

Das Servicekonto im Bayerischen Portalverbund (ohne Unternehmenskonto)



Dokumentation zur Anbindung von Drittanwendungen an das Nutzerkonto am Beispiel der BayernID.

Nutzung des Basisdienstes BayernID nach BayEGovG

Version 4.0

Stand: 04.08.2023

-
- 1. Einleitung
 - 2. Der Bayerische Portalverbund – eine offene Infrastruktur für Fachportale öffentlicher Verwaltungen in Bayern
 - 3. Übersicht über die Funktionsweise der offenen Infrastruktur
 - 4. Unterstützte Anwendungsfälle
 - 4.1 Anwendungsfall 1 – direkte Tokennutzung
 - 4.2 Anwendungsfall 2 – indirekte Tokennutzung
 - 5. Unterstützte Authentisierungsverfahren und Anfragearten
 - 5.1 Auswahl bestimmter Vertrauensniveaus
 - 5.2 Besonderheiten der optionalen Protokollierung bei Nutzung von Authega-Zertifikaten aus Sicht der Drittanwendung
 - 5.3 Migration eines Fachportals zur Nutzung von Authega-Zertifikaten
 - 5.4 Nutzung von organisationsspezifischen Nutzdaten (Unternehmenskonto-API) - ab Dezember 2022 abgekündigt
 - 5.5 Besonderheiten bei der Nutzung von interoperablen Nutzerkonten
 - 5.6 Besonderheiten bei der Nutzung der Methode "Temporärer Login"
 - 6. Attribute im SAML-Token
 - 6.1 Personenbezogene Stammdaten
 - 6.2 Technische Nutzdaten
 - 6.2.1 bPK - bereichsspezifisches Personenkennzeichen
 - 6.2.2 bPK2 - bereichsspezifisches Personenkennzeichen
 - 6.2.4 Version
 - 6.2.5 AssertionProvedBy
 - 6.2.6 Postkorb-Handle
 - 7. Betriebsvoraussetzungen
 - 7.1 Infrastruktur
 - 7.2 Metadaten
 - 7.3 Zusätzliche Metadaten
 - 7.4 Bestandener Integrationstest
 - 8. Entscheidungsunterstützung und Handreichungen
 - 8.1 Architekturüberlegungen bei Auswahl eines SAML-Bindings
 - 8.2 Zurückleiten in die Drittanwendung bei Abbruch durch Benutzer
 - 8.3 Handreichung für EntwicklerInnen von Drittanwendungen im Bayerischen Portalverbund
 - 8.5 Zurück zum Fachverfahren
 - 8.5.1 URL aus den Metadaten
 - 8.5.2 SAML-Response
 - 9. Konfiguration der Anfrage
 - 9.1 Einschränkung des Authentifizierungsverfahren
 - 9.2 Anforderung von Pflichtattributen
 - 9.2.1 Technische Attribute vom Servicekonto und die Authentisierungsverfahren
 - 9.2.2 Validieren von RequestedAttributes im SAML Request
 - 9.2.3 Validieren von RequestedAttributes vor dem Absenden
 - 9.3 Änderung des Einleitungstexts
 - 9.4 Übergabe von UI-Informationen (ab Release 6)
 - 9.5 Berechtigungszertifikat eines Bundeslandes
 - 10. Anhänge
 - 10.1 Verweise auf externe Dokumente
 - 10.2 Verwendete Abkürzungen
 - 11. Annex

- [11.1 Authentication Request zur Nutzung von Authega-Zertifikaten mit optionalen Attributen](#)
- [11.2 Beispiele für Requests](#)
- [11.3 Beispiel für Response](#)

1. Einleitung

Die AKDB ermöglicht im Auftrag des Freistaats Bayern allen Fachportalen der öffentlichen Verwaltungen die Nutzung von Daten aus dem Bayerischen Nutzerkonto über eine offene Infrastruktur, die mit den beteiligten Systemen den Bayerischen Portalverbund als sog. Identity Federation bildet.

Bürger schalten sich dafür individuelle Nutzerkonten auf dem BayernPortal frei und verwalten dort Ihre persönlichen Daten und Zusatzinformationen. Die Befüllung der personenbezogenen Datenfelder für das Bürgerkonto erfolgt entweder über die freiwillige Angabe (bei Nutzung von Benutzernamen/Passwort-Paar) oder automatisiert bei der erstmaligen Nutzung z.B. mittels Personalausweis am BayernPortal.

Fachportale als sog. Drittanwendungen im Bayerischen Portalverbund verbinden sich über definierte Standardprotokolle mittelbar mit dem BayernPortal und profitieren im Sinne der Datensparsamkeit von der zentralisierten Verwaltung der personenbezogenen Nutzerdaten im Nutzerkonto.

Auf Grundlage des Protokolls „Security Assertion Markup Language“ (SAMLv2 von OASIS Consortium) existiert bereits seit 2013 der Kern des Bayerischen Portalverbunds mit der ersten Fachanwendung "Staatliche Fischerprüfung Online" des StMELF/LfL. Diese und alle zukünftigen am Portalverbund teilnehmenden Fachportale (sog. Service Provider) gehen zu diesem Zweck eine Vertrauensstellung mit einer zentralen Authentisierungsinstanz (sog. Identity Provider), der BayernID, ein.

In diesem Dokument werden die gegenwärtig für Fachportale existierenden Schnittstellen zum BayernID Identity Provider beschrieben. Informationen über weitere Schnittstellen zum BayernPortal nach BayEGovG entnehmen Sie bitte den gesonderten Dokumentationen (Postfach, ePayment).

2. Der Bayerische Portalverbund – eine offene Infrastruktur für Fachportale öffentlicher Verwaltungen in Bayern

Ausgewählte personenbezogene Daten aus dem Basisdienst „Nutzerkonto“ stehen im Rahmen einer offenen Infrastruktur einem Kreis von Drittanwendungen (dem „Bayerischen Portalverbund“) außerhalb des eigentlichen BayernPortals zur Verfügung (s. Abschnitt 6).

Diese offene Infrastruktur basiert auf international anerkannten, quell-offenen Standardtechnologien^[1] und sichert die Drittanwendungen (z.B. Antragsverfahren) 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. Benutzernamen/Passwort, Personalausweis-Pseudonym, Authega-ID) sind mit den für das Nutzerkonto im BayernPortal hinterlegten Informationen identisch. Somit ist eine erneute Registrierung in den angebundenen Drittanwendungen hinfällig.

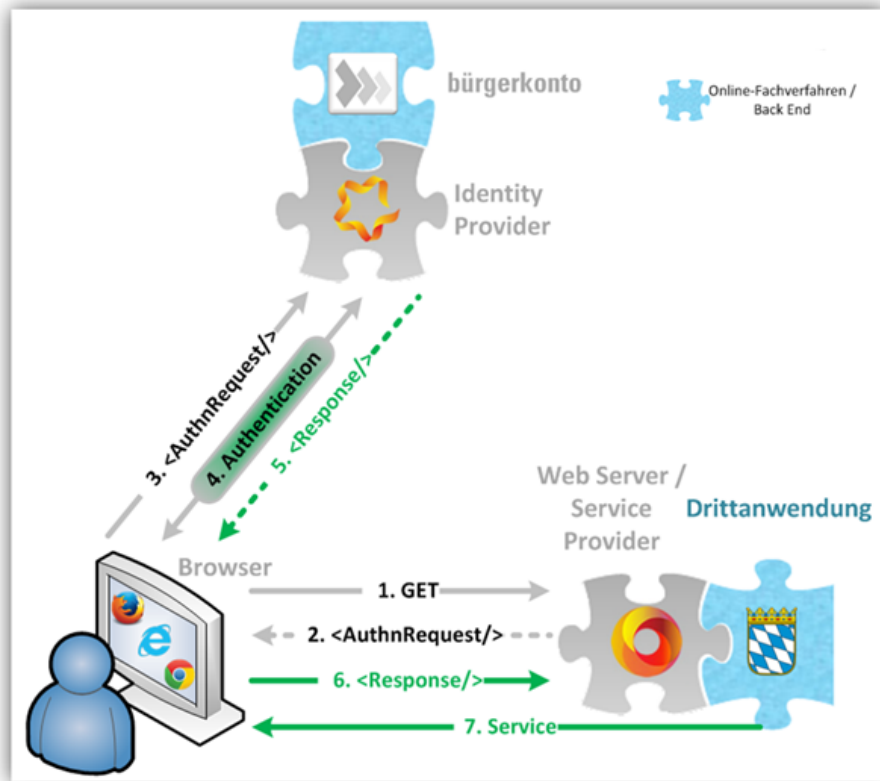
Die am Bayerischen Portalverbund teilnehmenden Fachportale werden dann „Service Provider“ genannt und verbleiben nicht nur in der rechtlichen, sondern auch in der operativen Zuständigkeit derjenigen Körperschaft, in deren Namen die Dienstleistung den Bürgerinnen und Bürgern angeboten wird. Der Fortbestand eigener Web-Angebote erweist sich insbesondere im Falle hoher systemischer Komplexität oder bereits vom Mandanten langfristig getätigter strategischer IT-Investitionen als sinnvoll.

Die Auslagerung des Zugriffsschutzes der Drittanwendungen an Komponenten des Bayerischen Portalverbunds erfordert allerdings einen, je nach Technologiestand des Service Providers, erheblichen 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 Bayerischen Portalverbund aufnehmen als jene Anwendungen, die anders geartete Zugriffskontrollmechanismen (wie z.B. Kerberos) nutzen.

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 des OASIS Consortium, wie sie auch im Kern der eCard-API des bundesdeutschen neuen elektronischen Personalausweises nPA zum Einsatz kommen^[2].

Darstellung 1: Zusammenspiel der Komponenten in der offenen Infrastruktur des Bayerischen Portalverbunds:




Die einzelnen Teilschritte sind nur vereinzelt für die Dienstanutzer 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 (z.B. zum verbindlichen Absenden eines Antrags), wird der Zugriffsversuch auf Seiten des Service Providers abgefangen (Schritt 1).

Seitens des Fachportals wird daraufhin eine Authentisierungsanfrage an den BayernID 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).

Das Bild zeigt die Anmeldeseite des **Bayerischen Portalverbunds** mit dem **BayernID**-Logo. Der Titel lautet **Bitte anmelden**. Der Text fordert den Benutzer auf, sich mit seiner BayernID anzumelden. Falls keine BayernID vorhanden ist, wird eine Registrierung empfohlen. Es folgen vier Auswahlmöglichkeiten für die Anmeldung: **Online-Ausweisfunktion (eID, eAT, eID-Karte)**, **authega-Zertifikat ***, **Benutzername/Passwort** und **Weitere Optionen +**. Ein **Zurück**-Button befindet sich am unteren Rand. Fußnoten und Links für **Datenschutz**, **Impressum** und **Kontakt** sind ebenfalls sichtbar.

Der Identity Provider fordert nun den Dienstanfrager auf, sich ihm gegenüber durch ein vorausgewähltes oder frei wählbares 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, durch die Nutzung des neuen Personalausweises nPA oder mittels Authega-Zertifikat erfolgen. Erst im Zuge einer positiv durchlaufenen Authentisierung (Schritt 4) erfolgt am Identity Provider die Erstellung einer Antwortnachricht, die unter Hinzuziehung der im Nutzerkonto für die Person hinterlegten Daten erweitert wird. Ab diesem Zeitpunkt kann der Dienstanutzer im rechtlichen Sinne als authentisierter Benutzer im Rahmen der Infrastruktur des Bayerischen Portalverbunds gelten.

