert werden.

2.8.3.a Registrierung

Der zentrale eRechnungseingang soll den Rechnungssendern die Möglichkeit bieten sich zu registrieren und nach erfolgreicher Registrierung elektronische Rechnungen an die Verwaltung digital zu verschicken. Eine Registrierung kann über den Governikus Autent realisiert werden.

2.8.3.b Authentifizierung

Der Rechnungssender muss sich vor der Erfassung einer Rechnung über ein Webformular zuerst am System authentifiziert haben. Der Governikus Autent kann diese Authentifizierung umsetzen und könnte daneben auch ein sogenanntes Single Sign-On, d. h. eine Einmalanmeldung, zur Verfügung stellen. Der Rechnungssender kann damit ohne erneute Anmeldung auch andere föderierte (an das System angeschlossene) Dienste nutzen.

2.8.4 Fazit

Die Basisanforderung einer Registrierung und Authentifizierung am zentralen eRechnungseingang gehören zum Kernfunktionsumfang des Governikus Autent. Ebenso ist er als Bestandteil der Anwendung Governikus bereits eine Komponente des IT-Planungsrates und kann sowohl vom Bund als auch von den Ländern lizenzkostenfrei genutzt werden. Die Komponente wird im weiteren Verlauf des Dokuments anhand der Abnahmekriterien des zentralen eRechnungseingangs überprüft.

Da eine rechtzeitige Umsetzung des Servicekontos des Bundes als signifikantes Projektrisiko für eine erfolgreiche Realisierung des zentralen eRechnungseingangs des Bundes identifiziert wurde, kann die Komponente Governikus Autent als alternative Übergangslösung zur Nutzung des Servicekontos angedacht und ebenso für den Bund geprüft werden.

2.9 Zusammenfassung

Auf Grundlage weniger Basisfunktionalitäten und unter der Maßgabe der konsequenten Nachnutzung vorhandener Komponenten und ggf. optional einzurichtenden zentralen Klärungsstelle wurden die folgenden in der Verwaltung bereits vorhandenen Komponenten identifiziert, die im weiteren Verlauf des Dokuments anhand von Abnahmekriterien überprüft werden.

Die folgende Tabelle gibt einen Überblick über die in der Verwaltung des Bundes identifizierten Komponenten:

Fachliche Aufgabe	Komponente (Bund)
Weberfassung/Upload	Formular Management System, Verwaltungsportal des Bundes als Rahmen
Übertragungskanäle	Governikus MultiMessenger
Authentifizierung	Servicekonto des Bundes (Governikus Autent als mögliche Übergangslösung)

Fachliche Aufgabe	Komponente (Bund)
Validierung	n. v.
Adressierung/Weiterleitung	WebSphere Process Server

Tabelle 2.3: Komponenten zur Nachnutzung im Bund

3 SOLL-Konzeption der Annahme und Weiterleitung von eRechnungen

Im Folgenden wird die SOLL-Konzeption der Annahme und Weiterleitung von eRechnungen anhand der grundlegenden Prozesse aus Sicht des Empfangssystems des Rechnungseingangs beschrieben.

Im ersten Unterkapitel erfolgt die Darstellung dieser grundlegenden Prozesse. Zunächst werden in einem geringen Detailgrad die Registrierung sowie die Rechnungsannahme und -weiterleitung unterschieden nach Einlieferungskanälen beschrieben. Im zweiten Unterkapitel erfolgt die Abgrenzung von Komponenten und deren Integration vom Komponentenmodell auf der Seite des Rechnungseingangs.

Die in diesem Kapitel dargestellten Prozesse und Komponenten dienen als Grundlage der in den Kapiteln 4 und 5 definierten funktionalen und nicht-funktionalen Anforderungen.

3.1 Grundlegende Prozesse der Rechnungsannahme und -weiterleitung

Die grundlegenden Prozesse der Registrierung und Benutzerselbstverwaltung (z. B. die Möglichkeit zur selbständigen Passwortanpassung) sowie der Einlieferung einer eRechnung und deren Verarbeitung sind hier im Überblick beschrieben. Es werden dabei durchgängig die Rollen des Rechnungssenders (**RS**) und des Rechnungseingangs (**RE**) als rechnungsempfangendes System unterschieden. Der Rechnungssender kann der Rechnungssteller sein, muss es aber nicht. Es kann sich dabei auch um einen vom Rechnungssteller beauftragten Dritten handeln. Der Fokus der Betrachtungen liegt auf den Prozessen beim Rechnungseingang.

Das Symbol  stellt einen Subprozess dar, der im hier gewählten Abstraktionsgrad nicht weiter aufgelöst wird und weitere Interaktionen mit der anderen Rolle enthalten kann (z. B. im Fehlerfall bei Prüfprozessen).

3.1.1 Registrierung

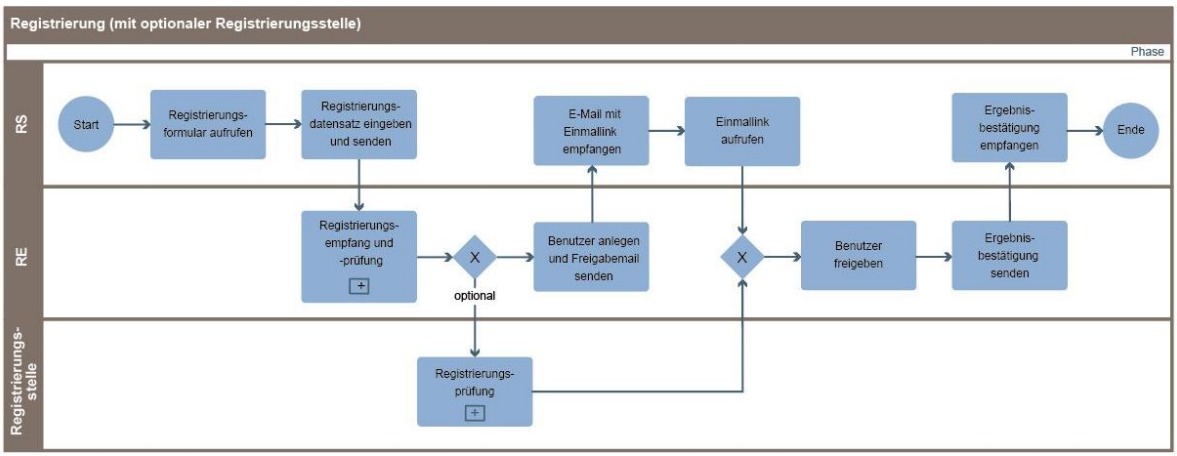

Abbildung 3.1: Prozess – Registrierung

Der Prozess der Registrierung beinhaltet optional den Subprozess der Prüfung und Freigabe des Benutzerkontos durch eine Registrierungsstelle. Es ist geplant, dabei auf die Entwicklungen beim Servicekonto aufzubauen. Da noch keine abschließenden Informationen über die geplanten Prozesse aus dem Schwesterprojekt vorliegen, ist der Zeitpunkt der Einbindung einer Registrierungsstelle noch nicht abschließend geklärt und hier als Platzhalter zu verstehen.

Insgesamt soll sich die Registrierung nach den Vorgaben des Onlinezugangsgesetzes (OZG) richten.

Name	Registrierung natürlicher oder juristischer Personen
Akteure/Rolle	(nicht registrierter) Rechnungssender
Beschreibung	Der Rechnungssender registriert sich mittels Webanwendung.
Vorbedingungen	keine
Nachbedingung/Ergebnis	Freischaltung des Benutzerkontos durch das Benutzen des Einmallinks in der erhaltenen E-Mail
Standardablauf	1. Registrierungsformular aufrufen: Der Rechnungssender ruft die Registrierfunktion der Webanwendung auf und wird auf eine Eingabemaske für die erforderlichen Identitäts- und Kommunikationsdaten geleitet. 2. Registrierungsdatensatz eingeben: Der Rechnungssender erfasst die erforderlichen Registrierungsdaten und sendet sie ab. 3. Subprozess Registrierungsempfang und -prüfung: Der Rechnungseingang empfängt die Registrierungsdaten und unterzieht sie einer (technischen) Prüfung. 4. Benutzer anlegen und Freigabemail senden: Das Benutzerkonto wird angelegt und eine Freigabemail mit Einmallink zur Bestätigung wird an den Rechnungssender versendet. 5. E-Mail mit Einmallink empfangen: Der Rechnungssender erhält die E-Mail mit dem Einmallink. 6. Einmallink aufrufen: Der Rechnungssender führt den Einmallink aus. 7. Benutzer freigeben: Der Rechnungssender wird durch das Benutzen des Einmallinks freigeschaltet. 8. Ergebnisbestätigung senden: Der Rechnungseingang versendet eine Bestätigungsnachricht über die Freischaltung.

Name	Registrierung natürlicher oder juristischer Personen
	9. Ergebnisbestätigung empfangen: Der Rechnungssender erhält die Bestätigungsnachricht.
Alternativer Ablauf	optionaler Subprozess Registrierungsprüfung: Optional führt eine (zentrale) Registrierungsstelle eine weitere Prüfung der Registrierung bzw. Freigabe durch.

Tabelle 3.1: Prozess – Registrierung

3.1.1.a Passwort nach Passwortverlust ändern

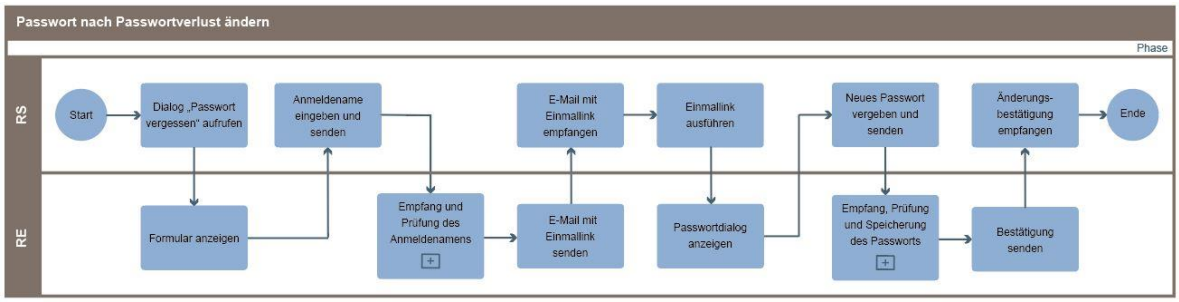

Abbildung 3.2: Prozess – Passwort ändern

Name	Passwort nach Passwortverlust ändern
Akteure/Rolle	(registrierter) Rechnungssender
Beschreibung	Der Rechnungssender ändert sein Passwort.
Vorbedingungen	Erfolgreiche Registrierung
Nachbedingung/Ergebnis	Neues Passwort gespeichert und freigegeben

Name	Passwort nach Passwortverlust ändern
Standardablauf	1. Dialog "Passwort vergessen" aufrufen: (Registrierter) nicht angemeldeter Rechnungssender ruft den Dialog „Passwort vergessen“ auf. 2. Formular anzeigen: Der Rechnungseingang fragt vom Rechnungssender den Benutzernamen über ein Formular ab. 3. Anmeldename eingeben und senden: Der Rechnungssender trägt seinen Benutzernamen in das Formular ein und sendet es ab. 4. Subprozess Empfang und Prüfung des Anmeldenamens: Der Anmeldename wird vom Rechnungseingang empfangen und gegen die Identitätsdatenbank geprüft. 5. E-Mail mit Einmallink senden: Der Rechnungseingang sendet einen Einmallink zur Passworteingabe an die E-Mail-Adresse (Rückkanaladresse) des Rechnungssenders. 6. E-Mail mit Einmallink empfangen: Der Rechnungssender erhält die E-Mail. 7. Einmallink ausführen: Der Rechnungssender führt den Link aus. 8. Passwortdialog anzeigen: Der Rechnungseingang sendet den Dialog zur Passwortvergabe an den Rechnungssender. 9. Neues Passwort vergeben und senden: Der Rechnungssender gibt zweimal sein neues Passwort in das bereitgestellte Formular ein und sendet es an den Rechnungseingang. 10. Subprozess Empfang, Prüfung und Speicherung des Passworts: Der Rechnungseingang erhält das neue Passwort, prüft es und speichert es in der Identitätsdatenbank. 11. Bestätigung senden: Der Rechnungseingang sendet eine Bestätigung der Passwortänderung an den Rechnungssender. 12. Änderungsbestätigung empfangen: Der Rechnungssender empfängt die Bestätigungsnachricht.
Alternativer Ablauf	1. Die Prüfung des Anmeldenamens schlägt fehl (Schritt 4). Der Rechnungssender erhält einen Hinweis und kann einen anderen Benutzernamen eingeben. 2. Die Prüfung des geänderten Passworts schlägt fehl (Schritt 10). Der Rechnungssender erhält einen Hinweis und kann ein anderes Passwort wählen.

Name	Passwort nach Passwortverlust ändern
	3. Optional könnte noch eine Freigabe der Passwortänderung durch eine Registrierungsstelle erfolgen. Näheres hierzu wird sich voraussichtlich aus den Vorgaben zum Servicekonto ergeben.

Tabelle 3.2: Prozess – Passwort ändern

3.1.1.b Benutzerdaten ändern

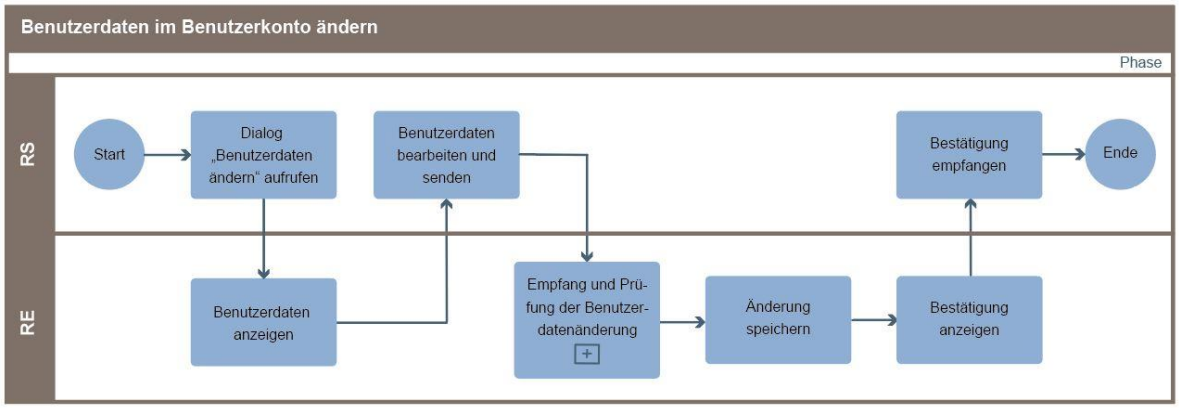

Abbildung 3.3: Prozess – Benutzerdaten ändern

Name	Benutzerdaten im Benutzerkonto ändern
Akteure/Rolle	(registrierter und angemeldeter) Rechnungssender
Beschreibung	Der Rechnungssender ändert persönliche oder verfahrensspezifische Daten.
Vorbedingungen	Benutzerkonto erstellen
Nachbedingung/Ergebnis	Änderungen gespeichert und protokolliert

Name	Benutzerdaten im Benutzerkonto ändern
Standardablauf	1. Dialog "Benutzerdaten ändern" aufrufen: Der Rechnungssender wählt die Funktion „Benutzerdaten ändern“ aus. 2. Benutzerdaten anzeigen: Die Benutzerdaten werden in einer Dialogmaske zur Bearbeitung angezeigt. 3. Benutzerdaten bearbeiten und senden: Der Rechnungssender kann freigegebene Felder bearbeiten und die Änderungen zum Speichern senden. 4. Subprozess Empfang und Prüfung der Benutzerdatenänderung: Der geänderte Identitäts- und/oder Verfahrensdatensatz wird empfangen und geprüft. 5. Änderung speichern: Die Änderungen werden im zugehörigen Benutzerkonto gespeichert. 6. Bestätigung senden: Dem Rechnungssender wird eine Bestätigung der Änderungen übermittelt. 7. Bestätigung empfangen: Der Rechnungssender empfängt eine Bestätigung seiner Änderungen.
Alternativer Ablauf	1. Die Änderung konnte nicht durchgeführt werden (Schritt 4). Der Rechnungssender erhält eine technische Rückmeldung über den hinterlegten Rückkanal.

Tabelle 3.3: Prozess – Benutzerdaten ändern

3.1.1.c Benutzerkonto löschen

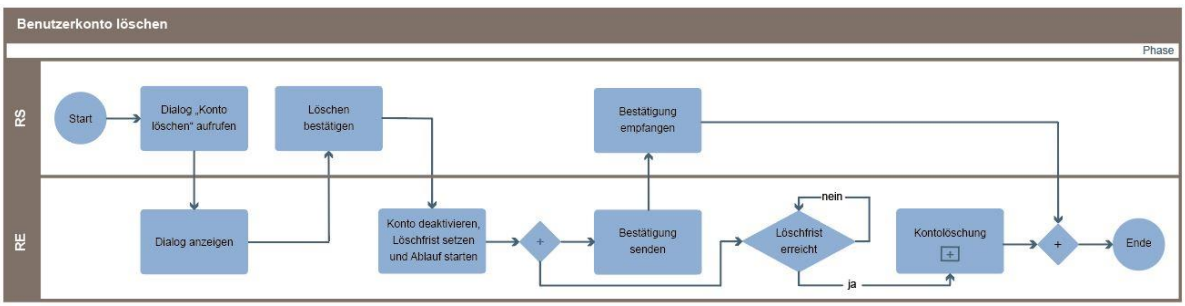

Abbildung 3.4: Prozess – Benutzerkonto löschen

Name	Benutzerkonto löschen
Akteure/Rolle	(registrierter und angemeldeter) Rechnungssender
Beschreibung	Der Rechnungssender löst einen Löschauftrag aus und löscht das vorhandene Benutzerkonto.
Vorbedingungen	Erfolgreiche Anmeldung am Benutzerkonto
Nachbedingung/Ergebnis	Protokollierung des Vorgangs in der Datenbank des Moduls AU
Standardablauf	1. Dialog "Konto löschen" aufrufen: Der Rechnungssender fordert die „Löschen"-Funktion an. 2. Dialog anzeigen: Der Rechnungseingang zeigt den Löschdialog mit der Bestätigungsabfrage an. 3. Löschen bestätigen: Der Rechnungssender bestätigt die Löschanforderung. 4. Konto deaktivieren, Löschfrist setzen und Ablauf starten: Das Konto wird deaktiviert, die Löschfrist wird gesetzt und deren Ablauf gestartet. 5. Bestätigung senden: Dem Rechnungssender wird eine Bestätigung gesendet. 6. Bestätigung empfangen: Dem Rechnungssender wird eine Bestätigung der Entgegennahme des Löschauftrages mit Hinweis auf die Löschfrist gesendet. 7. Subprozess Kontolöschung: Nach Erreichen der Löschfrist wird das Konto gelöscht.
Alternativer Ablauf	1. Der Rechnungssender beendet den Vorgang mittels „Abbrechen" (Schritt 3). 2. Die Löschung konnte nicht durchgeführt werden (Schritt 7). Der Rechnungssender erhält eine technische Rückmeldung über den hinterlegten Rückkanal.

Tabelle 3.4: Prozess – Benutzerkonto löschen

3.1.2 Erfassung über ein Webformular

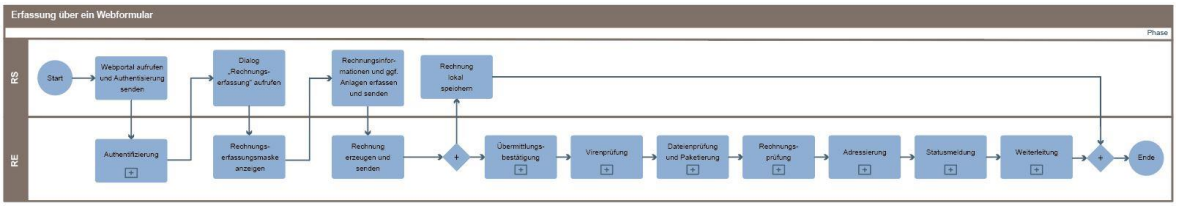

Abbildung 3.5: Prozess – Weberfassung

Name	Erfassung über ein Webformular
Akteure/Rolle	(registrierter) Rechnungssender
Beschreibung	Der Rechnungssender erfasst und sendet eine Rechnung über das Webformular.
Vorbedingungen	Der Rechnungssender ist registriert und hat die Weberfassung als Einlieferungskanal ausgewählt.
Nachbedingung/Ergebnis	Die technisch geprüfte Rechnung nebst Anlagen und Laufzettel ist an ein weiterverarbeitendes System (z. B. Workflow) weitergeleitet.
Standardablauf	1. Webportal aufrufen und Authentisierung senden: Der Rechnungssender ruft das Webportal des Rechnungsempfängers auf und meldet sich mit Benutzernamen und Passwort am System an. 2. Subprozess Authentifizierung: Der Rechnungsempfänger prüft die Anmeldeinformationen und meldet den Benutzer am System an. 3. Dialog "Rechnungserfassung" aufrufen: Der Rechnungssender wählt die Funktion "Rechnungserfassung" aus. 4. Rechnungserfassungsmaske anzeigen: Der Rechnungsempfänger stellt dem Rechnungssender eine Rechnungserfassungsmaske zur Verfügung. 5. Rechnungsinformationen und ggf. Anlagen erfassen und senden: Der Rechnungssender erfasst die Rechnungsinformation, lädt diese und ggf. begleitende Unterlagen hoch und versendet diese an den Rechnungsempfänger.

Name	Erfassung über ein Webformular
	6. Rechnung erzeugen und senden: Der Rechnungseingang empfängt die Rechnungsinformationen sowie ggf. begleitende Unterlagen und erzeugt aus den empfangenen Rechnungsinformationen ein valides XRechnungsdokument. 7. Rechnung lokal speichern: Die erzeugte Rechnung wird dem Rechnungssender zum lokalen speichern (download) bereitgestellt. 8. Subprozess Übermittlungsbestätigung: Dem Rechnungssender wird eine Bestätigung der erfolgreichen Übermittlung im Browser angezeigt. 9. Subprozess Virenprüfung: Es erfolgt eine Prüfung der Dateien auf Viren. 10. Subprozess Dateienprüfung und Paketierung: Die hochgeladenen Dateien werden einer ersten Prüfung (z. B. Format, Größe) unterzogen, ein Laufzettel wird angelegt und aus den empfangenen Dateien wird ein Rechnungspaket erstellt. 11. Subprozess Rechnungsprüfung: Die Rechnung aus dem Rechnungspaket wird auf Schemakonformität sowie auf Einhaltung der Geschäftsregeln geprüft. 12. Subprozess Adressierung: Die Adressierung der Rechnung wird ermittelt. 13. Subprozess Statusmeldung: Dem Rechnungssender wird eine Statusmeldung übermittelt/zur Verfügung gestellt. 14. Subprozess Weiterleitung: Das Rechnungspaket wird auf Basis der Adressierung an den entsprechenden Rechnungsworkflow weitergeleitet.
Alternativer Ablauf	1. Schlägt die Prüfung der Anmeldeinformationen (Schritt 2) fehl, erscheint wieder die Eingabemaske für die Anmeldeinformationen mit einem Hinweis auf die fehlgeschlagene Anmeldung. 2. Liegt ein Befund bei der Virenprüfung (Schritt 9) vor, erfolgt eine Rückmeldung an den Rechnungssender und die Dateien werden verworfen. 3. Wurden unzulässige Anlagen hochgeladen (Schritt 10), erfolgt eine Rückmeldung an den Rechnungssender, die Anlagen werden verworfen und können erneut hochgeladen werden. 4. Enthält das Ergebnis der Rechnungsprüfung (Schritt 11) annahmebehindernde Meldungen, wird die Rechnung verworfen und es erfolgt eine Rückmeldung an den Rechnungssender. 5. Optional: Ist eine Adressierung der Rechnung (Schritt 12) nicht möglich, ist die Rechnung an eine ggf. optional einzurichtende zentrale Klärungsstelle weiterzuleiten, die die Empfängerermittlung manuell durchführt.

Tabelle 3.5: Prozess – Weberfassung

3.1.2.a Zwischenstand einer Erfassung über ein Webformular lokal speichern

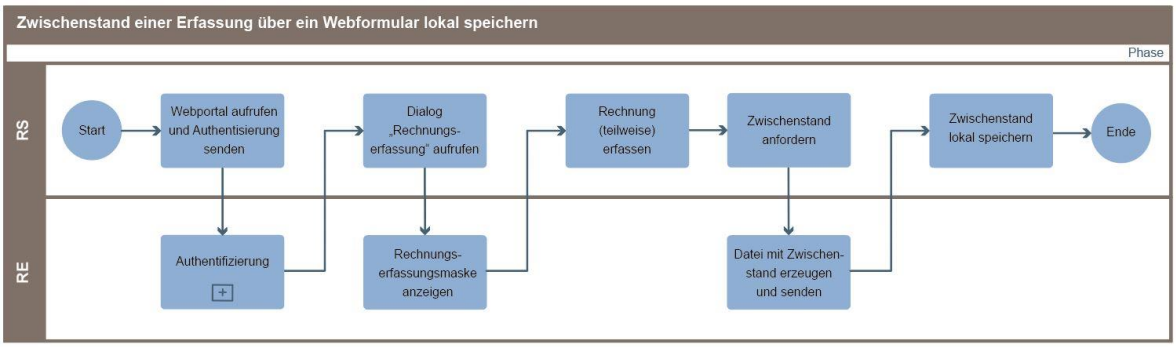

Abbildung 3.6: Prozess – Zwischenstand speichern

Name	Zwischenstand einer Erfassung über ein Webformular lokal speichern
Akteure/Rolle	(registrierter) Rechnungssender
Beschreibung	Der Rechnungssender speichert einen Erfassungszwischenstand einer Rechnung über ein Webformular lokal ab.
Vorbedingungen	Der Rechnungssender ist registriert und hat die Weberfassung als Einlieferungskanal ausgewählt.
Nachbedingung/Ergebnis	Der Zwischenstand ist lokal gespeichert.
Standardablauf	1. Webportal aufrufen und Anmeldeinformationen senden: Der Rechnungssender ruft das Webportal des Rechnungseingangs auf und meldet sich mit dem Benutzernamen und dem Passwort am System an. 2. Subprozess Authentifizierung: Der Rechnungseingang prüft die Anmeldeinformationen und meldet den Benutzer am System an. 3. Dialog "Rechnungserfassung" aufrufen: Der Rechnungssender wählt die Funktion "Rechnungserfassung" aus. 4. Rechnungserfassungsmaske anzeigen: Der Rechnungseingang stellt dem Rechnungssender eine Rechnungserfassungsmaske zur Verfügung.

Name	Zwischenstand einer Erfassung über ein Webformular lokal speichern
	5. Rechnung (teilweise) erfassen: Der Rechnungssender gibt die Rechnungsinformationen in der Erfassungsmaske ein. 6. Zwischenstand anfordern: Der Rechnungssender fordert einen Zwischenstand seiner Eingaben als lokal speicherbare Datei an. 7. Datei mit Zwischenstand erzeugen: Der Rechnungseingang erzeugt eine Zwischenstandsdatei und stellt sie dem Rechnungssender zur Verfügung. 8. Zwischenstand lokal speichern: Der Rechnungssender speichert die Zwischenstandsdatei lokal auf seinem Rechner.
Alternativer Ablauf	1. Schlägt die Prüfung der Anmeldeinformationen (Schritt 2) fehl, erscheint erneut die Eingabemaske für die Anmeldeinformationen mit einem Hinweis auf die fehlgeschlagene Anmeldung.

Tabelle 3.6: Prozess – Zwischenstand speichern

3.1.2.b Erfassung über ein Webformular aus lokalem Zwischenstand fortsetzen

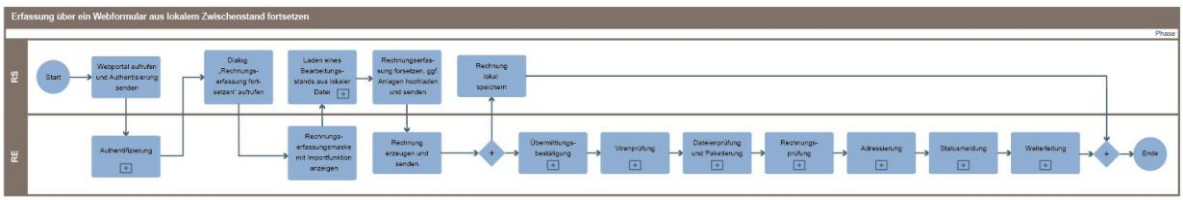

Abbildung 3.7: Prozess – Zwischenstand laden

Name	Erfassung über ein Webformular aus lokalem Zwischenstand fortsetzen
Akteure/Rolle	(registrierter) Rechnungssender
Beschreibung	Der Rechnungssender setzt die Erfassung einer Rechnung über ein Webformular aus einem lokal gespeicherten Zwischenstand fort.

Name	Erfassung über ein Webformular aus lokalem Zwischenstand fortsetzen
Vorbedingungen	Der Rechnungssender ist registriert, hat die Weberfassung als Einlieferungskanal ausgewählt und verfügt über einen lokal gespeicherten Zwischenstand.
Nachbedingung/Ergebnis	Die technisch geprüfte Rechnung nebst Anlagen und Laufzettel ist an ein weiterverarbeitendes System (z. B. Workflow) weitergeleitet.
Standardablauf	1. Webportal aufrufen und Anmeldeinformationen senden: Der Rechnungssender ruft das Webportal des Rechnungseingangs auf und meldet sich mit dem Benutzernamen und dem Passwort am System an. 2. Subprozess Authentifizierung: Der Rechnungseingang prüft die Anmeldeinformationen und meldet den Benutzer ggf. am System an. 3. Dialog "Rechnungserfassung fortsetzen" aufrufen: Der Rechnungssender wählt die Funktion "Rechnungserfassung fortsetzen" aus. 4. Rechnungserfassungsmaske mit Importfunktion anzeigen: Der Rechnungseingang stellt dem Rechnungssender eine Rechnungserfassungsmaske, in die eine lokale Zwischenstandsdatei importiert werden kann, zur Verfügung. 5. Subprozess Laden eines Bearbeitungsstands aus lokaler Datei: Der Rechnungssender lädt einen Zwischenstand aus lokaler Datei in die Rechnungserfassungsmaske. Ggf. wird die Maske durch den Rechnungseingang aus der Zwischenstandsdatei befüllt und dem Rechnungssender anschließend vorausgefüllt zur Verfügung gestellt. 6. Rechnungserfassung fortsetzen, ggf. Anlagen hochladen und senden: Der Rechnungssender vervollständigt die Erfassung der Rechnungsinformationen, lädt diese und ggf. begleitende Unterlagen hoch und versendet sie an den Rechnungseingang. 7. Rechnung erzeugen und senden: Der Rechnungseingang empfängt die Rechnungsinformationen sowie ggf. begleitende Unterlagen und erzeugt aus den empfangenen Rechnungsinformationen ein valides XRechnungsdokument. 8. Rechnung lokal speichern: Die erzeugte Rechnung wird dem Rechnungssender zum lokalen Speichern (Download) bereitgestellt. 9. Subprozess Übermittlungsbestätigung: Dem Rechnungssender wird eine Bestätigung der erfolgreichen Übermittlung im Browser angezeigt. 10. Subprozess Virenprüfung: Es erfolgt eine Prüfung der Dateien auf Viren.

Name	Erfassung über ein Webformular aus lokalem Zwischenstand fortsetzen
	11. Subprozess Dateienprüfung und Paketierung: Die hochgeladenen Dateien werden einer ersten Prüfung (z. B. Format, Größe) unterzogen und aus den empfangenen Dateien wird ein Rechnungspaket erstellt. 12. Subprozess Rechnungsprüfung: Die Rechnung aus dem Rechnungspaket wird auf Schemakonformität sowie auf Einhaltung der (harten/technischen) Geschäftsregeln geprüft. 13. Subprozess Adressierung: Die Adressierung der Rechnung wird ermittelt. 14. Subprozess Statusmeldung: Dem Rechnungssender wird eine Statusmeldung übermittelt/zur Verfügung gestellt. 15. Subprozess Weiterleitung: Das Rechnungspaket wird auf Basis der Adressierung an den entsprechenden Rechnungsworkflow weitergeleitet.
Alternativer Ablauf	1. Schlägt die Prüfung der Anmeldeinformationen (Schritt 2) fehl, erscheint erneut die Eingabemaske für die Anmeldeinformationen mit einem Hinweis auf die fehlgeschlagene Anmeldung. 2. Kann der Zwischenstand nicht importiert werden (Schritt 5), erhält der Rechnungssender eine Fehlermeldung und kann den Import bei Bedarf wiederholen. 3. Liegt ein Befund bei der Virenprüfung (Schritt 10) vor, erfolgt eine Rückmeldung an den Rechnungssender und die Dateien werden verworfen. 4. Wurden unzulässige Anlagen hochgeladen (Schritt 11), erfolgt eine Rückmeldung an den Rechnungssender. Die Anlagen werden verworfen und können erneut hochgeladen werden. 5. Enthält das Ergebnis der Rechnungsprüfung (Schritt 12) annahmebehindernde Meldungen, wird die Rechnung verworfen und es erfolgt eine Rückmeldung an den Rechnungssender. 6. Optional: Ist eine Adressierung der Rechnung (Schritt 13) nicht möglich, ist die Rechnung an eine zentrale Klärungsstelle weiterzuleiten, die die Empfängerermittlung manuell durchführt.

Tabelle 3.7: Prozess – Zwischenstand laden

3.1.2.c Upload über ein Webformular

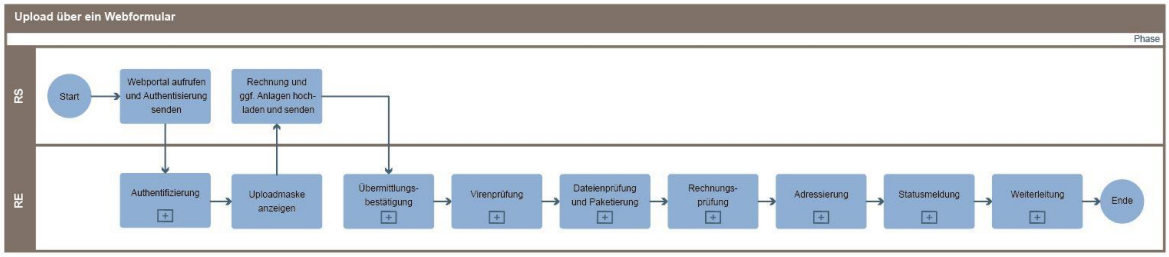

Abbildung 3.8: Prozess – Web-Upload

Name	Upload über ein Webformular
Akteure/Rolle	(registrierter) Rechnungssender
Beschreibung	Der Rechnungssender lädt eine aus einer Fachanwendung erstellte, vorhandene e-Rechnung hoch und versendet diese.
Vorbedingungen	Der Rechnungssender ist registriert und hat den Upload als Einlieferungskanal ausgewählt.
Nachbedingung/Ergebnis	Die technisch geprüfte Rechnung nebst Anlagen und Laufzettel ist an ein weiterverarbeitendes System (z. B. Workflow) weitergeleitet.
Standardablauf	1. Webportal aufrufen und Authentisierung senden: Der Rechnungssender ruft das Webportal des Rechnungsempfängers auf und meldet sich mit Benutzernamen und Passwort am System an. 2. Subprozess Authentifizierung: Der Rechnungsempfänger prüft die Anmeldeinformationen und meldet den Benutzer am System an. 3. Dialog "Rechnungserfassung" aufrufen: Der Rechnungssender wählt die Funktion "Rechnungserfassung" aus. 4. Rechnungserfassungsmaske anzeigen: Der Rechnungsempfänger stellt dem Rechnungssender eine Rechnungserfassungsmaske zur Verfügung. 5. Rechnungsinformationen und ggf. Anlagen erfassen und senden: Der Rechnungssender erfasst die Rechnungsinformation, lädt diese und ggf. begleitende Unterlagen hoch und versendet diese an den Rechnungsempfänger.

