NTT

NTT Information Sharing Platform Laboratories
NTT 情報流通プラットフォーム研究所

Proxying Assurance Between OpenID & SAML

Paul Madsen, NTT

RSA Conference 2009

NTT

Protocol Mash-ups

- More and more, the various identity protocols are being (or contemplated) deployed in combinations
- OpenID, SAML, Infocards, ID-WSF, Oauth, WS-Federation, etc
- Protocols not generally designed on the assumption of being deployed in combination
- Consequently, policy impedance possible at the joins
- We examine such impedance issues for assurance between OpenID & SAML

NTT

Assurance

- Assurance refers to the degree of confidence a Relying Party can ascribe to the assertions/claims of an IdP
- Assurance determined by a combination of legal, business, technical, and procedural factors
- Assurance frameworks (e.g. NIST 800 63, etc) quantify levels of assurance by stipulating the technical and procedural aspects to be followed by federated partners for each level
- Typically 3-4 levels defined, ranging from low to high
- Federation actors can refer to the more manageable LOA rather than the constituent factors

NTT

OpenID & Assurance

- OpenID Provider Authentication Policy Extension (PAPE)
- Defines an extension to core OpenID protocol by which RP/OPs can 'discuss' the nature of the authentication
- PAPE standardizes 3 URIs
  - Multi-factor
  - Multi-factor Hard token
  - Phishing Resistant
- Also allows OPs to indicate assurance in terms of NIST 800 63 levels

NTT

SAML & Assurance

- SAML allows IDP/SP to indicate assurance policy on SSO messages wrt
  - Identity proofing (e.g. Email verification or f2f)
  - Security processes (e.g. Key storage)
  - Authentication specifics (e.g. Biometric or OTP)
- Set of related mechanisms referred to as 'Authentication Context'
- Authentication Context 'classes' capture common combinations of above aspects - SSTC defined a number, e.g. 'mobile-no contract' class
- New classes can be defined by other some communities (not without some difficulty)

NTT

Motivating Use Cases

- PAPE & SAML AC, while logically similar, are not perfectly compatible
- Consider the following use cases that hilite the need for mapping assurance between SAML & OpenID
  - Use Case #1 – SAML SP starts
  - Use Case #2 – OpenID RP starts

NTT

Use Case #1 – SAML SP Starts

- A SAML IDP provides strong authentication services to a community of RPs
- The SAML IDP wants to focus on strong authentication, and to outsource low assurance requests to OPs through OpenID
- Value
  - For SAML IDP, can focus on (high-margin) strong authentication
  - For SAML RPs, can leverage their existing IDP relationship to mediate those with Ops
  - For OpenID OPs, (indirect) access to those erstwhile exclusively SAML RPs

NTT

Use Case #2 – OpenID RP Starts

- An OpenID OP provides low assurance password-based SSO to community of Rps
- OP does not itself support higher assurance authentication mechanisms
- For OpenID RPs that require higher assurance, the OP will proxy relevant authentication requests through SAML SSO to an IDP capable of meeting those higher assurance requirements
- Value
  - For OpenID RPs, (indirectly) access higher assurance IDPs without necessarily establishing relationships with SAML IDPs or supporting SAML

NTT

Issues

- PAPE does not define a password URI
- SAML does not (yet) define how to bind the NIST 800 63 assurance levels to AuthnContext
- Can we presume that the two protocols are equivalent with respect to LoA? And therefore we need not distinguish when mapping assurance to/fro?
  - Arguably so for OpenID & SAML Web SSO. What of ECP?

NTT

Summary

- Federation protocols like SAML & OpenID may be deployed in combination
- Federated identity requires assurance information to flow along with identity information for anything but trivial applications
- 'Policy interoperability' requires that assurance policy can persist across the boundaries between protocols
- Please join NRI, NTT, & Oracle at our workshop pod to see these use cases demonstrated.