Home » Welcome to OpenID Connect » OpenID Connect FAQ and Q&As

OpenID Connect FAQ and Q&As

What is OpenID Connect? How does it work?

OpenID Connect is an interoperable authentication protocol based on the OAuth 2.0 family of specifications. It uses straightforward REST/JSON message flows with a design goal of “making simple things simple and complicated things possible”. It’s uniquely easy for developers to integrate, compared to any preceding Identity protocol.

OpenID Connect lets developers authenticate their users across websites and apps without having to own and manage password files. For the app builder, it provides a secure verifiable, answer to the question: “What is the identity of the person currently using the browser or native app that is connected to me?”

OpenID Connect allows for clients of all types, including browser-based JavaScript and native mobile apps, to launch sign-in flows and receive verifiable assertions about the identity of signed-in users.

(Identity, Authentication) + OAuth 2.0 = OpenID Connect

Search for:

Search

News Archives

News Archives

Select Month

Categories

Categories

Select Category

Recent Posts

- Notice of Vote for Implementer’s Drafts of Two iGov Specifications
- Five HEART Implementer’s Drafts Approved
- Relying Party OpenID Certification Entering Production Phase
- FAPI Part 2 Implementer’s Draft Approved
- Public Review Period for Two iGov

http://www.youtube.com/watch?feature=player_embedded&v=Kb56GzQ2pSk or
kimura.org/2013/07/05/identity-authentication-oauth-openid-connect/

What problem does OpenID Connect solve?

It lets app and site developers authenticate users without taking on the responsibility of storing and managing passwords in the face of an Internet that is well-populated with people trying to compromise your users' accounts for their own gain.

What does authentication mean?

The process of establishing and communicating that the person operating a browser or native app is who they claim to be.

What is OAuth 2.0 and how does it related to OpenID Connect?

OAuth 2.0, is a framework, specified by the IETF in RFCs 6749 and 6750 (published in 2012) designed to support the development of authentication and authorization protocols. It provides a variety of standardized message flows based on JSON and HTTP; OpenID Connect uses these to provide Identity services.

What is the status of OpenID Connect?

Final OpenID Connect specifications were launched on February 26, 2014. The certification program for OpenID Connect was launched on April 22, 2015. Google, Microsoft, Ping Identity, ForgeRock, Nomura Research Institute, and PayPal OpenID Connect deployments were the first to self-certify conformance.

Are there live production deployments of OpenID Connect?

Yes. Some examples include Google, Gakunin (Japanese Universities Network), Microsoft, Ping Identity, Nikkei Newspaper, Tokyu Corporation, mixi, Yahoo! Japan and Softbank. There are also mature deployments underway by Working Group participant organizations, such as Deutsche Telecom, AOL, and Salesforce.

For an example of OpenID Connect at work, look at Google+ Sign-In, Google's flagship social-identity offering, which is entirely based on OpenID Connect.

Where can I find code implementing OpenID Connect?

The Libraries page lists libraries in a number of different languages that implement OpenID Connect and related specifications.

Where can I find more information on OpenID Connect?

The OpenID Foundation and OpenID Connect sites are a good place to start. Also, the Working Group leaders' blog sites are helpful: Mike Jones, Nat Sakimura, and John Bradley.

Tags

Account Chooser adoption board election board elections Certification code community connect developers Don Thibeau drummond reed election Errata events FAPI Final Specification Foundation google government HEART iGov Implementer's Draft information card foundation interop microsoft MODRNA myspace oidf openid OpenID Connect openiddevcamp OpenYOLO pape Public Review relying party research retail advisory committee security sourceforge spec specification summit usability user experience vote

s the history of OpenID?

OpenID Connect is the third generation of OpenID technology. The first was the original OpenID, a visionary's tool that never got much commercial adoption, but got industry leaders thinking about what was possible. OpenID 2.0 was much more fully thought through, offered excellent security, and worked well when implemented properly. However, it suffered from several design limitations – foremost among them that Relying Parties could be Web pages but not native applications; it also relied upon XML, leading to some adoption problems.

OpenID Connect's goal is to be much more developer-friendly, while expanding the set of use cases where it can be used. It has already been successful in this; there are production deployments operating at huge scale. Any programmer with sufficient experience to send and receive JSON messages over HTTP (which is most of them these days) should be able to implement OpenID Connect from scratch using standard crypto signature-verification libraries. Fortunately, most won't even have to go that far, as there are good commercial and open-source libraries that take care of the authentication mechanics.

How is OpenID Connect different from OpenID 2.0 and how does it overcome the problems experienced with OpenID 2.0?

OpenID Connect has many architectural similarities to OpenID 2.0, and in fact the protocols solve a very similar set of problems. However, OpenID 2.0 used XML and a custom message signature scheme that in practice sometimes proved difficult for developers to get right, with the effect that OpenID 2.0 implementations would sometimes mysteriously refuse to interoperate. OAuth 2.0, the substrate for OpenID Connect, outsources the necessary encryption to the Web's built-in TLS (also called HTTPS or SSL) infrastructure, which is universally implemented on both client and server platforms. OpenID Connect uses standard JSON Web Token (JWT) data structures when signatures are required. This makes OpenID Connect dramatically easier for developers to implement, and in practice has resulted in much better interoperability.

