OSI Servicekonto SAML-Schnittstelle

27.02.2020

Inhalt

SAML-Protokolle

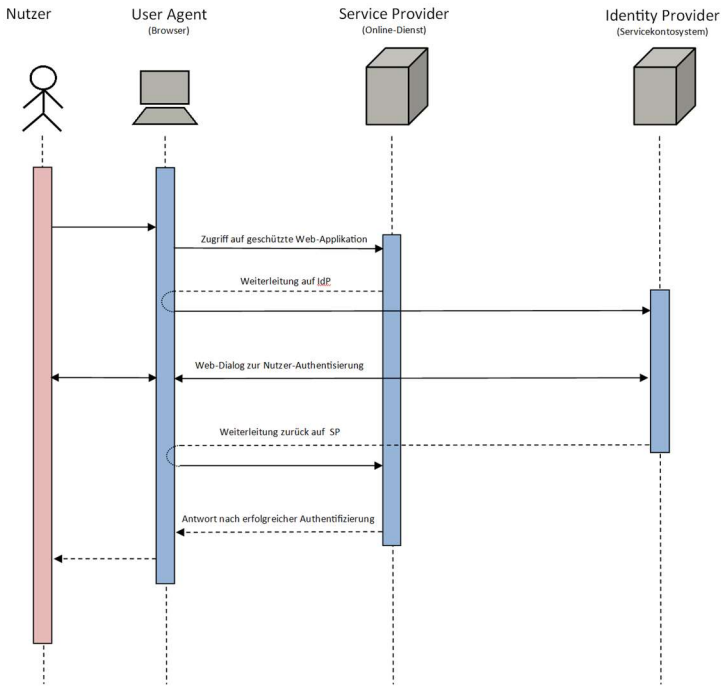
Diese Dokumentation beschreibt vornehmlich die einschränkende und erweiternde Profilierung von SAML 2.0 im Servicekontosystem. Eine allgemeine Kenntnis des SAML-Protokolls ist erforderlich, dazu sei auf die offiziellen OASIS-Spezifikationsdokumente verwiesen, insbesondere [SAML- Overview], [SAML- Core], [SAML- Bindings] und [SAML- Profiles].

Überblick und Terminologie

Eine der zentralen Funktionen des Servicekontosystems ist die Bereitstellung eines Identity Providers (IdP) gemäß SAML, der die wichtigsten Protokolle der Spezifikation von SAML 2.0 implementiert. Über diese standardisierten Protokollschnittstellen können Drittsysteme die Authentifizierung von Nutzern an den IdP delegieren und die Absicherung von Nutzersitzungen (Sessions) regeln. Nutzende Drittsysteme nehmen in der SAML-Begrifflichkeit die Rolle eines Service Providers (SP) ein. Ein SP kann die Laufzeitumgebung für mehrere Online-Dienste (SAML-Begriff: *AttributeConsumingServices*) bereitstellen. Der SP ist aber diejenige Instanz, die die SAML-Kommunikation mit dem IdP regelt und stellvertretend für die durch ihn bereitgestellten Online-Dienste verantwortet.

Kommunikationsmuster bei Authentifizierung

Die Nutzereingabe der sensiblen Authentisierungsinformationen wie z.B. Kennwort oder Zertifikat erfolgt bei SAML nicht beim SP, sondern unter der ausschließlichen Kontrolle des IdP. Dies erfordert einen Nachrichtenfluss zwischen den beteiligten Systemen SP und IdP, der Browser-Mechanismen zur Weiterleitung von http-Nachrichten verwendet (dieses Weiterleitungsmuster verwenden auch andere Authentisierungsprotokolle wie OAuth 2.0 bzw. Open ID Connect).



Nutzersitzungen und Single-Sign-On

Die OSI-Plattform verfolgt das Ziel, dem Nutzer den Eindruck eines virtuellen, geschlossenen Gesamtsystems zu vermitteln - auch bei einer verteilten Bereitstellung von Online-Diensten. Dies umfasst insbesondere auch den Aspekt der Nutzersitzungen (Sessions). Ein Nutzer, der sich an der Plattform authentisiert hat, wird i.d.R. nicht zum erneuten Login aufgefordert, wenn er auf weitere Online- oder Plattformdienste zugreifen will (Single-Sign-On / SSO).

Dazu unterstützt der IdP die Verwaltung von Sessions: Nach erfolgreicher Authentifizierung wird eine implizite IdP-Session erzeugt. Für jeden SP-Nutzer, für den der SP eine Authentifizierung angefordert hat, erzeugt der IdP eine logische SAML-Session und merkt sich diese in der IdP-Session des Nutzers. Die SAML-Session wird durch eine ID repräsentiert, die mit der vom IdP ausgestellten SAML-Assertion (strukturierter Token) zum SP transportiert wird.

Damit eine Abmeldung (Logout) an einem beliebigen SP, an dem der Nutzer eine Session besitzt, zu einer globalen Terminierung aller verteilten SP-Sessions führt, müssen alle SP-Implementierungen das SAML-Single-Logout-Profile unterstützen.

Vertrauensniveaus

Das Servicekontosystem unterstützt das Konzept der Vertrauensniveaus, die eine Klassifizierung der Vertrauenswürdigkeit einerseits von Profildaten (Name, Anschrift, Geburtsdatum) und andererseits der Authentisierungsmethode (z.B. Kennwort oder eID) repräsentieren. In Anlehnung an die eIDAS-Verordnung der Europäischen Union über elektronische Identifizierung sind diese Niveaus mit "niedrig", "substantiell" und "hoch" bezeichnet. Online-Dienste bzw. dessen SP können ein bestimmtes Niveau für die Authentifizierung vorgeben oder Autorisierungsentscheidungen abhängig machen vom Vertrauensniveau der übermittelten Profildaten.

SAML-Profile und -Bindings

Der IdP des Servicekontosystems realisiert folgende Profile der SAM 2.0 Spezifikation:

Web Browser SSO Profile

Für die Delegation der Authentifizierung wird das Protokoll gemäß „Web Browser SSO Profile“ angeboten. Unterstützt werden die SP-initiierten Szenarien von SAML 2.0, bei denen der SP die Authentifizierung durch den IdP selbst anfordert (siehe [SAML- Overview], Abschnitt 5.1.2).