	<p>Nach erfolgter Sichtung der Nutzdaten und deren explizite Freigabe durch den Benutzer wird die Antwortnachricht zusammengestellt.</p> <p>Die erzeugte Antwortnachricht wird als SAML-Response verschlüsselt und unter Einberechnung von Zertifikatsinformationen signiert in Schritt 5 an den Browser des potentiellen Dienstinutzers zurückgesendet. Von dort aus wird die SAML-Response an die Drittanwendung weiter durchgestellt. Die Verwendung BSI-konformer Verschlüsselungstechnologien^[3] im vorherigen Schritt stellt sicher, dass der Dienstinutzer an dieser Stelle keine Möglichkeit zur Vortäuschung oder beabsichtigten Veränderung des Inhalts hat</p>
	<p>Der Service Provider empfängt die SAML-Response (Schritt 6) per HTTP-POST auf einem speziell bekanntgemachten Endpunkt innerhalb der Drittanwendung (s. Kapitel 4) und überprüft zunächst nun die Nachricht auf ihre Authentizität und Integrität hin. Erst dann wird von der Drittanwendung bewertet, ob der Inhalt der vom Identity Provider stammenden Antwortnachricht den weiteren Erfordernissen des Fachverfahrens genügt. Erst jetzt ist der authentifizierte Dienstinutzer im rechtlichen Sinne auch autorisiert und zugriffsbefugt für weitere Aktionen (z.B. dem tatsächlichen Einstellen eines Antrags an die Sachbearbeitung).</p> <p>Der Service Provider gewährt nun in Folge Zugriff auf die zunächst geschützte Ressource (z.B. Absendefunktion des Antrags oder personenbezogene Dateneinsicht) und führt die ursprüngliche Zugriffsanfrage aus. Die Antwort wird auf dem zugehörigen Anwendungsserver generiert und an den Browser des Dienstinutzers gesendet (Schritt 7). Für den Zeitraum der weiteren Sitzung wird fortan die Auslieferung aller weiteren zugriffsgeschützten Ressourcen je nach Anfrage (und applikationsspezifischem Verhalten) erlaubt.</p> <p>Darüberhinausgehende Zugriffsrestriktionen (z.B. nach RBAC) sind ausschließlich Teil der Applikationslogik des Fachportals und liegen jenseits des Funktionsumfanges der zur Verfügung gestellten Infrastruktur.</p>

4. Unterstützte Anwendungsfälle

Die Fachportale im Bayerischen Portalverbund schließen sich mittelbar per OASIS SAML Web Browser Single-Sign-On-Profile^[4] an das BayernPortal an, und lagern Ihre Nutzerauthentisierung an die Identity Federation Infrastruktur aus.

Diese Service Provider müssen eine der beiden Anfragearten HTTP-REDIRECT oder HTTP-POST-Binding implementieren, sowie als HTTP-POST-Endpunkt für SAML v2-Token fungieren (AssertionConsumerService Location).

Dieses Endpunkt-Handling für die Antwort ist allgemein über zwei Wege möglich:

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

4.1 Anwendungsfall 1 – direkte Tokennutzung

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^[5].

4.2 Anwendungsfall 2 – indirekte Tokennutzung

Erlaubt die Infrastruktur des jeweiligen Rechenzentrums den Betrieb zusätzlicher Komponenten auf dem der Drittanwendung vorlagerten Web-Server, bietet sich darüber hinaus die Nutzung von sog. Reverse-Proxy-Installationen an: Diese agieren ihrerseits als Endpunkt des SAML-Protokolls und verarbeiten die entsprechenden Requests und Responses anstelle des Fachportals. Der Service Provider besteht dann aus der eigentlichen Drittanwendung (dem web-basierten 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^[6]" oder "Shibboleth Consortium^[7]" zur Verfügung stehen. Implementierungs- und Konfigurationsbeispiele zur Nutzung finden sich in den jeweiligen Produktdokumentationen der 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

Der Identity Provider der BayernID im Bayerischen Portalverbund unterstützt folgende verfügbare Authentisierungsmethoden, die auch über ein zugehöriges Vertrauensniveau (s. Kapitel 6.3.2) eindeutig für Drittanwendungen erkennbar sind:

Bezeichnung	Ausgestaltung
Benutzername/Passwort (entspricht Nicht-Vertrauensniveau Basisregistrierung, STORK-QAA-Level-1)	<ul style="list-style-type: none">• Ein software-basiertes Verfahren• Die Registrierung erfolgt einzig durch BayernID- Systemkomponenten• Attribute sind nicht überprüft
Authega-Zertifikat bzw. Elster-Zugang (entspricht Vertrauensniveau mittel, 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 Authega-Zentral oder bei Elster direkt• Die Nutzung kann auch schriftformwährend erfolgen, siehe dazu auch BayBITV §4.• Attribute sind Melderegister-geprüft
neuer elektronischer Personalausweis (entspricht Vertrauensniveau hoch, STORK-QAA-Level-4)	<ul style="list-style-type: none">• Ein hardware-basiertes PKI-Verfahren• Die Registrierung und Nutzung erfolgt in Koordination mit BSI-TR-zertifizierten eID-Servern• Attribute sind Melderegister-geprüft

5.1 Auswahl bestimmter Vertrauensniveaus

Authentisierungsverfahren können nach Vertrauensniveau gruppiert 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 werden auch weitere Authentifizierungsmittel angebunden werden, die gemäß eIDAS-Verordnung notifiziert wurden. Nach Anbindung können sie für die Authentifizierung auf den jeweiligen Vertrauensniveaus verwendet werden. Das Vorhandensein des nicht eIDAS-notifizierten Verfahrens Authega auf einem „mittleren“ Vertrauensniveau und Verfahren auf dem eIDAS-Vertrauensniveau „substantiell“ wird vermutlich zu einer Anpassung der Schnittstelle führen.

Eine Auswahl der zulässigen Verfahren am IDP erfolgt aufsteigend nach der Wertigkeit des Authentisierungsverfahrens (analog zum erwähnten Beispiel in Kapitel 11.1).

Die explizite Anforderung im Sinne einer nachträglichen Erweiterung der SAMLAuthenticationRequest-Nachrichten für Bestandsanwendungen ist nicht erforderlich: diese können wie bisher mit dem BayernID Identity Provider interagieren und sich auf das bisherige Standardverhalten verlassen, das alle unterstützten Authentisierungsverfahren zur Ansicht bringt.

Für den Fall der indirekten Tokennutzung (s. Kapitel 4.2) müssten die Erweiterungen über produktspezifische Konfigurationen vorgenommen werden, so z. B. beim Reverse-Proxy des Herstellers „Shibboleth Consortium“ mittels Templates zum SessionInitiator [\[8 / Beispiel am Ende der Herstelldokumentation, zuletzt abgerufen im Juni 2020\]](#), s. auch das Beispiel zur Veranschaulichung im Anhang 10.3.

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, also ohne permanentes Nutzerkonto, übergeben wird und wie bzw. ob diese später wieder zugeordnet werden kann.

5.2 Besonderheiten der optionalen Protokollierung bei Nutzung von Authega-Zertifikaten aus Sicht der Drittanwendung

Zusätzlich können bei der Benutzung von Authega-Zertifikaten zum Zwecke der Beweisführung im Streitfall (i.S.e. Nichtabstreitbarkeit) weitere Parameter zur Protokollierung übermittelt werden. Diese können dann in aggregierter Form nach durchlaufener Authentisierung als zusätzlicher Nachweis dienen. Dazu ist bei der Erstellung von SAMLAuthenticationRequests zusätzlich darauf zu achten, die folgenden Attribute als Request-Extension anzugeben (vgl. Beispiel in Kapitel 11.1, sowie für Details zur SAMLAuthenticationResponse auch die Kapitel 6.3.6 sowie 8.3):

Bezeichnung	Inhalt
-------------	--------

ClientIP_OriginSP	Die IP-Adresse, von der (aus Sicht der Drittanwendung) die Online-Sitzung angefragt wird
SessionToken_OriginSP	Die interne Sitzungsidentifikationsnummer, die derjenigen Online-Sitzung (aus Sicht der Drittanwendung) zugewiesen wurde

Weitere Ausführungen zu dieser nicht verpflichtenden Schnittstellennutzung können dem Kapitel 6.3.6 sowie dem gesonderten Dokument „Handreichung zum Nachweis der Beweiswerterhaltung“ entnommen werden.

5.3 Migration eines Fachportals zur Nutzung von Authega-Zertifikaten

Wie im vorangegangenen Kapitel erwähnt, sind aus Sicht einer Fachanwendung folgende Änderungen vorzunehmen:

1. Zwingend: Erweiterung des SAMLAuthenticationRequests um die Extensions zur Auswahl der Authentisierungsniveaus „mittel“, STORK-QAA-Level-3
2. Optional: Erweiterung des SAMLAuthenticationRequests um die Extensions zur Angabe der im vorherigen Kapitel genannten Attribute ClientIP_OriginSP und SessionToken_OriginSP
3. Zwingend: Verarbeitung des SAMLAuthenticationResponse mit allen zusätzlichen Attributen laut Kapitel 6.3.6
4. Optional: Prüfung auf Gleichheit der IP-Adressen aus dem ursprünglichen SAMLAuthenticationRequest (ClientIP_OriginSP) mit den Attributen aus der SAMLAuthenticationResponse (ClientIP_OriginSP, ClientIP_authgaldP und ClientIP_IntermediatIdP)
5. Optional: Prüfung auf Gleichheit der Sitzungsidentifikationsnummer aus dem ursprünglichen SAMLAuthenticationRequest (SessionToken_OriginSP) mit den Attributen aus der SAMLAuthenticationResponse (SessionToken_OriginSP)
6. Zwingend: Prüfung auf Gleichheit der in der „Handreichung zum Nachweis der Beweiswerterhaltung“ erwähnten Nachrichtenidentifikationsnummern der SAML-Nachrichten (inResponseTo-Inhalte der SAMLAuthenticationResponse müssen identisch sein mit der ursprünglichen ID des SAMLAuthenticationRequests)
7. Optional: Behandlung des etwaigen Fehlerfalls bei negativem Prüfergebnis einer der obigen Prüfpunkte
8. Optional: Protokollierung nach der in der „Handreichung zum Nachweis der Beweiswerterhaltung“ exemplarisch veranschaulichten Vorgehensweise

Sind die obigen zwingenden Schritte seitens eines Fachportals umgesetzt worden, kann die Drittanwendung als konform zum empfohlenen Vorgehen betrachtet werden. Eine gesonderte Zertifizierung seitens der Betreiber des Bayerischen Portalverbunds anhand von Quelltext-Analysen erfolgt nicht.

5.4 Nutzung von organisationsspezifischen Nutzdaten (Unternehmenskonto-API) - ab Dezember 2022 abgekündigt

Die Unternehmenskonto-API wurde mit Release 6 der BayernID im Dezember 2022 abgekündigt. Die Unternehmenskonto-Funktionen wurden zu diesem Zeitpunkt deaktiviert, sodass die Nutzung dieser Konten nicht mehr möglich ist.

Übergangsphase:

Für den Zeitraum von 6 Monaten wird eine Übergangsphase für Postfach-Nachrichten an Unternehmenskonten sichergestellt. In diesem Zeitraum ist es weiterhin möglich Nachrichten an Unternehmenskonten zu senden, die Inhaber der Unternehmenskonten werden auf gesichertem Wege informiert.

