

---

>

---

---

# **SAML Profile for SSO in Danish Public Sector V2.0**

## ***Assertion Examples,***

*Version 1.1*

# 1 Introduction

This non-normative document contains a number of examples of XML messages defined in the DK-SAML 2.0 profile.

Note that all examples are produced “by hand” and are thus not generated by a computer program. Therefore, differences may occur in real life deployments.

Note further that the examples have been simplified in order to improve readability and clarity. For example, encryption of elements is not shown and long binary values or repeated elements have been shortened etc. Therefore, the examples won’t validate directly against the SAML XML schemas published by OASIS.

## 2 SAML Assertion with OCES Attribute Profile

The first example shows an assertion conforming to the OCES Attribute Profile with citizen attributes (without encryption):

```
<saml:Assertion ID="idvalue31231231231312"
    IssueInstant="2001-12-31T12:00:00"
    Version="2.0"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

    <saml:Issuer>http://SomeIdentityProvider.dk/IdpService</saml:Issuer>

    <ds:Signature>
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
            <ds:Reference URI="#idvalue31231231231312">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#envelopedsignature" />
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
                <ds:DigestValue>TCDVSuG6grhyHbzhQFWFzGrxIPE=</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>
            x/GyPbzmFEe85pGD3claXG4Vspb9V9jGCjwcRCKrtwPS6vdVNCcY5rHaFPYWkf+5
            EIYcPzx+pXlh43SmwviCqXRjRtMANWbHLhWAptaKlywS7gFgsD0lqjyen3CP+m3D
            w6vKhaqlledl0BYyrIzb4KkH04ahNyBVXbJwqv5pUaE4=
        </ds:SignatureValue>
        <ds:KeyInfo>
            <ds:X509Data>
                <!-- The Identity Provider's OCES Certificate -->
            </ds:X509Data>
        </ds:KeyInfo>
    </ds:Signature>
</saml:Assertion>
```

```

        <ds:X509Certificate>
            MIICy jCCA jOgAwIBAgICAnUwDQYJKoZIhvcNAQEEBQAwgakkxCzAJBgNVBAYTA1VT
            MRIwEAYDVQQIEWlXaXNjb25zaW4xEDAOBgNVBACTB01hZGlzb24xIDAeBgNVBAoT
            FlVuaXZlcnNpdHkgb2YgV2lzy29uc2luMSswKQYDVQQLEyJEaXZpc2l...
        </ds:X509Certificate>
    </ds:X509Data>
</ds:KeyInfo>
</ds:Signature>

<saml:Subject>
    <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
        C=DK,O=Pølsevognen,CN=Hans Jensen
    </saml:NameID>
    <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
        <saml:SubjectConfirmationData
            Recipient="http://SomeServiceProvider.dk"
            NotOnOrAfter="2001-12-31T12:00:00"
            InResponseTo="Authn_request_identifier_1234567">
        </saml:SubjectConfirmationData>
    </saml:SubjectConfirmation>
</saml:Subject>

<saml:Conditions>
    <saml:AudienceRestriction>
        <saml:Audience>http://SomeServiceProvider.dk</saml:Audience>
    </saml:AudienceRestriction>
</saml:Conditions>

<saml:AuthnStatement AuthnInstant="2005-01-31T12:00:00Z" SessionIndex="29393948329">
    <saml:AuthnContext>
        <saml:AuthnContextClassRef>