Die unterstützten SAML-Bindings sind:

Nachrichtenfluss	Nachrichtentyp	Binding
SP → IdP	`<AuthnRequest>`	“HTTP redirect” oder “HTTP POST”
IdP → SP	`<Response>`	“HTTP POST”

Single Logout Profile

Für die Integration von übergreifenden Sessions wird das „Single Logout Profile“ realisiert. Die unterstützten SAML-Bindings sind:

Nachrichtenfluss	Nachrichtentyp	Binding
SP → IdP	`<LogoutRequest>`	“HTTP redirect” oder “HTTP POST”
IdP → SP	`<LogoutResponse>`	“HTTP POST”
IdP → SP	`<LogoutRequest>`	“SOAP”
SP → IdP	`<LogoutResponse>`	“SOAP”

Implementierungen von Service-Provider müssen beim Logout des Nutzers am SP einen LogoutRequest an den IdP des SKS versenden.

Ebenfalls müssen SP-Implementierungen den LogouRequest vom IdP entgegennehmen können und die Session des Nutzers im SP darauf terminieren. Dazu muss in den SAML-Metadaten des SP die URL des Logout-Endpoints für das Binding "SOAP" hinterlegt sein.

Authentifizierung

Das SP-initiierte Szenario von SAML sieht grundsätzlich vor, dass der SP (ggf. stellvertretend für die durch ihn bereitgestellten Online-Dienste) eine Authentisierungsanforderung (*AuthnRequest*) an den IdP leitet und bei erfolgreicher Authentifizierung am IdP von diesem eine Antwortnachricht (*Response*) zurück erhält. Die Antwortnachricht enthält einen strukturierten Token (*Assertion*), der diverse Informationen zum Nutzerkonto sowie zur aktuellen Session enthält.

Die Kommunikation zwischen SP und IdP verläuft bei den hier unterstützten Profile-Bindings grundsätzlich über den Web-Browser (Weiterleitungen per HTTP redirect oder HTTP POST). Daher kann der IdP-Webdialog zur Nutzereingabe der Authentifizierungsdaten in die Dialoge des SP eingeflochten werden (siehe [SAML-Overview], Abschnitt 5.1.2).

Request

Der SAML-konforme AuthnRequest (siehe Beispiel) muss wie folgt ausgeprägt sein:

Signature

Der Request muss mit dem Zertifikat aus den Metadaten (siehe Abschnitt Metadaten) signiert sein.

ProtocolBinding

Zulässige Bindings für den AuthnRequest sind:

- `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST`
- `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect`

Authentisierungsmethode

Der Request kann optional Angaben zu Authentisierungsmethoden enthalten. Diese sind gemäß SAML-Spezifikation als URI innerhalb des Elementes `samlp:AuthnnRequest/samlp:RequestedAuthnContext/samlp:AuthnContextClassRef` au szudrücken.

Zulässige Werte sind entweder an die eIDAS-Verordnung angelehnte Klassifizierung der Vertrauensniveaus oder dedizierte Methoden aus unten stehender Auflistung:

- `http://eidas.europa.eu/LoA/low`
- `http://eidas.europa.eu/LoA/substantial`
- `http://eidas.europa.eu/LoA/high`
- `urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport`
- `urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard`
- `urn:osp:servicekonto:authncontext:classes:Eid`
- `urn:osp:servicekonto:authncontext:classes:OneTimePassword`
- `urn:osp:servicekonto:authncontext:classes:IntranetSso`

Wird keine Authentisierungsmethode oder Niveau angegeben, wird standardmäßig das Vertrauensniveau „niedrig“ angenommen. In dem Authentisierungsdialog des SKS werden all die Methoden dem Nutzer angeboten, die dem geforderten Niveau oder höheren entsprechen. Enthält der AuthenRequest sowohl eine Angabe zum Niveau als auch zu einer oder mehreren Methoden, werden dem Nutzer die dem Niveau entsprechenden plus den konkreten Methoden (die ggf. nicht dem Niveau entsprechen) angeboten.

Der bei erfolgreicher Authentisierung ausgestellte Token (*Assertion*) enthält grundsätzlich die Angabe des Vertrauensniveaus der tatsächlich verwendeten Authentisierungsmethode in Form der eIDAS-URIs (siehe Abschnitt Response).

Konsumierender Online-Dienst

Im Request kann angegeben werden, für welchen konkreten Online-Dienst die Authentifizierung erfolgen soll. Zweck ist einerseits, dass das Servicekontosystem Authentisierungen abweisen kann, falls der betreffenden Nutzer für den Online-Dienst keine generelle Berechtigung besitzt (z.B. Online-Dienste für Unternehmen dürfen ggf. nicht von Bürgern genutzt werden). Andererseits werden ggf. Dienst-spezifische Rollen in die ausgestellte SAML-Assertion geschrieben.

Es gibt zwei alternative Mittel, den adressierten Online-Dienst im Request auszudrücken:

- In SAML-konformer Weise kann der für den SP eindeutige Index-Wert (*unsigned short integer*) des Online-Dienstes innerhalb des XML-Attributs `samlp:AuthnRequest/@AttributeConsumingServiceIndex` übermittelt werden.
- Alternativ kann in einer SAML-Erweiterung der für den SP eindeutige Kurzname des Online-Dienstes im Element `samlp:AuthnRequest/samlp:Extension/AuthnRequestExtension/AttributeConsumingService/@shortName` angegeben werden.

Sind im Request sowohl Index als auch Kurzname enthalten, wird der Kurzname aus der SAML-Erweiterung ignoriert. Im SKS sind alle Online-Dienste für alle SPs inkl. des Indexes und Kurznamen hinterlegt.