SAML-Requests mit RequestedAttributeSet und legalEntity werden nicht mehr unterstützt und direkt mit einer SAML-Response beantwortet. individualPerson und any wird so behandelt, also ob das RequestedAttributeSet nicht angefordert wurde (Default-Verhalten für natürliche Personen).

5.5 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 potentiell mitgelieferte Postfachreferenzen ebenfalls gefiltert und nicht verarbeitet.

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

5.6 Besonderheiten bei der Nutzung der Methode "Temporärer Login"

Gemäß OZG muss es Nutzer:innen möglich sein, das Nutzerkonto ohne Langzeitspeicherung von Daten 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) entfällt 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.

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]. "Keine Angabe" = 0 (fälschlicherweise Wert 9 bis NK Release 6.0.3.0) "Herr" = 1 "Frau" = 2
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	
Ausstellender Staat	issuingState	urn:oid:1.2.40.0.10.2.1.1.552244	seit 02/2019 nicht mehr unterstützt
Künstlername	artisticName	urn:oid:1.2.40.0.10.2.1.1.552233	seit 02/2021 (R2.2) 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	
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 (R3.3) als international gültige Telefonnummer; in der BayernID ab 07/2021 produktiv
eIDAS-Issuing-Country	eIDAS-Issuing-Country	urn:oid:1.3.6.1.4.1.25484.494450.10.1	Basiert auf SendingMemberState (TR-03130 eID-Server), optional, ISO 3166-1 alpha-2

Bitte beachten:

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

Siehe hierzu: <https://ec.europa.eu/cefdigital/wiki/download/attachments/82773108/eIDAS%20SAML%20Attribute%20Profile%20v1.2%20Final.pdf?version=2&modificationDate=1571068651772&api=v2>

<https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+available+attributes+of+pre-notified+and+notified+eID+schemes>

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 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 Email-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::mcR9heGIqQjldF0Pqlh1ETJcTUIrBo05DZtt8qyUiPE::2013-06-11T13:42:34
```

Es wird daher empfohlen, die bPK anderen Attributen zur eindeutigen Nutzerreferenzierung (z. B. Email) 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.

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 entspricht dem Wert der "eigentlichen ssPIN" (siehe Kapitel zur bPK).

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

bPK2 ist ab Release 3(3.2.1.0), August 2021 (IDP Version 2021.7.1) verfügbar. Das bPK wird noch 12 Monate nach Verfügbarkeit des bPK2 unterstützt. In der Zwischenzeit müssen die Service Provider ihre Software entsprechend umstellen. Die restlichen Informationen aus der bPK sind damit auch abgekündigt und sind an anderen Stellen bereits sinnvoller vorhanden. Der Algorithmus zur Erstellung der bPK2 verwendet als Parameter unter anderem den Host der EntityID aus den Metadaten um unterschiedliche Werte an unterschiedliche Onlinedienste weiterzugeben (analog dem Pseudonym aus der eID). Bei FINK wird der Identifier aus dem anderen SK übernommen und mit Prefixen versehen, damit keine Überschneidung mit existierenden bPK2s möglich ist.

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 dem Bürgerkonto) verfügbar gemacht.

Bezeichnung	FriendlyName	SAML2 Formal Name (URN-notiert)
Vertrauensniveau	EID-CITIZEN-QAA-LEVEL	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^[13] und im Lichte der eIDAS-Verordnung^[14], wurde zeitlich weit vor der Veröffentlichung entsprechender Technischer Richtlinien seitens des BSI der Trustlevel-Ansatz nach STORK-Methodik gewählt^[15]. 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 (= selbstregistriertes Bürgerkonto bzw. eIDAS-Äquivalent)
STORK-QAA-Level-3	aktuelle Authentisierung mittels Authega-Zertifikat oder Elster Zugang; registrierte Attributdaten aus dem Melderegister (= Authega/Elster-registriertes Bürgerkonto bzw. eIDAS-Äquivalent)
STORK-QAA-Level-4	aktuelle Authentisierung mittels Online-Ausweisfunktion (ePA, eAT, EU-Karte); registrierte Attributdaten aus dem Ausweismittel (= nPA-registriertes Bürgerkonto 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^[16] 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

Über das Attribut AssertionProvedBy wird die Quelle transportiert, welche die Identität überprüft hat. Im ersten Schritt wird hier eIDAS bei der Authentifizierung über eIDAS übergeben. 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
- Authega
- 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 das Vertrauensniveau mitzugeben. Nähere Informationen dazu können der gesonderten Dokumentation zur Postfach-API entnommen werden.

Dieses Attribut ist nicht für eine eindeutige Nutzerreferenzierung in der Drittanwendung geeignet.

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

Jedem Nutzerkonto 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 Sie der gesonderten Schnittstellendokumentation zur Postfach-API entnehmen.

6.2.7 Optionale Attribute bei der Nutzung von Authega-Zertifikaten

Drittanwendungen können bei der Nutzung von Authega-Zertifikaten nach Abschluss der Authentisierung und Attribut-Provisionierung durch die BayernID zusätzlich die folgenden Attribute zu Auditierungszwecken erhalten:

Bezeichnung	Inhalt
ClientIP_OriginSP	Die IP-Adresse, von der aus Sicht der Drittanwendung betrachtet die Online-Sitzung angefragt wird
SessionToken_OriginSP	Die interne Sitzungsidentifikationsnummer, die derjenigen Online-Sitzung aus Sicht der Drittanwendung betrachtet zugewiesen wurde
ClientIP_authegaIDP	Die IP-Adresse, von der aus Sicht des Authega-Zentral-IDP betrachtet die Online-Sitzung angefragt wird
SessionToken_authegaIDP	Die interne Sitzungsidentifikationsnummer, die derjenigen Online-Sitzung aus Sicht des Authega-Zentral-IDP betrachtet zugewiesen wurde
ClientIP_IntermediatIDP	Die IP-Adresse, von der aus Sicht des BPV-IDP betrachtet die Online-Sitzung angefragt wird
SessionToken_IntermediatIDP	Die interne Sitzungsidentifikationsnummer, die derjenigen Online-Sitzung aus Sicht des BPV-IDP betrachtet zugewiesen wurde

Weitere Ausführungen dazu können dem gesonderten Dokument „Handreichung zum Nachweis der Beweiswerterhaltung“ entnommen werden.

7. Betriebsvoraussetzungen

7.1 Infrastruktur

Als Betreiber der SAML-basierten Infrastruktur der Identity Federation des Bayerischen Portalverbunds sichert die AKDB nach Möglichkeit die dauernde Erreichbarkeit folgender Komponenten zu:

- Identity Provider für die unterstützten Authentisierungsmethoden

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

7.2 Metadaten

Voraussetzung zur Teilnahme an der Identity Federation Infrastruktur im Bayerischen Portalverbund ist die:

- Einreichung der Beitrittserklärung (Testbetrieb vor Wirkbetrieb), sowie die darauffolgende

- Bereitstellung der SAML-Metadaten seitens der Beitrittskandidaten.

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 URL 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 bPK 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:1234/serviceprovider>, sondern sprechend wie folgendes Vorbild <https://dorf-enigmatting.de/online-rathaus>

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

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

7.3 Zusätzliche Metadaten

Diese Informationen können in den Metadaten übergeben werden. Sie werden dem Nutzer angezeigt, bevor die Daten über die SAML-Response transportiert werden.

Falls die Informationen nicht zur Verfügung stehen, werden dem Nutzer keine Informationen über den Dienst angezeigt, an den er nach seiner Zustimmung die Daten übermittelt.

Die Informationen sind also technisch nicht relevant, bieten aber einen fachlichen Mehrwert.

Auszug aus den Metadaten:

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://example.com/sp">
  <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:Extensions>
      <md:UIInfo xmlns:md:ui="urn:oasis:names:tc:SAML:metadata:ui">
        <md:ui:DisplayName xml:lang="de">Beispielanwendung</md:ui:DisplayName>
        <md:ui:Description xml:lang="de">Die Beispieldomain example.com ist eine Second-level-Domain, die von der
        Internet Engineering Task Force permanent reserviert wurde.</md:ui:Description>
        <md:ui:InformationURL xml:lang="de">https://example.com/wir-ueber-uns</md:ui:InformationURL>
        <md:ui:PrivacyStatementURL xml:lang="de">https://example.com/datenschutz</md:ui:PrivacyStatementURL>
      </md:ui:UIInfo>
    </md:Extensions>
  </md:SPSSODescriptor>
</md:EntityDescriptor>
```

7.4 Bestandener Integrationstest

Erst nach erfolgreich bestandener Integrationstest (hinsichtlich Sitzungsaufbau und -beendigung) im Zusammenspiel mit einer dedizierten Testumgebung kann die Aufnahme der Drittanwendung in den Wirkbetrieb des Bayerischen Portalverbunds, verbunden mit der Kenntnissgabe der produktiven Endpunkt-URLs und weiterer produktiver Rahmendaten, erfolgen.

8. Entscheidungsunterstützung und Handreichungen

8.1 Architekturüberlegungen bei Auswahl eines SAML-Bindings

Für die Anbindung einer Drittanwendung an den Bayerischen Portalverbund werden derzeit die beiden Request-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 Loginvorgangs 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)
```

8.3 Handreichung für EntwicklerInnen von Drittanwendungen im Bayerischen Portalverbund

Für die Anbindung an die Identity Infrastruktur erhalten die EntwicklerInnen vom Verbundbetreiber [auf Nachfrage](#):

- die SAML-Metadaten der Identity Provider
- XSDs zur Nutzung der optionalen Zusatzattribute im SAMLAuthnRequest bei Benutzung von Authega-Zertifikaten

8.5 Zurück zum Fachverfahren

Der "Zurück" Button in der ersten Anmeldeseite vom IDP dient zur Zurücknavigation zum aufrufenden Fachverfahren. Die sprachspezifische Zurücknavigation-URLs können durch optionale BackURL-Elemente in den Metadaten definiert werden. Die Entscheidung zwischen BackURL oder SAML-Response bleibt dem SP überlassen.

8.5.1 URL aus den Metadaten

Beispielhafter Auszug. akdb:BackURL kann gesetzt werden. Einträge pro Sprache sind optional. Falls nur ein Eintrag vorhanden ist, wird dieser genommen. Falls die Sprache nicht gefunden wird, wird der erste Eintrag verwendet.