```

```
urn:oasis:names:tc:SAML:2.0:ac:classes:X509
</saml:AuthnContextClassRef>
</saml:AuthnContext>
</saml:AuthnStatement>

<saml:AttributeStatement>

  <!-- Sur Name Core Attribute -->
  <saml:Attribute
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
    Name="urn:oid:2.5.4.4"
    FriendlyName="surName">
    <saml:AttributeValue xsi:type="xs:string">
      Jensen
    </saml:AttributeValue>
  </saml:Attribute>

  <!-- Common Name Core Attribute -->
  <saml:Attribute
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
    Name="urn:oid:2.5.4.3"
    FriendlyName="CommonName">
    <saml:AttributeValue xsi:type="xs:string">
      Hans Jensen
    </saml:AttributeValue>
  </saml:Attribute>

  <!-- Uid Core Attribute - this is the Subject Serial Number -->
  <saml:Attribute
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
    Name="urn:oid:0.9.2342.19200300.100.1.1">
    <saml:AttributeValue xsi:type="xs:string">
```

```
PID:9802-2002-2-149339142439
</saml:AttributeValue>
</saml:Attribute>

<!-- Email Core Attribute -->
<saml:Attribute
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
  Name="urn:oid:0.9.2342.19200300.100.1.3"
  FriendlyName="email">
  <saml:AttributeValue xsi:type="xs:string">
    jens@email.dk
  </saml:AttributeValue>
</saml:Attribute>

<!-- Assurance Level Core Attribute -->
<saml:Attribute
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
  Name="dk:gov:saml:attribute:AssuranceLevel">
  <saml:AttributeValue xsi:type="xs:string">2</saml:AttributeValue>
</saml:Attribute>

<!-- SpecVer Core Attribute -->
<saml:Attribute
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
  Name="dk:gov:saml:attribute:SpecVer">
  <saml:AttributeValue xsi:type="xs:string">DK-SAML-2.0</saml:AttributeValue>
</saml:Attribute>
```

```
<!-- Now comes attributes from the OCES attribute profile -->

<!--- Certificate Serial Number Attribute -->
<saml:Attribute
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
  Name="urn:oid:2.5.4.5" FriendlyName="serialNumber">
  <saml:AttributeValue xsi:type="xs:string">
    234-2345-76745-23
  </saml:AttributeValue>
</saml:Attribute>

<!--- PID Number Attribute -->
<saml:Attribute
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
  Name="dk:gov:saml:attribute:PidNumberIdentifier">
  <saml:AttributeValue xsi:type="xs:string">
    9802-2002-2-9142544
  </saml:AttributeValue>
</saml:Attribute>

<!--- CPR Number Attribute -->
<saml:Attribute
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
  Name="dk:gov:saml:attribute:CprNumberIdentifier">
  <saml:AttributeValue xsi:type="xs:string">
    2702681273
  </saml:AttributeValue>
</saml:Attribute>

</saml:AttributeStatement>
</saml:Assertion>
```

### 3 Assertion with Persistent Pseudonym

The second example shows an assertion with a persistent pseudonym (without encryption):

```
<saml:Assertion ID="idvalue31231231231312"
  IssueInstant="2001-12-31T12:00:00"
  Version="2.0"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

  <saml:Issuer>http://SomeIdentityProvider.dk/IdpService</saml:Issuer>
  <saml:Subject>
    <!-- Here we have the persistent, opaque identifier -->
    <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent">
      005a06e0-ad82-110d-a556-004005b13a2b
    </saml:NameID>

    <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
      <saml:SubjectConfirmationData
        Recipient="http://SomeServiceProvider.dk"
        NotOnOrAfter="2001-12-31T12:00:00"
        InResponseTo="Authn_request_identifier_1234567">
      </saml:SubjectConfirmationData>
    </saml:SubjectConfirmation>
  </saml:Subject>

  <saml:Conditions>
    <saml:AudienceRestriction>
      <saml:Audience>http://SomeServiceProvider.dk</saml:Audience>
    </saml:AudienceRestriction>
  </saml:Conditions>
```

```
<saml:AuthnStatement AuthnInstant="2005-01-31T12:00:00Z"
    SessionIndex="29393948329">
  <saml:AuthnContext>
    <saml:AuthnContextClassRef>
      urn:oasis:names:tc:SAML:2.0:ac:classes:X509
    </saml:AuthnContextClassRef>
  </saml:AuthnContext>
</saml:AuthnStatement>

<saml:AttributeStatement>
  <!-- Assurance Level Core Attribute -->
  <saml:Attribute
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
    Name="dk:gov:saml:attribute:AssuranceLevel">
    <saml:AttributeValue xsi:type="xs:string">4</saml:AttributeValue>
  </saml:Attribute>

  <!-- SpecVer Core Attribute -->
  <saml:Attribute
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
    Name="dk:gov:saml:attribute:SpecVer">
    <saml:AttributeValue xsi:type="xs:string">DK-SAML-2.0</saml:AttributeValue>
  </saml:Attribute>
</saml:AttributeStatement>

</saml:Assertion>
```

