Session 2.2: Federations: Implementations

Scott Koranda

Support provided by the
National Institute of Allergy and Infectious Diseases

Scott Koranda's participation has been funded in whole or in part with federal funds from the National Institute of Allergy and Infectious Diseases (NIAID), National Institutes of Health (NIH), under Contract Nos. HHSN316201200160W/D14PD00002 & D13PD01160. The content of this presentation does not necessarily reflect the views or policies of the Department of Health and Human Services, nor does mention of trade names, commercial products, or organizations imply endorsement by the U.S. Government.

SAML Metadata

Why should an IdP and SP interoperate?

Why should an IdP accept an authentication request from an SP?

Why should an IdP authenticate a user and then assert details about that event and identity information to the SP?

Why should an SP trust an assertion about a user sent to it from an IdP?

Trust

- IdP maintains a "list" of trusted relying parties (SPs)
  - Only accept authentication requests from trusted SPs
  - Only send assertions to URLs for SPs that it trusts
  - Should sign/encrypt assertion/response so only the trusted SP can decrypt and consume
- SP maintains a "list" of trusted relying parties (IdPs)
  - Only send authentication requests to trusted IdPs
  - Only send authentication requests to URLs for IdPs that it trusts
  - Only accepts signed/encrypted assertion/response from IdPs that it trusts

SAML Metadata Establishes Trust

- XML description of the SAML entity
  - entityID
  - SAML role (IdP or SP)
  - URL endpoints for consuming SAML messages
  - signing/encryption public key material
  - organization information including contacts

```
<EntityDescriptor entityID="https://idp.ncsa.illinois.edu/idp/shibboleth">
  <IDPSSODescriptor errorURL="https://idp.ncsa.illinois.edu/error" protocolSupportEnumeration="...">
    <Extensions>
      <shibmd:Scope regexp="false">ncsa.illinois.edu</shibmd:Scope>
      <mdui:UIInfo>
        <mdui:DisplayName xml:lang="en">National Center for Supercomputing Applications</mdui:DisplayName>
        <mdui:Description xml:lang="en">National Center for Supercomputing Applications</mdui:Description>
        <mdui:PrivacyStatementURL xml:lang="en">...</mdui:PrivacyStatementURL>
        <mdui:Logo height="100" width="148" xml:lang="en">...</mdui:Logo>
      </mdui:UIInfo>
    </Extensions>
    <KeyDescriptor use="signing">SNIP</KeyDescriptor>
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
                         Location="https://idp.ncsa.illinois.edu/idp/profile/SAML2/Redirect/SSO"/>
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                         Location="https://idp.ncsa.illinois.edu/idp/profile/SAML2/POST/SSO"/>
  </IDPSSODescriptor>
  <Organization>SNIP</Organization>
  <ContactPerson>SNIP</ContactPerson>
</EntityDescriptor>
```

```
<EntityDescriptor entityID="https://cilogon.org/shibboleth">
  <SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <Extensions>...</Extensions>
    <KeyDescriptor>SNIP</KeyDescriptor>
    <AssertionConsumerService
           Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
           Location="https://cilogon.org/Shibboleth.sso/SAML2/POST"/>
    <AttributeConsumingService index="1">
      <ServiceName xml:lang="en">CILogon</ServiceName>
      <ServiceDescription xml:lang="en">...</ServiceDescription>
      <RequestedAttribute FriendlyName="displayName" Name="urn:oid:2.16.840.1.113730.3.1.241"
                          NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
      <RequestedAttribute FriendlyName="eduPersonPrincipalName" Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
                          NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
           <RequestedAttribute FriendlyName="mail" Name="urn:oid:0.9.2342.19200300.100.1.3"
                          NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
    </AttributeConsumingService>
  </SPSSODescriptor>
  <Organization>...</Organization>
  <ContactPerson>...</ContactPerson>
</EntityDescriptor>
```

```
    <KeyDescriptor use="signing">
      <ds:KeyInfo>
        <ds:X509Data>
          <ds:X509Certificate>
MIIDITCCAgmgAwIBAgIJAKu+jRod+TYIMA0GCSqGSIb3DQEBBQUAMCkxJzAlBgNV
BAMTHndlYmF1dGguc2VydmljZS5vaGlvLXN0YXRlLmVkdTAeFw0xMDAyMDkyMDA3
MzdaFw0zMDAyMDQyMDA3MzdaMCkxJzAlBgNVBAMTHndlYmF1dGguc2VydmljZS5v
aGlvLXN0YXRlLmVkdTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMpZ
P+xV7kNCuuUtg4X8MTxTnS2TSU/tompvYjI0af4q7N5od7uzEqHBD9FMvh9bZ7GS
CACX5yYjBYZCb59i0tstfpCsDBho2Wi497EjmaTw81EQ1AjM6EhRb/we0MLj0er8
8q+vnVC7Jb7DoStoNIEFoOTv8LvKldrrXVX3yHZR3bEVtvblZbGMSYtPdH/TYMDQ
cmqkpzldfz9rQFDLSM8mqBqf56zmB8uzkZKhujTXOzb4STvaq7hhAnDwT3z9c00O
XbDBWxd1CplgHwZvrbWxYxf5gTCaPvHuLY5WeA8Ky5SUZifO/szEDvEm8K0rHStK
H/blQiX5fUQ6t3SfxbsCAwEAAaNMMEowKQYDVR0RBCIwIIIed2ViYXV0aC5zZXJ2
aWNlLm9oaW8tc3RhdGUuZWR1MB0GA1UdDgQWBBR70C49vjOa/Ikk86hkX998wqQt
UDANBgkqhkiG9w0BAQUFAAOCAQEAlgMMaTIwrly4U896lUa92iif3bLGADPjc0Is
6a6k6RytjJm/r0lbtjCWW6zs1T6L7458Ow+57fyF0Oh/iXvj65m+dvCBWXnag7hN
1yMBJQMRpSjH7dLko7y0EJ/ZrKEYQwYnBGmCILvJB/MIj2eEkq2Z47uWpvrehJfb
zsEeAbjNqw1V/AJN7E4paw8aYg8TXEXAdOvNL5h7KRQw8Ui0kCw2DeTTIXExSxZd
bqw6ldfQD2fVYnLxDGTFqITCi1a9TidA4xCXD95F7uQaEao3O8ArZcyag62uiMtv
i24RvCRvD/vsnUhI82pV/DK+2icz6UDtiiKrFNAmIiR14TanfA==
          </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </KeyDescriptor>
```

