About federation and federated access management

The basics

The federated access scenario is that a user at organisation X wants to access something at provider Y. The user does not want to have another set of credentials to manage for provider Y, and provider Y does not want to create and manage hundreds or thousands of credentials for each organisation with a site licence, or trust in a shared single set of credentials.

Where trust exists between X and Y then SAML can be used to pass information between them so the user from X does not need additional credentials and provider Y is assured that the user is legitimately entitled to access. The identity provider does the authentication and the service provider does the authorisation.

Trust

There are two parts to the trust.

First is the trust fabric of the federation where identity providers and service providers agree to pass the information in predictable and consistent ways and this is defined and managed centrally by the federation.

Then there is the trust part of each interaction where the requests and responses passed between the parties are verifiably signed, timestamped and [usually] encrypted.

SAML

SAML (Security Assertion Markup Language) is the method used to pass information between parties in a federation and it is a method of encoding XML for transport via a user's browser. As this is passed as an encoded parameter, many people refer to it as a token.

The IdP or SP software used by entities will take care of encoding and decoding the SAML as well as checking timestamps and signatures (against a master list maintained by the federation - the 'federation metadata'). You normally will not need to worry about it, but depending on your SP software you may need to parse the decoded XML. Our own SP software makes the attributes available as system variables, but it is still useful to understand what is sent. A typical decoded response would look like this:

