



Bundesministerium
des Innern
und für Heimat



Schnittstellenbeschreibung BundID (Nutzerkonto des Bundes)

Basisdienst ID und Postfach-Nachricht

16. Mai 2025



Überblick über das Dokument

Name des Dokuments	Schnittstellenbeschreibung BundID (Nutzerkonto des Bundes) Basisdienst ID und Postfach-Nachricht
Dokument-Version	1.0
Release-Version	10.2.0.0
Zweck des Dokuments	Beschreibung der Schnittstellen zum BundID Identity Provider sowie Beschreibung der Schnittstelle für den Nachrichtenversand an das Postfach in der BundID
Herausgebende Stelle	Bundesministerium des Innern und für Heimat DVI5
Stand	16.05.2025

Zusammenfassung

Im ersten Teil dieses Dokumentes (Kapitel 1-10) werden die derzeit für Fachportale existierenden Schnittstellen zum BundID Identity Provider beschrieben. Über diese Schnittstelle können Online-dienste und Fachverfahren die Authentifizierung von Nutzenden über die BundID ansteuern.

Im zweiten Teil des vorliegenden Dokumentes (Kapitel 11-16) wird die Schnittstelle für den Nachrichtenversand an das Postfach in der BundID beschrieben. Diese Schnittstelle bietet externen Online-diensten und Fachverfahren die Möglichkeit, Nachrichten in das Postfach eines bestimmten Nutzers abzulegen.

Versionshistorie

BundID – Basisdienst ID und Postfach-Nachricht (Zusammengeführtes Dokument)

Version	Beschreibung	Datum
0.94	Übernahme, Überarbeitung und Zusammenführung der AKDB-Dokumente	11.12.2019
0.95	Endabnahme	18.12.2019
0.97	Endabnahme	06.01.2020
0.98	Endabnahme	08.01.2020
0.99	Endabnahme	09.01.2020
1.0	Freigabe	16.01.2020
1.1	Zusatz UK Schnittstelle	11.03.2020
1.2	ITZBund Abnahme	03.04.2020
1.3	Korrekturen	15.05.2020
1.4	Korrekturen Verweise	18.05.2020
1.5	Korrekturen	05.06.2020
1.6	Korrekturen Verweise	22.06.2020
1.7	Korrektur 1 Schema Dateien	22.09.2020
1.8	Korrektur 2 Schema Dateien	24.09.2020
1.9	Kapitel Sondersituation Unternehmenskonto [...] entfernt, Korrekturen Kap. 11, 12	02.10.2020
2.0	Erweiterungen in Kap. 5 und Kap. 6	10.11.2020
2.01	Korrekturen Kap 5. und Kap. 6	13.11.2020
2.02	Überarbeitung Kap 7.2 und Kap 8.4	11.02.2021
2.03	Korrekturen	16.02.2021
2.04	Entfernung „Künstlername“; Einarbeitung STORK-QAA-Level-3; Überarbeitung BSP-Quittung	11.03.2021

3.01	Ergänzung um Changes aus Release 3.1.0, redaktionelle Korrekturen, Entfernung Organisationskonto, Aufnahme Kap. 5.2 und 5.3, Anpassung Attribute in Kap. 6.1 und entspr. Hinweise, Entfernung Kap. 7, Kap. 8.3 ist obsolet, Aufnahme OZG-Hinweis in Kap. 11.2.5, Aufnahme Kap. 13 und 14	09.04.2021
3.02	Qualitätssicherung	20.04.2021
3.03	Korrektur technischer Begriff Postfach zu Postkorb	30.04.2021
3.2.0	Ergänzung um Changes Release 3.2.0.0, Kapitel 11.1.2, Kapitel 11.2.6 (Tabelle 9005), Kapitel 11.2.7	20.05.2021
3.2.1	Ergänzung um Changes Release 3.2.1.0, Kapitel 6.1, Kapitel 6.2.2, Kapitel 7.2, Kapitel 11.2.4	06.08.2021
3.2.1.1	Hotfix	09.09.2021
3.2.1.2	Hotfix und Aktualisierung 15.6.1 bspnachrichten-2.13.xsd	16.09.2021
4.0.0.0	Anpassung zu Release 4.0.0.0, Kapitel 6.2.6; Kapitel 8.3; Kapitel 9 eingefügt	16.11.2021
4.0.1.0	Kapitel 6 Hinweise zu Friendly Names, Kapitel 9.2 eingefügt	10.12.2021
4.0.1.0	Anpassung Logo und Bezeichnung BMI, Qualitätssicherung	21.12.2021
5.0.0.0	Überarbeitung Kapitel 8.3 und Kapitel 9 gesamt	04.04.2022
N/A	Qualitätssicherung	05.05.2022
5.0.2.0	Überarbeitung 6.1 und 9.1, Einarbeitung Kapitel 12.1.3	02.06.2022
N/A	Qualitätssicherung	07.07.2022
N/A	Ergänzung um Kapitel 10 SAML-Beispiele, Überarbeitung Kapitel 11.2, Trennung SAML-Response Beispiele als Anhang 1 zur Schnittstellenbeschreibung	12.08.2022
N/A	Qualitätssicherung	18.08.2022

N/A	Redaktionelle Änderungen, Kapitel 9.4 eingefügt, Korrekturen Kap. 5.4 und 6.2.5	27.01.2023
N/A	Entfernung Kapitel 17.4, Qualitätssicherung	23.02.2023
N/A	Link unter Kapitel 6.1, Seite 20 aktualisiert	04.05.2023
N/A	Entfernung bPK, Version 1, Überarbeitung Kapitel 5.1, 6.1, 6.2.2, 7.2, 9.2, 9.4, 9.5	07.08.2023
N/A	Layout	17.10.2023
N/A	Überarbeitung Kapitel 9.2.1, 9.2.2, 9.4, Erweiterungen in Kapitel 6.1, 6.2.1, 9., 9.5, Aufnahme Kapitel 9.6 und 9.7	16.11.2023

Bitte beachten Sie, dass ab Mai 2024 eine neue Form der Dokumenten-Versionierung angewendet wird. Fortan gilt die Release-Version der Software als führend. Die Dokument-Version bezieht sich auf die für das Release geltende Schnittstellenbeschreibung und beginnt somit bei einem neuen Major-Release mit Version 1.0. Sollte es innerhalb eines Major-Releases zu Anpassungen in der Schnittstellenbeschreibung kommen, folgt Dokument-Version 2.0.

Release-Version	Dokument-Version	Beschreibung	Datum
9.0.0.0	1.0	Überarbeitung Kapitel 6, 6.1, 6.2.6, 7.1, 7.2 (Metadaten), 8.1, 8.2, 9, 9.3, 9.4, 13, 14, Erweiterung Kapitel 6.2.7, 6.2.8, Entfernung Kapitel 7.2 (Zusätzliche Metadaten) und 8.3	23.05.2024
9.0.0.0	2.0	Anpassung Kapitel 6.1 (Staatsangehörigkeit und Dokumententyp)	12.06.2024
9.1.0.0	1.0	Überarbeitung Kapitel 5.1, 5.5, 6.1, 9.4, Erweiterung Kapitel 2.1, 6.2.1, 6.2.2, 10.1, 10.2	26.09.2024
9.1.0.0	2.0	Anpassung Kapitel 6.2.1, 6.2.2	12.11.2024
10.1.0.0	1.0	Anpassung Kapitel 5, 5.3, 5.5, 6.2.8, 7.1, 9.2, 9.5	17.04.2025

10.1.0.0	2.0	Korrekturen Kapitel 6.1	06.05.2025
10.2.0.0	1.0	Ergänzung Kapitel 6.2.10, Anpassung Kapitel 9	16.05.2025

Inhaltsverzeichnis

Zusammenfassung	1
Versionshistorie	2
1 Einleitung	10
2 Das Bundesportal – eine offene Infrastruktur für Fachportale öffentlicher Verwaltungen	11
2.1 Sichere Kodierung und Integration der BundID	11
3 Übersicht über die Funktionsweise der offenen Infrastruktur	13
4 Unterstützte Anwendungsfälle	17
4.1 Anwendungsfall 1 – direkte Token-Nutzung	17
4.2 Anwendungsfall 2 – indirekte Token-Nutzung.....	17
5 Unterstützte Authentisierungsverfahren und Anfragearten	19
5.1 Auswahl bestimmter Authentisierungsverfahren	20
5.2 Besonderheiten bei der Nutzung von interoperablen Nutzerkonten.....	20
5.3 Besonderheiten bei der Nutzung der Methode "Temporär Login"	21
5.4 Kryptographische Vorgaben	21
5.5 Verwendung von Keycloak.....	22
6 Attribute im SAML-Token	23
6.1 Personenbezogene Stammdaten	23
6.2 Technische Nutzdaten.....	27
6.2.1 bPK – bereichsspezifisches Personenkennzeichen	27
6.2.2 bPK2 – bereichsspezifisches Personenkennzeichen.....	28
6.2.3 Vertrauensniveau	29
6.2.4 Version	30
6.2.5 AssertionProvedBy.....	31
6.2.6 Postkorb-Handle.....	31

	7
6.2.7 Application ID (Antrags-ID)	32
6.2.8 Pseudonym	32
6.2.9 Vertrauensniveau der Attribute	33
6.2.10 SAML-Attribut für Zwei-Faktor-Authentifizierung	33
7 Betriebsvoraussetzungen	34
7.1 Infrastruktur	34
7.2 Metadaten	34
8 Entscheidungsunterstützung und Handreichungen	35
8.1 Architekturüberlegungen bei Auswahl eines SAML-Bindings.....	35
8.2 Zurückleiten in die Drittanwendung bei Abbruch durch Benutzer.....	35
9 Konfiguration der Anfrage	37
9.1 Einschränkung des Authentifizierungsverfahren	37
9.2 Anforderung von Pflichtattributen.....	38
9.2.1 Technische Attribute vom Servicekonto und die Authentifizierungsverfahren....	40
9.2.2 Validieren von RequestedAttributes im SAML Request.....	41
9.2.3 Validieren von RequestedAttributes vor dem Absenden.....	41
9.3 Implementierungsanleitung BundID-Weiterleitung Modaldialog.....	41
9.3.1 Implementierungsbeispiel	45
9.4 Übergabe von UI-Information	47
9.5 Übergabe von UI-Informationen (ab Release 6).....	47
9.6 Verwendete Fehlercodes am IDP bei unerwarteten SAML-Requests	49
9.7 Erweiterte Fehlermeldung im SAML-Response.....	50
10 Beispiele für SAML-Requests und SAML-Responses	51
10.1 Beispiele für SAML-Requests	51
10.2 Beispiele für SAML-Responses (entschlüsselter Bereich).....	54
11 Postfach-Nachricht an die BundID	57
11.1 Topologie.....	57

	8
11.2 SOAP-Web-Service.....	59
11.3 Adressierung des Bürgers (Postkorb-Handle)	59
12 Das Format der Postfach-Nachricht	61
12.1 Besondere Hinweise	61
12.1.1 NachrichtenKopf	61
12.1.2 NachrichtenInhalt.....	62
12.1.3 BSP-Quittung.....	64
12.1.4 Validierung Nachrichten-Inhalt.....	64
12.2 Beispiel einer Postfach-Nachricht.....	65
12.2.1 Schlüsseltabellen.....	66
13 Web-Service-Schnittstelle	70
13.1 Die WSDL Operation <code>sendBspNachrichtNative</code>	70
13.1.1 Beispiel-Requests und -Responses für den Webservice.....	71
13.2 Die WSDL Operation <code>sendBspNachricht</code>	72
13.2.1 OK.KOMM-Nachrichtenformat.....	73
13.2.2 Beispiel für ein OK.KOMM Nachrichtenformat	74
13.2.3 OK.KOMM-Antwort.....	75
13.2.4 Beispiel-Requests und -Responses für den Webservice.....	76
14 Absicherung der Schnittstelle	80
14.1 Two-Way-SSL Client Authentifizierung.....	80
15 Anhänge und Verzeichnisse	81
15.1 Abbildungen	81
15.2 Verweise auf externe Dokumente	81
15.3 Verwendete Abkürzungen.....	81
15.4 Annex: Webservice Schema Dateien.....	83
15.4.1 Schemadatei – <code>bspnachrichten-2.13.xsd</code>	83

		9
15.4.2	Schemadatei – bspnachrichten-schluesseltabellen-2.10.xsd	91
16	Quellen	99

1 Einleitung

Die BundID bildet über eine offene Infrastruktur mit den beteiligten Systemen den Portalverbund.

Die Bürgerinnen und Bürger legen sich eine individuelle BundID zu und verwalten dort Ihre persönlichen Daten und Zusatzinformationen. Die Befüllung der personenbezogenen Datenfelder für die BundID erfolgt entweder über die freiwillige Angabe (bei Nutzung von Benutzername/Passwort-Paar) oder automatisiert bei der erstmaligen Nutzung z.B. mittels des Online-Ausweises.

Fachportale als Drittanwendungen im Portalverbund binden sich über definierte Standardprotokolle mittelbar an das Bundesportal an und profitieren im Sinne der Datensparsamkeit von der zentralisierten Verwaltung der personenbezogenen Nutzerdaten in der BundID.

In diesem Dokument werden die derzeit für Fachportale existierenden Schnittstellen zum BundID Identity-Provider beschrieben.

2 Das Bundesportal – eine offene Infrastruktur für Fachportale öffentlicher Verwaltungen

Ausgewählte personenbezogene Daten aus dem Basisdienst „Nutzerkonto“ stehen im Rahmen einer offenen Infrastruktur auch einem weiteren Kreis an Drittanwendungen außerhalb des eigentlichen Bundesportals zur Verfügung (s. Kp. 8 – Entscheidungsunterstützung und Handreichungen).

Diese offene Infrastruktur basiert auf international anerkannten, quell-offenen Standardtechnologien [1] und sichert die Drittanwendungen gegen unberechtigte Zugriffsversuche (d. h. ohne vorherige Autorisierung durch die ordnungsgemäßen Benutzer) ab. Die von den Bürgerinnen und Bürgern dafür zu nutzenden Authentisierungsinformationen (u. a. Benutzername/Passwort, ePA-Pseudonym) sind identisch mit jenen, die für die BundID im Bundesportal hinterlegt sind, so dass eine erneute Registrierung in den angebundenen Drittanwendungen hinfällig ist.

Die an der BundID teilnehmenden Online-Leistungen werden dann „Service-Provider“ genannt und verbleiben daher nicht nur in der rechtlichen, sondern auch in der operativen Zuständigkeit derjenigen Körperschaft, in deren Namen die Dienstleistung den Bürgerinnen und Bürgern angeboten wird. Der Fortbestand eigener Web-Angebote erweist sich insbesondere in jenen Fällen als sinnvoll, in denen ein hohes Maß an systemischer Komplexität gefordert oder das vorrangige Augenmerk auf den Schutz von langfristig getätigten, strategischen IT-Investitionen gelegt wird.

Die Auslagerung des Zugriffsschutzes der Drittanwendungen an Komponenten des Portalverbunds erfordert allerdings einen, je nach Technologiestand des Service-Providers, nicht geringen Eingriff in die bisherige Funktionsweise der Web-Anwendung. Aus technologischer Sicht lassen sich neu aufzubauende oder bestehende Applikationen die bereits mit ähnlichen Standards wie OASIS SAML versehen sind, mit geringerem Aufwand in den Portalverbund aufnehmen als jene Anwendungen, die anders geartete Zugriffskontrollmechanismen (wie z. B. Kerberos) nutzen.

2.1 Sichere Kodierung und Integration der BundID

Die BundID ist integraler Bestandteil eines umfassenden Systemverbunds und übernimmt dabei die Funktion eines Identity Providers (IdP). Gegenüber dem Bürger ist die BundID ein wichtiger Vertrauensanker. Mit zunehmender Nutzung und Bekanntheit ist davon auszugehen, dass das System auch als Angriffsziel an Beliebtheit gewinnt. Deshalb empfehlen wir dringend darauf zu achten, Sicherheitsrichtlinien, wie z. B. zum Thema der sicheren Entwicklung, zu beachten und einzuhalten.

Neben den technischen Richtlinien des BSI, wie beispielsweise der BSI TR-03172-3, die Anforderungen zur sicheren Bereitstellung von Online-Verwaltungsleistungen beschreibt, möchten wir auch auf die OWASP-Empfehlungen hinweisen. Hier bieten beispielsweise die OWASP Secure Coding Practices, die OWASP Top Ten (häufigste Web-Sicherheitsrisiken) und der OWASP Developer Guide wertvolle Orientierung.

Unterstützung im Entwicklungsprozess kann darüber hinaus die Secure Developer Checklist bieten, die zur Definition sicherheitsrelevanter Kriterien, etwa in Scrum-Prozessen, genutzt werden kann. Für spezifische Anwendungsfälle, wie das SAML-basierte Single-Sign-On (SSO), ist das SAML Security Cheat Sheet eine hilfreiche Quelle.

Durch die Beachtung und Einhaltung dieser Sicherheitsvorgaben – von OWASP und BSI bis hin zu weiteren relevanten Standards – wird das Risiko von Sicherheitsvorfällen deutlich reduziert und die Integrität des Gesamtsystems bei der Integration der BundID nachhaltig gesichert.

3 Übersicht über die Funktionsweise der offenen Infrastruktur

Im Detail stellt die Übersichtsgrafik den Authentisierungs- und Autorisierungsvorgang von Dienstnutzern im Zusammenspiel mit der offenen Infrastruktur und einer daran angebundenen Drittanwendung dar. Der abgebildete Ablauf in sieben Teilschritten folgt den international weitverbreiteten Standards der OASIS Group, wie sie auch im Kern der eCard-API des bundesdeutschen elektronischen Identifikationsmittel (ePA, eAT, EU-Karte) zum Einsatz gelangen (https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03130/TR-03130_node.html).

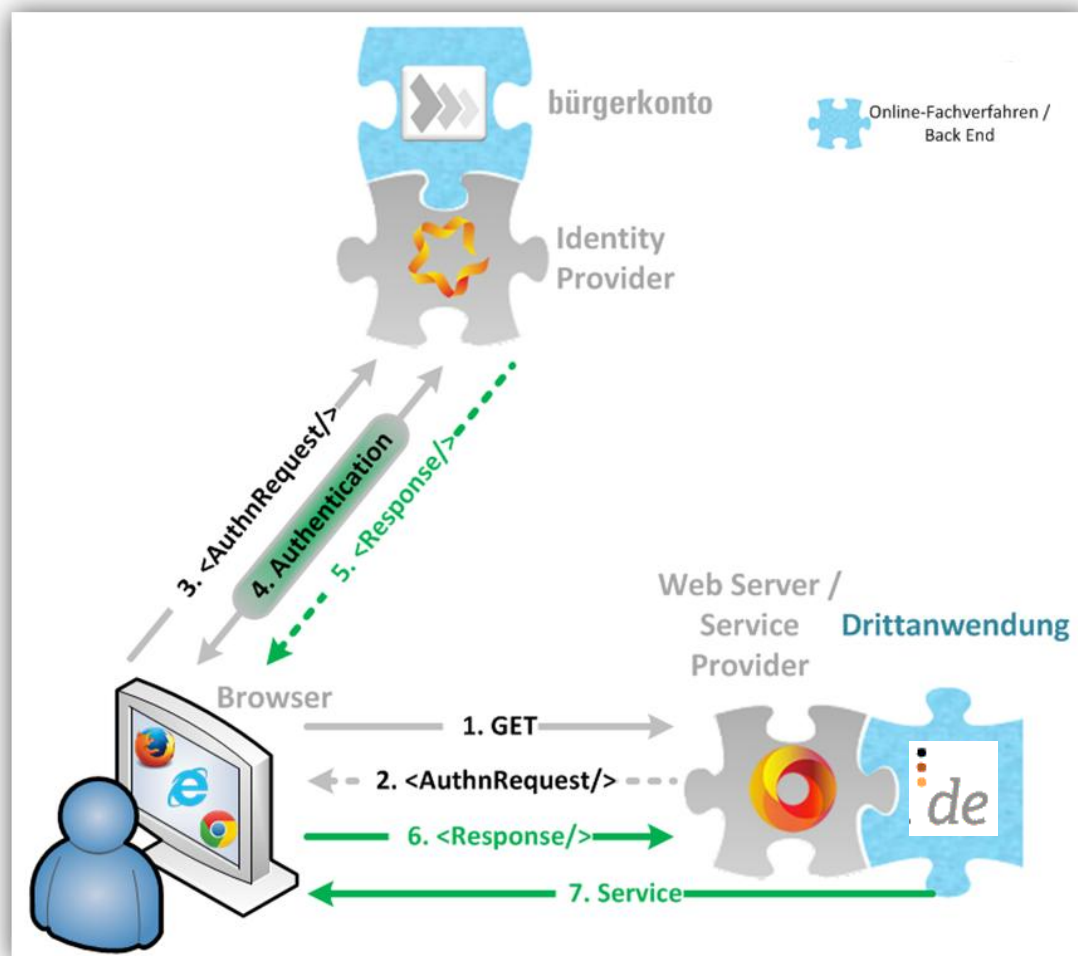


Abbildung 1: Zusammenspiel der Komponenten in der offenen Infrastruktur des Portalverbunds

Die einzelnen Teilschritte sind nur vereinzelt für die Dienstnutzer wahrnehmbar (wie aus den Screenshots ersichtlich) und erleichtern so die Handhabung des komplexen Authentisierungs- und Autorisierungsvorgangs:

Solange der Benutzer nicht authentisiert wurde, kann lediglich auf die öffentlich zugänglichen Bereiche der Service-Provider-Applikation zugegriffen werden. Sobald eine zugriffsgeschützte Ressource im Web-Angebot der Drittanwendung angefragt werden sollte, wird der Zugriffsversuch auf Seiten des Service-Providers abgefangen (Schritt 1).

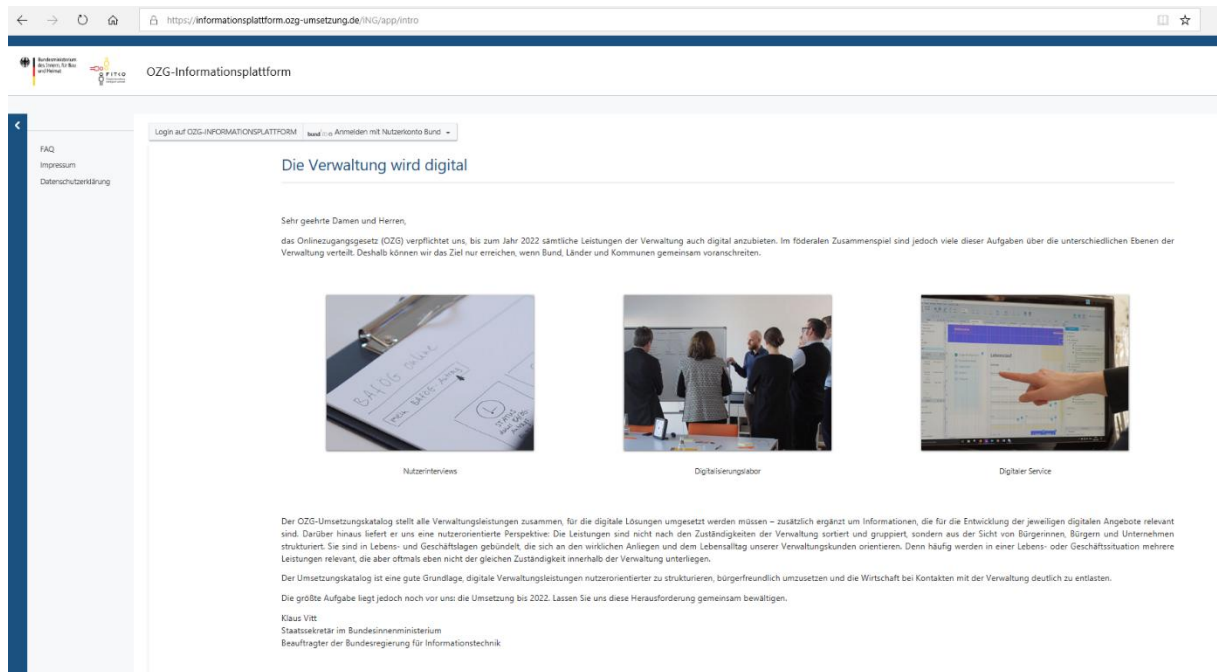


Abbildung 2: Öffentlich zugänglicher Bereich der Service-Provider-Applikation

Seitens des Fachportals wird daraufhin eine Authentisierungsanfrage an den BundID Identity-Provider als Authentisierungsinstanz gesendet und der Benutzer dorthin umgeleitet. Derzeit geschieht dies in Form eines OASIS SAMLv2-konformen Authentication Requests via HTTP-REDIRECT oder HTTP-POST über den Browser des Benutzers (Schritt 2). Diese Anfrage wird nicht direkt an den Identity Provider versendet, sondern mittelbar über den Browser des Dienstanfragers geleitet (Schritt 3).

Der Identity-Provider fordert nun den Dienstanfrager auf, sich ihm gegenüber durch ein vorkonfiguriertes Authentisierungsverfahren als bekannter Benutzer zu erkennen zu geben: Dies kann z. B. durch den Abgleich von Benutzername und Passwort mit den im Bürgerkonto hinterlegten Daten oder durch die Nutzung der Online-Ausweisfunktion erfolgen. Erst im Zuge einer positiv durchlaufenen Authentisierung (Schritt 4) erfolgt am Identity Provider die Erstellung einer Antwortnachricht, die unter Hinzuhaltung der in der BundID für die Person bzw. die Organisation hinterlegten Daten erweitert wird. Ab diesem Zeitpunkt kann der Dienstanutzer im rechtlichen Sinne als authentisierter Benutzer im Rahmen der Infrastruktur des Portalverbunds gelten.

