OpenID Enhanced Authentication Profile (EAP) Working Group

December 9, 2021

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
- Both became Implementer's Drafts 2019

Token Binding Update

- IETF Token Binding specs became RFCs in October 2018
  - Token Binding adoption stalled due to Chrome's removal
- 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
- ***Spec work currently on hold, pending adoption progress***

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
  - https://openid.net/specs/openid-provider-authentication-policy-extension-1_0.html

Recently also defined "pop" AMR Value

- RFC 8176 defines Authentication Method Reference (AMR) values
- New AMR value motivated by WebAuthn & FIDO use cases
  - "pop" – Authentication using a Proof-of-Possession Key
  - All WebAuthn/FIDO authenticators fulfill its requirements
- Complements these existing RFC AMR values
  - "hwk" – hardware-backed PoP key
  - "swk" – software-backed PoP key

Status

- Working group chairs are Brian Campbell and Mike Jones
- Likely time for second Implementer's Draft of ACR/AMR spec
- For more information, see the working group page
  - https://openid.net/wg/eap/