Kitten WG: SAML-EC Status

- draft-cantor-ietf-kitten-saml-ec-01.txt
- Rebase ECP adaptation on V2.0 of profile:
    - http://wiki.oasis-open.org/security/SAML2EnhancedClientProfile
    - http://wiki.oasis-open.org/security/SAML2ChannelBindingExt
- Adds channel binding and “holder of key” support

Channel Binding

- Offloads CB verification to IdP
- RP includes CB in SAML request (via extension), signs it
- Client includes CB in SOAP header attached to Client->IdP leg
- IdP verifies signature from RP, compares CB in SAML request to CB in SOAP header

Channel Binding

- Current SAML construct captures the CB type and data directly
- Needs to be extended to carry application-specific CB data

Holder of Key

- ECP 2.0 adds support for binding issued SAML token to a client key
- Assymmetric or symmetric, could be generated by client or IdP in-band
- Proof of possession via TLS or a message signature (latter more effective with channel binding, obviously)
- Might allow support for integrity / confidentiality at GSS layer in future rev