The screenshot shows the bund ID login interface. At the top is a blue header with the bund ID logo, a search icon, language options (DEUTSCH, HILFE), and a 'KONTO ERSTELLEN' button. The main heading is 'Womit möchten Sie sich anmelden?' followed by a subtext: 'Bitte wählen Sie eine der folgenden Optionen aus, um sich in Ihrem BundID-Konto anzumelden.' Below this are four selection cards: 'Online-Ausweis' (marked 'EMPFOHLEN'), 'EU Identität (nicht deutsch)', 'ELSTER-Zertifikat', and 'Benutzername & Passwort'. The 'Online-Ausweis' card is expanded, showing a 'VERTRAUENSNIVEAU HOCH' label, instructions about using a 'Personalausweis' with the online function, and two expandable sections: 'Was brauche ich dafür?' and 'Ich habe keinen Personalausweis. Welche anderen Ausweise kann ich nutzen?'. At the bottom of the expanded card is an 'ANMELDEN' button. A 'ZURÜCK' link is located at the bottom left of the page.

Abbildung 3: Authentisierung

Die erzeugte Antwortnachricht wird im Hintergrund als SAML-Response verschlüsselt und unter Einberechnung von Zertifikatsinformationen signiert (Schritt 5) an den Browser des potenziellen Dienstanwenders zurückgesendet. Von dort aus wird die SAML-Response an die Drittanwendung weiter durchgestellt. Die Verwendung BSI-konformer Verschlüsselungstechnologien [2] im vorherigen Schritt stellt sicher, dass der Dienstanwender an dieser Stelle keine Möglichkeit zur Vortäuschung oder beabsichtigten Veränderung des Inhalts hat.

Der Service-Provider empfängt die SAML-Response (Schritt 6) und überprüft zunächst die Nachricht auf ihre Authentizität und Integrität hin. Erst dann wird überprüft, ob der Inhalt, der vom Identity Provider stammenden Antwortnachricht den regelbasierten Erfordernissen der Drittanwendung genügt. Erst jetzt ist der authentifizierte Dienstanwender im rechtlichen Sinne auch autorisiert und zugriffsbefugt.

Der Service-Provider gewährt daraufhin den Zugriff auf die zunächst geschützte Ressource und führt die ursprüngliche Zugriffsanfrage aus. Die Antwort wird auf dem zugehörigen Anwendungsserver generiert und an den Browser des Dienstanwenders gesendet (Schritt 7).

Für den Zeitraum der weiteren Sitzung wird fortan die Auslieferung aller weiteren zugriffsgeschützte Ressource(n) je nach Anfrage (und applikationsspezifischem Verhalten) erlaubt.

Darüberhinausgehende Zugriffsrestriktionen (z. B. nach RBAC) sind ausschließlich Teil der Applikationslogik des Fachportals und liegen jenseits des Funktionsumfanges der zur Verfügung gestellten Infrastruktur.

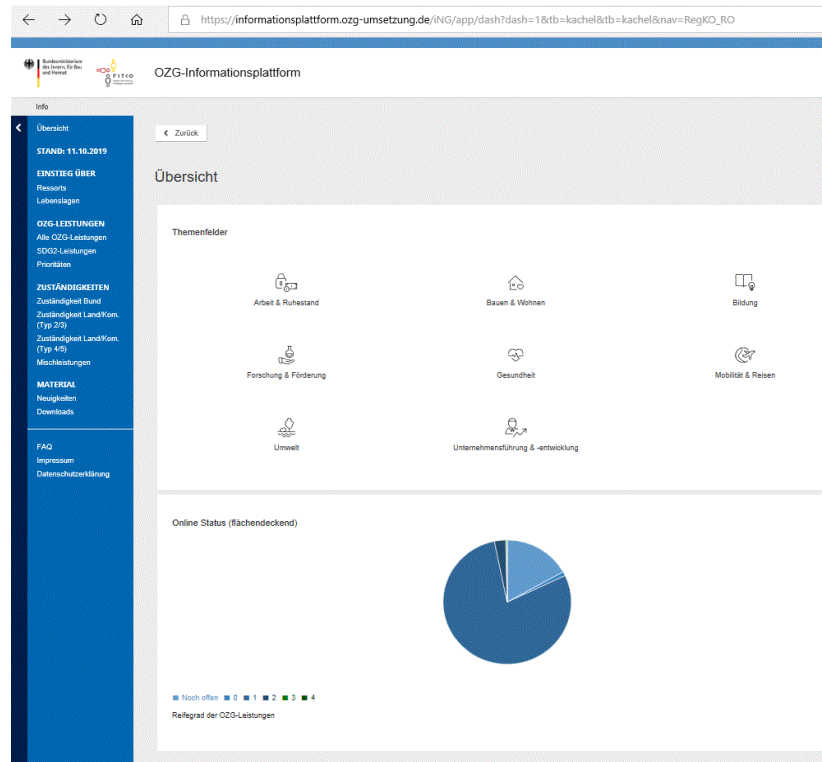


Abbildung 4: Geschützte Ressource – OZG-Informationsplattform

4 Unterstützte Anwendungsfälle

Die Online-Leistungen der Bundesverwaltung schließen sich mittelbar an die BundID an und lagern Ihre Nutzerauthentisierung an die Identity-Infrastruktur aus. Diese Service-Provider müssen als Endpunkt für OASIS SAML v2-Token i. S. d. Web Browser Single-Sign-On-Profile [3] mit HTTP-REDIRECT oder HTTP-POST-Binding fungieren können.

Dies ist allgemein über zwei Wege möglich:

1. Über direkte Token-Generierung und -Nutzung innerhalb der Drittapplikation (z. B. über Open-Source-Bibliotheken)
2. Über indirekte Token-Generierung und -Nutzung mittels Reverse-Proxy (z. B. über konfigurierbare Implementierungen diverser Hersteller)

4.1 Anwendungsfall 1 – direkte Token-Nutzung

Die Drittanwendung kann direkt als Endpunkt für die Erzeugung von Authentication Requests und der Nutzung von SAML-Assertions fungieren. Dafür muss die Anwendung das bereits erwähnte OASIS SAMLv2 Web Browser Single-Sign-On-Profile implementieren.

Bei Wahl dieser ersten Betriebsvariante empfiehlt sich die Nutzung der Open-Source-Bibliothek OpenSAML oder ähnlicher Frameworks. Implementierungsbeispiele zur Nutzung finden sich z.B. im Entwickler-Paket von Governikus-Autent oder in frei verfügbaren Quellen Dritter [4].

4.2 Anwendungsfall 2 – indirekte Token-Nutzung

Erlaubt die Rechenzentrumsinfrastruktur den Betrieb von zusätzlichen Komponenten auf dem der Drittanwendung vorgelagerten Web-Server, bietet sich darüber hinaus die Nutzung von sogenannten Reverse-Proxy-Installationen an, die ihrerseits als Endpunkt des SAML-Protokolls agieren und die entsprechenden Requests und Responses für das Fachportal verarbeiten. Der Service-Provider besteht dann aus der eigentlichen Drittanwendung (dem webbasierten Fachverfahren) und dem vorgeschalteten Reverse Proxy als SAML-v2-Endpunkt.

Bei der Wahl dieser zweiten Betriebsvariante bietet sich die Nutzung von Reverse-Proxy-Produkten an, wie sie von Herstellern wie "ForgeRock" [5] oder "Shibboleth Consortium" [6] zur Verfügung stehen.

Implementierungs- und Konfigurationsbeispiele zur Nutzung finden sich in den öffentlich zugänglichen Produktdokumentationen der jeweiligen Hersteller und sind einzelfallabhängig je nach Drittanwendung und Rechenzentrumsinfrastruktur zu interpretieren.

Die im SAML-Token enthaltenen Attribute werden in Abstimmung mit den Applikationsarchitekten nach erfolgter Anmeldung eines Benutzers als zusätzliche HTTP-Header-Attribute in die Online-Sitzung injiziert und stehen dann der Drittanwendung im folgenden Verlauf der Sitzung zur weiteren Verarbeitung zur Verfügung.

5 Unterstützte Authentisierungsverfahren und Anfragearten

Die BundID verfügt über folgende Authentisierungsmethoden, die auch ein zugehöriges Vertrauensniveau (s. Kapitel 6.2.2 bPK2 – bereichsspezifisches Personenkennzeichen

Da für die Service Provider das Entpacken und das Verarbeiten der bPK eine unnötige Hürde war, wurde die bPK2 eingeführt.

Das bPK (bereichsspezifisches Personenkennzeichen) dient in Anlehnung an die österreichische Bürgerkarten-Infrastruktur zur datenschutzfreundlichen, für die jeweilige Drittanwendung eindeutig geltenden Identifizierung eines Nutzers.

Bezeichnung	FriendlyName	SAML2 Formal Name (URN-notiert)
bPK2	bPK2	urn:oid:1.3.6.1.4.1.25484.494450.3

Bei FINK wird der Identifier aus dem anderen Servicekonto übernommen und mit Prefixen versehen, damit keine Überschneidung mit existierenden bPK2s möglich ist.

Achtung: Sofern das bPK2 durch OD/FV genutzt wird, ist bei der Änderung der URL eines Onlinedienstes (OD) darauf zu achten, dass der Hostname der entityID nicht verändert wird. Eine Änderung des Hostnames der entityID verursacht abweichend generierte bPK2.

Vertrauensniveau

Bezeichnung	Ausgestaltung
Benutzername/Passwort (entspricht Nicht-Vertrauensniveau Basisregistrierung, STORK-QAA-Level-1)	<ul style="list-style-type: none"> • Ein softwarebasiertes Verfahren • Die Registrierung erfolgt einzig durch die BundID • Attribute sind nicht überprüft
ELSTER Zertifikat (entspricht Vertrauensniveau substantiell, STORK-QAA-Level-3)	<ul style="list-style-type: none"> • Ein software-basiertes PKI-Verfahren • Die Registrierung und Nutzung erfolgt in Koordination mit den Systemkomponenten von ELSTER • Attribute sind Melderegister-geprüft

eID (Personalausweis, elektronischer Aufenthaltstitel, Unionsbürgerkarte) (entspricht Vertrauensniveau hoch, STORK-QAA-Level-4)	<ul style="list-style-type: none"> • Ein hardwarebasiertes PKI-Verfahren • Die Registrierung und Nutzung erfolgen in Koordination mit BSI-TR-zertifizierten eID-Servern • Attribute sind Melderegister geprüft
---	---

5.1 Auswahl bestimmter Authentisierungsverfahren

Authentisierungsverfahren können nach Vertrauensniveau gruppiert und im Rahmen des SAMLAuthenticationRequests von einer Drittanwendung angefordert werden (sog. RequestedAuthnContext). Es wird der Comparison-Qualifier „minimum“ unterstützt. Die implizite Einschränkung von Authentisierungsmethoden über den Qualifier „exact“ ist obsolet und wird explizit durch eine Extension im SAML-Request gelöst.

Perspektivisch ist es geplant weitere Authentifizierungsmittel, die gemäß eIDAS-Verordnung notifiziert wurden, anzubinden. Diese können dann für die Authentifizierung auf den jeweiligen Vertrauensniveau-Stufen verwendet werden.

Für den Fall der indirekten Token-Nutzung (s. Kapitel 4.2 Anwendungsfall 2 – indirekte) müssten die Erweiterungen über produktspezifische Konfigurationen vorgenommen werden, so z.B. beim Reverse-Proxy des Herstellers „Shibboleth Consortium“ mittels Templates zum SessionInitiator [7].

Bei der Authentifizierung mit eIDAS liegt uns momentan noch kein Feedback von Service-Providern vor. Des Weiteren ist noch in der Diskussion, welche Art von ID bei einer temporären Anmeldung (ohne permanentes Nutzerkonto) übergeben wird und wie bzw. ob diese später wieder zugeordnet werden kann.

5.2 Besonderheiten bei der Nutzung von interoperablen Nutzerkonten

Im Rahmen des Föderierten Identitätsmanagements Interoperable Nutzerkonten in Deutschland (FINK), ist es möglich, dass die Authentifizierung durch ein Nutzerkonto eines anderen Teilnehmers von FINK durchgeführt wird. Hierbei wird der SAMLAuthenticationRequests an das ausgewählte Nutzerkonto durchgereicht (siehe FINK-Informationsplattform). Das ggfs. vorgegebene Vertrauensniveau

wird dabei mitgegeben, sodass das empfangene Nutzerkonto entsprechend reagieren kann. Im Umkehrschluss reagiert das Nutzerkonto der AKDB gleichermaßen.

Die Attributmenge kann je Nutzerkonto eines Teilnehmers variieren. Sofern ein PersonIdentifier mitgeliefert wird, werden diese Attribute aus Datenschutz-Gründen gefiltert und nicht verarbeitet.

Die Interoperabilität von Postfächern wird zu einem späteren Zeitpunkt bereitgestellt, insofern werden potenziell mitgelieferte Postfachreferenzen ebenfalls gefiltert und nicht verarbeitet.

Für weitergehende Informationen wird auf die Informationsplattform des FINK-Verbunds verwiesen: <https://informationsplattform.efink.services/>

5.3 Besonderheiten bei der Nutzung der Methode "Temporär Login"

Gemäß OZG muss es Nutzenden möglich sein, das Nutzerkonto ohne Langzeitspeicherung von Daten zu verwenden und sich so gegenüber Drittanwendungen authentifizieren zu können. Hierfür bietet das Nutzerkonto die Methode "Temporärer Login", welche am IDP als zusätzliche Methode angeboten wird. Für den temporären Login können alle elektronischen Identifikationsmittel verwendet werden wie bspw. die Online-Ausweisfunktion. Zu beachten ist, dass bei dieser Methode nur Daten ausgelesen und weitergegeben werden. Es erfolgt keine weitergehende Speicherung oder Verarbeitung der Daten. Dies hat zur Folge, dass die technischen Nutzdaten nur bedingt bereitgestellt werden. Insbesondere das Postkorb-Handle und das bereichsspezifische Personenkennzeichen (bPK) entfallen bei dieser Methode.

Sofern eine Drittanwendung ohne diese Daten nicht nutzbar ist, muss das Error-Handling bei der Drittanwendung stattfinden und nicht im Nutzerkonto.

Diia und Benutzername werden nicht als temp. Login angeboten.

5.4 Kryptographische Vorgaben

BSI TR-03116-4 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 4 Stand 2023 wird als Basis verwendet. Dabei wird insbesondere der Punkt Vorgaben für SAML/XML Security betrachtet. Jede Änderung am Nutzerkonto wird versucht, möglichst kompatibel vorzunehmen, jedoch unterstützt nicht zwangsweise jede Appliance jede neue Vorgabe mit ausreichend Vorlauf. Etwaige Probleme kön-

nen damit leider erst in den Integrationstests vor der Produktivsetzung festgestellt werden. Die Vorgaben der TR-03116-4 am NK werden unterstützt, eine Abweichung ohne konkrete Begründung ist nicht vorgesehen. Die gleichen Vorgaben gelten auch für die Onlinedienste. Eine technische Überprüfung, ob die entsprechenden Vorgaben erfüllt werden, ist nicht vorgesehen. Diese Prüfung obliegt den einzelnen Onlineverfahren selbst.

Über die Metadaten können zwar eigene Algorithmen für EncryptionMethod, DigestMethod oder SigningMethod konfiguriert werden. Das Vorgehen ist jedoch nicht unterstützt, da es eine allgemeine Änderung erschwert und bei Self-Service-Portalen zur Verwaltung von Metadaten in der Regel keine Anwendung findet.

Änderungen (genaue Termine hängen vom Rollout der Version ab)

- 2024: Umstellung der Content Encryption auf AES GCM-Mode (XML Security WG namespaces)
- 2024: Umstellung auf RSASSA-PSS als Signaturverfahren (xmldsig-more namespace)

5.5 Verwendung von Keycloak

Wir möchten darauf hinweisen, dass seitens BundID keine Gewähr für die Funktionalität und Kompatibilität bei der Verwendung von Keycloak zwecks Anbindung der BundID übernommen wird.

Dennoch sind wir uns bewusst, dass einige Anbindungen eine Integration per Keycloak anstreben bzw. dies bereits einsetzen. Um dem gerecht zu werden, hat die BundID Keycloak-Behörden-Community einige Informationen zusammengestellt, die Ihnen bei der Umsetzung dieses Vorhabens helfen können. Bitte beachten Sie, dass der Verweis seitens BundID auf die nachfolgenden Anleitungen ohne Gewähr auf Aktualität und Richtigkeit erfolgt. Wir übernehmen keine Haftung für Schäden, die aus der Verwendung dieser Informationen entstehen. Wir empfehlen Ihnen, zusätzlich die von der BundID offiziell unterstützten Anbindungsmechanismen zu nutzen, um eine reibungslose Funktionalität und Kompatibilität sicherzustellen.

Weitere Informationen zur Integration mit Keycloak stehen in folgender externer Dokumentation bereit: <https://github.com/opdt/keycloak-extension-bundid>.

Ergänzend dazu existiert mit dem sogenannten BundID-Simulator ein fachlicher Mock, der die Funktion der BundID nachbildet. Dieser basiert auf der BundID-Spezifikation. Weitere Informationen stehen in folgender externer Dokumentation bereit: <https://github.com/opdt/bundid-simulator>.

6 Attribute im SAML-Token

Derzeit stellt die Identity Infrastruktur die nachfolgend aufgelisteten Attribute aus dem Bürgerkonto zur weiteren Nutzung in Fachportalen im Rahmen von SAML-Assertions zur Verfügung. Die darin übermittelten Daten entsprechen immer dem zum Zeitpunkt der Token-Ausstellung aktuellen Datensatz im Bürgerkonto. Die Daten werden im UTF-8-Zeichensatz NFC-kodiert.

Hinweis:

Entsprechend des verwendeten Protokolls (Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0) <https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf> darf für das Mapping der Attribute nicht das XML Attribut "FriendlyName" verwendet werden, da diese Werte nicht stabil und zudem optional sind. Hierfür ist der SAML2 Formal Name (URN-notiert) zu verwenden, da es sich hierbei um eine gleichbleibende ID handelt.

6.1 Personenbezogene Stammdaten

Die unmittelbar personenbezogenen Stammdaten aus dem Bürgerkonto werden in LDAP-konformer Notation zur Verfügung gestellt. Die Konversion in LDAP-Notation orientiert sich an den IETF-Standards aus RFC 4519[9] und RFC 4524[10].

Bezeichnung	FriendlyName	SAML2 Formal Name (URN-notiert)	Hinweise
Vorname(n)	givenName	urn:oid:2.5.4.42	
Nachname	surname	urn:oid:2.5.4.4	
Emailadresse (optional)	mail	urn:oid:0.9.2342.19200300.100.1.3	
Strasse	postalAddress	urn:oid:2.5.4.16	
PLZ	postalCode	urn:oid:2.5.4.17	
Wohnort	localityName	urn:oid:2.5.4.7	
Land (Adresse)	country	urn:oid:1.2.40.0.10.2.1.1.225599	Als ISO 3166-1 alpha-2 gepflegt. Ein D von der

			eID oder eIDAS wird durch DE ersetzt.
Akad. Titel (optional)	personalTitle	urn:oid: 0.9.2342.19200300.100.1.40	
Anrede	gender	urn:oid:1.3.6.1.4.1.33592.1.3.5	Die Anrede wird als numerischer Wert nach ISO 5218:2004 codiert [11]. 0 = unbekannt 1 = männlich 2 = weiblich 9 = keine Angabe / nicht zutreffend
Geburtsdatum	birthdate	urn:oid:1.2.40.0.10.2.1.1.55	Nach ISO 8601 im sog. extended Format in der Form JJJJ-MM-TT ohne weitere Zeitangabe
Geburtsort (optional)	placeOfBirth	urn:oid:1.3.6.1.5.5.7.9.2	
Ausstellen- der Staat	issuingState	urn:oid:1.2.40.0.10.2.1.1.552244	seit 02/2019 nicht mehr unterstützt
Geburtsname	birthName	urn:oid:1.2.40.0.10.2.1.1.225566	
Staatsangehörigkeit	nationality	urn:oid:1.2.40.0.10.2.1.1.225577	Als Ländercode wird nach ICAO für Deutschland der Wert „D“ verwendet. Ist kein Wert eingetragen, kann die Staatsangehörigkeit „D“ auch angenommen werden, wenn im Feld „Dokumententyp“ der Wert „ID“ vorhanden ist. Die Staatsangehörigkeit (Datengruppe 10, DG10) ist bei Personalausweisen (eID mit Dokumententyp „ID“) erst ab November 2019 mit dem Wert „D“ befüllt. Davor

			ist die DG10 bei Personalausweisen leer.
Dokumententyp	documentType	urn:oid:1.2.40.0.10.2.1.1.552255	In anderen Fällen steht der Wert nicht zur Verfügung. Mögliche Werte werden in der Technische Richtlinie TR-03127 definiert (Verlinkung Stand Oktober 2023).
De-Mail	DeMail	urn:oid:1.3.6.1.4.1.55605.70737875.1.1.1.7.1	
Telefonnummer	telephoneNumber	urn:oid:2.5.4.20	Darstellung ab 05/2021 (R3.2.0.0) als international gültige Telefonnummer; in der BundID ab 09/2021 produktiv
eIDAS-Issuing-Country	eIDAS-Issuing-Country	urn:oid:1.3.6.1.4.1.25484.494450.10.1	Basiert auf Sending-MemberState (TR-03130 eID-Server), optional, ISO 3166-1 alpha-2
Wohnort-ID	communityId	urn:oid:1.3.6.1.4.1.25484.494450.5	Der Wert wird übergeben, wenn die Authentifizierung mit der eID durchgeführt wird. Falls der Wert beim Hinterlegen der eID im Nutzerkonto gespeichert wurde, wird die Wohnort-ID auch übermittelt, wenn andere Verfahren als die eID zur Authentifizierung verwendet werden. Der Wert wird bei der Authentifizierung mit der eID aktualisiert (analog zur Adresse). Das Feld wird in <u>TR-03127</u> als <u>Datengruppe DG18</u> beschrieben. Die Verfügbarkeit ist abhängig vom Betreiber des NKs.

Bitte beachten:

Bei der Authentifizierung mit eIDAS-notifizierten Identifikationsmittel gilt der Mindestdatensatz nach eIDAS-VO, daher kann es zu einem reduzierten Datensatz kommen.

6.2 Technische Nutzdaten

Darüber hinaus werden technische Nutzdaten zur erleichterten Datenpersistenz in Drittanwendungen, zum Kontext des Authentisierungsvorgangs und zu weiteren Schnittstellen (Postfach) bereitgestellt.

6.2.1 bPK – bereichsspezifisches Personenkennzeichen

Die Verwendung des bPK kann von den Betreibenden eines Nutzerkontos deaktiviert werden. Die Information ob und wann dies stattfinden wird, wird durch die jeweiligen Verantwortlichen kommuniziert. Fachlich bedeutet die Abkündigung, dass das Feld nicht mehr bei der Auswertung ob eine temp. Anmeldung möglich ist, ausgewertet wird (siehe Anforderung von Pflichtattributen). Des Weiteren wird dafür kein Attribut mehr übertragen. Falls das bPK als Pflichtattribut angefordert wird, führt dies zu einem Fehler. Die bestehende Alternative ist das bPK2.

Das bPK (bereichsspezifisches Personenkennzeichen) dient in Anlehnung an die österreichische Bürgerkarten-Infrastruktur zur datenschutzfreundlichen, für die jeweilige Drittanwendung eindeutig geltenden Identifizierung eines Nutzers. Im sog. Exportformat wird diese als Base64-encodierte Zeichenkette generiert.

Bezeichnung	FriendlyName	SAML2 Formal Name (URN-notiert)
bPK	bPK	urn:oid:1.2.40.0.10.2.1.1.149

Dieses Kennzeichen kann in dekodierter Grundform und Zerlegung (interne bPK oder ssPIN, *sector-specific personal identification number*) als robuster Datenbankschlüssel dauerhaft auf Seiten des Service Providers zur Datensatzreferenzierung hinterlegt werden [12 / Vor etwaigen Änderungen der zugrundeliegenden Berechnung zur Erstellung der bPK (z. B. im Falle von Algorithmenwechsel auf Anraten des BSI), würden alle Verbundbetreiber im Bedarfsfall unter Gewährung einer entsprechend langen Vorlaufzeit vorab informiert. Die entsprechende Umsetzung (durch begleitende Prozesse, Instrumentarien) befindet sich derzeit im Planungsstadium und wird in zukünftigen Versionen dieses Dokuments Erwähnung finden.].

bPKs werden vom Identity Provider in einem Base64-encodierten Exportformat ausgegeben, die als Zeichenfolge zusätzlich zur eigentlichen ssPIN um weitere Nutzdaten angereichert ist, zumeist getrennt durch die Zeichenfolge '::':

1. version - die Konfigurationsnummer der Algorithmen zur Berechnung der bPK/ssPIN;
2. issuer - der Identity Provider, der die betreffende bPK ausgibt;
3. specific sector - der Service Provider/Fachportal, für den die bPK gültig ist;
4. bPK - die Base64-encodierte, eigentliche ssPIN (sektor-spezifische Personen-Identifikations-Nummern) die aus der Bürgerkonto UUID abgeleitet ist; ausschließlich diese sollte zur Referenzierung in Datenbanken herangezogen werden.
5. timestamp - der Zeitpunkt der Ausstellung der bPK in der Zeitzone Europe/Berlin; die Information zur Zeitzone wird leider nicht im Wert übergeben.