Wird im Request auf die Angabe des Online-Dienstes (Index oder Kurzname) verzichtet, hängt das Verhalten von der Konfiguration der Online-Dienstes im SKS ab: Ist für den SP ein Online-Dienst als *default* ausgewiesen, wird die Assertion für diesen Dienst ausgestellt (mit ggf- Dienst-spezifischen Rollen). Anderenfalls werden keine Dienst-spezifischen Rollen berücksichtigt.

Das vom IdP ausgestellte Token (*Assertion*) kann sich daher auf einen bestimmten Online-Dienst eines ServiceProviders beziehen. Dies wird innerhalb der Assertion ausgedrückt durch den *Audience*-URI innerhalb des *Condition*-Elements (siehe Abschnitt Response-Audience). Der SP ist dafür verantwortlich, die in der Assertion ausgedrückte Verwendungsbeschränkung zu beachten und durchzusetzen.

Subject

Der SP kann optional im Request ausdrücken, dass der Login für einen bestimmten Nutzer erfolgen soll. Konkret wird in dem Fall der Benutzername (E-Mail-Adresse) im Login-Dialog vorbelegt. Dazu ist SAML-konform im Request das Element `samlp:AuthnnRequest/saml:Subject/saml:NameID` zu hinterlegen. Der Wert des Elementes ist entweder die persistente ID (UUID-Syntax) oder die eindeutige E-Mail-Adresse. Das Attribut `saml:NameID/@Format` ist entsprechend mit `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent` bzw. `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress` zu besetzen.

Beispiel AuthnRequest:

```
<samlp:AuthnRequest ID="_abdef96d-8b56-41e7-aa67-727d353deb43"
                    Version="2.0"
                    IssueInstant="2018-09-26T07:07:06.048Z"
                    ForceAuthn="false"
                    IsPassive="false"
                    ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                    AssertionConsumerServiceURL="https://sp.domain/SAMLAssertionConsumerPost"
                    AttributeConsumingServiceIndex="42"
                    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
  <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:sp:id</saml:Issuer>
  <samlp:RequestedAuthnContext>
    <saml:AuthnContextClassRef xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">http://eidas.europa.eu/LoA/high</saml:AuthnContextClassRef>
  </samlp:RequestedAuthnContext>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
      <Reference URI="#_abdef96d-8b56-41e7-aa67-727d353deb43">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
          <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
            <InclusiveNamespaces PrefixList="#default samlp saml ds xs xsi"
```

```
                                xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"/>
          </Transform>
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
        <DigestValue>Base64Value...==</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>Base64Value...==</SignatureValue>
  </Signature>
</samlp:AuthnRequest>
```

Response

Bei erfolgreicher Authentifizierung des Nutzers und bei Vorhandensein einer grundsätzlichen Nutzungsberechtigung des Online-Dienstes, für den der AuthnRequest gestellt wurde, wird ein SAML-Response an den SP geliefert, der eine SAML-Assertion als strukturierten Token enthält.

Der Response (siehe Beispiel) ist wie folgt ausgeprägt:

Signatur

Sowohl der gesamte Response als auch die enthaltene Assertion ist mit dem IdP-Zertifikat aus den Metadaten (siehe Abschnitt Metadaten) signiert.

Nutzer-ID

Die ID des Nutzers wird im XML-Element `saml:Assertion/saml:Subject/saml:NameID` der SAML-Assertion abgebildet. Das Format ist `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent`, d.h. die ID ist stabil für ein Konto für alle Zeit. Für Nutzerkonten des SKS wird als Synatxformat *Universally Unique Identifier* (UUID) verwendet.

Das XML-Attribut `NameQualifier` enthält als Wert einen URI, der den Ursprung der Identität repräsentiert. Im Regelfall ist das das Servicekontosystem der Identitätsursprung, d.h. die Konten sind im im Identity-Store des SKS gespeichert. Lediglich bei IdP-Proxy-Szenarien (Interoperable Servicekonten oder Intranet-SSO) kann der URI den ursprünglichen Provider (z.B. ein Servicekontosystem eines anderen Bundeslandes) adressieren. In den Fällen bestimmt auch der ursprüngliche Provider das Syntaxformat der ID, d.h. es kann vom UUID-Format abweichen.

Audience

Mit der Audience-URI wird ausgedrückt, welche logische Stelle berechtigt ist, die Assertion zu konsumieren. Für die im Element `saml:Assertion/saml:Conditions/saml:AudienceRestriction/saml:Audience` hinterlegte URI gelten im SKS folgende Regeln:

- Grundsätzlich wird der URI des Issuer-Wertes aus dem *AuthnRequest* in die Assertion geschrieben. Der Wert ist identisch mit der *EntityID* aus den Metadaten des anfragenden SP.
- Ist im *AuthnRequest* ein bestimmter Online-Dienst des SP adressiert worden, wird zusätzlich der URI des Online-Dienstes als Audience-URI in die *Assertion* geschrieben.

Die allgemeinen Verarbeitungsregeln der SAML-Spezifikation für ServiceProvider geben vor, dass bei mehreren Audience-URIs innerhalb einer *Condition* mindestens ein URI den Konsumierenden adressieren muss. Es ist daher bei mehreren Audience-URIs der SP-Implementierung freigestellt, ob lediglich der Issuer-URI oder ergänzend auch der Online-Dienst-URI verifiziert wird.

Authentisierungsniveau

Das Vetrauensniveau der vom Nutzer gewählten und tatsächlich verwendeten Authentisierungsmethode wird durch den Wert des Elementes `saml:Assertion/saml:AuthnStatement/saml:AuthnContext/saml:AuthnContextClassRef` ausgedrückt. Mögliche Werte sind die URIs der eIDAS-Verordnung:

- `http://eidas.europa.eu/LoA/low`
- `http://eidas.europa.eu/LoA/substantial`
- `http://eidas.europa.eu/LoA/high`

Attribute

Die möglichen SAML-Attribute innerhalb `saml:Assertion/saml:AttributeStatement` der Assertion sind im Abschnitt Attributprofil beschrieben. Das Namensformat der Attribute ist `urn:oasis:names:tc:SAML:2.0:attrname-format:basic`.