Example SAML assertion

```
<?xml version="1.0" encoding="utf-8"?>
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" Destination="https://oasp-beta.athensams.net
/oa/auth/rcv/saml2/post" ID="c871631c2a1a4db4884990142c9ef3a0" InResponseTo="A1yj3KoJZSaZdxdQKDaB_Mq6lt8QjX2k"
IssueInstant="2015-11-11T14:46:52.263Z" Version="2.0">
  <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://idp.domain.com/openathens</saml:
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/2000/09/xmldsig#rsa-sha1" />
      <ds:Reference URI="#c871631c2a1a4db4884990142c9ef3a0">
        <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/2000/09/xmldsig#sha1" />
        <ds:DigestValue>owgDX94pPPpfzVfVoY4ub4ykvjY=</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>Jw/gylqq6mFr0yobBetUY1/LC2fKkZGUehJIeCfMXQGxASTGhkm7eWQw6d1132K84hEj+dBFskMZ
bsgNMhz0X0gYt5NJ5ezGHpoO/AWNpVxT8dU8oR+Y8ojVAwYmbZ64ANK0uLaP/ZIjcvMKPUX3hYUo
tLg+fqn+MuEHi6VdlY4umX9N4NMluXfxhkUX8+biqdThawOuPQEk/uIuVD17Zaxkv2BQhmwc5z8P
o6gaXFxgh/S97/oobrJdkMdJ7fB5CgvYtdTlCZq+iYSh+s5rQWdZ7vcx/DnT4yVst5jQt2KIdVti
+DagStcsyqpeJKamkzAeCxnBY4zgCus7qaZ74g==</ds:SignatureValue>
    <ds:KeyInfo>
      <ds:X509Data>
        <ds:X509Certificate>MIIDvjCCAqagAwIBAgIEVOxCIjANBgkqhkiG9w0BAQsFADCBoDEoMCYGCSqGSIb3DQEJARYZYXRo
ZW5zaGVscEBlZHVzZXJ2Lm9yZy51azELMAkGA1UEBhMCR0IxETAPBgNVBAgMCFNvbWVyc2V0MQ0w
CwYDVQQHDARCYXRoMRAwDgYDVQQKDAdFZHVzZXJ2MRMwEQYDVQQLDApPcGVuQXRoZW5zMR4wHAYD
VQQDDBVnYXRld2F5LmF0aGVuc2Ftcy5uZXQwHhcNMTUwMjI0MDkyMDA2WhcNMjUwMjI0MDkyMDA2
WjCBoDEoMCYGCSqGSIb3DQEJARYZYXRoZW5zaGVscEBlZHVzZXJ2Lm9yZy51azELMAkGA1UEBhMC
R0IxETAPBgNVBAgMCFNvbWVyc2V0MQ0wCwYDVQQHDARCYXRoMRAwDgYDVQQKDAdFZHVzZXJ2MRMw
EQYDVQQLDApPcGVuANDYQXRzMR4wHAYDVQQDDBVnYXRld2F5LmF0aGVuc2Ftcy5uZXQwggEiMA0G
CSqGSIb3DQEBAQUaaISadwDwggEKAoIBAQCpanda4o0Njtw1DqbrrNTfOVe1PqyXIIVmDrJ6VUR/
mokXXu+m5Gm+1f3+AWESOMEoYn9Z8Yo37JQjIHs+xVS3q4nT1ewS7S3en1pdXKsH1WnUnVWUmpl9
WJZrUwi5i8X80LNyr7PmudhuKNEATGUXkA/xWCkk2d8jf91hy7Qu+HA8LOKtdbbNigErh2IY/YuN
```

```
WUVUqgGbMH5BGr7ZEhPrz+Vwcf9lhPW+tKpKpZEzJfQiq8EoPaeMXEpKWBEErm67gkWFCA5VhfcJ
LqFjQEC3pWOxt5rZVS8gl/Z33VSJZVzY5jWcQzmGaLXPHXyiKPmixl6+DjGlUM0ylNF7GvtDAgMB
AAEwDQYJKoZIhvcNAQELBQADggEBAFhmhujLZueiJ6F7mQCpfB0Hj4Y8FyFUUc8NMAt5Set7H4DK
SSl4shcqisZBa5yTdyenYwkmBszvCWs6Yeep+zJmCR62cb/f1M32oMzLm02OlznWMkE8/IajGmdx
TnB6Z/XcdMMIiCeok4kqe5KMd5oRAyNskHYZ+8kzhs2zTveR+rqCtYxa/AYpwf7n0VQR9clBSNCI
T4BCRi10aPE531VIxl4ljY3CwNoZ4lQTU/0aj8O4j68V2neiQb8lewAii0b2xoyOGYP4okd7T2tl
4gl2noVbCvYNjd6GYze/w4lgwiemkby7wu5sN1lEudgKDV+H54wU29ZIyDEFM6DDNE4=</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:EncryptedAssertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
    <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" ID="ea43aecf4f0544e8996d0f2da3ead887"
IssueInstant="2015-11-11T14:46:52.264Z" Version="2.0">
      <saml:Issuer>https://idp.domain.com/openathens</saml:Issuer>
      <saml:Subject>
        <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" NameQualifier="https://idp.
domain.com/openathens" SPNameQualifier="http://oasp.beta.athensams.net/OaspMetadata">a7ab7e00:01618ce</saml:
NameID>
        <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
          <saml:SubjectConfirmationData InResponseTo="A1yj3KoJZSaZdxdQKDaB_Mq6lt8QjX2k" NotOnOrAfter="2015-11-
11T14:47:52.264Z" Recipient="https://oasp-beta.athensams.net/oa/auth/rcv/saml2/post" />
        </saml:SubjectConfirmation>
      </saml:Subject>
      <saml:Conditions NotBefore="2015-11-11T14:41:52.265Z" NotOnOrAfter="2015-11-11T14:51:52.265Z">
        <saml:AudienceRestriction>
          <saml:Audience>http://oasp.beta.athensams.net/OaspMetadata</saml:Audience>
        </saml:AudienceRestriction>
      </saml:Conditions>
      <saml:AuthnStatement AuthnInstant="2015-11-11T14:46:52.265Z" SessionIndex="
236bc0a578ecf2b913eeba012ecbabb8a6025acd2a36e0ecaa9717a1dc78c770">
        <saml:SubjectLocality Address="192.168.164.58" />
        <saml:AuthnContext>
          <saml:AuthnContextDeclRef>urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified</saml:
AuthnContextDeclRef>
        </saml:AuthnContext>
      </saml:AuthnStatement>
      <saml:AttributeStatement>
        <saml:Attribute Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.9" NameFormat="urn:oasis:names:tc:SAML:2.0:
attrname-format:uri">
          <saml:AttributeValue>member@domain.com</saml:AttributeValue>
          <saml:AttributeValue>student@domain.com</saml:AttributeValue>
        </saml:Attribute>
        <saml:Attribute Name="organisationNum" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
          <saml:AttributeValue>12345678</saml:AttributeValue>
        </saml:Attribute>
        <saml:Attribute Name="persistentUID" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
          <saml:AttributeValue>54df0704:0153fc5</saml:AttributeValue>
        </saml:Attribute>
        <saml:Attribute Name="identifier" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" />
        <saml:Attribute Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.7" NameFormat="urn:oasis:names:tc:SAML:2.0:
attrname-format:uri" />
        <saml:Attribute Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.10" NameFormat="urn:oasis:names:tc:SAML:2.0:
attrname-format:uri">
          <saml:AttributeValue>
            <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" NameQualifier="
https://idp.domain.com/openathens" SPNameQualifier="http://oasp.beta.athensams.net/OaspMetadata"
>2cdl3qjeeunjoh05143op7tq2r</saml:NameID>
          </saml:AttributeValue>
        </saml:Attribute>
      </saml:AttributeStatement>
    </saml:Assertion>
  </saml:EncryptedAssertion>
</samlp:Response>
```


