Upcoming specifications from the OpenID Foundation

Henrik Biering[1] · Axel Nennker[2]

[1] Peercraft, Lergravsvej 53, 2300 Copenhagen S, Denmark,
hb@peercraft.com

[2] Telekom Innovation Laboratories, Winterfeldtstr. 21, 10781 Berlin, Germany.
axel.nennker@telekom.de

Abstract: The OpenID Foundation (OIDF), is an international non-profit organization of individuals and companies committed to enabling, promoting and protecting OpenID technologies. Currently OIDF is finalizing the third generation of OpenID Single Sign-On protocols under the brand name ”OpenID Connect”. In parallel with this effort OIDF has also launched Working Groups for solving other problems that arise when users interact with an ecosystem of interoperable service providers rather than a single service provider.

The presentation will cover the status, features, and benefits of OpenID Connect, Account Chooser, and the Backplane Protocol supplemented by feedback collected from various stakeholder groups.

1 Introduction

Formed in June 2007, the OpenID Foundation (“OIDF”) serves as a public trust organization representing the open community of developers, vendors, and users. OIDF assists the community by providing standards and support for internet scale identity management and related technologies. This also entails managing intellectual property and brand marks as well as fostering viral growth and global participation in the proliferation of OpenID.

Currently OIDF is finalizing the third generation of OpenID Single Sign-On protocols under the brand name ”OpenID Connect”. In parallel with this effort OIDF has also launched the Account Chooser Working Group for solving the usability problems arising when a relying party supports multiple identity providers, and the Backplane Working Group which deals with the problems that arise when users interact with an ecosystem of interoperable service providers rather than a single service provider.

2 OpenID Connect

OpenID Connect is a suite of lightweight specifications that provide a framework for identity interactions via REST like APIs. A specific goal for OpenID Connect has been

to make it as easy as possible for relying parties to implement OpenID. The simplest deployment of OpenID Connect allows for clients of all types including browser-based, mobile, and JavaScript clients, to request and receive information about identities and currently authenticated sessions [Sa13a] [Sa13b]. The specification suite is extensible, allowing participants to optionally support more advanced features and encryption of identity data [Sa13e] [Sa13f], provider and user discovery [Sa13c], dynamic client registration [Sa13d], and advanced session management, including logout [Sa13g].

OpenID Connect performs many of the same tasks as OpenID 2.0, but does so in a way that is API-friendly. OpenID Connect also includes more robust mechanisms for signing and encryption allowing OpenID Connect to be used in scenarios requiring higher levels of assurance. Integration of OAuth 1.0a and OpenID 2.0 required an extension (the OpenID/OAuth hybrid). Being based directly on OAuth 2.0, OAuth capabilities are inherently built into OpenID Connect.

Additionally OpenID Connect supports propagation of both distributed and aggregated claims, and specifies a ”self-issued” mode allowing a user to host his/her own Identity Provider while still being able to present trusted third-party claims to service providers.

3 Account Chooser

Account Chooser is a technique to improve the user experience for logging into a website. It produces a uniform and standardized UI to handle the use cases where a device is used by different users, where a single user has more profiles on a particular website, and in particular it solves the ”Nascar Problem” [Me09] occurring when a new user wants to sign up at service provider supporting a large number of identity providers.

The Account Chooser will be implemented as a central service operated by OIDF at accountchooser.com, but may also be implemented locally by a service provider. Each method has its own distinct advantages and disadvantages.

The model is protocol agnostic and may in some cases improve usability on a website even if it does not support identity providers, or a website that only supports a single identity provider.

4 Backplane Protocol

Many websites on the Internet embed JavaScript applications into their web pages to provide social functionality such as single sign-on, commenting, sharing, polling, and chatting. As such applications are often developed and hosted by different vendors, they are effectively silos that cannot communicate with each other. This presents a significant problem because the user experience is disjointed and broken, which forces website operators to invest time and money to integrate these services through proprietary APIs.

