The Emerging JSON-Based Identity Protocol Suite

Michael B. Jones
Microsoft
May 24, 2011
Background

• Identity interop requires agreement on data representations and protocols
  – Numerous existing standards
    • Kerberos, X.509, SAML, WS-*, OpenID 2.0, etc.
  – Using a variety of data representations
    • ASN.1, XML, custom binary formats
  – None ubiquitously adopted
Emerging JSON-Based Protocol Suite

• A new suite of identity specifications emerging
  – Using JSON data representations
  – Using REST design pattern
  – Reusing lessons learned from previous efforts

• Advantage
  – JSON ubiquitously supported in browsers and modern web development tools
    • Can use tools developers have lying around the house
  – Chance for much greater reach than past efforts
    • Increasing scope of identity interop
Broad Community Effort

Google

facebook

Microsoft

OpenID

PingIdentity

JSON Spec Suite

NRI

AOL

salesforce.com

Yahoo!

Yahoo! Japan
JSON Web Token, Signature, Encryption, and Key Specifications

• JSON Web Token (JWT)
  – JSON representation of signed and optionally encrypted claims

• JSON Web Signature (JWS)
  – JSON-based signing representation

• JSON Web Encryption (JWE)
  – JSON-based encryption representation

• JSON Web Key (JWK)
  – JSON representation of set of public keys
Simple Web Discovery (SWD)

• Simple Web Discovery (SWD)
  – Discover location of a service for a principal
  – With just an HTTPS GET
  – Using simple JSON representation
OAuth 2.0 Specifications (Using JSON)

- **OAuth 2.0 Core**
  - Third party authorization protocol
- **OAuth 2.0 Bearer Tokens**
  - Using bearer tokens to access protected resources
- **JWT Bearer Profile for OAuth 2.0**
  - Using a JWT to request an access token
OpenID Connect*

• Enables simple site registration functionality
  – Like Facebook Connect with open set of providers
• Supports claims aggregation
• Works well on mobile phones
• Usable across range of security profiles
• Modular design
  – Build only the parts you need
• Underpinnings:
  – OAuth 2.0, JWT, JWS, JWE, and SWD

*Until recently, called “OpenID Artifact Binding/Connect” or “OpenID ABC”
Resources

- IETF OAuth mailing list
  - https://www.ietf.org/mailman/listinfo/oauth

- IETF Web Object Encryption and Signing (woes) mailing list
  - https://www.ietf.org/mailman/listinfo/woes

- OpenID Artifact Binding mailing list
  - http://lists.openid.net/mailman/listinfo/openid-specs-ab

- My blog
  - http://self-issued.info/