FOD Beleid & Ondersteuning
SPF Stratégie & Appui

S232-AttributeService 1.0

Cookbook v 0.4

Table of Content

Introduction

The Attribute service

The SOAP service “attribute service” calls the backend FAS component “attribute service”
This component has read access to the RMA database, and will return the roles for a specific user, for a specific issuer from a relying party.

The request must contain:

- The RRN of BIS number of a person
- The saml issuer (identifies the relying party) or client id

The Response will return a base64 encoded field that contain 0 , 1 or more roles with following fields:

- role name
- roleattribute email (email of the user in the enterprise context)
- roleattribute OrganizationId (KBO/BCE number)

WSDL

WSDL : https://fsb.services.int.belgium.be/1.00/CPS_AttributeService?WSDL

See also https://dtservices.bosa.be/nl/services/service-integrator-fsb/catalogue-service-integrator/authorizationservices-s160/documentatie

```
<wsdl:definitions name="AttributeQueryService"
targetNamespace="http://iamapps.fedict.be/attributeQueryService/v1_00"
xmlns:tns="http://iamapps.fedict.be/attributeQueryService/v1_00"
xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/" xmlns:fsb="http://fsb.belgium.be/v1_01"
xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
xmlns:err="http://iamapps.fedict.be/errors/v1"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:protocol">
   <wsdl:documentation>1.0</wsdl:documentation>
```

```
  <wsp:UsingPolicy wsdl:Required="true"/>
  <wsdl:types>
    <xsd:schema
targetNamespace="http://iamapps.fedict.be/attributeQueryService/v1_00">
      <xsd:import namespace="urn:oasis:names:tc:SAML:2.0:protocol"
schemaLocation="../../XML%20Schema/saml-schema-protocol-2.0.xsd"/>
      <xsd:import namespace="http://fsb.belgium.be/v1_01"
schemaLocation="../../../../../Commons/XML%20Schema/fsb-1.01.xsd"/>
      <xsd:import namespace="http://iamapps.fedict.be/errors/v1"
schemaLocation="../../XML%20Schema/AttributeQuery-errors-schema-v1.xsd"/>
    </xsd:schema>
  </wsdl:types>
  <wsdl:message name="headerRequest">
    <wsdl:part name="requestHeader" element="fsb:SyncHeader"/>
  </wsdl:message>
  <wsdl:message name="headerResponse">
    <wsdl:part name="responseHeader" element="fsb:SyncResponseHeader"/>
  </wsdl:message>
  <wsdl:message name="AttributeQuery">
    <wsdl:part name="AttributeQuery" element="saml:AttributeQuery"/>
  </wsdl:message>
  <wsdl:message name="Response">
    <wsdl:part name="Response" element="saml:Response"/>
  </wsdl:message>
  <wsdl:message name="BusinessError">
    <wsdl:part name="BusinessError" element="err:BusinessError"/>
  </wsdl:message>
  <wsdl:message name="SystemError">
    <wsdl:part name="SystemError" element="err:SystemError"/>
  </wsdl:message>
  <wsdl:portType name="AttributeQueryPortType">
    <wsdl:operation name="AttributeQuery">
      <wsdl:documentation>some text
      </wsdl:documentation>
      <wsdl:input message="tns:AttributeQuery"/>
      <wsdl:output message="tns:Response"/>
      <wsdl:fault name="SystemError" message="tns:SystemError"/>
      <wsdl:fault name="BusinessError" message="tns:BusinessError"/>
    </wsdl:operation>
  </wsdl:portType>
  <wsdl:binding name="AttributeQuerySOAPBinding"
type="tns:AttributeQueryPortType">
    <soap:binding transport="http://schemas.xmlsoap.org/soap/http"
style="document"/>
    <wsdl:operation name="AttributeQuery">
      <soap:operation style="document" soapAction=""/>
      <wsdl:input>
```

```
        <soap:header message="tns:headerRequest" part="requestHeader"
use="literal"/>
        <soap:body use="literal"/>
        <wsp:Policy>
          <wsp:PolicyReference URI="policy:X509TokenIntegrity-2.00"/>
          <wsp:PolicyReference URI="policy:X509TokenIdentificationWOTokenSignature-
2.00"/>
        </wsp:Policy>
      </wsdl:input>
      <wsdl:output>
        <soap:header message="tns:headerResponse" part="responseHeader"
use="literal"/>
        <soap:body use="literal"/>
      </wsdl:output>
      <wsdl:fault name="SystemError">
        <soap:fault name="SystemError" use="literal"/>
      </wsdl:fault>
      <wsdl:fault name="BusinessError">
        <soap:fault name="BusinessError" use="literal"/>
      </wsdl:fault>
    </wsdl:operation>
  </wsdl:binding>
  <wsdl:service name="attributeQueryService">
    <wsdl:port name="AttributeQuerySOAP11"
binding="tns:AttributeQuerySOAPBinding">
      <soap:address
location="https://fsb.services.pr.belgium.be/1.00/CPS_AttributeService"/>
    </wsdl:port>
  </wsdl:service>
</wsdl:definitions>
```

The Attribute service - example

Request:

issuer Is visible in the saml requests, and is configured in FAS to identify the relying party and link this information to the DMA “application”, and the functional roles that are available for that relying party.