Beispiel Response:

```
<samlp:Response ID="_e6888462-4f14-42f4-a54e-5ed82ff65bc1"
        InResponseTo="_daf23624-2371-4d05-8082-c9941d7ea137"
        Version="2.0"
        IssueInstant="2018-10-04T12:49:10.407Z"
        Destination="https://sp.domain/SAMLAssertionConsumerPost"
        xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
  <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:idp:id</saml:Issuer>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
```

```
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
/>
      <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha25
6" />
      <Reference URI="#_e6888462-4f14-42f4-a54e-5ed82ff65bc1">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signat
ure" />
          <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
            <InclusiveNamespaces PrefixList="#default samlp saml ds xs xsi"
                        xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"/>
          </Transform>
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
        <DigestValue>Base64Value...==</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>Base64Value...==</SignatureValue>
    <KeyInfo>
      <X509Data>
                                  <X509Certificate>Base64Value...==</X509Certificat
e>
      </X509Data>
    </KeyInfo>
  </Signature>
  <samlp:Status>
    <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
  </samlp:Status>
  <saml:Assertion Version="2.0"
          ID="_c93f20b9-7fe6-4d77-840c-16ec741d3a7c"
          IssueInstant="2018-10-04T12:49:10.392Z"
          xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
    <saml:Issuer>urn:idp:id</saml:Issuer>
    <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
      <SignedInfo>
        <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#
" />
```

```
        <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha
256" />
        <Reference URI="#_c93f20b9-7fe6-4d77-840c-16ec741d3a7c">
          <Transforms>
            <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-sign
ature" />
            <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
              <InclusiveNamespaces PrefixList="#default saml ds xs xsi"
                        xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </Transform>
          </Transforms>
          <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
          <DigestValue>Base64Value...==</DigestValue>
        </Reference>
      </SignedInfo>
      <SignatureValue>Base64Value...==</SignatureValue>
      <KeyInfo>
        <X509Data>
          <X509Certificate>Base64Value...==</X509Certificate>
        </X509Data>
      </KeyInfo>
    </Signature>
    <saml:Subject>
      <saml:NameID NameQualifier="urn:idp:realm"
             Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent">94bc0af
9-ec23-4f65-ac1e-a2670dc7c1c9</saml:NameID>
    </saml:Subject>
    <saml:Conditions NotOnOrAfter="2018-10-04T22:49:10.392Z">
      <saml:AudienceRestriction>
        <saml:Audience>urn:sp:id</saml:Audience>
        <saml:Audience>urn:sp:id:MyOnlineService</saml:Audience>
      </saml:AudienceRestriction>
    </saml:Conditions>
    <saml:AuthnStatement AuthnInstant="2018-10-04T12:49:10.392Z"
              SessionIndex="afbf29b5-7c67-45e2-9970-5ccf72a122d8"
              SessionNotOnOrAfter="2018-10-04T13:19:10.392Z">
      <saml:AuthnContext>
```

```
        <saml:AuthnContextClassRef>http://eidas.europa.eu/LoA/low</saml:AuthnConte
xtClassRef>
      </saml:AuthnContext>
    </saml:AuthnStatement>
    <saml:AttributeStatement>
      <saml:Attribute Name="Username"
              NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml:AttributeValue xsi:type="xs:string"
                    xmlns:xs="http://www.w3.org/2001/XMLSchema"
                    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">Max.Muste
rmann@ACME.com</saml:AttributeValue>
      </saml:Attribute>
      <saml:Attribute Name="AssuranceLevel"
              NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml:AttributeValue xsi:type="xs:string"
                    xmlns:xs="http://www.w3.org/2001/XMLSchema"
                    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">Low</sam
l:AttributeValue>
      </saml:Attribute>
      <saml:Attribute Name="AcademicTitle"
              NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml:AttributeValue xsi:type="xs:string"
                    xmlns:xs="http://www.w3.org/2001/XMLSchema"
                    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">Dr.</sam
l:AttributeValue>
      </saml:Attribute>
      <saml:Attribute Name="Gender"
              NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml:AttributeValue xsi:type="xs:string"
                    xmlns:xs="http://www.w3.org/2001/XMLSchema"
                    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">Male</sam
l:AttributeValue>
      </saml:Attribute>
      <saml:Attribute Name="GivenNames"
              NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml:AttributeValue xsi:type="xs:string"
                    xmlns:xs="http://www.w3.org/2001/XMLSchema"
                    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">Max</sam
l:AttributeValue>
```

```
      </saml:Attribute>
      <saml:Attribute Name="FamilyNames"
              NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml:AttributeValue xsi:type="xs:string"
                    xmlns:xs="http://www.w3.org/2001/XMLSchema"
                    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">Musterman
n</saml:AttributeValue>
      </saml:Attribute>
      <saml:Attribute Name="EmailAddress"
              NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml:AttributeValue xsi:type="xs:string"
                    xmlns:xs="http://www.w3.org/2001/XMLSchema"
                    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">Max.Muste
rmann@ACME.com</saml:AttributeValue>
      </saml:Attribute>
      <saml:Attribute Name="Telephone"
              NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml:AttributeValue xsi:type="xs:string"
                    xmlns:xs="http://www.w3.org/2001/XMLSchema"
                    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">+49 40 30
30303-1234</saml:AttributeValue>
      </saml:Attribute>
      <saml:Attribute Name="Cellphone"
              NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml:AttributeValue xsi:type="xs:string"
                    xmlns:xs="http://www.w3.org/2001/XMLSchema"
                    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">+49 16097
644660</saml:AttributeValue>
      </saml:Attribute>
      <saml:Attribute Name="PrincipalType"
              NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml:AttributeValue xsi:type="xs:string"
                    xmlns:xs="http://www.w3.org/2001/XMLSchema"
                    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">Employee<
/saml:AttributeValue>
      </saml:Attribute>
      <saml:Attribute Name="LegalEntity"
              NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml:AttributeValue>
```

```
          <LegalEntityType xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                   xmlns:q1="urn:osp:servicekonto:schemas:identity"
                   xsi:type="q1:CompanyType"
                   id="8c9f988b-89a0-42ac-9f39-d388c7dd583b">
            <q1:PermitAdministratorServiceUsage>false</q1:PermitAdministratorServi
ceUsage>
            <q1:OrganizationName>ACME</q1:OrganizationName>
            <q1:OrganizationUnit>Sales</q1:OrganizationUnit>
            <q1:EmailAddress>info@ACME.com</q1:EmailAddress>
            <q1:Telephone>++49 40 30303030</q1:Telephone>
            <q1:Address>
              <q1:Street>Billstraße</q1:Street>
              <q1:StreetNumber>82</q1:StreetNumber>
              <q1:City>Hamburg</q1:City>
              <q1:ZipCode>20539</q1:ZipCode>
              <q1:Country>DEU</q1:Country>
            </q1:Address>
            <q1:PostofficeBox>
              <q1:PostboxNumber>PF 1000</q1:PostboxNumber>
              <q1:ZipCode>20095</q1:ZipCode>
              <q1:Country>DEU</q1:Country>
            </q1:PostofficeBox>
            <q1:CommercialRegistrationNumber>HRB 22119</q1:CommercialRegistrationN
umber>
          </LegalEntityType>
        </saml:AttributeValue>
      </saml:Attribute>
      <saml:Attribute Name="Role" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname
-format:basic">
        <saml:AttributeValue xsi:type="xs:string"
                   xmlns:xs="http://www.w3.org/2001/XMLSchema"
                   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">urn:osp:n
ames:rolecontext:legalentity:Administrator</saml:AttributeValue>
      </saml:Attribute>
    </saml:AttributeStatement>
  </saml:Assertion>
</samlp:Response>
```

