SAML-EC Status

Scott Cantor
cantor.2@osu.edu

Status of Drafts

- draft-ietf-kitten-sasl-saml-ec-01 uploaded in February with minor changes
- OASIS ECP 2.0 and Channel Binding left as working drafts for now
- NCSA implementing prototype against I-D using SSH as a test case

Known Open Issues

- SAML / GSS naming
- Per-message tokens and PRF

Naming

- Non-EC SAML mechanism (apparently) avoids standardization of initiator name through unspecified SP/mechanism interaction
- SP is “part of” EC mechanism, so need mechanism name type for SAML assertion subjects (<NameID>)
- Need link to draft-ietf-abfab-gss-eap-naming for standardization of GSS name attributes

Crypto Additions

- Provisioning of a key for per-msg tokens and PRF in bearer and holder of key cases
- Latter probably algorithm-dependent, probably reuse key derivation specified by XML Encryption