Shibboleth 2.0: New Stuff

Spring Internet2 Member Meeting -- 2008
Identity Provider

- Servlet engine connecting core enterprise integration functionality to protocol-specific encoding and messaging plugins
- Internal or external authentication tagged with supported SAML context classes
- Only exact matching initially supported
- Explicit session management, tracks SPs and types of authentication used to allow for SSO and eventually SLO
• Attribute resolver is similar to older version, with new twists:
  • name and syntax on the wire handled by protocol-specific encoders
  • old NameMappers merged into new PrincipalConnectors and NameID encoders
  • filtering engine deals with simpler, site-specific attribute IDs rather than long, complex URI names
• ARPs transformed into a generic filtering engine for attributes:
  • Extensible boolean functors run to determine what policies to apply and then what values to keep.
  • Consequence of change from the old “list of attributes” ARP engine is that everything is resolved ahead of time, so caching is important.
• New defaults:
  • SAML 2: POST, push attributes, always encrypt assertion
  • SAML 1: same as 1.3
  • Blocks anonymous SPs (those w/o metadata)
• Rewritten to expose a “stable” API and eliminate non-portable IPC code
• Greatly reduced Apache/IIS library footprint
• Increased granularity of components so extension is simpler and more robust
• Persistence API for clustering
• Configurable SSO protocol selection
• Regular expressions in content matching and access control.
• Attribute subsystems:
  • Extractor (SAML -> AttributeDecoder)
    • XML-based ruleset
  • Decoder (SAML -> neutral form)
    • Small footprint plugin for handling XML details
  • Resolver (session state -> neutral form)
    • Encapsulates SAML queries or other data access technologies
  • Filter (neutral form -> neutral form)
Service Provider

- Local and global logout functionality
- Application hooks for monitoring/hooking logout events
- Requires significant UI customization
Discovery Service

• WAYF on steroids
• Implements OASIS Committee Specification
• SSO-protocol-independent means of selecting IdP
• Composes with SP functions for discovery and protocol selection