OpenID Enhanced Authentication Profile (EAP) Working Group

May 14, 2019

Dr. Michael B. Jones

Identity Standards Architect – Microsoft

What is the EAP WG?

- Working group description at https://openid.net/wg/eap/
- Chartered to:
  - "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
  - https://openid.net/specs/openid-connect-token-bound-authentication-1_0.html
- EAP ACR Values
  - Defines “acr” values strong authentication profiles
  - https://openid.net/specs/openid-connect-eap-acr-values-1_0.html

Token Binding Update

- IETF Token Binding specs became RFCs in October 2018
- OAuth Token Binding spec
  - https://tools.ietf.org/html/draft-ietf-oauth-token-binding
  - Defines Token Binding of OAuth 2.0 access tokens, refresh tokens, authorization codes, JWT authorization grants, and JWT client authentication
- OpenID Connect Token Binding spec
  - https://openid.net/specs/openid-connect-token-bound-authentication-1_0.html
  - Defines Binding of OpenID Connect ID Tokens
- Adoption slowed due to Chrome's removal of Token Binding

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) specification

Status

- Both drafts currently undergoing Implementer's Draft review
  - See https://openid.net/2019/04/22/public-review-period-for-two-proposed-eap-implementers-drafts/
- Working group active
  - Chairs Brian Campbell and Mike Jones
- Calls scheduled every two weeks on Thursdays
- For more information, see the working group page
  - https://openid.net/wg/eap/