```
<md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
  <md:Extensions>
    <md:UIInfo xmlns:md:ui="urn:oasis:names:tc:SAML:metadata:ui">
      <akdb:BackURL xmlns:akdb="https://www.akdb.de/idp/metadata/ui" xml:lang="de">https://www.example.com/de/back?a=1&b=2&error=user_cancelled&lang=de</akdb:BackURL>
      <akdb:BackURL xmlns:akdb="https://www.akdb.de/idp/metadata/ui" xml:lang="en">https://www.example.com/en/back?a=1&b=2&error=user_cancelled&lang=en</akdb:BackURL>
    </md:UIInfo>
  </md:Extensions>
</md:SPSSODescriptor>
```

Das Attribut `xmlns:akdb="https://www.akdb.de/idp/metadata/ui"` definiert den Namensraum für die Erweiterung von SAML-XML. Die URL "https://www.akdb.de/idp/metadata/ui" muss im gesamten Dokument unique sein. Zu beachten ist, dass nicht spezifiziert ist, dass diese URL auf irgendein bestimmtes Ziel zeigen muss. Das Präfix "akdb" wird benutzt um die Erweiterung-Elemente und Attribute in Metadaten eindeutig mit dem Namensraum zu verknüpfen. Diese Zeichenfolge (z. B. "akdb") ist frei wählbar, muss aber im gesamten Metadaten-Dokument eindeutig sein. Das Präfix muss NCName sein (siehe <https://www.w3.org/TR/xml-names/#NT-NCName>).

8.5.2 SAML-Response

Falls keine BackURL konfiguriert ist, erhält der SP beim Click auf zurück des Users eine SAML-Response, solange die Sitzung des Nutzers am IdP noch aktiv ist. Das Verhalten ist hierbei analog zu Elster oder eIDAS.

Auszug:

```
<saml2p:Response ID="_2aff60381b89b2b79d61df834af072e70810315a" InResponseTo="ID_43fd6782-7ef0-429b-8e30-4549238154f3">
  <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:AuthnFailed"/>
    </saml2p:StatusCode>
  </saml2p:Status>
</saml2p:Response>
```

9. Konfiguration der Anfrage

Über eine Extension ist es möglich die Anfrage weiter anzupassen, als das mit Standard SAML2 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>
  </akdb:AuthenticationRequest>
</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 auch 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>
```

Version 1

```
<akdb:AllowedMethods>
  <akdb:AuthnMethod>eIDAS</akdb:AuthnMethod>
  <akdb:AuthnMethod>eID</akdb:AuthnMethod>
  <akdb:AuthnMethod>Authega</akdb:AuthnMethod>
  <akdb:AuthnMethod>Diia</akdb:AuthnMethod>
  <akdb:AuthnMethod>Elster</akdb:AuthnMethod>
  <akdb:AuthnMethod>Benutzername</akdb:AuthnMethod>
  <akdb:AuthnMethod>FINK</akdb:AuthnMethod>
</akdb:AllowedMethods>
```

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. Ein 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 Erfolgsfalle) die verpflichtenden Attribute beinhaltet. Falls die erforderlichen Daten nicht vorliegen, wird eine SAML-Response als Fehler ohne Daten übertragen. RequiredAttribute ist per Default false.

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>
```

In Version 1 wurde das RequiredAttribute implizit auf true gesetzt. Ein explizites false hat keinen Einfluss. Die Liste der RequestedAttribute hat keinen Einfluss auf die Attribute die vom IdP zurückgeliefert werden. Sie dienen um die Notwendigkeit bestimmter Attribute anzuzeigen, auf deren Basis bestimmte Verfahren ausgeblendet wurde. Da diese Semantik nicht nahtlos mit der Datensparsamkeit in Einklang zu bringen war, wurde das Verhalten in Version 2 angepasst.

Version 1

```
<akdb:RequestedAttributes>
  <akdb:RequestedAttribute Name="urn:oid:2.5.4.4" />
  <akdb:RequestedAttribute Name="urn:oid:2.5.4.18" />
</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:

- bPK (urn:oid:1.2.40.0.10.2.1.1.149)
- bPK2 (urn:oid:1.3.6.1.4.1.25484.494450.3)
- legacyPostkorbHandle (urn:oid:2.5.4.18)

Werden ein, mehrere oder alle drei Attribute als benötigt angefordert, werden die Authentisierungsverfahren ausgeblendet, welche die geforderten Attribute nicht erfüllen (siehe 9.2 zur Unterscheidung zwischen V1 und V2).

Sofern eine Drittanwendung beispielhaft ein bPK2 zwingend erfordert, kann die Drittanwendung im SAML Request mindestens eins 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. Bei FINK werden in den nächsten Monaten auch Werte in der bPK2 übertragen, jedoch noch kein legacyPostkorbHandle. Das Attribut bPK ist abgekündigt und wird bald nicht mehr unterstützt.

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.

```
<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 Änderung des Einleitungstexts

Der Purpose ist auf allen Seiten am IDP sichtbar. Nur gewisse HTML Elemente (h1 p a i b small strong u br) und Attribute (href, title, rel, target auf a) sind erlaubt. Des weiteren nur https-URLs für href.

Der Purpose fand im UX-Relaunch keine Berücksichtigung, wird aktuell also an keiner Stelle im UI angezeigt, ist technisch aber weiterhin unterstützt, jedoch ist aktuell keine fachlich sinnvolle Verwendung möglich, weswegen wir aktuell (Stand 7. Juli 2023) von der Verwendung abraten.

```

<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:Version>
</akdb:DisplayInformation>

```

9.4 Übergabe von UI-Informationen (ab Release 6)

Purpose bleibt in der Schnittstelle bestehen (siehe oben). 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. Die Übergabe ist 12 Monate nach dem Rollout von Release 6 verpflichtend. 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. Der Wert kann auch für Releases davor übergeben werden, hat dann aber keine Auswirkung. 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 Wert der Organisation zu übermitteln, die den SAML-Request stellt, sondern es können fachlich hilfreiche Informationen übermittelt werden.

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 12 Monate nach dem Rollout von Release 6 verpflichtend. Bis dahin wird der vorhandene Weg verwendet (zurück mit SAML-Response ohne Werte oder in den Metadaten vorhandene URL). Die URL wird nicht validiert, sollte aber https verwenden und keine Möglichkeit bieten Zugriff auf Daten des Benutzers zu erlangen.

OnlineServiceId (ab Release 7) In Schnittstellen-Request soll das Attribut Onlinedienst den Wert der ID enthalten der in KOOPV durch das BMI vergeben wurde. Damit soll erreicht werden das trotz Verwendung geteilter Länder-Zertifikate eine eindeutige Erkennung des Onlinedienstes möglich ist.

```

<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>

```

9.5 Berechtigungszertifikat eines Bundeslandes

Der Service Provider kann damit andeuten, dass für eID und eIDAS das Berechtigungszertifikat des Bundeslandes verwendet wird. Dafür müssen aber die organisatorischen Vorbereitungen getroffen sein, damit diese auch vom Betreiber des Servicekontos hinterlegt wurden. Alternativ kann das auch in den Metadaten des Service Providers hinterlegt werden, was dann aber kein setzen im SAML-Requests mehr ermöglicht. Für die Abkürzungen siehe auch <https://www.destatis.de/DE/Methoden/abkuerzung-bundeslaender-DE-EN.html> (DE ist kein gültiger Wert). Falls der Standard des Nutzerkontos gewünscht wird, muss der Eintrag weggelassen werden.

Mit Version 2 wird es als Kindelement von <akdb:eID> definiert.

Version 2

```
<akdb:AuthnMethods>
  <akdb:eID>
    <akdb:Berechtigungszertifikat Bundesland="BY" />
    <akdb:Enabled>true</akdb:Enabled>
  </akdb:eID>
  ...
</akdb:AuthnMethods>
```

Version 1

```
<akdb:Berechtigungszertifikat Bundesland="BY" />
```

Beispielhafter Auszug zur Konfiguration über Metadaten (relevanter Teil ist <akdb:Berechtigungszertifikat Bundesland="BY" xmlns:akdb="https://www.akdb.de/request/2018/09"/>). Das ist nur relevant, wenn ein Betreiber des Nutzerkontos auch unterschiedliche Berechtigungszertifikate anbietet.

Metadaten

```
<md:SPSSODescriptor WantAssertionsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:
protocol">
  <md:Extensions>
    <mdui:UIInfo xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui">
      <mdui:DisplayName xml:lang="de">Beispiel der Konfiguration des Berechtigungszertifikats über
Metadaten</mdui:DisplayName>
    </mdui:UIInfo>
    <akdb:Berechtigungszertifikat Bundesland="BY" xmlns:akdb="https://www.akdb.de/request/2018/09"/>
  </md:Extensions>
```

10. Anhänge

10.1 Verweise auf externe Dokumente

- Portalverbundvereinbarung
- Beitrittserklärung zum Portalverbund im Testbetrieb
- Beitrittserklärung zum Portalverbund im Wirkbetrieb
- Handreichung zum Nachweis der Beweiswerterhaltung bei Authega-Nutzung
- Handreichung zum Nachweis der Beweiswerterhaltung bei nPA-Nutzung

10.2 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

11. Annex

11.1 Authentication Request zur Nutzung von Authega-Zertifikaten mit optionalen Attributen

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:AuthnRequest
  AssertionConsumerServiceURL="https://infra-pre-bayernid.freistaat.bayern/authegafachdienst/secure/backFromIdp.xhtml"
  Destination="https://infra-pre-bayernid.freistaat.bayern/idp/profile/SAML2/Redirect/SSO"
  ID="_c27f2ea23338501b3f09e488c51d011a"
  IssueInstant="2018-05-11T10:27:10.346Z"
  ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
  Version="2.0" xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol">
  <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
https://infra-pre-bayernid.freistaat.bayern/authegafachdienst
</saml2:Issuer>
  <saml2p:Extensions>
    <byauth:AuthSessionAttribute Name="ClientIP_OriginSP"
Origin="https://www.fachportal.de" Value="193.28.249.15" xmlns:byauth="https://www.authega.bayern.de/authsession/2017/08"/>
    <byauth:AuthSessionAttribute Name="SessionToken_OriginSP"
Origin="https://www.fachportal.de"
Value="38B86E2B86277F211C48BD88DA5F0D7F" xmlns:byauth="https://www.authega.bayern.de/authsession/2017/08"/>
  </saml2p:Extensions>
  <saml2p:NameIDPolicy AllowCreate="true"
Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"/>
  <saml2p:RequestedAuthnContext Comparison="exact">
    <saml2:AuthnContextClassRef xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
STORK-QAA-Level-3
</saml2:AuthnContextClassRef>
  </saml2p:RequestedAuthnContext>
</saml2p:AuthnRequest>
```

11.2 Beispiele für Requests

```
<saml2p:AuthnRequest
xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
AssertionConsumerServiceURL="https://samltool-ewg.pre.buergerserviceportal.de/saml/SSO"
Destination="https://pre-d-bayernid.freistaat.bayern/idp/profile/SAML2/POST/SSO"
ForceAuthn="true"
ID="8b3460e7-da7d-454b-80ca-4068b2237530"
IsPassive="false"
IssueInstant="2022-03-04T19:29:04.827Z"
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://samltool-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>
FINK
  </akdb:AuthnMethod>
```

```

<akdb:AuthnMethod>
eID
</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:Berechtigungszertifikat
Bundesland="BY"
/>
</akdb:AuthenticationRequest>
</saml2p:Extensions>
<saml2p:RequestedAuthnContext
Comparison="minimum">
<saml2:AuthnContextClassRef
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
STORK-QAA-Level-3
</saml2:AuthnContextClassRef>
</saml2p:RequestedAuthnContext>
</saml2p:AuthnRequest>

<saml2p:AuthnRequest
xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
AssertionConsumerServiceURL="https://samltool-ewg.pre.buergerserviceportal.de/saml/SSO"
Destination="https://pre-d-bayernid.freistaat.bayern/idp/profile/SAML2/POST/SSO"
ForceAuthn="true"
ID="e0dc8abd-d5cb-4767-8fa7-5c581c9f8aa7"
IsPassive="false"
IssueInstant="2022-03-04T19:30:38.033Z"
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://samltool-ewg.pre.buergerserviceportal.de
</saml2:Issuer>
<saml2p:Extensions>
<akdb:AuthenticationRequest
xmlns:akdb="https://www.akdb.de/request/2018/09"
Version="2">
<akdb:AuthnMethods>
<akdb:eID>
<akdb:Berechtigungszertifikat
Bundesland="BY"
/>
<akdb:Enabled>
true
</akdb:Enabled>
</akdb:eID>
<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: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:2.5.4.42"
RequiredAttribute="false"
/>
<akdb:RequestedAttribute
Name="urn:oid: 1.2.40.0.10.2.1.1.261.94"
RequiredAttribute="false"
/>
<akdb:RequestedAttribute
Name="urn:oid:2.5.4.4"
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:AuthenticationRequest>
</saml2p:Extensions>
<saml2p:RequestedAuthnContext
Comparison="minimum">
<saml2:AuthnContextClassRef
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
STORK-QAA-Level-3
</saml2:AuthnContextClassRef>
</saml2p:RequestedAuthnContext>
</saml2p:AuthnRequest>