Logout

Die SAML-Spezifikation definiert ein Protokoll (*Single Logout Protocol*), um Sitzungen (*Sessions*) eines Nutzers von mehreren Onlien-Diesten gleichzeitig zu terminieren - auch dann, wenn die Online-Dienste durch unterschiedliche SP bereitgestellt werden. Meldet sich der Nutzer bei einem Online-Dienst bzw. SP ab, wird ein *LogoutRequest* an alle anderen SP, bei denen der Nutzer eine Sitzung hält, propagiert (*Single Logout / SLO*).

Die SP-Implementierungen müssen daher SLO unterstützen. Dazu muss der SP sowohl *LogoutRequests* vom IdP entgegennehmen als auch selbst an den IdP versenden können.

Session Management

Eine SP-Implementierung muss alle Nutzersitzungen nach einer erfolgreichen Authentisierung verwalten. Dazu sind aus der *Assertion* mindenstens die ID des Nutzerkontos aus `saml:Assertion/saml:Subject/saml:NameID` inkl. dem Attribut `@NameQualifier`, den Index der Sitzung aus `saml:Assertion/saml:AuthnStatement/@SessionIndex` sowie die Gültigkeitsdauer der Sitzung zu halten. Dieses Session-Management ist erforderlich, um auf Anforderung des IdP Nutzersitzungen terminieren zu können.

Entgegennahme von LogoutRequests vom IdP

Ein SP muss einen REDIRECT- oder SOAP-Endpoint zur Entgegennahme von *LogoutRequests* bereitstellen und in den Metadaten entsprechend dokumentieren (siehe Abschnitt Metadaten). Der *LogoutRequest* enthält die persistente ID des Nutzerkontos im Element `samlp:LogoutRequest/saml:NameID`. Ggf. sind zusätzlich ein oder mehrere Indizes von Sitzungen im Element `samlp:LogoutRequest/samlp:SessionIndex`im Request enthalten.

Ist kein *SessionIndex* angegeben, so sind alle Sitzungen des Nutzers mit der übermittelten ID zu terminieren. Bei Übermittlung von *SessionIndex*-Werten sind nur die adressierten Sitzungen des Nutzers zu terminieren.

Versenden von LogoutRequests zum IdP

Führt ein Nutzer aktiv eine Abmeldung am Online-Dienst bzw. dessen SP durch, so muss der SP einen *LogoutRequest* per REDIRECT- oder POST-Binding an den IdP versenden - vor oder unmittelbar nach der Terminierung der Nutzersitzung am SP. Der IdP wird daraufhin allen anderen SPs, bei denen der Nutzer ebenfalls eine aktive Sitzung hält, einen *LogoutRequest* versenden. Der auslösende SP selbst erhält keinen *LogoutRequest* vom IdP.

Der *LogoutRequest* ist mit der ID des Nutzerkontos im Element `samlp:LogoutRequest/saml:NameID` zu versehen und mit dem Zertifikat des SP zu signieren.

Entgegennahme von LogoutResponses vom IdP

Um den vom IdP zurückgesendeten *LogoutResponse* zu empfangen, muss der SP einen Endpoint für REDIRECT- oder POST-Binding bereitstellen und in den Metadaten entsprechend dokumentieren (siehe Abschnitt Metadaten).

Beispiel LogoutRequest:

```
<samlp:LogoutRequest ID="_d7342dfe-b174-49a8-8b47-30e0abe666ea"
                     Version="2.0"
                     IssueInstant="2018-10-08T06:47:17.75Z"
                     xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
  <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:idp:id</sam
l:Issuer>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
/>
      <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha25
6"/>
      <Reference URI="#_d7342dfe-b174-49a8-8b47-30e0abe666ea">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signat
ure"/>
          <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
            <InclusiveNamespaces PrefixList="#default samlp saml ds xs xsi"
                                 xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"/>
          </Transform>
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
        <DigestValue>Base64Value...==</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>Base64Value...==</SignatureValue>
  </Signature>
  <saml:NameID SPNameQualifier="urn:sp:id"
               NameQualifier="urn:idp:realm"
```

```
                Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
                xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">8bf35530-9c62-47
f3-b403-e045c3488b06</saml:NameID>
  <samlp:SessionIndex>355bbeca-ea52-437a-b57f-619c8a470d8f</samlp:SessionIndex>
</samlp:LogoutRequest>
```

