SAML-EC Status

Scott Cantor
cantor.2@osu.edu

Status of Drafts

- draft-ietf-kitten-sasl-saml-ec-04 uploaded
  - proposed "final" text on naming and keying
- OASIS ECP 2.0 and Channel Binding drafts nominally ready for standardization at OASIS
- NCSA has prototype using SSH as a test case

Naming

- Trying to deal with federation reality
  - name at RP != name at IdP != name in token
- Not specifying new name types at present
- Require GSS_C_NT_USER_NAME initiator name at completion based on <NameID> in assertion
  - name!Format!NameQualifier!SPNameQualifier

Session Keys

- Structurally: define some XML local to the draft for carrying the information inside assertions or SOAP headers
- Practically: allow for key agreement protocols, but specify a fall-back of the IdP generating a key and sending to both parties

IdP Generated Key

- Reuse 3961 enctypes
- Generate the protocol key directly and pass in encrypted assertion and SOAP header

```
<samlec:SessionKey>
    <samlec:GeneratedKey Algorithm="aes128-cts-hmac-sha1-96">
    b64(key)
    </samlec:GeneratedKey>
</samlec:SessionKey>
```

- Is more complexity required to turn the input material into a 4121 protocol key?