Issuer und specific sector werden in E-Mail-Notation mit der Zeichenfolge '@' getrennt. Diese Erweiterung ist spezifisch für den Bayerischen Portalverbund und die vorliegende Identity Federation Infrastruktur konzipiert. Eine typische bPK im Exportformat sieht daher wie folgt aus:

```
V1::de.bund.id@portal.zoll.de::mcR9heGIqQj1dF0PqlhLETJcTJIrBo05DZtt8qyUiPE::2013-06-11T13:42:34
```

Es wird daher empfohlen, die bPK anderen Attributen zur eindeutigen Nutzerreferenzierung (z. B. E-Mail) in der jeweiligen Datenhaltung vorzuziehen.

Zusätzlich zur Nutzung der internen bPK als Datenbankschlüssel kann die bPK im unbehandelten Exportformat als API-Key genutzt werden: die Exportformat-bPK als API-Key ist an die Laufzeit der Online-Sitzung eines authentisierten Benutzers gebunden und nur während dieser gültig.

Achtung: Sofern das bPK durch OD/FV genutzt wird, ist bei der Änderung der URL eines Online-dienstes (OD) darauf zu achten, dass der Hostname der entityID nicht verändert wird. Eine Änderung des Hostnames der entityID verursacht abweichend generierte bPK.

6.2.2 bPK2 – bereichsspezifisches Personenkennzeichen

Da für die Service Provider das Entpacken und das Verarbeiten der bPK eine unnötige Hürde war, wurde die bPK2 eingeführt.

Das bPK (bereichsspezifisches Personenkennzeichen) dient in Anlehnung an die österreichische Bürgerkarten-Infrastruktur zur datenschutzfreundlichen, für die jeweilige Drittanwendung eindeutig geltenden Identifizierung eines Nutzers.

Bezeichnung	FriendlyName	SAML2 Formal Name (URN-notiert)
bPK2	bPK2	urn:oid:1.3.6.1.4.1.25484.494450.3

Bei FINK wird der Identifier aus dem anderen Servicekonto übernommen und mit Prefixen versehen, damit keine Überschneidung mit existierenden bPK2s möglich ist.

Achtung: Sofern das bPK2 durch OD/FV genutzt wird, ist bei der Änderung der URL eines Online-dienstes (OD) darauf zu achten, dass der Hostname der entityID nicht verändert wird. Eine Änderung des Hostnames der entityID verursacht abweichend generierte bPK2.

6.2.3 Vertrauensniveau

Informationen über die vom Benutzer gewählte Authentisierungsmethode zur Initialisierung der Sitzung werden mittelbar in Form einer akkumulierten Trustlevel-Angabe (d. h. zum Authentisierungsvorgang und zur Herkunft der Attribute aus der BundID) verfügbar gemacht.

Bezeichnung	FriendlyName	SAML2 Formal Name (URN-notiert)
Vertrauensniveau	EID-CITIZEN-QAA-LE-VEL	urn:oid: 1.2.40.0.10.2.1.1.261.94

Aufgrund der strategischen Wichtigkeit des von der Europäischen Kommission geförderten Large-Scale-Pilot-Projekts STORK [11] und im Lichte der eIDAS-Verordnung [12], wurde bis zur Veröffentlichung entsprechender Technischer Richtlinien seitens des BSI der Trustlevel-Ansatz nach STORK-Methodik gewählt [13]. Zum derzeitigen Zeitpunkt unterscheidet die Identity Infrastruktur folgende Trustlevel nach STORK, die zukünftig als Kategorien mehrere gleichrangige Authentisierungsmethoden beinhalten können:

Bezeichnung	Bedeutung für Drittanwendungen
STORK-QAA-Level-1	aktuelle Authentisierung mittels Benutzername/Passwort; registrierte Attributdaten ohne hoheitliche Prüfung (= selbstregistrierte BundID bzw. eIDAS-Äquivalent)
STORK-QAA-Level-3	Aktuelle Authentisierung mittels ELSTER-Zertifikat; Registrierte Attribute aus dem ELSTER Zertifikat (= ELSTER Zertifikat registrierte BundID bzw. eIDAS-Äquivalent)
STORK-QAA-Level-4	aktuelle Authentisierung mittels Online-Ausweisfunktion (ePA, eAT, EU-Karte); registrierte Attributdaten aus Ausweismittel (= eID-registrierte BundID bzw. eIDAS-Äquivalent)

6.2.4 Version

Das Attribut Version dient als Vorbereitung um Änderungen besser kommunizieren zu können. Damit können Service-Provider technisch feststellen, mit welcher fachlichen Version der Schnittstelle sie es zu tun haben und können besser darauf reagieren. Die initiale Version lautet 2020.2.1 und als Konvention wird Calendar Versioning [14] verwendet.

Bezeichnung	FriendlyName	SAML2 Formal Name (URN-notiert)
Version	Version	urn:oid:1.3.6.1.4.1.25484.494450.1

6.2.5 AssertionProvedBy

Darüber wird die Quelle transportiert, die die Identität überprüft hat. Im ersten Schritt wird hier eIDAS bei der Authentifizierung über eIDAS übermittelt. In den nächsten Versionen werden die weiteren IDs auch in der Schnittstelle übergeben.

Bezeichnung	FriendlyName	SAML2 Formal Name (URN-notiert)
AssertionProvedBy	AssertionProvedBy	urn:oid:1.3.6.1.4.1.25484.494450.2

Liste der möglichen IDs:

- eIDAS
- eID
- Smart-eID
- Elster
- Benutzername
- FINK
- Diia

6.2.6 Postkorb-Handle

Das Postkorb-Handle in seiner jetzigen Form kann als Eingabeparameter für die Zustellung von Postfachnachrichten genutzt werden. Um Nachrichten einem bestimmten Vertrauensniveau in der späteren Ansicht zuzuordnen, ist bei der Benutzung der eigenen Postfach-API zusätzlich noch das Vertrauensniveau mitzugeben.

Dieses Attribut ist nicht dafür geeignet, als eindeutige Nutzerreferenzierung in der Drittanwendung verwendet zu werden.

Bezeichnung	FriendlyName	SAML2 Formal Name (URN-notiert)
Postkorb-Handle	legacyPostkorbHandle	urn:oid:2.5.4.18

Jeder BundID ist immer ein Postkorb-Handle zugeordnet, welches wiederum genutzt werden kann, um ein Postfach eindeutig zu referenzieren.

Weiterführende Informationen zur Nutzung dieses Attributs bei der Kommunikation mit einem Postfach können den Kapiteln 11 ff. entnommen werden.

Der String ist eine UUID mit 36 Zeichen.

6.2.7 Application ID (Antrags-ID)

Ein Antrag gruppiert alle Nachrichten, Dokumente und Statusmeldungen im ZBP. Jede Statusmeldung wird über die Antrags-ID mit diesem Antrag verknüpft. Dies gilt auch für Nachrichten. Mehr und aktuelle Informationen dazu bietet der Statusmonitor. Eine Antrags-ID kann technisch ab Release 9 übergeben werden, unter dem Vorbehalt, dass das Feature auch damit aktiviert wird.

Bezeichnung	FriendlyName	SAML2 Formal Name (URN-notiert)
Application ID (Antrags-ID)	applicationId	urn:oid:1.3.6.1.4.1.25484.494450.4

Schema der FITKO zum Statusmonitor (Stand 20.12.2023): <https://schema.fitko.de/statusmonitor/status-schema/0.9.0/status-update.schema.json>

Der String ist eine UUID mit 36 Zeichen.

6.2.8 Pseudonym

Das Pseudonym transportiert die Pseudonyme anderer Systeme. Die Weitergabe des dienste- und kartenspezifischen Kennzeichens (DKK) aus der eID erfolgt, um auch bei einer Gastanmeldung mit der eID über das Nutzerkonto einen Benutzer nicht nur Anhand des Mindestdatensatzes, sondern auch Anhand einer ID, wieder identifizieren zu können. Es existiert hierbei keine Garantie, dass das Pseudonym an sich für eine Identität stabil bleibt (eine neue eID liefert ein neues Pseudonym für dieselbe Identität). Falls weitere Pseudonyme transportiert werden sollen, z. B. von ELSTER oder eIDAS, wird das über dieses Feld transportiert. Um eine Eineindeutigkeit zu erhalten, muss das erhaltene Pseudonym mit AssertionProvedBy kombiniert werden, denn das Nutzerkonto gibt die Daten aus der Quelle unverändert weiter.

Bezeichnung	FriendlyName	SAML2 Formal Name (URN-notiert)
Pseudonym	pseudonym	urn:oid:1.2.40.0.10.2.1.1.226699

6.2.9 Vertrauensniveau der Attribute

Die übermittelten Attribute können andere Vertrauensniveaus als die Authentisierung selbst aufweisen. Das Vertrauensniveau des SAML-Attributs wird über das Attribut akdb:TrustLevel übermittelt.

```
<saml2:Attribute FriendlyName="legacyPostkorbHandle" Name="urn:oid:2.5.4.18" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" akdb:TrustLevel="NORMAL"
xmlns:akdb="https://www.akdb.de/request/2018/09">
```

Dabei sind folgende Werte analog zur TR 03160-1 definiert:

Vertrauensniveau	Wert
STORK-QAA-Level-1	Basisregistrierung
STORK-QAA-Level-2	Niedrig
STORK-QAA-Level-3	Substantiell
STORK-QAA-Level-4	Hoch

Falls kein Vertrauensniveau ermittelt werden kann, wird das Attribut nicht übergeben, auch nicht als Basisregistrierung.

6.2.10 SAML-Attribut für Zwei-Faktor-Authentifizierung

Das Attribut mfa mit OID urn:oid:1.3.6.1.4.1.25484.494450.7 kann an den Onlinedienst innerhalb der SAML Response zurückgegeben werden. Es enthält die Angabe (Werte "true" oder "false"), ob die Authentifizierung des Nutzens bei der BundID durch einen zweiten Faktor abgesichert war.

Bei einer Anmeldung mittels Zugangsmittel eID oder ELSTER ist dies immer gegeben, bei Anmeldung per Benutzername/Passwort ist dies optional möglich.

7 Betriebsvoraussetzungen

7.1 Infrastruktur

Das ITZBund als Betreiber der SAML-basierten Identity-Infrastruktur der BundID sichert die dauernde Erreichbarkeit folgender Komponenten zu:

- Identity-Provider für die unterstützten Authentisierungsmethoden

Drittanwendungen können in jeder Technologie und Nutzungsweise (vgl. Kapitel 4) entwickelt werden unter der Maßgabe, dass sie das Web-Browser-SSO-Profil des OASIS SAML v2 Standards zu implementieren haben.

7.2 Metadaten

(Technische) Voraussetzung zur Teilnahme an der SAML-basierten Identity Infrastruktur ist:

- Bereitstellung der SAML-Metadaten seitens der Drittanwendung

Es ist darauf zu achten, dass

1. die einzureichenden Metadaten kein Ablaufdatum enthalten (validUntil-Attribut),
2. die Metadaten kein ID-Attribut enthalten,
3. die entityID als URI in URL-Notation mit https-Protokoll-Prefix ohne Portnummer anzugeben ist. Diese muss nicht(!) zwingend mit der tatsächlich genutzten URL-Domain übereinstimmen, ist aber in Zusammenhang mit dem Attribut bPK2 in dieser Notation anzugeben. Die Auswahl der entityID kann nach Aufnahme in den Wirkbetrieb nicht(!) mehr verändert werden und sollte daher den Betreiber der Drittanwendung eindeutig identifizieren (also nicht unspezifisch sein) wie folgendes Negativbeispiel „https://drittanwendung.com/serviceprovider“.

Erst nach erfolgter Bereitstellung der SAML-Metadaten kann dem Teilnehmer die Metadaten des Identity Providers (bzw. für Drittanwendungen innerhalb des ITZBund-RZ die URL zu den Federation-Metadaten) mitgeteilt werden.

Die Bekanntgabe der Metadaten des Identity Providers durch das ITZBund ist als technologische Schnittstelle hinreichend für die Entwicklung einer Drittanwendung.

Für die Integrationsumgebung wird auch die IP-Adresse des zu verbindenden Verfahrens benötigt. Für die Produktionsumgebung ist dies nicht nötig.

8 Entscheidungsunterstützung und Handreichungen

8.1 Architekturüberlegungen bei Auswahl eines SAML-Bindings

Für die Anbindung einer Drittanwendung an die BundID werden derzeit die beiden Bindings HTTP-REDIRECT und HTTP-POST unterstützt. Beide Bindings haben nachfolgend erwähnte Vor- und Nachteile im Praxisbetrieb, die im Rahmen der Architekturüberlegungen seitens der Bereitsteller von Drittanwendungen abzuwägen sind.

Das HTTP-REDIRECT-Binding ermöglicht das Übersenden des SAMLRequests als HTTP-GET-Parameter in der Anfrage-URL an den Identity Provider und unterliegt folglich den individuell regulierbaren Längenbegrenzungen aller zwischen Drittanwendung und Identity Provider befindlichen aktiven und passiven Netzwerkkomponenten (also Switches, Web-Application-Firewalls, Proxies, Web-Server, Personal Firewalls der Benutzer, etc.).

Bei Nutzung des HTTP-POST-Bindings wird der SAMLRequest innerhalb des HTTP-Body übermittelt, so dass aktive und passive Netzwerkkomponenten den Protokollablauf nicht in der gleichen Weise wie oben beschrieben, negativ beeinflussen können. Andererseits ist in diesem Zusammenhang die Nutzung der „Zurück“-Funktionalität bei einem gewollten Abbruch auf der Identity Provider-Seite browserabhängig beeinträchtigt. Die Folge kann eine Weiterleitungsschleife sein, die den Benutzer bei Abbruch des Login Vorgangs immer wieder auf den Identity Provider vorwärtsleitet. Dieses Problem zeigt sich generell bei Nutzung des SAML-HTTP-POST-Bindings und in kein Spezifikum der hier genutzten Produkte.

Tendenziell soll daher die Benutzung des HTTP-POST-Bindings bevorzugt werden.

8.2 Zurückleiten in die Drittanwendung bei Abbruch durch Benutzer

Aufgrund der Architektur der meisten Drittanwendungen bei Nutzung des HTTP-POST-Bindings, ist besonderes Augenmerk auf die Usability des Zurück-Buttons zu legen. Für eine reibungslose Zurückleitung in die Drittanwendung ist ein geordnetes Session-Handling der Drittanwendung gefordert, um ein zyklisches erneutes Absenden eines SAML-Requests und dessen Interpretation als Replay-Attacke zu vermeiden.

Umgesetzt werden kann ein solches Vorgehen z.B.: durch Setzen und Prüfen eines zusätzlichen Cookies zum Zeitpunkt der Erstellung des SAML-Requests der Art:

```
if found_AlreadySentSAMLRequestCookie():
    invalidate_AlreadySentSAMLRequestCookie()
    forwardTo(previousStatus)
else:
    set_AlreadySentSAMLRequestCookie()
    sendSAMLRequest(SAMLRequest)
```

9 Konfiguration der Anfrage

SAML unterstützt Extensions im SAML-Request. Dort können neben dem SAML-Standard Erweiterungen verwendet werden. Fachlich nennen wir das die AkdbExtension (im SAML-Request akdb:AuthenticationRequest). Beispiele für einen vollständigen SAML-Request sind unten aufgeführt.

Die Verwendung des AuthenticationRequests in Version 2 kann von den Betreibern eines Nutzerkontos als verpflichtend konfiguriert werden. Die Information ob und wann dies stattfinden wird, wird durch die jeweiligen Verantwortlichen kommuniziert. In der Regel geht das einher, mit der Forderung, den OrganizationDisplayName als verpflichtend zu übergeben.

Damit müssen im SAML-Request folgende Bedingungen verpflichtend erfüllt werden:

- Der Request muss signiert sein.
- OrganizationDisplayName muss übergeben werden.
- akdb:AuthenticationRequest in Version 2 muss verwendet werden
- akdb:RequestedAttributes müssen mindesten ein akdb:RequestedAttribute anfordern

Falls diese Bedingungen nicht erfüllt sind, antwortet der IDP direkt mit einer SAML-Response, da der Request nicht verarbeitet werden kann.

Über eine Extension ist es möglich die Anfrage weiter anzupassen, als das mit Standard SAML-Elementen möglich wäre. Der SAML-Request muss signiert sein, damit die Extension ausgewertet wird.

Die Hülle der Anfrage sieht folgendermaßen aus:

```
<akdb:AuthenticationRequest xmlns:akdb="https://www.akdb.de/request/2018/09" Version="2">
</akdb:AuthenticationRequest>
```

Achtung: Version ist ein Pflichtfeld. Aktuell werden Version 1 und Version 2 unterstützt. Die nachfolgenden Abschnitte beschreiben jeweils ein Kindelement der Extension.

9.1 Einschränkung des Authentifizierungsverfahren

Zusätzlich zu Kapitel 5.1, können die Authentifizierungsverfahren folgendermaßen eingeschränkt werden: Die Smart-eID kann nicht als dediziertes Verfahren angefordert werden, da sie fachlich mit der eID gleichgestellt werden soll.

Es werden die aufgelisteten Authentifizierungsverfahren herangezogen, die kein <akdb:Enabled> definiert haben oder deren Wert true entspricht.

Version 2

```
<akdb:AuthnMethods>
  <akdb:Authega>
    <akdb:Enabled>true</akdb:Enabled>
  </akdb:Authega>
  <akdb:Benutzername>
    <akdb:Enabled>true</akdb:Enabled>
  </akdb:Benutzername>
  <akdb:eID>
    <akdb:Enabled>true</akdb:Enabled>
  </akdb:eID>
  <akdb:eIDAS>
    <akdb:Enabled>true</akdb:Enabled>
  </akdb:eIDAS>
  <akdb:Diia>
    <akdb:Enabled>true</akdb:Enabled>
  </akdb:Diia>
  <akdb:Elster>
    <akdb:Enabled>true</akdb:Enabled>
  </akdb:Elster>
  <akdb:FINK>
    <akdb:Enabled>true</akdb:Enabled>
  </akdb:FINK>
</akdb:AuthnMethods>
```

Die unterstützten Werte entsprechen denen aus Kapitel 6.3.5 (AssertionProvedBy). Die temporäre Anmeldung ist kein eigenständiges Verfahren, weswegen dieser nicht über diese Liste ausgewählt werden kann.

9.2 Anforderung von Pflichtattributen

Im SAML Request können Pflichtattribute angefordert werden.

Die Änderung in Version 2 dient grundsätzlich zur Gewährleistung der Datensparsamkeit, indem die Attribute spezifiziert werden müssen, deren Daten aus dem Nutzerkonto an den Aufrufer übertragen werden sollen. Wenn die Version 1 nicht mehr zur Verfügung steht, müssen die gewünschten Attribute

angefragt werden. Eine Rückgabe aller vorhandener Daten wird dann nicht mehr unterstützt. Es werden danach nur noch die angefragten Daten übermittelt. Eine zeitnahe Umstellung ab der Verfügbarkeit von Version 2 wird deswegen empfohlen.

Achtung: Ab Version 2 ist <akdb:RequestedAttributes> **verpflichtend**, bei Nutzung des <akdb:AuthenticationRequest>. Es werden nur die Attribute zurückgeliefert, die aufgelistet sind. Fehlende <akdb:RequestedAttributes> oder leere <akdb:RequestedAttribute>s führt dazu, dass die Extension im SAML-Request ignoriert wird. Mit RequiredAttribute können Attribute als verpflichtend gekennzeichnet werden. Dadurch wird garantiert, dass die Antwort (im Erfolgsfall) die verpflichtenden Attribute beinhaltet. Falls die erforderlichen Daten nicht vorliegen, wird eine SAML-Response als Fehler ohne Daten übertragen. RequiredAttribute ist per Default false.

Empfehlung zum Umgang mit Pflichtattributen

Es wird empfohlen, nur in begründeten Ausnahmen vom Standardfall abzuweichen und ein Attribut als verpflichtend (RequiredAttribute=true) anzugeben. Bei vielen Attributen besteht die Möglichkeit, dass diese im Einzelfall aus unterschiedlichen Gründen nicht vorhanden sind, was bei RequiredAttribute=true dazu führt, dass in der SAML-Response ein Fehler enthalten ist - und somit der Prozess für den Nutzenden an dieser Stelle abbricht.

Insbesondere, sofern nur das Nicht-Vertrauensniveau "Basisregistrierung" vorausgesetzt wird, empfehlen wir auf Pflichtattribute gänzlich zu verzichten. Für den Antrag erforderliche Angaben könnten dann ebenso im Antragsprozess beim Onlinedienst durch den Nutzenden - ohne Verlust des Vertrauensniveaus - angegeben werden. Aber auch bei einem echten Vertrauensniveau wie bspw. "substanziell", empfehlen wir den zurückhaltenden Einsatz von RequiredAttribute=true. Die Identität des Nutzenden ist durch das Vertrauensniveau entsprechend bestätigt; weitere Attribute sollten nur durch eine fachliche Prüfung begründet als verpflichtend markiert werden.

Hinweise zu nicht vorhandenen Attributen

Die Rückmeldung des Nutzerkontos an den Onlinedienst im Rahmen der Authentifizierung (die SAML-Response) basiert auch auf den Daten des Zugangsmittels, welches vom Nutzenden für den Authentifizierungsvorgang verwendet wird. So können Attribute vom Zugangsmittel nicht an das Nutzerkonto übermittelt worden sein (vgl. bspw. eIDAS) oder auch nicht auf dem Zugangsmittel vorhanden sein (bspw. Vorname oder Anschrift bei einer eID). Entsprechend können solch fehlende Attribute auch

nicht an den Onlinedienst zurückgegeben werden. Das Nutzerkonto ermöglicht es dem Nutzenden bei der Registrierung mit Benutzername/Passwort, gewisse Daten als “nicht zutreffend” zu deklarieren und somit nicht zu befüllen, die i.d.R. vorhanden sein sollten. Diese sind: Vorname, Geburtsname, Geburtsort, Adresse/Anschrift. Der Nutzende hat im Nachhinein die Möglichkeit, diese Daten zu ergänzen. Um einer “Falschnutzung” dieses Features durch den Nutzenden entgegenzuwirken, kann der Onlinedienst ein Vertrauensniveau größer gleich “substanziell” anfordern, um zu gewährleisten, dass die Attribute von vertrauenswürdiger externer Stelle überprüft wurden.

Sollte entsprechend ein vom Onlinedienst angefragtes Attribut nicht vorhanden sein, wird dies nicht in der SAML-Response enthalten sein.

Version 2

```
<akdb:RequestedAttributes>
  <akdb:RequestedAttribute Name="urn:oid:2.5.4.18" RequiredAttribute="false" />
  <akdb:RequestedAttribute Name="urn:oid:1.2.40.0.10.2.1.1.149" RequiredAttribute="true" />
  <akdb:RequestedAttribute Name="urn:oid:1.3.6.1.4.1.25484.494450.3"/>
</akdb:RequestedAttributes>
```

Das XML Attribut Name muss SAML2 Formal Name (URN-notiert) sein.

9.2.1 Technische Attribute vom Servicekonto und die Authentisierungsverfahren

Es können nachfolgende Attribute angefordert werden:

- bPK2 (urn:oid:1.3.6.1.4.1.25484.494450.3)
- legacyPostkorbHandle (urn:oid:2.5.4.18)

Werden ein, mehrere oder alle Attribute angefordert, werden die Authentisierungsverfahren ausgeblendet, welche die geforderten Attribute nicht erfüllen.

Sofern eine Drittanwendung beispielhaft ein bPK2 zwingend erfordert, kann die Drittanwendung im SAML-Request mindestens eines der Attribute anfordern, um das Ausblenden der temporären Anmeldung zu erreichen.

Bitte beachten Sie, dass sich die Daten, die ein Verfahren liefert, über die Zeit ändern können. FINK wurde zuerst ausgeblendet bei einer Anfrage nach bPK2, jedoch wurde das Verhalten über die Zeit geändert, da mittlerweile auch über den Portalverbund Kennzeichen übertragen werden, jedoch noch

kein passendes Attribut um ein legacyPostkorbHandle zu unterstützen. Das Attribut bPK ist abgekündigt und wird bald nicht mehr unterstützt (siehe Kapitel zu bPK).

9.2.2 Validieren von RequestedAttributes im SAML Request

Die Requests mit der leeren Liste von RequestedAttributes oder mit falsch formatierten Attribut-Namen führt zum Ausschluss des <akdb:AuthenticationRequest>. Der IdP verhält sich so, als ob kein <akdb:AuthenticationRequest> übermittelt wäre. Dieses Verhalten ändert sich, wenn V2 der Schnittstelle verpflichtend ist. Danach gelten diese leeren Anfragen als Fehler und der SAML-Request wird abgewiesen.

```
<akdb:RequestedAttributes>  
</akdb:RequestedAttributes>
```

```
<akdb:RequestedAttributes>  
  <akdb:RequestedAttribute Name="" />  
</akdb:RequestedAttributes>
```

9.2.3 Validieren von RequestedAttributes vor dem Absenden

Falls die angeforderten Attribute vom Servicekonto nicht bereitgestellt werden können, wird im SAML Response mit SAML statuscode=urn:oasis:names:tc:SAML:2.0:status:RequestDenied geantwortet.

9.3 Implementierungsanleitung BundID-Weiterleitung Modaldialog

Für Onlinedienste besteht die Möglichkeit zur Einbindung eines Modal-Dialogs, der Nutzende eines Onlinedienstes vor dem Verlassen des Onlinedienst-Angebots darauf hinweist, dass die soeben ausgeführte Nutzenden-Aktion die Weiterleitung zu id.bund.id auslösen wird.