Name	Upload über ein Webformular
	6. Rechnung erzeugen und senden: Der Rechnungsempfänger empfängt die Rechnungsinformationen sowie ggf. begleitende Unterlagen und erzeugt aus den empfangenen Rechnungsinformationen ein valides XRechnungsdokument. Das XRechnungsdokument wird an den Rechnungssender zum Herunterladen gesendet. 7. Rechnung lokal speichern: Die erzeugte Rechnung wird dem Rechnungssender zum lokalen speichern (download) bereitgestellt. 8. Subprozess Übermittlungsbestätigung: Dem Rechnungssender wird eine Bestätigung der erfolgreichen Übermittlung im Browser angezeigt. 9. Subprozess Virenprüfung: Es erfolgt eine Prüfung der Dateien auf Viren. 10. Subprozess Dateienprüfung und Paketierung: Die hochgeladenen Dateien werden einer ersten Prüfung (z. B. Format, Größe) unterzogen, ein Laufzettel wird angelegt und aus den empfangenen Dateien wird ein Rechnungspaket erstellt. 11. Subprozess Rechnungsprüfung: Die Rechnung aus dem Rechnungspaket wird auf Schemakonformität sowie auf Einhaltung der Geschäftsregeln geprüft. 12. Subprozess Adressierung: Die Adressierung der Rechnung wird ermittelt. 13. Subprozess Statusmeldung: Dem Rechnungssender wird eine Statusmeldung übermittelt/zur Verfügung gestellt. 14. Subprozess Weiterleitung: Das Rechnungspaket wird auf Basis der Adressierung an den entsprechenden Rechnungsworkflow weitergeleitet.
Alternativer Ablauf	1. Schlägt die Prüfung der Anmeldeinformationen (Schritt 2) fehl, erscheint erneut die Eingabemaske für die Anmeldeinformationen mit einem Hinweis auf die fehlgeschlagene Anmeldung. 2. Liegt ein Befund bei der Virenprüfung (Schritt 7) vor, erfolgt eine Rückmeldung an den Rechnungssender und die Dateien werden verworfen. 3. Schlägt die Dateiprüfung fehl (Schritt 8), erfolgt eine Rückmeldung an den Rechnungssender und die Dateien werden verworfen. Der Rechnungssender erhält die Möglichkeit, die hochgeladenen Dateien auszutauschen. 4. Enthält das Ergebnis der Rechnungsprüfung (Schritt 9) annahmebehindernde Meldungen, wird die Rechnung verworfen und es erfolgt eine Rückmeldung an den Rechnungssender.

Name	Upload über ein Webformular
	5. Optional: Ist eine Adressierung der Rechnung (Schritt 10) nicht möglich, ist die Rechnung an eine ggf. optional einzurichtende zentrale Klärungsstelle weiterzuleiten, die die Empfängerermittlung manuell durchführt.

Tabelle 3.8: Prozess – Web-Upload

3.1.3 Einlieferung über Webservice

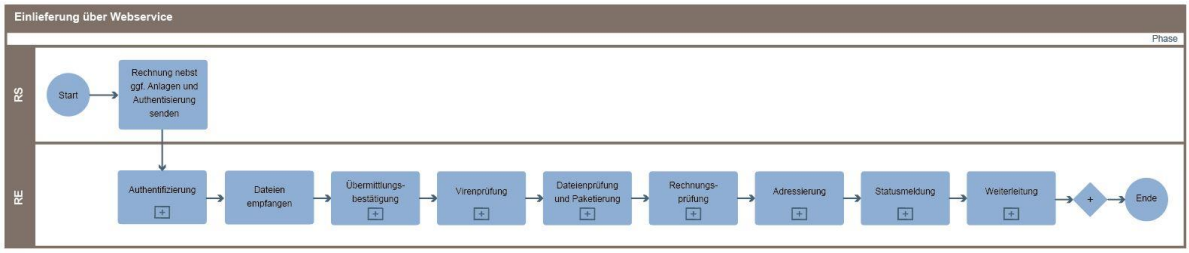

Abbildung 3.9: Prozess – Einlieferung über Webservice

Name	Einlieferung über Webservice
Akteure/Rolle	(registrierter) Rechnungssender
Beschreibung	Der Rechnungssender verschickt eine eRechnung (ggf. nebst Anlagen) über eine Webservice-Schnittstelle.
Vorbedingungen	Der Rechnungssender ist registriert und hat den Webservice als Einlieferungskanal ausgewählt.
Nachbedingung/Ergebnis	Die technisch geprüfte Rechnung nebst Anlagen und Laufzettel ist an ein weiterverarbeitendes System (z. B. Workflow) weitergeleitet.

Name	Einlieferung über Webservice
Standardablauf	1. Rechnung nebst ggf. Anlagen und Authentisierung senden: Der Rechnungssender versendet über seine Fachanwendung als Client des Webservices die Rechnung sowie ggf. ergänzende Anlagen. Dabei werden auch der Benutzername und das Passwort mitgeliefert. 2. Subprozess Authentifizierung: Der Rechnungseingang prüft die Anmeldeinformationen und lässt den Benutzer ggf. zur Einlieferung zu. 3. Dateien empfangen: Der Rechnungseingang nimmt die gesendeten Dateien über die Webservice-Schnittstelle entgegen. 4. Subprozess Virenprüfung: Es erfolgt eine Prüfung der Dateien auf Viren. 5. Subprozess Dateienprüfung und Paketierung: Die gesendeten Dateien werden einer ersten Prüfung (z. B. Format, Größe) unterzogen und aus den empfangenen Dateien wird ein Rechnungspaket erstellt. 6. Subprozess Empfangsbestätigung: Der Rechnungseingang protokolliert den Empfang, legt einen Laufzettel an und versendet eine Empfangsbestätigung an den Rechnungssender. 7. Subprozess Rechnungsprüfung: Die Rechnung aus dem Rechnungspaket wird auf Schemakonformität sowie auf Einhaltung der (harten/technischen) Geschäftsregeln geprüft. 8. Subprozess Adressierung: Die Adressierung der Rechnung wird ermittelt. 9. Subprozess Statusmeldung: Dem Rechnungssender wird eine Statusmeldung übermittelt/zur Verfügung gestellt. 10. Subprozess Weiterleitung: Das Rechnungspaket wird auf Basis der Adressierung an den entsprechenden Rechnungsworkflow weitergeleitet.
Alternativer Ablauf	1. Schlägt die Prüfung der Anmeldeinformationen (Schritt 2) fehl, wird der Dateiempfang verweigert und es erfolgt eine Rückmeldung an den Rechnungssender. 2. Liegt ein Befund bei der Virenprüfung (Schritt 4) vor, erfolgt eine Rückmeldung an den Rechnungssender und die Dateien werden verworfen. 3. Schlägt die Dateiprüfung fehl (Schritt 5), erfolgt eine Rückmeldung an den Rechnungssender und die Dateien werden verworfen. 4. Enthält das Ergebnis der Rechnungsprüfung (Schritt 7) annahmebehindernde Meldungen, wird die Rechnung verworfen und es erfolgt eine Rückmeldung an den Rechnungssender.

Name	Einlieferung über Webservice
	5. Optional: Ist eine Adressierung der Rechnung (Schritt 8) nicht möglich, ist die Rechnung an eine ggf. optional einzurichtende zentrale Klärungsstelle weiterzuleiten, die die Empfängerermittlung manuell durchführt.

Tabelle 3.9: Prozess – Webservice

3.1.4 Einlieferung über De-Mail

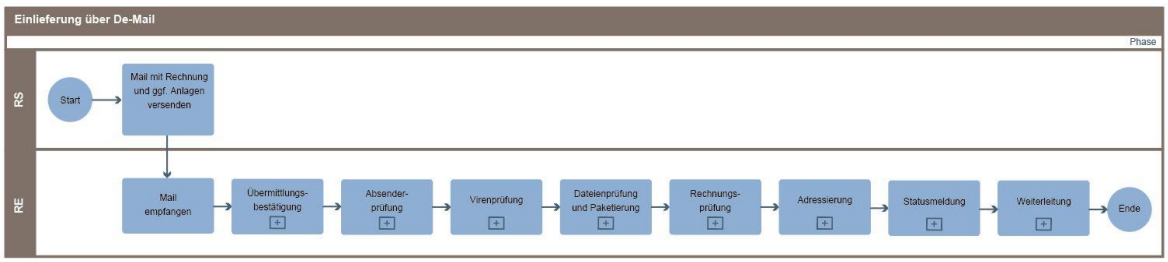

Abbildung 3.10: Prozess – Einlieferung über De-Mail

Name	Lieferung per De-Mail
Akteure/Rolle	(registrierter) Rechnungssender
Beschreibung	Der Rechnungssender verschickt eine eRechnung per De-Mail.
Vorbedingungen	Der Rechnungssender ist registriert und hat De-Mail als Einlieferungskanal ausgewählt.
Nachbedingung/Ergebnis	Die technisch geprüfte Rechnung nebst Anlagen und Laufzettel ist an ein weiterverarbeitendes System (z. B. Workflow) weitergeleitet.
Standardablauf	1. Mail mit Rechnung und ggf. Anlagen versenden: Der Rechnungssender versendet die Rechnung nebst ggf. ergänzenden Anlagen per De-Mail an die ihm mitgeteilte Empfangsadresse. 2. Mail empfangen: Der Rechnungsempfänger empfängt die Nachricht des Rechnungssenders.

Name	Lieferung per De-Mail
	3. Subprozess Übermittlungsbestätigung: Der Rechnungsempfänger erhält eine automatisierte Übertragungsprotokollierung seiner De-Mail. 4. Subprozess Absenderprüfung: Der Rechnungsempfänger prüft die Absenderadresse gegen die bei ihm registrierten Absenderadressen und ordnet die Mail dem Benutzerkonto zu. 5. Subprozess Virenprüfung: Es erfolgt eine Prüfung der Dateien auf Viren. 6. Subprozess Dateienprüfung und Paketierung: Die hochgeladenen Dateien werden einer ersten Prüfung (z. B. Format, Größe) unterzogen, ein Laufzettel wird angelegt und aus den empfangenen Dateien wird ein Rechnungspaket erstellt. 7. Subprozess Rechnungsprüfung: Die Rechnung aus dem Rechnungspaket wird auf Schemakonformität sowie auf Einhaltung der Geschäftsregeln geprüft. 8. Subprozess Adressierung: Die Adressierung der Rechnung wird ermittelt. 9. Subprozess Statusmeldung: Dem Rechnungssender wird eine Statusmeldung übermittelt/zur Verfügung gestellt. 1. Subprozess Weiterleitung: Das Rechnungspaket wird auf Basis der Adressierung an den entsprechenden Rechnungsworkflow weitergeleitet.
Alternativer Ablauf	1. Schlägt die Prüfung der Absenderadresse (Schritt 4) fehl, wird das Rechnungspaket verworfen und es erfolgt eine Mitteilung an die Absenderadresse. 2. Liegt ein Befund bei der Virenprüfung (Schritt 5) vor, erfolgt eine Rückmeldung an den Rechnungssender und die Mail wird verworfen. 3. Schlägt die Dateiprüfung fehl (Schritt 6), erfolgt eine Rückmeldung an den Rechnungssender und die Dateien werden verworfen. 4. Enthält das Ergebnis der Rechnungsprüfung (Schritt 8) annahmebehindernde Meldungen, wird die Rechnung verworfen und es erfolgt eine Rückmeldung an den Rechnungssender. 5. Optional: Ist eine Adressierung der Rechnung (Schritt 8) nicht möglich, ist die Rechnung an eine ggf. optional einzurichtende zentrale Klärungsstelle weiterzuleiten, die die Empfängerermittlung manuell durchführt.

Tabelle 3.10: Prozess – Einlieferung über De-Mail

3.1.5 Einlieferung über E-Mail

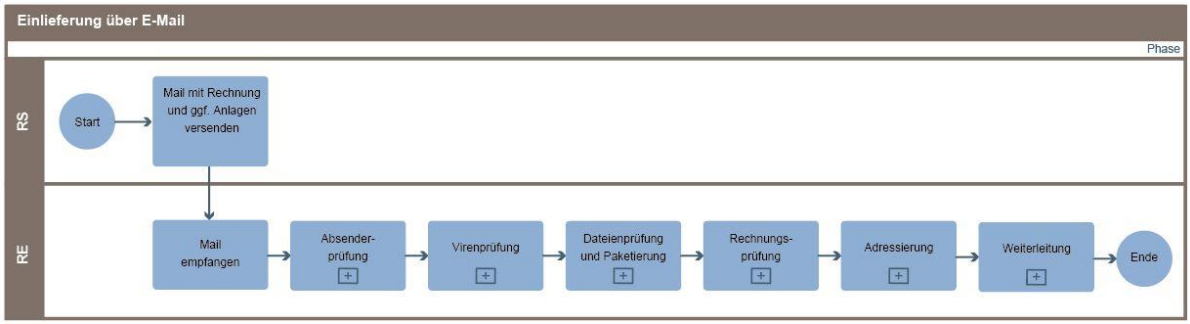

Abbildung 3.11: Prozess – Einlieferung über E-Mail

Name	Lieferung per E-Mail
Akteure/Rolle	(registrierter) Rechnungssender
Beschreibung	Der Rechnungssender verschickt eine eRechnung per E-Mail.
Vorbedingungen	Der Rechnungssender ist registriert und hat E-Mail als Einlieferungskanal ausgewählt.
Nachbedingung/Ergebnis	Die technisch geprüfte Rechnung nebst Anlagen und Laufzettel ist an ein weiterverarbeitendes System (z. B. Workflow) weitergeleitet.
Standardablauf	1. Mail mit Rechnung und ggf. Anlagen versenden: Der Rechnungssender versendet die Rechnung nebst ggf. ergänzenden Anlagen per E-Mail an die ihm mitgeteilte Empfangsadresse. 2. Mail empfangen: Der Rechnungseingang empfängt die Nachricht des Rechnungssenders. 3. Subprozess Absenderprüfung: Der Rechnungseingang prüft die Absenderadresse gegen die bei ihm registrierten Absenderadressen und ordnet die Mail dem Benutzerkonto zu. 4. Subprozess Virenprüfung: Es erfolgt eine Prüfung der Dateien auf Viren.

Name	Lieferung per E-Mail
	5. Subprozess Dateienprüfung und Paketierung: Die hochgeladenen Dateien werden einer ersten Prüfung (z. B. Format, Größe) unterzogen, ein Laufzettel wird angelegt und aus den empfangenen Dateien wird ein Rechnungspaket erstellt. 6. Subprozess Rechnungsprüfung: Die Rechnung aus dem Rechnungspaket wird auf Schemakonformität sowie auf Einhaltung der Geschäftsregeln geprüft. 7. Subprozess Adressierung: Die Adressierung der Rechnung wird ermittelt. 8. Subprozess Statusmeldung: Dem Rechnungssender wird eine Statusmeldung übermittelt/zur Verfügung gestellt. 9. Subprozess Weiterleitung: Das Rechnungspaket wird auf Basis der Adressierung an den entsprechenden Rechnungsworkflow weitergeleitet.
Alternativer Ablauf	1. Schlägt die Prüfung der Absenderadresse (Schritt 3) fehl, wird das Rechnungspaket verworfen und es ergeht eine Mitteilung an die Absenderadresse. 2. Liegt ein Befund bei der Virenprüfung (Schritt 4) vor, erfolgt eine Rückmeldung an den Rechnungssender und die Mail wird verworfen. 3. Schlägt die Dateiprüfung fehl (Schritt 5), erfolgt eine Rückmeldung an den Rechnungssender und die Dateien werden verworfen. 4. Enthält das Ergebnis der Rechnungsprüfung (Schritt 6) annahmebehindernde Meldungen, wird die Rechnung verworfen und es erfolgt eine Rückmeldung an den Rechnungssender. 5. Optional: Ist eine Adressierung der Rechnung (Schritt 7) nicht möglich, ist die Rechnung an eine ggf. optional einzurichtende zentrale Klärungsstelle weiterzuleiten, die die Empfängerermittlung manuell durchführt.

Tabelle 3.11: Prozess – Einlieferung über E-Mail

3.2 Fachlicher Schnitt der Komponenten

In diesem Unterkapitel werden Komponenten identifiziert, die einen oder mehrere der im vorangegangenen Kapitel dargestellten Prozessschritte aus fachlicher und technischer Sicht sinnvoll zusammenfassen. Die Darstellung der grundlegenden Prozesse in Kapitel 3.1 hat aufgezeigt, dass verschiedene Prozessschritte in den unterschiedlichen Prozessen in identischer oder ähnlicher Weise auftreten (z. B. Virenprüfung, Empfangsbestätigung) und somit in einer gemeinsam genutzten Komponente implementiert werden können. Hauptkriterien für die Agrenzung der Komponenten gegeneinander sind die funktionale Abgeschlossenheit und die Kontextabgrenzung.

In den grafischen Darstellungen der Komponenten (3.2.1 bis 3.2.6) wird jeweils Bezug auf die in Kapitel 3.1 beschriebenen Prozesse bzw. Prozessschritte oder Subprozesse genommen.

3.2.1 Benutzerverwaltung/Authentifikation (AU)

In der Komponente "Authentifikation" werden sämtliche Prozesse der Benutzerverwaltung und Authentifikation zusammengefasst: Registrierung, Passwortänderung, Benutzerdatenänderung, Kontolöschung sowie der Subprozess Authentifikation.

Die Komponente ist nicht auf die Nutzung im Rahmen der Einlieferung von eRechnungen beschränkt. Es ist lediglich sicherzustellen, dass verfahrensspezifische Daten (z. B. Übertragungskanäle) ergänzend zu den Identitätsdaten abgelegt werden können.

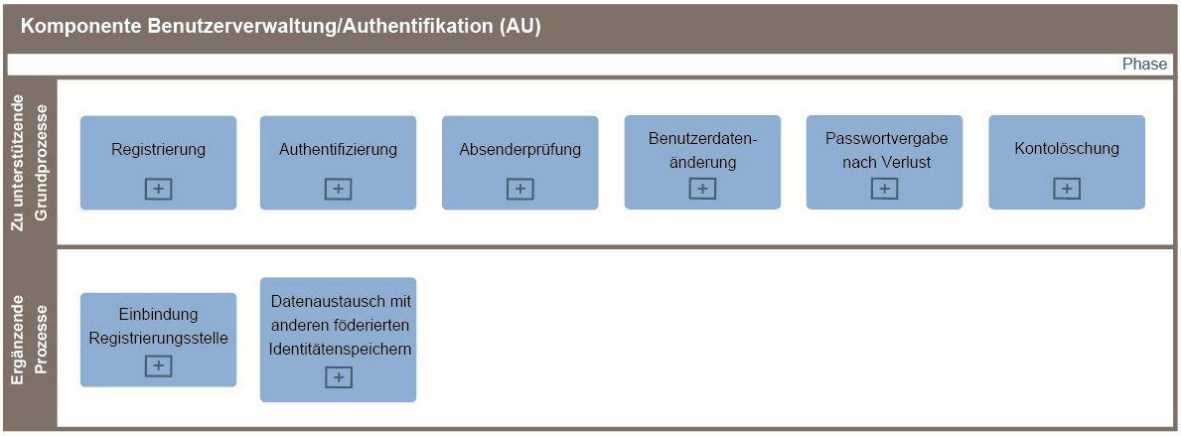

Abbildung 3.12: Komponente – Benutzerverwaltung/Authentifikation

3.2.2 Weberfassung (WF)

Die Komponente "Weberfassung" stellt Dialogmasken für die formularbasierte Erfassung von Rechnungen, den Upload von Rechnungsanlagen, das Speichern und Laden von Erfassungszwischenständen sowie für den Upload von Rechnungsdateien bereit. Die Komponente enthält auch die Logiken, die für die Erzeugung von eRechnungen aus der formularbasierten Erfassung nötig sind.

Die Komponente ist spezifisch für eRechnung. Die Dialogmasken und Logiken können in einem anderen Kontext nicht verwendet werden.

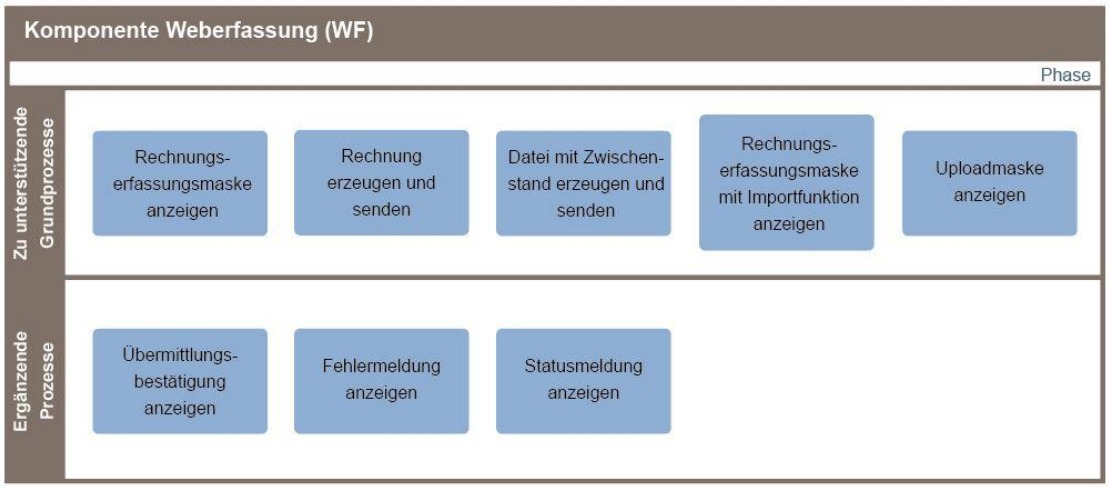

Abbildung 3.13: Komponente – Weberfassung

3.2.3 Übertragungskanäle (ÜK)

Die Komponente "Übertragungskanäle" lauscht auf den freigegebenen Kanälen (Webservice, De-Mail, E-Mail) auf eingehende Nachrichten und stellt das zentrale Bindeglied zwischen dem Rechnungssender und dem Rechnungsempfänger dar. Über die Komponente wird die Kommunikation zwischen diesen beiden Akteuren abgewickelt. Damit ist sie auch für den Versand von Rückmeldungen an den Rechnungssender zuständig. Innerhalb dieser Komponente erfolgt zudem die Anlage eines Laufzettels zur Protokollierung der Verarbeitungshistorie der Nachricht bzw. eRechnung.

Die Komponente ist nicht auf den Kontext der eRechnung begrenzt, vielmehr besteht sie aus Grundfunktionalitäten des Nachrichten- und Dateienaustausches.

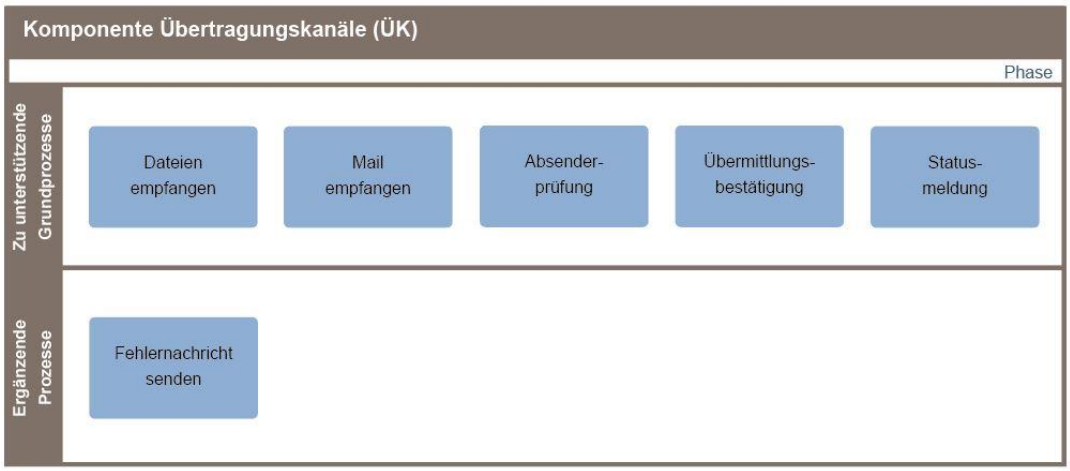

Abbildung 3.14: Komponente – Übertragungskanäle

3.2.4 Dateien- und Nachrichtenprüfung (DP)

Innerhalb der Komponente "Dateien- und Nachrichtenprüfung" erfolgt die Virenprüfung, die ggf. zur Ablehnung der Eingangsnachricht/Dateien führt. Darüber hinaus ist diese Komponente für die allgemeine Prüfung der Dateien (z. B. Format, Größe) und die Paketierung der Rechnung mit ihren Anlagen sowie dem Laufzettel verantwortlich.

Die Komponente ist nicht auf den Kontext der eRechnung begrenzt. Vielmehr besteht sie aus Grundfunktionalitäten der Dateien- und Nachrichtenprüfung. Konfigurationen, die spezifisch für die eRechnung sind, müssen jedoch möglich sein, z. B. die Prüfung auf zulässige Dateiformate.

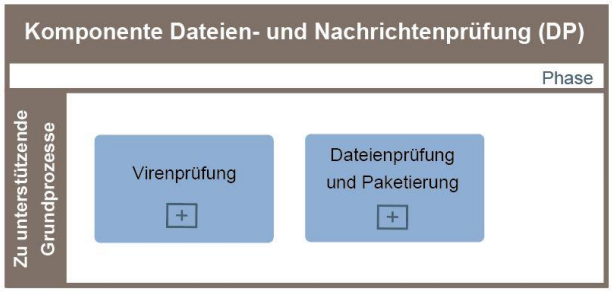

Abbildung 3.15: Komponente – Dateien- und Nachrichtenprüfung

3.2.5 Rechnungsprüfung (PR)

Die Komponente "Rechnungsprüfung" führt die fachspezifische Prüfung der elektronischen Rechnung gegen die Vorgaben des XRechnungsstandards durch. Dies umfasst eine Prüfung der Rechnung auf Schemakonformität sowie auf Einhaltung der Geschäftsregeln.

Die Prüfung einer XML-Datei gegen eine Schemadatei und Regeln eines Schematrons ist nicht kontextspezifisch. Die hier hinterlegten Schema- und Schematrondateien sind hingegen spezifisch für die eRechnung.

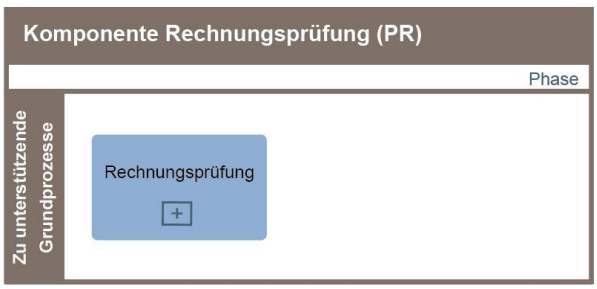

Abbildung 3.16: Komponente – Rechnungsprüfung

3.2.6 Adressierung und Weiterleitung (AW)

Die Komponente "Adressierung und Weiterleitung" ermittelt aus den Empfängerangaben der Rechnung unter Zuhilfenahme von Mappingtabellen das Zielsystem zur Weiterverarbeitung (z. B. Rechnungsbearbeitungsworkflow). Zudem erfolgt von hier aus die entsprechende Weiterleitung des Rechnungspakets an das Zielsystem.

Das Auslesen der Empfängerinformation, das Mapping und die Weiterleitung sind spezifisch für die eRechnung und können nicht in anderem Kontext verwendet werden.

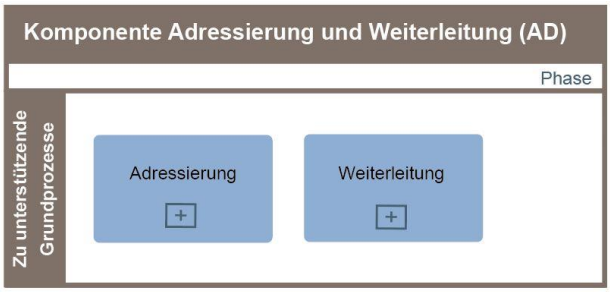

Abbildung 3.17: Komponente – Adressierung und Weiterleitung

3.2.7 Zuordnung der fachlichen Komponenten zu technischen Modulen

Die fachlichen Komponenten lassen sich wie folgt auf die Module des technischen Architekturmodells für ein modulares Empfangs- und Weiterleitungssystem, das im Rahmen des Steuerungsprojekt des IT-Planungsrates zur eRechnung entwickelt wird (Ergebnisdokument EG3 v0.8), abbilden:

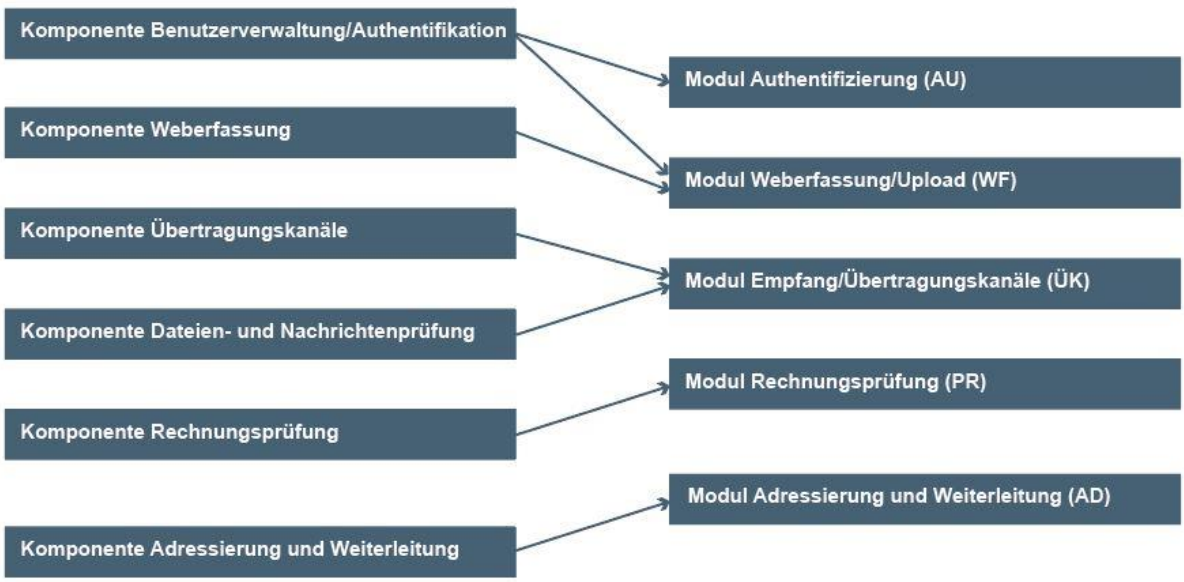

Abbildung 3.18: Zuordnung der fachlichen Komponenten zu technischen Modulen

Die Module des technischen Architekturmodells sind dabei in weitere Submodule untergliedert:

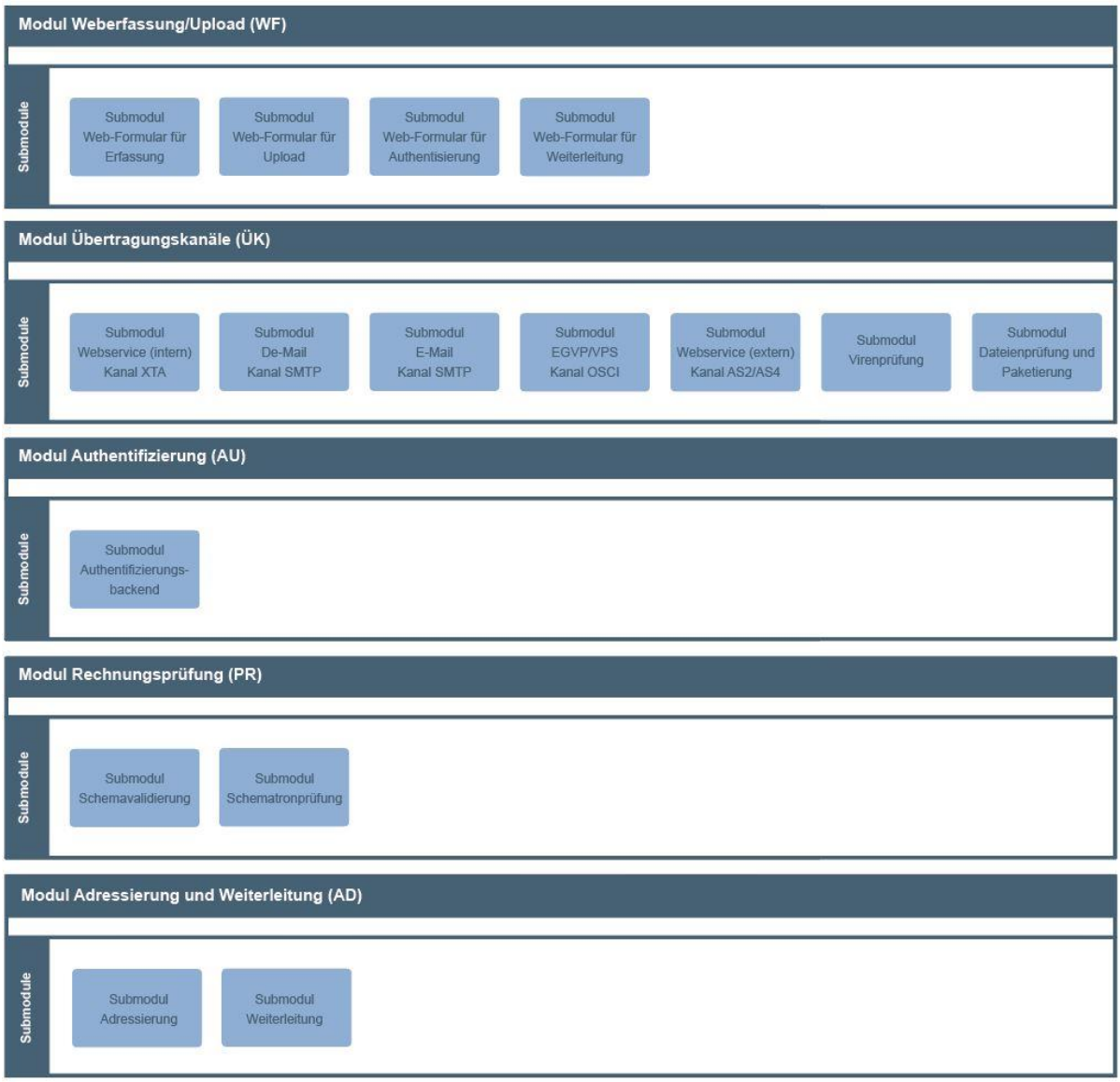

Abbildung 3.19: Submodule

Als interner Schnittstellenstandard auf der Seite des Rechnungseingang wird XTA2 eingesetzt. Die Schnittstellenstandards für die externe Kommunikation sind übertragungskanalabhängig.

4 Funktionale Anforderungen

In diesem Kapitel werden abstrakte funktionale Anforderungen beschrieben, die noch keine Lösungen (wie z. B. Servicekonten) darstellen. Diese Anforderungen dienen zur Ableitung von Abnahmekriterien, gegen die die konkreten technischen Lösungen geprüft werden.

Die funktionalen Anforderungen an den zentralen eRechnungseingang werden nachfolgend in Form von User Storys aufgeführt (für weiter Informationen vgl. Cohn, Mike: User Stories Applied - For Agile Software Development, Addison-Wesley - Pearson Education: 2004 S. 4ff). Es handelt sich hierbei ausdrücklich um eine weniger formale Form der Anforderungserhebung als z. B. bei der Beschreibung von Anwendungsfällen. Dies ist beabsichtigt, da der konkrete Ablauf eines Prozesses (mit einem festen Standardablauf und einer Vielzahl von möglichen abweichenden Varianten) weniger im Vordergrund steht, sondern vielmehr die Akzeptanzkriterien als solche. Diese beschreiben klar die zu erreichenden Ziele/Ergebnisse und schränken den einzuschlagenden Weg dabei nicht ein. Dies hilft bei der späteren Prüfung von bereits vorhandenen Komponenten gegen die Anforderungen, da nur die Leistung der Komponente, jedoch kein konkreter Prozessablauf mit den Akzeptanzkriterien verglichen werden kann.

Bei der im Folgenden vorgestellten Strukturierung der User Storys werden die beteiligten Module, die entsprechende Nutzergruppen und die erforderliche Berechtigung mit aufgezeigt. Des Weiteren werden nur zwingend notwendige Anforderungen erhoben, die für die Annahme, Prüfung und korrekte Weiterleitung unbedingt nötig sind.

Die User Storys werden anhand der folgenden Themen gruppiert:

AU: In der Gruppe *Authentifikation* werden die Anforderungen an die Registrierung und Authentifikation von Rechnungssendern zusammengefasst.

