OAuth & Assertions

Assertion Framework for OAuth 2.0
draft-ietf-oauth-assertions-10

SAML 2.0 Bearer Assertion Profiles for OAuth 2.0
draft-ietf-oauth-saml2-bearer-15

JSON Web Token Bearer Token Profiles for OAuth 2.0
draft-ietf-oauth-jwt-bearer-04

Brian Campbell et al.
IETF #86, March 2013
Document Status

- draft-ietf-oauth-assertions
  - Received DISCUSSes (& other comments) in IESG Evaluation and was sent back to the WG to resolve and resubmit
  - “main concern is that these documents do not sufficiently specify the functionality that is needed in order to develop an interoperable implementation”
  - There will be a lunch discussion earlier today, which is tomorrow when I’m wrote this…
- draft-ietf-oauth-saml2-bearer & draft-ietf-oauth-jwt-bearer
  - Dependent on the above
  - Possibly submit together with the above once resolved
    - JWT Assertions also dependent on draft-ietf-oauth-json-web-token
Discussing DISCUSSes

- On interoperable implementations
  - Out of band (or not), out of scope
    - Keys and identifiers must be exchanged and agreed upon
    - Not a well solved problem but inappropriate to try and solve here
  - Identify and tighten language on identifiers and comparisons
  - Provide example of common case with explanatory context
Wire Examples

< Assertion IssueInstant="2010-10-01T20:07:34.619Z" Version="2.0"
ID="ef1xsbZxPV2oqjd7HTLRLIBb7" xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
  < Issuer >https://saml-idp.example.com</ Issuer >
  < Subject >
    < NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">brian@example.com</NameID>
    < SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
      < SubjectConfirmationData NotOnOrAfter="2010-10-01T20:12:34.619Z" Recipient="https://authz.example.net/token.oauth2" />
    </ SubjectConfirmationData >
  </ Subject >
  < Conditions >
    < AudienceRestriction >
      < Audience >https://saml-sp.example.net</ Audience >
    </ AudienceRestriction >
  </ Conditions >
  < AuthnStatement >
    < AuthnInstant >2010-10-01T20:07:34.371Z</ AuthnInstant >
    < AuthnContext >
      < AuthnContextClassRef >urn:oasis:names:tc:SAML:2.0:ac:classes:X509</ AuthnContextClassRef >
    </ AuthnContext >
  </ AuthnStatement >
</ Assertion >

{
  "iss": "https://idp.example.com",
  "exp": 1357255788,
  "aud": "https://sp.example.org",
  "jti": "tmvY2x.LvN72B5Q_EacH._5A",
  "acr": "2",
  "sub": "Brian"
}