The OpenID Connect interoperability story has been proven in practice during an extended series of interoperability trials conducted by members of the OpenID Connect Working Group and the developers behind numerous OpenID Connect implementations.

What do "IDP" and "RP" stand for?

These terms are commonly used when describing digital identity systems. IDP stands for Identity Provider, a party that offers user authentication as a service. RP stands for Relying Party, an app that outsources its user authentication function to an IDP.

Who can be an IDP?

The OpenID Connect protocol's design is wide-open and deliberately aimed at encouraging an open ecosystem of IDPs. While the leading IDPs are currently large Internet services such as Google and Microsoft, OpenID Connect opens the doors for many kinds of IDPs, including people running their own IDPs on Web sites and on personal devices, such as mobile phones and tablets.

'as OpenID Connect developed?

OpenID Connect was developed in an OpenID Foundation working group. OpenID working groups are open to all who sign the IPR Contribution agreement, free of charge. A wide range of perspectives and use cases were represented in the working group discussions.

The standardization process is documented in OpenID Process and follows the terms of “Annex 3: Code of Good Practice for the Preparation, Adoption and Application of Standards” of WTO TBT Agreement.

What people and/or companies were involved in the development of OpenID Connect?

Contributors included a diverse international representation of industry, academia and independent technology leaders: AOL, Deutsche Telekom, Facebook, Google, Microsoft, Mitre Corporation, mixi, Nomura Research Institute, Orange, PayPal, Ping Identity, Salesforce, Yahoo! Japan, among other individuals and organizations.

Is a certification or registration process required to be able to implement OpenID Connect?

OpenID Connect can be freely used by anyone. The developers of OpenID Connect assert no intellectual-property claims on it.

How were the OpenID Connect specs tested while they were being developed?

Five rounds of interoperability testing have been conducted as the specifications evolved in which implementations were tested against one another. This process identified any deficiencies and ambiguities in the specs, enabling them to be addressed before the specs became final. This also verified that implementations will work well together.

Why should developers use OpenID Connect?

Because it’s easy, reliable, secure, and lets them get out of the difficult and dangerous business of storing and managing other people’s passwords. There is the added benefit that it also make users’ lives easier during sign-up and registration thus reducing site abandonment.

Does OpenID Connect work for native and mobile apps?

Yes. There are already system-level APIs built into the Android operating system to provide OpenID Connect services. OpenID Connect can also accessed by interacting with the built-in system browser on mobile and desktop platforms; a variety of libraries are under construction to simplify this process.

Why should network operators care about

D Connect?

Simply stated, there is a significant increase of online services being accessed via mobile devices and there is an increase in online identity thefts. The GSMA has articulated the business case for Mobile Network Operators (MNOs) http://www.gsma.com/mobileidentity. In summary, it states that MNOs, with their differentiated identity and authentication assets, have the ability to provide sufficient authentication to enable consumers, businesses, and governments to interact in private, trusted and secure environment and enable access to services.

MNOs increasingly are interested in identity services currently being used online (i.e. login, marketing, post sales engagement, payments, etc.), to mitigate some of the pain points encountered in existing services, in order to meet the rapidly increasing market demand for mobile identity services.

How does it improve security?

Public-key-encryption-based authentication frameworks like OpenID Connect (and its predecessors) globally increase the security of the whole Internet by putting the responsibility for user identity verification in the hands of the most expert service providers. Compared to its predecessors, OpenID Connect is dramatically easier to implement and integrate and can expect to receive much wider adoption.

Does it protect peoples’ privacy or provide them more control over their personal information and what is shared?

OpenID Connect identifies a set of personal attributes that can be exchanged between Identity Providers and the apps that use them, and includes an approval step so that users can consent (or deny) the sharing of this information.

What about new authentication technologies like biometrics and devices?

This is an exciting time; innovators are working on several new kinds of authentication technologies to replace or supplement passwords – in particular, the use of hardware authentication devices and embedded cryptography.

These new methods can be adopted by OpenID Connect Identity Providers as they mature to provide more secure authentication to them. For example, two-factor identification is already in production at some OpenID Connect IDPs.

The fact that professionally run OpenID Connect IDPs can take advantage of these new technologies as they mature only increases the value proposition of OpenID Connect. Without doing anything extra, it means that OpenID Connect Relying Parties can benefit from the adoption of stronger authentication technologies by IDPs, simply because they already use OpenID Connect.

How does OpenID Connect relate to the FIDO Alliance?

The FIDO Alliance is one organization in which non-password authentication technologies are being explored. Some OpenID Foundation members are also members of the FIDO Alliance, working on authentication technologies there that can OpenID Providers.

How does OpenID Connect relate to SAML?

The Security Assertion Markup Language (SAML) is an XML-based federation technology used in some enterprise and academic use cases. OpenID Connect can satisfy these same use cases but with a simpler, JSON/REST based protocol. OpenID Connect was designed to also support native apps and mobile applications, whereas SAML was designed only for Web-based applications. SAML and OpenID Connect will likely coexist for quite some time, with each being deployed in situations where they make sense.

How does OpenID Connect enable creating an Internet identity ecosystem?

- Interoperability
- Security
- Ease of deployment
- Flexibility
- Wide support of devices
- Enabling Claims Providers to be distinct from Identity Providers

Back to top