WF: Die Gruppe *Weberfassung* enthält sowohl die Anforderungen für die manuelle Erfassung einer Rechnung über ein Webformular als auch die Anforderungen an den Web-Upload einer elektronischen Rechnung.

ÜK: Die Anforderungen an die unterschiedlichen Übertragungskanäle Webservice, De-Mail und E-Mail werden in der Gruppe *Übertragungskanäle* skizziert.

PR: Die für die Prüfung einer elektronischen Rechnung erforderlichen Anforderungen werden in der Gruppe *Prüfung* beschrieben.

AD: Die Gruppe *Adressierung* beinhaltet die Anforderungen an die Weiterleitung einer elektronischen Rechnung und ihrer rechnungsbegründenden Unterlagen an die korrekte Zielbehörde.

4.1 Authentifikation (AU)

Nachfolgend werden die Anforderungen an die Authentifikation/Registrierung eines Rechnungssenders entworfen. Die konkrete Durchführung der Prüfung findet im Modul Authentifizierung statt. Die direkte Kommunikation mit dem Nutzer erfolgt über die Weberfassung.

4.1.1 FA-AU-1 Mehrsprachigkeit

4.1.1.a User Story

Story: Als Rechnungssender möchte ich zwischen deutscher und englischer Benutzerführung wählen dürfen.

Nutzer: Rechnungssender

Beteiligte Module: Authentifizierung, Weberfassung

Berechtigung: E-RECHNUNGS-NUTZER

4.1.1.b Funktionen

Dem Rechnungssender müssen mindestens eine deutsche und eine englische Benutzerführung angeboten werden. Damit soll fremdsprachigen Nutzern der Einstieg in das Portal erleichtert werden.

4.1.1.c Akzeptanzkriterien

- Die Standard-Benutzerführung wird aus der eingestellten Browsersprache ausgelesen. Falls diese weder deutsch noch englisch ist, wird die deutsche Benutzerführung als Standard gesetzt.
- Die Schaltfläche *Englisch* führt zur englischen Benutzerführung.
- Die Schaltfläche *Deutsch* führt zurück zur deutschen Benutzerführung.
- Die getroffene Wahl wird beim nächsten Besuch des Portals automatisch berücksichtigt.

4.1.2 FA-AU-2 Erfassung von Registrierungsdaten

4.1.2.a User Story

Story: Als Rechnungssender möchte ich mich in der Webanwendung registrieren können, damit ich eine elektronische Rechnung versenden kann.

Nutzer: Rechnungssender

Beteiligte Module: Authentifizierung, Weberfassung

Berechtigung: E-RECHNUNGS-NUTZER

4.1.2.b Funktionen

Für die Registrierung eines neuen Rechnungssenders wird auf der Startseite der Webanwendung eine entsprechende Registrierungsmaske zur Verfügung gestellt. Sie ermöglicht die Eingabe von Anmelde- und Stammdaten des Benutzers.

Die eingegebene Nutzerkennung – ein eindeutiger Benutzername oder eine E-Mail-Adresse wären hier denkbar – wird gegen die Identitätsdatenbank abgeglichen. Eine Fehlermeldung wird angezeigt, sofern der Benutzername bereits vergeben ist. Das angegebene Passwort wird entsprechend den Passwortregeln überprüft und ggf. eine Fehlermeldung angezeigt.

4.1.2.c Validierung

Die Erfassung und Validierung der Daten sollen dem Kerndatensatz nach §8 des Onlinezugangsgesetz (OZG vgl. http://www.bundesfinanzministerium.de/Content/DE/Downloads/Gesetze/2016-12-14-neuregelung-bundesstaatliches-finanzausgleichssystem.pdf?__blob=publicationFile&v=4) mit seinen Pflichtfeldern (Name, Vorname, Anschrift, Geburtsdatum, E-Mail-Adresse) folgen.

Zusätzlich sollen verfahrensspezifische Daten (z. B. die Auswahl von Übertragungskanälen und damit verbundenen kanalspezifischen Daten wie eine De-Mail-Adresse, ein Webservice-Nutzer usw.) erfasst und validiert werden.

4.1.2.d Validierungsregeln Passwort

- Die Validierungsregeln müssen den Vorgaben des IT-Grundschutz-Katalogs folgen (vgl. Abschnitt. M 2.11 Regelung des Passwortgebrauchs – https://www.bsi.bund.de/DE/Themen/IT-Grundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02011.html).

4.1.2.e Akzeptanzkriterien

- Bei der Eingabe des Passworts soll der Nutzer durch eine Entropie-Messung (Anzeige der Passwort-Güte) unterstützt werden.
- Der Nutzer muss sein Passwort ein zweites Mal identisch eingeben.
- Bei der Eingabe wird das Passwort nicht auf dem Bildschirm angezeigt.
- Passwörter werden im System z. B. mittels Einweg-Verschlüsselung zugriffssicher gespeichert.
- Nach erfolgreicher Eingabe der Registrierungsdaten wird eine E-Mail mit einem temporären Aktivierungslink an die hinterlegte E-Mail-Adresse verschickt.
- Die Erfassung erfolgt getrennt nach dem Kerndatensatz (§8 OZG) und den verfahrensspezifischen Daten.

4.1.3 FA-AU-3 Aktivierung des Benutzerkontos

4.1.3.a User Story

Story: Als Rechnungssender möchte ich mein Benutzerkonto aktivieren und Übertragungskanäle auswählen können.

Nutzer: Rechnungssender

Beteiligte Module: Authentifizierung, Weberfassung

Berechtigung: E-RECHNUNGS-NUTZER

4.1.3.b Funktionen

Nachdem die Registrierungsdaten gespeichert wurden, versendet das System eine E-Mail mit einem temporären Aktivierungslink an die hinterlegte E-Mail-Adresse. Um das Benutzerkonto zu aktivieren, öffnet der Nutzer den Link und wird anschließend auf das Portal weitergeleitet Der Registrierungsprozess ist hiermit beendet und der Rechnungssender kann sich mit seinen Anmeldedaten in der Webanwendung authentisieren.

4.1.3.c Akzeptanzkriterien

- Die Schaltfläche *Speichern* initiiert die Übergabe der Daten an das Modul Authentifizierung, sofern die erforderlichen Felder ausgefüllt wurden.
- Schlägt das Speichern fehl, erhält der Nutzer eine Fehlermeldung.

4.1.4 FA-AU-4 Anmeldung

4.1.4.a User Story

Story: Als Rechnungssender möchte ich mich an der Webanwendung anmelden können.

Nutzer: Rechnungssender

Beteiligte Module: Authentifizierung, Weberfassung

Berechtigung: E-RECHNUNGS-NUTZER

4.1.4.b Funktionen

Für die Anmeldung eines registrierten Rechnungssenders wird auf der Startseite der Webanwendung eine entsprechende Anmeldemaske zur Verfügung gestellt. Sie ermöglicht die Eingabe von Anmeldedaten zum Zwecke der Authentisierung des Benutzers. Die Authentisierungsinformationen werden an das Modul Authentifizierung übermittelt. Das Modul Authentifizierung überprüft die Authentisierungsinformationen und gibt das Prüfergebnis an die Webanwendung zurück. Bei erfolgreicher Authentisierung erhält der Nutzer Zugriff auf das Portal. Erfolglose Anmeldeversuche sollten mit einer kurzen Fehlermeldung ohne Angabe von Einzelheiten abgelehnt werden. Nach fünf aufeinanderfolgenden fehlerhaften Passworteingaben für dieselbe Kennung sollte das Authentisierungssystem den Zugang hierfür für eine bestimmte (administrativ konfigurierbare) Zeitspanne sperren. Die Sperrung einer Kennung darf bei nachfolgenden erfolglosen Anmeldeversuchen nicht erkennbar sein, sondern sollte dem jeweiligen Nutzer per E-Mail mitgeteilt werden.

4.1.4.c Benutzeroberfläche

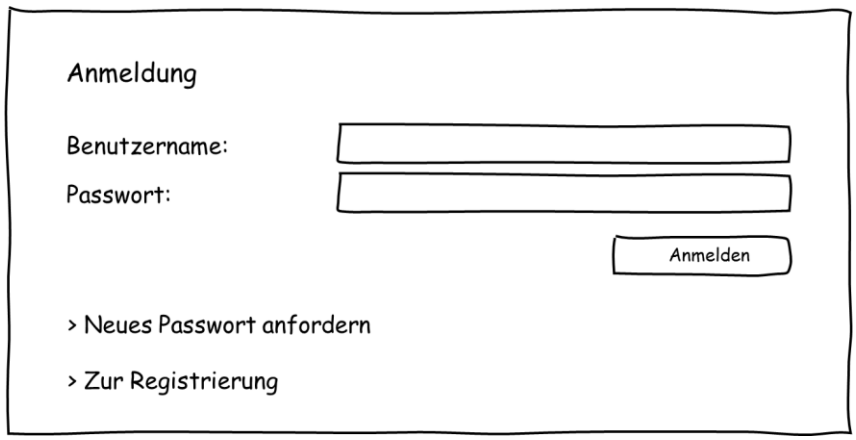

Abbildung 4.1: Anmeldung

4.1.4.d Akzeptanzkriterien

- Die Anmeldung ist nur registrierten Rechnungssendern möglich.
- Die Schaltfläche *Anmelden* initiiert die Übergabe der Authentisierungsdaten an das Modul Authentifizierung, sofern die erforderlichen Felder ausgefüllt wurden.
- Ein Link *Neues Passwort anfordern* öffnet die Eingabemaske zur Wiederherstellung des Passworts.
- Ein Link *Zur Registrierung* öffnet die Eingabemaske zur Registrierung eines neuen Nutzers.

4.1.5 FA-AU-5 Wiederherstellen des Passworts

4.1.5.a User Story

Story: Als Rechnungssender möchte ich mein Passwort bei Verlust wiederherstellen können.

Nutzer: Rechnungssender

Beteiligte Module: Authentifizierung, Weberfassung

Berechtigung: E-RECHNUNGS-NUTZER

4.1.5.b Funktionen

Für die Wiederherstellung des Passworts eines registrierten Rechnungssenders wird auf der Startseite der Webanwendung eine Schaltfläche zur Verfügung gestellt. Sie öffnet eine Eingabemaske, in die der Rechnungssender seine E-Mail-Adresse oder seinen Benutzernamen einträgt. Ist die E-Mail-Adresse bzw. der Benutzername in der Datenbank vorhanden, so wird dem Rechnungssender per E-Mail ein Link zugesendet, der auf eine Seite zur Vergabe eines neuen Passworts führt. Nach Eingabe des Passworts wird dieses gespeichert.

4.1.5.c Benutzeroberfläche

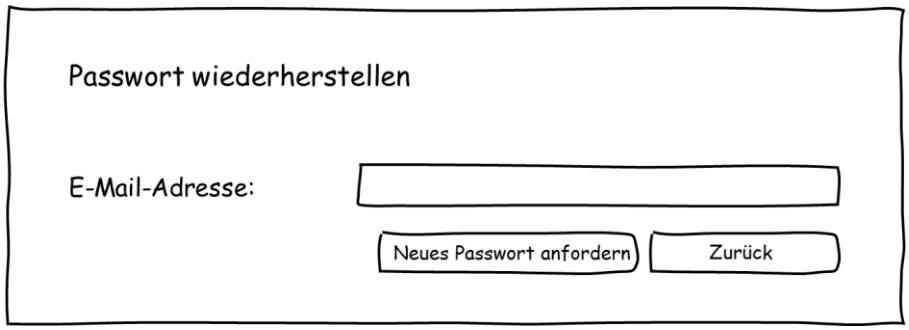

Abbildung 4.2: Wiederherstellen des Passworts

4.1.5.d Akzeptanzkriterien

- Eine Schaltfläche *Passwort vergessen* öffnet eine Eingabemaske für die Eingabe des Benutzernamens bzw. der E-Mail-Adresse.
- Eine Schaltfläche *Neues Passwort anfordern* initiiert den Versand eines temporären Links an die angegebene bzw. hinterlegte E-Mail-Adresse, sofern der Benutzername bzw. die E-Mail-Adresse in der Datenbank gelistet sind.

- Eine Schaltfläche *Zurück* schließt die Eingabemaske und öffnet die Eingabemaske zur Anmeldung.
- Der temporäre Link in der E-Mail führt zu einer Eingabemaske, in der der Nutzer ein neues Passwort vergeben kann.
- Der Nutzer muss ein Passwort gemäß den Passwortregeln aus den Vorgaben des IT-Grundschutz-Katalogs eingeben (vgl. Abschnitt. M 2.11 Regelung des Passwortgebrauchs – https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02011.html). Entspricht ein Passwort nicht den Regeln, erhält der Nutzer eine Fehlermeldung.
- Der Nutzer muss das Passwort ein zweites Mal identisch eingeben. Bei Abweichung erhält er eine Fehlermeldung.
- Eine Schaltfläche *Speichern* initiiert die Speicherung des neuen Passworts und schließt die Eingabemaske. Das erfolgreiche Speichern des Passworts wird dem Nutzer in einem Dialog bestätigt.
- Der Nutzer erhält eine Fehlermeldung, wenn das Passwort nicht gespeichert werden konnte.

4.1.6 FA-AU-6 Änderung von Anmeldedaten

4.1.6.a User Story

Story: Als Rechnungssender möchte ich die zum Login in der Webanwendung angegebene E-Mail-Adresse (Benutzername) oder das Passwort ändern können.

Nutzer: Rechnungssender

Beteiligte Module: Authentifizierung, Weberfassung

Berechtigung: E-RECHNUNGS-NUTZER

4.1.6.b Funktionen

Für die Änderung von Anmeldedaten wird eine entsprechende Eingabemaske zur Verfügung gestellt.

4.1.6.c Akzeptanzkriterien

- Das Entfernen des Benutzerkontos ist nur registrierten Rechnungssendern möglich, die sich vorher in der Webanwendung angemeldet haben.

4.1.7 FA-AU-7 Änderung von Stammdaten

4.1.7.a User Story

Story: Als Rechnungssender möchte ich hinterlegte Stammdaten in der Webanwendung ändern können.

Nutzer: Rechnungssender

Beteiligte Module: Authentifizierung, Weberfassung

Berechtigung: E-RECHNUNGS-NUTZER

4.1.7.b Funktionen

Für die Änderung von Stammdaten wird dem Nutzer eine Eingabemaske zur Verfügung gestellt. Die Felder der Maske werden mit den Stammdaten aus dem Identitätsdatensatz vorausgefüllt. Nach der Bearbeitung aktualisiert das System den Identitätsdatensatz in der Identitätsdatenbank. Der Nutzer wird über die erfolgreiche Aktualisierung des Datensatzes informiert.

4.1.7.c Benutzeroberfläche

4.1.7.d Akzeptanzkriterien

- Die Schaltfläche *Bearbeiten* öffnet die Eingabemaske.
- Die Schaltfläche *Speichern* schließt die Eingabemaske und speichert geänderte Stammdaten.

4.1.8 FA-AU-8 Benutzerkonto löschen

4.1.8.a User Story

Story: Als Rechnungssender möchte ich mein Benutzerkonto löschen können.

Nutzer: Rechnungssender

Beteiligte Module: Authentifizierung, Weberfassung

Berechtigung: E-RECHNUNGS-NUTZER

4.1.8.b Funktionen

Der Rechnungssender kann sein Benutzerkonto über eine Funktion in der Benutzerverwaltung löschen. Die Anwendung sichert das Löschen durch eine Benutzerbestätigung in Form eines Dialoges ab. Das System meldet den Nutzer ab und das Konto wird inaktiv geschaltet. Es wird eine Löschfrist gestartet, nach deren Ablauf der Datensatz entfernt wird.

4.1.8.c Benutzeroberfläche

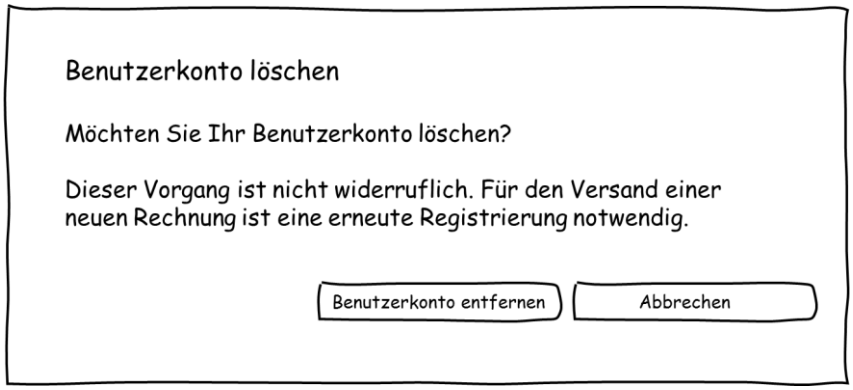

Abbildung 4.3: Benutzerkonto löschen

4.1.8.d Akzeptanzkriterien

- Das Entfernen des Benutzerkontos ist nur registrierten Rechnungssendern möglich, die sich vorher in der Webanwendung angemeldet haben.
- Der Rechnungssender erhält vor dem endgültigen Entfernen eine Meldung, in der er das Löschen mit der Schaltfläche *Benutzerkonto entfernen* bestätigen muss.
- Der Dialog zum Entfernen kann über die Schaltfläche *Abbrechen* beendet werden.
- In der Bestätigungsmeldung des Löschvorgangs steht: „Das Benutzerkonto wird nach Ablauf der folgenden Löschfrist entfernt."
- Nach Ablauf einer konfigurierbaren Löschfrist wird das Benutzerkonto entfernt.

4.1.9 FA-AU-9 Ändern/Freischalten von Übertragungskanälen

4.1.9.a User Story

Story: Als Rechnungssender möchte ich die Auswahl der Übertragungskanäle, über die eine Rechnung versendet werden soll, ändern bzw. freischalten.

Nutzer: Rechnungssender

Beteiligte Module: Authentifizierung, Weberfassung

Berechtigung: E-RECHNUNGS-NUTZER

4.1.9.b Funktionen

Für die Änderung von Übertragungskanälen wird dem Nutzer eine Übersicht mit allen verfügbaren Übertragungskanälen zur Verfügung gestellt. Über ein Optionsfeld kann ein Übertragungskanal aktiviert bzw. deaktiviert werden. Bei Aktivierung eines neuen Übertragungskanals muss der Nutzer kanalspezifische Identifikationsdaten angeben (z. B. eine eindeutige Nutzerkennung des technischen Webservice-Nutzers bei der Webservice-Kanalwahl). Nach erfolgreicher Speicherung erhält der Benutzer eine Bestätigungsmitteilung.

Ein gesperrter Webservice-Zugang, z. B. weil zu oft ein falsches Passwort mitgeliefert wurde, kann hier durch den Nutzer selbst wieder freigeschaltet werden.

Bei der Aktivierung des Übertragungskanals E-Mail werden die angegebenen E-Mail-Adressen in eine **Whitelist** eingetragen. Nur von diesen Absenderadressen aus ist eine Einlieferung per E-Mail möglich.

Eine Rückfrage-Adresse kann angegeben werden.

4.1.9.c Akzeptanzkriterien

- Die Änderung ist nur registrierten Rechnungssendern möglich.
- Die Schaltfläche *Speichern* initiiert die Übergabe der Authentisierungsdaten an das Modul Authentifizierung, sofern die erforderlichen Felder ausgefüllt wurden.
- Schlägt das Speichern fehl, erhält der Nutzer eine Fehlermeldung.
- Bei den Übertragungskanälen De-Mail und E-Mail werden die De-Mail- und E-Mail-Adressen in eine Whitelist eingetragen.
- Bei Freischaltung des Webservice-Zugangs ist ein zuvor gesperrter Zugang wieder entsperrt.

4.2 Weberfassung/Upload (WF)

Nachfolgend werden die Anforderungen an die Erfassung einer Rechnung über ein Webformular für Rechnungssender, die keine Rechnungen in einem elektronischen Format erstellen und versenden können, aufgeführt. Dabei soll Rechnungssendern die Möglichkeit gegeben werden, Rechnungen, die bereits in einem elektronischen Format (nach dem Standard XRechnung) vorliegen, über ein Webformular hochzuladen und damit bei dem zentralen Rechnungseingang einzuliefern.

4.2.1.a FA-WF-1 Manuelle Erfassung einer Rechnung

4.2.1.b User Story

Story: Als Rechnungssender möchte ich eine elektronische Rechnung über ein Webformular erfassen können.

Nutzer: Rechnungssender

Beteiligte Module: Weberfassung

Berechtigung: E-RECHNUNGS-WEB-NUTZER

4.2.1.c Funktionen

Für die Erstellung einer Rechnung wird eine entsprechende Eingabemaske zur Verfügung gestellt. Sie ermöglicht es, die Rechnungsdaten einfach, konsistent und innerhalb von Wertgrenzen (z. B. Länge von Textfeldern) eingeben zu können. Über ein Upload-Formular kann der Nutzer ggf. nach der Erfassung Dateien hochladen, die der Rechnung angehängt werden.

Der Nutzer wird bei der Erfassung mit Auswahlfeldern unterstützt. Die Daten werden den Validierungsregeln entsprechend überprüft und es werden ggf. Fehlermeldungen angezeigt. Ein für eine Grobadressierung zur rechnungsempfangenden Behörde ausreichender Teil der Auftragskennnummer baut sich automatisch (je nachdem welche Behörde ausgewählt wird) zusammen, falls diese beim Rechnungssender nicht bekannt ist. Hochgeladene Dateien werden auf Schadsoftware überprüft.

Nach der Erstellung einer Rechnung wird eine elektronische Rechnung nach dem Standard XRechnung (mit der Syntax UBL) erzeugt und an den zentralen eRechnungseingang übergeben. Nach dem erfolgreichen Versand wird dem Rechnungssender dies im Browser mitgeteilt. Nach dem Absenden der Rechnung ist eine Bearbeitung nicht mehr möglich.

4.2.1.d Validierung

Die Validierung der Eingabefelder muss den Datenfeldern innerhalb der Schemadefinition des Standards XRechnung folgen.

4.2.1.e Akzeptanzkriterien

- Die Schaltfläche *Zurücksetzen* löscht alle zuvor getätigten Angaben und setzt die Eingabefelder auf den Ursprungszustand zurück.
- Die Schaltfläche *Zurück* beendet die Rechnungserstellung und kehrt zur Startseite zurück.
- Über die Schaltfläche *Anlagen hochladen* können rechnungsbegründende Unterlagen hochgeladen werden.

- Der für eine Grobadressierung zur rechnungsempfangenden Behörde ausreichende Teil der Auftragskennnummer baut sich automatisch (je nachdem welche Behörde ausgewählt wird) zusammen, falls diese beim Rechnungssender nicht bekannt ist.
- Es werden dem XRechnungsstandard folgend nur die folgenden Formate als Anlagen akzeptiert: PDF, PNG, JPEG, CSV, XLSX, ODS.
- Mit Betätigen der Schaltfläche *Senden* wird die erfolgreich generierte elektronische Rechnung im XML-Format an den zentralen eRechnungseingang versendet.
- Nach erfolgreichem Versenden wird dem Rechnungssender dies im Browser mitgeteilt.
- Nach erfolgreichem Versenden kann der Rechnungssender über die Schaltfläche *Download-Rechnungsoriginal* die versendete XML-Datei lokal auf seinem Rechner speichern.

4.2.2 FA-WF-2 Speichern eines Zwischenstands einer Rechnung

4.2.2.a User Story

Story: Als Rechnungssender möchte ich den Zwischenstand einer Rechnung lokal speichern.

Nutzer: Rechnungssender

Beteiligte Module: Weberfassung

Berechtigung: E-RECHNUNGS-WEB-NUTZER

4.2.2.b Funktionen

Für die Erstellung einer Rechnung wird eine entsprechende Eingabemaske zur Verfügung gestellt. Sie ermöglicht es, die Rechnungsdaten einfach, konsistent und innerhalb von Wertgrenzen einzugeben.

Es besteht die Möglichkeit, Zwischenstände lokal zu speichern und die Erfassung der Rechnung zu einem späteren Zeitpunkt fortzusetzen.

4.2.2.c Akzeptanzkriterien

- Die Schaltfläche *Zwischenstand speichern* erzeugt aus den erfassten Daten einen Datensatz im Format XML und initiiert den Download über den Webbrowser.
- Schlägt die Erzeugung fehl, erhält der Nutzer eine Fehlermeldung.

4.2.3 FA-WF-3 Hochladen eines Zwischenstands einer Rechnung

4.2.3.a User Story

Story: Als Rechnungssender möchte ich einen zuvor lokal gesicherten Zwischenstand einer Rechnung hochladen.

Nutzer: Rechnungssender

Beteiligte Module: Weberfassung

Berechtigung: E-RECHNUNGS-WEB-NUTZER

4.2.3.b Funktionen

Für die Erstellung einer Rechnung wird eine entsprechende Eingabemaske zur Verfügung gestellt. Sie ermöglicht es, die Rechnungsdaten einfach, konsistent und innerhalb von Wertgrenzen einzugeben.

Es besteht die Möglichkeit, lokal gespeicherte Zwischenstände hochzuladen. Die Eingabefelder werden mit dem gespeicherten Zwischenstand belegt und die Rechnung kann weiter erfasst werden. Sollte ein Fehler beim Hochladen signalisiert werden, wird dem Nutzer eine konkrete Fehlermeldung angezeigt.

4.2.3.c Akzeptanzkriterien

- Die Schaltfläche *Zwischenstand laden* öffnet einen Dokumenten-Auswahl-Dialog. Nach Auswahl einer Datei im Format XML wird diese hochgeladen.
- Nach dem erfolgreichen Hochladen werden erfasste Daten in die jeweiligen Eingabefelder geschrieben.
- Schlägt der Upload fehl, erhält der Benutzer eine Fehlermeldung.

4.2.4 FA-WF-4 Upload einer Rechnung

4.2.4.a User Story

Story: Als Rechnungssender möchte ich eine elektronische Rechnungsdatei hochladen und versenden können.

Nutzer: Rechnungssender

Beteiligte Module: Weberfassung

Berechtigung: E-RECHNUNGS-WEB-NUTZER

4.2.4.b Funktionen

Für den Upload einer Rechnung und ggf. dazugehöriger Anhänge wird eine entsprechende Maske zur Verfügung gestellt. Es wird dem Rechnungssender ermöglicht, Dateien auszuwählen, die lokal gespeichert sind und außerhalb der Webanwendung erstellt wurden.

Die ausgewählten Dateien müssen gegen die Formatvorgaben geprüft und anschließend temporär hochgeladen werden. Rechnungsdateien und Anhänge in nicht unterstützten Datenformaten sollen nicht weiterverarbeitet werden. Dem Nutzer wird ggf. eine Fehlermeldung angezeigt. Anhänge müssen vor der Weiterverarbeitung auf Schadsoftware untersucht werden. Nach dem Versenden der Rechnung wird dem Benutzer auf der Weboberfläche die erfolgreiche Annahme in einer Mitteilung bestätigt.

4.2.4.c Validierung

- Als Rechnung wird nur eine elektronische Rechnung, welche dem Standard XRechnung folgt, anerkannt.
- Es werden dem XRechnungsstandard folgend nur die folgenden Formate als Anlagen akzeptiert: PDF, PNG, JPEG, CSV, XLSX, ODS.
- Es dürfen maximal 200 Anhänge angefügt werden.
- Die Gesamtgröße aller Anlagen darf 15 Megabyte nicht übersteigen.

4.2.4.d Benutzeroberfläche

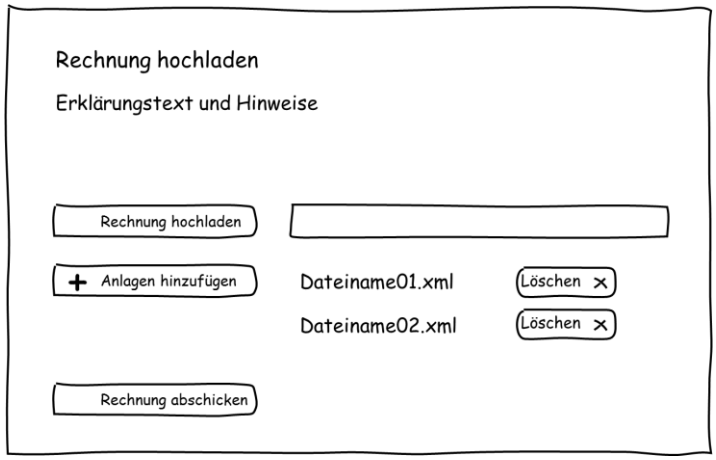

Abbildung 4.4: Upload einer Rechnung

4.2.4.e Akzeptanzkriterien

- Das Hochladen einer Rechnung ist nur registrierten Rechnungssendern möglich, die sich vorher in der Webanwendung angemeldet haben.
- Die Schaltfläche *Rechnung hochladen* öffnet eine Maske zur Dokumentenauswahl. Nach Auswahl einer Datei durch den Nutzer wird der ausgewählte Dateipfad in einem unveränderlichen Feld angezeigt.
- Die Schaltfläche *Anlagen hinzufügen* öffnet eine Maske zur Dokumentenauswahl. Nach Auswahl einer Datei durch den Nutzer werden der Dateiname und die Dateiendung angezeigt.
- Die Schaltfläche *Löschen* erscheint hinter dem Dateinamen, sobald eine Anlage hinzugefügt wurde. Das Betätigen der Schaltfläche löscht die Auswahl der Anlage.
- Die Schaltfläche *Rechnung abschicken* initiiert die Validierung der ausgewählten Dateien und zeigt dem Nutzer ggf. eine Fehlermeldung an. Die ausgewählten Dateien werden hochgeladen.

4.2.5 FA-WF-5 Einsehen von Statusinformationen zu eingelieferten elektronischen Rechnungen

4.2.5.a User Story

Story: Als Rechnungssender möchte ich, unabhängig vom Übertragungskanal, Statusinformationen zu meinen eingelieferten elektronischen Rechnungen einsehen.

Nutzer: Rechnungssender

Beteiligte Module: Weberfassung, Übertragungskanäle, Prüfung, Adressierung

Berechtigung: E-RECHNUNGS-NUTZER

4.2.5.b Funktionen

Dem Rechnungssender soll eine Liste mit Statusinformationen zu seinen eingelieferten elektronischen Rechnungen zur Verfügung gestellt werden. Die Listenansicht unterstützt die Filterung, Sortierung und Navigation durch die gelieferten elektronischen Rechnungen. Die elektronischen Rechnungen selbst werden nicht gespeichert und auch nicht angezeigt, sondern nur verfügbare Statusinformationen.

4.2.5.c Mögliche Status

Die folgenden Status kann eine elektronische Rechnung aufweisen:

- Empfangen: Die elektronische Rechnung ist auf dem spezifischen Übertragungskanal empfangen worden.
- Weitergeleitet: Die elektronische Rechnung hat alle technischen Prüfungen bestanden und wurde an die zuständige Behörde digital zur Freigabeprüfung weitergeleitet.
- Abgewiesen: Die elektronische Rechnung wurde aufgrund eines negativen Prüfprotokolls abgewiesen. Die Fehlermeldungen/Verletzungen aus dem Prüfprotokoll sind online einsehbar. Die Rechnung ist nicht mehr im System vorhanden.
- Fehler: Die elektronische Rechnung konnte aufgrund eines Fehlers z. B. durch eine fehlerhafte Auftragskennnummer, einen technischen Übertragungsfehler bei der Weiterleitung usw. nicht weitergeleitet werden. Die Rechnung ist nicht mehr im System vorhanden.

4.2.5.d Akzeptanzkriterien

- Der Nutzer erhält eine Listenansicht mit den Status aller von ihm eingelieferten elektronischen Rechnungen.
- Der Nutzer erhält über ein entsprechendes Eingabefeld die Möglichkeit zur Filterung der Ergebnismenge.
- Die Tabelle enthält die Spalten Einlieferungsdatum, Übertragungskanal, Auftragskennnummer, Fehlermeldung und ein Icon zum Download des Prüfprotokolls.
- Die Tabelle ist standardmäßig nach der Spalte Einlieferungsdatum sortiert.
- Der Nutzer erhält die Möglichkeit zur Sortierung der Ergebnismenge.
- Der Nutzer erhält die Möglichkeit zum Blättern in der Ergebnismenge.

4.2.6 FA-WF-6 Einsehen der Nutzungsbedingungen

4.2.6.a User Story

Story: Als Rechnungssender möchte ich an prominenter Stelle auf die Nutzungsbedingungen und die Funktionsweise des zentralen eRechnungseingangs hingewiesen werden.

Nutzer: Rechnungssender

Beteiligte Module: Weberfassung

Berechtigung: E-RECHNUNGS-NUTZER

4.2.6.b Funktionen

Dem Rechnungssender sollen innerhalb des Portals an prominenter Stelle die Nutzungsbedingungen des zentralen eRechnungseingangs präsentiert werden. An dieser Stelle kann er ebenfalls alle zu beachtenden Standards der elektronischen Rechnungserstellung über Links erreichen. Der Rechnungssender soll über die Nutzungsbedingungen und einen visuell ansprechenden Walkthrough möglichst schnell in die Lage versetzt werden, elektronische Rechnungen an den zentralen eRechnungseingang zu liefern.

4.2.6.c Akzeptanzkriterien

- Der Nutzer erhält alle notwendigen Nutzungsbedingungen in einem visuell ansprechenden Format.
- Dem Nutzer werden Links zu allen Standards der elektronischen Rechnungserstellung präsentiert.
- Die Nutzung des zentralen eRechnungseingangs wird anhand eines visuell ansprechenden Walkthroughs anschaulich erklärt.

4.3 Übertragungskanäle (ÜK)

Dem Rechnungssteller stehen neben der Lieferung über die Webanwendung folgende Übertragungskanäle zur Verfügung:

- Übertragung mittels Webservice
- Übertragung mittels De-Mail
- Übertragung mittels E-Mail

4.3.1 FA-ÜK-1 Übertragung mittels Webservice

4.3.1.a User Story

Story: Als Rechnungssender möchte ich eine elektronische Rechnung per Webservice an den zentralen eRechnungseingang schicken.

Nutzer: Rechnungssender (technischer Webservice-Nutzer)

Beteiligte Module: Übertragungskanäle

Berechtigung: E-RECHNUNGS-WS-NUTZER

4.3.1.b Funktionen

Der Rechnungssender hat per Webservice die Möglichkeit, eine elektronische Rechnung an den zentralen eRechnungseingang zu schicken. Die gesamte elektronische Rechnung mit maximal 200 rechnungsbegründenden Dokumenten darf eine Gesamtgröße von 15 Megabyte nicht überschreiten.

Der Rechnungssender erhält per Webservice im Fehlerfall eine sofortige Antwort. Alle Informationen sind im Portal über die Statusansicht einsehbar.

4.3.1.c Validierungen

- Als Rechnung wird nur eine elektronische Rechnung nach dem XRechnungsstandard anerkannt.
- Es werden dem XRechnungsstandard folgend nur die folgenden Formate als Anlagen akzeptiert: PDF, PNG, JPEG, CSV, XLSX, ODS.
- Es dürfen maximal 200 rechnungsbegründende Anhänge angefügt werden.
- Die Gesamtgröße der elektronischen Rechnung inklusive aller Anlagen darf 15 Megabyte nicht übersteigen.

4.3.1.d Akzeptanzkriterien

- Der Status einer per Webservice eingelieferten elektronischen Rechnung wird innerhalb des Portals gespeichert.
- Verletzungen der Validierungsregeln führen zur Ablehnung der gesamten elektronischen Rechnung.

4.3.2 FA-ÜK-2 Übertragung mittels De-Mail

4.3.2.a User Story

Story: Als Rechnungssender möchte ich eine elektronische Rechnung per De-Mail an den zentralen eRechnungseingang schicken.

Nutzer: Rechnungssender

Beteiligte Module: Übertragungskanäle

Berechtigung: E-RECHNUNGS-DE-MAIL-NUTZER

4.3.2.b Funktionen

Der Rechnungssender hat per De-Mail die Möglichkeit, eine elektronische Rechnung an den zentralen eRechnungseingang zu schicken. Die gesamte elektronische Rechnung mit maximal 200 rechnungsbegründenden Dokumenten darf eine Gesamtgröße von 15 Megabyte nicht überschreiten. Als Rechnung wird nur eine elektronische Rechnung, die dem Standard XRechnung folgt, anerkannt.

Der Rechnungssender erhält per De-Mail nur im Fehlerfall eine Antwort. Sonstige Informationen sind im Portal über die Statusansicht einsehbar.