Note: in the Case of OAuth, the issuer is the client id

Examples of issuers are:

- bosa_dis_daic (This is a client id)

- *dummy.apps.digital.belgium.be/GDPR_REGISTRY (INT)*

- *fediam.acc.minfin.fgov.be (INT)*

- *https://telemarc.be (INT and PROD)*

- https://sso.health.belgium.be/sso/realms/appss *(production)*

RRNumber is the RRN of BIS number of the person

```
<soapenv:Envelope xmlns:soapenv=http://schemas.xmlsoap.org/soap/envelope/
xmlns:v1=http://fsb.belgium.be/v1_01>
  <soapenv:Header>
    <v1:SyncHeader>
      <v1:CMessageID>ATTRSERVTEST</v1:CMessageID>
    </v1:SyncHeader>
  </soapenv:Header>
  <soapenv:Body>
    <samlp:AttributeQuery Consent="urn:string:consent" ID="aaf23196-1773-2113-474a-
fe114412ab72" IssueInstant="2008-12-09T09:42:18.038Z" Version="2.0"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
      <saml:Issuer>issuer</saml:Issuer>
      <saml:Subject>
        <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:egovNRN">RRNumber</saml:NameID>
      </saml:Subject>
    </samlp:AttributeQuery>
  </soapenv:Body>
</soapenv:Envelope>
```

Response

To be able to see the roles you need to Base decode the response field <Attribute Name="urn:oid:2.5.4.4">

```
<soapenv:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soap-env:Header xmlns:soap-env="http://schemas.xmlsoap.org/soap/envelope/">
    <fsb:SyncResponseHeader xmlns:fsb="http://fsb.belgium.be/v1_01">
      <fsb:FSBMessageID>84f57d4d-5ad9-42e9-ac06-8ed8fd77c970</fsb:FSBMessageID>
      <fsb:CMessageID>C1</fsb:CMessageID>
      <fsb:PMessageID/>
    </fsb:SyncResponseHeader>
  </soap-env:Header>
  <soap:Body xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
    <ns3:Response ID="a6f0739bc-24bb-4baa-807c-b1346375b07f"
InResponseTo="_aaf23196-1773-2113-474a-fe114412ab72" Version="1.0"
IssueInstant="2020-04-17T08:28:43.012+02:00"
xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:ns2="http://www.w3.org/2000/09/xmldsig#"
xmlns:ns3="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:ns4="http://www.w3.org/2001/04/xmlenc#"
xmlns:ns5="http://iamapps.fedict.be/errors/v1"
xmlns:ns6="http://fsb.belgium.be/v1_01">
      <Issuer
NameQualifier="issuer">http://iamapps.fedict.be/attributeQueryService/v1_00</Issuer>
      <ns3:Status>
        <ns3:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
      </ns3:Status>
      <Assertion Version="2.0" ID="aeeb6a20e-519e-4188-888b-55768ad5bd40"
IssueInstant="2020-04-17T06:28:42.961Z">
        <Issuer>bosa_dis_daic</Issuer>
        <AuthnStatement AuthnInstant="2020-04-17T06:28:42.961Z"
SessionNotOnOrAfter="2020-04-17T06:43:42.961Z">
          <AuthnContext>

<AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</AuthnContex
tClassRef>
          </AuthnContext>
        </AuthnStatement>
        <AttributeStatement>
          <Attribute Name="context">
            <AttributeValue xsi:type="xs:string"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xs="http://www.w3.org/2001/XMLSchema">enterprise</AttributeValue>
          </Attribute>
          <Attribute Name="urn:oid:egovnrn-oid">
            <AttributeValue xsi:type="xs:string"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xs="http://www.w3.org/2001/XMLSchema">66101927925</AttributeValue>
          </Attribute>
          <Attribute Name="urn:oid:2.5.4.4">


            <AttributeValue xsi:type="xs:string"
xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
xmlns:xs=http://www.w3.org/2001/XMLSchema>PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZ
GluZz0iVVRGLTgiIHN0YW5kYWxvbmU9InllcyI/Pjxyb2w6Um9sZVJlc3VsdCB4bWxuczpyb2w9
Imh0dHA6Ly9iZS5mZWRpY3Qucm9sZW1nbXQvUm9sZVhNTFNjaGVtYSI+PHJvbDpSb2xlIG5
```

```
hbWU9IlRFTEVNQVJDX1BVQkxJQ19CVVlFUiI+PHJvbDpSb2xlQXR0cmlidXRlIG5hbWU9Ik9yZ2
FuaXphdGlvbklkIj4wMjEyMzU4MTQwPC9yb2w6Um9sZUF0dHJpYnV0ZT48cm9sOlJvbGVBdH
RyaWJ1dGUgbmFtZT0iRW1haWwiPmRhdmlkLm1hbXBhZXlAYm9zYS5mZ292LmJlPC9yb2w6
Um9sZUF0dHJpYnV0ZT48L3JvbDpSb2xlPjwvcm9sOlJvbGVSZXN1bHQ+</AttributeValue>

          </Attribute>
          <Attribute Name="relyingParty">
            <AttributeValue xsi:type="xs:string"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xs="http://www.w3.org/2001/XMLSchema">https://sso.health.belgium.be/sso/realms/appss</AttributeValue>
          </Attribute>
        </AttributeStatement>
      </Assertion>
    </ns3:Response>
  </soap:Body>
</soapenv:Envelope>
```