Dieser Modaldialog kann wie folgt im Hinblick auf Layout, Design, Funktionalität eingebunden werden, damit die UX als optimal empfunden wird:

Pop-Up Dialog

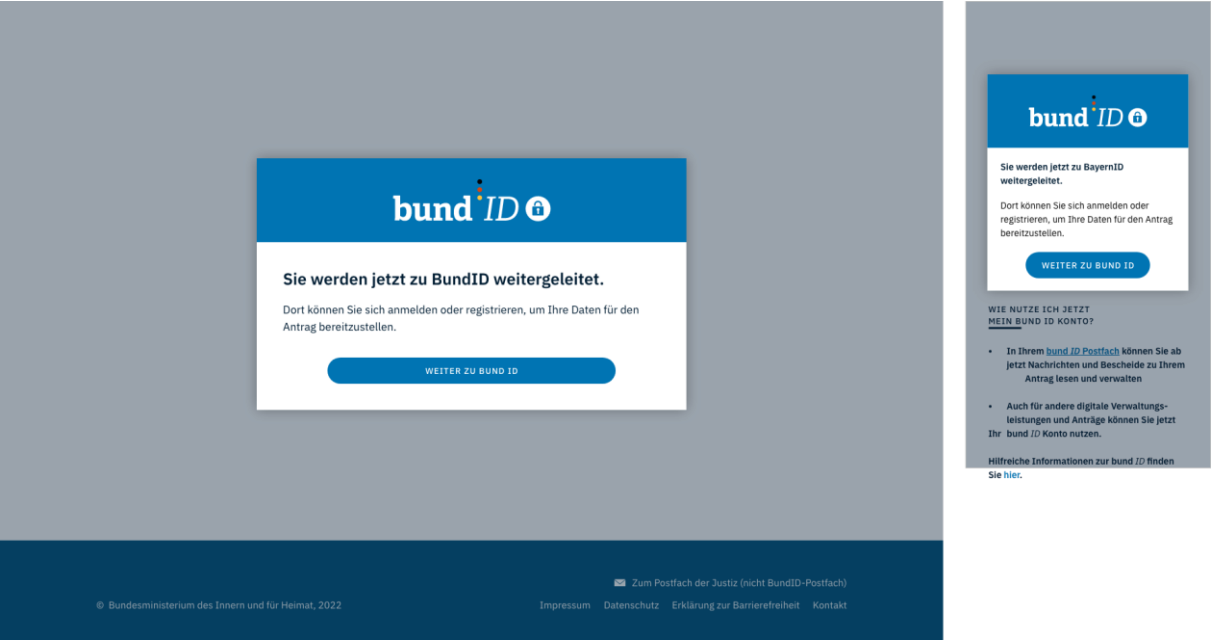



Abbildung 5: Pop-Up Dialog zur Weiterleitung an die BundID

Pop Up Mobile	<p><u>Breite:</u> 307 px / ca. 19 rem (Übernommen aus bekannten Maßen vom letzten Jahr) BITTE PRÜFEN</p> <p><u>Höhe Logo-Section (blau):</u> 112px / 7rem</p> <p><u>Höhe Gesamt:</u> flex</p>
Pop Up Desktop	<p><u>Breite:</u> 656px / 41rem</p> <p><u>Höhe Logo-Section (blau):</u> 128px / 8rem</p> <p><u>Höhe Gesamt:</u> flex</p>
Farben	<p><u>BundID-Blau:</u> #0074B3 </p> <p><u>Weiß:</u> #FFFFFF </p> <p><u>Grau:</u> #666666 </p> <p><u>Schwarz:</u> #011D33 </p>

Buttons Vorschau

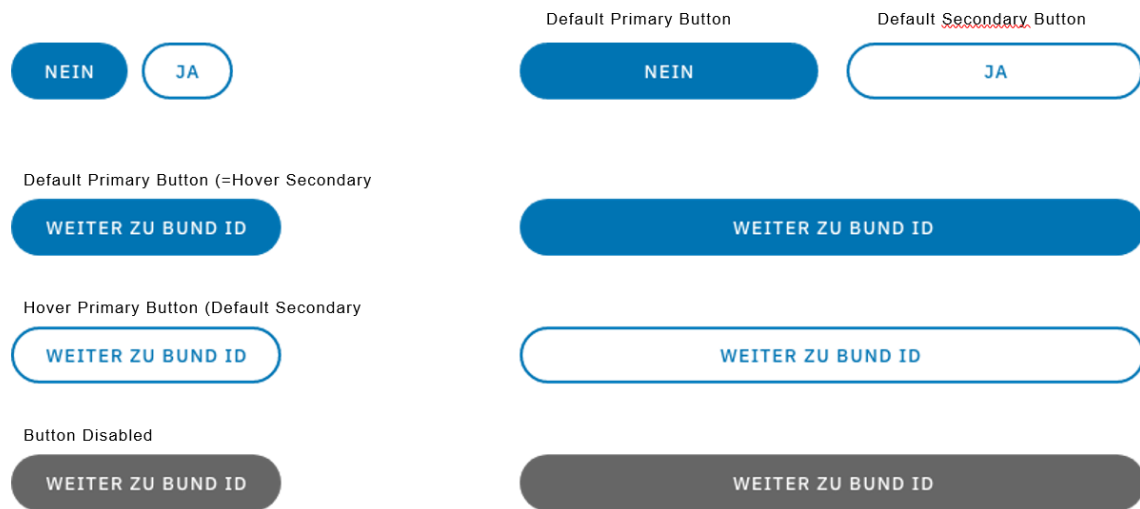


Abbildung 6: Buttons der BundID

Typografie Button (Desktop/ Tablet/ Mobile)	<p><u>font:</u> IBM Plex Sans</p> <p><u>font-hight:</u> 14px</p> <p><u>line-hight:</u> 21px / 150 %</p> <p><u>letter-spacing:</u> 8 %</p>
Größe Button Mobile	<p><u>Breite:</u> 24 px / 1,5 rem Spacing + Labertext + 24 px / 1,5 rem Spacing) (Übernommen aus bekannten Maßen vom letzten Jahr, nicht in xd-Files vorhanden, da selbständig von Entwicklung festgelegt) BITTE PRÜFEN</p> <p><u>Spacing zwischen Buttons</u> laut xd-File Mobile: 10 px BITTE PRÜFEN (scheint für den Abstand zu gering zu sein?)</p> <p><u>Höhe (Standard-Höhe für Buttons BundID):</u> 40px / 2,5rem</p>
Button Tablet/ Desktop	<p><u>Breite wie bei IDP-Komponente:</u> 500px / 32,25rem</p> <p><u>Breite bei zwei Buttons je Button:</u> 242px / 15,125rem</p> <p><u>Abstand zwischen Buttons:</u> 16px / 1rem</p> <p><u>Höhe (Standard-Höhe für Buttons BundID):</u> 40px / 2,5rem</p>

Desktop Details



Abbildung 7: BundID Desktop Details

Mobile Details

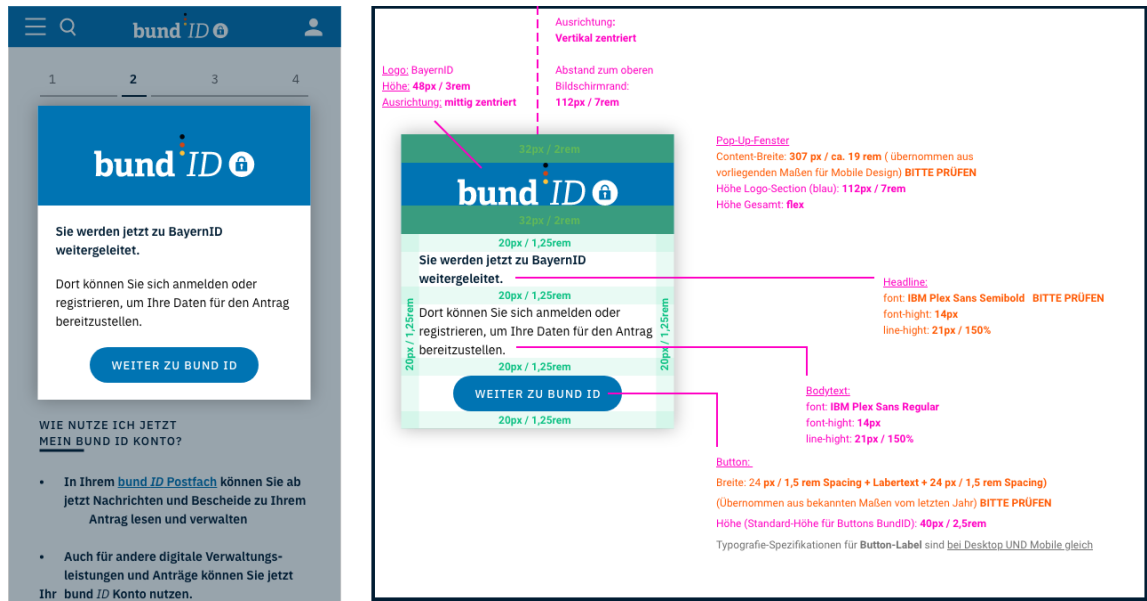


Abbildung 8: BundID Mobile Details

9.3.1 Implementierungsbeispiel

Das Beispiel verwendet zur Formatierung Tailwind CSS (<https://tailwindcss.com/>)

```
<div id="modal-container">

  <div data-modal="" data-test-id="db0f7modal-overlay" class="fixed inset-0 w-full h-screen
  last:bg-neutral last:bg-opacity-50 overflow-y-hidden flex items-center overscroll-none cur-
  sor-pointer" style="z-index: 1100;">

    <div class="max-h-screen max-w-fit overflow-auto mx-auto p-2">

      <div class="h-40 bg-primary flex justify-center items-center">

      </div>

      <div data-test-id="db0f7modal" class="bg-secondary flex shadow-lg cursor-auto"
      role="group" aria-live="polite" aria-label="modal" tabindex="0" aria-modal="true">

        <div class="flex flex-col m-2 overflow-auto relative" tabindex="0">

          <div id="modalContent" tabindex="-1" class="flex flex-col gap-5 justify-between
          mx-4 sm:mx-8 mb-12 mt-12" data-test-id="db0f7modal-content">

            <div class="max-w-[40rem]">

              <div class="flex flex-col text-styles">

                <h3 class="break-words">Sie werden jetzt zur BundID weitergeleitet.</h3>

                <p><p>Dort können Sie sich anmelden oder registrieren, um Ihre Daten für den
                Antrag bereitzustellen.</p></p>

              </div>

            </div>

            [BUTTON INTEGRIEREN siehe unten]

          <div><div><div></div></div></div>

        </div>

      </div>

    </div>

  </div>
```

Einen Button integrieren

```
<div class="grid gap-5 w-full mt-3 max-w-[28rem] mx-auto self-center grid-cols-1">

  <button data-v-96f246fc="" class="transition duration-200 ease-out border-2 cursor-pointer
  min-h-[2.5rem] rounded-[1.25rem] text-spitzmarke bg-skin-primary text-skin-primary border-
  skin-primary hover:bg-skin-secondary hover:text-skin-secondary disabled:bg-skin-disabled
  disabled:text-skin-disabled disabled:border-skin-disabled" data-test-id="d0gQ0">

    <div data-v-96f246fc="" class="flex align-middle justify-between w-full relative items-
    center">

      <span data-v-96f246fc="" class="flex px-3"></span>

      <span data-v-96f246fc="" class="inline-block justify-self-center align-
```

```

        midle">WEITER</span>

        <span data-v-96f246fc="" class="flex px-3"></span>

    </div>

</button>
</div>

```

Zwei Buttons integrieren

```

<div class="grid gap-5 w-full mt-3 max-w-[28rem] mx-auto self-center grid-cols-[repeat(auto-fill,_minmax(12rem,_1fr))]">
    <button data-v-96f246fc="" class="transition duration-200 ease-out border-2 cursor-pointer min-h-[2.5rem] rounded-[1.25rem] text-spitzmarke bg-skin-primary text-skin-primary border-skin-primary hover:bg-skin-secondary hover:text-skin-secondary disabled:bg-skin-disabled disabled:text-skin-disabled disabled:border-skin-disabled" data-test-id="awwnM">
        <div data-v-96f246fc="" class="flex align-middle justify-between w-full relative items-center">
            <span data-v-96f246fc="" class="flex px-3"></span>
            <span data-v-96f246fc="" class="inline-block justify-self-center align-middle">AB-
BRECHEN</span>
            <span data-v-96f246fc="" class="flex px-3"></span>
        </div>
    </button>
    <button data-v-96f246fc="" class="transition duration-200 ease-out border-2 cursor-pointer min-h-[2.5rem] rounded-[1.25rem] text-spitzmarke bg-skin-primary text-skin-primary border-skin-primary hover:bg-skin-secondary hover:text-skin-secondary disabled:bg-skin-disabled disabled:text-skin-disabled disabled:border-skin-disabled" data-test-id="IRZBW">
        <div data-v-96f246fc="" class="flex align-middle justify-between w-full relative items-center">
            <span data-v-96f246fc="" class="flex px-3"></span>
            <span data-v-96f246fc="" class="inline-block justify-self-center align-middle">WEITER</span>
            <span data-v-96f246fc="" class="flex px-3"></span>
        </div>
    </button>
</div>

```


9.4 Übergabe von UI-Information

```
<akdb:DisplayInformation>
  <classic-ui:Version xmlns:classic-ui="https://www.akdb.de/request/2018/09/classic-ui/v1">
    <classic-ui:Purpose>
      <![CDATA[<h1>My HTML</h1>]]>
    </classic-ui:Purpose>
    <classic-ui:OrganizationDisplayName>
      <![CDATA[Meine Organisation]]>
    </classic-ui:OrganizationDisplayName>
    <classic-ui:Lang>de</classic-ui:Lang>
    <classic-ui:BackURL>
      <![CDATA[https://example.com?a=1&b=2]]>
    </classic-ui:BackURL>
    <classic-ui:OnlineServiceId>
      <![CDATA[BMI-X0000]]>
    </classic-ui:OnlineServiceId>
  </classic-ui:Version>
</akdb:DisplayInformation>
```

9.5 Übergabe von UI-Informationen (ab Release 6)

Bei der Änderung des Einleitungstextes ist der `Purpose` auf allen Seiten am IDP sichtbar. Nur gewisse HTML-Elemente (u.a. `h1 p a b i`) und Attribute (`href` auf `a`) sind erlaubt. Des Weiteren nur https-URLs für href.

Der Purpose bleibt in der Schnittstelle bestehen. Mit dem Redesign der BundID in Release 6 wird jedoch der Purpose nicht mehr angezeigt.

OrganizationDisplayName wird vor der Übermittlung der Daten des Benutzers vom IDP an den Onlinedienst angezeigt. Bei Werten mit mehr als 50 Zeichen behalten wir uns vor, den Text im UI entsprechen zu kürzen. Aus Gründen der Abwärtskompatibilität wird im Übergangszeitraum bei fehlendem `OrganizationDisplayName` ein neutraler Wert angezeigt. Zuvor wurden die Daten aus den SAML-Metadaten aus `Organization/OrganizationDisplayName` verwendet, weswegen der technische Begriff hier wieder aufgenommen wurde. Fachlich wird der Wert auf `https://id.bayernportal.de` auch im Kontext der Anmeldeinformationen für den Benutzer "Anmelden im Online-Verfahren "{OrganizationDisplayName}" verwendet (Stand 7. Juli 2023). Es besteht hier keine Anforderung den Namen der Organisation zu übermitteln, die den SAML-Request stellt, sondern es können fachlich hilfreiche Informationen übermittelt werden. Ob die Übergabe verpflichtend ist, hängt vom Betreiber des Nutzerkontos ab.

Lang kann verwendet werden, wenn im Onlinedienst bereits die gewünschte Sprache des Benutzers bekannt ist, damit dieser am SK nicht nochmals die Sprache wechseln muss. Valide Werte sind de, en, ru, uk. Der Wert ist optional und kann auch für Releases davor übergeben werden, hat dann aber keine Auswirkung. Der Default ist de.

BackURL wird für "zurück zum Onlinedienst" verwendet. Die Übergabe ist optional. Die URL wird nicht validiert, sollte aber https verwenden und keine Möglichkeit bieten, Zugriff auf Daten des Benutzers zu erlangen. Falls kein Wert übergeben wird, findet die Navigation zurück zum Onlinedienst über eine SAML-Response statt. Um Open-Redirects zu vermeiden, muss die URL vor der Übergabe im SAML-Requests validiert sein und darf nicht vom User verändert werden.

OnlineServiceId (ab Release 7) In Schnittstellen-Request soll das Attribut Onlinedienst den Wert der ID enthalten, der in KOOPV durch das BMI vergeben wurde (BMI-ID). Damit soll erreicht werden, dass trotz Verwendung geteilter Länder-Zertifikate eine eindeutige Erkennung des Onlinedienstes möglich ist. Es wird darum gebeten, die BMI-ID im Attribut OnlineServiceId mit zu übergeben. (Stand Oktober 2024 für die BundID: Die BMI-ID wird als OnlineServiceId übergeben und ist ab 30.06.2025 verpflichtend.)

```
<akdb:DisplayInformation>
  <classic-ui:Version xmlns:classic-ui="https://www.akdb.de/request/2018/09/classic-ui/v1">
    <classic-ui:Purpose>
      <![CDATA[<h1>My HTML</h1>]]>
    </classic-ui:Purpose>
    <classic-ui:OrganizationDisplayName>
      <![CDATA[Meine Organisation]]>
    </classic-ui:OrganizationDisplayName>
    <classic-ui:Lang>de</classic-ui:Lang>
    <classic-ui:BackURL>
      <![CDATA[https://example.com?a=1&b=2]]>
    </classic-ui:BackURL>
    <classic-ui:OnlineServiceId>
      <![CDATA[89479871264-DE]]>
    </classic-ui:OnlineServiceId>
```

```
</classic-ui:Version>  
  
</akdb:DisplayInformation>
```

9.6 Verwendete Fehlercodes am IDP bei unerwarteten SAML-Requests

Nicht alle Codes können zur gleichen Zeit auftreten und manche sind abhängig von der Konfiguration des jeweiligen Nutzerkontos. Der Code wird in der Regel in der Fehlerseite des NKs angezeigt und taucht in der URL als `idp.code` auf.

akdb-extension-missing

Anfrage mit fehlender AKDB-Extension.

akdb-extension-v1-deprecated

Anfrage mit veralteter AKDB-Extension.

saml-request-not-signed

SAML-Request ist nicht signiert.

purpose-does-not-support-restricted-html

Purpose mit HTML, das nicht den Richtlinien entspricht.

missing-berca

Angefragtes Berechtigungszertifikat ist nicht hinterlegt.

requested-attributes-empty

Requested Attributes wurden nicht übergeben.

requested-attributes-missing-name

Requested Attributes ohne Name.

empty-authentication-methods

Leere Liste für Authentication Methods (keine Liste oder mind. ein Eintrag werden erwartet).

organization-display-name-missing

Name des Onlinedienstes fehlt.

9.7 Erweiterte Fehlermeldung im SAML-Response

Das Attribut EnableStatusDetail schaltet die erweiterte/detaillierte Status-Meldung ein.

Das Setzen des Attributes

```
<akdb:AuthenticationRequest xmlns:akdb="https://www.akdb.de/request/2018/09" Version="2" EnableStatusDetail="true">
    ...
</akdb:AuthenticationRequest>
```

SAML-Response mit der detaillierten Fehlermeldung

```
<saml2p:Response>
    ...
    <saml2p:Status>
        <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Requester">
            <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:RequestDenied"/>
        </saml2p:StatusCode>
        <saml2p:StatusMessage>security-msg</saml2p:StatusMessage>
        <saml2p:StatusDetail>
            <akdb:StatusDetail xmlns:akdb="https://www.akdb.de/request/2018/09">
                {
                    "version": "1.0",
                    "errors": [{
                        "code": "IDP_REQUIRED_ATTRIBUTES_MISSING",
                        "message": "Attribute
urn:oid:0.9.2342.19200300.100.1.20 is required but not available in Nutzerkonto. Attribute
urn:oid:0.9.2342.19200300.100.1.42 is required but not available in Nutzerkonto. Attribute
urn:oid:2.5.4.42 is required but not available in Nutzerkonto."
                    }
                ]
            </akdb:StatusDetail>
        </saml2p:StatusDetail>
    </saml2p:Status>
</saml2p:Response>
```

10 Beispiele für SAML-Requests und SAML-Responses

10.1 Beispiele für SAML-Requests

Beispiel für SAML-Request V1

```
<saml2p:AuthnRequest
  xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
  AssertionConsumerServiceURL="https://samltool2-ewg.pre.buergerserviceportal.de/saml/SSO"
  Destination="https://id.bayernportal.de/idp/profile/SAML2/POST/SSO"
  ForceAuthn="true"
  ID="79c01d07-5c07-46d8-ba7a-4f96e6a1f6e3"
  IsPassive="false"
  IssueInstant="2023-08-04T14:03:08.074Z"
  ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
  Version="2.0">
  <saml2:Issuer
    xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
    https://samltool2-ewg.pre.buergerserviceportal.de
  </saml2:Issuer>
  <saml2p:Extensions>
    <akdb:AuthenticationRequest
      xmlns:akdb="https://www.akdb.de/request/2018/09"
      Version="1">
      <akdb:AllowedMethods>
        <akdb:AuthnMethod>
          eID
        </akdb:AuthnMethod>
        <akdb:AuthnMethod>
          eIDAS
        </akdb:AuthnMethod>
        <akdb:AuthnMethod>
          Benutzername
        </akdb:AuthnMethod>
      </akdb:AllowedMethods>
      <akdb:RequestedAttributes>
        <akdb:RequestedAttribute
          Name="urn:oid:2.5.4.18"
        />
        <akdb:RequestedAttribute
          Name="urn:oid:1.3.6.1.4.1.25484.494450.3"
        />
      </akdb:RequestedAttributes>
      <akdb:DisplayInformation>
        <classic-ui:Version
          xmlns:classic-ui="https://www.akdb.de/request/2018/09/classic-ui/v1">
          <classic-ui:Purpose>
            <![CDATA[Dieses Feld wird fachlich in der Schnittstelle akzeptiert, jedoch aktuell
nicht verwendet. Das ist aber zu Dokumentationszwecken weiterhin vorhanden. Von einer Verwen-
dung wird aber abgeraten.]]>
          </classic-ui:Purpose>
          <classic-ui:OrganizationDisplayName>
            <![CDATA[Der Name des Onlinedienstes kann hier gesetzt werden]]>
          </classic-ui:OrganizationDisplayName>
          <classic-ui:Lang>
            de oder en oder run oder uk (Abhängig der Sprachen des NKs)
          </classic-ui:Lang>
          <classic-ui:BackURL>
            <![CDATA[https://www.example.com/eine-url-zurueck?auch-mit=parametern]]>
          </classic-ui:BackURL>
          <classic-ui:OnlineServiceId>
            <![CDATA[Eine Onlinedienst-ID (fachliche Verwendung noch offen - also aktuell noch
nicht relevant)]]>
          </classic-ui:OnlineServiceId>
        </classic-ui:Version>
      </akdb:DisplayInformation>
    </akdb:AuthenticationRequest>
  </saml2p:Extensions>
  <saml2p:RequestedAuthnContext
    Comparison="minimum">
```

```

    <saml2:AuthnContextClassRef
      xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
      STORK-QAA-Level-1
    </saml2:AuthnContextClassRef>
  </saml2p:RequestedAuthnContext>
</saml2p:AuthnRequest>

```

Beispiel für SAML-Request V2

```

<saml2p:AuthnRequest
  xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
  AssertionConsumerServiceURL="https://samltool2-ewg.pre.buergerserviceportal.de/saml/SSO"
  Destination="https://id.bayernportal.de/idp/profile/SAML2/POST/SSO"
  ForceAuthn="true"
  ID="64e1f1b9-acf9-4076-b727-2833cd01200f"
  IsPassive="false"
  IssueInstant="2023-08-04T14:05:00.353Z"
  ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
  Version="2.0">
  <saml2:Issuer
    xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
    https://samltool2-ewg.pre.buergerserviceportal.de
  </saml2:Issuer>
  <saml2p:Extensions>
    <akdb:AuthenticationRequest
      xmlns:akdb="https://www.akdb.de/request/2018/09"
      EnableStatusDetail="true"
      Version="2">
      <akdb:AuthnMethods>
        <akdb:Authega>
          <akdb:Enabled>
            true
          </akdb:Enabled>
        </akdb:Authega>
        <akdb:Benutzername>
          <akdb:Enabled>
            true
          </akdb:Enabled>
        </akdb:Benutzername>
        <akdb:Diia>
          <akdb:Enabled>
            true
          </akdb:Enabled>
        </akdb:Diia>
        <akdb:eID>
          <akdb:Enabled>
            true
          </akdb:Enabled>
        </akdb:eID>
        <akdb:eIDAS>
          <akdb:Enabled>
            true
          </akdb:Enabled>
        </akdb:eIDAS>
        <akdb:Elster>
          <akdb:Enabled>
            true
          </akdb:Enabled>
        </akdb:Elster>
        <akdb:FINK>
          <akdb:Enabled>
            true
          </akdb:Enabled>
        </akdb:FINK>
      </akdb:AuthnMethods>
      <akdb:RequestedAttributes>
        <akdb:RequestedAttribute
          Name="urn:oid:1.3.6.1.4.1.33592.1.3.5"
          RequiredAttribute="false"