## 4 Authentication Request

Below is shown a signed authentication request sent from a Service Provider:

```
<samlp:AuthnRequest
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  ID="Authn_request_identifier_1234567"
  Version="2.0"
  IssueInstant="2004-12-05T09:21:59Z"
  AssertionConsumerServiceIndex="1">

  <saml:Issuer>https://www.SomeServiceProvider.dk/SAML2</saml:Issuer>

  <ds:Signature>
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
      <ds:Reference URI="#Authn_request_identifier_1234567">
        <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#envelopedsignature" />
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
        <ds:DigestValue>TCDVSuG6grhyHbzhQFWFzGrxIPE=</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>
      x/GyPbzmFEe85pGD3claXG4Vspb9V9jGCjwcRCKrtwPS6vdVNCcY5rHaFPYWkf+5
      EIYcPzx+pXlh43SmwviCqXRjRtMANWbHLhWAptaKlywS7gFgsD0lqjyen3CP+m3D
      w6vKhaqlledl0BYyrIzb4KkH04ahNyBVXbJwqv5pUaE4=
    </ds:SignatureValue>
  </ds:KeyInfo>
```

```
<ds:X509Data>
  <ds:X509Certificate>
    MIICy jCCA jOgAwIBAgICAnUwDQYJKoZIhvcNAQEEBQAwgakkxCzAJBgNVBAYTA1VT
    MRIwEAYDVQQIEWlXaXNjb25zaW4xEDAOBgNVBACTB0lhZGlzb24xIDAeBgNVBAoT
    FlVuaXZlcnNpdHkgb2YgV2lzyY29uc2luMSswKQYDVQQLEyJEaXZpc2l...
  </ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</ds:Signature>
</samlp:AuthnRequest>
```

## 5 Authentication Response

Below is shown a signed response to an authentication response. Note that the actual assertion is left out for brevity (examples of assertions can be found earlier in this document):

```
<samlp:Response
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  ID="identifier_2"
  InResponseTo="Authn_request_identifier_1234567"
  Version="2.0"
  IssueInstant="2004-12-05T09:22:05Z"
  Destination="https://www.SomeServiceProvider.dk">

  <saml:Issuer>http://SomeIdentityProvider.dk/IdpService</saml:Issuer>

  <ds:Signature>
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
      <ds:Reference URI="#identifier_2">
        <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#envelopedsignature" />
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
        <ds:DigestValue>TCDVSuG6grhyHbzhQFWFzGrxIPE=</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>
      x/GyPbzmFEe85pGD3c1aXG4VspB9V9jGCjwcRCKrtwPS6vdVNCcY5rHaFPYWkf+5
      EIYcPzx+pX1h43SmwviCqXRjRtMANWbHLhWAptaKlywS7gFgsD01qjyen3CP+m3D
      w6vKhaql10BYyrIzb4KkH04ahNyBVXbJwqv5pUaE4=
    </ds:SignatureValue>
  </ds:Signature>
</samlp:Response>
```

```
</ds:SignatureValue>
<ds:KeyInfo>
  <ds:X509Data>
    <ds:X509Certificate>
      MIICy jCCAjOgAwIBAgICAnUwDQYJKoZIhvcNAQEEBQAwgakkxCzAJBgNVBAYTA1VT
      MRIwEAYDVQQIEWlXaXNjb25zaW4xEDAOBgNVBACTB01hZGlzb24xIDAeBgNVBAoT
      FlVuaXZlcnNpdHkgb2YgV2lzy29uc2luMSswKQYDVQQLEyJEaXZpc2l...
    </ds:X509Certificate>
  </ds:X509Data>
</ds:KeyInfo>
</ds:Signature>

<samlp:Status>
  <samlp:StatusCode      Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
</samlp:Status>

<saml:Assertion>
  <!-- Left out for brevity -->
</saml:Assertion>
</Response>
```

## 6 Attribute Query Examples

This chapter contains a number of example request / response messages illustrating different scenarios with attribute queries.