This is the decode info with the ROLE key: (in this example the issuer is https://telemarc.be so we see the Roles key's that are relevant for the Telemarc application)

Base64 decoded Attribute Name="urn:oid:2.5.4.4

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?><rol:RoleResult
xmlns:rol=http://be.fedict.rolemgmt/RoleXMLSchema><rol:Role
name="TELEMARC_PUBLIC_SUPPLIER"><rol:RoleAttribute
name="OrganizationId">0367302178</rol:RoleAttribute></rol:Role><rol:Role
name="TELEMARC_REPORTER"><rol:RoleAttribute
name="Email">harry.potter@bosa.fgov.be</rol:RoleAttribute><rol:RoleAttribute
name="OrganizationId">0367302178</rol:RoleAttribute></rol:Role><rol:Role
name="TELEMARC_PUBLIC_BUYER"><rol:RoleAttribute
name="OrganizationId">0367302178</rol:RoleAttribute></rol:Role></rol:RoleResult>
```

Response without roles , this is the case where the user has no roles for that saml issuer, then the response does not contain the Attribute Name urn:oid:2.5.4.4:

```
<soapenv:Envelope xmlns:env=http://schemas.xmlsoap.org/soap/envelope/
xmlns:soapenv=http://schemas.xmlsoap.org/soap/envelope/>
 <soap-env:Header xmlns:soap-env=http://schemas.xmlsoap.org/soap/envelope/>
  <fsb:SyncResponseHeader xmlns:fsb=http://fsb.belgium.be/v1_01>
   <fsb:FSBMessageID>9bf9d63e-f486-4c1f-8107-682b082a380a</fsb:FSBMessageID>
   <fsb:CMessageID>SDQTEST1001</fsb:CMessageID>
   <fsb:PMessageID/>
  </fsb:SyncResponseHeader>
 </soap-env:Header>
 <soap:Body xmlns:soap=http://schemas.xmlsoap.org/soap/envelope/>
  <ns3:Response ID="ac3312f31-c81d-4ed9-87b4-6327249bfe3d"
InResponseTo="_aaf23196-1773-2113-474a-fe114412ab72" Version="1.0"
IssueInstant="2022-03-08T11:55:58.302+01:00"
xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:ns2=http://www.w3.org/2000/09/xmldsig#
xmlns:ns3="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:ns4=http://www.w3.org/2001/04/xmlenc#
xmlns:ns5=http://iamapps.fedict.be/errors/v1 xmlns:ns6=http://fsb.belgium.be/v1_01>
   <Issuer
NameQualifier="issuer">http://iamapps.fedict.be/attributeQueryService/v1_00</Issuer>
   <ns3:Status>
    <ns3:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
   </ns3:Status>
   <Assertion Version="2.0" ID="a02723746-939d-4a5f-9b53-3709d80b5cf5"
IssueInstant="2022-03-08T10:55:58.273Z">
    <Issuer>https://iamapps.belgium.be/cma</Issuer>
    <AuthnStatement AuthnInstant="2022-03-08T10:55:58.273Z"
SessionNotOnOrAfter="2022-03-08T11:10:58.273Z">
     <AuthnContext>

<AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</AuthnContex
tClassRef>
     </AuthnContext>
    </AuthnStatement>
    <AttributeStatement>
     <Attribute Name="context">
      <AttributeValue xsi:type="xs:string"
xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
xmlns:xs=http://www.w3.org/2001/XMLSchema>enterprise</AttributeValue>
     </Attribute>
     <Attribute Name="urn:oid:egovnrn-oid">
      <AttributeValue xsi:type="xs:string"
xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
xmlns:xs=http://www.w3.org/2001/XMLSchema>93092149122</AttributeValue>
     </Attribute>
     <Attribute Name="relyingParty">
      <AttributeValue xsi:type="xs:string"
xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
```

```
xmlns:xs=http://www.w3.org/2001/XMLSchema>https://iamapps.belgium.be/cma</AttributeValue>
          </Attribute>
        </AttributeStatement>
      </Assertion>
    </ns3:Response>
  </soap:Body>
</soapenv:Envelope>
```