4.3.2.c Validierungen

- Dem CEN folgend werden nur die folgenden Formate als Anlagen akzeptiert: PDF, PNG, JPEG, CSV, XLSX, ODS.
- Es dürfen maximal 200 rechnungsbegründende Anhänge angefügt werden.
- Die Gesamtgröße der elektronischen Rechnung inklusive aller Anlagen darf 15 Megabyte nicht übersteigen.

4.3.2.d Akzeptanzkriterien

- Der Status einer per De-Mail eingelieferten elektronischen Rechnung wird innerhalb des Portals gespeichert.
- Verletzungen der Validierungsregeln führen zur Ablehnung der gesamten elektronischen Rechnung. Der Rechnungssender wird über die Ablehnung informiert.
- Wenn sich die elektronische Rechnung nicht öffnen lässt, wird die Nachricht gelöscht.
- Der Text der De-Mail-Nachricht wird ignoriert und nicht als rechnungsbegründendes Dokument weitergeleitet.

4.3.3 FA-ÜK-3 Übertragung mittels E-Mail

4.3.3.a User Story

Story: Als Rechnungssender möchte ich eine elektronische Rechnung per E-Mail an den zentralen eRechnungseingang schicken.

Nutzer: Rechnungssender

Beteiligte Module: Übertragungskanäle

Berechtigung: E-RECHNUNGS-E-MAIL-NUTZER

4.3.3.b Funktionen

Der Rechnungssender hat per E-Mail die Möglichkeit, eine elektronische Rechnung an den zentralen eRechnungseingang zu schicken. Die gesamte elektronische Rechnung mit maximal 200 rechnungsbegründenden Dokumenten darf eine Gesamtgröße von 15 Megabyte nicht überschreiten. Als Rechnung wird nur eine elektronische Rechnung, die dem Standard XRechnung folgt, anerkannt.

Der Rechnungssender erhält per E-Mail keine Bestätigung und auch keine Nachricht im Fehlerfall. Diese Informationen sind im Portal über die Statusansicht einsehbar. Die E-Mail als Hülle wird gelöscht.

Die Verschlüsselung und Signatur der E-Mail-Nachricht wird grundsätzlich unterstützt, ist aber nicht zwingend erforderlich.

4.3.3.c Validierungen

- Es werden dem XRechnungsstandard folgend nur die folgenden Formate als Anlagen akzeptiert: PDF, PNG, JPEG, CSV, XLSX, ODS.
- Es dürfen maximal 200 rechnungsbegründende Anhänge angefügt werden.
- Die Gesamtgröße der elektronischen Rechnung inklusive aller Anlagen darf 15 Megabyte nicht übersteigen.

4.3.3.d Akzeptanzkriterien

- Der Status einer per E-Mail eingelieferten elektronischen Rechnung wird innerhalb des Portals gespeichert.
- Verletzungen der Validierungsregeln führen zur Ablehnung der gesamten elektronischen Rechnung. Der Rechnungssender wird über die Ablehnung informiert.
- Wenn sich die elektronische Rechnung nicht öffnen lässt, wird die Nachricht gelöscht.
- Der Text der E-Mail-Nachricht wird ignoriert und nicht als rechnungsbegründendes Dokument weitergeleitet.

4.3.4 Gesonderte Fehlerbehandlung bei den Übertragungskanälen

4.3.4.a Überschreitung der maximal erlaubten Anzahl an Anhängen

Kanal: E-Mail, De-Mail, Webservice

Beschreibung: Es werden mehr als 200 Anhänge übertragen.

Konsequenz: Bei dem Übertragungskanal E-Mail wird die Nachricht ohne Rückmeldung gelöscht. Die Rechnung wird abgewiesen und nicht weiterverarbeitet. Bei allen Übertragungskanälen wird der Status im Portal gesetzt.

Fehlermeldung: noch zu definieren

4.3.4.b Überschreitung der maximal erlaubten Gesamtgröße der Anhänge

Kanal: E-Mail, De-Mail, Webservice

Beschreibung: Die Gesamtgröße aller Anlagen übersteigt 15 Megabyte.

Konsequenz: Bei dem Übertragungskanal E-Mail wird die Nachricht ohne Rückmeldung gelöscht. Die Rechnung wird abgewiesen und nicht weiterverarbeitet. Bei allen Übertragungskanälen wird der Status im Portal gesetzt.

Fehlermeldung: noch zu definieren

4.3.4.c Nachricht enthält keine Rechnungsdatei

Kanal: E-Mail, De-Mail, Webservice

Beschreibung: Eine Nachricht enthält keine elektronische Rechnungsdatei, die als XML interpretiert werden kann.

Konsequenz: Bei dem Übertragungskanal E-Mail wird die Nachricht ohne Rückmeldung gelöscht. Bei allen Übertragungskanälen wird der Fehlerstatus im Portal gesetzt.

Fehlermeldung: noch zu definieren

4.3.4.d Nachricht enthält mehrere Rechnungsdateien

Kanal: E-Mail, De-Mail, Webservice

Beschreibung: Eine Nachricht enthält mehrere separate Rechnungsdateien.

Konsequenz: Bei dem Übertragungskanal E-Mail wird die Nachricht ohne Rückmeldung gelöscht. Die Rechnung wird abgewiesen und nicht weiterverarbeitet. Bei allen Übertragungskanälen wird der Status im Portal gesetzt.

Fehlermeldung: noch zu definieren

4.3.4.e Format der Rechnungsdatei nicht unterstützt

Kanal: E-Mail, De-Mail, Webservice

Beschreibung: Eine Nachricht enthält eine elektronische Rechnungsdatei in einem nicht unterstützten Format.

Konsequenz: Bei dem Übertragungskanal E-Mail wird die Nachricht ohne Rückmeldung gelöscht. Bei allen Übertragungskanälen wird der Fehlerstatus im Portal gesetzt.

Fehlermeldung: noch zu definieren

4.3.4.f Unbekannte Absenderadresse

Kanal: E-Mail

Beschreibung: Die Absenderadresse kann nicht erfolgreich abgeglichen werden, da diese keinem Benutzerkonto zugeordnet werden kann oder der Übertragungskanal nicht aktiviert wurde.

Konsequenz: Die Nachricht wird ohne Rückmeldung gelöscht.

Fehlermeldung: n. v.

4.3.4.g Falsche Anmeldedaten

Kanal: Webservice

Beschreibung: Es wurde kein Benutzername angegeben oder der Benutzername ist nicht vorhanden.

Konsequenz: Die elektronische Rechnung kann nicht eingeliefert werden.

Fehlermeldung: noch zu definieren

4.3.4.h Falsches Passwort

Kanal: Webservice

Beschreibung: Es wurde kein Passwort angegeben oder das Passwort ist nicht korrekt.

Konsequenz: Die elektronische Rechnung kann nicht eingeliefert werden.

Fehlermeldung: noch zu definieren

4.3.4.i Rechnungsbegründende Informationen im Nachrichtentext

Kanal: E-Mail, De-Mail

Beschreibung: Eine Nachricht enthält neben einer elektronischen Rechnungsdatei und Anlagen noch weitere rechnungsbegründende Informationen im Nachrichten-Text.

Konsequenz: Die zusätzlichen Informationen werden ignoriert.

Fehlermeldung: n. v.

4.3.4.j Nachricht enthält unzulässiges Dateiformat

Kanal: E-Mail, De-Mail, Webservice

Beschreibung: Eine Nachricht enthält ein Dateiformat, das nicht zu den zulässigen Dateiformaten zählt. Dem XRechnungsstandard folgend werden nur die folgenden Dateiformate für Anlagen unterstützt: PDF, PNG, JPEG, CSV, XLSX, ODS

Konsequenz: Falls ein unzulässiges Dateiformat übermittelt wird, wird die gesamte Rechnung abgelehnt. Bei dem Übertragungskanal E-Mail wird die Nachricht ohne Rückmeldung gelöscht. Bei allen Übertragungskanälen wird der Status im Portal gesetzt.

Fehlermeldung: noch zu definieren

4.3.4.k Konto gesperrt

Kanal: Webservice

Beschreibung: Das Konto ist gesperrt, da der Nutzer zu häufig ein falsches Passwort mitgeschickt hat.

Konsequenz: Die elektronische Rechnung kann nicht eingeliefert werden.

Fehlermeldung: noch zu definieren

4.4 Prüfung der elektronischen Rechnung (PR)

Nachfolgend werden die Anforderungen an die Prüfung einer elektronischen Rechnung beschrieben. Die Prüfung soll in einem eigenen funktionalen Modul umgesetzt werden.

Das Modul prüft eingehende elektronische Rechnungen auf Konformität zum XRechnungsstandard, bevor eine Weiterleitung an den Rechnungsempfänger angestoßen wird. Die Konformitätsprüfung umfasst sowohl die Prüfung der technischen Validität hinsichtlich der zu verwendenden Syntaxen (UBL, UN/CEFACT) als auch die Prüfung der Konformität hinsichtlich der zugrundeliegenden semantischen Datenmodelle (nach dem Standard XRechnung). Rechnungen, die konform zu einer der beiden Syntaxen und zum semantischen Datenmodell sind, werden als spezifikationskonform bezeichnet und sind vom Rechnungsempfänger innerhalb der öffentlichen Verwaltung anzunehmen. Die Geschäftsregeln beinhalten „harte“ und „weiche“ Kriterien. Erfüllt eine Rechnung die „harten“ Kriterien nicht, darf die Rechnung nicht weiterverarbeitet werden. Werden die „weichen“ Kriterien nicht eingehalten, darf die Rechnung trotzdem verarbeitet werden.

4.4.1 FA-PR-1 Schemaprüfung der elektronischen Rechnung

4.4.1.a User Story

Story: Als Modul des zentralen eRechnungseingangs will das System die übergebene elektronische Rechnung anhand eines XML Schemas auf strukturelle Korrektheit überprüfen.

Nutzer: System

Beteiligte Module: Prüfung

Berechtigung: E-RECHNUNGS-PRUEFUNGS-NUTZER

4.4.1.b Funktionen

Die übergebene elektronische Rechnung im XML-Format wird technisch anhand eines XML-Schemas überprüft. Das Prüfergebnis ist entweder positiv oder negativ. Bei einem negativen Prüfergebnis werden alle auftretenden Schemaverletzungen als Teil des Prüfergebnisses zurückgeliefert.

4.4.1.c Akzeptanzkriterien

- Ist die gelieferte elektronische Rechnung im XML-Format schemakonform, wird ein positives Prüfergebnis geliefert.
- Ist die elektronische Rechnung nicht schemakonform, werden alle auftretenden Verletzungen als Teil eines negativen Prüfergebnisses zurückgeliefert.

4.4.2 FA-PR-2 Austausch des XML-Schemas

4.4.2.a User Story

Story: Als Administrator des zentralen eRechnungseingangs will ich das XML-Schema zur strukturellen Überprüfung von elektronischen Rechnungen einfach austauschen können.

Nutzer: Administrator des zentralen eRechnungseingangs

Beteiligte Module: Prüfung

Berechtigung: E-RECHNUNGS-ADMINISTRATOR

4.4.2.b Funktionen

Der Austausch des XML-Schemas muss ohne eine neue Auslieferung oder Installation der gesamten Software erfolgen. Der Administrator des zentralen eRechnungseingangs muss hierfür lediglich die XML-Schemadateien austauschen bzw. die URL oder den Dateipfad anpassen.

4.4.2.c Akzeptanzkriterien

- Der Austausch eines XML-Schemas, das zur strukturellen Überprüfung von elektronischen Rechnungen verwendet wird, benötigt keine wiederholte Auslieferung oder Installation der gesamten Software. Lediglich die XML-Schemadateien selbst bzw. die URL (oder der Dateipfad) sind anzupassen.
- Nach der Anpassung werden übergebene elektronische Rechnungen anhand der neu hinterlegten Dateien validiert.
- Sind die neu hinterlegten XML-Schemadateien fehlerhaft, wird der Fehler protokolliert (z. B. in einer Protokolldatei des Applikationsservers).
- Werden unter der hinterlegten URL oder dem Dateipfad keine gültigen XML-Schemadateien gefunden, wird dies protokolliert (z. B. in der Protokolldatei des Applikationsservers).

4.4.3 FA-PR-3 Schematronprüfung der elektronischen Rechnung

4.4.3.a User Story

Story: Als Modul des zentralen eRechnungseingangs will das System die übergebene elektronische Rechnung anhand eines Schematron-Schemas durch definierte Geschäftsregeln validieren.

Nutzer: System

Beteiligte Module: Prüfung

Berechtigung: E-RECHNUNGS-PRUEFUNGS-NUTZER

4.4.3.b Funktionen

Die gelieferte elektronische Rechnung im XML-Format wird anhand der Geschäftsregeln in einem Schematron-Schema überprüft. Hierbei gibt es zwei Kategorien von Geschäftsregeln. Die beiden Kategorien umfassen harte und weiche Geschäftsregeln. Die Verletzung von harten Geschäftsregeln führt zu einem negativen Prüfergebnis. Die Verletzung von weichen Geschäftsregeln wird in einem Prüfprotokoll vermerkt und als Teil eines positiven Prüfergebnisses zurückgeliefert.

4.4.3.c Akzeptanzkriterien

- Ist die gelieferte elektronische Rechnung im XML-Format schemakonform, wird ein positives Prüfergebnis geliefert. Das positive Prüfergebnis wird innerhalb eines Prüfprotokolls vermerkt und zurückgeliefert.
- Werden nur weiche Geschäftsregeln verletzt, werden die Verletzungen als Teil des Prüfprotokolls vermerkt und ein positives Prüfergebnis geliefert.
- Wenn harte Geschäftsregeln verletzt werden, hat dies ein negatives Prüfergebnis zur Folge. Alle Verletzungen werden als Teil des Prüfergebnisses zurückgeliefert.

4.4.4 FA-PR-4 Austausch des Schematron-Schemas

4.4.4.a User Story

Story: Als Administrator des zentralen eRechnungseingangs will ich das Schematron-Schema zur Überprüfung von elektronischen Rechnungen einfach austauschen können.

Nutzer: Administrator des zentralen eRechnungseingangs

Beteiligte Module: Prüfung

Berechtigung: E-RECHNUNGS-ADMINISTRATOR

4.4.4.b Funktionen

Der Austausch des Schematron-Schemas muss ohne eine neue Auslieferung oder Installation der gesamten Software erfolgen. Der Administrator des zentralen eRechnungseingangs muss hierfür lediglich die Schematron-Schemadateien austauschen bzw. die URL oder den Dateipfad anpassen.

4.4.4.c Akzeptanzkriterien

- Der Austausch eines Schematron-Schemas, das zur Überprüfung von elektronischen Rechnungen anhand von definierten Geschäftsregeln genutzt werden soll, benötigt keine wiederholte Auslieferung oder Installation der gesamten Software. Lediglich die XML-Schemadateien selbst bzw. die URL (oder der Dateipfad) sind anzupassen.
- Nach der Anpassung werden übergebene elektronische Rechnungen anhand der neu hinterlegten Dateien validiert.
- Sind die neu hinterlegten Schematron-Schemadateien fehlerhaft, wird der Fehler protokolliert (z. B. in einer Protokolldatei des Applikationsservers).
- Werden unter der hinterlegten URL oder dem Dateipfad keine gültigen Schematron-Schemadateien gefunden, wird dies protokolliert (z. B. in der Protokolldatei des Applikationsservers).

4.5 Adressierung und Weiterleitung (AD)

Dieses Kapitel befasst sich mit der Adressierung und Weiterleitung der elektronischen Eingangsrechnung vom zentralen Rechnungseingang zum nachgelagerten Rechnungsfreigabeworkflow (ERP-System). Hierfür ist es notwendig, die eingelieferte elektronische Rechnung korrekt an das nachgelagerte Rechnungsfreigabesystem (z. B. ein ERP-System) des Rechnungsempfängers zu liefern. Die Adressierung an das jeweilige nachgelagerte System muss anhand eines eindeutigen Kriteriums (die Auftragskennnummer) erfolgen, welches in der elektronischen Rechnung selbst mitgeliefert wird. Um dies zu bewerkstelligen, muss der XML-Datensatz ausgelesen, das Kriterium extrahiert und anhand einer Mappingtabelle entschieden werden, welches nachgelagerte System das korrekte System des Rechnungsempfängers ist. Anschließend erfolgt die Weiterleitung (über die technische Zieladresse) an das jeweilige nachgelagerte System.

4.5.1 FA-AD-1 Pflege der Zieladressen

4.5.1.a User Story

Story: Als Administrator des zentralen Rechnungseingangs muss ich die technischen Zieladressen der jeweiligen Behörden einspielen und aktualisieren können.

Nutzer: Administrator des zentralen eRechnungseingangs

Beteiligte Module: Adressierung

Berechtigung: E-RECHNUNGS-ADMINISTRATOR

4.5.1.b Funktionen

Eine Mappingtabelle, bei der die technische Adresse der jeweiligen Zielbehörde anhand der Auftragskennnummer (bzw. anhand eines definierten Abschnitts der Auftragskennnummer) der elektronischen Rechnung gefunden wird, muss von dem Administrator des zentralen Rechnungseingangs gepflegt werden. Anhand der technischen Adresse werden die elektronische Rechnung und alle rechnungsbegründenden Dokumente sowie das Prüfprotokoll an die korrekte Behörde digital weitergeleitet.

4.5.1.c Akzeptanzkriterien

- Nach der Aktualisierung der Mappingtabelle durch den Administrator des zentralen eRechnungseingangs werden für eine Suche nach der korrekten Adresse nur die aktuellen Daten sätze genutzt.
- Eine Aktualisierung ist durch den Administrator durchführbar und bedarf keiner neuen Auslieferung oder Neuinstallation des Systems.

4.5.2 FA-AD-2 Finden der korrekten Zieladresse

4.5.2.a User Story

Story: Als Modul des zentralen eRechnungseingangs will das System anhand der in der elektronischen Rechnung enthaltenen Auftragskennnummer die technische Zieladresse finden.

Nutzer: System

Beteiligte Module: Adressierung

Berechtigung: E-RECHNUNGS-ADRESSIERUNGS-NUTZER

4.5.2.b Funktionen

In einer elektronischen Rechnung dient die Auftragskennnummer (bzw. ein Teil der Auftragskennnummer) als eindeutiges Kriterium für die Weiterleitung an das korrekte nachgelagerte System der jeweiligen Zielbehörde. Hierfür muss eine Mappingtabelle existieren, anhand derer die korrekte technische Zieladresse gefunden wird. Wenn kein passendes Mapping gefunden wird, soll ein eindeutiger Fehler (keine generische Fehlermeldung) signalisiert werden.

4.5.2.c Akzeptanzkriterien

- Wird anhand der gelieferten Auftragskennnummer ein passender Eintrag gefunden, wird die technische Adresse des Zielsystems der jeweiligen Behörde zurückgeliefert.
- Es wird ein eindeutiger Fehler mit einer Fehlerbeschreibung protokolliert (z. B. in der Protokolldatei des Applikationsservers), falls kein eindeutiger Eintrag in der Mappingtabelle gefunden wird. Der Fehler wird zurückgeliefert.

4.5.3 FA-AD-3 Weiterleitung der elektronischen Rechnung an die korrekte Zieladresse

4.5.3.a User Story

Story: Als Modul des zentralen eRechnungseingangs will das System die übergebene elektronische Rechnung und die rechnungsbegründenden Anlagen sowie das Prüfprotokoll an die korrekte Zieladresse weiterleiten.

Nutzer: System

Beteiligte Module: Adressierung

Berechtigung: E-RECHNUNGS-ADRESSIERUNGS-NUTZER

4.5.3.b Funktionen

In einer elektronischen Rechnung dient die Auftragskennnummer (bzw. ein Teil der Auftragskennnummer) als eindeutiges Kriterium für die Weiterleitung an das korrekte nachgelagerte System der jeweiligen Zielbehörde. Wenn die Zieladresse anhand der Auftragskennnummer gefunden wurde, wird die übergebene elektronische Rechnung inklusive aller rechnungsbegründenden Unterlagen und des Prüfprotokolls digital an die Zielbehörde weitergeleitet.

4.5.3.c Akzeptanzkriterien

- Die elektronische Rechnung inklusive aller rechnungsbegründenden Unterlagen und des Prüfprotokolls wird digital an die Zielbehörde bzw. das zuständige elektronische System weitergeleitet.
- Es wird ein eindeutiger Fehler mit einer Fehlerbeschreibung protokolliert (z. B. in der Protokolldatei des Applikationsservers), wenn ein Übertragungsfehler auftritt.

4.6 Berechtigungskonzept

In der folgenden Tabelle werden die erforderlichen Mindestberechtigungen für Nutzergruppen des zentralen eRechnungseingangs skizziert:

Nutzergruppe	Berechtigung	Bemerkungen
Rechnungssender	E-RECHNUNGS-NUTZER	Ein Rechnungssender, der sich am Portal registriert hat, benötigt die Berechtigung, um sich anzumelden und sein Benutzerkonto aufzurufen.
Rechnungssender	E-RECHNUNGS-WEB-NUTZER	Ein registrierter Rechnungssender, der die Weberfassung oder den Web-Upload nutzt.
Rechnungssender	E-RECHNUNGS-WS-NUTZER	Ein registrierter Rechnungssender, der elektronische Rechnungen über den Webservice einliefert.
Rechnungssender	E-RECHNUNGS-E-MAIL-NUTZER	Ein registrierter Rechnungssender, der elektronische Rechnungen per E-Mail einliefert; Die genutzte

Nutzergruppe	Berechtigung	Bemerkungen
		E-Mail-Adresse muss in der White-list vorhanden sein.
Rechnungssender	E-RECHNUNGS-DE-MAIL-NUTZER	Ein registrierter Rechnungssender, der elektronische Rechnungen per De-Mail einliefert.
Administrator des zentralen eRechnungseingangs	E-RECHNUNGS-ADMINISTRATOR	Ein Administrator des zentralen e-Rechnungseingangs benötigt diese Berechtigung, um administrative Aufgaben wie z. B. Austausch des XML-Schemas oder der Schemat-ron-Dateien durchzuführen.
System	E-RECHNUNGS-PRUEFUNGS-NUT-ZER	Ein technischer Nutzer, der diese Berechtigung benötigt, um elektro-nische Rechnungen zu überprüfen.
System	E-RECHNUNGS-ADRESSIERUNGS-NUTZER	Ein technischer Nutzer, der diese Berechtigung benötigt, um elektro-nische Rechnungen weiterzuleiten.

Tabelle 4.1: Berechtigungskonzept

5 Nicht-funktionale Anforderungen

In diesem Kapitel werden die nicht-funktionalen Anforderungen gemäß ISO 25010 beschrieben. Die Anforderungen wurden in die Hauptkategorien Funktionalität, Zuverlässigkeit, Benutzbarkeit, Sicherheit, Effizienz, Wartbarkeit, Portabilität und Kompatibilität untergliedert.

Im Unterkapitel 5.1 werden Berechnungen für den Bund über zu erwartende Mengen von eRechnungen aufgestellt. Die aus diesen Berechnungen resultierende Anzahl an elektronischen Rechnungen muss von den Komponenten, die in diesem Dokument behandelt werden, verarbeitet werden können.

Im Unterkapitel 5.2 werden sämtliche Anforderungen, die für alle Module Gültigkeit haben, aufgeführt.

5.1 Berechnung des durchschnittlichen Rechnungsaufkommens

Der zentrale eRechnungseingang und seine vorhandenen Komponenten müssen in der Lage sein, die aus den folgenden Berechnungen resultierende Anzahl an elektronischen Rechnungen zu verarbeiten. Ebenso sollten die Ergebnisse der Mengenberechnung als Grundlage für eine ausreichende Dimensionierung der Hardware des Systems dienen.

5.1.1 Annahmen zur Berechnung

Für die Dimensionierung der Hardware des Systems inklusive seiner Komponenten werden die folgenden Annahmen getroffen:

1. Elektronische Rechnungen werden überwiegend innerhalb der Arbeitswoche und nicht während des Wochenendes eingeliefert. Daraus ergeben sich ca. 300 Tage im Jahr, an denen Rechnungssender elektronische Rechnungen an den zentralen Rechnungseingang übermitteln.
2. Elektronische Rechnungen werden nicht 24 Stunden am Tag, sondern möglicherweise eher zwischen 08:00 Uhr und 18:00 Uhr eingeliefert. Hieraus ergibt sich ein Zeitfenster von 10 Stunden.
3. Die Einlieferung von elektronischen Rechnungen per Weberfassung/Web-Upload umfasst nicht mehr als 50 % des Gesamtvolumens.
4. Die Erfassungsdauer von elektronischen Rechnungen per Weberfassung beträgt 10 Minuten.
5. Eine eingelieferte elektronische Rechnung ist i. d. R. nicht größer als 1 MB (das reine XML).
6. Die durchschnittliche Größe einer elektronischen Rechnung inklusive aller rechnungsbegründenden Anlagen beträgt 3 MB. Die maximale Größe wurde auf 15 MB und 200 Anlagen festgelegt.

Wenn Rechnungen an Wochenenden und nach 18:00 Uhr eingeliefert werden, käme es zu einer Entlastung des Systems, da sich die Anzahl der Rechnungen auf eine größere Zeitspanne verteilt. Werden weniger als

50 % des Gesamtvolumens der Rechnungen über die Weberfassung/Web-Upload eingeliefert, wird das System ebenfalls entlastet.

5.1.2 Berechnung für den Bund

Vom BMF wird pro Jahr ein Aufkommen von ca. 4 Millionen Rechnungen für die unmittelbaren Bundesbehörden geschätzt. Wird die mittelbare Bundesverwaltung hinzugezählt, schätzt das BMF das Rechnungsaufkommen auf insgesamt ca. 8 Millionen Rechnungen pro Jahr (vgl. Implementierungskonzept zur eRechnung für die Bundesverwaltung).

Daraus ergibt sich die folgende Durchschnittsberechnung:

Abbildung 5.1: Durchschnittsberechnung Rechnungen/Minute (Bund)

Es wird durchschnittlich der Empfang von 44 elektronischen Rechnungen pro Minute angenommen.

Weberfassung: Durchschnittlich **22 elektronische Rechnungen** (50 % von 44 Rechnungen) müssen **pro Minute** erfasst werden können.

Übertragungskanäle: Durchschnittlich **44 elektronische Rechnungen pro Minute** müssen über die angebotenen Übertragungskanäle eingeliefert werden können.

Prüfung: Durchschnittlich **44 elektronische Rechnungen** müssen **pro Minute** geprüft werden können.

Adressierung/Weiterleitung: Durchschnittlich 44 elektronische Rechnungen müssen **pro Minute** weitergeleitet werden können.

5.1.3 Berechnung für das Land Bremen

Das Rechnungsvolumen wird vom Land Bremen auf ca. 500.000 Rechnungen pro Jahr geschätzt.

Daraus ergibt sich die folgende Durchschnittsberechnung:

Abbildung 5.2: Durchschnittsberechnung Rechnungen/Minute (Bremen)

Es wird durchschnittlich der Empfang von 3 elektronischen Rechnungen pro Minute angenommen.

Weberfassung: Durchschnittlich müssen **1,5 elektronische Rechnungen** (50 % von 3 Rechnungen) **pro Minute** erfasst können.

Übertragungskanäle: Durchschnittlich **3 elektronische Rechnungen pro Minute** müssen über die angebotenen Übertragungskanäle eingeliefert werden können.

Prüfung: Durchschnittlich **3 elektronische Rechnungen** müssen **pro Minute** geprüft werden können.

Adressierung/Weiterleitung: Durchschnittlich **3 elektronische Rechnungen** müssen **pro Minute** weitergeleitet werden können.

5.2 Gesamtsystem (modulübergreifend)

Im Folgenden werden nicht-funktionale Anforderungen beschrieben, die modulübergreifend für das Gesamtsystem Gültigkeit haben und deshalb auch von den einzelnen Modulen selbst unterstützt werden müssen. Die hier genannten Anforderungen werden in den modulspezifischen Anforderungen nicht wiederholt.

5.2.1 Funktionalität (FU)

5.2.1.a NFA-FU-1 Vollständigkeit

Das Gesamtsystem, bestehend aus seinen einzelnen Modulen mit entsprechenden technischen Komponenten, muss die Anforderungen vollständig erfüllen. Dies gilt sowohl für die spezifischen Anforderungen an die einzelnen Module als auch an die Integration der einzelnen Module in ein Gesamtsystem.

Die Leistungspflicht umfasst somit alle Leistungen, die – unabhängig von ihrer ausdrücklichen Erwähnung – erforderlich sind, um die Vollständigkeit und Funktionsfähigkeit des Gesamtsystems herbeizuführen.

5.2.2 Zuverlässigkeit (ZU)

5.2.2.a NFA-ZU-1 Reife

Nur ausgereifte Lösungen sind einzusetzen. Systemversagen durch Fehlerzustände sind auszuschließen (siehe auch Fehlertoleranz). Praxiserprobte Lösungen sind Neuentwicklungen vorzuziehen. Nur an den Stellen, an denen nicht auf vorhandene technische Lösungen aufgebaut werden kann und fertige Lösungen am Markt nicht verfügbar sind, ist eine Neuentwicklung zu erwägen.

5.2.2.b NFA-ZU-2 Verfügbarkeit

Es muss eine Verfügbarkeit des Gesamtsystems von mindestens 98,5% gewährleistet sein.

5.2.2.c NFA-ZU-3 Fehlertoleranz

Das Gesamtsystem muss auch bei auftretenden Fehlern ohne Unterbrechung betrieben werden können. Fehler müssen protokolliert und berichtet werden. Wiedereinsetzung sowie Rücksetzung der Prozessierung am Fehlerpunkt sollte möglich sein.

5.2.2.d NFA-ZU-4 Wiederherstellbarkeit

Entfällt, da fehlertolerant.

5.2.3 Benutzbarkeit (BU)

5.2.3.a NFA-BU-1 Erlernbarkeit

Mit der Weberfassung soll insbesondere Rechnungssendern mit nur wenigen einzubringenden Rechnungen ein Zugangsweg eröffnet werden. Daher muss diese Komponente möglichst intuitiv benutzbar bzw. im Selbststudium leicht erlernbar sein.

Die Erlernbarkeit des Gesamtsystems bezieht sich auf die Administration, da das Gesamtsystem nur von Administratoren bedient wird. Aspekte der Erlernbarkeit hinsichtlich der Rechnungssender werden in diesem Dokument in den entsprechenden Modulen gesondert aufgeführt.

Die Administratoren sind durch die Bereitstellung von Handbüchern und Dokumentationen in die Lage zu versetzen, die Bedienung des System selbstständig zu erlernen. Für detaillierte Nachfragen muss ein Support des Herstellers zur Verfügung stehen.

5.2.3.b NFA-BU-2 Bedienbarkeit

Für das Gesamtsystem gilt, dass Administrationsoberflächen zur Verfügung gestellt werden sollen, über die grundlegende Einstellungen bzw. Customizings vorgenommen werden können.

Für die Gestaltung sämtlicher Oberflächen (sowohl Administrationsoberflächen als auch Oberflächen für Rechnungssender) sind die einschlägigen Kriterien zur Softwareergonomie (insbesondere DIN EN ISO 9241 und BildscharbV) zu berücksichtigen.

5.2.3.c NFA-BU-3 Schutz vor Fehlern des Benutzers

Das Ergebnis einer Erfassung über das Webformular sollte in einer validen XRechnung münden. Entsprechend sind fehlerhafte Eingaben durch die Benutzer zu verhindern.

Für das Gesamtsystem gilt, dass die Administrationsoberfläche nur gültige Eingaben zulassen soll und ggf. bei Logikprüfungen Warnmeldungen erzeugen sollte.

5.2.3.d NFA-BU-4 Barrierefreiheit

Benutzeroberflächen sind unter Beachtung der einschlägigen Normen barrierefrei zu gestalten, um eine Benutzung für Menschen mit körperlichen und kognitiven Beeinträchtigungen zu ermöglichen. Entsprechende Anforderungen sind u. a. im Sozialgesetzbuch IX (SGB IX), im Allgemeinen Gleichbehandlungsgesetz (AGG), im Behindertengleichstellungsgesetz BGG (§11 Barrierefreie Informationstechnik), in der Barrierefreien Informationstechnik Verordnung (BITV) und in der BremBITV 2.0 definiert.

5.2.4 Sicherheit (SI)

5.2.4.a NFA-SI-1 Vertraulichkeit

Die zu verarbeitenden Informationen in den Rechnungen können unterschiedlichen Vertrauensniveaus unterliegen. Dazu werden unterschiedliche Eingangskanäle mit einem unterschiedlichen Vertrauensschutz angeboten. Innerhalb der Rechnungseingangskomponente findet eine technische Prüfung der Rechnung auf Inhaltsebene statt (z. B. Virenprüfung, Schemaprüfung). Entsprechend sind technische und organisatorische Vorkehrungen zu treffen, damit die Vertraulichkeit gewahrt wird. Dabei kann vom Schutzbedarf "normal" im Sinne der Schutzkategorien des IT-Grundschutzes des BSI ausgegangen werden, da sich das schwerwiegendste Schadensszenario nur auf wenige Beteiligte auswirken dürfte und/oder im eigenen Bereich überschaubare Auswirkungen hätte.

Der Transport der Anmeldeinformationen sowie der Rechnungsdaten bzw. Rechnungsdatei ist aus Sicherheitsgründen stets nach den Vorgaben des BSI (vgl. BSI TR-02102-2) durch TLS (Transport Layer Security) zu verschlüsseln.

5.2.4.b NFA-SI-2 Integrität

Das System muss die Integrität (Unversehrtheit) der transportieren, ggf. verarbeiteten sowie erzeugten Daten sicherstellen. Rechnungsdaten müssen vollständig und unverändert erhalten bleiben.

5.2.4.c NFA-SI-3 Nachweisbarkeit

Die Nachweisführung über den Empfang einer Rechnung obliegt i. d. R. dem Rechnungssteller. Zur Nachweisbarkeit werden verschiedene Einlieferungskanäle eröffnet, die unterschiedlich rechtssichere Nachweise ermöglichen (z. B. De-Mail).

Im System wird für jede elektronsiche Rechnung ein Laufzettel geführt, der durch die unterschiedlichen Module durchgereicht und ggf. angereichert wird. In diesem Laufzettel werden die Prozessschritte und durchgeführten Aktivitäten protokolliert.

5.2.4.d NFA-SI-4 Ordnungsmäßigkeit

Die ordnungsgemäße Funktionsweise des Systems entsprechend seiner Dokumentation muss gewährleistet und nachgewiesen werden.

5.2.4.e NFA-SI-5 Authentizität

Das System soll die Weiterleitung von eingehenden Rechnungen und Anhängen nur zulassen, wenn der Rechnungssteller zuvor registriert wurde. Allerdings sind die Anforderungen an diesen Nachweis – je nach Eingangskanal – gering zu halten. Der Einsatz digitaler Signaturen ist verzichtbar. Sofern eine Nachricht mit digitaler Signatur übermittelt wird, ist diese zu prüfen.

Zugangsbeschränkungen zum System selbst sind durch entsprechende Benutzerverwaltung auf Betriebs- und Datenbanksystemebene zu gewährleisten.

5.2.5 Effizienz (EF)

5.2.5.a NFA-EF-1 Zeitverhalten

Das System muss auch unter kurzfristigen Belastungsspitzen kurze Reaktionszeiten aufweisen. Insbesondere darf es nicht zu Verarbeitungsstaus kommen. Die Verarbeitungsdauer muss linear skalieren.

Die Verweildauer einer eingelieferten Rechnung im System darf 24 Stunden nicht überschreiten. Innerhalb dieser Zeit hat – im Falle von Fehlern bei der Schema- und Schematronprüfung – eine Nachricht an den Rechnungssteller zu ergehen.

5.2.5.b NFA-EF-2 Ressourcenverbrauch

Der Ressourcenverbrauch muss linear mit der Anzahl der zu verarbeitenden Rechnungen skalieren, sodass aufgrund von Erfahrungswerten über die Anzahl der zu erwartenden Rechnungen entsprechende Hardwareressourcen zur Verfügung gestellt werden können, die die Anforderungen im Zeitverhalten erfüllbar machen. Softwareseitig ist dafür Sorge zu tragen, dass der Ressourcenverbrauch bei Erfüllung aller sonstigen Anforderungen minimal gehalten wird. Eine Benennung der erforderlichen Ressourcen in Abhängigkeit vom Verarbeitungsvolumen hat zu erfolgen.

5.2.5.c NFA-EF-3 Kapazität

Die Verarbeitungskapazität des Systems darf softwareseitig nicht beschränkt sein und muss linear mit den zur Verfügung gestellten Hardwareressourcen skalieren.