```

11.3 Beispiel für Response

```

<?xml version="1.0" encoding="UTF-8"?><saml2p:Response xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
Destination="https://samltool-ewg.pre.buergerserviceportal.de/saml/SSO" ID="_21bddecdb86d6b7dee3bb223c9716c1"
InResponseTo="454221b8-0db3-4185-9220-927ba20323c3" IssueInstant="2022-03-04T19:35:27.397Z" Version="2.0"><saml2:
Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">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="#_21bddecdb86d6b7dee3bb223c9716c1"><ds:Transforms><ds:Transform Algorithm="http://www.w3.org
/2000/09/xmldsig#enveloped-signature" /><ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" /><ds:
Transforms><ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmenc#sha256" /><ds:
DigestValue>I1ljrKGtq2F8hTkjQXtCGndMamfvbTXkvTtPh7f4530=</ds:DigestValue></ds:Reference></ds:SignedInfo><ds:
SignatureValue>lNjShXgrGTVZslYfqRrXDrQDQbcDQGVGWQAcjT5olz6B+3WTRR
/hS74KveD7ULjgvl6lJlLIM0L8+fnxXaL1E2lkog4vwJ70AedZTkTebQQEelsjSYwnHQCfyNnXRnY0fyobWwbTt0Pg
/W4eOj6AvCw9FgRboK3yMIy7GlgMpHuoqnvGSUxdTI
/GvKNOSxsz5wiN3l6efXAghVidez+8OdFDYU6TfJGd3nl2sLheo+hhHI2d4sawaAFLMLhmpiJuH5s6RUSkYFmf0JbG3IgmPSB9qBMNHFTiFKrSZgyF
1ELCIKDSH0bzwDvvGhg3cLUYEGZrekUyxH6DK0HMLJ/CEA==</ds:SignatureValue><ds:KeyInfo><ds:X509Data><ds:
X509Certificate>MIIDGCCAgCgAwIBAgIVAN5phAtPmCFBPamoDoX4vLS59JT4MA0GCSqGSIb3DQEBAQUAAwFjEUMBIG
A1UEAxMLaWRwLmFrZGluZGUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQQD4sFNoPXy
JWRW+oIOJjWoxuQSqtI63VulrRxYAObwjJdT7NLDJ0UyRwMShvs7ggvEtT3nfvKKEpW0lnQRa0Va
jrS2lEQTJKEOC28ikI3dlpb6YIRcEaEAYEj99lIm4gnB4DS6XNUK08yUvQr2UiJgppw9Xn3EuC
5/LcxD464ubyyJqBZJfDnl+KFKGsA9YJomdppb5Xoce/MdlO6Eh5eEGSX2dyPRk02wVQtOjQImvM
Qhtv+JgLh3YxxRTQpay/NAhGJIRfVqk+iVUyMwLWvgWiUN3VsbYZwVj+3GiY+mz30q5CQt3ENi4I
OOonKqJkSx+kmuEfnC+/tiGImGqxAgMBAAGjXTBbMDoGAlUdeQQzMDGCC2lkC5ha2RiLmRlhiJo

```

dHRwcZovL2lkcC5ha2RiLmRlL2lkcC9zaGliYm9sZXRoMB0GA1UdDgQWBQBDRiSLzK7LbBi6KZHK
Ij29z5kMHdANBgqhkiG9w0BAQUFAAOCAQEAmc3lv4QjVvHn5ko08ex/f+NyGOOGXXhWB7S7CcKz
X7ln89FVyzB02uEUu0YB48TgMLDKmMeBRkYUumKhWh6Px42JWZjpQYJC2fj+w/axrnPSJsYq18v
uypuB3/EI1l6dX7g15l9CfVAd9YEOXqIUlF4C+BIbgiomtgoQATGVvXUKyGHJbc5eI+Zfxcv+KKFMy
QkU6AQbQ9UNTFnIUJCDqRTpFpIcju1BdCU5eX/FspCA33RmTeJtXGHkbKwakLyHb6Z3Z7hP9pUws
zwBZJKZM702G0lU7i7XhLenuMM/Cg2sfJ0FS8pOJrU1zhDwrm28Cwrl2v73NQCClm2Do2FrQ7Og==</ds:X509Certificate></ds:X509Data><
/ds:KeyInfo></ds:Signature><saml2p:Status xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"><saml2p:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:Success"/></saml2p:Status><saml2:EncryptedAssertion xmlns:saml2="urn:
oasis:names:tc:SAML:2.0:assertion"><xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" Id="
_3ad5581e90958be63e559640d6374c06" Type="http://www.w3.org/2001/04/xmlenc#Element"><xenc:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc" xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"><ds:
KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"><xenc:EncryptedKey Id="_9c62a263f73e823ealab890ed215eea8"
Recipient="https://samltool-ewg.pre.buergerserviceportal.de" xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"><xenc:
EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p" xmlns:xenc="http://www.w3.org/2001/04/
xmlenc#"><ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" xmlns:ds="http://www.w3.org/2000/09/
xmldsig#"></ds:EncryptionMethod><ds:KeyInfo><ds:X509Data><ds:
X509Certificate>MIIFnZCCA4CFE2xSSbfW3sh3ONTgVYa4QZJZu/RMA0GCSqGSIb3DQEBCwUAMIGLMRUwEwYDVQQD
DaxTYWl1sdG9vbCBFV0cxETAPBgNVBACMEllZW5jaGVuMQ8wDQYDVQQIDAZCYXllcm4xCzAJBgNV
BAYTAkRFMSIwIAZJKoZIhvcNAQkBFHhN1Z292LWRLdm9wc0Bha2RiLmRlMQ0wCwYDVQQKDARBSORC
MQ4wDAYDVQQLDAVHRjQ2NDAAeFw0YMTExMjYwOTA3MjFaFw0YnJExMjUwOTA3MjFaMIGLMRUwEwYD
VQDDAaxTYWl1sdG9vbCBFV0cxETAPBgNVBACMEllZW5jaGVuMQ8wDQYDVQQIDAZCYXllcm4xCzAJ
BgNVBAYTAkRFMSIwIAZJKoZIhvcNAQkBFHhN1Z292LWRLdm9wc0Bha2RiLmRlMQ0wCwYDVQQKDARBS
SORCMQ4wDAYDVQQLDAVHRjQ2NDCCAIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBALoLiGHe
k0QxvqQaZ3vwlXJ3rSrftz2nlK80deJB96tKkYX8BMF8sbC3sjz1LPdQVBSM6kPGR2+7wTdsqP
K8b0FFKwXlYn1fddVqih3nDTFYjqqcPjxi+89pBKgufSctNpQ4hQuq7IvtOUWJALXCYGR/OL1AwPcc
ddhL8JH3j9ORrqZTV5p7ck+2ukOWqUyZJfPOK+i6eSd4h6GG2I0eJpXOTIWIJHLsLuTweHbQunt8T
WJNJna4bml4L20jBr+7hvf19SN5PLScPUs0b2ryBP2MBN1hPQwtm3K78q5R3M75YYZUTrWViVKq
QwjCD//+0NiQUd1q50TVPwP9LXiE850kwo1l28BlamXX9TQa4+0VthV1Id0hcXpFr86Ldd9hW
jRwDzX5sJypjTgG7kyuDR1tRfX04zcwBtA6NdQpV/07cByw1Y1Ssqz9Ts0wDFNT+/joEF9OqMlQ24
x9JU56u6DD1vdFyMv5q3mn9nXnzXk9gUWguGg3JwUIQJQs4JzAX2e4ItBM5Yc+ZeX4SwdAVvTo