Beispiel LogoutResponse:

```
<samlp:LogoutResponse ID="_17fe1ffe-99e7-4a93-8e9a-99f413090766"
                      InResponseTo="_d7342dfe-b174-49a8-8b47-30e0abe666ea"
                      Version="2.0"
                      IssueInstant="2018-10-08T06:47:18.078Z"
                      Destination="https://sp.domain/LogoutResponse/SingleLogoutSe
rviceViaPost"
                      xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
  <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:idp:id</sam
l:Issuer>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
/>
      <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha25
6"/>
      <Reference URI="#_17fe1ffe-99e7-4a93-8e9a-99f413090766">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signat
ure"/>
          <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
            <InclusiveNamespaces PrefixList="#default samlp saml ds xs xsi"
                                 xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"/>
          </Transform>
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
        <DigestValue>Base64Value...==</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>Base64Value...==</SignatureValue>
    <KeyInfo>
```

```
      <X509Data>
        <X509Certificate>Base64Value...==</X509Certificate>
      </X509Data>
    </KeyInfo>
  </Signature>
  <samlp:Status>
    <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
    <samlp:StatusMessage>urn:oasis:names:tc:SAML:2.0:status:PartialLogout</samlp:S
tatusMessage>
  </samlp:Status>
</samlp:LogoutResponse>
```

Attributprofil

Folgende Attribute können in der SAML-Assertion innerhalb des XML-Elementes `<AttributeStatement>` enthalten sein:

Name	Typ	Wert/Format	Beschreibung	Principal-Typ
PrincipalType	xs:string	`Citizen` `Employee` `System`	Ausprägung des Principals	*Principal*
AssuranceLevel	xs:string	`Low` `Substantial` `High`	Vertrauensniveau der Identifizierung	*Person*
GivenNames	xs:string			*Person*
FamilyNames	xs:string			*Person*
EmailAddress	xs:string			*Person*
Telephone	xs:string			*Person*
Cellphone	xs:string			*Person*
Title	xs:string	`Herr` `Frau`	Anrede	*Person*
AcademicTitle	xs:string		Akademischer Titel	*Person*
Gender	xs:string	`Male` `Female` `Unknown`	Geschlecht	*Person*
DateOfBirth	xs:string	*dd-mm-yyyy*	Geburtsdatum (ggf. inexakt)	Citizen
PlaceOfResidence	AdressType	*komplex*	Wohnanschrift	Citizen
Language	xs:string	`de` `en`	Favorisierte Sprache	Citizen
Fax	xs:string			Employee
LegalEntityType	LegalEnityType	komplex	Juristische Person, bei der der Mitarbeiter Mitglied ist	Employee
Role	xs:string	URI	Rollen-URI, ggf. n-fach	Employee
Groups	GroupType	komplex	Liste von Gruppen	Employee

AdressType

Komplexer Typ im Namensraum `urn:osp:servicekonto:schemas:identity`.

Name	Typ	Wert/Format	Beschreibung
Street	xs:string		Straße
StreetNumber	xs:string		Hausnummer
City	xs:string		Stadt
ZipCode	xs:string		Postleitzahl
Country	xs:string	ISO 3166-1 alpha-3	Ländercode

LegalEnityType

Komplexer Typ im Namensraum `urn:osp:servicekonto:schemas:identity`.

Der konkrete Typ wird als `xsi:type`angegeben. Mögliche werte sind `CompanyType`, `AuthorityType` und `OrganizationType`.

Name	Typ	Wert/Format	Beschreibung	LegalEnity-Typ
OrganizationName	xs:string		Name der juristischen Person	*LegalEnity*
OrganizationUnit	xs:string		Name der Organisationeinheit	*LegalEnity*
EmailAddress	xs:string			*LegalEnity*
Telephone	xs:string			*LegalEnity*
Address	AdressType	*komplex*	Postalische Anschrift	*LegalEnity*
PostofficeBox	PostofficeBoxType	*komplex*	Postfachadresse	*LegalEnity*
CommercialRegistrationNumber	xs:string		Handelsregisternummer	Company

PostofficeBoxType

Komplexer Typ im Namensraum `urn:osp:servicekonto:schemas:identity`.

Name	Typ	Wert/Format	Beschreibung
PostboxNumber	xs:string		
ZipCode	xs:string		Postleitzahl
Country	xs:string	ISO 3166-1 alpha-3	Ländercode

###GroupType Komplexer Typ im Namensraum `urn:osp:servicekonto:schemas:identity`.

Name	Typ	Wert/Format	Beschreibung
Id	UUIDType	XML-Attribute	
XML-Element-Content	xs:string		Gruppenname

Metadaten

Die SAML 2.0 Spezifikation definiert ein XML-Schema, um Informationen zu Endpunkten, Zertifikaten und Profileinstellungen in einem formalen Dokument beschreiben zu können. Mit Hilfe der Metadaten-Dokumente handeln IdP und SP benötigte Informationen und Daten untereinander aus, um sicher und vertrauensbasiert kommunizieren zu können. Ohne Austausch von Metadaten ist keine Zusammenarbeit zwischen Servicekontosystem (IdP) und den Online-Diensten (bzw. dessen SPs) möglich. Die gegenseitige Anerkennung der Metadaten ist die Basis für die Vertrauensstellung zwischen IdP und den SPs.

