These modifications must be made by the relying party in order to work with levels:

* **Extended metadata – Service Provider:**

1. Add the following values to your ‘spAuthncontextClassrefMapping’ attribute:

* context:urn:be:fedict:iam:fas:citizen:Level500                 500
* context:urn:be:fedict:iam:fas:enterprise:Level500           500
* context:urn:be:fedict:iam:fas:citizen:Level450                 450
* context:urn:be:fedict:iam:fas:enterprise:Level450           450
* context:urn:be:fedict:iam:fas:citizen:Level400                 400
* context:urn:be:fedict:iam:fas:enterprise:Level400           400
* context:urn:be:fedict:iam:fas:citizen:Level300                 300
* context:urn:be:fedict:iam:fas:enterprise:Level300           300
* context:urn:be:fedict:iam:fas:citizen:Level200                 200
* context:urn:be:fedict:iam:fas:enterprise:Level200           200
* context:urn:be:fedict:iam:fas:citizen:Level100                 100
* context:urn:be:fedict:iam:fas:enterprise:Level100           100

Example:

<Attribute name="spAuthncontextClassrefMapping">

<Value>urn:be:fedict:iam:fas:citizen:Level500|500|</Value>

<Value>urn:be:fedict:iam:fas:enterprise:Level500|500|</Value>

<Value>urn:be:fedict:iam:fas:citizen:Level450|450|</Value>

<Value>urn:be:fedict:iam:fas:enterprise:Level450|450|</Value>

<Value>urn:be:fedict:iam:fas:citizen:Level400|400|</Value>

<Value>urn:be:fedict:iam:fas:enterprise:Level400|400|</Value>

<Value>urn:be:fedict:iam:fas:citizen:Level300|300|</Value>

<Value>urn:be:fedict:iam:fas:enterprise:Level300|300|</Value>

<Value>urn:be:fedict:iam:fas:citizen:Level200|200|</Value>

<Value>urn:be:fedict:iam:fas:enterprise:Level200|200|</Value>

<Value>urn:be:fedict:iam:fas:citizen:Level100|100|</Value>

<Value>urn:be:fedict:iam:fas:enterprise:Level100|100|</Value>

</Attribute>

1. Set the ‘spAuthncontextComparisonType’ attribute value to ‘minimum’ (default is ‘exact’):

Example:

<Attribute name="spAuthncontextComparisonType">

<Value>minimum</Value>

</Attribute>

Why?

If a relying party requests level 200 in the SAML Authentication request, the end-user will see all the authentication methods of level 200 and above. If a user selects eID, the FAS will send level 500 in the SAML response. If the comparison type is still ‘exact’, the SP will return an error because level 500 is not an exact match to level 200. However if the comparison type is set to ‘minimum’ the SP will agree because level 500 > level 200.

* **SAML AuthN request towards the FAS:**

Current:

<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"

ID="s2b1692e2ed3293d8d225e21dc37241de438dab72a"

Version="2.0"

IssueInstant="2016-11-30T11:52:05Z"

Destination="https://openam1.fedictlab.be/fas/SSORedirect/metaAlias/idp"

ForceAuthn="false"

IsPassive="false"

ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"

AssertionConsumerServiceURL="http://openam1.fedictlab.be:8080/demo1/fedletapplication"

>

<saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">http://openam1.fedictlab.be:8080/demo1</saml:Issuer>

<samlp:NameIDPolicy xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"

Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"

SPNameQualifier="http://openam1.fedictlab.be:8080/demo1"

AllowCreate="true"

/>

<samlp:RequestedAuthnContext xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"

Comparison="exact"

>

<saml:AuthnContextClassRef xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:be:fedict:iam:fas:citizen:eid</saml:AuthnContextClassRef>

</samlp:RequestedAuthnContext>

</samlp:AuthnRequest>

Levels:

<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"

ID="s2c15ad6e3651bd85b12d7745146992700a57df24e"

Version="2.0"

IssueInstant="2016-11-30T11:47:49Z"

Destination="https://openam1.fedictlab.be/fas/SSORedirect/metaAlias/idp"

ForceAuthn="false"

IsPassive="false"

ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"

AssertionConsumerServiceURL="http://openam1.fedictlab.be:8080/demo1/fedletapplication"

>

<saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">http://openam1.fedictlab.be:8080/demo1</saml:Issuer>

<samlp:NameIDPolicy xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"

Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"

SPNameQualifier="http://openam1.fedictlab.be:8080/demo1"

AllowCreate="true"

/>

**<samlp:RequestedAuthnContext xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"**

**Comparison="minimum"**

**>**

**<saml:AuthnContextClassRef xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:be:fedict:iam:fas:citizen:Level200</saml:AuthnContextClassRef>**

**</samlp:RequestedAuthnContext>**

</samlp:AuthnRequest>

🡪 Change the ‘samlp:RequestedAuthnContext’ type to ‘minimum’. This should be done automatically since you’ve change this in the extended metadata of the Service Provider.

🡪 Now set the value of the ‘saml:AuthnContextClassRef’ to the minimum level you want the user to be authenticated. (with the correct context: ‘citizen’ or ‘enterprise’)