```

```

/>
<akdb:RequestedAttribute
  Name="urn:oid:1.3.6.1.4.1.25484.494450.3"
  RequiredAttribute="true"
/>
<akdb:RequestedAttribute
  Name="urn:oid:1.3.6.1.5.5.7.9.2"
  RequiredAttribute="false"
/>
<akdb:RequestedAttribute
  Name="urn:oid:2.5.4.16"
  RequiredAttribute="false"
/>
<akdb:RequestedAttribute
  Name="urn:oid:1.2.40.0.10.2.1.1.149"
  RequiredAttribute="false"
/>
<akdb:RequestedAttribute
  Name="urn:oid:2.5.4.17"
  RequiredAttribute="false"
/>
<akdb:RequestedAttribute
  Name="urn:oid:1.2.40.0.10.2.1.1.225599"
  RequiredAttribute="false"
/>
<akdb:RequestedAttribute
  Name="urn:oid:1.2.40.0.10.2.1.1.225566"
  RequiredAttribute="false"
/>
<akdb:RequestedAttribute
  Name="urn:oid:1.2.40.0.10.2.1.1.225577"
  RequiredAttribute="false"
/>
<akdb:RequestedAttribute
  Name="urn:oid:2.5.4.18"
  RequiredAttribute="true"
/>
<akdb:RequestedAttribute
  Name="urn:oid:0.9.2342.19200300.100.1.40"
  RequiredAttribute="false"
/>
<akdb:RequestedAttribute
  Name="urn:oid:2.5.4.7"
  RequiredAttribute="false"
/>
<akdb:RequestedAttribute
  Name="urn:oid:1.2.40.0.10.2.1.1.261.94"
  RequiredAttribute="false"
/>
<akdb:RequestedAttribute
  Name="urn:oid:2.5.4.42"
  RequiredAttribute="false"
/>
<akdb:RequestedAttribute
  Name="urn:oid:2.5.4.4"
  RequiredAttribute="false"
/>
<akdb:RequestedAttribute
  Name="urn:oid:1.2.40.0.10.2.1.1.55"
  RequiredAttribute="false"
/>
<akdb:RequestedAttribute
  Name="urn:oid:0.9.2342.19200300.100.1.3"
  RequiredAttribute="false"
/>
</akdb:RequestedAttributes>
<akdb:DisplayInformation>
  <classic-ui:Version
    xmlns:classic-ui="https://www.akdb.de/request/2018/09/classic-ui/v1">
    <classic-ui:Purpose>
      <![CDATA[Dieses Feld wird fachlich in der Schnittstelle akzeptiert, jedoch aktuell
nicht verwendet. Das ist aber zu Dokumentationszwecken weiterhin vorhanden. Von einer Verwen-
dung wird aber abgeraten.]]>
    </classic-ui:Purpose>
  </classic-ui:Version>
</akdb:DisplayInformation>

```

```

    <classic-ui:OrganizationDisplayName>
      <![CDATA[Der Name des Onlinedienstes kann hier gesetzt werden]]>
    </classic-ui:OrganizationDisplayName>
    <classic-ui:Lang>
      de oder en oder run oder uk (Abhängig der Sprachen des NKs)
    </classic-ui:Lang>
    <classic-ui:BackURL>
      <![CDATA[https://www.example.com/eine-url-zurueck?auch-mit=parametern]]>
    </classic-ui:BackURL>
    <classic-ui:OnlineServiceId>
      <![CDATA[Eine Onlinedienst-ID (fachliche Verwendung noch offen - also aktuell noch
nicht relevant)]]>
    </classic-ui:OnlineServiceId>
    </classic-ui:Version>
  </akdb:DisplayInformation>
</akdb:AuthenticationRequest>
</saml2p:Extensions>
<saml2p:RequestedAuthnContext
  Comparison="minimum">
  <saml2:AuthnContextClassRef
    xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
    STORK-QAA-Level-1
  </saml2:AuthnContextClassRef>
</saml2p:RequestedAuthnContext>
</saml2p:AuthnRequest>

```

10.2 Beispiele für SAML-Responses (entschlüsselter Bereich)

```

<?xml version="1.0" encoding="UTF-8"?><saml2:Assertion xmlns:saml2="urn:oasis:na-
mes:tc:SAML:2.0:assertion" ID="_11a0a649e6bd232b84ca908e5f898ec4" IssueInstant="2023-08-
04T14:07:46.231Z" Version="2.0" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <saml2:Issuer>https://int.id.bund.de/idp</saml2:Issuer>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
      <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256"/>
      <ds:Reference URI="#_11a0a649e6bd232b84ca908e5f898ec4">
        <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-sig-
nature"/>
          <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
            <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-
c14n#" PrefixList="xsd"/>
          </ds:Transform>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmenc#sha256"/>
        <ds:DigestValue>JPRhAhjU5cJXh63HJuDaZ4rxXS+aYjlHL16YakDzuvE=</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>R27/7nb3l00ilgGiPDQCdJSEKr6NH8XErMwshrO17x12mfa-
i0oDLxh9Q4LcCHZcsLV4lsiM-
pEdL/LO83e1EXdU8eNU/fU5yxqD/proGr0CMxGxbqap4Flwv6vrpz1oA81/FBUhWBmIHMR8IOT7R9EMmrM2aQ07XU8q60l
j9c4UKUv45AZ0KfTTgiO3nZ3awY/AHMg9lKVBmoGJpo3bNDWVynx1AR8VGQGsSLtu7hOAJfA2XQxSGbwtY0BT+9+OmA-
jJyR5r4WNlfzQjr0SVYRZW20nOWLUj/G2ilt3ldyC2TOQ6zliUft-
mUI00RlMFJlvJGQBPSr+jq7oL5HQgkQ+GQ==</ds:SignatureValue>
    <ds:KeyInfo>
      <ds:X509Data>
        <ds:X509Certificate>MIIDGCCAgCgAwIBAgIVAN5phAtPmCFBPamoDoX4vLS59JT4MA0GCSqG-
S1b3DQEBBQUAMBYxFDAS
BgNVBAMTC2lkC5ha2RiLmRlMB4XDTEyMTAzMDA5NTY0Ml0xDTMyMTAzMDA5NTY0Ml0wFjEUMBIG
A1UEAxMLaWRwLmFrZGluZGUwggEiMA0GCSqGS1b3DQEBBAQUAA4IBDwAwggEKAoIBAQQDD4sFNoPXy
JWRW+oIoJJwoXuXsQsTi63VulrRxYAObwjJdT7NLDJ0UyRwMSHvs7ggvEtT3nfVKKEpW01nQra0Va
jrS2lEQTJKEOC28ikI3dlpbb6YIRcEaAEYIej99lIm4gNB4DS6XNUKD8yUvQr2Uiijgpwp9Xn3EuC
5/LcxD464ubyyJqBZJfDn1+KFKGsA9YJomdpD5Xoce/Mdl06Eh5eEGSX2dyPRk02wVQtOjQImvM
Qhtv+JqLh3YxxRTqpay/NAhGJIRfvQk+iVuYmWlWvgWiUN3VsbYZwVj+3GiY+mz30q5CQt3ENi4I
OOonKqJKsX+kmuEfnC+/tiGImGqxAgMBAAGjXTBbMD0GA1UdEQQzMDGCC2lkC5ha2RiLmRlhiJo

```



```

dHRwcZovL2lkcC5ha2RiLmRlL2lkcC9zaGlicm9sZXRoMB0GA1UdDgQWBBDriSLzK7LbBi6KZHK
Ij29z5kMHDANBgkqhkiG9w0BAQUFAAOCAQEAmc3lv4QjVvHn5ko08ex/f+NyGOOGXXhWB7S7CcKz
X7ln89FVyzB02uEWUOYB48TgMLDKmMeBRbKyUumKhWh6Px42JWZjpQYJC2fj+w/axrnPSJsYq18v
uypuB3/EI1I6dX7g1519CfvAd9YEOXqIU1F4C+BIbgiomtgoQATGVxUKyghJbc5eI+Zfxv+KKFMy
QkU6AQBQ9UNTfN1UJCDgRTpFp1cju1BdCU5eX/FspCA33RmTeJtXGHkbKwakLyHb6Z3Z7hP9pUws
zwBZJkZw702G01U7iTxHLenuMM/Cg2sfJ0Fs8pOjRulzhDWrm28Cwrl2v73NQCc1m2Do2Fq7Og==</ds:X509Certifi-
cate>

    </ds:X509Data>
  </ds:KeyInfo>
</ds:Signature>
<saml2:Subject>
  <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient" NameQuali-
fier="https://int.id.bund.de/idp" SPNameQualifier="https://samltool2-ewg.pre.buergerserv-
iceportal.de">_ebb5259433f7e69608a59e32d0352d4f</saml2:NameID>
  <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
    <saml2:SubjectConfirmationData Address="93.199.14.87" InResponseTo="f83affde-7b9c-
4987-93e2-907649f03647" NotOnOrAfter="2023-08-04T14:12:46.253Z" Recipient="https://samltool2-
ewg.pre.buergerserviceportal.de/saml/SSO"/>
  </saml2:SubjectConfirmation>
</saml2:Subject>
<saml2:Conditions NotBefore="2023-08-04T14:07:46.231Z" NotOnOrAfter="2023-08-
04T14:12:46.231Z">
  <saml2:AudienceRestriction>
    <saml2:Audience>https://samltool2-ewg.pre.buergerserviceportal.de</saml2:Audience>
  </saml2:AudienceRestriction>
</saml2:Conditions>
<saml2:AuthnStatement AuthnInstant="2023-08-04T14:07:43.661Z" SessionIn-
dex="_8373c263f578eb77327fd61eafb4b1a6">
  <saml2:SubjectLocality Address="93.199.14.87"/>
  <saml2:AuthnContext>
    <saml2:AuthnContextClassRef>STORK-QAA-Level-4</saml2:AuthnContextClassRef>
  </saml2:AuthnContext>
</saml2:AuthnStatement>
<saml2:AttributeStatement>
  <saml2:Attribute FriendlyName="legacyPostkorbHandle" Name="urn:oid:2.5.4.18" NameFor-
mat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" akdb:TrustLevel="NORMAL"
xmlns:akdb="https://www.akdb.de/request/2018/09">
    <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xsd:string">b980f78d-f5e0-45d9-8971-cc0e27f0beaf</saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute FriendlyName="postalCode" Name="urn:oid:2.5.4.17" NameFormat="urn:oa-
sis:names:tc:SAML:2.0:attrname-format:uri" akdb:TrustLevel="HOCH"
xmlns:akdb="https://www.akdb.de/request/2018/09">
    <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xsd:string">51147</saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute FriendlyName="postalAddress" Name="urn:oid:2.5.4.16" NameFor-
mat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" akdb:TrustLevel="HOCH"
xmlns:akdb="https://www.akdb.de/request/2018/09">
    <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xsd:string">HEIDESTRAÙE 17</saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute FriendlyName="givenName" Name="urn:oid:2.5.4.42" NameFormat="urn:oa-
sis:names:tc:SAML:2.0:attrname-format:uri" akdb:TrustLevel="HOCH"
xmlns:akdb="https://www.akdb.de/request/2018/09">
    <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xsd:string">ERIKA</saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute FriendlyName="bPK2" Name="urn:oid:1.3.6.1.4.1.25484.494450.3" Name-
Format="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" akdb:TrustLevel="NORMAL"
xmlns:akdb="https://www.akdb.de/request/2018/09">
    <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xsd:string">k2jBT0cykDVqikWialVMzqmntTu-EwGskIYlcIGt_8</saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute FriendlyName="placeOfBirth" Name="urn:oid:1.3.6.1.5.5.7.9.2" NameFor-
mat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" akdb:TrustLevel="HOCH"
xmlns:akdb="https://www.akdb.de/request/2018/09">
    <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xsd:string">BERLIN</saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute FriendlyName="country" Name="urn:oid:1.2.40.0.10.2.1.1.225599" Name-
Format="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" akdb:TrustLevel="HOCH"
xmlns:akdb="https://www.akdb.de/request/2018/09">

```

```

        <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xsd:string">DE</saml2:AttributeValue>
    </saml2:Attribute>
    <saml2:Attribute FriendlyName="mail" Name="urn:oid:0.9.2342.19200300.100.1.3" NameFor-
mat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" akdb:TrustLevel="NORMAL"
xmlns:akdb="https://www.akdb.de/request/2018/09">
        <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xsd:string">test.automat.nkb.aa@byom.de</saml2:AttributeValue>
    </saml2:Attribute>
    <saml2:Attribute FriendlyName="birthName" Name="urn:oid:1.2.40.0.10.2.1.1.225566"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" akdb:TrustLevel="HOCH"
xmlns:akdb="https://www.akdb.de/request/2018/09">
        <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xsd:string">GABLER</saml2:AttributeValue>
    </saml2:Attribute>
    <saml2:Attribute FriendlyName="bPK" Name="urn:oid:1.2.40.0.10.2.1.1.149" NameFor-
mat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" akdb:TrustLevel="NORMAL"
xmlns:akdb="https://www.akdb.de/request/2018/09">
        <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xsd:string">VlQ6OmRlLmFrZGIuYnBrLnNzb0BzYWlscG9vbDItdXdnLnByZS5id-
WVYzZWVyc2VydmljZXBvcnRhbnC5kZTo6azJqQlQwY3lrRFZxaUtXaWExVk16cWludFRlLUV3R3NrSVlsY0NJR3RfODo6MjA-
yMyOwOC0wNFQxNjowNzo0Mw==</saml2:AttributeValue>
    </saml2:Attribute>
    <saml2:Attribute FriendlyName="surname" Name="urn:oid:2.5.4.4" NameFormat="urn:oa-
sis:names:tc:SAML:2.0:attrname-format:uri" akdb:TrustLevel="HOCH"
xmlns:akdb="https://www.akdb.de/request/2018/09">
        <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xsd:string">MUSTERMANN</saml2:AttributeValue>
    </saml2:Attribute>
    <saml2:Attribute FriendlyName="localityName" Name="urn:oid:2.5.4.7" NameFor-
mat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" akdb:TrustLevel="HOCH"
xmlns:akdb="https://www.akdb.de/request/2018/09">
        <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xsd:string">KÖLN</saml2:AttributeValue>
    </saml2:Attribute>
    <saml2:Attribute FriendlyName="gender" Name="urn:oid:1.3.6.1.4.1.33592.1.3.5" NameFor-
mat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" akdb:TrustLevel="UNTERGEORDNET"
xmlns:akdb="https://www.akdb.de/request/2018/09">
        <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xsd:string">0</saml2:AttributeValue>
    </saml2:Attribute>
    <saml2:Attribute FriendlyName="EID-CITIZEN-QAA-LEVEL"
Name="urn:oid:1.2.40.0.10.2.1.1.261.94" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-for-
mat:uri" akdb:TrustLevel="NORMAL" xmlns:akdb="https://www.akdb.de/request/2018/09">
        <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xsd:string">STORK-QAA-Level-4</saml2:AttributeValue>
    </saml2:Attribute>
    <saml2:Attribute FriendlyName="birthdate" Name="urn:oid:1.2.40.0.10.2.1.1.55" NameFor-
mat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" akdb:TrustLevel="HOCH"
xmlns:akdb="https://www.akdb.de/request/2018/09">
        <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xsd:string">1964-08-12</saml2:AttributeValue>
    </saml2:Attribute>
</saml2:AttributeStatement>
</saml2:Assertion>

```

11 Postfach-Nachricht an die BundID

Hinweis zur Abkündigung der SOAP Schnittstelle:

Die SOAP-Schnittstelle der BundID wird perspektivisch abgeschaltet. Das genaue Datum entnehmen Sie bitte dem Abkündigungskalender. Den Abkündigungskalender finden Sie im BundID SSP Downloadbereich (https://ssp.id.bund.de/ip?id=downloads_internal) in der Kategorie „Allgemeine Informationen“ unter dem Reiter „BundID Übergreifend“.

Mit Release 9.0.0.0 der BundID Schnittstellendokumentation und Release 3.0.0.0 ist die neue Schnittstelle des Zentralen Bürgerpostfachs (ZBP) auf Basis von REST auch außerhalb des Pilotbetriebs erreichbar. Für die Nutzung des ZBP verwenden Sie bitte die entsprechende Dokumentation "ZBP_Schnittstellenbeschreibung_Zentrales Bürgerpostfach".

Die nachfolgende Dokumentation der SOAP-Schnittstelle ist somit zukünftig nicht mehr zu verwenden.

Im vorliegenden Dokument wird die Schnittstelle für den Nachrichtenversand an das Postfach in der BundID beschrieben.

Diese Schnittstelle bietet externen Online-Leistungen und Fachverfahren die Möglichkeit, Nachrichten in das Postfach eines bestimmten Nutzers abzulegen.

11.1 Topologie

Für den Transport der Postfachnachrichten sind unterschiedliche Transportwege möglich:

Variante 1: direkte Verbindung

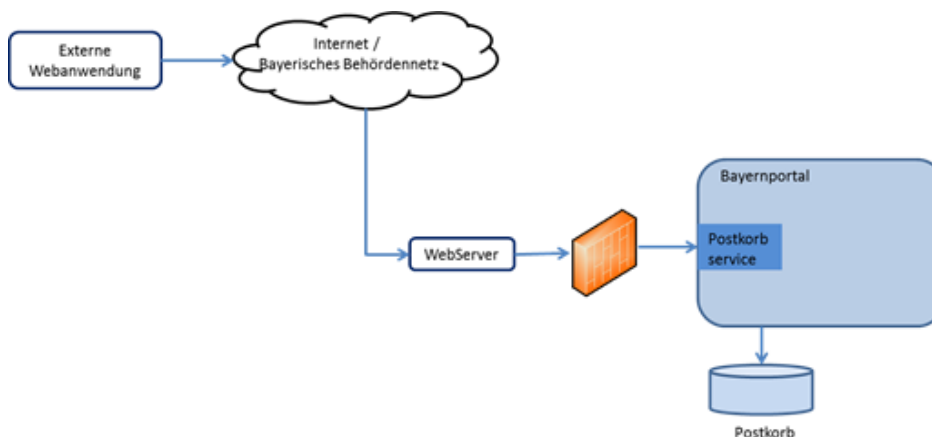


Abbildung 9: Postfachnachrichten Transportwege Variante 1

Sollte der externe Web-Dienst selbst über kein OK.KOMM verfügen, erfolgt der Nachrichtentransport zwischen der externen Webanwendung und dem Nutzerkonto per HTTPS-Soap. Die Verbindung sollte dabei vorzugsweise über das Bayerische Behördennetz erfolgen, wenn auch dies technisch nicht möglich ist, kann die Verbindung auch direkt über das Internet erfolgen.

Für den Produktivbetrieb sind dabei entsprechende Sicherheitsanforderungen (Authentisierung per Client-Zertifikat) zu berücksichtigen (siehe Kapitel "Client Authentifizierung einbinden").

Variante 2: über OK.KOMM:

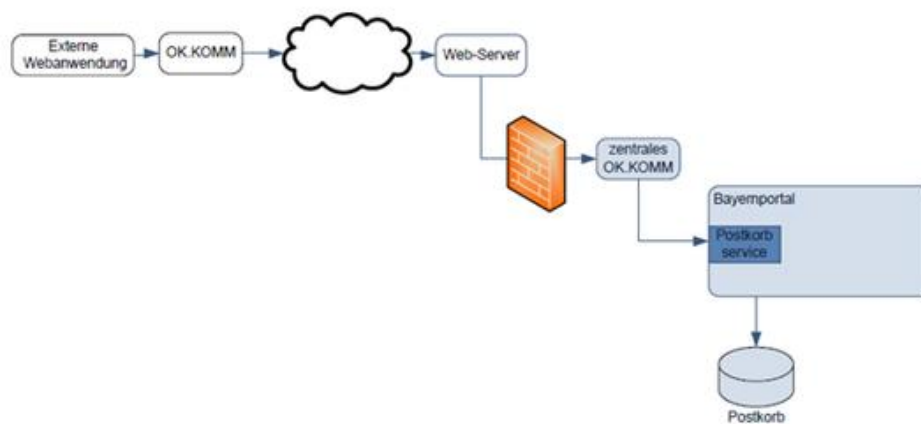


Abbildung 10: Postfachnachrichten Transportwege Variante 2

Wenn die externe Anwendung über ein eigenes OK.KOMM verfügt, kann der Transport über Transportplattform OK.KOMM erfolgen.

In diesem Fall ist der Nachrichtentransportweg zwischen den externen Web-Dienst und dem Nutzerkonto automatisch gegen unberechtigte Zugriffe abgesichert.

11.2 SOAP-Web-Service

Die Übergabe der Postfachnachrichten erfolgt über eine synchrone SOAP-Webservice-Schnittstelle per HTTPS.

Es werden zwei unterschiedliche Operationen angeboten:

- `sendeBspNachrichtNativ`

Erwartet eine Nachricht, in der die Postfach-Nachricht als XML mittels einem einfachen, embedded, String übergeben wird. Als Antwort wird hierbei eine XML-Antwort mit einer speziellen „Postfach-Empfangs-Quittung“ geliefert.

- `sendeBspNachricht`

Erwartet eine Nachricht, in der die Postfach-Nachricht als XML übermittelt wird, die aber zusätzlich noch in eine zweite, OK.KOMM-spezifische „Hülle“ verpackt ist. Als Antwort darauf wird eine OK.KOMM-spezifische „Antwort-Hülle“ geliefert, falls die Postfachnachricht erfolgreich übernommen werden konnte (Soap-Body bzw. OK.KOMM Kontent ist Base64 kodiert.)

Falls die Nachricht aus technischen oder fachlichen Gründen nicht übernommen werden konnte, wird eine SOAP-Exception ausgelöst und an den Aufrufer signalisiert. In dieser SOAP-Exception wird die Fehlerursache als `<faultstring>` näher beschrieben.

Beide Eingänge sind als synchrone Aufrufe realisiert, d.h. die jeweilige Antwort wird unmittelbar nach Übernahme der Postfachnachricht zurückgeschickt; die aufrufende Anwendung kann auf die Antwort warten und entsprechend darauf reagieren.

11.3 Adressierung des Bürgers (Postkorb-Handle)

Die Postfach-Nachricht des Nutzerkonto ist eine spezielle Form der allgemeinen, universellen Nachricht im Nutzerkonto. Postfach-Nachrichten im Kontext des Nutzerkonto kennen nur eine Richtung, von der externen Webanwendung zum Nutzerkonto.

Für die Postfach-Nachricht im Kontext des Nutzerkonto ist eine Adressierung des Bürgers über das sogenannten *Postkorb-Handle* vorgesehen.

Der *Postkorb-Handle* identifiziert das Postfach eines Bürgers eindeutig. Jeder registrierte Bürger hat einen einmaligen und eindeutigen Postkorb-Handle, welcher sich auf sein persönliches Postfach bezieht.

Fiktives Beispiel für ein Postkorb-Handle: S0tU_AL6FOnJm9IfIKkdq_1NqqWPLYOl1llptHbbes4

Das *Postkorb-Handle* wird dem Fachportal/Drittanbieter nach einer erfolgreichen Authentisierung des Bürgers als Attribut im Rahmen des SAML-Tokens übermittelt.

12 Das Format der Postfach-Nachricht

Eine Postfach-Nachricht besteht aus einem Nachrichtenkopf und dem Nachrichteninhalt:

- Der Nachrichtenkopf enthält technische Informationen sowie Absender und Empfänger-Daten.
- Der Nachrichteninhalt enthält die eigentliche Nachricht samt Anhängen, sowie zusätzliche fachliche Attribute zur Nachricht.

Die Postfach-Nachricht ist eine Nachricht im XML-Format, deren Aufbau über ein XSD-Schema definiert ist und dem XSD Element BspNachricht entspricht (siehe [2]).

Wenn nicht gesondert ausgeführt, gilt die Dokumentation im XSD-Schema.

12.1 Besondere Hinweise

Manche Felder der Postfach-Nachricht müssen immer gefüllt sein, auch wenn sie im zugehörigen XML-Schema (BspNachricht) als optional gekennzeichnet sind.

Diese und andere Besonderheiten werden nachfolgend näher erläutert (zusätzlich zur Dokumentation innerhalb des Schemas).

Die für Postfach-Nachrichten zwingend erforderlichen Felder sind im Folgenden als **Pflichtfelder (***)** in Fettdruck gekennzeichnet.

12.1.1 NachrichtenKopf

- **NachrichtenId (***)**
 - Schema-Pfad: *BspNachricht / NachrichtenKopf / Identifikation.Nachricht / NachrichtenId*
 - technisch, beliebig. Empfohlen: GUID/UUID.
 - Beispiele: "1694163650234", "5d0ebee8-d782-4e1b-a35a-5562ac1de578"
 - Dieses Feld sollte eindeutig pro Nachricht sein. Sie hat nur informativen Charakter und wird vorerst nur für Debug-Zwecke oder Fehleranalysen benötigt.
- **Absender (***)**

- **Dienst (***)**
 - Schema-Pfad: *BspNachricht / NachrichtenKopf / Absender / Dienst*
 - Beispiele: "Gehaltsabrechnung", "iKfz-Antrag", "Kitaplatz - Bedarfsanmeldung", "BayernID"
 - Die Anzeige dieser Information ist Portal/UI-abhängig.
- **Mandant (***)**
 - Schema-Pfad: *BspNachricht / NachrichtenKopf / Absender / Mandant*
 - Beispiele: "Verwaltungsgemeinschaft Polling", "Landgericht Bamberg", "Herrsching", "Personalstelle", "09179123".
 - Die Anzeige dieser Information ist Portal/UI-abhängig.
- **Empfänger (***)**
 - **PostkorbId (***)**
 - Pfad: *BspNachricht / NachrichtenKopf / Empfaenger/ PostkorbId*
 - Dieses Feld muss mit einem existierenden Postkorb-Handle des Empfängers (des Bürgers) besetzt sein.

12.1.2 NachrichtenInhalt

- Stork-QAA-Level
 - Schema-Pfad: *BspNachricht / NachrichtenInhalt / StorkQaaLevel*
 - Über dieses Feld kann eine Nachricht dahingehend geschützt werden, dass sie nur dann sichtbar ist, wenn vorher eine erfolgreiche Authentisierung mit dem entsprechenden (Nicht-)Vertrauensniveau erfolgt ist.