The Backplane Protocol is a proposed open standard to solve this problem. Backplane Protocol is a secure framework for interaction between multiple, independent client- and server-side parties in the context of a browser session. The Backplane Protocol lets trusted applications share information. When placed together on a web page, Backplane-enabled applications share user identity and other information, seamlessly, regardless of their source. In essence, Backplane Protocol defines a message distribution system where messages are delivered securely, reliably, in order, and in real-time. When a user takes action in one app, the other apps will get the news using the Backplane Protocol.

5 Participation and timeline

The vast majority of OIDF's work is done in the Working Groups. A working group is focused on a specific problem, technology, or opportunity for which the members will deliver a document or series of documents, after which they may disband or create a revised charter for further work. The completion of a working group charter and subsequent disbanding of the group are viewed as a sign of success.

Membership of the Foundation is not required to participate in a working group but participants must agree to the IPR Policy by executing a Contribution Agreement and subscribe to the groups' mailing list. This allows anyone to participate in technology development while ensuring that the specifications remain freely implementable by anyone.

Each working group has one or more editors and a charter that the group is supposed to follow. When a specification is considered complete, an approvals process is initiated. First a review period followed by a vote among the OIDF members is conducted to approve an ”Implementer's Draft” version of the specification. When sufficient feedback has been gathered and processed, a second review and vote is conducted to approve the specification as an official OIDF standard.

The OpenID Connect specification is presently entering the implementers draft review period and is expected to enter the final review period by fall 2013.

6 General Feedback

OpenID Connect has technically been designed to work in a variety of environments requiring different levels of security, identity assurance, and privacy. The Account Chooser proposal is expected to facilitate a smoother transition from local login to login via one or more identity providers.

Hence OIDF is currently soliciting feedback from both developer and business communities to determine how the new features of OpenID Connect and Account Chooser can be promoted to overcome the scepticism associated with current alternatives to local login, such as the previous OpenID versions, current government issued ID's, Facebook Connect, and various federation solutions.

References

[Sa13a] Sakimura, N.; Bradley, J.; Jones, M.; Medeiros, B.; Mortimore, C.: *OpenID Connect Basic Client Profile 1.0*, http://openid.net/specs/openid-connect-basic-1_0.html, 2013.

[Sa13b] Sakimura, N.; Bradley, J.; Jones, M.; Medeiros, B.; Mortimore, C.; Jay, E.: *OpenID Connect Implicit Client Profile 1.0*, http://openid.net/specs/openid-connect-implicit-1_0.html, 2013.

[Sa13c] Sakimura, N.; Bradley, J.; Jones, M.; Jay, E: *OpenID Connect Discovery 1.0*, http://openid.net/specs/openid-connect-discovery-1_0.html, 2013.

[Sa13d] Sakimura, N.; Bradley, J.; Jones, M.: *OpenID Connect Dynamic Client Registration 1.0*, http://openid.net/specs/openid-connect-registration-1_0.html, 2013.

[Sa13e] Sakimura, N.; Bradley, J.; Jones, M.; Medeiros, B.; Jay, E.: *OpenID Connect Standard 1.0*, http://openid.net/specs/openid-connect-standard-1_0.html, 2013.

[Sa13f] Sakimura, N.; Bradley, J.; Jones, M.; Medeiros, B.; Mortimore, C.; Jay, E.: *OpenID Connect Messages 1.0*, http://openid.net/specs/openid-connect-messages-1_0.html, 2013.

[Sa13g] Sakimura, N.; Bradley, J.; Jones, M.; Medeiros, B.; Agarwal, N.: *OpenID Connect Session Management 1.0*, http://openid.net/specs/openid-connect-session-1_0.html, 2013.

[Me09] Messina, C.: *Does OpenID need to be hard?*, http://factoryjoe.com/blog/2009/04/06/does-openid-need-to-be-hard/, 2009