5.2.6 Wartbarkeit (WA)

5.2.6.a NFA-WA-1 Modularität

Das Gesamtsystem ist modular aufzubauen. Damit ist die Wartbarkeit und Austauschbarkeit einzelner technischer Lösungen sowie die Nachnutzbarkeit vorhandener Lösungen maximiert.

5.2.6.b NFA-WA-2 Wiederverwendbarkeit

Die Wiederverwendbarkeit der Komponenten des System muss gewährleistet werden, damit die Lösung auf andere öffentliche Auftraggeber übertragbar ist. Idealerweise bedeutet dies, dass die technischen Lösungen als Komponenten des IT-Planungsrates betrieben werden. Diese Anforderung ist modulabhängig unterschiedlich stark ausgeprägt.

5.2.6.c NFA-WA-3 Analysierbarkeit

Das System muss durchgängig analysierbar sein. Ein Logging mit unterschiedlichen Log-Leveln unterstützt die Analysierbarkeit.

5.2.6.d NFA-WA-4 Änderbarkeit

Das System muss änderbar sein. Möglichst viele Einstellungen müssen über ein Customizing vor Ort konfigurierbar sein.

5.2.6.e NFA-WA-5 Testbarkeit

Jede Änderung am System muss testbar sein. Die Einrichtung einer Testinstanz muss ermöglicht werden. Testfälle müssen erstellbar, speicherbar, löschbar und im Bedarfsfall auslösbar sein. Testläufe müssen protokolliert werden und gegen eine Ergebniserwartung prüfbar sein.

5.2.7 Portabilität (PO)

5.2.7.a NFA-PO-1 Anpassbarkeit

Durch Customzingeinstellungen soll das System auch an anderen Umgebungen als den hier primär angestrebten (Standardserver im ITZBund und bei Dataport AöR) anpassbar sein. Dies zielt vor allem auch darauf ab, dass die hier entwickelte Lösung übertragbar sein soll und potenziell durch andere öffentliche Verwaltungen und damit in anderen Zielumgebungen aufgebaut und betrieben werden kann.

5.2.7.b NFA-PO-2 Installierbarkeit

Die Komponenten des Gesamtsystems müssen mit Installationsroutinen ausgeliefert werden, die die Herstellung der Betriebsbereitschaft in der Zielumgebung (Server der Rechenzentren des ITZBund sowie Dataport AöR) erlauben. Installationsanweisungen müssen mitgeliefert werden. Ein Support muss bereitstehen.

5.2.7.c NFA-PO-3 Austauschbarkeit

Die einzelnen technischen Komponenten des System sowie das Gesamtsystem sollen so gestaltet sein, dass ein Austausch gegen andere technische Lösungen grundsätzlich möglich ist. Dazu sind entsprechend produktneutrale Schnittstellen zwischen den einzelnen Komponenten vorzusehen.

5.2.8 Kompatibilität (KO)

5.2.8.a NFA-KO-1 Koexistenz

Sowohl das Gesamtsystem als auch die einzelnen Komponenten müssen neben anderen Anwendungen in derselben Betriebsumgebung laufen, ohne sich gegenseitig negativ zu beeinflussen. Durch Servervirtualisierungen fokussiert diese Anforderung überwiegend auf den gleichzeitigen Betrieb der einzelnen Komponenten des Gesamtsystems.

5.2.8.b NFA-KO-2 Interoperabilität

Das System muss die Interoperabilitätsstandards der XRechnung, insbesondere die Ergebnisses des Expertengremiums 3, implementieren, auch in der Interaktion zwischen den Modulen.

6 Abnahmekriterien

In diesem Kapitel werden die Abnahmekriterien, die eine Auswahl aus den funktionalen und nicht-funktionalen Anforderungen darstellen, erhoben und beschrieben. Nur zwingend notwendige konkrete Anforderungen werden hierfür in die Kriterien aufgenommen. Diese Abnahmekriterien werden für eine Prüfung der in Kapitel 2 beschriebenen Komponenten auf Nachnutzung innerhalb des zentralen eRechnungseingangs herangezogen.

Bei der späteren Realisierung sollten ebenso die allgemeiner formulierten Anforderungen Beachtung finden, die für eine Prüfung der Komponenten als weniger wichtig eingestuft wurden.

Zur Erleichterung der Nachverfolgung besitzt jedes Abnahmekriterium eine eindeutige Identifikationsnummer (ID). Für ein tieferes Verständnis des Abnahmekriteriums und um Redundanzen zu mindern, wird auf die zugrunde liegende Anforderung verwiesen.

6.1 Authentifikation

Kriterium ID	Zugrunde liegende Anforderung	Abnahmekriterien
AK-AU-1	Mehrsprachigkeit FA-AU-1	Die Benutzerführung erfolgt standardmäßig in der Browsersprache. Ist diese weder Englisch noch Deutsch, wird Deutsch verwendet. Schaltflächen ermöglichen einen Wechsel zwischen deutscher und englischer Benutzerführung. Das Portal speichert die Auswahl für künftige Besuche.
AK-AU-2	Erfassung von Registrierungsdaten FA-AU-2	Der Nutzer gibt sein Passwort zweimal identisch ein, wobei das Passwort nicht klar angezeigt wird. Der Nutzer wird durch eine Anzeige der Passwort-Güte unterstützt. Das Passwort muss den Vorgaben des IT-Grundschutz-Katalogs genügen (vgl. Abschnitt. M 2.11 Regelung des Passwortgebrauchs – https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02011.html). Nach erfolgreicher Eingabe der Registrierungsdaten werden die Passwörter zugriffssicher im System gespeichert und eine temporäre Aktivierungsmail mit dem Aktivierungslink an die hinterlegte E-Mail-Adresse verschickt.

Kriterium ID	Zugrunde liegende Anforderung	Abnahmekriterien
AK-AU-3	Aktivierung des Benutzerkontos FA-AU-3	Der Nutzer muss den Übertragungskanal auswählen und die erforderlichen Felder ausfüllen. Durch das Speichern werden die Daten an das Modul Authentifizierung übergeben.
AK-AU-4	Anmeldung FA-AU-4	Registrierte Nutzer können sich nach Eingabe der erforderlichen Felder anmelden, wodurch die Authentisierungsdaten an das Modul Authentifizierung übergeben werden. Über einen entsprechenden Link kann die Wiederherstellung des Passworts angefordert werden. Neue Nutzer können sich über eine verlinkte Eingabemaske registrieren.
AK-AU-5	Wiederherstellung des Passworts FA-AU-5	Die Wiederherstellung eines Passworts erfolgt über eine Maske zur Eingabe des Benutzernamens bzw. der E-Mail-Adresse. Nach Eingabe und Bestätigung wird ein temporärer Link an die hinterlegte E-Mail-Adresse versendet, sofern diese in der Datenbank enthalten ist. Über den temporären Link gelangt der Nutzer zu einer Maske zur Eingabe eines neuen Passworts, welches den Vorgaben des IT-Grundschutz-Katalogs (vgl. Abschnitt. M 2.11 Regelung des Passwortgebrauchs – https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02011.html) genügen muss. Bestätigt der Nutzer die Eingabe, wird das neue Passwort gespeichert und die Eingabemaske geschlossen.
AK-AU-6	Änderung von Stammdaten FA-AU-6	Die Bearbeitung der Stammdaten erfolgt über eine Eingabemaske.
AK-AU-7	Benutzerkonto löschen FA-AU-7	Nutzer können ihr Benutzerkonto entfernen. Vor der endgültigen Entfernung wird der Nutzer zur Bestätigung aufgefordert. Bricht der Nutzer nicht ab, erhält der Nutzer eine Bestätigungsmeldung.

Kriterium ID	Zugrunde liegende Anforderung	Abnahmekriterien
AK-AU-8	Ändern/ Freischalten von Übertragungskanälen FA-AU-8	Nutzer können Übertragungskanäle ändern. Nach Ausfüllen aller erforderlichen Felder kann der Nutzer die Übergabe der Authentisierungsdaten an das Modul Authentifizierung initiieren. Bei Freischaltung der Übertragungskanäle De-Mail und E-Mail werden die eingegebenen De-Mail- und E-Mail-Adressen in eine Whitelist eingetragen. Bei Freischaltung des Webservice-Zugangs ist ein zuvor gesperrter Zugang wieder entsperrt.
AK-AU-9	Vertraulichkeit NFA-SI-1	Die Übertragung der Daten erfolgt transportverschlüsselt.
AK-AU-10	Bedienbarkeit NFA-BU-2	Die Benutzeroberflächen entsprechen den ergonomischen Anforderungen der DIN EN ISO 9241 und der BildscharbV.
AK-AU-11	Wiederverwendbarkeit NFA-WA-2	Andere öffentliche Auftraggeber können diese Komponente nutzen. Sie ist im Idealfall eine Komponente des IT-Planungsrates.

Tabelle 6.1: Abnahmekriterien zur Authentifikation

6.2 Weberfassung

Kriterium ID	Zugrunde liegende Anforderung	Abnahmekriterien
AK-WF-1	Manuelle Erfassung einer Rechnung FA-WF-1	Nutzer können Rechnungen manuell erfassen. Über eine Schaltfläche können rechnungsbegründende Anlagen hochgeladen werden. Das Hochladen ausführbarer Dateien wird verhindert. Der für eine Grobadressierung zur rechnungsempfangenden Behörde ausreichender Teil der Auftragskennnummer baut sich automatisch (je nachdem welche Behörde ausgewählt wird) zusammen, falls diese beim Rechnungssender nicht bekannt ist Nutzer können die Eingabefelder zurücksetzen und damit alle zuvor getätigten Angaben löschen. Des Weiteren können Nutzer die Erstellung abbrechen. Nach abschließender Eingabe der Daten kann der Nutzer eine Generierung der elektronischen Rechnung sowie einen Versand im XML-Format an den zentralen eRechnungseingang anfordern. Der Nutzer kann die versendete XML-Datei lokal speichern. Der Eingang wird im Browser des Nutzers bestätigt.
AK-WF-2	Speichern eines Zwischenstands einer Rechnung FA-WF-2	Über eine Schaltfläche kann der Nutzer einen Zwischenstand der erfassten Daten erzeugen. Der Datensatz wird als XML formatiert und über den Webbrowser heruntergeladen.
AK-WF-3	Hochladen eines Zwischenstands einer Rechnung FA-WF-3	Über eine Schaltfläche kann der Nutzer einen Zwischenstand im XML-Format mittels eines Dokumenten-Auswahl-Dialogs laden. Nach erfolgreichem Hochladen werden erfasste Daten in die entsprechenden Eingabefelder übernommen.
AK-WF-4	Upload einer Rechnung FA-WF-4	Nutzer können Rechnungen über eine Schaltfläche hochladen. Über eine Maske kann ein Dokument ausgewählt werden. Anlagen können über Schaltflächen hinzugefügt und anschließend gelöscht werden. Über eine weitere Schaltfläche kann die Rechnung abgeschickt werden.

Kriterium ID	Zugrunde liegende Anforderung	Abnahmekriterien
AK-WF-5	Einsehen von Statusinformationen zu eingelieferten elektronischen Rechnungen FA-WF-5	Ein Nutzer kann sich den Status aller von ihm eingelieferten elektronischen Rechnungen in einer Tabelle anzeigen lassen. Die Tabelle enthält die Spalten Einlieferungsdatum, Übertragungskanal, Auftragskennnummer, Fehlermeldung und ein Icon zum Download des Prüfprotokolls. Die Tabelle ist standardmäßig nach der Spalte Einlieferungsdatum sortiert. Der Nutzer kann in der Ergebnismenge blättern, diese sortieren sowie über ein Eingabefeld filtern.
AK-WF-6	Einsehen der Nutzungsbedingungen FA-WF-6	Der Nutzer erhält alle notwendigen Nutzungsbedingungen in einem visuell ansprechenden Format. Links zu allen Standards der elektronischen Rechnungserstellung werden angezeigt. Die Nutzung des zentralen eRechnungseingangs wird anhand eines visuell ansprechenden Walkthroughs anschaulich erklärt.
AK-WF-7	Bedienbarkeit NFA-BU-2	Die Benutzeroberflächen entsprechen den ergonomischen Anforderungen der DIN EN ISO 9241 und der BildscharbV.
AK-WF-8	Vertraulichkeit NFA-SI-1	Die Übertragung der Daten erfolgt transportverschlüsselt.
AK-WF-9	Interoperabilität NFA-KO-2	Die Weberfassungskomponente nutzt für die Annahme/Erfassung sowie für die interne Weiterleitung an Modul ÜK die Interoperabilitätsstandards innerhalb des Standards XRechnung.

Tabelle 6.2: Abnahmekriterien zur Weberfassung

6.3 Übertragungskanäle

Kriterium ID	Zugrunde liegende Anforderung	Abnahmekriterien
AK-ÜK-1	Übertragung mittels Webservice FA-ÜK-1	Der Status einer per Webservice eingelieferten elektronischen Rechnung wird innerhalb des Portals gespeichert.
AK-ÜK-2	Übertragung mittels De-Mail FA-ÜK-2	Der Status einer per De-Mail eingelieferten elektronischen Rechnung wird innerhalb des Portals gespeichert. Wenn sich die elektronische Rechnung nicht öffnen lässt, wird die Nachricht gelöscht. Der Text der De-Mail-Nachricht wird ignoriert.
AK-ÜK-3	Übertragung mittels E-Mail FA-ÜK-3	Der Status einer per E-Mail eingelieferten elektronischen Rechnung wird innerhalb des Portals gespeichert. Wenn sich die elektronische Rechnung nicht öffnen lässt, wird die Nachricht gelöscht. Der Text der E-Mail-Nachricht wird ignoriert.
AK-ÜK-4	Vertraulichkeit NFA-SI-1	Die Übertragung der Daten erfolgt transportverschlüsselt.
AK-ÜK-5	Interoperabilität NFA-KO-2	Das Modul ÜK nutzt für die Annahme, den Laufzettel sowie für die interne Weiterleitung an das Modul PR die Interoperabilitätsstandards innerhalb des Standards XRechnung.
AK-ÜK-6	Wiederverwendbarkeit NFA-WA-2	Andere öffentliche Auftraggeber können diese Komponente nutzen. Sie ist im Idealfall eine Komponente des IT-Planungsrates.

Tabelle 6.3: Abnahmekriterien zu den Übertragungskanälen

6.4 Prüfung von elektronischen Rechnungen

Kriterium ID	Zugrunde liegende Anforderung	Abnahmekriterien
AK-PR-1	Schemaprüfung der elektronischen Rechnung FA-PR-1	Ist die elektronische Rechnung im XML-Format schemakonform, wird ein positives Prüfergebnis geliefert. Andernfalls werden alle auftretenden Verletzungen als Teil eines negativen Prüfergebnisses zurückgeliefert.
AK-PR-2	Austausch des XML-Schemas FA-PR-2	Der Austausch eines XML-Schemas, das zur strukturellen Überprüfung von elektronischen Rechnungen verwendet wird, benötigt keine wiederholte Auslieferung oder Installation der gesamten Software. Lediglich die XML-Schemadateien selbst bzw. die URL (oder der Dateipfad) sind anzupassen. Werden unter der hinterlegten URL oder dem Dateipfad keine gültigen XML-Schemadateien gefunden oder sind die neuen XML-Schemadateien fehlerhaft, wird der Fehler protokolliert. Nach erfolgreicher Anpassung werden übergebene elektronische Rechnungen neu validiert.
AK-PR-3	Schematronprüfung der elektronischen Rechnung FA-PR-3	Ist die elektronische Rechnung im XML-Format schemakonform, wird ein positives Prüfergebnis geliefert, innerhalb eines Prüfprotokolls vermerkt und zurückgeliefert. Werden nur weiche Geschäftsregeln verletzt, werden die Verletzungen als Teil des Prüfprotokolls vermerkt und ein positives Prüfergebnis wird geliefert. Werden harte Geschäftsregeln verletzt, werden die Verletzungen als Teil des Prüfergebnisses vermerkt und ein negatives Prüfergebnis wird geliefert.
AK-PR-4	Austausch des Schematron-Schemas FA-PR-4	Der Austausch eines Schematron-Schemas benötigt keine wiederholte Auslieferung oder Installation der gesamten Software. Lediglich die XML-Schemadateien selbst bzw. die URL (oder der Dateipfad) sind anzupassen. Werden unter der hinterlegten URL oder dem Dateipfad keine gültigen Schematron-Schemadateien gefunden oder sind die neu hinterlegten Schematron-Schemadateien fehlerhaft, wird der Fehler protokolliert.

Kriterium ID	Zugrunde liegende Anforderung	Abnahmekriterien
		Nach erfolgreicher Anpassung werden übergebene elektronische Rechnungen neu validiert.
AK-PR-5	Wiederverwendbarkeit AK-ÜK-5	Andere öffentliche Auftraggeber können diese Komponente nutzen. Sie ist im Idealfall eine Komponente des IT-Planungsrates.
AK-PR-6	Interoperabilität NFA-KO-2	Das Modul PR nutzt für die Annahme, die Fortschreibung des Laufzettels sowie für die interne Weiterleitung an das Modul AD die Interoperabilitätsstandards innerhalb des Standards XRechnung.

Tabelle 6.4: Abnahmekriterien zur Prüfung

6.5 Adressierung/Weiterleitung von elektronischen Rechnungen

Kriterium ID	Zugrunde liegende Anforderung	Abnahmekriterien
AK-AD-1	Pflege der Zieladressen FA-AD-1	Der Administrator des zentralen eRechnungseingangs kann eine Aktualisierung der Mappingtabelle vornehmen. Eine neue Auslieferung oder eine Neuinstallation des Systems ist nicht nötig. Nach der Aktualisierung berücksichtigt die Suche nach korrekten Adressen nur die aktuellen Datensätze.
AK-AD-2	Finden der korrekten Zieladresse FA-AD-2	Wird anhand der gelieferten Auftragskennnummer ein passender Eintrag gefunden, wird die technische Adresse des Zielsystems der jeweiligen Behörde zurückgeliefert. Wird kein passender Eintrag gefunden, wird ein eindeutiger Fehler mit einer Fehlerbeschreibung protokolliert und zurückgeliefert.

Kriterium ID	Zugrunde liegende Anforderung	Abnahmekriterien
AK-AD-3	Weiterleitung der elektronischen Rechnung an die korrekte Zieladresse FA-AD-3	Die elektronische Rechnung inklusive aller rechnungsbegründenden Unterlagen und des Prüfprotokolls wird digital an die Zielbehörde bzw. das zuständige elektronische System weitergeleitet. Tritt ein Übertragungsfehler auf, wird ein eindeutiger Fehler mit einer Fehlerbeschreibung protokolliert und zurückgeliefert.
AK-AD-4	Vertraulichkeit NFA-SI-1	Die Übertragung der Daten nach Verlassen der internen Zone erfolgt transportverschlüsselt.
AK-AD-5	Interoperabilität NFA-KO-2	Das Modul AD nutzt für die Annahme, die Fortschreibung des Laufzettels sowie für die Weiterleitung an das nachgelagerte Workflowsystem die Interoperabilitätsstandards innerhalb des Standards XRechnung.

Tabelle 6.5: Abnahmekriterien zur Adressierung/Weiterleitung

7 Prüfung vorhandener Module gegen Abnahmekriterien

Die im vorangegangenen Kapitel erhobenen Abnahmekriterien dienen nachfolgend für eine Bewertung der identifizierten Komponenten und der für eine Prüfung vorgesehenen Komponenten.

Die Bewertungstabellen haben dabei den folgenden Aufbau:

- **Kriterium ID**: eindeutige ID des Abnahmekriteriums
- **Zugrunde liegende Anforderung**: funktionale bzw. nicht-funktionale Anforderung, auf der das Abnahmekriterium basiert
- **Bemerkungen**: Erläuterungen zur Bewertung der Komponente
- **Standard-Funktionalität**:

Wert	Beschreibung
ja	Das Abnahmekriterium wird durch eine Standard-Funktionalität der Komponente realisiert.
nein	Das Abnahmekriterium wird nicht durch eine Standard-Funktionalität der Komponente realisiert.

Tabelle 7.1: Wert-Beschreibung zur Standard-Funktionalität

- **Grad der Erfüllung der Kriterien**:

Wert	Beschreibung
++	Die Kriterien werden vollumfänglich erfüllt.
+	Die Kriterien werden mit kleineren Einschränkungen erfüllt. Kleinere Anpassungen können zur vollumfänglichen Erfüllung führen.
0	Die Kriterien werden nicht erfüllt. Größere Anpassungen können zu einer Erfüllung führen.

Wert	Beschreibung
-	Die Kriterien werden nicht erfüllt. Nur über signifikante Anpassungen kann eine Erfüllung der Kriterien erreicht werden.
--	Die Kriterien werden nicht erfüllt. Selbst signifikante Anpassungen führen kaum zur Erfüllung der Kriterien.

Tabelle 7.2: Wert-Beschreibung zum Grad der Erfüllung der Kriterien

7.1 Prüfung der vorhandenen Komponenten des Bundes

Im Folgenden werden die Komponenten, die innerhalb der Bundesverwaltung identifiziert wurden, anhand der erhobenen Abnahmekriterien für die Authentifikation, die Weberfassung, die anzubietenden Übertragungskanäle, die Prüfung und die Adressierung/Weiterleitung von elektronischen Rechnungen geprüft. Außerdem wird eine Empfehlung für eine mögliche Nutzung der jeweiligen Komponente als Teil des zentralen eRechnungseingangs des Bundes gegeben.

Die nachfolgend genannten Komponenten werden geprüft:

- das Verwaltungsportal mit dem Servicekonto des Bundes für die Authentifikation und Registrierung von Rechnungssendern
- das Formular Management System (FMS) für die Weberfassung von elektronischen Rechnungen
- der WebSphere Process Server für die Adressierung/Weiterleitung von elektronischen Rechnungen

Für die Prüfung von elektronischen Rechnungen existiert aktuell keine Komponente zur Nachnutzung innerhalb der Bundesverwaltung.

7.1.1 Authentifikation anhand des Verwaltungsportals/Servicekontos des Bundes

Das Verwaltungsportal/Servicekonto des Bundes wird anhand der Abnahmekriterien zur Authentifikation auf eine Nutzung innerhalb des zentralen eRechnungseingangs des Bundes geprüft. Das Verwaltungsportal und das Servicekonto des Bundes werden aktuell im ITZBund konzipiert und anschließend implementiert. Die funktionalen Anforderungen wurden den Projektbeteiligten zur Verfügung gestellt. Die Prüfung und die Empfehlung basiert auf den zurückgelieferten Antworten. Technische Details waren während der Erstellung dieses Dokuments nicht verfügbar. Allgemeine Basisfunktionalitäten, wie z. B. die Durchführung der Registrierung, die Durchführung der Authentifizierung, eine Passwortwiederherstellung usw., werden als angebotene Standardfunktionalität angenommen.

7.1.1.a Prüfung anhand der Abnahmekriterien

Kriterium ID	Zugrunde liegende Anforderung	Bemerkungen	Standard-Funktionalität	Grad der Erfüllung der Kriterien
AK-AU-1	Mehrsprachigkeit FA-AU-1	Das Servicekonto soll langfristig einen mehrsprachigen Registrierungsprozess unterstützen. In der ersten Realisierung ist eine Umsetzung noch nicht zu erwarten.	nein	0
AK-AU-2	Erfassung von Registrierungsdaten FA-AU-2	Basisfunktionalitäten bei der eigenen Passwortvergabe (z. B. wiederholte identische Passworteingabe) durch den Rechnungssender werden unterstützt. Eine E-Mail mit einem Aktivierungslink wird vom Servicekonto verschickt.	ja	++
AK-AU-3	Aktivierung des Benutzerkontos FA-AU-3	Die erforderlichen Daten des Rechnungssenders werden vom Servicekonto überprüft. Die Aktivierung erfolgt über das Senden einer E-Mail mit einem Aktivierungslink.	ja	++
AK-AU-4	Anmeldung FA-AU-4	Das Servicekonto bietet die Registrierung und Authentifizierung für angeschlossene Portale und Dienste.	ja	++
AK-AU-5	Wiederherstellung des Passworts FA-AU-5	Standardfunktionalitäten zur Passwortwiederherstellung werden vom Servicekonto angeboten.	ja	++
AK-AU-6	Änderung von Stammdaten FA-AU-6	Nachträgliche Anpassungen von Stammdaten innerhalb des Servicekontos sind möglich.	ja	++

Kriterium ID	Zugrunde liegende Anforderung	Bemerkungen	Standard-Funktionalität	Grad der Erfüllung der Kriterien
AK-AU-7	Benutzerkonto löschen FA-AU-7	Das Entfernen eines Servicekontos ist möglich.	ja	++
AK-AU-8	Ändern/Freischalten von Übertragungskanälen FA-AU-8	Die Aktivierung und Deaktivierung von Übertragungskanälen ist im Servicekonto nicht vorgesehen. Dies kann innerhalb des FMS realisiert werden.	nein	--
AK-AU-9	Vertraulichkeit NFA-SI-1	Die Verbindung/Übertragung erfolgt transportverschlüsselt.	ja	++
AK-AU-10	Bedienbarkeit NFA-BU-2	Die Benutzeroberflächen entsprechen den ergonomischen Anforderungen der DIN EN ISO 9241 und der BildscharbV.	ja	++
AK-AU-11	Wiederverwendbarkeit NFA-WA-2	Die Wiederverwendbarkeit ist gegeben.	ja	++

Tabelle 7.3: Bewertung des Verwaltungsportals/Servicekontos

7.1.1.b Empfehlung zur Nutzung

Das Servicekonto erfüllt fast alle Abnahmekriterien zur Authentifikation. Zukünftig bzw. in nachfolgenden Ausbaustufen wird eine Mehrsprachigkeit angestrebt. Lediglich die Aktivierung und Deaktivierung von Übertragungskanälen ist nicht vorgesehen. Diese Funktionalität kann aber innerhalb des FMS realisiert werden. Allerdings ist die rechtzeitige Fertigstellung des Servicekontos nicht gewährleistet und stellt damit ein Risiko dar. Alternativ könnte die Komponente Governikus Autent genutzt werden.

Es wird empfohlen, bei rechtzeitiger Fertigstellung das Servicekonto des Bundes als Authentifizierungs-/ Registrierungskomponente im zentralen eRechnungseingang des Bundes zu nutzen. Bei nicht rechtzeitiger Bereitstellung könnte alternativ die Komponente Governikus Autent eingesetzt werden.

7.1.2 Weberfassung über das Formular Management System

Das Formular Management System (FMS) des Bundes wird anhand der Abnahmekriterien zur Weberfassung auf eine Nutzung innerhalb des zentralen eRechnungseingangs des Bundes geprüft. Die erhobenen Abnahmekriterien werden dabei mit der angebotenen Funktionalität verglichen und eine Empfehlung ausgesprochen.

7.1.2.a Prüfung anhand der Abnahmekriterien

Kriterium ID	Zugrunde liegende Anforderung	Bemerkungen	Standard-Funktionalität	Grad der Erfüllung der Kriterien
AK-WF-1	Manuelle Erfassung einer Rechnung FA-WF-1	Das FMS kann Formulare für eine manuelle Erfassung von Rechnungen bereitstellen. Rechnungsbegründende Unterlagen können hochgeladen werden. Die Anzahl, Größe und Art der Anlagen ist konfigurierbar. Das aus der erfassten Rechnung resultierende strukturierte Datenformat kann vom Nutzer als Originalrechnung lokal gespeichert werden. Eine Bestätigung der Einlieferung ist mit einem digitalen Eingangsstempel (mit Datum) versehen und kann vom Rechnungssender über seinen Browser ausgedruckt werden.	ja	++
AK-WF-2	Speichern eines Zwischenstands einer Rechnung FA-WF-2	Die Formularbearbeitung kann vom Rechnungssender jederzeit unterbrochen werden. Das FMS bietet die Möglichkeit, den Zwischenstand lokal zu speichern.	ja	++

Kriterium ID	Zugrunde liegende Anforderung	Bemerkungen	Standard-Funktionalität	Grad der Erfüllung der Kriterien
AK-WF-3	Hochladen eines Zwischenstands einer Rechnung FA-WF-3	Ein Rechnungssender kann seinen zuvor lokal gespeicherten Zwischenstand einer erfassten Rechnung jederzeit wieder hochladen und die Erfassung fortsetzen.	ja	++
AK-WF-4	Upload einer Rechnung FA-WF-4	Über einen sogenannten Datei-Upload kann eine bereits in einem strukturierten Datenformat (XRechnung oder ein CEN-konformes Format) vorliegende Rechnung hochgeladen und anhand eines Schemas validiert werden.	ja	++
AK-WF-5	Einsehen von Statusinformationen zu eingelieferten elektronischen Rechnungen FA-WF-5	Das FMS kann Statusinformationen eines Rechnungssenders anzeigen. Hierfür ist eine Erweiterung des FMS notwendig. Die Statusinformationen (mit Fehlermeldungen) werden entweder in der lokalen Datenbank des FMS gespeichert und geladen oder können dynamisch von einem Dienst abgerufen werden, der die Daten bereitstellt.	nein	+
AK-WF-6	Einsehen der Nutzungsbedingungen FA-WF-6	Das FMS kann dem Rechnungssender die Nutzungsbedingungen visuell präsentieren.	ja	++
AK-WF-7	Bedienbarkeit NFA-BU-2	Das FMS orientiert sich an den ergonomischen Anforderungen.	ja	++
AK-WF-8	Vertraulichkeit NFA-SI-1	Die Übertragung der Daten an das FMS kann transportverschlüsselt erfolgen.	ja	++

Kriterium ID	Zugrunde liegende Anforderung	Bemerkungen	Standard-Funktionalität	Grad der Erfüllung der Kriterien
AK-WF-9	Interoperabilität NFA-KO-2	Die geforderte Interoperabilität kann über eine Anpassung des FMS erreicht werden.	nein	0

Tabelle 7.4: Bewertung des FMS

7.1.2.b Empfehlung zur Nutzung

Das FMS erfüllt alle erhobenen Anforderungen an eine Weberfassung des zentralen eRechnungseingangs. Bis auf ein Kriterium gehören alle anderen zu den angebotenen Standardfunktionalitäten des FMS. Für die Anzeige von Statusinformationen und Fehlermeldungen ist eine Erweiterung des FMS nötig. Aufgrund der technologischen Plattform des FMS ist diese Erweiterung technisch nicht hochkomplex und kann durchgeführt werden. Daher wird eine Empfehlung zur Nutzung des FMS für die Weberfassung ausgesprochen.

7.1.3 Übertragungskanäle – Bereitstellung durch den Governikus MultiMessenger

Der Governikus MultiMessenger wird anhand der Abnahmekriterien zu den Übertragungskanälen auf eine Nutzung innerhalb des zentralen eRechnungseingangs des Bundes geprüft. Die erhobenen Abnahmekriterien werden dabei mit der angebotenen Funktionalität verglichen und eine Empfehlung ausgesprochen.

7.1.3.a Prüfung anhand der Abnahmekriterien

Kriterium ID	Zugrunde liegende Anforderung	Bemerkungen	Standard-Funktionalität	Grad der Erfüllung der Kriterien
AK-ÜK-1	Übertragung mittels Webservice FA-ÜK-1	Elektronische Rechnungen können beim Governikus MultiMessenger über einen Webservice eingeliefert werden.	ja	+

Kriterium ID	Zugrunde liegende Anforderung	Bemerkungen	Standard-Funktionalität	Grad der Erfüllung der Kriterien
		Bei der Übergabe an das nachfolgende Modul Prüfung kann der Eingangskanal als Teil des elektronischen Laufzettels mitgeliefert und dort ausgewertet werden. Dadurch kann ein Status mit dem konkreten Eingangskanal im Portal gespeichert werden.		
AK-ÜK-2	Übertragung mittels De-Mail FA-ÜK-2	Elektronische Rechnungen können beim Governikus MultiMessenger über De-Mail eingeliefert werden. Bei der Übergabe an das nachfolgende Modul Prüfung kann der Eingangskanal als Teil des elektronischen Laufzettels mitgeliefert und dort ausgewertet werden. Dadurch kann ein Status mit dem konkreten Eingangskanal im Portal gespeichert werden.	ja	+
AK-ÜK-3	Übertragung mittels E-Mail FA-ÜK-3	Elektronische Rechnungen können beim Governikus MultiMessenger über E-Mail eingeliefert werden. Bei der Übergabe an das nachfolgende Modul Prüfung kann der Eingangskanal als Teil des elektronischen Laufzettels mitgeliefert und dort ausgewertet werden. Dadurch kann ein Status mit dem konkreten Eingangskanal im Portal gespeichert werden.	ja	+
AK-ÜK-4	Vertraulichkeit NFA-SI-1	Die Übertragung der Daten erfolgt transportverschlüsselt.	ja	++
AK-ÜK-5	Interoperabilität NFA-KO-2	Das Modul ÜK nutzt für die Annahme, den Laufzettel sowie für die interne Weiterleitung an das Modul PR die Interoperabilitätsstandards innerhalb des Standards XRechnung.	ja	++

Kriterium ID	Zugrunde liegende Anforderung	Bemerkungen	Standard-Funktionalität	Grad der Erfüllung der Kriterien
AK-ÜK-6	Wiederverwendbarkeit NFA-WA-2	Andere öffentliche Auftraggeber können diese Komponente nutzen. Sie ist im Idealfall eine Komponente des IT-Planungsrates.	ja	+

Tabelle 7.5: Bewertung des Governikus MultiMessengers

7.1.3.b Empfehlung zur Nutzung

Der Governikus MultiMessenger erfüllt alle Abnahmekriterien für eine Nutzung innerhalb des zentralen eRechnungseingangs des Bundes. Die Speicherung von Statusinformationen (mit Angabe des Eingangskanals) ist keine Standardfunktionalität des MultiMessengers. Der elektronische Laufzettel, der vom MultiMessenger zu jeder eingegangenen und weitergeleiteten Nachricht erstellt und mitgeliefert wird, enthält allerdings alle notwendigen Informationen (vgl. Benutzerdokumentation für Fachadministratoren Governikus MultiMessenger Release 3, 2016 S. 38). Das Speichern des Status kann von einer nachfolgenden (z. B. für die Prüfung einer elektronischen Rechnung) oder übergeordneten Komponente (z. B. einer Komponente, die alle Komponenten orchestriert) übernommen werden.

Zur Bereitstellung von unterschiedlichen Übertragungskanälen innerhalb des zentralen eRechnungseingangs des Bundes wird die Nutzung des Governikus MultiMessengers empfohlen.

7.1.4 Prüfung von elektronischen Rechnungen – keine Komponente vorhanden

Zum aktuellen Zeitpunkt existiert keine Komponente, die gegen die Abnahmekriterien zur Prüfung von elektronischen Rechnungen geprüft werden kann. Das Land Bremen hat im Verlauf der kooperativen Erstellung dieses Dokuments angeboten, eine Komponente mit den erhobenen Anforderungen zu entwickeln und diese in den IT-Planungsrat einzugeben. Eine Nutzung dieser Komponente innerhalb der Bundesverwaltung wäre damit sichergestellt.

7.1.4.a Prüfung anhand der Abnahmekriterien

Eine Prüfung entfällt, da zum aktuellen Zeitpunkt keine Komponente für eine Nachnutzung vorhanden ist.

7.1.4.b Empfehlung zur Nutzung

Es wird empfohlen, vom Land Bremen eine Komponente zur Prüfung von elektronischen Rechnungen entwickeln zu lassen und diese nach der Einbringung in den IT-Planungsrat als Teil des zentralen eRechnungseingangs des Bundes nachzunutzen.

7.1.5 Adressierung/Weiterleitung von elektronischen Rechnungen durch den WebSphere Process Server

Der WebSphere Process Server wird anhand der Abnahmekriterien zu den Übertragungskanälen auf eine Nutzung innerhalb des zentralen eRechnungseingangs des Bundes geprüft. Die erhobenen Abnahmekriterien werden dabei mit der angebotenen Funktionalität verglichen und eine Empfehlung ausgesprochen.