The examples only show SAML messages conforming to the profile and do not detail the encapsulation in SOAP envelopes.

Please note that:

- Details of XML digital signatures and encryptions have been omitted from the examples for the sake of clarity.
- Some attribute names have been invented for the examples. These should *not* be regarded as official identifiers. Further standardization of attributes names should occur within the Danish eGovernment sector.

### 6.1 Requesting one attribute

The first example shows a request of a Production Site Number attribute (P-number). The request identifies the Subject via the DN from the OCES certificate and the uid core attribute which contains the subject serial number.

#### Request message:

```
<samlp:AttributeQuery ID="idvalue31231231231312"
  IssueInstant="2001-12-31T12:00:00"
  Version="2.0"
  Consent="urn:oasis:names:tc:SAML:2.0:consent:current-explicit"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

  <saml:Issuer>http://SomeServiceProvider.dk</saml:Issuer>

  <ds:Signature>
    ....
  </ds:Signature>

  <!-- Here is the subject - in this case the DN from the OCES certificate -->
```

```
<saml:Subject>
  <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
    C=DK,O=Pølsevognen,CN=Hans Jensen
  </saml:NameID>
</saml:Subject>

<!-- Here is the Uid Core Attribute which contains the OCES Subject Serial Number -->
<saml:Attribute
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
  Name="urn:oid:0.9.2342.19200300.100.1.1">
  <saml:AttributeValue xsi:type="xs:string">
    CVR:20688092-RID:1180636224562
  </saml:AttributeValue>
</saml:Attribute>

<!-- Here is the attribute we request (no value) -->
<saml:Attribute
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
  Name="dk:gov:saml:attribute:ProductionSiteNumberIdentifier">
</saml:Attribute>
</samlp:AttributeQuery>
```

### Response message from the Attribute Service:

```
<samlp:Response ID="idvalue31231231231312"
  IssueInstant="2006-12-31T12:10:00"
  Version="2.0"
  Consent="urn:oasis:names:tc:SAML:2.0:consent:current-implicit"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

```
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<saml:Issuer>http://SomeAttributeService.dk</saml:Issuer>

<ds:Signature>
    ...
</ds:Signature>

<samlp:Status>
    <samlp:StatusCode Value="samlp:Success"/>
    <samlp:StatusMessage>Success</samlp:StatusMessage>
</samlp:Status>

<!-- Here is the subject - in this case the DN from the OCES certificate -->
<saml:Subject>
    <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
        C=DK,O=Pølsevognen,CN=Hans Jensen
    </saml:NameID>
</saml:Subject>

<saml:Assertion ID="idvalue131231231312"
    IssueInstant="2006-12-31T12:12:00"
    Version="2.0">

    <saml:Issuer>http://SomeAttributeService.dk</saml:Issuer>

    <!-- Here is the subject - in this case the DN from the OCES certificate -->
    <saml:Subject>
        <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
            C=DK,O=Pølsevognen,CN=Hans Jensen
        </saml:NameID>
    </saml:Subject>
```

```
<saml:Conditions>
  <saml:AudienceRestriction>
    <saml:Audience>http://SomeServiceProvider.dk</saml:Audience>
  </saml:AudienceRestriction>
</saml:Conditions>