Rolle: ServiceProvider

Der IdP des Servicekontosystems akzeptiert nur Requests von SPs, für die Metadaten in der Rolle *ServiceProvider* hinterlegt sind. Dazu sind vom Betreiber des SP folgende Daten auf vertrauenswürdigem Weg zu übermitteln:

- **Entity-ID**
  Die Entity-ID dient der eindeutigen Identifizierung des Serviceproviders und der Metadaten. Die Entity-ID muss eine URN (https://tools.ietf.org/html/rfc2141) oder eine URL mit http oder https Schema sein.
- **Signatur-Zertifikat**
  Das öffentliche X.509-Zertifikat, mit dem die SAML-Requests, die der SP an den IdP versendet (*AuthnRequest*, *LogoutRequest*, *LogoutResponse*), elektronisch sigiert werden. Es können auch mehrere, alternative Zertifkate angegeben werden, um z.B. den Wechsel von Zertifkaten wegen ablaufender Gültigkeitszeiträume unterbrechungsfrei gestalten zu können.
- **Enpunkt für Entgegennahme von *Responses* zu *AuthnRequests***
  Der Endpunkt (URL) für *HTTP-POST-Binding*, auf den der IdP den Response zu einem AuthnRequest mit der enthaltenen *Assertion* (oder ggf. mit einem Fehlerstatus) weiterleitet.
- **Endpunkt für *Single Logout Service***
  Ein *HTTP redirect*-Endpunkt (URL), auf dem der SP LogoutRequests vom IdP entgegennimmt und asynchron via *HTTP redirect* beantwortet oder ein SOAP-Endpunkt (URL), der *LogoutRequests* per SOAP-Binding vom IdP entgegennimmt und synchron *LogoutResponses* zurücksendet.
- **Endpunkt für Entgegennahme von *LogoutResponses***
  Der Endpunkt (URL) für *HTTP POST* oder *HTTP redirect*, auf den der IdP *LogoutResponses* weiterleitet, nachdem der SP *LogoutRequests* per *HTTP redirect* oder *HTTP POST* gesendet hat.

Die Daten können geschlossen als XML-Dokument gemäß SAML2.0-Metadata-Schema formuliert und transferiert werden oder in einer anderen geeigneten Form. Eine Signatur des XML-Dokuments ist nicht erforderlich.

Beispiel Metadata für ServiceProvider:

```
<?xml version='1.0' encoding='UTF-8'?>
<EntitiesDescriptor xmlns='urn:oasis:names:tc:SAML:2.0:metadata'>
  <EntityDescriptor entityID='urn:sp:id' xmlns='urn:oasis:names:tc:SAML:2.0:metadata'>
    <SPSSODescriptor AuthnRequestsSigned='true'
                     WantAssertionsSigned='true'
                     protocolSupportEnumeration='urn:oasis:names:tc:SAML:2.0:protocol'>
      <KeyDescriptor use='signing'>
        <ds:KeyInfo xmlns:ds='http://www.w3.org/2000/09/xmldsig#'>
          <ds:X509Data>
            <ds:X509Certificate>Base64Value...==</ds:X509Certificate>
          </ds:X509Data>
        </ds:KeyInfo>
      </KeyDescriptor>

      <AssertionConsumerService Binding='urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST'
                                Location='https://sp.domain/AssertionConsumerServicePOST'
                                index='0'/>

      <SingleLogoutService Binding='urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST'
                           Location=''
                           ResponseLocation='https://sp.doamin/LogoutResponse/SLOServicePOST'/>

      <SingleLogoutService Binding='urn:oasis:names:tc:SAML:2.0:bindings:SOAP'
                           Location='https://sp.domain/LogoutRequest/SLOServiceSOAP'/>

    </SPSSODescriptor>
  </EntityDescriptor>
</EntitiesDescriptor>
```

Rolle: IdentityProvider

Die Daten, die ein SP benötigt, um sicher mit dem IdP des Servicekontosystems interagieren zu können, werden in Form eines XML-Dokuments gemäß SAML2.0-Metadata-Schema bereitgestellt.

Personalausweis eID-Funktion

Der neue, elektronische Personalausweis (nPA) bietet eine Funktionalität zum sicheren Identitätsnachweis im Internet. Die eID-Funktion des nPA wird vom Servicekontosystem in drei unterschiedlichen Szenarien verwendet:

- **Registrierung / Profilpflege**
  Bürger können entweder im Rahmen der Registrierung oder mittels Profilpflege die Identitätsüberprüfung mit dem Personalausweis vornehmen. Die Identitätsfeststellung und die damit erhobenen Profildaten erhalten so ein hohes Vertrauensniveau.
- **Authentisierung mit Konto**
  Nutzer können die Authentisierung am Servicekontosystem mittels eID-Funktion vornehmen, sofern sie ihren Personalausweis mit ihrem Konto verknüpft haben. ServiceProvider können Einfluss darauf nehmen, welche Authentisierungsmethoden dem Nutzer geboten werden, z.B. um ausschließlich die eID-Funktion zuzulassen (siehe Abschnitt Authentisierungsmethode). In der *Assertion* ist ausgedrückt, ob ein Nutzer sich mittels eID-Funktion authentisiert hat (siehe Abschnitt Authentisierungsniveau).
- **Identifizierung ohne Konto**
  Es gibt Anwendungsfälle, in denen ein Online-Dienst ad-hoc eine Identifizierung eines Bürgers mittels eID/Personalausweis einfordert, ohne dass der Bürger ein Konto besitzen muss. Diese manchmal auch als "temporäres Bürgerkonto" bezeichnete Form der eID-Nutzung wird vom Servicekontosystem unterstützt (SAML-Erweiterung).

Für die Nutzung der eID-Funktion ist ein geeignetes Kartenlesegerät sowie die installierte AusweisApp2 auf dem Arbeitsplatzrechner des Bürgers vorhenden sein.

Temporäres Bürgerkonto

Erfordert der fachliche Prozess eines (ggf. anonymen) Online-Dienstes eine eID-Identifizierung des Bürgers mittels elektronischen Personalausweis, kann dies vom Servivekontosystem ausgeführt werden lassen. Dazu sendet der SP einen *AuthnRequest* an den IdP des Servicekontosystems analog einer normalen Authentisierung. Abweichend ist jedoch die SAML-Erweiterung durch das XML-Attribut `samlp:AuthnRequest/samlp:Extension/AuthnRequestExtension/@transient` mit dem Wert `true` auszudrücken. Zudem muss als Authentisierungsmethode eID-Funktion im Request gewählt werden (siehe Abschnitt Authentisierungsmethode.