7.1.5.a Prüfung anhand der Abnahmekriterien

Kriterium ID	Zugrunde liegende Anforderung	Abnahmekriterien	Standard-Funktionalität	Grad der Erfüllung der Kriterien
AK-AD-1	Pflege der Zieladressen FA-AD-1	Die Pflege der korrekten Zieladressen ist möglich. Die jeweils aktuellen Adressen werden ohne eine erneute Installation oder einen Neustart des Systems übernommen.	neutral (Definition des korrekten Prozesse über BPMN)	+
AK-AD-2	Finden der korrekten Zieladresse FA-AD-2	Der Process Server kann anhand eines eindeutigen Kriteriums eine Weiterleitungsadresse ermitteln. Wird kein passender Eintrag gefunden, kann ein eindeutiger Fehler mit einer Fehlerbeschreibung protokolliert und z. B. an ein Portal zurückgeliefert werden.	neutral (Definition des korrekten Prozesses über BPMN)	+
AK-AD-3	Weiterleitung der elektronischen Rechnung an die korrekte Zieladresse FA-AD-3	Der Process Server kann anhand eines eindeutigen Kriteriums die elektronische Rechnung an beliebige Systeme weiterleiten. Eine Protokollierung und der Aufruf eines Systems zur Speicherung von Status- und Fehlerinformationen (hier das Portal) sind möglich.	neutral (Definition des korrekten Prozesses über BPMN)	+
AK-AD-4	Vertraulichkeit NFA-SI-1	Die Übertragung der Daten erfolgt transportverschlüsselt.	ja	++

Kriterium ID	Zugrunde liegende Anforderung	Abnahmekriterien	Standard-Funktionalität	Grad der Erfüllung der Kriterien
AK-AD-5	Interoperabilität NFA-KO-2	Die geforderte Interoperabilität kann über eine Anpassung erreicht werden.	nein	0

Tabelle 7.6: Bewertung des WebSphere Process Servers

7.1.5.b Empfehlung zur Nutzung

Der WebSphere Process Server erfüllt alle Anforderungen für die Adressierung/Weiterleitungen von elektronischen Rechnungen. Die Definition der korrekten Prozessabläufe kann über BPMN definiert werden. Eine Nutzung zur übergeordneten Orchestrierung der einzelnen Komponenten ist ebenso möglich, da diese zu seiner Kernfunktionalität zählt. Auch wenn das kein ausdrückliches Abnahmekriterium darstellt, kann es bei der konkreten Umsetzung bedacht werden. Im ITZBund existiert bereits ein umfassendes Wissen zur Erstellung und Adaption von Prozessabläufen innerhalb des Process Servers.

Die Nutzung des WebSphere Process Servers zur Adressierung/Weiterleitung von elektronischen Rechnungen als Teil des zentralen eRechnungseingangs des Bundes wird empfohlen.

7.2 Prüfung der vorhandenen Komponenten des Landes Bremen

7.2.1 Authentifikation anhand des Governikus Autent

Die Komponente Governikus Autent wird anhand der Abnahmekriterien zur Authentifikation auf eine Nutzung innerhalb des zentralen eRechnungseingangs der Freien Hansestadt Bremen geprüft. Der Governikus Autent wird aktuell im Rechenzentrum des Bremer IT-Dienstleisters Dataport betrieben. Die funktionalen Anforderungen wurden den Projektbeteiligten zur Verfügung gestellt. Die Prüfung und die Empfehlung basiert auf den zurückgelieferten Antworten.

7.2.1.a Prüfung anhand der Abnahmekriterien

Kriterium ID	Zugrunde liegende Anforderung	Bemerkungen	Standard-Funktionalität	Grad der Erfüllung der Kriterien
AK-AU-1	Mehrsprachigkeit FA-AU-1	Der Governikus Autent unterstützt einen mehrsprachigen Registrierungsprozess.	ja	++
AK-AU-2	Erfassung von Registrierungsdaten FA-AU-2	Basisfunktionalitäten bei der eigenen Passwortvergabe (z. B. wiederholte identische Passworteingabe) durch den Rechnungssender werden unterstützt. Eine E-Mail mit einem Aktivierungslink wird vom Servicekonto verschickt.	ja	++
AK-AU-3	Aktivierung des Benutzerkontos FA-AU-3	Die erforderlichen Daten des Rechnungssenders werden vom Governikus Autent überprüft. Die Aktivierung erfolgt über das Senden einer E-Mail mit einem Aktivierungslink.	ja	++
AK-AU-4	Anmeldung FA-AU-4	Der Governikus Autent bietet die Registrierung und Authentifizierung für angeschlossene Portale und Dienste.	ja	++
AK-AU-5	Wiederherstellung des Passworts FA-AU-5	Standardfunktionalitäten zur Passwortwiederherstellung werden vom Governikus Autent angeboten.	ja	++
AK-AU-6	Änderung von Stammdaten FA-AU-6	Nachträgliche Anpassungen von Stammdaten innerhalb des Governikus Autent sind möglich.	ja	++

Kriterium ID	Zugrunde liegende Anforderung	Bemerkungen	Standard-Funktionalität	Grad der Erfüllung der Kriterien
AK-AU-7	Benutzerkonto löschen FA-AU-7	Das Entfernen eines Kontos im Governikus Autent ist möglich.	ja	++
AK-AU-8	Ändern/Freischalten von Übertragungskanälen FA-AU-8	Die Aktivierung und Deaktivierung von Übertragungskanälen ist im Governikus Autent nicht vorgesehen. Dies kann innerhalb des FMS realisiert werden.	nein	+
AK-AU-9	Vertraulichkeit NFA-SI-1	Die Übertragung der Daten erfolgt transportverschlüsselt.	ja	++
AK-AU-10	Bedienbarkeit NFA-BU-2	Die Benutzeroberflächen entsprechen den ergonomischen Anforderungen der DIN EN ISO 9241 und der BildscharbV.	ja	+
AK-AU-11	Wiederverwendbarkeit NFA-WA-2	Andere öffentliche Auftraggeber können diese Komponente nutzen. Sie ist im Idealfall eine Komponente des IT-Planungsrates.	ja	++

Tabelle 7.7: Bewertung des Governikus Autent

7.2.1.b Empfehlung zur Nutzung

Der Governikus Autent erfüllt fast alle Abnahmekriterien zur Authentifikation. Lediglich die Aktivierung und Deaktivierung von Übertragungskanälen und weiteren verfahrensspezifischen Daten ist noch nicht im Autent implementiert.

Es wird empfohlen, die Komponente Governikus Autent einzusetzen. Es sind keine Alternativen vorgesehen.

7.2.2 Übertragungskanäle – Bereitstellung durch den Governikus MultiMessenger

Der Governikus MultiMessenger wird anhand der Abnahmekriterien zu den Übertragungskanälen auf eine Nutzung innerhalb des zentralen eRechnungseingangs des Landes Bremen geprüft. Die erhobenen Abnahmekriterien werden dabei mit der angebotenen Funktionalität verglichen und eine Empfehlung ausgesprochen.

7.2.2.a Prüfung anhand der Abnahmekriterien

Kriterium ID	Zugrunde liegende Anforderung	Bemerkungen	Standard-Funktionalität	Grad der Erfüllung der Kriterien
AK-ÜK-1	Übertragung mittels Webservice FA-ÜK-1	Elektronische Rechnungen können beim Governikus MultiMessenger über einen Webservice eingeliefert werden. Bei der Übergabe an das nachfolgende Modul Prüfung kann der Eingangskanal als Teil des elektronischen Laufzettels mitgeliefert und dort ausgewertet werden. Dadurch kann ein Status mit dem konkreten Eingangskanal im Portal gespeichert werden.	ja	+
AK-ÜK-2	Übertragung mittels De-Mail FA-ÜK-2	Elektronische Rechnungen können beim Governikus MultiMessenger über De-Mail eingeliefert werden. Bei der Übergabe an das nachfolgende Modul Prüfung kann der Eingangskanal als Teil des elektronischen Laufzettels mitgeliefert und dort ausgewertet werden. Dadurch kann ein Status mit dem konkreten Eingangskanal im Portal gespeichert werden.	ja	++
AK-ÜK-3	Übertragung mittels E-Mail FA-ÜK-3	Elektronische Rechnungen können beim Governikus MultiMessenger über E-Mail eingeliefert werden. Bei der Übergabe an das nachfolgende Modul Prüfung kann der Eingangskanal als Teil des elektronischen Laufzettels mitgeliefert und dort ausgewertet werden. Dadurch kann	ja	++

Kriterium ID	Zugrunde liegende Anforderung	Bemerkungen	Standard-Funktionalität	Grad der Erfüllung der Kriterien
		ein Status mit dem konkreten Eingangskanal im Portal gespeichert werden.		
AK-ÜK-4	Vertraulichkeit NFA-SI-1	Die Übertragung der Daten erfolgt transportverschlüsselt.	ja	++
AK-ÜK-5	Interoperabilität NFA-KO-2	Das Modul ÜK nutzt für die Annahme, den Laufzettel sowie für die interne Weiterleitung an das Modul PR die Interoperabilitätsstandards innerhalb des Standards XRechnung.	ja	++
AK-ÜK-6	Wiederverwendbarkeit NFA-WA-2	Andere öffentliche Auftraggeber können diese Komponente nutzen. Sie ist im Idealfall eine Komponente des IT-Planungsrates.	ja	+

Tabelle 7.8: Bewertung des Governikus MultiMessengers

7.2.2.b Empfehlung zur Nutzung

Der Governikus MultiMessenger erfüllt alle Abnahmekriterien für eine Nutzung innerhalb des zentralen eRechnungseingangs des Landes Bremen. Die Speicherung von Statusinformationen (mit Angabe des Eingangskanals) ist keine Standardfunktionalität des MultiMessengers. Der elektronische Laufzettel, der vom MultiMessenger zu jeder eingegangenen und weitergeleiteten Nachricht erstellt und mitgeliefert wird, enthält allerdings alle notwendigen Informationen (vgl. Benutzerdokumentation für Fachadministratoren Governikus MultiMessenger Release 3, 2016 S. 38). Das Speichern des Status kann von einer nachfolgenden (z. B. für die Prüfung einer elektronischen Rechnung) oder übergeordneten Komponente (z. B. einer Komponente, die alle Komponenten orchestriert) übernommen werden.

Zur Bereitstellung von unterschiedlichen Übertragungskanälen innerhalb des zentralen eRechnungseingangs des Landes Bremen wird die Nutzung des Governikus MultiMessengers empfohlen.

7.2.3 Weberfassung über das Content Managementsystem KoGIs

Das Baukastensystem KoGIs der Freien Hansestadt Bremen wird anhand der Abnahmekriterien zur Weberfassung auf eine Nutzung innerhalb des zentralen eRechnungseingangs des Landes Bremen geprüft. Die erhobenen Abnahmekriterien werden dabei mit der angebotenen Funktionalität verglichen und eine Empfehlung ausgesprochen.

7.2.3.a Prüfung anhand der Abnahmekriterien

Kriterium ID	Zugrunde liegende Anforderung	Bemerkungen	Standard-Funktionalität	Grad der Erfüllung der Kriterien
AK-WF-1	Manuelle Erfassung einer Rechnung FA-WF-1	Mit Hilfe von KoGIS können Formulare für eine manuelle Erfassung von Rechnungen definiert und bereitgestellt werden. Eine Funktionalität, um rechnungsbegründende Unterlagen hochzuladen, kann geschaffen werden. Eine Funktionalität, um dem Nutzer das aus der erfassten Rechnung resultierende strukturierte Datenformat als Originalrechnung zum lokalen Speichern zur Verfügung zu stellen, kann programmiert werden. Eine Weiterleitung aus dem KoGIs heraus in ein weiterverarbeitendes Modul ist in KoGIs nicht vorgesehen. Eine entsprechende API existiert nicht.	nein	-
AK-WF-2	Speichern eines Zwischenstands einer Rechnung FA-WF-2	Eine Funktionalität zur Zwischenspeicherung der aktuellen Formularbearbeitung durch den Rechnungssender kann implementiert werden.	nein	0
AK-WF-3	Hochladen eines Zwischenstands einer Rechnung	Eine Erweiterung des KoGIs zum Hochladen eines lokal gespeicherten Zwischenstands zwecks Erfassungsfortsetzung kann geschaffen werden.	nein	0

Kriterium ID	Zugrunde liegende Anforderung	Bemerkungen	Standard-Funktionalität	Grad der Erfüllung der Kriterien
	FA-WF-3			
AK-WF-4	Upload einer Rechnung FA-WF-4	Eine Funktionalität, mit der über einen sogenannten Datei-Upload eine bereits in einem strukturierten Datenformat (XRechnung oder ein CEN-konformes Format) vorliegende Rechnung hochgeladen und anhand eines Schemas validiert werden kann, ist realisierbar. Eine Weiterleitung aus dem KoGIs heraus in ein weiterverarbeitendes Modul ist in KoGIs nicht vorgesehen. Eine entsprechende API existiert nicht.	nein	-
AK-WF-5	Einsehen von Statusinformationen zu eingelieferten elektronischen Rechnungen FA-WF-5	Das KoGIs ist nicht geeignet, Statusinformationen eines Rechnungssenders anzuzeigen. Hierfür wäre eine Erweiterung des KoGIs notwendig, für die derzeit keine offene API existiert.	nein	-
AK-WF-6	Einsehen der Nutzungsbedingungen FA-WF-6	Mit Hilfe des KoGIS kann eine Funktionalität zur Verfügung gestellt werden, mit der dem Rechnungssender die Nutzungsbedingungen visuell präsentiert werden.	ja	+
AK-WF-7	Bedienbarkeit NFA-BU-2	Die Benutzeroberflächen entsprechen den ergonomischen Anforderungen der DIN EN ISO 9241 und der BildscharbV.	ja	++
AK-WF-8	Vertraulichkeit	Die Übertragung der Daten erfolgt transportverschlüsselt.	ja	++

Kriterium ID	Zugrunde liegende Anforderung	Bemerkungen	Standard-Funktionalität	Grad der Erfüllung der Kriterien
	NFA-SI-1			
AK-WF-9	Interoperabilität NFA-KO-2	Die Weberfassungskomponente nutzt für die Annahme/Erfassung sowie für die interne Weiterleitung an Modul ÜK die Interoperabilitätsstandards innerhalb des Standards XRechnung.	ja	-

Tabelle 7.9: Bewertung des KoGIs

7.2.3.b Empfehlung zur Nutzung

Das KoGIS erfüllt die erhobenen Anforderungen nur in geringem Maße. Vorhandene Funktionalitäten können aus dem KoGIS-System nicht außerhalb des Systems für weitere Anwendungen bereitgestellt werden und die Schaffung von Schnittstellen zu weiterverarbeitenden Systemen wie dem GMM sind nicht vorgesehen. Daher kann keine Empfehlung zur Nutzung des KoGIS für die Weberfassung ausgesprochen werden.

7.2.4 Prüfung von elektronischen Rechnungen – keine Komponente vorhanden

Zum aktuellen Zeitpunkt existiert keine Komponente, die gegen die Abnahmekriterien zur Prüfung von elektronischen Rechnungen geprüft werden kann. Das Land Bremen hat im Verlauf der kooperativen Erstellung dieses Dokuments angeboten, eine Komponente mit den erhobenen Anforderungen zu entwickeln und diese in den IT-Planungsrat einzugeben. Eine Nutzung dieser Komponente innerhalb der Verwaltung wäre damit sichergestellt.

7.2.4.a Prüfung anhand der Abnahmekriterien

Eine Prüfung entfällt, da zum aktuellen Zeitpunkt keine Komponente für eine Nachnutzung vorhanden ist.

7.2.4.b Empfehlung zur Nutzung

Es wird empfohlen, vom Land Bremen eine Komponente zur Prüfung von elektronischen Rechnungen entwickeln zu lassen und diese nach der Einbringung in den IT-Planungsrat als Teil des zentralen eRechnungseingangs zu nutzen.

7.2.5 Adressierung/Weiterleitung von elektronischen Rechnungen – keine Komponente vorhanden

Zum gegenwärtigen Zeitpunkt kann noch keine vorhandene Komponente identifiziert werden, die gegen die Abnahmekriterien geprüft werden kann. Eine Eigenentwicklung scheint aber entbehrlich, da die notwendigen Funktionalitäten durchaus durch am Markt verfügbare Produkte abgedeckt werden. Der Suchradius nach einer geeigneten Komponente wird daher nochmal vergrößert. Ähnlich wie bei der Bundesverwaltung wäre die Verwendung als Orchestrierungskomponente sinnvoll, solange der Governikus MultiMessanger die Orchestrierung als zentrale Komponente noch nicht übernehmen kann.

7.2.5.a Prüfung anhand der Abnahmekriterien

Eine Prüfung entfällt, da zum aktuellen Zeitpunkt keine Komponente für eine Nachnutzung vorhanden ist.

7.2.5.b Empfehlung zur Nutzung

Da noch keine Komponente identifiziert werden konnte, kann keine Empfehlung ausgesprochen werden.

8 Empfohlenes Architekturmodell zur Umsetzung

Der wesentliche Erfolgsfaktor bei der Implementierung des zentralen eRechnungseingangs ist die termingerechte Umsetzung. Deshalb wurden Komponenten des IT-Planungsrates sowie bereits in der Verwaltung eingesetzte Komponenten, die für eine Weiterverwendung beim eRechnungseingang in Frage kommen, anhand von Basisfunktionalitäten identifiziert. Die Konzeption von SOLL-Prozessen, welche den Empfang, die Prüfung und die Weiterleitung von elektronischen Rechnungen (nach dem jeweils gültigen Standard XRechnung) abbilden, führte zur Erhebung von funktionalen und nicht-funktionalen Anforderungen. Diese Anforderungen dienten in Form von Abnahmekriterien zur Prüfung der identifizierten technischen Komponenten.

Die mit einem positiven Ergebnis geprüften Komponenten fließen nunmehr in die konkrete technische Ausgestaltung des zentralen eRechnungseingangs ein. Sie bilden jeweils eine technische Implementierung der produktneutralen fachlichen Module Weberfassung, Übertragungskanäle, Authentifizierung, Prüfung, Adressierung/Weiterleitung ab und gestalten damit wesentlich das in diesem Kapitel beschriebene Architekturmodell.

Die empfohlene Lösung baut – soweit möglich – stringent auf bereits bekannte, beschaffte und genutzte Produkte auf und kann über deren Erweiterungen und Konfigurationen umgesetzt werden. Eigenentwicklungen sind lediglich für die Module erforderlich, für die keine konkrete technische Realisierung gefunden werden konnte.

8.1 Architekturmodell des Bundes zur eRechnung

Das konkrete Architekturmodell des Bundes zur eRechnung ist durch die Verwendung des Formular Management Systems für die Bereitstellung der Funktionalität des Moduls Weberfassung/Upload, des Governikus MultiMessengers für das Modul Übertragungskanäle, des Servicekontos des Bundes für die Authentifizierung und des WebSphere Process Servers für das Modul Adressierung/Weiterleitung gekennzeichnet. Als Rahmen bzw. ersten Anlaufpunkt für den Rechnungssender dient das Verwaltungsportal des Bundes.

Lediglich für den Fall, dass sich das Servicekonto nicht in die Zeitplanung des hiesigen Projekts integrieren ließe, kann sekundär auch der Governikus Autent die Funktionalität des Moduls Authentifizierung bereitstellen.

Die Funktionalität des Moduls Prüfung (einer eRechnung) kann nur über eine Eigenentwicklung realisiert bzw. eine vom IT-Planungsrat möglicherweise bereitgestellte Komponente nachgenutzt werden.

Die folgende Abbildung ordnet die eingesetzten Produkte/Komponenten in die Module des zentralen eRechnungseingangs ein.

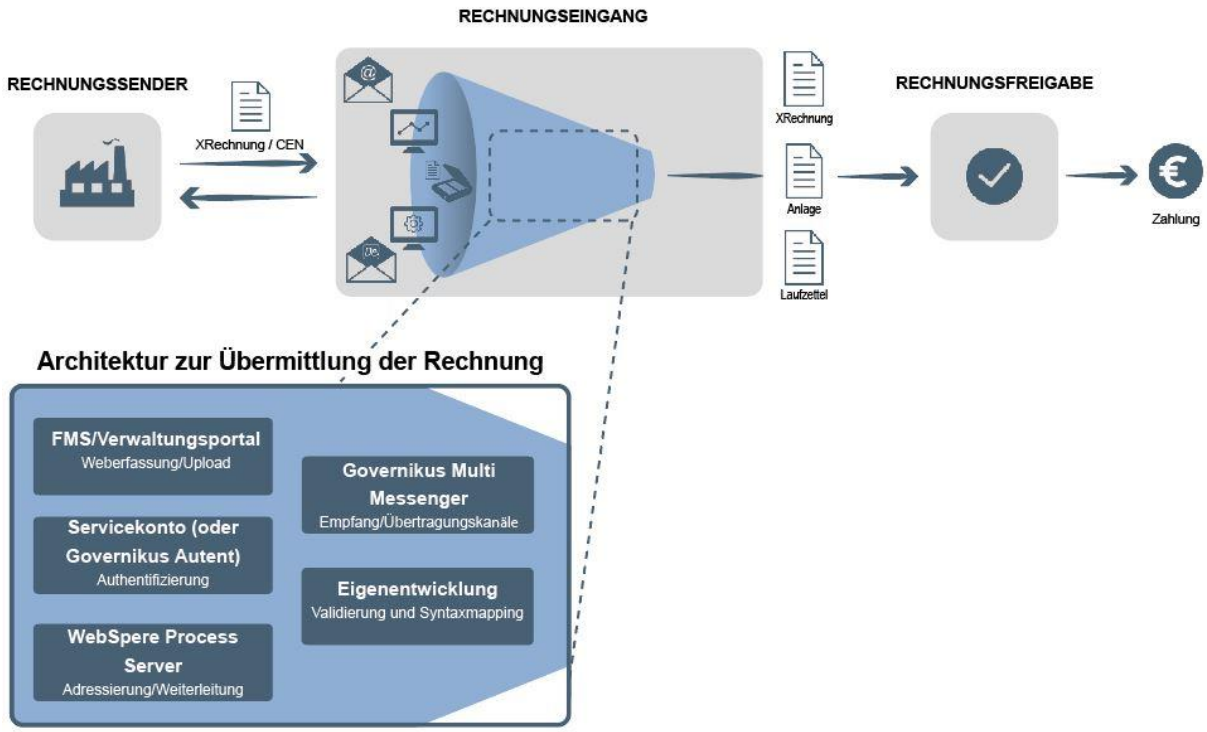

Abbildung 8.1: Architektur mit konkreten Komponenten (Bund)

8.1.1 Systembeschreibung

Der zentrale eRechnungseingang des Bundes wird an das Verwaltungsportal und das Servicekonto des Bundes angeschlossen. Er nutzt das Servicekonto für die Durchführung einer einheitlichen Registrierung der Rechnungssender und für die Authentifizierung basierend auf dem Standard SAML.

Die Kommunikation der Komponenten innerhalb des zentralen Rechnungseingangs wird über die Orchestrierung der einzelnen Komponenten durch den WebSphere Process Server erreicht. Dieser kann als zentrale Orchestrierungsstelle alle Protokollierungsfunktionen der Status und signalisierten Fehler innerhalb des Systems realisieren. Diese Fehler- und Statusinformationen können vom FMS eingebunden und visualisiert werden.

Für die Kommunikation mit den externen Rechnungsfreigabesystemen wird ein externer Datenaustausch vorgesehen.

Die folgende Abbildung skizziert den zentralen eRechnungseingang mit der Einordnung unterhalb des Verwaltungsportals und dem externen Datenaustausch mit den verschiedenen Rechnungsfreigabesystemen der angeschlossenen Verwaltung.

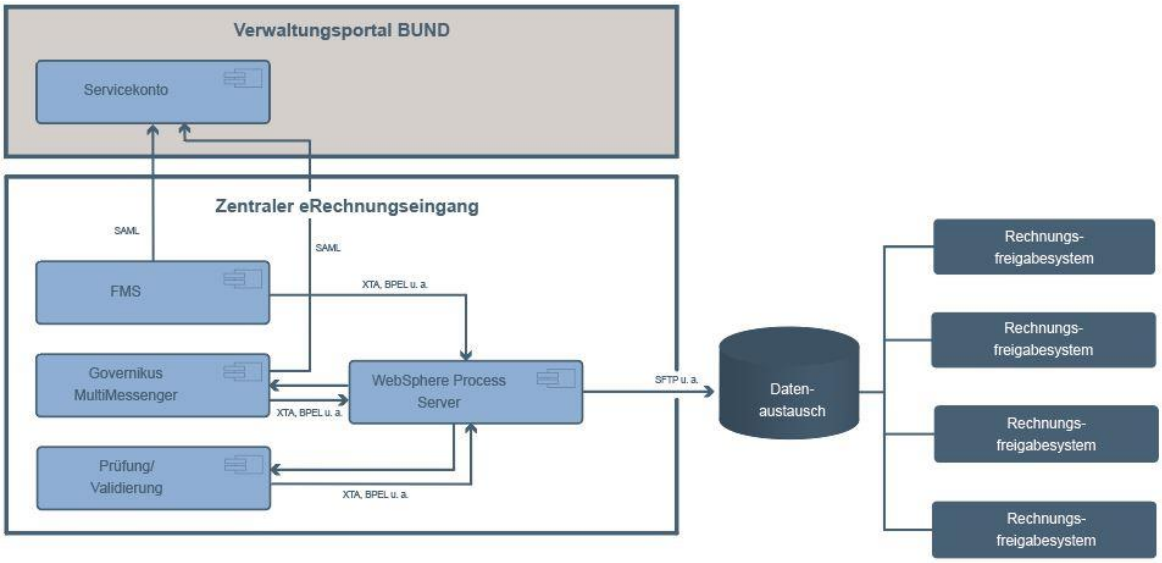

Abbildung 8.2: Abbildung des Gesamtsystems (Bund)

8.1.2 Herausforderungen bei der Realisierung

Die folgende Tabelle fasst die wesentlichen Herausforderungen bei der Realisierung des zentralen eRechnungseingangs anhand der eingesetzten Produkte zusammen. Diese liegen sowohl in der Realisierung der Kommunikation der Komponenten untereinander als auch in der Konfiguration, Anpassung/Erweiterung der bereits angebotenen Funktionalitäten. Da für das Modul Prüfung keine bereits vorhandene Komponente eingesetzt werden kann, ist hierfür eine vollständige Neuentwicklung vorzusehen.

Modul	Produkt	Umzusetzende Funktionalität
Weberfassung/Upload	Formular Management System, Verwaltungsportal des Bundes als Rahmen	Bereitstellung der Formulare Realisierung der Statusanzeige Anbindung an das Servicekonto
Übertragungskanäle	Governikus MultiMessenger	Bereitstellung der verschiedenen Kanäle

Modul	Produkt	Umzusetzende Funktionalität
Authentifizierung	Servicekonto des Bundes, (Governikus Autent als mögliche Übergangslösung)	Anbindung des FMS und des Governikus MultiMessengers Generierung von Whitelists
Prüfung	n. v. – Eigenentwicklung bzw. über den IT-Planungsrat, sofern über diesen bereitgestellt	Realisierung der Prüfung von XRechnungen
Adressierung/Weiterleitung	WebSphere Process Server	Mapping der Auftragskennung auf die jeweilige technische Adresse des rechnungsempfangenden Freigabesystems Zusammenstecken bzw. Orchestrierung der einzelnen Komponenten Realisierung der Status- und Fehlerprotokollierung für den Rechnungssender Übergabe der XRechnung an die jeweiligen Freigabesysteme

Tabelle 8.1: Herausforderungen der Realisierung

8.1.3 Hinweise und Empfehlungen zur Realisierung

Nachfolgend werden Hinweise und/oder Empfehlungen für die Realisierung der geforderten Funktionalität gegeben. Abschließend wird zu jeder umzusetzenden Funktionalität tabellarisch eine Einordnung der Komplexität der Umsetzung vorgenommen. Diese kann bei der Planung der späteren Umsetzung genutzt werden. Die folgenden Einordnungen wurden dabei gewählt:

- Konfiguration: Die Realisierung kann durch die Konfiguration der Komponente erreicht werden.
- Erweiterung: Die vorhandene Funktionalität muss erweitert werden.
- Neuentwicklung: Die Funktionalität kann nur durch eine komplette Neuentwicklung erreicht werden.

8.1.3.a Bereitstellung der Formulare (Weberfassung/Upload)

Die Bereitstellung von unterschiedlichen Formularen ist eine der Kernfunktionalitäten des FMS. Die Realisierung der konkreten Formulare, die eine einfache und fehlerresistente Erfassung von XRechnungen ermöglichen, muss einmalig erbracht werden. Sobald der Standard XRechnung finalisiert wird, können die Formulare umgesetzt werden.

Einordnung der Komplexität:

Produkt	Umzusetzende Funktionalität	Einordnung der Komplexität	Bemerkungen
FMS	Bereitstellung der Formulare	Konfiguration/ Erweiterung	Die Formulare müssen auf Grundlage des jeweils gültigen Standards XRechnung erstellt werden. Die Validierungen der Eingabefelder werden über eine Konfiguration erreicht.

Tabelle 8.2: Bereitstellung der Formulare

8.1.3.b Realisierung der Statusanzeige (Weberfassung/Upload)

Der WebSphere Process Server persistiert als Teil der Orchestrierung der einzelnen Komponenten den Status einer Rechnung und die möglichen Fehler beim Aufruf der Komponenten bzw. bei der Prüfung einer XRechnung (vgl. 8.1.3.j). Die Status werden nicht in das DB-Schema der eigenen Datenhaltung gespeichert, sondern in einem separaten Status-DB-Schema. Das FMS bindet das Status-Schema neben seiner eigenen Datenhaltung als zusätzliche Datenquelle ein. Anhand eines eindeutigen Kriteriums (z. B. die interne Nutzer-ID, eine eindeutige E-Mail-Adresse des Nutzers o. ä.) können dem angemeldeten Nutzer die Status- und Fehlerinformationen präsentiert werden.

Die folgende Abbildung zeigt die Einbindung des Status-Schemas durch das FMS und den WebSphere Process Server. Der WebSphere Process Server greift schreibend und das FMS nur lesend auf das Status-Schema zu.

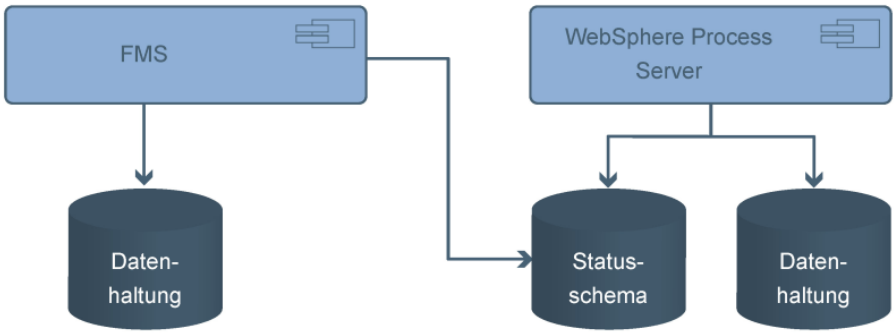

Abbildung 8.3: Einbindung des Status-DB-Schemas (Bund)

Einordnung der Komplexität:

Produkt	Umzusetzende Funktionalität	Einordnung der Komplexität	Bemerkungen
FMS	Realisierung der Statusanzeige	Erweiterung	Die Einbindung und Visualisierung der Statusinformationen kann über die Erweiterung der bestehenden Funktionalität erreicht werden.

Tabelle 8.3: Realisierung der Statusanzeige

8.1.3.c Anbindung an das Servicekonto (Weberfassung/Upload)

Die Anbindung des FMS an das Servicekonto des Bundes geschieht über den Standard SAML, mit dem ein Single Sign-On erreicht werden kann. Eine separate Anmeldung an das FMS ist damit nicht mehr nötig. Hierbei fungiert das FMS als sogenannter ServiceProvider innerhalb einer föderierten Landschaft. Das Servicekonto ist der Identitätsprovider, der die Identitätsprüfung sicherstellt und dem sich unterschiedliche ServiceProvider anschließen können.

Mögliche Ausgestaltung des Anmeldevorgangs:

Wenn sich ein Rechnungssender am FMS anmelden will, wird er auf das Servicekonto umgeleitet. Er führt dort die Authentisierung durch, wird vom Servicekonto authentifiziert und an das FMS weitergeleitet. Ein SAML-Token signalisiert dem FMS die erfolgreiche Authentifizierung. Anhand eines mitgelieferten eindeutigen Kriteriums (interne User-ID, E-Mail-Adresse usw.) erkennt das FMS den Rechnungssender und gleicht diesen mit der eigenen Nutzerverwaltung ab. Wird der Rechnungssender dort gefunden, werden die Nutzerdaten aus dem FMS geladen und der Rechnungssender kann z. B. die Statusinformationen zu seinen eingelieferten XRechnungen einsehen.

Wird der Rechnungssender nicht in der internen Nutzerverwaltung gefunden, wird ein neues Konto angelegt.

Einordnung der Komplexität:

Produkt	Umzusetzende Funktionalität	Einordnung der Komplexität	Bemerkungen
FMS	Anbindung an das Servicekonto	Konfiguration/ Erweiterung	Die Anbindung eines ServiceProviders geschieht in kompatiblen Systemen aufgrund von Konfigurationen. Die Anbindung bzw. Nutzung der FMS-eigenen Nutzerverwaltung (zur Referenzierung der Statusinformationen) wird als Erweiterung angesehen.

Tabelle 8.4: Anbindung an das Servicekonto

8.1.3.d Bereitstellung der verschiedenen Übertragungskanäle

Der Empfang einer XRechnung über den Governikus MultiMessenger ist über die Kanäle De-Mail und E-Mail möglich. Auch der Empfang über einen angebotenen Webservice ist standardmäßig vorgesehen. Die präferierte, sichere und etablierte Variante eines Empfangs über einen Webservice auf Basis des Standards AS2/AS4 ist möglich, muss allerdings noch realisiert werden.

Einordnung der Komplexität:

Produkt	Umzusetzende Funktionalität	Einordnung der Komplexität	Bemerkungen
Governikus MultiMessenger	Bereitstellung der verschiedenen Kanäle	Erweiterung	Die Bereitstellung des Übertragungskanals Webservice basierend auf dem Standard AS4 ist im Moment nicht realisiert, kann aber über eine Erweiterung realisiert werden.

Tabelle 8.5: Bereitstellung der verschiedenen Übertragungskanäle

8.1.3.e Anbindung des FMS (Authentifizierung)

Das Servicekonto dient in einer föderierten Umgebung als Identitätsprovider, welcher die Registrierung und Authentifizierung von Rechnungssendern durchführt. Es dient als Vertrauensstelle, an der sich ServiceProvider (hier das FMS) registrieren können. Die erfolgreiche Anmeldung wird dem ServiceProvider durch einen SAML-Token signalisiert, den der Rechnungssender beim Aufruf des FMS sendet (vgl. 8.1.3.c).

Einordnung der Komplexität:

Produkt	Umzusetzende Funktionalität	Einordnung der Komplexität	Bemerkungen
Servicekonto	Anbindung des FMS	Konfiguration	Die Anbindung von ServiceProvidern an das Servicekonto (als Identitätsprovider) geschieht über Konfiguration.

Tabelle 8.6: Anbindung des FMS

8.1.3.f Generierung von Whitelists (Authentifizierung)

Zur effizienten Prüfung, ob die E-Mail- oder De-Mail-Adresse eines Absenders im Identitätenspeicher bekannt und damit zur Einreichung von eRechnungen berechtigt ist, erfolgt über eine Whitelistprüfung. Eine solche Whitelist ist zyklisch aus den verfahrensspezifischen Registrierungsdaten (bzw. den vom Rechnungssender erfassten Daten zu den Übertragungskanälen) zu generieren.

Einordnung der Komplexität:

Produkt	Umzusetzende Funktionalität	Einordnung der Komplexität	Bemerkungen
Servicekonto bzw. FMS	Generierung von Whitelists	Erweiterung	Die verfahrensspezifischen Registrierungsdaten bzw. die zusätzlichen Daten für die Nutzung der verschiedenen Übertragungskanäle werden im FMS erfasst. Die Generierung von Whitelists kann über eine Erweiterung realisiert werden. Hierzu könnte beispielsweise mit Hilfe eines cronjob per SQL-Statement eine Liste aller hinterlegten E-Mail-/ De- Mail-Adressen generiert werden.

Tabelle 8.7: Generierung von Whitelists

8.1.3.g Anbindung des Governikus MultiMessenger (Authentifizierung)

Neue Rechnungssender, die eine erfolgreiche Registrierung am Servicekonto durchlaufen haben, müssen dem Governikus MultiMessenger bekannt gemacht werden. Diese Bekanntmachung kann z. B. über die vom MultiMessenger angebotene SPML-Schnittstelle durchgeführt werden. Die erforderlichen Daten des Rechnungssenders können durch das FMS (nach erfolgreicher Registrierung des Rechnungssenders am Servicekonto) an den MultiMessenger geliefert werden. Die Anbindung bzw. Nutzung der SPML-Schnittstelle würde damit nicht vom Servicekonto, sondern durch das möglicherweise flexibler anpassbare FMS erbracht werden.