Technische Bezeichnung	Bezeichnung nach TR-03160-1 bzw. Beschluss der Projektgruppe eID Strategie von Juli 2021
STORK-QAA-Level-1	Basisregistrierung
STORK-QAA-Level-2	Niedrig
STORK-QAA-Level-3	Substantiell

STORK-QAA-Level-4	Hoch
-------------------	------

- Entgegen der Schema-Definition ist dieses Feld optional. Wenn es nicht gegeben oder unbekannt ist, dann wird automatisch "STORK-QAA-Level-4" für die Nachricht gesetzt.
- **Nachrichten-Text (***)**
 - Schema-Pfad: *BspNachricht / NachrichtenInhalt / FreiText / Text*
 - Der Text einer Nachricht kann sowohl einfachen (plain) Text als auch HTML enthalten.
 - Der Umfang der erlaubten HTML-Tags ist abhängig von der Umgebung. Nähere Informationen finden sich im Kapitel **Validierung Nachrichten-Inhalt**.
- Nachrichten-Encoding
 - Schema-Pfad: *BspNachricht / NachrichtenInhalt / FreiText / Encoding*
 - Entgegen der Schema-Definition ist dieses Feld optional und wird nicht verwendet.
- Nachrichten-Anhänge
 - Schema-Pfad: *BspNachricht / NachrichtenInhalt / FreiText / DataContainer / ...*
 - Den Postfach-Nachrichten können mehrere Anhänge beigefügt werden. Wenn kein Anhang übermittelt werden soll, dann ist dieses Element wegzulassen.
 - Eine Liste der möglichen Anhang-Typen ist in **Tabelle 9005** in Abschnitt 4.2.6 festgelegt.
 - Wenn ein Dateiname mitgeliefert wird, muss dessen Dateinamenendung zum angegebenen Filetype korrespondieren.
 - Die Zeichen \ / : * ? " < | > werden beim Dateinamen aufgrund Dateisystem-Kompatibilität durch einen Unterstrich (_) ersetzt.
 - Der Inhalt eines Anhangs muss im XML als "base64 (standard)" codiert sein (also kein - oder _ Zeichen) mit explizitem Padding. (vgl. https://en.wikipedia.org/wiki/Base64#Variants_summary_table)
 - Größe, Anzahl sowie zulässige Typen für Nachrichtenanhänge können durch technische Gegebenheiten eingeschränkt sein. **Die Limitierung liegt derzeit bei maximal 5 Anhängen mit jeweils 2 MB Größe.**

12.1.3 BSP-Quittung

Hinweis zu § 9 OZG (i. d. F. v. 03.12.2020):

Die BSP-Quittung wird nach der fachlichen Verarbeitung der Nachricht im Nutzerkonto synchron quittiert. Daher kann die Quittierung nach Tabelle 9006 als rechtssichere Annahme und Zustellung der Nachricht an das angesprochene Postfach gewertet werden.

12.1.4 Validierung Nachrichten-Inhalt

Die Postkorbempfangsschnittstelle kann Nachrichten zurückweisen, welche "unerlaubtes HTML" enthalten. Sollte diese Validierung gesetzt/eingeschaltet sein, dann darf in der Nachricht zusätzlich auch nur "https://" verwendet werden, "http://" ist untersagt.

Bitte erfragen Sie die Einstellung der erlaubten HTML-Elemente vom Betreiber des Nutzerkontos, an welches sie Nachrichten senden möchten.

Der Sender erhält Status-Code 31 "Unerlaubter Nachrichteninhalte", der ihn darauf hinweist, dass er nicht unterstützte HTML-Elemente verwendet. Die unzulässigen Elemente werden im Einzelnen aufgelistet.

Validiert werden 4 xml Elemente:

```
<BspNachricht xmlns="http://www.akdb.de/egov/bsp/nachrichten" version="1.5" fassung="2020-03-15">
  <NachrichtenKopf>
    ....
    <Absender>
      .....
      <Mandant>Ingolstadt</Mandant>                                html-
whitelist-valedierung 1
    ...
      <Hyperlink>http://www.akdb.de</Hyperlink>                    html-
whitelist-valedierung 2
    </Absender>
    .....
  </NachrichtenKopf>
  <NachrichtenInhalt>
    <Betreff>Nachrichtenbetreff Fri Mar 25 05:44:52 GMT 2022</Betreff>      html-
valedierung 3
    .....
    <FreiText>
      .....
      <Text>Nachrichtentext Fri Mar 25 05:44:52 GMT 2022</Text>          html-
whitelist-valedierung 4
    </FreiText>
  </NachrichtenInhalt>
</BspNachricht>
```

12.2 Beispiel einer Postfach-Nachricht

Minimale Postfach-Nachricht mit einem Anhang:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<BspNachricht xmlns="http://www.akdb.de/egov/bsp/nachrichten" version="1.5" fassung="2020-03-15">
  <NachrichtenKopf>
    <Identifikation.Nachricht>
      <Erstellungszeitpunkt>2023-09-08T12:29:03.419+02:00</Erstellungszeitpunkt>
      <NachrichtenId>1694168943419</NachrichtenId>
    </Identifikation.Nachricht>
    <Absender>
      <Dienst>Kitaanmeldung</Dienst>
      <Mandant>Ingolstadt</Mandant>
    </Absender>
    <Empfaenger>
      <PostkorbId>b10ae88e-8ca8-4a7f-b70c-f97b60f5f70c</PostkorbId>
    </Empfaenger>
  </NachrichtenKopf>
  <NachrichtenInhalt>
    <Betreff>Kitaanmeldung</Betreff>
    <StorkQaaLevel>LEVEL_1</StorkQaaLevel>
    <FreiText>
      <Encoding>
        <Tabelle>9004</Tabelle>
        <Schluessel>text/plain</Schluessel>
      </Encoding>
      <Text>Hallo,
      wie geht's?
      Viele Grüße</Text>
    </FreiText>
    <DataContainer>
      <Inhalt>ZG1lcyBpc3QgZWluIFRlc3QgQW5oYW5n</Inhalt>
      <FileName>testAnhang.txt</FileName>
      <FileType>
        <Tabelle>9005</Tabelle>
        <Schluessel>text/plain</Schluessel>
      </FileType>
    </DataContainer>
  </NachrichtenInhalt>
</BspNachricht>
```

12.2.1 Schlüsseltabellen

Die folgenden Schlüsseltabellen legen die zulässigen Werte für die jeweiligen Schlüsselfelder (z. B. bspEreignis im Nachrichtenkopf) in den Postfachnachrichten fest.

Einige werden nicht mehr genutzt und dienen nur noch der Dokumentation.

12.2.1.1 Schlüsseltabelle 9001

UNGENUTZT – KEINE VERWENDUNG.

Tabelle	9001
Name	Ereignisse
Beschreibung	Liste der möglichen Ereignisse
Schlüssel	Bedeutung
BSP	Nachricht vom oder zum Nutzerkonto

12.2.1.2 Schlüsseltabelle 9002

UNGENUTZT – KEINE VERWENDUNG.

Tabelle	9002
Name	Kategorie
Beschreibung	Nachrichtenkategorien
Schlüssel	Bedeutung
KAT_STATUS	Statusmeldung
KAT_INFOBSP	Information vom Nutzerkonto
KAT_INFOKOMMUNE	Information von der Kommune

12.2.1.3 Schlüsseltabelle 9003

UNGENUTZT – KEINE VERWENDUNG.

Tabelle	9003
Name	VorgangStatus
Beschreibung	Vorgangsstatus
Schlüssel	Bedeutung
ST_ERHALTEN	Nachricht wurde erhalten
ST_GELESEN	Nachricht wurde gelesen
ST_IN_ARBEIT	Nachricht wird bearbeitet
ST_FERTIG	Nachricht fertig bearbeitet

12.2.1.4 Schlüsseltabelle 9004

UNGENUTZT – KEINE VERWENDUNG.

Tabelle	9004
Name	TextEncoding
Beschreibung	Codierungsvarianten für Freitexte
Schlüssel	Bedeutung
text/plain	Einfacher ASCII-Text
text/html	Der Inhalt wird im HTML-Format übermittelt.
text/rtf	Der Inhalt wird im RTF-Format übermittelt.
text/xml	Der Inhalt wird im XML-Format übermittelt.

12.2.1.5 Schlüsseltabelle 9005

Tabelle	9005
Name	MIMETypes
Beschreibung	Codierungsvarianten für MIME-Anhänge
Schlüssel	Bedeutung
text/plain	Der Anhang wird als einfacher Text übermittelt (Dateinamenendung: „.txt“)
text/rtf	Der Anhang wird im RTF-Format übermittelt (Dateinamenendung: „.rtf“)
text/calendar	Der Anhang wird im ICS-Format übermittelt (Dateinamenendung: „.ics“)
text/comma-separated-values	Der Anhang wird im CSV-Format übermittelt (Dateinamenendung: „.csv“)
image/jpeg	Der Anhang wird als Bild im JPEG-Format übermittelt (Dateinamenendung: „.jpg“, „.jpe“, „.jpeg“, „.jfif“)
image/gif	Der Anhang wird als Bild im GIF-Format übermittelt (Dateinamenendung: „.gif“)
image/png	Der Anhang wird als Bild im PNG-Format übermittelt (Dateinamenendung: „.png“)
image/tiff	Der Anhang wird als Bild im TIF-Format übermittelt (Dateinamenendung: „.tiff“, „.tif“)
image/bmp	Der Anhang wird als Bild im BMP-Format übermittelt (Dateinamenendung: „.bmp“)

image/svg+xml	Der Anhang wird als Bild im SVG-Format übermittelt (Dateinamenendung: „.svg“)
application/pdf	Der Anhang wird im PDF-Format übermittelt (Dateinamenendung: „.pdf“)

12.2.1.6 Schlüsseltabelle 9006

Tabelle	9006
Name	Ergebnisstatus
Beschreibung	Ergebnisstatus des Empfangs einer Nachrichte
Schlüssel	Bedeutung
0	Nachricht wurde erfolgreich übernommen
10	Fehler im OK.KOMM-Schema
11	Ungültige Parameter im OK.KOMM-Schema
20	Fehler im BSP-Nachrichtenschema
30	Ungültiger Postkorb-Handle
31	Unzulässiger Nachrichteninhalt
32	Unzulässiger Nachrichtenanhang
99	Sonstiger technischer Fehler

13 Web-Service-Schnittstelle

Der Postfach-Service wird über eine Webservice-Schnittstelle angesprochen. Deren Definition ist in [1] zu finden.

Die WSDL [1] kann auch per URL-Aufruf `https://<HOST>/bspx-postkorb-okkomm-ws/bspservices/postkorbkomm.wsdl` abgefragt werden (gegebenenfalls sind Zugriffsbeschränkungen aktiv).

Beispiel: <https://id.bund.de/bspx-postkorb-okkomm-ws/bspservices/postkorbkomm.wsdl>.

Für einen erfolgreichen Request an den Webservice sind folgende Header erforderlich:

- SOAPAction: "urn:akdb:bsp:postkorb:komm:webservice"
- Content-Type: "text/xml; charset=utf-8"

Für den direkten Aufruf des Schnittstellen-Endpunkten ist üblicherweise ein Client-Zertifikat notwendig, welches beim Kundenservice gesondert angefordert werden muss.

Hinweis: Mit dem Programm *curl* kann man die Webservice-Requests einfach testen. Nachfolgend ein Beispiel-Aufruf unter Windows 10, wobei `<FILE_PATH>` auf eine Datei zeigt, die den kompletten SOAP-XML-Request enthält und `<HOST>` durch die reale Domain zu ersetzen ist.

Unter Umständen muss noch das Client Zertifikat bei diesem Aufruf angegeben werden (hier nicht mit angeben):

```
curl -k -H 'SOAPAction: "urn:akdb:bsp:postkorb:komm:webservice"' -H "Content-Type: text/xml; charset=utf-8" --data-binary @<FILE_PATH> -X POST https://<HOST>/bspx-postkorb-okkomm-ws/bspservices/postkorbkomm
```

13.1 Die WSDL Operation `sendBspNachrichtNative`

Diese Operation des Webservices stellt das einfachere Übertragungsformat der Postfach-Nachricht da.

Der Inputparameter `sendBspNachrichtNative/bspNachricht` enthält hier die jeweilige Postfach-Nachricht als String. Diese kann sowohl als "embedded XML" (escaped) oder als CDATA übergeben werden.

Ausgabe ist ebenfalls ein einfacher String mit der BSP-Quittung.

Wichtig: XML mit embedded XML unterliegt speziellen "Escaping"-Regeln. Wir empfehlen, dass die Request durch geeignete XML-Bibliotheken erzeugt und nicht von Hand erstellt werden.

13.1.1 Beispiel-Requests und -Responses für den Webservice

Webservice-Request einer minimalen Postfach-Nachricht mit einem Anhang:

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <ns3:sendBspNachrichtNative xmlns:ns3="urn:akdb:bsp:postkorb:komm:webservice">
      <bspNachricht>&lt;?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
&lt;BspNachricht xmlns="http://www.akdb.de/egov/bsp/nachrichten" version="1.5" fassung="2020-03-15" >
  &lt;NachrichtenKopf>
    &lt;Identifikation.Nachricht>
      &lt;Erstellungszeitpunkt>2023-09-08T12:29:03.419+02:00&lt;/Erstellungszeitpunkt>
      &lt;NachrichtenId>1694168943419&lt;/NachrichtenId>
    &lt;/Identifikation.Nachricht>
    &lt;Absender>
      &lt;Dienst>Kitaanmeldung&lt;/Dienst>
      &lt;Mandant>Ingolstadt&lt;/Mandant>
    &lt;/Absender>
    &lt;Empfaenger>
      &lt;PostkorbId>b10ae88e-8ca8-4a7f-b70c-f97b60f5f70c&lt;/PostkorbId>
    &lt;/Empfaenger>
  &lt;/NachrichtenKopf>
  &lt;NachrichtenInhalt>
    &lt;Betreff>Kitaanmeldung&lt;/Betreff>
    &lt;StorkQaaLevel>LEVEL_1&lt;/StorkQaaLevel>
    &lt;FreiText>
      &lt;Encoding>
        &lt;Tabelle>9004&lt;/Tabelle>
        &lt;Schluessel>text/plain&lt;/Schluessel>
      &lt;/Encoding>
      &lt;Text>Hallo,
wie geht's?
Viele Grüße&lt;/Text>
    &lt;/FreiText>
    &lt;DataContainer>
      &lt;Inhalt>ZGllcyBpc3QgZWluIFRlc3QgQW5oYW5n&lt;/Inhalt>
      &lt;FileName>testAnhang.txt&lt;/FileName>
      &lt;FileType>
        &lt;Tabelle>9005&lt;/Tabelle>
        &lt;Schluessel>text/plain&lt;/Schluessel>
      &lt;/FileType>
    &lt;/DataContainer>
  &lt;/NachrichtenInhalt>
&lt;/BspNachricht>
&lt;/sendBspNachrichtNative>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

```

        </ns3:sendBspNachrichtNative>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>

```

Webservice-Response – Erfolgreich:

```

SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <ns2:sendBspNachrichtNativeOutput xmlns:ns2="urn:akdb:bsp:postkorb:komm:webservice">
      <bspQuittung><?xml version="1.0" encoding="UTF-8" standalone="yes"?>
        <BspQuittung version="1.5" fassung="2020-03-15" xmlns="http://www.akdb.de/egov/bsp/nachrich-
        ten"><AnnahmeErfolgreich>true</AnnahmeErfolgreich> <ErgebnisStatus>
        <Tabelle>9006</Tabelle> <Schluessel>0</Schluessel> </ErgebnisSta-
        tus> </BspQuittung></bspQuittung>
      </ns2:sendBspNachrichtNativeOutput>
    </SOAP-ENV:Body>
  </SOAP-ENV:Envelope>

```

Webservice-Response – Fehler:

```

<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <ns2:sendBspNachrichtNativeOutput xmlns:ns2="urn:akdb:bsp:postkorb:komm:webservice">
      <bspQuittung><?xml version="1.0" encoding="UTF-8" standalone="yes"?>
        <BspQuittung version="1.5" fassung="2020-03-15" xmlns="http://www.akdb.de/egov/bsp/nachrich-
        ten"> <AnnahmeErfolgreich>false</AnnahmeErfolgreich> <ErgebnisStatus>
        <Tabelle>9006</Tabelle> <Schluessel>32</Schluessel> <ErgebnisSta-
        tus> <ErgaenzendeHinweise>Ein Anhang("testAnhang.txt") der Nachricht enthält eine un-
        zulässige Extension: "txt"</ErgaenzendeHinweise> </BspQuittung></bspQuittung>
      </ns2:sendBspNachrichtNativeOutput>
    </SOAP-ENV:Body>
  </SOAP-ENV:Envelope>

```

13.2 Die WSDL Operation `sendBspNachricht`

Diese Operation des Webservices stellt ein Übertragungsformat der Postfach-Nachricht da, welches primär für den Kommunikationsweg über die Transportplattform OK.KOMM gedacht ist.

Der Inputparameter `sendBspNachricht/okKommBspNachrichtInput` ist ein base64-codiertes Byte-Array, welches das OK.KOMM-Nachrichtenformat mit eingebetteter Postfach-Nachricht enthält.

Hinweis: Die eingebettete Postfach-Nachricht ist damit effektiv zweifach base64-codiert.

Ausgabe ist ebenfalls ist ein base64-codiertes Byte-Array, welches ein OK.KOMM-Nachrichtenformat mit den entsprechenden Bestätigungs- oder Fehlercode enthält.

13.2.1 OK.KOMM-Nachrichtenformat

Postfach-Nachrichten ans Nutzerkonto über OK.KOMM übermittelt. Deswegen erwartet der bisherige Postfach-Empfangsservice immer ein Format, in dem die reine Postfach-Nachricht zusätzlich in ein OK.KOMM-spezifisches XML-Nachrichtenformat (oft auch *OK.KOMM-Hülle* oder *ZKOCXML-Hülle* genannt) eingepackt ist.

Auch die OK.KOMM-Nachricht besitzt ein vordefiniertes XML-Schema, welches in [3] spezifiziert ist.

Die Postfach-Nachricht wird dabei als base64-codierter String Wert für das Element *ZKOCXML / XML_PROFIL / SUCHE / OK_KOMM_RAW_BASE64* der OK.KOMM-Nachricht eingebaut.

Folgende OK.KOMM-spezifischen Parameter müssen gesetzt werden, damit die Nachricht korrekt zum Ziel transportiert werden kann:

AKT_VERFAHREN	BSP
AKT_TYP	NACHRICHT
AKT_AUSFUEHRUNG	UEBERMITTELN
AKT_ZIEL_AGS	09999001

13.2.2 Beispiel für ein OK.KOMM Nachrichtenformat

Nachfolgend ein Beispiel einer fachlichen OK.KOMM Nachricht.

Beispiel einer OK.KOMM Nachricht einer minimalen Postfach-Nachricht mit einem Anhang:

```
<?xml version="1.0" encoding="UTF-8"?>
<ZKOCXML xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="../zkocxml.xsd">
  <XML_SYSTEM>
    <SYSTEM>
      <AKTION>
        <AKT_VERFAHREN>BSP</AKT_VERFAHREN>
        <AKT_TYP>NACHRICHT</AKT_TYP>
        <AKT_AUSFUEHRUNG>UEBERMITTELN</AKT_AUSFUEHRUNG>
        <AKT_ZIEL_AGS>09999001</AKT_ZIEL_AGS>
      </AKTION>
      <AKT_LOGIN>
        <AKT_TECHUSER/>
        <AKT_TECHPWD/>
      </AKT_LOGIN>
      <ANTWORT>
        <ANT_TYP/>
        <ANT_APPS/>
        <ANT_STRUKTUR/>
        <ANT_DATUM/>
        <ANT_UHRZEIT/>
        <FEHLER>
          <FEH_TYP/>
          <FEH_TEXT/>
          <FEH_WERT/>
          <FEH_FELD/>
        </FEHLER>
      </ANTWORT>
      <APPS_INFO>
        <APPS_TYP>APPS_TYP</APPS_TYP>
        <APPS_NAME>ZDL</APPS_NAME>
        <APPS_VERSION>1.0.0</APPS_VERSION>
        <APPS_AGS>yyy</APPS_AGS>
        <APPS_DATUM>12.09.2023</APPS_DATUM>
        <APPS_UHRZEIT>14:38:55</APPS_UHRZEIT>
        <APPS_REQUEST_ID/>
        <APPS_SOURCE_ID/>
        <APPS_KENNUNG/>
        <APPS_IP_ADRESSE/>
        <APPS_ZIEL_URL/>
        <APPS_RETURN_QUEUE/>
      </APPS_INFO>
    </SYSTEM>
  </XML_SYSTEM>
</ZKOCXML>
```

```

</XML_SYSTEM>
<XML_DATEN>
  <DATEN/>
</XML_DATEN>
<XML_PROFIL>
  <SUCHE>

    <OK_KOMM_RAW_BASE64>PD94bWwgdmVyc2lvcj0iMS4wIiBlbmNvZGluZz0iVVRGLT-
giIHN0YW5kYWxvbmU9InllcyI/Pg0KPEJzcE5hY2hyaWNodCB4bWxucz0iaHR0cDovL3d3dy5ha2RiLm-
RlL2Vnb3YvYnNwL25hY2hyaWNodGVuIiB2ZXJzaW9uPSIxLjUiIGZhc3N1bmc9IjIwMjAtMDMtMTUuPg0KI-
CAGIDxOYWNocmljaHRlbktvcGY+DQogICAgICAgIDxJZGVudGlmawthdGlvbi5OYWNocmljaHQ+DQogICAgICAgI-
CAGICA8RXJzdGVsbHVuZ3N6ZWl0cHVua3Q+MjAyMy0wOS0wOFQxMjoyOTowMy40MTkrMDI6MDA8L0Vyc3RlbGx1bmd-
zemVpdHB1bmt0Pg0KICAgICAgICAgICAgPE5hY2hyaWNodGVuSWQ+MTY5NDE2ODk0MzQxOTwvTmF-
jaHJpY2h0ZW5JZD4NCiAgICAgICAgPC9JZGVudGlmawthdGlvbi5OYWNocmljaHQ+DQogICAgICAgIDxBYnN-
lbmRlcj4NCiAgICAgICAgICAgIDxEaWVuc3Q+S2l0YWFubWVzZHVuZzZwvRG1lbnN0Pg0KICAgICAgICAgI-
CAGPE1hbmRhbHQ+SW5nb2xzZGFkdDwvTWFuZGFudD4NCiAgICAgICAgPC9BYnNlbmRlcj4NCiAgICAgICAgPE-
VtcGZhZW5nZXI+DQogICAgICAgICAgICA8UG9zdGtvcmlJZD5iMTBhZTg4ZS04Y2E4LTRhN2YtYjcwYy1mOTdiN-
jBmNWY3MGM8L1Bvc3Rrb3JiSWQ+DQogICAgICAgICAgIDwvRWlWZmFlbmdlcj4JDQogICAgPC9OYWNocmljaHRlbkt-
vcGY+DQogICAgPE5hY2hyaWNodGVuSW5oYWw0Pg0KICAgI-
CAGICA8QmV0cmVmZj5LaXRhYW5tZWxkdW5nPC9CZXRYZWZmPg0KICAgICAgICA8U3RvcmtRY-
WFMZXXZ1bD5MRVZFTF8xPC9TdG9ya1FhYUxldmVsPg0KICAgICAgICA8RnJlaVRleHQ+DQogICAgICAgI-
CAGICA8RW5jb2Rpbmc+DQogICAgICAgICAgICAgICAgPFRhYmVsbGU+OTAwNDwvVGFiZWxsZT4NCiAgICAgICAgICAgI-
CAGICA8U2NobHVlc3N1bD50ZXh0L3BsYWluPC9TY2hsdWVzc2VsPg0KICAgICAgICAgICAgPC9FbmNvZGluZz4NCiAgI-
CAGICAgICAgIDxUZXh0PkhhbGxvLCAncGkKJCXdpZSBnZW50J3M/DQoJCQlWaWVsZSBHcs08w59lPC9UZXh0Pg0KICAgI-
CAGICA8L0ZyZWlUZXh0Pg0KCQk8RGF0YUNvbnRhaW5lcj4NCgkKJCTxJbmhhbHQ+WkdsbGN5QnBjM1FnWlZsdU1-
GUmxjM1FnUVc1b1lXNW48L0luaGFsdD4NCgkKJCTxGaWxlTmFtZT50ZXN0QW5oYW5nLnR4dDwvRm-
lsZU5hbWU+DQoJCQk8RmlsZVR5cGU+DQoJCQkJPFRhYmVsbGU+OTAwNTwvVGFiZ-
WxsZT4NCgkKJCQk8U2NobHVlc3N1bD50ZXh0L3BsYWluPC9TY2hsdWVzc2VsPg0KCQkJPJC9GaWxlVH1-
wZT4NCgkKJPC9EYXRhQ29udGFpbmVYPgkKJCQ0KICAgIDwvTmFjaHJpY2h0ZW5JbmhhbHQ+DQo8L0JzcE5hY2hya-
WNodD4=</OK_KOMM_RAW_BASE64>