Higher Ed & Research SAML Trust Model

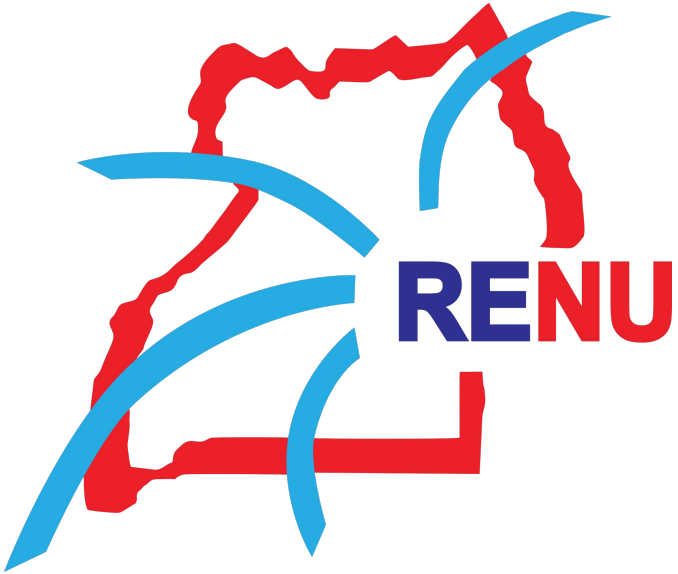
- Explicit Key Trust Model
- IdP/SP explicitly trusts the "keys" it finds in SAML metadata
  - Keys used for digital signing and/or encryption
- Keys obtained from X.509 digital certificates
  - X.509 certs contain a lot of information in addition to keys
  - Only the keys are used! (Mostly)
  - So X.509 certs do NOT need to be part of a public key infrastructure
  - No "well known" certificate authority needs to issue the certificate
- **Self-signed X.509 digital certificates preferred for higher ed & research SAML**

SAML Federations

The Role of Federations

- Enable us to scale up to 1000s of IdPs and SPs
- Publish digitally signed SAML metadata containing public keys, endpoint URLs, and other info about IdPs and SPs
- Set standards for SAML attributes, levels of assurance, etc.
- Provide support and training

RENU Identity Federation



Federation SAML Metadata

- RENU Identity Federation (RIF) SAML Metadata available at

  https://rif.renu.ac.ug/rr/signedmetadata/federation/RIF/metadata.xml

RENU SAML Federation Trust Model

- SAML metadata bootstraps the trust
- Trust federation operators to only let in "good" metadata
- Each entity (IdP or SP) consumes the metadata and has details for all other entities necessary for interoperability
- Before consuming metadata each entity **must** verify it is *properly signed* by federation operator and *still valid*
- TLS is **not** a substitute for verifying signature on metadata