QZfZvSmw28orUZqnq6xV/2Zkf+e7tcqpmSy29nys7020NIhN10iEs6gM0v5HxDmBGV6HJCVAOVum
HxwVlYH90RwATLFTglTcmFPLXuldkFEBGjJQ44rpmwsjG/2FQayKlE9yK1w/MEKD+M+Z7AgMBAAEw
DQYJKoZIhvcNAQELBQADggIBAAGX/6B8nC7cah2izQput7r5ToPoJ2j3L1iedhEQZ2NHMKnibo259
c7g55a4FTEtv3Wx6cCLY+iJCD8At7RSKMIPs2qr32CvJURBqedVcMtyhG2aKEqkOesW0br533nO
/TxJL9K2oo81eFXh/XfChSM6x/vBFmWRQTqf9pEgkON4eVLwqClvpScf1kyleVW4RMivtZtYUoA
Q2j+X7VmkFRqgftj3McA6u7PHJned4gT9P4KSV1V0Mow7q55FEzYRN1VxN/Yrjn3bg6YXGb3S6N
S12rNX9ZAqD16Kwz58uVDDUFjmuFMIj64JfGhnzOlvtbkwikXfV9q6fJLlZepUC+Q2vQL5VCilG8
G90Tm37JriUbf9P4FQHM39LkCmFPLXuldkFEBGjJQ44rpmwsjG/2FQayKlE9yK1w/MEKD+M+Z7AgMBAAEw
DDJG2XqpFe+luGp2rm6J8Gsd283cK9/Pfi+Qt5+u98RTDHKEmrPvLKN7SMTiv8afFL2CQJZaAv1L
RK8nEF04cWfHGnqvJ83GQBP89uTUlTKzi8ls8dnORmJv9P+Wz/Sz+670f6oub9Lc8tDdXZbqf5eQb
Ha10KhDt20d8j0ZGdkbemptElNlyM1V++1Br3zBlV0bCvxadLdCREFvcgCaMpy/r7/1HJNEmr6DJ
tJjodB6Rzt1lMCQyHUdClhsa</ds:X509Certificate></ds:X509Data></ds:KeyInfo><xenc:CipherData xmlns:xenc="http://www.
w3.org/2001/04/xmlenc#"><xenc:
CipherValue>IUUA+f0BSBm6wvsqX7FGCCSxb7kGY64ozCiNaF6zfBb6l88+qBM6qc9F4HUOQP64lxb8xYsFXsNB5rt1QCS
/YfhPhisEylQ3bzOphlrlLv2zxnbfpP4iGiY3bgDBmXTNqUYB205
/tD1ob2gIhdwpOuBBDF+0lqpt60LtjdCYGGrce66tIs1SeJRfIR45G2nkHVQ2THHYIu8kf5r0JrITBdf42WivvZSb2tX1GM0lar2bmg18uVq3CWWGa
d21T/Xnx94VxcZyZB7XCB+9NkfToJZHTYiZK5HhPq2KlaImid8w0/H1L82F2YWCsWU5xj2Ly
/SSEAaorJNBtAgLSF9gnK0d0kbj9qD6cEruUlcYVf8PVPvi/acUxa7hf945pMsnjCk1ivGiLbpf3eibFMSAAfOmaX7/N2nUT2xqsKjCO
/Ce7aVukx+cfx7wwQqgtEtuxuc2U5Eh14ol45fjeLv0u0k+3zcBvCLcZiLKp3znvs3LSQhPrnF9oDliStnyUv8WiJbCmDYB7L5NiTw+IGbjZl
/tIGBdLbYquEZhd9sgr0kL8cLJUK97tumKUTKhIWUPfzweLwW98t4Wlg0IbHL+P9L2p1lAS4pWJme+lbWv0jYxQjZpCI2+2ygCLjIkZaiKB3nz
/5Yjml8ceFTPltZ+A7vZ5Gmx2ummdyis=</xenc:CipherData></xenc:CipherValue></ds:KeyInfo><xenc:
CipherData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"><xenc:CipherValue>PJfGqKJ
/yrIlcFjUJIHZGuJGWMftaj+WmWVZvOnGvph+zHTTVXJzW7YnxPk8FTGT27lQms7bneigx9JtzPcw+bEfIU+rVRpepnvka4yLVWUJ8qZnQfjKLWXFf
h1YgloGgzTJ/3oMjd3ZQLMhI/tza5/X8+oPfkGkwLUMNd6kU06fTxrPOAud7MPV3+3yLVhc6WbW+FNRRqXlt0vAbREZpAnpeYIP8kALCZlpZzVAE
/lomDim4v4vxep2RPlXNNNotEADP
/SVYncnJ3nRr3jpK4Wv6iznFbJnZjhYczPgK2tATOlDF1bXP5QXKm6YXQ3h1AP+6la7sPLgnf8JW4FOR12zJYQQCLY7Rkqq
/tsqVShyKr+YUuFfxXqj9k3jQh2cSk0jSTSS4GugK7b4SGH6x/W5b135/N
/6zzFuZIGUEWVYeA9fCXV4udVwXW130eJLuSQQY63ZYyEbmCwXIEPGfyTpr
/m1Z4VY4vxa7XTXtY5eQm3MkqKZKznfhqOYXRtXnWwPD1RiWzIGP5kiVv9pju/rswh4HiGF81EdZ6R1t8Oys5IewloARunz9pZ/rNcaV
/qvJScUcJevvWpVwNpvsfvd7YxgPhyvNhMPKRKPiOXIBRmnsulskTWADIdvCL7bV3ZeAD
/Zd2QvYUTud31ZUOz3EskC2pZ4z4RW6DyLjYHRTHrm0A0yo0idcLmJzW7vnmidv/E
/F4rNIUx2fcbtDL252BxrwlcaatiIicwWfGCB+wx+oLvzSJ29NEXGokmcadOXpKy0cAgpmx1U+UJ0yKjR61P0BqZxG7zFpRu
/HRb4OGBGLP4U4x4tWmbl6pJvVer/pe+/hpCOazARSnbJLXkcSsJof0ZghgHu34qGo4XPdxS/CHI0Z+3GMJE2rqehQRutk/GIFQLJ7hXYTH1OK
/TH41lnu/99eigQi07Dl+Djqr7Gk/CwoZfCW91C+oB4YXVHQawlXd6fVft26vZ4nbnamrtGaH2vngfXA+
/0wW+4NQgaU5gQ6sUN89cv6HAysOmQ0yWJnipUg8VWB5Uetw4NmpQ8r2XY3qOgdfdBJFJWJ9iRortF2ajjKPYASN0td806Bt3lv9iA4Iw8NXHMzMp
3uEj2VX4YY5YMPGQy77cJrJB77djEPb9coeNuGFOLIsZq8oQq
/lvN+ztpybk3+dgkX8qUHSfANBGWoiQlJyEtAYSSG6GjhaHndJ4juWQ1xs7nNoXdgsIGZS
/PtjsRMZIrXWoS5NTRIP+1Rh4003DGP3n8J+WjaaQITaZsOIaWd0l+EcKs123ZffsDGRndtuFiUtKnpjGxhR3PkiWdCs+n0DBPH4lvbMNH5dNUKh4
HdfWGHr2CVByZ1woUxVJ01xiY7ek7KisGEz7VkeZLa01xlIdzil9v53nzyCW+4UezopWHZ6BcT7G2wZg6ZHf3V9wmTj8DiUlQuRkt7SzZayLPCHWy
GQHFEZ4Yu0J/or/opisIsQnzedlNwi3Cqe9CWGyzsm7nK+cLU6xaRfC5KwG2w4GcK7ypjRZppYooemv61uLa1qnjpy/PjyuLVG
/rXLLF5Cr7zWjKdV4mmkPz28nPKM5LZ
/BIWXYT7Kw7tv2ak1Mqj4mv+0gm78HJVUoeOyMk5oArXWT8PY2uo93VThmkJUB+CplmeWzuZ2GabbV6FJO40udEmElY6Di8A6adtbOrDxtPuutmh
3eK3VQ+X6MsU8hqb+GdIlA/v2k9M6+Bmi7ahsDEVQYD/Hcpjs2rIeYnt2100KFVASsbTh0RQdHrG+hP234
/H6N4fJsYFPyXWAl3OFHcDbUyfzMo8YMZnVCw6EM3RN5XClfswVYTEV+mKPP6jd7JurGsa8+2aBY19kD3RUFudDplaC2yUcTgrfHbaODPlQZdV6XPZ
69LSn3MibYTyWLJQnZmWCLZXDND0E6AE+joBHPK608tAQ9zIOGK
/SkVnFy1aLKB5xLkY3637B700V00zdkJLK04Q4kxhJulpx6CoPrloWVWTWJevEceMVLdWSQR8DW+18cpWrfmXofdsf36pTcgFKZ2kLFYof8D6
/a0wsM8YU6Sg/7Hblpb0qN5C2q+PwqTT56U4
/hF1EK2I9CKc8h8WGL1DuvHUdS0yk9hY4u3qOcb1rMWSKZv5Ut9M2YaeZoGtVUMSVwjgkiiQJWj2Nsrhd+bkoIVPwRCKR3CrPXJjWnKXP0HvF3itqf
GPL7dcdu/PJmbsPKEAoegIN/KbstnHwuoKjRorQITCK7G81WWXf+o5OQjKYM3c7JMotA/Mq8
/R9URBoKcwK91vKbe3khtbqLTH82NshHHu66MHSKoc8w6Di+NmZv1+LHbtCMTfYRrkVJbhu
/JPY6U7fHzd0Q+Fxwwhbx2A0hfsPQfyrj7oJSQD5c7Yuf/608jbWeCNx4aqFETGFFFRMFCiy
/kApGx0upbJpkLCJrmY24SMWppjxd3F9vXwNahOgVTRHYoQKExQ5yKtQ7aA8MPxUf
/Ezf2AxxPwJCuFR3NHZNePhudqo3C0qAYkvQ8p0+xiAMVNO1Czjy0Qm
/WeGtjZwyJL4TrK2HlosVfDy2AJqhU6l0ADYyRcxxiMSCN3nYxNmqsZ1cU6PUvCq1op8a+KFSKr8aq3b0pZsFnFJwT8UDqy8gyJPS21NmgoTbgx5