The main elements you will be dealing with are in the 'Attribute Statement' sub-section as this will contain all the standard attributes and any extended attributes that the IdP is returning for that user. You will notice that some attributes may have multiple values:

Example AttributeStatement from a SAML assertion

```
      <saml:AttributeStatement>
         <saml:Attribute Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.9" NameFormat="urn:oasis:names:tc:SAML:2.0:
attrname-format:uri">
            <saml:AttributeValue>member@domain.com</saml:AttributeValue>
            <saml:AttributeValue>student@domain.com</saml:AttributeValue>
         </saml:Attribute>
         <saml:Attribute Name="organisationNum" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
            <saml:AttributeValue>12345678</saml:AttributeValue>
         </saml:Attribute>
         <saml:Attribute Name="persistentUID" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
            <saml:AttributeValue>54df0704:0153fc5</saml:AttributeValue>
         </saml:Attribute>
         <saml:Attribute Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.7" NameFormat="urn:oasis:names:tc:SAML:2.0:
attrname-format:uri">
            <saml:AttributeValue>This is an entitlement value</saml:AttributeValue>
            <saml:AttributeValue>This is also an entitlement value</saml:AttributeValue>
         </saml:Attribute>
         <saml:Attribute Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.10" NameFormat="urn:oasis:names:tc:SAML:2.0:
attrname-format:uri">
            <saml:AttributeValue>
               <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" NameQualifier="
https://idp.domain.com/openathens" SPNameQualifier="http://sp.domain.tld/OaspMetadata"
>2ps1fih5rvli9dcd0g5u7la9ph</saml:NameID>
            </saml:AttributeValue>
         </saml:Attribute>
      </saml:AttributeStatement>
```

User flow

1. User attempts to access a resource
2. SP asks the user where they are from
3. User tells the SP where they are from
4. SP looks up the entityID of the IdP (our own software provides organisation names and entityIDs as a value-paired list)
5. SP software uses entityID to look up the relevant part of the federation metadata that describes that organisation - mainly how and where to send a SAML request to the user's IdP
6. SP software redirects user's browser to their IdP with a signed SAML request (HTTP-REDIRECT)
7. User arrives at the IdPs login page
8. User is challenged for credentials if they have no existing session with the IdP.
    a. User journey ends here if authentication fails.
9. IdP creates a response containing relevant attributes and encodes it
10. IdP returns the user's browser to the SP with a signed SAML response (HTTP-POST)
11. SP receives the SAML response, decodes it and looks at the attributes
12. SP authorises access (or not) based on those attributes

Notes

- Steps 1 - 3 are often replaced by a WAYFless URL (one that includes the IdP's entityID).
- The IdP should be expected to send a response for authenticated users, whether or not those users should have access to the SP's content - it's up to the SP to authorise access.
- All the interaction between the SP and IdP takes place via the user's browser over http**s**
- If both the IdP and SP say in the metadata that they support encryption, then the SAML is also encrypted

More about SAML

- Wikipedia - https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language
- Oasis - https://www.oasis-open.org/standards#samlv2.0
- Interoperable SAML 2.0 Web Browser SSO deployment profile - http://saml2int.org/profile/current