  </SUCHE>
</XML_PROFIL>
</ZKOCXML>

```

13.2.3 OK.KOMM-Antwort

Zu jeder erfolgreich übernommenen OK.KOMM-Postfach-Nachricht wird eine OK.KOMM-Antwort zurückgeschickt (synchrone Kommunikation).

Der Aufbau der OK.KOMM-Antwort ist dabei identisch zur Anfrage, lediglich die <XML_PROFIL></XML_PROFIL>-Komponente ist aus Performancegründen nicht mehr gefüllt.

Fehlersituationen beim Empfang von OK.KOMM-Postfach-Nachrichten werden über SOAP-Exceptions signalisiert.

Dabei wird der Fehlergrund in der Komponente <faultString> der SOAP-Exception mitgeteilt.

Dieser setzt sich aus einem Fehlercode und einem erläuternden Text zusammen.

In der aktuellen Version des Nutzerkonto wenden folgende Fehlerkonstellationen unterschieden:

Fehlercode	Fehlerursache
BSP1010	Fehler im OK.KOMM-Schema
BSP1011	Ungültige Parameter im OK.KOMM-Schema
BSP1020	Fehler im BSP-Nachrichtenschema
BSP1030	Ungültiger Postfach-handle
BSP1031	Unzulässiger Nachrichteninhalt
BSP1032	Unzulässiger Nachrichtenanhang
BSP1999	Sonstiger technischer Fehler

13.2.4 Beispiel-Requests und -Responses für den Webservice

Nachfolgende ein Request bei dem die fachliche OK:KOMM Nachricht in Base64 umgewandelt und im Webservice-Request benutzt wurde.

Webservice-Request einer minimalen Postfach-Nachricht mit einem Anhang:

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <ns3:sendBspNachricht xmlns:ns3="urn:akdb:bsp:postkorb:komm:webservice">
      <okKommBspNachrichtInput>PD94bWwgdmVyc2lrbj0iMS4wIiBlbmNvZGluZz0iVVRGLT-
giPz4NCjxaS09DWE1MIHhtbG5zOnhzaT0iaHR0cDovL3d3dy53My5vcmcvMjAwMS9YTUxTY2h1bWEtaW5zdGFuY2UiIHh-
zaTpub05hbWVzcGFjZVNjaGVtYUxvY2F0aW9uPSIuLi96a29jeG1sLnhzZCI+DQr-
CoCA8WE1MX1NZU1RFTT4NCsKgIMKgIDxTWVNURU0+DQrCoCDCoCDCoCA8QUtUSU9OPg0KwqAgwqAgwqAg-
wqAgPEFLVF9WRVJGQUhSRU4+Q1NQPC9BS1RfVkvSRkFIUkVOPg0KwqAgwqAgwqAg-
wqAgPEFLVF9UWVA+TkFDSFJJQ0hUPC9BS1RfVf1QPg0KwqAgwqAgwqAgwqAgPEFLVF9BVVNGVUVIU1-
VORz5VRUJFuk1JVFRFTE48L0FLVF9BVVNGVUVIU1VORz4NCsKgIMKgIMKgIMKgIDxBS1RfWk1FTF9BR1M+MDk5OT-
kwMDE8L0FLVF9aSUVMX0FHUz4NCsKgIMKgIMKgIDwvQUtUSU9OPg0KwqAgwqAg-
wqAgPEFLVF9MT0dJTj4NCsKgIMKgIMKgIMKgIDxBS1RfVEVDSFVTR
```

VIgIz4NCsKgIMKgIMKgIMKgIDxBs1RfVEVDSFBXRCaVpG0KwqAgwqAgwqAgPC9BS1RfTE9HSU4+DQr-
 CoCDCoCDCoCA8QU5UV09SVD4NCsKgIMKgIMKgIMKgIDxBt1RfVf1QIC8+DQrCoCDCoCDCoCDCoCA8QU5UX0FQUFM-
 gLz4NCsKgIMKgIMKgIMKgIDxBt1RfU1RSVUtUVVIgIz4NCsKgIMKgIMKgIMKgIDxBt1RfREFUVU0gLz4NCsKgIMKgIMKgIMKgIDxBt1RfVUhSWkVJVCaVpG0KwqAgwqAgwqAgwqAgPEZFSEx-
 FUj4NCsKgIMKgIMKgIMKgIMKgIDxGRUhfVf1QIC8+DQr-
 CoCDCoCDCoCDCoCA8RkVIX1RFWFQgIz4NCsKgIMKgIMKgIMKgIMKgIDxGRUhfV0VSVCAvPg0KwqAgwqAgwqAgwqAgwqAgPEZFSF9GRUXEIC8+DQrCoCDCoCDCoCDCoCA8L0ZFSEx-
 FUj4NCsKgIMKgIMKgIDwvQU5UV09SVD4NCsKgIMKgIMKgIDxBUFBTX0lORk8+DQr-
 CoCDCoCDCoCDCoCA8QVBQU19UWVA+QVBQU19UWVA8L0FQUFNfVf1QPg0KwqAgwqAgwqAgwqAgPEFQUFNfT-
 kFNRT5aREw8L0FQUFNfTkJFNRT4NCsKgIMKgIMKgIMKgIDxBUFBTX1ZFU1NJT04+MS4wLjA8L0FQUF-
 NfVkvSU01PTj4NCsKgIMKgIMKgIMKgIDxBUFBTX0FHUz55eXk8L0FQUFNfQUdTPg0KwqAgwqAgwqAgwqAgPEFQUFN-
 fREFUVU0+MTIuMDkuMjAyMzwvQVBQU19EQVRVTT4NCsKgIMKgIMKgIMKgIDxBUFBTX1VIU1-
 pFSVQ+MTQ6Mzg6NTU8L0FQUFNfVUhSWkVJVD4NCsKgIMKgIMKgIMKgIDxBUF-
 BTX1JFUVVFU1RfSUQgIz4NCsKgIMKgIMKgIMKgIDxBUFBTX1NPVVJDRV9JRCaVpG0KwqAgwqAgwqAgwqAgPEFQUF-
 NfS0VOT1VORyAvPg0KwqAgwqAgwqAgwqAgPEFQUFNfSVBfQURSRVNTRSaVpG0KwqAgwqAgwqAgwqAgPEFQUF-
 NfWk1FTF9VUkwgIz4NCsKgIMKgIMKgIMKgIDxBUFBTX1JFVfVST19RVUVVRSaVpG0KwqAgwqAgwqAgPC9BUF-
 BTX0lORk8+DQr-
 CoCDCoCDCoCA8L1NZU1RFTT4NCsKgIMKgIMKgIDwvWE1MX1NZU1RFTT4NCsKgIMKgIMKgIDxYTUxfREFURU4+DQo8REFUR
 U4gLz48L1hNTF9EQVRFTj4NCsKgIMKgIMKgIDxYTUxfUFJPRklMPg0KwqAgwqAgPFNVQ0hFPg0KwqAgwqAg-
 wqAgPE9LX0tPTU1fUkFXX0JBU0U2ND5QRDk0Yld3Z2RtVnljMmx2YmowaU1TNHdJaUJsYm1Od-
 lpHbHVaejBpVlZSR0xUZ2lJSE4wWVc1a1lXeHziBVU5SW5sbGN5SS9QZzBLUEVKem-
 NFNWhZMmh5YVdOb2RDQjRiV3h1Y3owaWFIUjBjRG92TDNkM2R5NWhhMlJpTG1SbE-
 wyVm5iM1l2WW5Od0wyNWhZMmh5YVdOb2RHVNvJaUiYlWhKemFXOXVQU0l4TGpVaU1HWmhjM04xYm1jOUlqSXd-
 NakF0TURNdE1UVWlQZzBLSUNBZ0lEeE9ZV05vY2l1samFIUmXia3R2Y0dZK0RRb2dJQ0FnSUNBZ0lEeEpaR1Z1ZEds-
 bWFXdGhkR2x2Ymk1T1lXTm9jbWxqYUhrK0RRb2dJQ0FnSUNBZ0lDQWdJQ0E4UlhKemRHVNnISFZ1WjNON-
 lpXbDBjSFZ1YTNRK0lqQXlNeTB3T1Mwd09GUXhNam95T1Rvd0l5NDBNVGtyTURJNk1EQThMMFZ5YzNSbGJHeD-
 FibWR6ZW1wCGRIQjFibXQwUGcwS0lDQWdJQ0FnSUNBZ0lDQWdQRTVoWTJoewFXtm9kr1Z1U1dRK0lUWT-
 VOREUyT0RrME16UXhPVhd2VG1GamFISnBZMmgwW1c1SlpENE5DaUFnSUNBZ0lDQWdQZz1KwkdWdWRHbG1hV3RoZE-
 dsdmJpNU9ZV05vY2l1samFIUStEUW9nSUNBZ0lDQWdJRhhCWW5ObGJtUmxjaJROQ2lBZ0lDQWdJQ0FnSUNBZ0lEeE-
 VhV1Z1YzNRK1MybDBZV0Z1YldWc1pIVnVaend2UkdsbGJuTjBQZz-
 BLSUNBZ0lDQWdJQ0FnSUNBZ1BFMWhibVJoYm5RK1NXNW5iMnh6ZEdGa2Red3ZUV0Z1WkdGdWRENE5DaUF-
 nSUNBZ0lDQWdQZz1CWW5ObGJtUmxjaJROQ2lBZ0lDQWdJQ0FnUEVWdGNHwM-
 haVzVuW1hJK0RRb2dJQ0FnSUNBZ0lDQWdJQ0E4VUc5emRHdHZjbUpKwKQ1aU1UQmhaVGc0W1MwNFkyRTRMVfJoTjJZd-
 FlqY3dZeTfTt1RkaU5qQm1OV1kzTudNOEwxQnzjM1JyYjNKAVNxu-
 StEUW9nSUNBZ0lDQWdJRhd2Ulcxd1ptRmxibWRsY2o0SkRRb2dJQ0FnUEM5T1lXTm9jbWxqYUhsbGJrdHHzjR1krR-
 FFvZ0lDQWdQRTVoWTJoewFXtm9kr1Z1U1c1b1lXeDBQZzBLSUNBZ0lDQWdJQ0E4UW1WMGntVm1aaJVMYVhSaF-
 lXNXRAv3hrZFc1b1BDOUNaWfJ5WldabVBnMEtJQ0FnSUNBZ0lDQThVM1J2Y210U1lXRk1aWfPysYkQ1TVJWWk-
 ZURjh4UEM5VGRHOXlhMUZoWVv4bGRtVnNQZzBLSUNBZ0lDQWdJQ0E4Um5KbGFWUmx1SFER-
 FFvZ0lDQWdJQ0FnSUNBZ0lDQThSVzVqYjJScGJtYyTEUW9nSUNBZ0lDQWdJQ0FnSUNBZ0lDQWdQR1JoWW1Wc2JHVSt-
 PVEF3Tkr3dlZHRmlaV3hzWlQ0TkNpQWdJQ0FnSUNBZ0lDQWdJQ0FnSUNBOFUyTm9iSFZsYzNOBgJENT-
 BaWGgWTDNCc1lXbHVQQz1UWTJoc2RXVnpjM1ZzUGcwS0lDQWdJQ0FnSUNBZ0lDQWdQZz1GYm1Od-
 lpHbHVaejROQ2lBZ0lDQWdJQ0FnSUNBZ0lEeEFVaWGgUGtoagJHeHZMQ0FOQ2drSkNYZHBaU0JuWldoMEo-
 zTS9EUW9KQ1FsV2FXVnNaU0JiY3NPOhc1OWxQZz1VWlhoMFBnMEtJQ0FnSUNBZ0lDQThMMFp5WldsvVpYaDBQZz-
 BLQ1FrOfJHRjBZVU52Ym5SaGFXNWxjaJROQ2drSkNUeEpibWhoYkhRK1drZHNiR04lUW5Cak0xRm5XbGrZzFVsR1VteG-
 pNMUzuVvZjMWIxbFhOVzQ4TDBsdWfHRnNkRDROQ2drSkNUeEdhV3hsVG1GdFpUNT-
 BaWE4uUvc1b1lXNW5Mb1I0ZER3dlJtbHNaVTVoYldVK0RRb0pDUWs4Um1sc1pWUjVjR1UrRFFvS-
 kNRa0pQR1JoWW1Wc2JHVStPVEF3TlR3dlZHRmlaV3hzWlQ0TkNna0pDUWs4VTJob2JIV-
 mxjM05sYkQ1MFpYaDBMM0JzWVdsdVBDOVRZMmhZzFdwemMyVnNQZz-

```

BLQ1FrS1BDOUdhV3hsVkhsd1pUNE5DZ2tKUEM5RV1YUmhRmj1lZEdGcGJtVn1QZ2tKQ1Ews0lDQWdJRhd2VG1GamFIS-
nBZMmgwW1clSmJtaGhiSFERFFvOEwwSnpjRTVoWTJoeWFXtm9kRDQ9PC9PS19LT01NX1JBV19CQVNFNjQ+DQr-
CoCDCoCa8L1NVQ0hFFpG0KwqAgPC9YTUxfUfJPRklMPg0KPC9aS09DWE1MPg==</okKommBspNachrichtInput>

</ns3:sendBspNachricht>

</SOAP-ENV:Body>

</SOAP-ENV:Envelope>

```

Response einer OK.KOMM Nachricht: **Webservice-Response – Erfolgreich**

[illegible]

Webservice-Response – Fehler:

```

SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <SOAP-ENV:Fault>
      <faultcode>BSP1032</faultcode>
      <faultstring>Unzulässiger Nachrichtenanhang</faultstring>
    </SOAP-ENV:Fault>
    <ns2:sendBspNachrichtOutput xmlns:ns2="urn:akdb:bsp:postkorb:komm:webservice">
      <okKommBspNachrichtOutput>PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluz0idXRmLT-
giIHNOYW5kYWxvbmU9InllcyI/PjxaS09DWE1MPjxYTUxfU1lTVEVNPjxTWVNURU0+PEFLVElPTi8+PEFOVfdPULQ+PE-
FOVF9UWVA+RkVITEVSPC9BTlRfVf1QPjxBTlRfREFUVU0+MTIuMDkuMjAyMzwvQU5UX0RBVFNPNjxBTlRfVUhS-
WkVJVd4wODoyMD0NDwvQU5UX1VIUlpFSVQ+PEZFSEx-
FUj48RkVIX1RZUD5CU1AxMDMyPC9GRUhfVf1QPjxGRUhfVEVYVD5FaW4gQW5oYW5nKCJ0ZXNQW5oYW5nLnR4dCI-
pIGRlciBOYWNocml-
jaHQgZW50aM0kbHQgZWluZSB1bnplbM0kc3NpZ2UgRXh0ZW5zaW9uOiAidHh0IjwvRkVIX1RFRWFQ+PEZ-
FSF9XRJVJUP1VuenVsw6Rzc2lnZXIgtmFjaHJpY2h0ZW5hbmhbmhc8L0ZFSEF9XRJVJUPjxGRUh-
frkVMRD5CU1AtQU5IPC9GRUhfRkVMRD48L0ZFSEx-
FUj48L0FOVfdPULQ+PC9TWVNURU0+PC9YTUxfU1lTVEVNPjwvWktPQ1hNTD4=</okKommBspNachrichtOutput>
    </ns2:sendBspNachrichtOutput>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>

```



```
</SOAP-ENV:Body>  
</SOAP-ENV:Envelope>
```

14 Absicherung der Schnittstelle

Der Endpunktpfad der Webservice-Schnittstelle ist in der Regel mit einer Art Authentifizierung über ein Client Zertifikat (Stichwort: two-way-ssl) oder IP Whitelisting versehen.

Bitte erfragen Sie die Art der Absicherung vom Betreiber des Nutzerkontos, an welches sie Nachrichten senden möchten.

14.1 Two-Way-SSL Client Authentifizierung

Wenn die Webservice-Schnittstelle mit einer Authentifizierung über ein Client Zertifikat (Stichwort: two-way-ssl) abgesichert ist, muss dieses in der **sendenden Anwendung** importiert/benutzt werden, damit die Anwendung den Endpunkt erfolgreich aufrufen kann.

Ein Client Zertifikat zum Einstellen von Postfach-Nachrichten kann vom Kundenservice/Support/Betrieb angefordert werden.

Die Einbindung des Zertifikates in die Anwendung ist dabei abhängig von der verwendeten Technologie und ist nicht Bestandteil dieser Dokumentation.

15 Anhänge und Verzeichnisse

15.1 Abbildungen

Abbildung 1: Zusammenspiel der Komponenten in der offenen Infrastruktur des Portalverbunds	13
Abbildung 2: Öffentlich zugänglicher Bereich der Service-Provider-Applikation.....	14
Abbildung 3: Authentisierung	15
Abbildung 4: Geschützte Ressource – OZG-Informationsplattform.....	16
Abbildung 5: Pop-Up Dialog zur Weiterleitung an die BundID.....	42
Abbildung 6: Buttons der BundID.....	43
Abbildung 7: BundID Desktop Details.....	44
Abbildung 8: BundID Mobile Details.....	44
Abbildung 9: Postfachnachrichten Transportwege Variante 1	57
Abbildung 10: Postfachnachrichten Transportwege Variante 2	58

15.2 Verweise auf externe Dokumente

- Portalverbundvereinbarung
- Beitrittserklärung zum Portalverbund im Testbetrieb
- Beitrittserklärung zum Portalverbund im Wirkbetrieb
- Handreichung zum Nachweis der Beweiswerterhaltung bei Online Ausweis Funktion-Nutzung

15.3 Verwendete Abkürzungen

Kürzel	Ausführliche Benennung
SAML	Security Assertion Markup Language von OASIS
OASIS	Organization for the Advancement of Structured Information Standards
IDP	Identity Provider , die Authentisierungsinstanz
SP	Service-Provider, die Drittanwendung (ggf. inkl. Reverse Proxy)
SSO	Single Sign On

TLS

Transport Layer Security

15.4 Annex: Webservice Schema Dateien

15.4.1 Schemadatei – bspnachrichten-2.13.xsd

```
<?xml version="1.0" encoding="UTF-8"?>
<!--

Service- und Portalplattform
AKDB München, Geschäftsfeld eGovernment

Copyright (c) AKDB

-->
<xsd:schema targetNamespace="http://www.akdb.de/egov/bsp/nachrichten"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:bsp="http://www.akdb.de/egov/bsp/nachrichten"
  elementFormDefault="qualified">

  <xsd:element name="BspNachricht">
    <xsd:annotation>
      <xsd:appinfo>
        <title>Nachricht für die Kommunikation zwischen Bürgerservice-Portal
          und externen Fachverfahren</title>
      </xsd:appinfo>
      <xsd:documentation>Einheitliches Nachrichtenschema für die
        Kommunikation zwischen Bürgerservice-Portal und externem Verfahren.
        Nachrichten vom Bürgerservice-Portal an den Postkorb eines
        Verfahrens
        oder Nachrichten von den Verfahren an das Bürgerservice-Portal müssen
        gemäß diesem Schema aufgebaut sein.
      </xsd:documentation>
    </xsd:annotation>
    <xsd:complexType>
      <xsd:sequence>
        <xsd:element name="NachrichtenKopf" type="bsp:NachrichtenKopfType"/>
        <xsd:element name="NachrichtenInhalt" type="bsp:NachrichtenInhaltType"/>
      </xsd:sequence>
      <xsd:attribute name="version" use="required">
        <xsd:annotation>
          <xsd:documentation>Dieses Attribut kennzeichnet die
            Nachrichten-Version, z. B. "1.0", "1.1".</xsd:documentation>
        </xsd:annotation>
      <xsd:simpleType>
        <xsd:restriction base="xsd:string">
```

```

    <xsd:enumeration value="1.1"/>
    <xsd:enumeration value="1.2"/>
    <xsd:enumeration value="1.3"/>
    <xsd:enumeration value="1.4"/>
    <xsd:enumeration value="1.5"/>
  </xsd:restriction>
</xsd:simpleType>
</xsd:attribute>
<xsd:attribute name="fassung" use="required" >
  <xsd:annotation>
    <xsd:documentation>Dieses Attribut kennzeichnet das Datum, an dem
      die diesen Schemata im Status final produziert wurde. Format:
      YYYY-MM-DD.</xsd:documentation>
  </xsd:annotation>
</xsd:simpleType>
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="2017-03-15"/>
    <xsd:enumeration value="2018-04-01"/>
    <xsd:enumeration value="2018-11-01"/>
    <xsd:enumeration value="2019-06-28"/>
    <xsd:enumeration value="2020-03-15"/>
  </xsd:restriction>
</xsd:simpleType>
</xsd:attribute>
<xsd:attribute name="produkt" type="xsd:string" use="optional">
  <xsd:annotation>
    <xsd:documentation>In diesem Attribut ist der Name des Produktes
      (der Software) einzutragen, mit dem diese Nachricht erstellt
      worden ist. z.B. BSP, PWS</xsd:documentation>
  </xsd:annotation>
</xsd:attribute>
<xsd:attribute name="produkthersteller" type="xsd:string" use="optional"/>
<xsd:attribute name="produktversion" type="xsd:string" use="optional"/>
</xsd:complexType>
</xsd:element>

<xsd:element name="BspQuittung">
  <xsd:annotation>
    <xsd:appinfo>
      <title>Quittung über den Empfang einer BSO-Nachricht</title>
    </xsd:appinfo>
    <xsd:documentation>Zu einer empfangenen BSP-Nachricht wird eine
      Quittung geliefert, die bestätigt, dass die Nachricht übernommen wurde

```

oder aufgrund eines technischen oder fachlichen Fehlers abgewiesen wurde.

```

</xsd:documentation>
</xsd:annotation>
<xsd:complexType>
  <xsd:sequence>
    <xsd:element name="AnnahmeErfolgreich" type="xsd:boolean" minOccurs="1" maxOccurs="1"/>
    <xsd:element name="ErgebnisStatus" type="bsp:SchluesseltabelleType" minOccurs="1" maxOccurs="1">
      <xsd:annotation>
        <xsd:documentation>Schluesseltabelle 9006 (0 (erfolgreich angenommen), 99 (sonstiger technischer Fehler), ...)</xsd:documentation>
      </xsd:annotation>
    </xsd:element>
    <xsd:element name="ErgaenzendeHinweise" type="xsd:string" minOccurs="0" maxOccurs="1"/>
  </xsd:sequence>
  <xsd:attribute name="version" use="required">
    <xsd:annotation>
      <xsd:documentation>Dieses Attribut kennzeichnet die
        Nachrichten-Version, z. B. "1.0", "1.1".</xsd:documentation>
    </xsd:annotation>
  <xsd:simpleType>
    <xsd:restriction base="xsd:string">
      <xsd:enumeration value="1.1"/>
      <xsd:enumeration value="1.2"/>
      <xsd:enumeration value="1.3"/>
      <xsd:enumeration value="1.4"/>
      <xsd:enumeration value="1.5"/>
    </xsd:restriction>
  </xsd:simpleType>
</xsd:attribute>
<xsd:attribute name="fassung" use="required">
  <xsd:annotation>
    <xsd:documentation>Dieses Attribut kennzeichnet das Datum, an dem
      die diesen Schemata im Status final produziert wurde. Format:
      YYYY-MM-DD.</xsd:documentation>
  </xsd:annotation>
<xsd:simpleType>
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="2017-03-15"/>
    <xsd:enumeration value="2018-04-01"/>
    <xsd:enumeration value="2018-11-01"/>
    <xsd:enumeration value="2019-06-28"/>
    <xsd:enumeration value="2020-03-15"/>
  </xsd:restriction>
</xsd:simpleType>

```

```

</xsd:attribute>
<xsd:attribute name="produkt" type="xsd:string" use="optional">
  <xsd:annotation>
    <xsd:documentation>In diesem Attribut ist der Name des Produktes
      (der Software) einzutragen, mit dem diese Nachricht erstellt
      worden ist. z.B. BSP, PWS</xsd:documentation>
  </xsd:annotation>
</xsd:attribute>
<xsd:attribute name="produkthersteller" type="xsd:string" use="optional"/>
<xsd:attribute name="produktversion" type="xsd:string" use="optional"/>
</xsd:complexType>
</xsd:element>

<xsd:complexType name="NachrichtenKopfType">
  <xsd:sequence>
    <xsd:element name="Identifikation.Nachricht" type="bsp:Identifikation.NachrichtType" maxOccurs="1" minOccurs="1"/>
    <xsd:element name="Anwenderkennung" type="xsd:string" minOccurs="0">
      <xsd:annotation>
        <xsd:documentation> Die Anwenderkennung stellt Informationen über die absendende Person
          zur Verfügung und dient der Protokollierung.
          Anhand dieser Kennung kann die absendende Person identifiziert werden.
        </xsd:documentation>
      </xsd:annotation>
    </xsd:element>
    <xsd:element name="Absender" type="bsp:AbsenderType" maxOccurs="1" minOccurs="1"/>
    <xsd:element name="Empfaenger" type="bsp:EmpfaengerType" maxOccurs="1" minOccurs="1"/>
    <xsd:element name="AntwortAuf" type="xsd:string" maxOccurs="1" minOccurs="0">
      <xsd:annotation>
        <xsd:documentation>Eine Nachricht kann mit einer exisiterenden
          Nachricht in Beziehung gebracht werden als Antwortnachricht oder
          weitergeleitete Nachricht. Der Bezug erfolgt hierbei über die
          NachrichtenId.
        </xsd:documentation>
      </xsd:annotation>
    </xsd:element>
    <xsd:element name="WeiterleitungZu" type="xsd:string" minOccurs="0"/>
    <xsd:element name="lesebestaetigungAntwortAdresse" type="xsd:string" minOccurs="0"/>
  </xsd:sequence>
</xsd:complexType>
<xsd:complexType name="Identifikation.NachrichtType">
  <xsd:sequence>
    <xsd:element name="Ereignis" type="bsp:SchluesseltabelleType">
      <xsd:annotation>

