1) Working Group Name

Enhanced Authentication Profile (EAP) for OpenID Connect

2) Purpose

The purpose of this working group is 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.

3) Scope

- Develop a set of applicable use cases and requirements that are specific enough to guide the profiling design work, considering interrelations with risk mitigation and user experience efforts.
- Define a profile of OpenID Connect for requesting and reporting the use of strong authentication and/or token binding.
- Specify the way that token binding is used with OpenID Connect.
- Promote progressive harmonization with existing specifications and protocols, as appropriate.
- The specification is to be based on OpenID Connect, OAuth 2.0, JWT, JOSE, FIDO, and other related OpenID Foundation, IETF, W3C, and FIDO Alliance specifications.

The following efforts are out of scope:

- Development existing and future FIDO protocols and specifications.
- Development of new extensions or technical specifications beyond adding new values to existing data structures.

All items not expressly mentioned as in scope or out of scope are to be determined by the Working Group.

4) Proposed Specifications

The following layered specifications will be produced, with precise specification names and boundaries subject to change:

- Enhanced Authentication Profile for OpenID Connect.

5) Anticipated audience or users

The anticipated audience for the documents produced by this Working Group includes developers, deployers, and designers of online services and network devices that act on behalf of

individuals using strong authentication services. The group also anticipates gathering input from individual users of online services in order to respond to their needs and preferences.

6) Language

Work will be conducted in English.

7) Method of work

E-mail discussions on the working group mailing list, regular working group conference calls, and opportunistic face-to-face meetings when a significant number of active members are co-located.

8) Basis for determining when the work is completed

The work will be considered complete once it is apparent that maximal consensus on the drafts has been achieved, consistent with the purpose and scope of the charter, and interoperability with at least two independently developed implementations of software based on the profiles has been demonstrated.

Background information

The working group intends to expedite the process of gathering stakeholder representatives to collaborate in the development of profiles to support secure and privacy enhancing online authentication, authorization, and consent when accessing public sector and/or other high value private sector services.

Related work and liaison relationships

This Working Group has a number of dependencies on, and shared goals with, the output of these other efforts:

- IETF JavaScript Object Signing and Encryption (JOSE) Working Group
- IETF OAuth Working Group
- IETF Token Binding Working Group
- OpenID Foundation OpenID Connect Working Group
- OpenID Foundation MODRNA Working Group
- OpenID Foundation HEART Working Group
- OpenID Foundation iGov Working Group
- FIDO UAF, U2F and FIDO 2.0 Working Groups
- W3C Web Authentication Working Group (proposed)

Proposers

- Anthony Nadalin, Microsoft
- Michael B. Jones, Microsoft

- John Bradley, Ping Identity
- Nat Sakimura, Nomura Research Institute
- Torsten Lodderstedt, Deutsche Telekom
- Adam Dawes, Google

Proposed Timelines

This Working Group will target producing use cases and requirements within 2 months of inception in order to guide its design effort, and will target 6-12 months overall to develop a V1.0 set of profiles and other auxiliary materials, facilitating the development of multiple independent draft implementations during this time. The following are suggested initial milestones for consideration by the Working Group:

- November 2015: Approval of Working Group creation.
- June 2016 Approve Implementer's drafts (within 12 months after formal kickoff of WG).
- Interop testing among multiple implementations (once Implementer's Drafts are available).
- December 2016 Approve Final profiles (6-12 months after Implementer's Drafts)