Der Response des Servicekontosystems enthält eine *Assertion* mit Attributen aus dem Personalausweis. Bei dieser "transienten Identifizierung" wird keine Session im IdP erzeugt. Die folgenden Attribute werden standardmäßig abgefragt:

- Vorname
- Nachname
- Adresse
- Geburtsdatum
- Akademischer Titel (optional, kann durch Anwender abgewählt werden)
- Pseudonym (optional, kann durch Anwender abgewählt werden)

Beispiel AuthnRequest für transiente Identifizierung ("temporäres Bürgerkonto"):

```
<samlp:AuthnRequest ID="_abdef96d-8b56-41e7-aa67-727d353deb43"
                    Version="2.0"
                    IssueInstant="2018-09-26T07:07:06.048Z"
                    ForceAuthn="false"
                    IsPassive="false"
                    ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                    AssertionConsumerServiceURL="https://sp.domain/SAMLAssertionConsumerPost"
                    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
  <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:sp:id</saml:Issuer>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    ...
  </Signature>
  <samlp:Extensions>
    <AuthnRequestExtension xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" transient="true" xmlns="urn:dataport:osp:servicekonto:idp:authnRequestExtensions:V1_1">
      <RequestedAttributes/>
    </AuthnRequestExtension>
  </samlp:Extensions>
  <samlp:RequestedAuthnContext>
    <saml:AuthnContextClassRef xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:osp:servicekonto:authncontext:classes:Eid</saml:AuthnContextClassRef>
  </samlp:RequestedAuthnContext>
</samlp:AuthnRequest>
```

Anfordern zusätzlicher Attribute aus dem Ausweis bei transienter Anmeldung

Neben den oben genannten standardmäßig abfragbaren Attributen können weitere Attribute aus dem Ausweis ausgelesen werden. Dies sind:

- Geburtsort
- DokumentTyp
- Künstler- oder Ordensname
- Ausstellendes Land
- Ablaufdatum

- Geburtsname
- ResidencePermitI
- Nationalität

Beim Anfragen dieser Attribute kann angegeben werden, ob diese Angaben Pflicht sind (required) oder optional.

Beispiel AuthnRequest für transiente Identifizierung unter Angabe zusätzlicher abzufragender Attribute

```
<samlp:AuthnRequest ID="_abdef96d-8b56-41e7-aa67-727d353deb43"
                    Version="2.0"
                    IssueInstant="2018-09-26T07:07:06.048Z"
                    ForceAuthn="false"
                    IsPassive="false"
                    ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                    AssertionConsumerServiceURL="https://sp.domain/SAMLAssertionConsumerPost"
                    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
  <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:sp:id</saml:Issuer>
  <samlp:RequestedAuthnContext>
    <saml:AuthnContextClassRef xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:osp:servicekonto:authncontext:classes:Eid</saml:AuthnContextClassRef>
  </samlp:RequestedAuthnContext>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    ...
  </Signature>
  <samlp:Extensions>
    <AuthnRequestExtension xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" transient="true" xmlns="urn:dataport:osp:servicekonto:idp:authnRequestExtensions:V1_1">
    <RequestedAttributes>
      <RequestedAttribute name="PlaceOfBirth" required="true"/>
      <RequestedAttribute name="DocumentType" required="true"/>
      <RequestedAttribute name="ArtisticName" required="true"/>
      <RequestedAttribute name="IssuingState" required="true"/>
      <RequestedAttribute name="DateOfExpiry" required="true"/>
      <RequestedAttribute name="BirthName" required="true"/>
```

```
      <RequestedAttribute name="ResidencePermitI" required="true"/>
      <RequestedAttribute name="Nationality" required="true"/>
    </RequestedAttributes>
    </AuthnRequestExtension>
  </samlp:Extensions>
</samlp:AuthnRequest>
```

AuthnRequest Erweiterung

Die AuthnRequestExtensions sind eine SAML-Erweiterung für den AuthnRequest, um Services und Attribute anzufragen.

AuthnRequest Erweiterung:

```
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
           xmlns:tns="urn:dataport:osp:servicekonto:idp:authnRequestExtensions:V1_
1"
           targetNamespace="urn:dataport:osp:servicekonto:idp:authnRequestExtensio
ns:V1_1"
           elementFormDefault="qualified"
           attributeFormDefault="unqualified"
           version="1.1">


  <xs:complexType name="AttributeConsumingServiceType">
    <xs:annotation>
      <xs:documentation>Die eindeutige Kurzbezeichnung des vom ServiceProvider ang
efragte Dienstes.</xs:documentation>
    </xs:annotation>
    <xs:attribute name="shortName" type="xs:string" use="required" />
  </xs:complexType>


  <xs:complexType name="RequestedAttributesType">
    <xs:annotation>
      <xs:documentation>Über dieses Element kann dem IdP mitgeteilt werden, welche
 Attribute in der Assertion geliefert werden sollen.</xs:documentation>
    </xs:annotation>
    <xs:sequence>
      <xs:element name="RequestedAttribute" type="tns:RequestedAttributeType" minO
ccurs="0" maxOccurs="unbounded" />
    </xs:sequence>
  </xs:complexType>


  <xs:complexType name="RequestedAttributeType">
    <xs:annotation>
      <xs:documentation>Das Attribute name ist Name des geforderten Attributes im
NameFormat 'urn:oasis:names:tc:SAML:2.0:attrname-format:basic' und das Attribute r
equired gibt an, ob der Benutzer das Attribut abwählen kann.</xs:documentation>
    </xs:annotation>
```

```
    <xs:attribute name="name" type="xs:string" use="required" />
    <xs:attribute name="required" type="xs:boolean" default="true" />
  </xs:complexType>

  <xs:complexType name="AuthnRequestExtensionType">
    <xs:sequence>
      <xs:element name="AttributeConsumingService" type="tns:AttributeConsumingSer
viceType" minOccurs="0" maxOccurs="1" />
      <xs:element name="RequestedAttributes" type="tns:RequestedAttributesType" mi
nOccurs="0" maxOccurs="1" />
    </xs:sequence>
    <xs:attribute name="transient" type="xs:boolean" default="false" />
  </xs:complexType>

  <xs:element name="AuthnRequestExtension" type="tns:AuthnRequestExtensionType" />

</xs:schema>
```