```



```

    <xsd:documentation>Schluesseltabelle 9001, Schluesel: BspNachricht
  </xsd:documentation>
</xsd:annotation>
</xsd:element>
<xsd:element name="Erstellungszeitpunkt" type="xsd:dateTime" maxOccurs="1" minOccurs="1"/>
<xsd:element name="NachrichtenId" type="xsd:string" maxOccurs="1" minOccurs="1">
  <xsd:annotation>
    <xsd:documentation>eine beliebige, eindeutige ID, die durch den
      erstellenden Client generiert wird. Zusammen mit
      Erstellungszeitpunkt und Absender kann eine Nachricht bsp-global
      eindeutig identifiziert werden.
    </xsd:documentation>
  </xsd:annotation>
</xsd:element>
</xsd:sequence>
</xsd:complexType>

<xsd:complexType name="AbsenderType">
  <xsd:sequence>
    <xsd:element name="PostkorbId" type="xsd:string" maxOccurs="1" minOccurs="0"/>
    <xsd:element name="Verfahren" type="xsd:string" maxOccurs="1" minOccurs="0"/>
    <xsd:element name="Dienst" type="bsp:NonEmptyString" maxOccurs="1" minOccurs="0"/>
    <xsd:element name="Mandant" type="bsp:NonEmptyString" maxOccurs="1" minOccurs="0"/>
    <xsd:element name="Gemeindeschluessel" type="bsp:SchluesseltabelleType" minOccurs="0">
      <xsd:annotation>
        <xsd:documentation>Der amtliche Gemeindeschlüssel (AGS).
          Als Tabellennummer ist hier die 36 (OSCI-XMeld-Schlüsseltabelle "Amtlicher Gemeindeschluessel") zu verwenden.
        </xsd:documentation>
      </xsd:annotation>
    </xsd:element>
    <xsd:element name="Name" type="xsd:string" maxOccurs="1" minOccurs="0"/>
    <xsd:element name="Anschrift" type="xsd:string" maxOccurs="1" minOccurs="0"/>
    <xsd:element name="Email" type="xsd:string" maxOccurs="1" minOccurs="0"/>
    <xsd:element name="Telefon" type="xsd:string" maxOccurs="1" minOccurs="0"/>
    <xsd:element name="Hyperlink" type="xsd:string" maxOccurs="1" minOccurs="0"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="EmpfaengerType">
  <xsd:sequence>
    <xsd:element name="PostkorbId" type="xsd:string" maxOccurs="1" minOccurs="1"/>
    <xsd:element name="Verfahren" type="xsd:string" maxOccurs="1" minOccurs="0"/>
    <xsd:element name="Dienst" type="xsd:string" maxOccurs="1" minOccurs="0"/>

```

```

<xsd:element name="Mandant" type="xsd:string" maxOccurs="1" minOccurs="0"/>
<xsd:element name="Gemeindeschluessel" type="bsp:SchluesseltabelleType" minOccurs="0">
  <xsd:annotation>
    <xsd:documentation>Der amtliche Gemeindeschlüssel (AGS).
      Als Tabellennummer ist hier die 36 (OSCI-XMeld-Schlüsseltabelle "Amtlicher Gemeindeschlüssel") zu verwenden.
    </xsd:documentation>
  </xsd:annotation>
</xsd:element>
<xsd:element name="Name" type="xsd:string" maxOccurs="1" minOccurs="0"/>
<xsd:element name="Anschrift" type="xsd:string" maxOccurs="1" minOccurs="0"/>
</xsd:sequence>
</xsd:complexType>

<xsd:complexType name="NachrichtenInhaltType">
  <xsd:sequence>
    <xsd:element name="Betreff" type="bsp:NonEmptyString" maxOccurs="1" minOccurs="1"/>
    <xsd:element name="Kategorie" type="bsp:SchluesseltabelleType" minOccurs="0">
      <xsd:annotation>
        <xsd:documentation>Schluesseltabelle 9002 (KAT_STATUS, KAT_INFOBSP, ...)
      </xsd:documentation>
    </xsd:annotation>
    </xsd:element>
    <xsd:choice minOccurs="0">
      <xsd:element name="StorkQaaLevel" type="bsp:StorkQaaLevel"/>
      <xsd:element name="NpaGescheutzt" type="xsd:boolean" >
        <!-- deprecated, wird durch StorkQaaLevel="STORK-QAA-Level-1" ersetzt -->
      <xsd:annotation>
        <xsd:documentation>
          Diese Nachricht kann im BÜS-P-Postkorb nur nach
          vorheriger Anmeldung mit dem nPA gelesen werden.
        </xsd:documentation>
      </xsd:annotation>
    </xsd:element>
    </xsd:choice>
    <xsd:element name="ZuVorgang" type="bsp:ZuVorgangType" minOccurs="0"/>
    <xsd:element name="FreiText" type="bsp:FreiTextType"/>
    <xsd:element name="DataContainer" type="bsp:DataContainerType" minOccurs="0" maxOccurs="unbounded"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="ZuVorgangType">
  <xsd:annotation>
    <xsd:documentation>VorgangsName oder VorgangsId müssen angegeben
  </xsd:annotation>

```

```

    werden. Es können auch beide angegeben werden.</xsd:documentation>
</xsd:annotation>
<xsd:sequence minOccurs="0">
  <xsd:element name="VorgangsName" type="xsd:string"/>
  <xsd:element name="VorgangsId" type="xsd:string"/>
  <xsd:element name="VorgangStatus" type="bsp:SchluesseltabelleType">
    <xsd:annotation>
      <xsd:documentation>Schluesseltabelle 9003 (ST_ERHALTEN, ST_GELESEN,...)
    </xsd:documentation>
    </xsd:annotation>
  </xsd:element>
</xsd:sequence>
</xsd:complexType>

<xsd:complexType name="FreiTextType">
  <xsd:sequence>
    <xsd:element name="Encoding" type="bsp:SchluesseltabelleType" maxOccurs="1" minOccurs="1">
      <xsd:annotation>
        <xsd:documentation>Schluesseltabelle 9004 (text/plain, text/html, ...)
      </xsd:documentation>
    </xsd:annotation>
    </xsd:element>
    <xsd:element name="Text" type="bsp:NonEmptyString" maxOccurs="1" minOccurs="1">
      <xsd:annotation>
        <xsd:documentation>
          Wenn als Encoding text/plain festgelegt ist, so wird die Zeichensequenz "\n" als ein Zeilenvorschub interpretiert.
          Das Backslash-Zeichen (\) wird mit einem weiteren Backslash-Zeichen entwertet.
        </xsd:documentation>
      </xsd:annotation>
    </xsd:element>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="DataContainerType">
  <xsd:sequence minOccurs="0">
    <xsd:element name="Inhalt" type="xsd:base64Binary" maxOccurs="1" minOccurs="1"/>
    <xsd:element name="FileName" maxOccurs="1" minOccurs="0">
      <xsd:simpleType>
        <xsd:restriction base="xsd:string">
          <xsd:maxLength value="255"/>
        </xsd:restriction>
      </xsd:simpleType>
    </xsd:element>
  </xsd:sequence>
</xsd:complexType>

```

```

<xsd:element name="FileType" type="bsp:SchluesseltabelleType" maxOccurs="1" minOccurs="1">
  <xsd:annotation>
    <xsd:documentation>Schluesseltabelle 9005 (application/pdf, text/html, ...)
  </xsd:documentation>
</xsd:annotation>
</xsd:element>
</xsd:sequence>
</xsd:complexType>

```

```

<xsd:complexType name="SchluesseltabelleType">
  <xsd:annotation>
    <xsd:documentation>Dieser Datentyp wird für Schlüsselwerte benötigt.
    Mit dem Datentyp SchluesseltabelleType übermittelt man den Schlüssel
    und die Nummer der Tabelle, in der das Schlüssel-Wert Paar definiert
    worden ist.
  </xsd:documentation>
</xsd:annotation>
  <xsd:sequence>
    <xsd:element name="Tabelle" type="xsd:string"/>
    <xsd:element name="Schluessel" type="xsd:string"/>
  </xsd:sequence>
</xsd:complexType>

```

```

<xsd:simpleType name="StorkQaaLevel">
  <xsd:restriction base="xsd:string">
    <!-- since version 1.2 - deprecated -->
    <xsd:enumeration value="LEVEL_1"/>
    <xsd:enumeration value="LEVEL_2"/>
    <xsd:enumeration value="LEVEL_3"/>
    <xsd:enumeration value="LEVEL_4"/>
    <!-- since version 1.3 -->
    <xsd:enumeration value="STORK-QAA-Level-1"/>
    <xsd:enumeration value="STORK-QAA-Level-2"/>
    <xsd:enumeration value="STORK-QAA-Level-3"/>
    <xsd:enumeration value="STORK-QAA-Level-4"/>
  </xsd:restriction>
</xsd:simpleType>
<xsd:simpleType name="NonEmptyString">
  <xsd:restriction base="xsd:string">
    <xsd:minLength value="1"/>
  </xsd:restriction>
</xsd:simpleType>
</xsd:schema>

```

15.4.2 Schemadatei – bspnachrichten-schluesstabelle-2.10.xsd

```
<?xml version="1.0" encoding="UTF-8"?>
<!--

Service- und Portalplattform
AKDB München, Geschäftsfeld eGovernment

Copyright (c) AKDB

-->
<xsd:schema targetNamespace="http://www.akdb.de/egov/bsp/nachrichten"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:bsp="http://www.akdb.de/egov/bsp/nachrichten"
  elementFormDefault="qualified">

  <xsd:element name="BspNachricht">
    <xsd:annotation>
      <xsd:appinfo>
        <title>Nachricht für die Kommunikation zwischen Bürgerservice-Portal
          und externen Fachverfahren</title>
      </xsd:appinfo>
      <xsd:documentation>Einheitliches Nachrichtenschema für die
        Kommunikation zwischen Bürgerservice-Portal und externem Verfahren.
        Nachrichten vom Bürgerservice-Portal an den Postkorb eines
        Verfahrens
        oder Nachrichten von den Verfahren an das Bürgerservice-Portal müssen
        gemäß diesem Schema aufgebaut sein.
      </xsd:documentation>
    </xsd:annotation>
    <xsd:complexType>
      <xsd:sequence>
        <xsd:element name="NachrichtenKopf" type="bsp:NachrichtenKopfType"/>
        <xsd:element name="NachrichtenInhalt" type="bsp:NachrichtenInhaltType"/>
      </xsd:sequence>
      <xsd:attribute name="version" use="required">
        <xsd:annotation>
          <xsd:documentation>Dieses Attribut kennzeichnet die
            Nachrichten-Version, z. B. "1.0", "1.1".</xsd:documentation>
        </xsd:annotation>
      </xsd:attribute>
    </xsd:complexType>
  </xsd:element>
</xsd:schema>
```

```

    <xsd:restriction base="xsd:string">
      <xsd:enumeration value="1.1"/>
      <xsd:enumeration value="1.2"/>
      <xsd:enumeration value="1.3"/>
      <xsd:enumeration value="1.4"/>
      <xsd:enumeration value="1.5"/>
    </xsd:restriction>
  </xsd:simpleType>
</xsd:attribute>
<xsd:attribute name="fassung" use="required" >
  <xsd:annotation>
    <xsd:documentation>Dieses Attribut kennzeichnet das Datum, an dem
      die diesen Schemata im Status final produziert wurde. Format:
      YYYY-MM-DD.</xsd:documentation>
  </xsd:annotation>
</xsd:simpleType>
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="2017-03-15"/>
    <xsd:enumeration value="2018-04-01"/>
    <xsd:enumeration value="2018-11-01"/>
    <xsd:enumeration value="2019-06-28"/>
    <xsd:enumeration value="2020-03-15"/>
  </xsd:restriction>
</xsd:simpleType>
</xsd:attribute>
<xsd:attribute name="produkt" type="xsd:string" use="optional">
  <xsd:annotation>
    <xsd:documentation>In diesem Attribut ist der Name des Produktes
      (der Software) einzutragen, mit dem diese Nachricht erstellt
      worden ist. z.B. BSP, PWS</xsd:documentation>
  </xsd:annotation>
</xsd:attribute>
<xsd:attribute name="produkthersteller" type="xsd:string" use="optional"/>
<xsd:attribute name="produktversion" type="xsd:string" use="optional"/>
</xsd:complexType>
</xsd:element>

<xsd:element name="BspQuittung">
  <xsd:annotation>
    <xsd:appinfo>
      <title>Quittung über den Empfang einer BSO-Nachricht</title>
    </xsd:appinfo>
    <xsd:documentation>Zu einer empfangenen BSP-Nachricht wird eine

```

```

    Quittung geliefert, die bestätigt, dass die Nachricht übernommen wurde
    oder aufgrund eines technischen oder fachlichen Fehlers abgewiesen wurde.
</xsd:documentation>
</xsd:annotation>
<xsd:complexType>
  <xsd:sequence>
    <xsd:element name="AnnahmeErfolgreich" type="xsd:boolean" minOccurs="1" maxOccurs="1"/>
    <xsd:element name="ErgebnisStatus" type="bsp:SchluesseltabelleType" minOccurs="1" maxOccurs="1">
      <xsd:annotation>
        <xsd:documentation>Schluesseltabelle 9006 (0 (erfolgreich angenommen), 99 (sonstiger technischer Fehler), ...)</xsd:documentation>
      </xsd:annotation>
    </xsd:element>
    <xsd:element name="ErgaenzendeHinweise" type="xsd:string" minOccurs="0" maxOccurs="1"/>
  </xsd:sequence>
  <xsd:attribute name="version" use="required">
    <xsd:annotation>
      <xsd:documentation>Dieses Attribut kennzeichnet die
        Nachrichten-Version, z. B. "1.0", "1.1".</xsd:documentation>
    </xsd:annotation>
  </xsd:attribute>
  <xsd:simpleType>
    <xsd:restriction base="xsd:string">
      <xsd:enumeration value="1.1"/>
    </xsd:restriction>
  </xsd:simpleType>
</xsd:complexType>
<xsd:attribute name="fassung" use="required">
  <xsd:annotation>
    <xsd:documentation>Dieses Attribut kennzeichnet das Datum, an dem
      die diesen Schemata im Status final produziert wurde. Format:
      YYYY-MM-DD.</xsd:documentation>
  </xsd:annotation>
</xsd:attribute>
<xsd:simpleType>
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="2017-03-15"/>
  </xsd:restriction>
</xsd:simpleType>
</xsd:attribute>
<xsd:attribute name="produkt" type="xsd:string" use="optional">
  <xsd:annotation>
    <xsd:documentation>In diesem Attribut ist der Name des Produktes
      (der Software) einzutragen, mit dem diese Nachricht erstellt
      worden ist. z.B. BSP, PWS</xsd:documentation>
  </xsd:annotation>
</xsd:attribute>

```

```

</xsd:attribute>
<xsd:attribute name="produktHersteller" type="xsd:string" use="optional"/>
<xsd:attribute name="produktversion" type="xsd:string" use="optional"/>
</xsd:complexType>
</xsd:element>

<xsd:complexType name="NachrichtenKopfType">
  <xsd:sequence>
    <xsd:element name="Identifikation.Nachricht" type="bsp:Identifikation.NachrichtType" maxOccurs="1" minOccurs="1"/>
    <xsd:element name="Anwenderkennung" type="xsd:string" minOccurs="0">
      <xsd:annotation>
        <xsd:documentation> Die Anwenderkennung stellt Informationen über die absendende Person
          zur Verfügung und dient der Protokollierung.
          Anhand dieser Kennung kann die absendende Person identifiziert werden.
        </xsd:documentation>
      </xsd:annotation>
    </xsd:element>
    <xsd:element name="Absender" type="bsp:AbsenderType" maxOccurs="1" minOccurs="1"/>
    <xsd:element name="Empfaenger" type="bsp:EmpfaengerType" maxOccurs="1" minOccurs="1"/>
    <xsd:element name="AntwortAuf" type="xsd:string" maxOccurs="1" minOccurs="0">
      <xsd:annotation>
        <xsd:documentation>Eine Nachricht kann mit einer existierenden
          Nachricht in Beziehung gebracht werden als Antwortnachricht oder
          weitergeleitete Nachricht. Der Bezug erfolgt hierbei über die
          NachrichtenId.
        </xsd:documentation>
      </xsd:annotation>
    </xsd:element>
    <xsd:element name="WeiterleitungZu" type="xsd:string" minOccurs="0"/>
    <xsd:element name="lesebestaetigungAntwortAdresse" type="xsd:string" minOccurs="0"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="Identifikation.NachrichtType">
  <xsd:sequence>
    <xsd:element name="Ereignis" type="bsp:SchluesseltabelleType">
      <xsd:annotation>
        <xsd:documentation>Schluesseltabelle 9001, Schluessel: BspNachricht
        </xsd:documentation>
      </xsd:annotation>
    </xsd:element>
    <xsd:element name="Erstellungszeitpunkt" type="xsd:dateTime" maxOccurs="1" minOccurs="1"/>
    <xsd:element name="NachrichtenId" type="xsd:string" maxOccurs="1" minOccurs="1">
      <xsd:annotation>

```



```

<xsd:documentation>eine beliebige, eindeutige ID, die durch den
    erstellenden Client generiert wird. Zusammen mit
    Erstellungszeitpunkt und Absender kann eine Nachricht bsp-global
    eindeutig identifiziert werden.
</xsd:documentation>
</xsd:annotation>
</xsd:element>
</xsd:sequence>
</xsd:complexType>

<xsd:complexType name="AbsenderType">
    <xsd:sequence>
        <xsd:element name="PostkorbId" type="xsd:string" maxOccurs="1" minOccurs="0"/>
        <xsd:element name="Verfahren" type="xsd:string" maxOccurs="1" minOccurs="0"/>
        <xsd:element name="Dienst" type="bsp:NonEmptyString" maxOccurs="1" minOccurs="0"/>
        <xsd:element name="Mandant" type="bsp:NonEmptyString" maxOccurs="1" minOccurs="0"/>
        <xsd:element name="Gemeindeschluessel" type="bsp:SchluesseltabelleType" minOccurs="0">
            <xsd:annotation>
                <xsd:documentation>Der amtliche Gemeindeschlüssel (AGS).
                    Als Tabellennummer ist hier die 36 (OSCI-XMeld-Schlüsseltabelle "Amtlicher Gemeindeschluessel") zu verwenden.
                </xsd:documentation>
            </xsd:annotation>
        </xsd:element>
        <xsd:element name="Name" type="xsd:string" maxOccurs="1" minOccurs="0"/>
        <xsd:element name="Anschrift" type="xsd:string" maxOccurs="1" minOccurs="0"/>
        <xsd:element name="Email" type="xsd:string" maxOccurs="1" minOccurs="0"/>
        <xsd:element name="Telefon" type="xsd:string" maxOccurs="1" minOccurs="0"/>
        <xsd:element name="Hyperlink" type="xsd:string" maxOccurs="1" minOccurs="0"/>
    </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="EmpfaengerType">
    <xsd:sequence>
        <xsd:element name="PostkorbId" type="xsd:string" maxOccurs="1" minOccurs="1"/>
        <xsd:element name="Verfahren" type="xsd:string" maxOccurs="1" minOccurs="0"/>
        <xsd:element name="Dienst" type="xsd:string" maxOccurs="1" minOccurs="0"/>
        <xsd:element name="Mandant" type="xsd:string" maxOccurs="1" minOccurs="0"/>
        <xsd:element name="Gemeindeschluessel" type="bsp:SchluesseltabelleType" minOccurs="0">
            <xsd:annotation>
                <xsd:documentation>Der amtliche Gemeindeschlüssel (AGS).
                    Als Tabellennummer ist hier die 36 (OSCI-XMeld-Schlüsseltabelle "Amtlicher Gemeindeschluessel") zu verwenden.
                </xsd:documentation>
            </xsd:annotation>
        </xsd:element>
    </xsd:sequence>

```

```

</xsd:element>
<xsd:element name="Name" type="xsd:string" maxOccurs="1" minOccurs="0"/>
<xsd:element name="Anschrift" type="xsd:string" maxOccurs="1" minOccurs="0"/>
</xsd:sequence>
</xsd:complexType>

<xsd:complexType name="NachrichtenInhaltType">
  <xsd:sequence>
    <xsd:element name="Betreff" type="bsp:NonEmptyString" maxOccurs="1" minOccurs="1"/>
    <xsd:element name="Kategorie" type="bsp:SchluesseltabelleType" minOccurs="0">
      <xsd:annotation>
        <xsd:documentation>Schluesseltabelle 9002 (KAT_STATUS, KAT_INFOBSP, ...)</xsd:documentation>
      </xsd:annotation>
    </xsd:element>
    <xsd:choice minOccurs="0">
      <xsd:element name="StorkQaaLevel" type="bsp:StorkQaaLevel"/>
      <xsd:element name="NpaGescheutzt" type="xsd:boolean" >
        <!-- deprecated, wird durch StorkQaaLevel="STORK-QAA-Level-1" ersetzt -->
      <xsd:annotation>
        <xsd:documentation>
          Diese Nachricht kann im B sP-Postkorb nur nach
          vorheriger Anmeldung mit dem nPA gelesen werden.
        </xsd:documentation>
      </xsd:annotation>
    </xsd:element>
    </xsd:choice>
    <xsd:element name="ZuVorgang" type="bsp:ZuVorgangType" minOccurs="0"/>
    <xsd:element name="FreiText" type="bsp:FreiTextType"/>
    <xsd:element name="DataContainer" type="bsp:DataContainerType" minOccurs="0" maxOccurs="unbounded"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="ZuVorgangType">
  <xsd:annotation>
    <xsd:documentation>VorgangsName oder VorgangsId m ssen angegeben
    werden. Es k nnen auch beide angegeben werden.</xsd:documentation>
  </xsd:annotation>
  <xsd:sequence minOccurs="0">
    <xsd:element name="VorgangsName" type="xsd:string"/>
    <xsd:element name="VorgangsId" type="xsd:string"/>
    <xsd:element name="VorgangStatus" type="bsp:SchluesseltabelleType">
      <xsd:annotation>

```

```

    <xsd:documentation>Schluesseltabelle 9003 (ST_ERHALTEN, ST_GELESEN,...)
  </xsd:documentation>
</xsd:annotation>
</xsd:element>
</xsd:sequence>
</xsd:complexType>

<xsd:complexType name="FreiTextType">
  <xsd:sequence>
    <xsd:element name="Encoding" type="bsp:SchluesseltabelleType" maxOccurs="1" minOccurs="1">
      <xsd:annotation>
        <xsd:documentation>Schluesseltabelle 9004 (text/plain, text/html, ...)
      </xsd:documentation>
    </xsd:annotation>
  </xsd:element>
    <xsd:element name="Text" type="bsp:NonEmptyString" maxOccurs="1" minOccurs="1">
      <xsd:annotation>
        <xsd:documentation>
          Wenn als Encoding text/plain festgelegt ist, so wird die Zeichensequenz "\n" als ein Zeilenvorschub interpretiert.
          Das Backslash-Zeichen (\) wird mit einem weiteren Backslash-Zeichen entwertet.
        </xsd:documentation>
      </xsd:annotation>
    </xsd:element>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="DataContainerType">
  <xsd:sequence minOccurs="0">
    <xsd:element name="Inhalt" type="xsd:base64Binary" maxOccurs="1" minOccurs="1"/>
    <xsd:element name="FileName" maxOccurs="1" minOccurs="0">
      <xsd:simpleType>
        <xsd:restriction base="xsd:string">
          <xsd:maxLength value="255"/>
        </xsd:restriction>
      </xsd:simpleType>
    </xsd:element>
    <xsd:element name="FileType" type="bsp:SchluesseltabelleType" maxOccurs="1" minOccurs="1">
      <xsd:annotation>
        <xsd:documentation>Schluesseltabelle 9005 (application/pdf, text/html, ...)
      </xsd:documentation>
    </xsd:annotation>
  </xsd:element>
</xsd:sequence>

```

```

</xsd:complexType>

<xsd:complexType name="SchluesseltabelleType">
  <xsd:annotation>
    <xsd:documentation>Dieser Datentyp wird für Schlüsselwerte benötigt.
      Mit dem Datentyp SchluesseltabelleType übermittelt man den Schlüssel
      und die Nummer der Tabelle, in der das Schlüssel-Wert Paar definiert
      worden ist.
    </xsd:documentation>
  </xsd:annotation>
  <xsd:sequence>
    <xsd:element name="Tabelle" type="xsd:string"/>
    <xsd:element name="Schluessel" type="xsd:string"/>
  </xsd:sequence>
</xsd:complexType>

<xsd:simpleType name="StorkQaaLevel">
  <xsd:restriction base="xsd:string">
    <!-- since version 1.2 - deprecated -->
    <xsd:enumeration value="LEVEL_1"/>
    <xsd:enumeration value="LEVEL_2"/>
    <xsd:enumeration value="LEVEL_3"/>
    <xsd:enumeration value="LEVEL_4"/>
    <!-- since version 1.3 -->
    <xsd:enumeration value="STORK-QAA-Level-1"/>
    <xsd:enumeration value="STORK-QAA-Level-2"/>
    <xsd:enumeration value="STORK-QAA-Level-3"/>
    <xsd:enumeration value="STORK-QAA-Level-4"/>
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="NonEmptyString">
  <xsd:restriction base="xsd:string">
    <xsd:minLength value="1"/>
  </xsd:restriction>
</xsd:simpleType>
</xsd:schema>

```

16 Quellen

- [1] OASIS SAML: <http://saml.xml.org/saml-specifications>
- [2] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_1_2_Version_1_0.pdf?__blob=publicationFile
- [3] <http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf>
- [4] <http://www.capcourse.com/Library/OpenSAML/index.html>
- [5] <http://forgerock.com/products/open-identity-stack/openig/>
- [6] <https://shibboleth.atlassian.net/wiki/spaces/SP3/overview>
- [7] Beispiel am Ende der Herstelldokumentation: <https://wiki.shibboleth.net/confluence/display/SP3/SAML2+SessionInitiator>
- [8] <https://tools.ietf.org/html/rfc4519>
- [9] <https://tools.ietf.org/html/rfc4524>
- [10] <https://tools.ietf.org/html/draft-gryphon-ldap-schema-vcard4-00#section-3.5>
- [11] <https://ec.europa.eu/digital-agenda/en/trust-services-and-eid>
- [12] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG
- [13] https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=6:d32-qaa-status-report&Itemid=175) [Abrufdatum 14.06.2018]
- [14] <https://calver.org>
- [15] <https://tools.ietf.org/html/rfc4519#section-2.25>
- [16] <http://docs.oracle.com/cd/E19462-01/819-4670/gbanp/index.html>