<saml:AttributeStatement>

  <!-- Here is the Uid Core Attribute which contains the Subject serialnumber -->
  <saml:Attribute
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
    Name="urn:oid:0.9.2342.19200300.100.1.1">
    <saml:AttributeValue xsi:type="xs:string">
      CVR:20688092-RID:1180636224562
    </saml:AttributeValue>
  </saml:Attribute>

  <!-- The returned attribute with the P-Number Identifier -->
  <saml:Attribute
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
    Name="dk:gov:saml:attribute:ProductionSiteNumberIdentifier">
    <saml:AttributeValue xsi:type="xs:string">
      2739661287
    </saml:AttributeValue>
  </saml:Attribute>
</saml:AttributeStatement>

</saml:Assertion>
</samlp:Response>
```

## 6.2 Requesting a set of attributes

Multiple attributes can be requested by simply including multiple `<saml:Attribute>` elements in the request (one for each requested attribute):

```
<samlp:AttributeQuery ID="idvalue31231231231312"
    IssueInstant="2001-12-31T12:00:00"
    Version="2.0"
    Consent="urn:oasis:names:tc:SAML:2.0:consent:current-explicit"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

    <saml:Issuer>http://SomeServiceProvider.dk</saml:Issuer>

    <ds:Signature>
        ....
    </ds:Signature>

    <!-- Here is the subject - in this case the DN from the OCES certificate -->
    <saml:Subject>
        <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
            C=DK,O=Pølsevognen,CN=Hans Jensen
        </saml:NameID>
    </saml:Subject>

    <!-- Here is the Uid Core Attribute which contains the Subject serialnumber -->
    <saml:Attribute
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
        Name="urn:oid:0.9.2342.19200300.100.1.1">
        <saml:AttributeValue xsi:type="xs:string">
```

```

    CVR:20688092-RID:1180636224562
  </saml:AttributeValue>
</saml:Attribute>

  <!-- Here is an attribute we request (no value) -->
  <saml:Attribute
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
    Name="dk:gov:saml:attribute:ProductionSiteNumberIdentifier">
  </saml:Attribute>

  <!-- Here is an attribute we request (no value) -->
  <saml:Attribute
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
    Name="dk:gov:saml:attribute:IsManager">
  </saml:Attribute>

  <!-- Here is an attribute we request (no value) -->
  <saml:Attribute
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
    Name="dk:gov:saml:attribute:IsAdministrator">
  </saml:Attribute>
</samlp:AttributeQuery>

```

### 6.3 Requesting all attributes

All attributes can be requested by omitting `<saml:Attribute>` elements from the query. However, an attribute specifying the uid core attribute for identification of the subject can still be included.

## 6.4 Requester doesn't have access to all attributes

When a requester queries for an attribute he is not authorized to receive, the Attribute Service returns a second-level status code being: `urn:oasis:names:tc:SAML:2.0:status:RequestDenied` followed by a sequence `<StatusDetail>` elements describing the reason for not disclosing the attribute:

```
...
<samlp:Status>
  <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Requester">

    <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:RequestDenied">
      </samlp:StatusCode>

    <samlp:StatusDetail>Requested attribute "CPR" is reserved for government organizations
  </samlp:StatusDetail>

</samlp:StatusCode/>
</samlp:Status>
...
```

## 6.5 Values do not exist for all requested attributes

Suppose attributes with names `"attr_A"` and `"attr_B"` have been requested. Both are recognized by the Attribute Service but the value of `"attr_A"` is unknown for this subject. In this situation an empty `<AttributeValue>` element is returned and the reserved `xsi:nil` attribute is set:

```
...
<saml:AttributeStatement>
  <saml:Attribute Name="attr_A">
    <saml:AttributeValue xsi:nil="true"></saml:AttributeValue>
  </saml:Attribute>
</saml:AttributeStatement>
```

```
</saml:Attribute>
```

```
<saml:Attribute Name="attr_B">
```

```
  <saml:AttributeValue xsi:type="xs:string">foobar</saml:AttributeValue>
```

```
</saml:Attribute>
```

```
</saml:AttributeStatement>
```

```
...
```

```
<end of examples>
```