/ANh/2wfwN7A0zjcvQVGzseORsH96LoJhYuvoHkNugY5vupKyKOKnlvuhFVjvRDdWO6h3deKc8Fp4AGNQAXqyj
/OAE8RiBlmq5vni+PadXk70PPncXfibmooZ0Y4baefet3slX+FtIoH6Q83NeV9mbEaGJLUX8338JHaRpmHTrav7A4k2sHj5rrQd4tZt4YwRoRqNuIUus
+6pBo7esOWJ0xiL0XAC3e2R0xnT7SfxyqoG0m7ru14qlKm+4TdAhbYqGmb
/zLcLCfd4YqITaLzotXmgZ6GiefdnUQGnsmICFa9tDD16NsMjvaLRAZclU6CEmr7ot/0Xdchfc+Jm7zys+weqnazz2nLx7YikXq8e/j06Jc1S
/ChEanDt/XoFkRhCV3NwcZkX
/yGQQC8u92PwarLVR8F0S0YU0V7P9Mgae198eQjD2WQpCrcLNa5eHavQXmfjwQN3hJxTxbILnGL69y4DyD725gsahYUV63R0CPbTH7Z51svy91MB8NQ
LYHKMD9RhFOYJCgct9geWXX6qVL5y5P7K55XnfUp8pkxMh1FM3xBCxOzvPm+6xs/CCOWpNSVMUdPM9qxX7CxxKrv5jNjdhUenKAH+j7JYvc
/XXg2v14mdhgMoHrbjULlQppYo/B254kWP5+LPLHU17Qo0J03opc+db
/3C6Lrs4JTz+3QWukvLe7NvYgeKpSPcN815f6bJRExNZ0y1plxogHUFM7Ea5LnuFsz0EluMbWeZjOow+rfb8KxpGYdvWyKu3WSq+E6q4tzQU1NRPd
VHJXHsYaXmhCMds2VjY39+8taZ9ObHUU/943odhm
/zAPdS+T0BkCLExRIGVNTvBSzcrHHwF7EFFG2UK1mh8GUSz81786EX9SEqNY3SExXIPsXs84eUuaAVJGWBfYaWVUKKG3jfI4qwx98LGHxc2HqxZCP
AjlG7G26Ih0Uz566NsXDE5hwwBevJruP3RdayJVF5SiYfWFQpUTW1J5Xr8BCv9ZLmX+S+0NE85eiJF54e3sAX12PQW
/eDpsqWuremT12RbIGBDkrQnvIVtaLaM9OLNS+tZaPjJdnXjJcdZ0IkW0oprNnLdNpGfBTM4H3PodkW+psIUxG+3lQjrdghe5A5LFF5OBGcZUnFYezw
VeAK1+kWeM1yFxrMvERoknwr7aGtLBM1MyaSI
/+0mjteDkb0IpeAQUUhJkY+NqXKcL1lIhQCzeJljpplot6LT4j7gaBlCWTdpAmfizFQ9ixGSaSPutdtztBFI8
/j+x7bJAWUeBn9+4v0z5h9dYx6FvjZci+XGO+6Jxtumi4JghIyYeTrR3nCqwiT0EPpzDVTwPmB0gzQgZvnUDALmZsS7PBR8nOWPb+pb5li44bj6jjo
kpXTrK
/IbmEJoJmXMRzmcaoRrH3Dn78Wb5INEHxHEPRzaS0VpGpPPT1btIhWejE97fXHmHl9yelyw655JmtF4lwIHcEIBofIqcqqyMhFC8htOsZgVSXE7e
/JK+6+Q//H1SPQDDe03Cg
/MEwgKKQ5rA93WcRwFVEDHzZvlWmxt2WXnhx1J0QFYMaXyQ1ml3JxqNvzztZdKjObGTU+0EZMfos0Pe98Vu9HhBqNnvw3geWtMp2z0
/tJmwOMbQLcnjZv/zv9P42SLZ9ATHYWsZESaqeNtdpQDmkOhv9wx5c9p0xaBplsiYh8NEWj7AsaGZxOu
/ZXQM6+NvxxjbaVnG1EjXLuPetvF51Q53VBWNTucdSgQVCuXL4n+QtlJ36uY/f9IGOC7YorNF91qXXZsAnWDEK51lKKT/8ewqGvXhRi4k7ptji
/ZFHAc5OqlSiqBg1l3S4EyiE9BLmtlfAXbWcGPU0HvU6+XPoBXVDZnaGrqK0C8YEpTQIAsThBrjN/Aj/fRVmHz7Go1D
/3FSt04TewZa3bfMU57WqYP7Qumuz6YTKsuniTyx+4BaUpJnVTP8jRZkBQiMpKbc4QbyZkYjQTB0X6QKxJGzItZmKQSZSvYlXsbb8LaUIuBV5EFiEM
sm0/Keel0r8epwuTfKGyQZa6MymAd7B3gS5/CwFPxyMRqI4go7NVIFn/WglXjN
/+uSidsIg53qBskjctAdR3Cu5jx0bM5ZdhfxnJi02iwwjGqLWBzsGsEX2mtQzjq88gJPDR0GzIG8jFkuF6vqXhXH79Pz+iABCyueZx7ghirg61Qx
/qSfYcCufb1AUjYDZaklU5UAXjS3rfDEbm606zN06PwDcymdo+Q4tb+4a6/LonHlfyq8
/oY4y1PkU1KbVDDYjB53abxaQcxRukQBaw9ugt3awkEAV4Ubb01bYqKbqbup04kjODX0tlLip+vmiIhYl+K7tCtTNdr+a
/fAXbdYH73ndEo8CHeehYPOmXUbqbrUhHykmHhah6K1zCtsA2CgSfQU379xcKZBK2ND1RcggSuNYrNtKr7KF4Y4wWZxmictiLav4ckwbaPmpW0uVqy
uMRYPbmZKg5icntELTSBncUKga4whRie8qwkOoe6zN17XeTrvGuv783iAetQyb53+8futc6Pw9Ocw9UU6x7TymSfncLtm3Rf9HiklGMXtU3Qp1XeP
uHy+Vb4zVf0qBTTmOWt1gX1002cmem2rjz
/Hh+ome1HEy39HuDuZ5kOd4XGNj1P7F3Z8Wxax37nq9oRuQ4w+K2Yy2P+CCxm4XaXxSTeZJYn95LNG3aU9SG6hTIOepMQ8YJNp3fDiNsVsaY9Eigwq
PBQBHPTI3X2KAZonsSz0VRwwxMeRhQmUjrYzptYqu7yV7EsgXpQGeg8hmXz1AdDB0VKgGaORJ6H5ONHchvqrrrPAF6o4RDwyMrIac2QeOY7U9rcNLU
LqK2L6k6frToQrsmjgELglSCEWA3R0bpb4zRdEMhRfW7847y28v3kRAeC7u0sPfxfnTeOt45FGFOVH31fLGLgCswks8f9NQX4HEGFSSqluuDljdysS
gnNLpVXxbwPg2sJmNSYA8GsK15K8U57rYaorzV8jEBKY3QZGEwistBBN03/voEF/XXadzxS+GzX5EW/IppNGqYT0qmpPyjnnvf+jNZScdb6
/xxyoQstM9w72K3WbaNdaFzqvwgRNccc3HmBP0qHwkW4S1fWytKXF26ccFlqNE5Y97H+WeayAqVhANQefGX063jgM2A07J7bTpBlVd4kJEpyW
/pk76kup/ZSeBNoLloyJ85sPC2MKm3dq1GH53y+FYakPCkxdFoA/qMAwgNmu3
/ON0ca53k15ZIdY6aJQZzChnriN7iUjXT2tsRCC9KO1NOeUhxzotqyxSd0rxqZrLmaSuS57DPWFHECQAYRX
/Wv2PNPkpTGzne2P0aMdnPFV7v7ABi2D6JQ6CNG8ksZjKbFfTal/0gkhvYNwqiicBGdVNFAM4GroGlyOeOilLLKgwbyH/dJ7cU2J7yU9uK3yXd3
/VZaHJF+lqOuA3+d8bw4Z6ElTyGye/huy/25GmB0zEc51y9w5FlvL2NM82kZJ50jps5gn7pVG/t64zX9ibqFX272DqtY81HrZ4a/BIEP5OkkjNed
/MaHlRkzZGU3Zq3gte3h/OwIHEU1mLMJk8pOue6wHVLDPd06jks/QQLVcKESYRUBv5pTY/x+ntn81+yGysW2NvBfmz1WnB/uSN6NDP2yOrxWE
/8Bx4uy0xiOhLeiQO/BOVsRA/KgER7mzSwhJ7prXYw7FaU
/aEomp3J0B32Kc4XiTmKkEaZUT1RXXx1ULD0wm+UoKH061lNXI7n14ups0fbQ+u8qoCieLrVzbJAI84qZCWI1JGSUUhj4hKJJDVO9pwAZHJHwaADwkFc
bmr7NWPYp6QDKu4dmaWxkO+wg8g8k1hW1SnJMjTJpCWOqZJZwJkm7Lcy6rH4VF92EiyW1bAdY7iUwF4Cq8r1y2B3th2fUoWo6gsuXbdfixAcawNB
KBFyA3w47WXIczjji4TVd5GIG8LhD3+9XAGb2yelwT0vev6rlC2b08S3HMirQZJyGOSpCs3G2a4/3Gzs5Hx01U7p
/JfP8R2hMwdKnhDitQwGd9ZtXBWUF2iBivMBE4N36JXYK1lmGLYAAcyH6DXd9fHXxaFwTRUGfy0KEG3dtUbx8awy9QmLY9iBPJwfyv
/AGQdTDtPtesJjhnifr5/1R7FP8VBRLIeORgeoJ5uIhK8fI
/aEqk7pafomCC6FLVaf1f14Zhl2fNaxnNzBpUyRXdna3pmf29zXF6pr8tWdkRa6N2qCplCnlIyLQE3ns++GV9GuXDcsJbnKqoPihBCafflYJhxfiFz
NM1xWehajsWdKsS51baeN3iJes1O20wKTPdb7dreIWRyf9wPekFp+IbmiiuA4A8+X5vSaas/GFBbNKPeFchrTZ
/E2x1wt6py1+fTJULZn2XtwPXOMWdB1R8216jiQ2
/PDC+PHR5YkednXaKzOnON9jml4BPvh3MbfpMnECWI5N3KpVBNCPje0g4QBSleHP8iRLmnnwXLjXe0O4QcFZY2c2NvP3mwoHbpLqMrFOZ
/DiFbV31axQ
/jr94rprq2A+Rfu09baffioFt16ZMD6CpXgWfOSWCoc7jtLlkJXL34U659egeOThMt9LZTcZLvpB+nwCaJzLGBHCvweuQzXlMsZFNB2QDW2VZafHmH
70yYmITg+UNTJwM8
/G3OLYc2LjplLvKsJRiaotgmGfPgr1eY083Qt7vpEdaICubUGNCTykZc6iXdbVH486ytXwmI5Sp7CE19XdDzHdNZ2+TX8H9QmS17aMKMYDW9gIE5sS
pYWiGRwivX4yN/eaV0J+uhAiE7lN6g6JlRod322RJn5JLQ9SLnf4A1m9dt/c3fU5wqW7hg51B
/yH7WnriqRCeO+xULGAFuaTtnCeK03qH9ptjFQpILfYhMUBSWi26blUstK3
/XDM9cLsLbia0k9qjQOKCzwsYWHrH9tGCR8v58hm3Q+BxQIo9JN9E7HtNdvVQ3wyYy+6rSTGwuX8S7FVFgJMJ7RvOhEzYCLY83E41QGoUL5Yck1NbZ
go1qe9ZN7YdV6khyed231otZwQj/rpMCTCJlgy4LB+M9fMbdrzeluUHFJghlnjVrNGJ/iwKs
/f8Sx1vvv+Xo7x51oBNGf5qQj6UBNyOGx8UeFDlY9742VWF3AYDtOZFyzWoEDICa3pudDyRYs4kgKb0iZYyIABCD3qypf0aQHna+Jun
/McGB3AtNjUwjn4rYeldXmc3M6UBNyOGx8UeFDlY9742VWF3AYDtOZFyzWoEDICa3pudDyRYs4kgKb0iZYyIABCD3qypf0aQHna+Jun
/mVgByAlguhBFyDRSchlCV4SSJBefKVT00dilyNCDz0Ty6d60geMQKCZvLMTQPV6x85LSJRB1hFAhStbOnsFAd913kmvd60Ik4mDxPB5R2brV7zig
7Gu4uoT9a3T2GIhWDB/9/oBMOmIgAZsqaG+tBPNGkU1OfyH9QUWu66GTSaIPhXrcPHvVnsR2NwuJ+C+kaIPY8eyS9TIERRN+j5GA
/RXPCWkljti5zr8k0uhJtWzyqX09haz70fOyLZXpowbGzCRbjgd3owu3RO7GneXJS4KbwgtIxxKyUM
/oUuUK6F0DTbRBUqThMvOwYrFfWapRyNwI15jm17UTtRQcjz15wCsbjGZU961ymLw3uGBTh42b7a63DuKX6Tqng+q1b1SSkhsa81aLlL9ksULuas1
dfFnPgl+En2ed5aupRDHqzB41EufsOBAiICI
/uTx1sfmhbzParLsHJYUOdCbOIFo8NwKLCJaxZpmEmKRQVxS1+L70aGiv7NtAOM+9mZQifK0PGbuatWYTb0FyTs90A8Y7
/NMjfrF45EbTBJ8B92jbfTYagLVtYfPh4HochGD4pd5+06EfcdnBGLDob6h3aLBxBqd3KxrQout22hTAGRZdm4Swnl3xrnHsXO
/gvYPD7GnXHW612ogUk002jfhPzDmTECXthtHFNRUesj6GB5bEVk4
/BE4OkEzvevClkjPxsK0c14IMKGAW14WMSMSaW720GcUqXcaNnad6xAWwZd5WU5VZ7Ck74S5CcEzrcc0KHjXiXBTSMZme9jb3
/KwLWQKo+X6b6gOZ0a8TN0QLToirtfhsGGBgUuehOCBxAKwIeoUfRwwAioZoraJCQ45jvQIXTiTsQTA3
/SatYm1l3lenQy4LfjYFRdn+ev8alv9z5bBxlZhFWgGjN2Tp+OHGXBsUiMCx2XmioyU9CToqMY5a0qbwIsI8JGzD6lcsbZ164BB5PlKsYuDT03+po
q0bZnbugrmuTGYs8n86S42LJND
/U+1VbvHCif7y54tvDjI0DlOYxfZGaJ0u9btVxYud9eMjQcy9Sxi14GiVSUZgggBzWzY2NzTdqLbvrLXTKHbQOozf1K40WK1J0NdZFlwxOW5LgoJ0s
XYWrgjHz21tBnarCrt7L38EVsHo+I8/6t6kOUEtCT+ceD6LBMyctwuVdof9QFYhhtjnuS87WAjy6Ab
/x1PSTThwnMAfNFfXr+RdRvDoxXy44vkm70L0CSPwHdlHk01dJHr0UEmmGfXiBz/Ekf+pDXXYQ6
/vRuNmMCCOMGBnbY90dneEGsTRL63n3bsGTi+WGFVfCUXLI6kssHRxjQXBAZ4To+f23PLadjlVZa16wGclcd9OD8vx+ffXns4q2N9MhfufDTOfx1lp
E6RRPFm0TVdJDIXSuVhLmSCHG1LDbucKfTigS1qT9TrsVzTu3vc/1Lsv300x8y5+psUp9NAS9aVKxVSmSbnvxlrHX8dGKixy7q8oXOGDWZU
/mB31fWtxIx31Zh/ugHkEt8Xu2axLmLA+3N4IJZElynaETD66diaU3U/5mxBgMnKsB71lxrOW66mWEi9y
/Tbh4u5QuGqlAf2paOHGpOaQu6cOmQqlpUjLPUiYIE4QBRRn0ydg41Vwp5ZNRFFudABhQAE23zObB8LtY2af2RlaM6bsaYxDIVYxM3ROgaryV4eOK
TrkKrfdIlLj+qx0HEK4Zh2TH3Qa72zIsm+aCAPFqxXz0nFqUGtXC4B9Rluef6xhy4tEQrg5S7i0YWLKCONPI
/DCMYXF8aWv5KCCqSd6ERR5yrobUEnUJNkZfx3F2IiQcPDsVayB7
/2kgDQzyqmIR3aslygJfySAFfZAXGcoqAECagbsjvpOPcbfSZm0JvKSHOXImQmL7Ec+GUj4fVMSuzJkrrfZECMe+r
/HYR17ivb568vdmS4tUvOIR45M8HNYAg00inJvZ6TRCQ0cUTPQdTyserDawvAed360rhGGOC67+3x8XQZnv96ZmxjIyDe5kxIxnQORLvQw5koUkc2


```
<?xml version="1.0" encoding="UTF-8" standalone="1" ?>
<saml2:Assertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
ID="_lb06bf2238267d077d67db7034865f23" IssueInstant="2022-03-04T19:35:27.397Z" Version="2.0">
<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="#_lb06bf2238267d077d67db7034865f23">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
<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/2000/09/xmldsig#sha1" />
<ds:DigestValue/>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue/>
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>MIIDGCCAgCgAwIBAgIVAN5phAtPmCFBPamoDoX4vLS59JT4MA0GCSqGSIb3DQEBBQUAMBYxFDAS
BgNVBAMTC2lkC5ha2RiLmRlLmB4XDTYmTAzMDA5NTY0Ml oXDTMyMTAzMDA5NTY0Ml oFjEUMBIG
A1UEBAxMLaWwLmFrZGluZGZGUGwgcEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQQDD4sFNpXy
