draft-ietf-abfab-aaa-saml

- Main issue
  - Mapping/binding between SAML names and AAA names
  - When policy is applied based on SAML names
  - Preliminar proposal based on:
    - Definition of two RoleDescriptorTypes: *RADIUSIDPDescriptor* and *RADIUSRPDescriptor*
    - Definition of a RADIUS URI scheme (this might need to be avoided according to Sam’s comment)

draft-ietf-abfab-aaa-saml

- Other relevant issues
  - Include a nomenclature table at the beggining for non ABFAB readers (Done)
  - Change SAML-Message → SAML-Protocol (Jim will do)
  - Are domain-only NAI representations allowed in the *Network Access Identifier Name Identifier Format*? (ask Rhys)
  - Should section 6.1 Confirmation Method identifiers also refer to the ones in section 8.1? (ask Scott or any other SAML expert)

draft-ietf-abfab-aaa-saml

- <RADIUSIDPDescriptor> Element
  - Extends RoleDescriptorType
  - Includes the <RADIUSIDPService> Element
    - Zero or more elements of type EndpointType
    - Binding = urn:ietf:params:abfab:bindngs:radius
    - Location = URI naming the AAA IDP entity
- <RADIUSRPDescriptor> Element
  - Extends RoleDescriptorType
  - Includes the <RADIUSRPService> Element
    - Zero or more elements of type EndpointType
    - Binding = urn:ietf:params:abfab:bindngs:radius
    - Location = URI naming the AAA RP entity

draft-ietf-abfab-aaa-saml

- Need a URI representation for AAA names
- RP
  - «radius:rp:nas-ip-address:{ip_address}»
  - «radius:rp:nas-identifier:{identifier}»
  - «radius:rp:gss-eap:{gss_eap_identifier}»
- IDP
  - «radius:idp:{nai_realm}»

draft-ietf-abfab-aaa-saml

- Example RP metadata

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
                  entityID="https://IdentityProvider.com/SAML">
    <RADIUSIDPDescriptor protocolSupportEnumeration=
                         "urn:oasis:names:tc:SAML:2.0:protocol">
        <RADIUSIDPService
            Binding="urn:ietf:params:abfab:bindings:radius"
            Location="radius:idp:idp.com"/>
    </RADIUSIDPDescriptor>
</EntityDescriptor>
```

draft-ietf-abfab-aaa-saml

- Example IDP metadata

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
                  entityID="https://RelyingParty.com/SAML">
      <RADIUSRPDescriptor protocolSupportEnumeration=
                          "urn:oasis:names:tc:SAML:2.0:protocol">
         <RADIUSRPService
            Binding="urn:ietf:params:abfab:bindings:radius"
            Location="radius:rp:gss-eap:nfs%2Ffileserver.rp.com
%40rp.com"/>
      </RADIUSRPDescriptor>
   </EntityDescriptor>
```