OpenID Enhanced Authentication Profile (EAP) Working Group

October 16, 2017

Michael B. Jones

Identity Standards Architect – Microsoft

OpenID

What is the EAP WG?

- Charter at http://openid.net/wg/eap/ …
- “Develop a security and privacy profile of the OpenID Connect specifications that enable users to authenticate to OpenID Providers using strong authentication specifications. The resulting profile will enable
  - use of IETF Token Binding specifications with OpenID Connect and
  - integration with FIDO relying parties and/or other strong authentication technologies.”

Two EAP Specifications

- Token Bound Authentication
  - Defines how to apply Token Binding to OpenID Connect ID Tokens
  - http://openid.net/specs/openid-connect-token-bound-authentication-1_0.html
- EAP ACR Values
  - Defines “acr” values strong authentication profiles
  - http://openid.net/specs/openid-connect-eap-acr-values-1_0.html

OpenID Token Binding Update

- IETF Token Binding specs ready for IETF last call
- OAuth Token Binding spec
  - Defines Token Binding of OAuth 2.0 access tokens, refresh tokens, and authorization codes
- Connect Token Binding spec
  - Defines Binding of OpenID Connect ID Tokens
- Refinements to phase-in logic about to occur
- Implementation available for interop testing
  - Created by Brian Campbell
  - See https://www.ietf.org/mail-archive/web/unbearable/current/msg01332.html

OpenID Two ACR Values Defined

- “phr” – Phishing-Resistant
  - An authentication mechanism where a party potentially under the control of the Relying Party cannot gain sufficient information to be able to successfully authenticate to the End User's OpenID Provider as if that party were the End User.
- “phrh” – Phishing-Resistant Hardware Protected
  - An authentication mechanism meeting the requirements for phishing-resistant authentication above in which additionally information needed to be able to successfully authenticate to the End User's OpenID Provider as if that party were the End User is held in a hardware-protected device or component.
- Phishing-Resistant definition based on 2008 OpenID Provider Authentication Policy Extension (PAPE) spec

Status

- Working group active
  - Chairs Mike Jones and Brian Campbell
- Calls scheduled every two weeks on Thursdays
- For more info see the working group page
  - http://openid.net/wg/eap/