JWRW+oIOJJwoXuQsQtI63VULrRxYAObwjJdT7NLDJ0UyRwMShvs7ggvEtT3nfvKKEpW01nQRa0Va
jrS2lEQ7JKEOC28ikI3dlpbpb6YIrcEaAEYIe j99lIm4gNB4DS6XNUKD8yUvQr2Ui jgpwp9Xn3EuC
5/LcxD464ubyyjgBZJfDn1+KFKGsA9YJomdpD5Xoce/Mdl06Eh5eEGSX2dyPRk02wVQtOjQJlmvM
Qhtv+JqLh3YxxRTqpay/NAhGJIRfvQk+ivUyMwLWvgWiUN3VsbYzWVj+3GiY+mz30q5CQt3ENi4I
O0onKqJKsX+xmuEfnc+/tiGImGqxAGMBAAGjXTBbmMDoGAlUdEQQzMDGCC2lkC5ha2RiLmRlLhiJk
dHRwcwovL2lkC5ha2RiLmRlL2lkC9zaGgliYm9sZXR0MB0GAlUdDQOwBBOdriSLzK7LbBi6KZHK
```



```
Ij29z5kMHDANBgkqhkiG9w0BAQUFAAOCAQEAmc3lv4QjVvHn5ko08ex/f+NyGOOGXXhWB7S7CcKz
X7ln89FVyzB02uEwUOYB48TgMLDKmMeBRbKyUumKhWh6Px42JWZjpQYJC2fj+w/axrnPSJsYq18v
uypuB3/EI1I6dX7g1519CfvAd9YEOXqIU1F4C+BIbgiomtgoQATGVxUKyghJbc5eI+Zfxv+KKFMy
QkU6AQBQ9UNTfN1UJCDqRTpFplcjulBdCU5eX/FspCA33RmTeJtXGHkbKwakLyHb6Z3Z7hP9pUws
zwBZJkZW702G01u7iTXhLenuMM/Cg2sfJ0Fs8p0jRulzhDWRm28Cwrl2v73NQcclm2Do2Fq70g=<=/ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</ds:Signature>
<saml2:Subject>
<saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient" NameQualifier="https://int.id.bund.de
/idp" SPNameQualifier="https://samltool-ewg.pre.buergerserviceportal.de">_aleeefa3f12e0d18ac3294762055dfa37</saml2:
NameID>
<saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
<saml2:SubjectConfirmationData Address="46.84.44.40" InResponseTo="454221b8-0db3-4185-9220-927ba20323c3"
NotOnOrAfter="2022-03-04T19:40:27.401Z" Recipient="https://samltool-ewg.pre.buergerserviceportal.de/saml/SSO"/>
</saml2:SubjectConfirmation>
</saml2:Subject>
<saml2:Conditions NotBefore="2022-03-04T19:35:27.397Z" NotOnOrAfter="2022-03-04T19:40:27.397Z">
<saml2:AudienceRestriction>
<saml2:Audience>https://samltool-ewg.pre.buergerserviceportal.de</saml2:Audience>
</saml2:AudienceRestriction>
</saml2:Conditions>
<saml2:AuthnStatement AuthnInstant="2022-03-04T19:35:27.396Z" SessionIndex="_f62b34ec5824f588e84b39ce9574ca87">
<saml2:SubjectLocality Address="46.84.44.40"/>
<saml2:AuthnContext>
<saml2:AuthnContextClassRef>STORK-QAA-Level-4</saml2:AuthnContextClassRef>
</saml2:AuthnContext>
</saml2:AuthnStatement>
<saml2:AttributeStatement>
<saml2:Attribute xmlns:akdb="https://www.akdb.de/request/2018/09" FriendlyName="legacyPostkorbHandle" Name="urn:
oid:2.5.4.18" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" akdb:TrustLevel="NORMAL">
<saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string">82207950-08ae-
4b87-abc7-a17cd3e0e80b</saml2:AttributeValue>
</saml2:Attribute>
<saml2:Attribute xmlns:akdb="https://www.akdb.de/request/2018/09" FriendlyName="postalCode" Name="urn:oid:
2.5.4.17" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" akdb:TrustLevel="HOCH">
<saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string">51147</saml2:
AttributeValue>
</saml2:Attribute>
<saml2:Attribute xmlns:akdb="https://www.akdb.de/request/2018/09" FriendlyName="postalAddress" Name="urn:oid:
2.5.4.16" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" akdb:TrustLevel="HOCH">
<saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string">HEIDESTRAE 17<
/saml2:AttributeValue>
</saml2:Attribute>
<saml2:Attribute xmlns:akdb="https://www.akdb.de/request/2018/09" FriendlyName="gender" Name="urn:oid:
1.3.6.1.4.1.33592.1.3.5" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" akdb:TrustLevel="
UNTERGEORDNET">
<saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string">2</saml2:
AttributeValue>
</saml2:Attribute>
<saml2:Attribute xmlns:akdb="https://www.akdb.de/request/2018/09" FriendlyName="country" Name="urn:oid:
1.2.40.0.10.2.1.1.225599" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" akdb:TrustLevel="HOCH">
<saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string">DE</saml2:
AttributeValue>
</saml2:Attribute>
<saml2:Attribute xmlns:akdb="https://www.akdb.de/request/2018/09" FriendlyName="birthdate" Name="urn:oid:
1.2.40.0.10.2.1.1.55" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" akdb:TrustLevel="HOCH">
<saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string">1964-08-12<
/saml2:AttributeValue>
</saml2:Attribute>
<saml2:Attribute xmlns:akdb="https://www.akdb.de/request/2018/09" FriendlyName="telephoneNumber" Name="urn:oid:
2.5.4.20" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" akdb:TrustLevel="UNTERGEORDNET">
<saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string">+49 231 1081
1085</saml2:AttributeValue>
</saml2:Attribute>
<saml2:Attribute xmlns:akdb="https://www.akdb.de/request/2018/09" FriendlyName="AssertionProvedBy" Name="urn:oid:
1.3.6.1.4.1.25484.494450.2" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" akdb:TrustLevel="NORMAL">
<saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string">eID</saml2:
AttributeValue>
</saml2:Attribute>
<saml2:Attribute xmlns:akdb="https://www.akdb.de/request/2018/09" FriendlyName="bPK2" Name="urn:oid:
1.3.6.1.4.1.25484.494450.3" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" akdb:TrustLevel="NORMAL">
<saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string">
>91QdLBnd22dUIRWiy7N2DWjsBPasHVggzyCjGm58LCY</saml2:AttributeValue>
</saml2:Attribute>
<saml2:Attribute xmlns:akdb="https://www.akdb.de/request/2018/09" FriendlyName="placeOfBirth" Name="urn:oid:
1.3.6.1.5.5.7.9.2" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" akdb:TrustLevel="HOCH">
<saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string">BERLIN</saml2:
AttributeValue>
</saml2:Attribute>
<saml2:Attribute xmlns:akdb="https://www.akdb.de/request/2018/09" FriendlyName="Version" Name="urn:oid:
1.3.6.1.4.1.25484.494450.1" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" akdb:TrustLevel="NORMAL">
<saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string">2021.7.1</saml2:
AttributeValue>
```

```
<saml2:Attribute>
<saml2:Attribute xmlns:akdb="https://www.akdb.de/request/2018/09" FriendlyName="givenName" Name="urn:oid:
2.5.4.42" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" akdb:TrustLevel="HOCH">
<saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string">ERIKA</saml2:
AttributeValue>
</saml2:Attribute>
<saml2:Attribute xmlns:akdb="https://www.akdb.de/request/2018/09" FriendlyName="bPK" Name="urn:oid:
1.2.40.0.10.2.1.1.149" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" akdb:TrustLevel="NORMAL">
<saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string"
">VLQ6OmRlLmFrZGiuYnBrLnNzb0BzYwlsdG9vbCld2cucHJlLmJlZXJnZXJzZXJ2aWNlcG9ydGFsLmRlOjo5MVfKTEJuZDIyZVFVJldJeTDOMkRXa
nNCUGFzSFZnZ3p5Q2pHbTU4TENZOjoyMDIyLTAzLTA0VDIwOjMlOjI3</saml2:AttributeValue>
</saml2:Attribute>
<saml2:Attribute xmlns:akdb="https://www.akdb.de/request/2018/09" FriendlyName="localityName" Name="urn:oid:
2.5.4.7" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" akdb:TrustLevel="HOCH">
<saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string">KÖLN</saml2:
AttributeValue>
</saml2:Attribute>
<saml2:Attribute xmlns:akdb="https://www.akdb.de/request/2018/09" 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">
<saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string">GABLER</saml2:
AttributeValue>
</saml2:Attribute>
<saml2:Attribute xmlns:akdb="https://www.akdb.de/request/2018/09" FriendlyName="mail" Name="urn:oid:
0.9.2342.19200300.100.1.3" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" akdb:TrustLevel="NORMAL">
<saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string">f5-martin.
henkel@init.de</saml2:AttributeValue>
</saml2:Attribute>
<saml2:Attribute xmlns:akdb="https://www.akdb.de/request/2018/09" 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-format:uri" akdb:TrustLevel="
NORMAL">
<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 xmlns:akdb="https://www.akdb.de/request/2018/09" FriendlyName="surname" Name="urn:oid:2.5.4.4"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" akdb:TrustLevel="HOCH">
<saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string">MUSTERMANN<
/saml2:AttributeValue>
</saml2:Attribute>
</saml2:AttributeStatement>
</saml2:Assertion>
```

[16] <https://calver.org>

[17] <https://tools.ietf.org/html/rfc4519#section-2.25>

[18] der „Sun Java System Access Manager“^[TM] des Herstellers Oracle

[19] <http://docs.oracle.com/cd/E19462-01/819-4670/gbanp/index.html>