Einordnung der Komplexität:

Produkt	Umzusetzende Funktionalität	Einordnung der Komplexität	Bemerkungen
Servicekonto	Anbindung des Governikus MultiMessengers	Erweiterung	Die Bedienung der SPML-Schnittstelle ist über eine Erweiterung möglich.

Tabelle 8.8: Anbindung des Governikus MultiMessengers

8.1.3.h Realisierung der Prüfungskomponente (Prüfung)

Die Prüfungskomponente ist eine vollständig neu zu entwickelnde Komponente. Möglicherweise kann das Land Bremen diese Entwicklung erbringen und die Komponente durch die Einbringung über den IT-Planungsrat für den Bund nachnutzbar machen. Es wird dabei empfohlen, eine einfach zu nutzende moderne Standardschnittstelle (z. B. einen Webservice) zu realisieren.

Einordnung der Komplexität:

Produkt	Umzusetzende Funktionalität	Einordnung der Komplexität	Bemerkungen
Eigenentwicklung	Realisierung der Prüfung von XRechnungen	Neuentwicklung	Die Komponente existiert noch nicht und muss neu entwickelt werden.

Tabelle 8.9: Realisierung der Prüfung von XRechnungen

8.1.3.i Mapping der Auftragskennnummer (Adressierung/Weiterleitung)

Für die Pflege und spätere Ermittlung der korrekten Zieladresse der angeschlossenen Rechnungsfreigabesysteme wird eine Mappingtabelle benötigt, auf die der WebSphere Process Server Zugriff hat.

Es wird empfohlen, den Aufbau der Mappingtabelle wie folgt zu untergliedern:

Tabelle A dient der logischen Zuordnung mit folgenden Attributen (Auswahl):

- Grob klassifizierender Teil der Auftragskennnummer
- Logische Zieladresse
- Gültig ab

Tabelle B als Mapping der logischen Zieladresse zu einer technischen Zieladresse:

- Logische Zieladresse
- Technische Zieladresse (Die Ausgestaltung der technischen Zieladresse bleibt hier offen. Diese könnte z. B. auch durch einen Dateipfad gekennzeichnet sein.)

Tabelle A wird wahrscheinlich häufiger aktualisiert als Tabelle B. Die Pflege kann durch Nicht-Techniker (z. B. durch das KKR) erfolgen. Änderungen an Tabelle B werden seltener erwartet und können vom technischen Betreiber erfüllt werden.

Einordnung der Komplexität:

Produkt	Umzusetzende Funktionalität	Einordnung der Komplexität	Bemerkungen
WebSphere Process Server	Mapping der Auftragskennung	Erweiterung	Das Mapping kann über eine Erweiterung realisiert werden.

Tabelle 8.10: Mapping der Auftragskennung

8.1.3.j Orchestrierung (Adressierung/Weiterleitung)

Eine Kernfunktionalität des WebSphere Process Servers besteht in der Orchestrierung bzw. dem Zusammenstecken von verschiedenen Komponenten/Anwendungen/Diensten. Diese Orchestrierung kann über die Definition und Ausführung eines Prozesses in BPEL erfolgen. Die folgende Abbildung skizziert grob den empfohlenen Ablauf des Prozesses innerhalb des zentralen eRechnungseingangs.

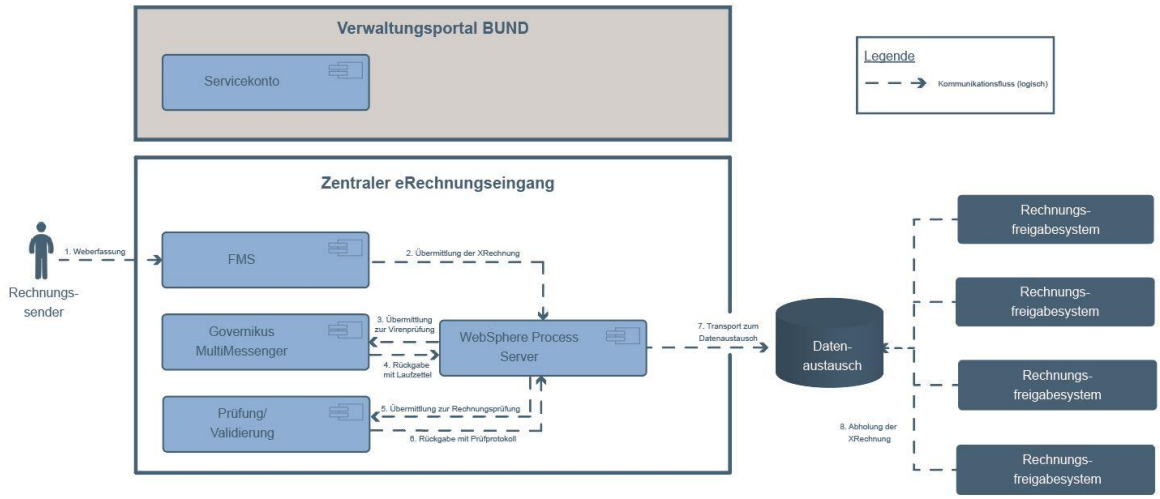

Abbildung 8.4: Kommunikationsfluss bei der Orchestrierung der Komponenten (Bund)

1. Der (bereits authentifizierte) Rechnungssender erfasst eine Rechnung über die Weberfassung und sendet diese ab.
2. Die daraus generierte XRechnung (nebst allen Anlagen) wird an den Process Server übermittelt. Dieser protokolliert den Eingang. Die Protokollierung findet grundsätzlich in einem separaten Status-DB-Schema statt (vgl. 8.1.3.b).
3. Der Process Server übergibt die XRechnung (inklusive der Anlagen) für die Virenprüfung an den Governikus MultiMessenger.
4. Die XRechnung (nebst Anlagen) wird mit dem Ergebnis der Virenprüfung (und einem digitalen Laufzettel) an den Process Server zurückgegeben. Das Ergebnis der Virenprüfung wird protokolliert.
5. Der Process Server schickt die XRechnung an die Prüfungskomponente.
6. Die XRechnung wird mit dem Ergebnis der Prüfung (vermerkt im Laufzettel) an den Process Server übergeben. Der Status und ein möglicher Fehler werden vom Process Server protokolliert.
7. Der Process Server übergibt die XRechnung, alle Anlagen und den digitalen Laufzettel nach erfolgreicher Adressierung an den Datenaustausch Server. Der Satus wird vom Process Server protokolliert.
8. Die Rechnungsfreigabesysteme können sich die XRechnung inklusive Anlagen und Laufzettel abholen.

Einordnung der Komplexität:

Produkt	Umzusetzende Funktionalität	Einordnung der Komplexität	Bemerkungen
WebSphere Process Server	Orchestrierung der einzelnen Komponenten	Konfiguration/ Erweiterung	Die Realisierung der Orchestrierung kann über eine Konfiguration erfolgen. Hierunter wird auch eine Prozessdefinition verstanden. Die Bedienung der internen Schnittstellen der Komponenten muss über eine Erweiterung erfolgen.

Tabelle 8.11: Orchestrierung der Komponenten

8.1.3.k Realisierung der Status- und Fehlerprotokollierung

Die Status- und Fehlerprotokollierung wird durch die Realisierung der Orchestrierung der Komponenten durch den Process Server umgesetzt. Die wesentlichen Status und signalisierten Fehler werden bei der Kommunikation mit den Komponenten umgesetzt (vgl. 8.1.3.j).

Einordnung der Komplexität:

Produkt	Umzusetzende Funktionalität	Einordnung der Komplexität	Bemerkungen
WebSphere Process Server	Realisierung der Status- und Fehlerprotokollierung	Erweiterung	Die separate Protokollierung der Status- und signalisierten Fehler kann durch eine Erweiterung realisiert werden.

Tabelle 8.12: Realisierung der Status- und Fehlerprotokollierung

8.1.4 Schnittstellen zu den Rechnungsfreigabesystemen

8.1.4.a SFTP-Schnittstelle zu den Freigabesystemen

Ein in der Verwaltung seit Jahren erprobtes und etabliertes Verfahren für einen robusten Datenaustausch (z. B. bei buchungsrelevanten Daten) ist der dateibasierte Austausch über einen File-Server. Die Kommunikation wird dabei verschlüsselt per SFTP realisiert. Es wird deshalb empfohlen, diese auch als grundsätzliche Schnittstelle des zentralen eRechnungseingangs zu den unterschiedlichen Rechnungsfreigabesystemen anzubieten.

Nachdem der WebSphere Process Server die korrekte technische Adresse innerhalb der Mappingtabelle gefunden hat, wird die XRechnung (inklusive aller Anhänge und des Laufzettels) per SFTP in den Ordner der rechnungsempfangenden Stelle auf einen separaten FTP-Server transportiert (Push per SFTP).

Das Rechnungsfreigabesystem der jeweiligen Behörde kann die XRechnung in dem ihr zugewiesenen Ordner zeitgesteuert abholen (Pull per SFTP). Für eine erneute Abholung ist die XRechnung in dem konkreten Ordner der jeweiligen Behörde über einen konfigurierbaren Zeitraum vorzuhalten und nach Überschreitung des Zeitraums zu löschen. Es wird empfohlen, die XRechnung auf dem FTP-Server für einen konfigurierbaren Zeitraum vorzuhalten. Sollten die angeschlossenen Rechnungsfreigabesysteme Schwierigkeiten beim Transport oder der Verarbeitung der XRechnung haben, können sie diese einfach erneut abholen. Nach Ablauf der Frist kann die XRechnung (inklusive der Anlagen und des Laufzettels) gelöscht werden. Die folgende Abbildung skizziert die SFTP-Schnittstelle zwischen dem zentralen eRechnungseingang und den unterschiedlichen Rechnungsfreigabesystemen der Verwaltung.

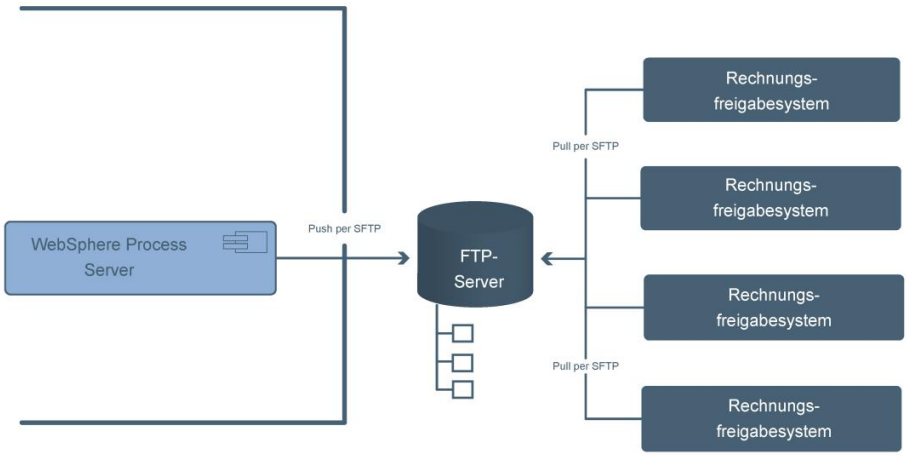

Abbildung 8.5: Schematische Skizze der SFTP-Schnittstelle (Bund)

8.1.4.b XTA-Schnittstelle zu den Freigabesystemen

Neben der beschriebenen SFTP-Schnittstelle wird empfohlen, zukünftig ebenso eine Webservice-Schnittstelle nach dem XTA-Standard anzubieten. Hierdurch können moderne Freigabesysteme über eine strikter

definierte Schnittstelle angebunden werden, die damit möglicherweise Fehler beim Aufruf und bei der späteren Verarbeitung mindern kann.

8.1.4.c Rückkanal der Rechnungsfreigabesysteme

Falls eine Auftragskennnummer bzw. der für die rechnungsempfangende Behörde qualifizierende Teil nicht mit dem korrekten Rechnungsempfänger korrespondiert, wird die eRechnung nicht in das korrekte Rechnungsfreigabesystem geleitet. Für diese Fälle sollte zukünftig eine (Rück-)Schnittstelle der empfangenden Behörde zum zentralen eRechnungseingang vorgesehen werden.

8.1.5 Logisches Architekturmodell im ITZBund

Das logische Architekturmodell der folgenden Abbildung bildet die Grundlage für die konkrete Zuordnung der logischen Komponenten auf physikalische Server im ITZBund. Das Servicekonto des Bundes und der Governikus Autent dienen dabei als alternative Implementierungen. Die Anbindung des Übertragungskanals EGVP innerhalb des Governikus MultiMessengers wurde hierbei für mögliche zukünftige Ausbaustufen berücksichtigt.

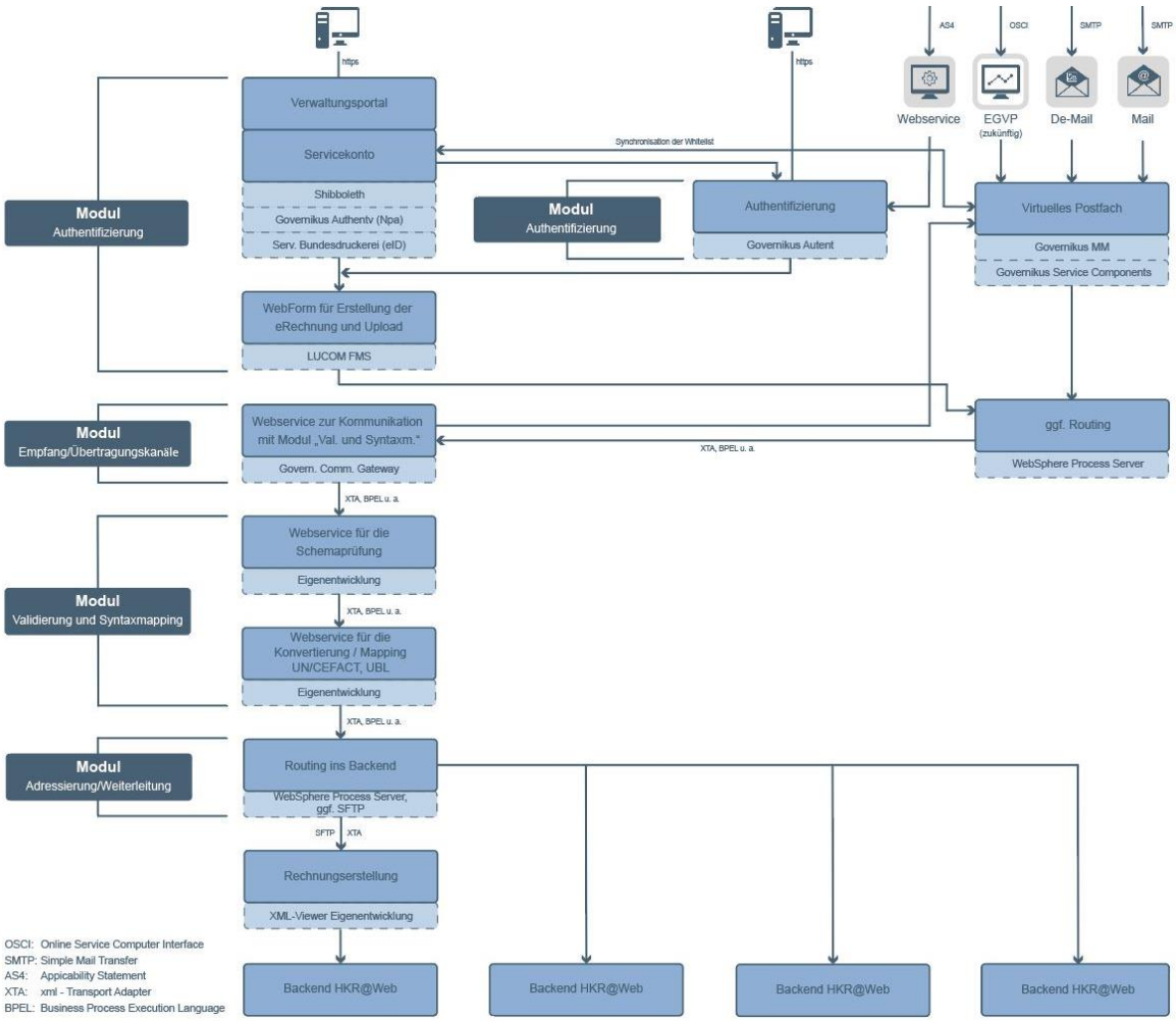

Abbildung 8.6: Logisches Architekturmodell im ITZBund

8.1.6 Physikalisches Architekturmodell im ITZBund

Basierend auf dem logischen Architekturmodell beschreibt die folgende Abbildung das Architekturmodell abgebildet auf physikalische Server. Bisher sind insgesamt vier Systeme für Entwicklung, Test, Staging und Produktion mit unterschiedlichen Dimensionierungen vorgesehen.

Beispielhaft skizziert die folgende Abbildung die Dimensionierung innerhalb des Produktions-Systems des zentralen eRechnungseingangs, wie es aktuell geplant ist. Die Dimensionierung orientiert sich dabei an der in Kapitel 5.1.2 aufgestellten Berechnung zum durchschnittlichen Empfang von elektronischen Rechnungen.

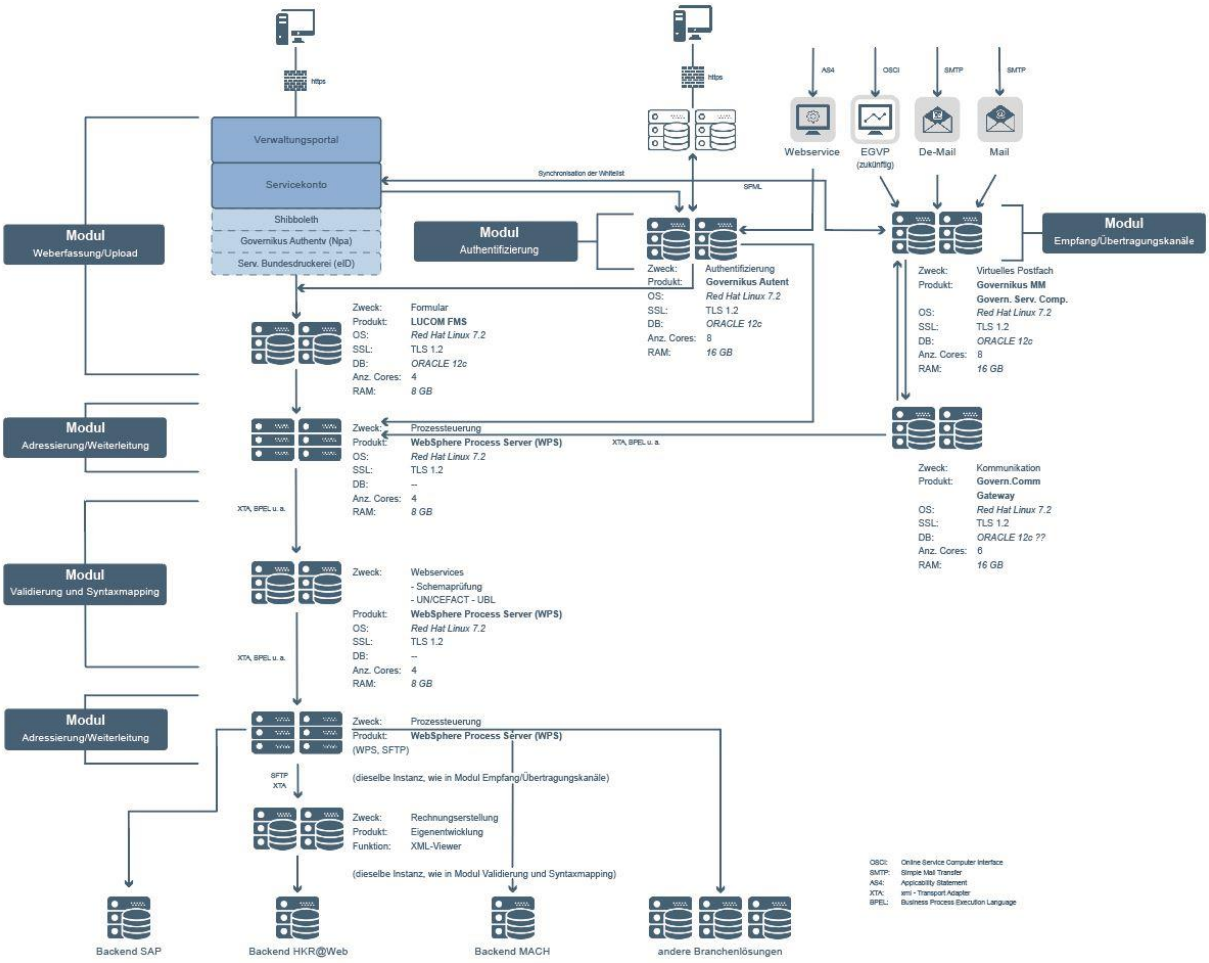

Abbildung 8.7: Physikalische Abbildung der Architektur (Bund)

8.2 Architekturmodell des Landes Bremen

Das auf Basis der obigen Betrachtung entstehende konkrete Architekturmodell der Freien Hansestadt Bremen basiert auf

- einer Eigenentwicklung für die Funktionalitäten des Moduls Weberfassung/Upload
- dem Governikus MultiMessenger für das Modul Übertragungskanäle
- dem Governikus Autent/Autent Frontend für das Modul Authentifizierung (ggf. in Kombination mit Governikus Autent ID Connect zur Verknüpfung mit anderen Identitätsspeichern)
- einer Eigenentwicklung für das Modul Rechnungsprüfung bzw. ggf. der Nachnutzung einer vom IT-Planungsrat zur Verfügung gestellten Komponente
- einer noch zu bestimmenden technischen Lösung für das Model Adressierung/Weiterleitung

Die folgende Abbildung visualisiert die Zuordnung der Produkte/Komponenten zu den Modulen und deren Verortung im Gesamtprozess des zentralen eRechnungseingangs.

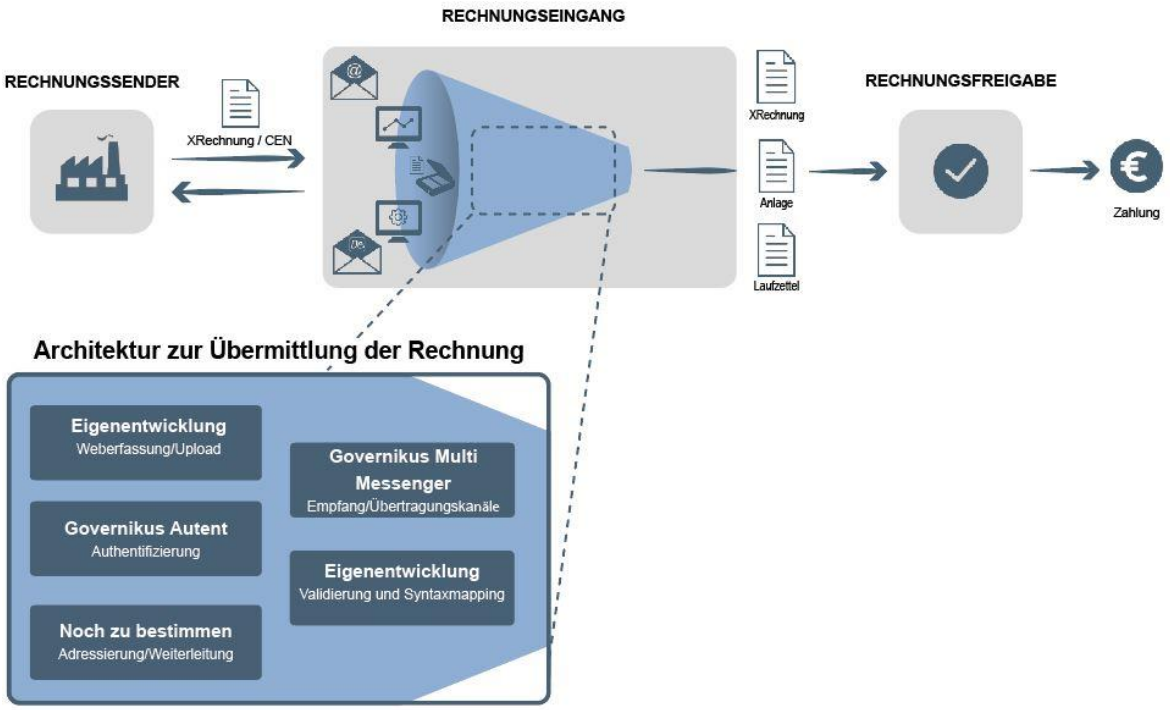

Abbildung 8.8: Architektur mit konkreten Komponenten (Bremen)

8.2.1 Systembeschreibung

Der zentrale eRechnungseingang der Freien Hansestadt Bremen basiert auf den Komponenten, die auch für den Aufbau der föderierten Servicekonten gemäß Onlinezugangsgesetz (OZG) eingesetzt werden sollen. Eine Integration bzw. ein Verweis im Serviceportal Bremen ist vorgesehen. Auch die Zugangseröffnung über

Governikus MultiMessenger bettet sich in die Gesamtstrategie der Freien Hansestadt Bremen zur Zugangseröffnung der Verwaltung ein. Die Anwendung für den zentralen eRechnungseingang wird als erster Anwendungsfall realisiert.

Ob eine gesonderte Orchestrierungskomponente erforderlich wird, hängt im Wesentlichen von der Leistungsfähigkeit des Moduls Rechnungsprüfung ab, da dieses Modul als Verbindungskomponente zwischen dem Empfangsmodul und dem Weiterleitungsmodul fungieren kann. Derzeit wird davon ausgegangen, dass das Prüfmodul über eine eigene Empfangs- und Weiterleitungslogik zum Vorgänger- und Folgemodul verfügt. Je nach Wahl der technischen Lösung für das Modul Adressierung/Weiterleitung könnte aber möglicherweise auch dieses als Process Engine die Orchestrierung als SOA ermöglichen. Als weitere Alternative könnte auch der Governikus MultiMessenger wird mit entsprechenden Orchestrierungsfunktionalitäten erweitert werden. Eine automatisierte Rückkommunikation aus dem Prüfmodul über das Modul Empfang/Übertragungskanäle in definierten Fehlerfällen ist vorgesehen. Eine automatisierte Rückkommunikation im Fehlerfall im Modul Adressierung/Weiterleitung wird nicht realisiert. Tritt der Fall ein, dass eine Adressierung bzw. Weiterleitung an das Freigabe-/Workflowsystem nicht möglich ist, erfolgt eine Aussteuerung der Nachricht (inkl. zugehöriger Dateien) an eine zentrale Clearingstelle, die eine weitere manuelle Prüfung vornimmt. Ist eine Weiterleitung möglich, erfolgt diese über für jedes Workflowsystem festgelegte Schnittstellen.

In der folgenden Abbildung ist der Datenaustausch der Module untereinander sowie mit föderierten Servicekonten und den Freigabe-/Workflowsystemen grob skizziert.

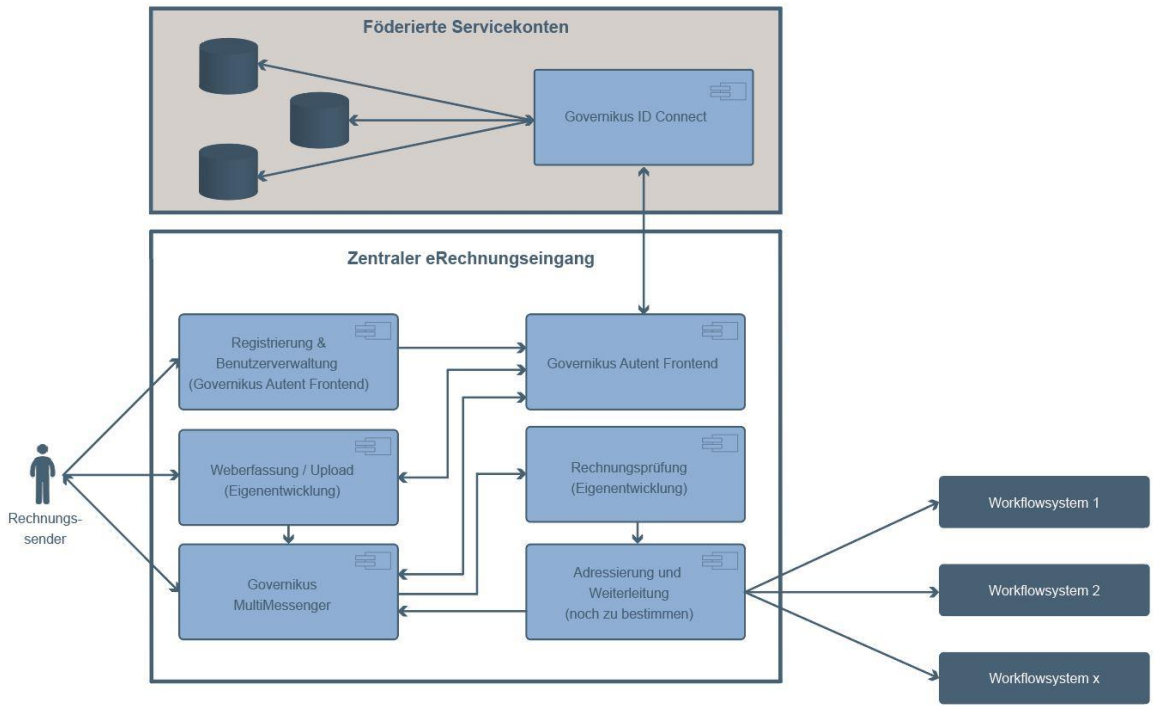

Abbildung 8.9: Abbildung des Gesamtsystems (Bremen)

8.2.2 Herausforderungen bei der Realisierung

Die folgende Tabelle fasst die wesentlichen Herausforderungen bei der Realisierung des zentralen eRechnungseingangs anhand der eingesetzten Produkte zusammen. Diese liegen sowohl in der Realisierung der Kommunikation der Komponenten untereinander als auch in der Konfiguration, Anpassung/Erweiterung der bereits angebotenen Funktionalitäten. Da für das Prüfmodul keine bereits vorhandene Komponente eingesetzt werden kann, ist hierfür eine vollständige Neuentwicklung bzw. der Einsatz einer vom IT-Planungsrat zur Verfügung gestellten Komponente vorzusehen. Ebenfalls eine Neuentwicklung ist für die Weberfassung/Upload vorgesehen. Für die Komponente Adressierung/Weiterleitung konnte noch keine konkrete technische Lösung bestimmt werden. Es wird allerdings davon ausgegangen, dass eine solche noch gefunden werden kann und diese durch Erweiterungen und Konfigurationen die umzusetzenden Funktionalitäten bietet.

Modul	Produkt	Umzusetzende Funktionalität
Weberfassung/Upload	Eigenentwicklung	Bereitstellung der Formulare Generierung und Bereitstellung der eRechnung Anbindung an den Governikus Autent Anbindung an den Governikus MultiMessenger
Übertragungskanäle	Governikus MultiMessenger	Bereitstellung der verschiedenen Eingangs- und Ausgangskanäle
Authentifizierung	Governikus Autent	Erfassung und Speicherung von Identitäts- und Verfahrensdaten Anbindung des Moduls Weberfassung/Upload Anbindung des Governikus MultiMessengers Generierung von Whitelists
Prüfung	n. v. – Eigenentwicklung bzw. über den IT-Planungsrat, sofern über diesen bereitgestellt	Realisierung der Prüfung von XRechnungen Anbindung an den Governikus MultiMessenger Anbindung an das Modul Adressierung/Weiterleitung

Modul	Produkt	Umzusetzende Funktionalität
Adressierung/ Weiterleitung	noch zu bestimmen	Mapping der Grobadressierung (Buyer reference) auf die jeweilige technische Adresse des rechnungsempfangenden Freigabesystems Erstellung der Empfangsbestätigungsnachricht und Übergabe an Modul Übertragungskanäle Übergabe der XRechnung (inkl. Anlagen und Laufzettel) an die jeweiligen Freigabesysteme oder eine Clearingstelle

Tabelle 8.13: Herausforderungen der Realisierung

8.2.3 Hinweise und Empfehlungen zur Realisierung

Nachfolgend werden Hinweise und/oder Empfehlungen für die Realisierung der geforderten Funktionalität gegeben. Abschließend wird zu jeder umzusetzenden Funktionalität tabellarisch eine Einordnung der Komplexität der Umsetzung vorgenommen. Diese kann bei der Planung der späteren Umsetzung genutzt werden. Die folgenden Einordnungen wurden dabei gewählt:

- Konfiguration: Die Realisierung kann durch die Konfiguration der Komponente erreicht werden.
- Erweiterung: Die vorhandene Funktionalität muss erweitert werden.
- Neuentwicklung: Die Funktionalität kann nur durch eine komplette Neuentwicklung erreicht werden.

8.2.3.a Bereitstellung der Formulare (Weberfassung/Upload)

Die Realisierung der konkreten Formulare, die eine einfache und fehlerresistente Erfassung von XRechnungen, den Upload von mit Fachverfahren erzeugten XRechnungen sowie den Upload von Anlagen ermöglichen, muss einmalig erbracht und bei Änderungen am Standard XRechnung ggf. angepasst werden. Sobald der Standard XRechnung finalisiert ist, können die Formulare und geeignete Formularvalidierungen umgesetzt werden.

Einordnung der Komplexität:

Produkt	Umzusetzende Funktionalität	Einordnung der Komplexität	Bemerkungen
Eigenentwicklung	Bereitstellung der Formulare	Neuentwicklung basierend auf vorhandenem CSS und Standardwebframework	Die Formulare müssen auf Grundlage des jeweils gültigen Standards XRechnung erstellt werden.

Tabelle 8.14: Bereitstellung der Formulare

8.2.3.b Generierung und Bereitstellung der eRechnung (Weberfassung/Upload)

Im Falle der Erfassung einer Rechnung über das Formular muss nach dem Absenden des Formulars eine XRechnungsinstanz durch das Modul Weberfassung/Upload auf Basis der gesendeten Formularinhalte erzeugt werden. Die erzeugte XML-Instanz ist sodann dem Rechnungssender zum Download zur Verfügung zu stellen sowie für die Weiterleitung an den Governikus MultiMessenger zu verwenden.

Einordnung der Komplexität:

Produkt	Umzusetzende Funktionalität	Einordnung der Komplexität	Bemerkungen
Eigenentwicklung	Generierung und Bereitstellung der eRechnung	Neuentwicklung	Eine Funktionalität zur Erzeugung einer XRechnung muss neu geschaffen werden, lässt sich aber durch Marshalling/Serialisierung realisieren.

Tabelle 8.15: Generierung und Bereitstellung der eRechnung

8.2.3.c Anbindung an den Governikus Autent (Weberfassung/Upload)

Die Anbindung des Webfrontends an den Governikus Autent geschieht mittels REST-Service über den Standard SAML, mit dem ein Single Sign-On erreicht werden kann. Hierbei fungiert das Webfrontend als sogenannter ServiceProvider innerhalb einer Landschaft föderierter Identitäten. Der Governikus Autent ist der Identitätsprovider, der die Identitätsprüfung sicherstellt und dem sich unterschiedliche ServiceProvider anschließen können.

Einordnung der Komplexität:

Produkt	Umzusetzende Funktionalität	Einordnung der Komplexität	Bemerkungen
Eigenentwicklung	Anbindung an den Governikus Autent	Konfiguration	Die Anbindung eines ServiceProviders geschieht in kompatiblen Systemen aufgrund von Konfigurationen.

Tabelle 8.16: Anbindung an den Governikus Autent

8.2.3.d Anbindung an den Governikus MultiMessenger (Weberfassung/Upload)

Die Anbindung des Webfrontends an den Governikus MultiMessenger geschieht über eine XTA-Schnittstelle. Hierüber wird die XRechnungsnachricht mit ggf. übermittelten Anlagen gesendet.

Einordnung der Komplexität:

Produkt	Umzusetzende Funktionalität	Einordnung der Komplexität	Bemerkungen
Eigenentwicklung	Anbindung an den Governikus Multi-Messenger	Neuentwicklung	Die Bedienung der XTA-Schnittstelle des GMM wird im Webframework voraussichtlich neu entwickelt werden müssen und anschließend eine spezifische Konfiguration in Bezug auf die konkrete GMM-Instanz erfordern.

Tabelle 8.17: Anbindung an den Governikus MultiMessenger

8.2.3.e Bereitstellung der verschiedenen Übertragungskanäle (Empfang/Übertragungskanäle)

Der Empfang einer Nachricht mit enthaltener XRechnung über den Governikus MultiMessenger ist über die Kanäle De-Mail und E-Mail möglich. Auch der Empfang über einen angebotenen Webservice ist standardmäßig vorgesehen. Eine XTA-Schnittstelle für den Empfang von Nachrichten, die das Modul Weberfassung/Upload sendet, steht ebenfalls zur Verfügung. Die präferierte, sichere und etablierte Variante eines

Empfangs über einen Webservice auf Basis des Standards AS4 für externe Kommunikationspartner ist möglich, muss allerdings noch realisiert werden.

Einordnung der Komplexität:

Produkt	Umzusetzende Funktionalität	Einordnung der Komplexität	Bemerkungen
Governikus MultiMessenger	Bereitstellung der verschiedenen Kanäle	Erweiterung	Die Bereitstellung des Übertragungskanals Webservice basierend auf dem Standard AS4 ist im Moment nicht realisiert, kann aber über eine Erweiterung realisiert werden.

Tabelle 8.18: Bereitstellung der verschiedenen Übertragungskanäle

8.2.3.f Erfassung und Speicherung von Identitäts- und Verfahrensdaten (Authentifizierung)

Der Governikus Autent ist als Identitätsprovider darauf ausgelegt, Identitätsdaten zu verwalten. Für spezielle Fachanwendungen wie das zentrale eRechnungseingangssystem ist die Speicherung von verfahrensspezifischen Daten, die den Identitätsdaten zugeordnet sind, erforderlich. Im Falle der eRechnung gehören dazu z. B. die freigeschalteten Einlieferungskanäle und die Rückkommunikationsadresse. Die Speicherung der Verfahrensdaten ist derzeit nicht vorgesehen.

Einordnung der Komplexität:

Produkt	Umzusetzende Funktionalität	Einordnung der Komplexität	Bemerkungen
Governikus Autent	Erfassung und Speicherung von Identitäts- und Verfahrensdaten	Erweiterung	Die Erfassung und Speicherung der zusätzlichen Daten kann über eine Erweiterung der Datenbank und der Benutzeroberflächen realisiert werden.

Tabelle 8.19: Erfassung und Speicherung von Identitäts- und Verfahrensdaten

8.2.3.g Anbindung des Moduls Weberfassung/Upload (Authentifizierung)

Der Governikus Autent dient als Identitätsprovider, welcher die Registrierung und Authentifizierung von Rechnungssendern durchführt. Er dient als Vertrauensstelle, an der sich ServiceProvider registrieren können. Die erfolgreiche Anmeldung wird dem ServiceProvider durch einen SAML-Token signalisiert, den der Rechnungssender beim Aufruf der Weberfassung/des Uploads sendet.

Einordnung der Komplexität:

Produkt	Umzusetzende Funktionalität	Einordnung der Komplexität	Bemerkungen
Governikus Autent	Anbindung des Moduls Weberfassung/Upload	Konfiguration	Die Anbindung von ServiceProvidern am Identitätsprovider geschieht über Konfigurationen.

Tabelle 8.20: Anbindung des Moduls Weberfassung/Upload

8.2.3.h Anbindung des Governikus MultiMessenger (Authentifizierung)

Neue Rechnungssender, die eine erfolgreiche Registrierung am Servicekonto durchlaufen haben, müssen dem Governikus MultiMessenger bekannt gemacht werden. Diese Bekanntmachung kann z. B. über die vom MultiMessenger angebotene SPML-Schnittstelle durchgeführt werden.

Einordnung der Komplexität:

Produkt	Umzusetzende Funktionalität	Einordnung der Komplexität	Bemerkungen
Governikus Autent	Anbindung des Governikus Multi-Messengers	Erweiterung	Die Bedienung der SPML-Schnittstelle ist über eine Erweiterung möglich.

Tabelle 8.21: Anbindung des Governikus MultiMessengers

8.2.3.i Generierung von Whitelists (Authentifizierung)

Zur effizienten Prüfung, ob die E-Mail- oder De-Mail-Adresse eines Absenders im Identitätenspeicher bekannt und damit zur Einreichung von eRechnungen berechtigt ist, erfolgt über eine Whitelistprüfung. Eine solche Whitelist ist zyklisch aus dem Identitätenspeicher zu generieren.

Einordnung der Komplexität:

Produkt	Umzusetzende Funktionalität	Einordnung der Komplexität	Bemerkungen
Governikus Autent	Generierung von Whitelists	Erweiterung	Die Generierung von Whitelists kann über eine Erweiterung realisiert werden. Hierzu könnte beispielsweise mithilfe eines cronjob per SQL-Statement eine Liste aller hinterlegten E-Mail-/ De- Mail-Adressen generiert werden.

Tabelle 8.22: Generierung von Whitelists

8.2.3.j Realisierung der Prüfungskomponente (Prüfung)

Die Prüfungskomponente ist eine vollständig neu zu entwickelnde Komponente. Dabei ist zwischen dem Prüftool, das die Prüfung einer XML-Instanz auf Konformität zum Standard XRechnung vollzieht, und dem Prüfmodul, das die Auswertung und Behandlung des Prüfprotokolls inkl. ggf. Erstellung des Return-to-Sender-Nachrichteninhalts übernimmt, zu unterscheiden. Das Prüftool ist ein Bestandteil des Prüfmoduls. Zur Erhöhung der Nachnutzbarkeit ist die Realisierung von Standardschnittstellen zu empfehlen.

Einordnung der Komplexität:

Produkt	Umzusetzende Funktionalität	Einordnung der Komplexität	Bemerkungen
Eigenentwicklung	Realisierung der Prüfung von XRechnungen	Neuentwicklung	Die Komponente existiert noch nicht und muss neu entwickelt werden.

Tabelle 8.23: Realisierung der Prüfung von XRechnungen

8.2.3.k Anbindung an den Governikus MultiMessenger (Prüfung)

Für den Versand von Return-to-Sender-Nachrichten ist eine Anbindung an den Governikus MultiMessenger erforderlich. Dabei sollte eine Anbindung über eine vom GMM bereits zur Verfügung gestellte Standardschnittstelle erfolgen.

Einordnung der Komplexität:

Produkt	Umzusetzende Funktionalität	Einordnung der Komplexität	Bemerkungen
Eigenentwicklung	Anbindung des Governikus Multi-Messengers	Neuentwicklung/ Konfiguration	Da die Komponente noch nicht existiert, muss auch die Schnittstelle neu entwickelt werden. Anschließend ist eine Konfiguration in Bezug auf die konkrete GMM-Instanz vorzunehmen.

Tabelle 8.24: Anbindung des Governikus MultiMessengers

8.2.3.l Anbindung an das Modul Adressierung/Weiterleitung (Prüfung)

Für die Weiterleitung von Rechnungen nebst Anlagen und Laufzettel ohne annahmeverhindernde Regelverstöße bei der Rechnungsprüfung an das Modul Adressierung/Weiterleitung ist im Prüfmodul eine Standardschnittstelle (XTA) vorzusehen.

Einordnung der Komplexität:

Produkt	Umzusetzende Funktionalität	Einordnung der Komplexität	Bemerkungen
Eigenentwicklung	Anbindung an das Modul Adressierung/Weiterleitung	Neuentwicklung/ Konfiguration	Da die Komponente noch nicht existiert, muss auch die Schnittstelle neu entwickelt werden. Anschließend ist eine Konfiguration auf die konkrete Instanz des Moduls Adressierung/Weiterleitung auszuprägen.

Tabelle 8.25: Anbindung an das Modul Adressierung/Weiterleitung

8.2.3.m Mapping der Grobadressierung (Buyer reference) auf die jeweilige technische Adresse des rechnungsempfangenden Freigabesystems (Adressierung/Weiterleitung)

Für die Pflege und spätere Ermittlung der korrekten Zieladresse der angeschlossenen Rechnungsfreigabesysteme wird eine Mappingtabelle benötigt, auf die das noch näher zu bestimmende Produkt für die Implementierung des Moduls Adressierung/Weiterleitung Zugriff hat.

Das Mapping erfolgt dabei zwischen der Grobadressierung im Element Buyer reference der XRechnung und der technischen Zieladresse (XTA oder SFTP) des Freigabe-/Workflowsystems.

Einordnung der Komplexität:

Produkt	Umzusetzende Funktionalität	Einordnung der Komplexität	Bemerkungen
Noch zu bestimmen	Mapping der Grobadressierung	Erweiterung	Es wird vermutet, dass eine Mappingfunktionalität über eine Erweiterung realisiert werden kann.

Tabelle 8.26: Mapping der Grobadressierung

8.2.3.n Erstellung der Empfangsbestätigungsnachricht und Übergabe an den Governikus MultiMessenger

Bei erfolgreicher Adressierung einer Rechnung wird eine Empfangsbestätigungsnachricht generiert. Diese wird über eine Standardschnittstelle an den Governikus MultiMessenger übergeben, der diese über den Rückkommunikationskanal an den Rechnungssender überträgt.

Einordnung der Komplexität:

Produkt	Umzusetzende Funktionalität	Einordnung der Komplexität	Bemerkungen
Noch zu bestimmen	Erstellung der Empfangsbestätigungsnachricht und Übergabe an den Governikus MultiMessenger	Erweiterung/ Konfiguration	Es ist zu erwarten, dass eine Funktionalität zur Erzeugung einer Empfangsbestätigungsnachricht sowie die Schaffung einer Schnittstelle zum Governikus MultiMessenger über Erweiterungen realisiert werden können.

			Die Anbindung der konkreten GMM-Instanz wird über Konfigurationen erfolgen.

Tabelle 8.27: Erstellung der Empfangsbestätigungsnachricht und Übergabe an den Governikus MultiMessenger

8.2.3.o Übergabe der XRechnung (inkl. Anlagen und Laufzettel) an das jeweilige Freigabesystem oder eine Clearingstelle

Bei erfolgreicher Adressierung einer Rechnung erfolgt nach dem Versand einer Empfangsbestätigungsnachricht die Weiterleitung an ein Freigabesystem. Bei nicht erfolgreicher Adressierung findet eine Übergabe an eine Clearingstelle statt. Das noch zu bestimmende Produkt muss die Logik bereitstellen und die entsprechenden Übertragungswege (XTA, SFTP, E-Mail) bedienen.

Einordnung der Komplexität:

Produkt	Umzusetzende Funktionalität	Einordnung der Komplexität	Bemerkungen
Noch zu bestimmen	Übergabe der XRechnung (inkl. Anlagen und Laufzettel) an das jeweilige Freigabesystem oder eine Clearingstelle	Erweiterung/ Konfiguration	Es ist zu erwarten, dass das noch zu bestimmende Produkt einen Teil der erforderlichen Schnittstellen bereits bedienen kann. Darüber hinaus erforderliche Schnittstellen sind durch Erweiterungen zu schaffen. Die Ausprägung der Schnittstellen erfolgt über Konfigurationen.

Tabelle 8.28: Übergabe der XRechnung an das jeweilige Freigabesystem oder eine Clearingstelle

8.2.4 Schnittstellen zu den Rechnungsfreigabesystemen

Nachdem die noch zu bestimmende Adressierungskomponente die korrekte technische Adresse innerhalb der Mappingtabelle gefunden hat, wird die XRechnung (inklusive aller Anlagen und des Laufzettels), je nach rechnungsempfangenden Workflowsystem, per XTA-Schnittstelle sowie alternativ per SFTP übertragen.

Das Workflowsystem zur Rechnungs- bzw. Zahlungsfreigabe kann die XRechnung in dem ihr zugewiesenen Ordner zeitgesteuert abholen (Pull per SFTP) oder über die XTA-Schnittstelle synchron empfangen. Die folgende Abbildung skizziert den Datenaustausch zwischen dem zentralen eRechnungseingang und den

Workflowsystemen der Verwaltung (ein Workflowsystem für die Kernverwaltung, ggf. weitere für Dienstnutzer assoziierte Organisationen, z. B. Anstalten, Eigenbetriebe und ggf. Gesellschaften).

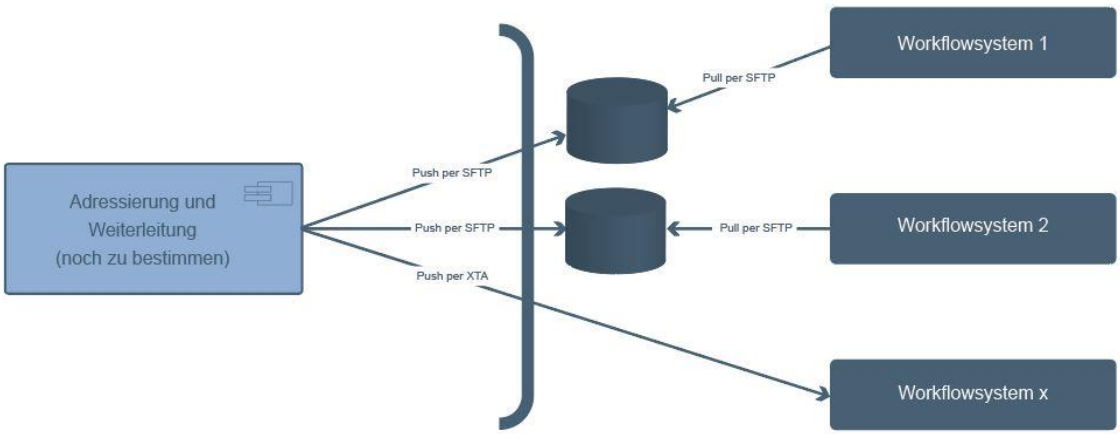

Abbildung 8.10: Schematische Skizze der XTA- und SFTP-Schnittstelle (Bremen)

8.2.5 Logisches Architekturmodell

Das logische Architekturmodell der folgenden Abbildung bildet die Grundlage für die spätere konkrete Zuordnung der logischen Komponenten auf physikalische Server beim IT-Dienstleister.

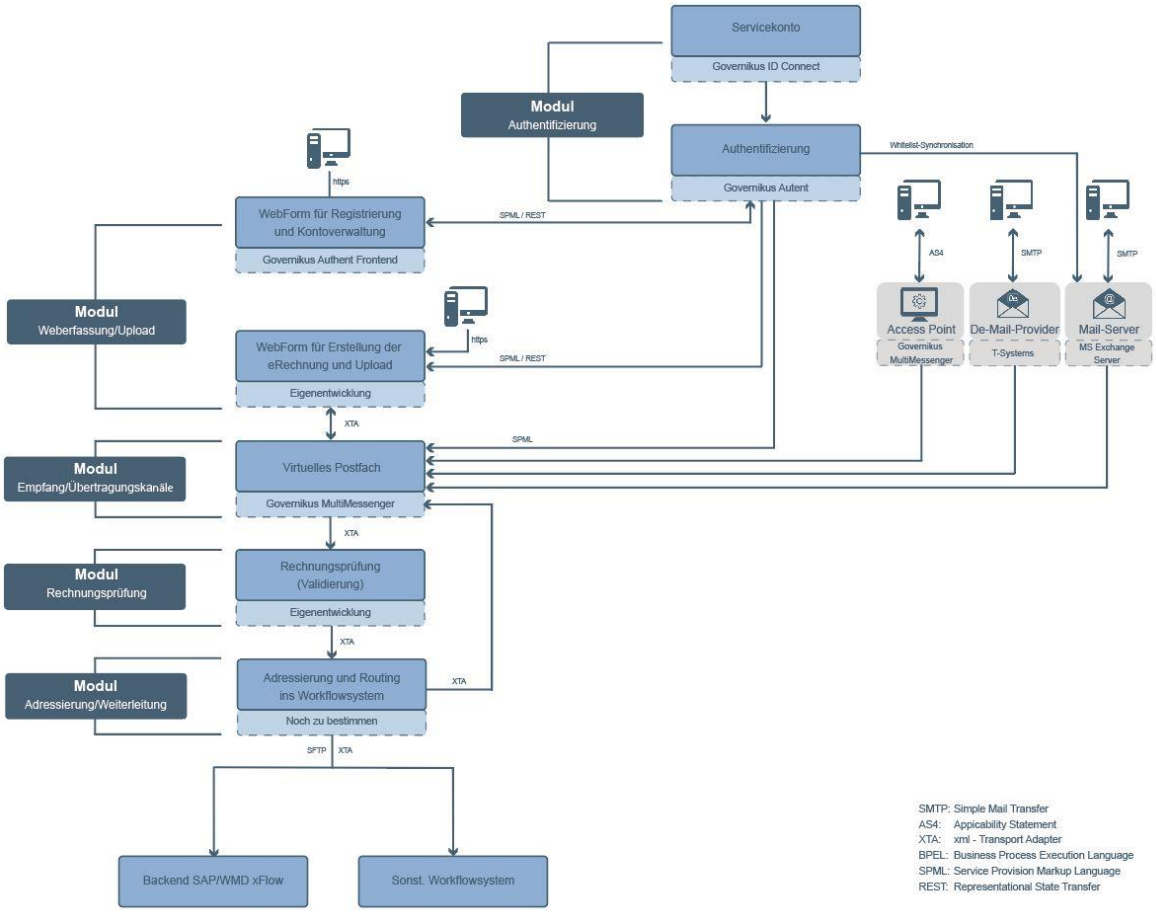

Abbildung 8.11: Logisches Architekturmodell (Bremen)

8.2.6 Physikalisches Architekturmodell bei Dataport

Die Implementierung des Architekturkonzepts ist im Rechenzentrum RZ² des IT-Dienstleisters der Freien Hansestadt Bremen, Dataport AöR, geplant. Die Systeme laufen auf virtualisierten Maschinen, denen Hardwareressourcen entsprechend den über den Zeitablauf steigenden Anforderungen zur Verfügung gestellt werden können.

Abkürzungsverzeichnis

AGG	Allgemeines Gleichbehandlungsgesetz
AK	Abnahmekriterium
AöR	Anstalt des öffentlichen Rechts
API	Application Programming Interface
AU	Authentifikation
AW	Adressierung und Weiterleitung
BGG	Behindertengleichstellungsgesetz
Bild-scharbV	Bildschirmarbeitsverordnung
BITV	Barrierefreie Informationstechnik Verordnung
BPEL	Business Process Execution Language
BPMN	Business Process Model and Notation
BSI	Bundesamts für Sicherheit in der Informationstechnik
CEF	Connecting Europe Facility
CEN	Comité Européen de Normalisation (Europäisches Komitee für Normung)
CMS	Content Management System

CSV	Comma-Seperated Values
DMS	Dokumenten Management System
DP	Dateien- und Nachrichtenprüfung
EGVP	Elektronisches Gerichts- und Verwaltungspostfach
eID	Online-Ausweisfunktion
eIDAS	Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG
EJB	Enterprise JavaBeans
ERP	Enterprise-Resource-Planning
FA	Funktionale Anforderung
FMS	Formular Management System
GMM	Governikus MultiMessenger
IBM DB2	IBM Database Software
IE	Internet Explorer
ITZBund	Informationstechnikzentrum Bund
J2EE	Java Platform Enterprise Edition
Java SE	Java Platform Standard Edition

JDBC	Java Database Connectivity
JEE	Java Platform Enterprise Edition
JMS	Java Message Service
JRE	Java Runtime Environment
JSP	Java Server Pages
KoGIs	Kompetenzzentrum für die Gestaltung der Informationssysteme
LDAP	Lightweight Directory Access Protocol
LIP	Lucom Interaction Platform
LoA	Level of Assurance
nPA/eAT	Neuer Personalausweis/Elektronischer Aufenthaltstitel
OSCI	Online Services Computer Interface
OZG	Onlinezugangsgesetz
PDF	Portable Document Format
PHP	Hypertext Preprocessor
Post-GreSQL	Post Ingres Structured Query Language
PR	Rechnungsprüfung

prEN	preliminary European Norm
RE	Rechnungsempfänger
REST	Representational State Transfer
RS	Rechnungssender
SAML	Security Assertion Markup Language
SCIM	System for Cross-domain Identity Management
SGB	Sozialgesetzbuch
SigG	Gesetz über Rahmenbedingungen für elektronische Signaturen
SMTP	Simple Mail Transfer Protocol
SOA	Serviceorientierte Architektur
SOAP	Simple Object Access Protocol
SPML	Service Provisioning Markup Language
SQL	Structured Query Language
St-Nr	Steuernummer
TLS	Transport Layer Security
TR-03107-1	Technische Richtlinie Elektronische Identitäten und Vertrauensdienste im E-Government - Teil 1

TREATS	TRans-European AuThentication Services
TR-ESOR	Technische Richtlinie - BEweiSwerterhaltung kryptOgRaphisch signierter Dokumente
UBL	Universal Business Language
ÜK	Übertragungskanäle
UN/CE-FACT	United Nations Centre for Trade Facilitation and E-business
URL	Uniform Resource Locator
USt-Nr	Umsatzsteuernummer
VPF	Virtuelle Postfächer
VPS	Virtual Private Server
WF	Weberfassung
WPS	WebSphere Process
WS	Webservice
XHTML	Extensible HyperText Markup Language
XML	Extensible Markup Language
XSLT	Extensible Stylesheet Language Transformation
XTA	Transport Adapter für XML in der öffentlichen Verwaltung

Glossar

Fremdwörter

Caching	Ein Datenspeicher mit verhältnismäßig hoher Zugriffsgeschwindigkeit, der als Puffer bei der Übertragung von Daten zum Einsatz kommt, um aufwendigen Abfragen vorzubeugen.
Client	Ein Rechner oder ein Programm, der/das Funktionen anderer Rechner oder Programme nutzt.
Cluster	Ein Zusammenschluss von Ressourcen wie Server oder Dienste, der parallele Verarbeitung ermöglicht, während nach außen nur ein geschlossenes System sichtbar ist.
Content Management System	Ein IT-System zur kollaborativen Erstellung und Pflege von publizierten Inhalten, häufig im Kontext von Webseiten.
Cookie	Eine lokal auf dem Rechner eines Web-Nutzers gespeicherte Datei mit Informationen über besuchte Webseiten, etwa zur Authentifizierung.
Customizing	Die Anpassung eines generischen Produkts an die speziellen Anforderungen eines konkreten Einsatzes.
Fail-Over	Ein Sicherheitskonzept für IT-Systeme, in dem durch redundante Komponenten ein gewisses Maß an Ausfallsicherheit gewährleisten wird.
Framework	Eine Rahmenstruktur bei der Anwendungs-Programmierung, mit der Komponenten, Laufzeitumgebungen sowie Bibliotheken vorgegeben werden können.
Human Tasks	Aufgaben, die manuell und nicht automatisiert erfolgen.
IF-THEN-Regelset	Die Gliederung von (Geschäfts-)Regeln in zwei Komponente "IF" und "THEN, bei der die "IF"-Elemente Bedingungen und die "THEN"-Elemente von den Bedingungen abhängige Konsequenzen darstellen.

Inbound Nachricht	Im Kontext der Kommunikation zwischen Anwendungen eine bei der empfangenden Anwendung eingehende Nachricht.
Level of Assurance	Ein Maß für die Vertrauenswürdigkeit eines Identitätsprüfungsprozesses.
Loadbalancer	Ein Mechanismus zur Verteilung der Anfrage-Auslastung auf mehrere parallel betriebene Systeme.
Logging	Die automatische Protokollierung von Ereignissen in Software-Systemen.
Log-Level	Die Selektivität der Kriterien zur Bestimmung der Relevanz von Ereignissen für die Protokollierung, etwa "alle" oder "nur Fehler".
Look&Feel	Die Beschreibung des Designs von Benutzeroberflächen hinsichtlich der grafischen Umsetzung von Elementen sowie deren Verhalten.
Mapping	Die Abbildung von Elementen einer Grundmenge auf eine Zielmenge, etwa bei der Zuordnung von Rechnungen zu Empfängern.
Middleware	Zusätzliche Programmschicht in komplexen IT-Systemen, die der Kommunikation zwischen verteilen Anwendungen dient.
One Stop Government	Eine zentrale Stelle, an der Bürger alle anfallenden bürokratischen Vorgänge erledigen können.
Outbound Nachricht	Im Kontext der Kommunikation zwischen Anwendungen eine von der sendenden Anwendung ausgehende Nachricht.
Push-Mechanismus	Ein Vorgehen bei der Übertragung von Daten, bei dem der Datensender den passiven Datenempfänger über Änderungen informiert.
Queue	Eine auch als Warteschlange bezeichnete Datenstruktur, in der die Daten nach der Reihenfolge ihrer jeweiligen Ablage gespeichert und wiedergegeben werden.
Roadmap	Eine Strategie bzw. ein Plan für ein durchzuführendes Projekt.

Routing	Bestimmung der zu nehmenden Wege bei der Übermittlung von Nachrichten in vernetzten Rechnersystemen.
Scriptsprache	Eine Programmiersprache zur Umsetzung kleiner Anwendungen, deren Code in einer Laufzeitumgebung ausgeführt wird.
Security	Die Gewährleistung von Schutzzielen wie Vertraulichkeit, Verfügbarkeit und Integrität bei informationsverarbeitenden Systemen.
Server	Ein Rechner oder ein Programm, auf den/das andere Rechner oder Programme zugreifen können, um dessen zur Verfügung gestellte Funktionen zu nutzen.
Service	Eine IT-Komponente, die bestimmte Funktionen über Schnittstellen anbietet.
Single Sign-On	Ein Authentifizierungskonzept, welches im Anschluss an eine einmalige Authentifizierung die Nutzung einer Vielzahl von Diensten ermöglicht.
Store-And-Forward	Ein Ansatz bei der Vernetzung von Systemen, bei dem die Kommunikation über zwischengeschaltete Warteschlangen erfolgt, um eine fehlerfreie Kommunikation auch bei temporären Netzwerkausfällen zu gewährleisten
Token	Ein Software- oder Hardware-Merkmal zur Identifizierung und Authentifizierung von Anwendern in IT-Systemen.
User Story	Eine kurze Umschreibung einer Software-Anforderung in für Anwender leicht verständlicher Sprache.
Webformular	Ein Formular in einer Webanwendung oder einer Webseite, über welches Daten erfasst werden.
Webportal	Ein Anwendungssystem, das sich durch die Integration von Anwendungen, Prozessen und Diensten auszeichnet.
Webservice	Eine technische Lösung für die automatische Kommunikation zwischen Computern.

Web-Upload	Die Übertragung von lokalen Daten auf einen entfernen Computer über einen Webbrowser.
Whitelist	Eine Liste von Elementen, die bei der Filterung von Daten in jedem Fall akzeptiert werden sollen, etwa E-Mail-Adressen bei Spam-Filtern.
Workflow	Die Abfolge von Arbeitsvorgängen sowie die dazugehörigen Zuständigkeiten und Beziehungen zwischen Beteiligten.

Abkürzungen

API	Eine Schnittstelle, über die ein Anwendungsprogramm anderen IT-Systemen Funktionalitäten zur Verfügung stellt.
AS2	Ein Standard für die gesicherte Übertragung von Nachrichten über Rechnernetzwerke.
AS4	Ein Standard für die elektronische Übertragung von Nachrichten zwischen Unternehmen, der auf AS2 aufbaut (siehe auch "AS2").
BPEL	Ein Standard zur XML-basierten Spezifikation von Geschäftsprozessen.
BPMN	Ein Standard zur graphischen Modellierung von Geschäftsprozessen.
CEF	Ein Förderprogramm der Europäischen Union für Infrastruktur im Bereich Verkehr, Energie und Telekommunikation.
CEN	Das Europäische Komitee für Normung, welches technische Normen für den europäischen Wirtschaftsraum entwickelt, darunter die CEN-Norm für elektronische Rechnungen.
CSV	Ein Dateiformat für Textdateien, bei denen die Daten lediglich einfach strukturiert und einzelne Felder etwa durch Kommata getrennt werden.
eAT	Ein elektronischer Aufenthaltstitel in Scheckkartenformat, der dem Nachweis des Aufenthaltsrechts von Ausländern in Deutschland sowie in der Europäischen Union dient.
EGVP	Ein deutscher Standard zur elektronischen Kommunikation zwischen Gerichten und Behörden.
eID	Die Online-Ausweisfunktion des deutschen Personalausweises, mit der eine Identifizierung im Internet und an Bürgerterminals möglich ist.

EJB	Eine Standardkomponente im Kontext der Plattform "Java EE" (siehe auch "Java EE").
ERP-System	Eine komplexe Software oder eine Vielzahl von miteinander kommunizierenden Anwendungssoftwaren bzw. IT-Systemen, die zur Unterstützung der Ressourcenplanung des gesamten Unternehmens eingesetzt werden.
J2EE	Eine standardisierte Sammlung von Programmbibliotheken der Programmiersprache Java, aufbauend auf Java SE (siehe auch "Java", "Java SE").
Java	Eine verbreitete objektorientierte Programmiersprache, die sich unter anderem durch Plattformunabhängigkeit auszeichnet.
Java SE	Eine standardisierte Sammlung von Programmbibliotheken der Programmiersprache Java (siehe auch "Java").
JavaScript	Eine Programmiersprache, die vor allem im Kontext von Webanwendungen für dynamische Nutzerinteraktionen genutzt wird (siehe auch "Scriptsprache").
JDBC	Eine Datenbankschnittstelle für den Datenbankenzugriff in Java-Anwendungen (siehe auch "Java").
JEE	(siehe "J2EE")
JMS	Eine Programmierschnittstelle für den Nachrichtenaustausch in Java-Anwendungen (siehe auch "Java").
JRE	Eine Ausführungsumgebung, in der Java-Anwendungen ausgeführt werden (siehe auch "Java").
JSP	Eine Programmiersprache für Webanwendungen, die auf der Einbindung von Java-Programmen in Webseiten basiert (siehe auch "Java").
LDAP	Ein Protokoll für den Zugriff auf Verzeichnisdienste in Rechnernetzwerken.

nPA	Der neue Personalausweis, der im Jahr 2010 eingeführt wurde.
OSCI	Netzwerkprotokolle für den Datenaustausch in der öffentlichen Verwaltung in Deutschland.
PDF	Ein plattformunabhängiges Dateiformat für Dokumente, das vom Unternehmen Adobe Systems entwickelt und 1993 veröffentlicht wurde.
PHP	Eine Programmiersprache, die vor allem für dynamische Webanwendungen genutzt wird (siehe auch "Scriptsprache").
REST	Ein Programmierparadigma für verteilte Systeme, das als Schwerpunkt auf die Maschine-zu-Maschine-Kommunikation zielt.
SAML	Eine Auszeichnungssprache für die Kommunikation von Informationen mit Bezug zu Autorisierung, Authentifizierung oder anderen Sicherheitsaspekten.
SCIM	Ein Protokoll für den automatisierten Austausch von Information über Benutzeridentitäten zwischen IT-Systemen.
Servlet	Eine Webserver-Anwendung zur Bearbeitung von Webseiten-Anfragen, welche in Java-Code geschrieben ist (siehe auch "Java").
SMTP	Ein Protokoll für den Versand von E-Mails in Rechnernetzwerken.
SOA	Ein Entwurfsmuster für die Architektur verteilter IT-Systeme, bei der die Strukturierung um Dienste herum zentral ist.
SOAP	Ein Netzwerkprotokoll zum Datenaustausch zwischen Systemen.
SPML	Eine Auszeichnungssprache für die Kommunikation von Informationen bezüglich Benutzer-, Ressourcen- und Dienste-Bereitstellung zwischen vernetzten Organisationen.
SQL	Eine formale Sprache zur Nutzung relationaler Datenbanken.

TLS	Ein hybrides Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet.
TREATS	Projekt zur Erweiterung der Online-Ausweisfunktion des deutschen Personalausweises für eine europaweite Interoperabilität.
UBL	Eine Spezifikation für standardisierte E-Business-Dokumente (z. B. Rechnung oder Bestellung).
UN/CEFACT	Eine UN-Institution mit dem Ziel, den internationalen Handel zu vereinfachen sowie Transparenz und Effektivität zu fördern.
URL	Ein Standard zur Lokalisierung von Ressource, bspw. im Web zur Adressierung von Webseiten.
VPF	Virtuelle Postfächer in der Multikanal-Kommunikationsplattform von Governikus (siehe "Governikus MultiMessenger").
XHTML	Eine Weiterentwicklung von der Auszeichnungssprache HTML, die konform zu den Regeln der XML-Syntax ist.
XML	Eine Auszeichnungssprache zur Darstellung hierarchisch strukturierter Daten in Form von Textdateien.
XTA	Ein vom IT-Planungsrat beauftragter Interoperabilitätsstandard.

Eigenwörter

De-Mail	Ein auf E-Mail-Technik beruhendes, hiervon aber technisch getrenntes Kommunikationsmittel zur „sicheren, vertraulichen und nachweisbaren" Kommunikation im Internet.
eAkte	Elektronische Aktenführung in der öffentlichen Verwaltung.
eDelivery	Ein CEF-gefördertes Projekt, das öffentlichen Verwaltungen hinsichtlich eines sicheren Austausches elektronischer Daten hilft (siehe auch "CEF").
E-Postbrief	Ein Internetdienst der Deutschen Post für den Austausch elektronischer Nachrichten.
eRechnung	Elektronische Rechnung. Gemäß EU-Richtlinie definiert als Rechnung, die in einem strukturierten elektronischen Format ausgestellt, übermittelt und empfangen wird, das ihre automatische und elektronische Verarbeitung ermöglicht.
Ersetzendes Scannen	Elektronische Erfassung von Papierdokumenten sowie Weiterverarbeitung des entstehenden elektronischen Abbildes bei späterer Vernichtung des Papieroriginale.
FMS	Das Produkt Formular Management System der Firma Lucom GmbH zur webbasierten Erfassung unterschiedlicher Formulare.
Governikus	Eine IT-Anwendung für die öffentliche Verwaltung in der Bundesrepublik Deutschland, die von der Governikus KG entwickelt wird.
Governikus Autent	Eine IT-Lösung zur Authentisierung mittels elektronischer Identitäten für die öffentliche Verwaltung in der Bundesrepublik Deutschland, die von der Governikus KG entwickelt wird.
Governikus MultiMessenger	Eine Multikanal-Kommunikationsplattform für die öffentliche Verwaltung in der Bundesrepublik Deutschland, die von der Governikus KG entwickelt wird.
ITZBund	Das Informationstechnikzentrum Bund, welches als IT-Dienstleister zur Konsolidierung der IT des Bundes beitragen soll.

KoGIs	Das Kompetenzzentrum für die Gestaltung der Informationssysteme der Senatorin für Finanzen Bremen.
LIP	Das Produkt Lucom Interaction Plattform der Firma Lucom GmbH, welches die Basis für das Formular Management System bildet.
XRechnung	Spezifikation der deutschen Verwaltung zur Regelung der Entgegennahme elektronischer Rechnungen auf der semantischen Ebene.

Gesetze, Verordnungen, Richtlinien

Allgemeines Gleichbehandlungsgesetz (AGG)	Deutsches Bundesgesetz zur Verhinderung oder Beseitigung verbotener Diskriminierung.
Barrierefreie Informationstechnik Verordnung (BITV)	Deutsche Bundesrechtsverordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz.
Behindertengleichstellungsgesetz (BGG)	Deutsches Bundesgesetz zur Gleichstellung von Menschen mit Behinderungen.
BildscharbV	Deutsche Bundesrechtsverordnung über Sicherheit und Gesundheitsschutz bei der Arbeit an Bildschirmgeräten.
BremBITV	Bremische Barrierefreie Informationstechnik-Verordnung.
DIN EN ISO 9241	Internationaler Standard zur Ergonomie der Mensch-System-Interaktion.
eIDAS	EU-Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen.
ISO 25010	Internationaler Standard zu Leitlinien für die Bewertungen von Softwareprodukten.
Onlinezugangsgesetz (OZG)	Geplantes deutsches Bundesgesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen.
prEN	Eine Europäische Norm im Entwurfsstadium.
SigG	Deutsches Bundesgesetz über Rahmenbedingungen für elektronische Signaturen.
Sozialgesetzbuch IX (SGB IX)	Deutsches Neuntes Buch Sozialgesetzbuch - Rehabilitation und Teilhabe behinderter Menschen.

TR-03107-1	Technische Richtlinie des BSI zu elektronischen Identitäten und Vertrauensdiensten im E-Government.
TR-ESOR	Technische Richtlinie des BSI zur Beweiswerterhaltung kryptographisch signierter Dokumente.
TR-Resiscan	Technische Richtlinie des BSI zu ersetzendem Scannen (siehe auch "Ersetzendes Scannen").