OpenID Connect Standard for Federation

1. OpenID Connect 2*

Open ID Connect 1.0 is a simple identity layer on top of OAuth 2.0 protocol. It allows a client application to request the identity of users in a standardized REST-like manner as an ID token.

It supports various applications like web-based clients, mobile, cloud and JavaScript clients. It requests and receives information about authenticated sessions and end users. Open ID Connect enables clients to use features like encryption of identity data, discovery of Open ID Providers and session management.

Open ID Connect is different from its previous standard- Open ID 2.0 as it supports mobile application and is more user friendly than Open ID 2.0. Moreover, it provides a strong and robust mechanism for signing and encrypting data which was earlier not widely accepted in OpenID2.0 by industry due to security reasons.

1.1 OpenID Connect Specification

The following diagram is taken from the OpenID Foundation's website gives an overview of the protocols that make up the OpenID Connect specification and how they relate to one another

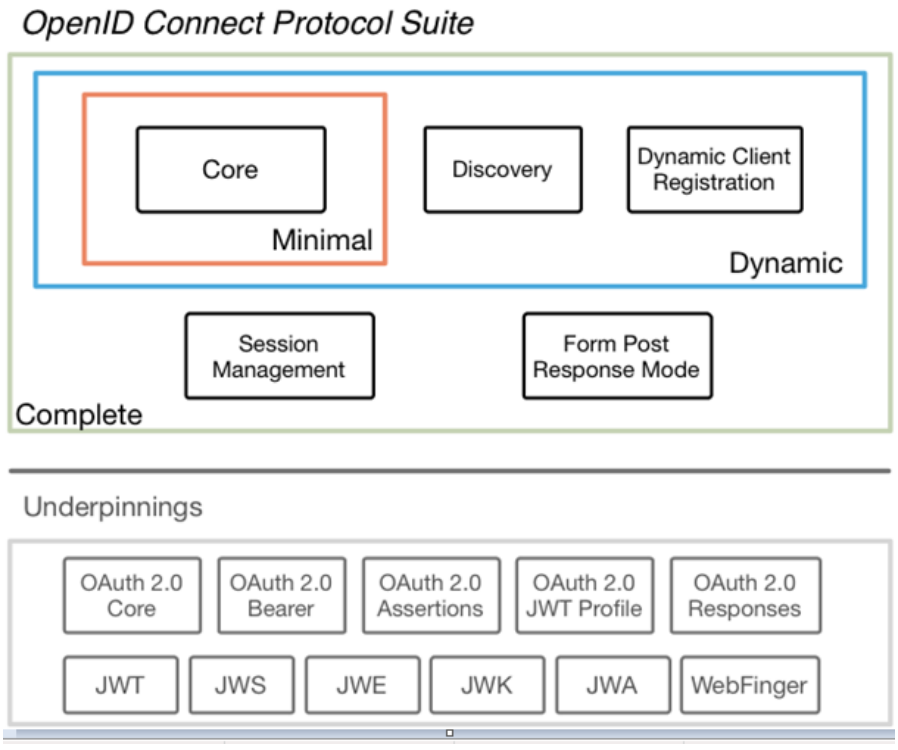

Figure 1: Open ID Connect Protocol Suite

The OpenID Connect 1.0 specification consists of following components:

1. **Core:** This component defines the core functionality of Open ID Connect. It defines authentication built on top of OAuth2.0 and Claims to communicate information about the End-User.
2. **Discovery:** It defines how Clients discover information about Open ID Providers dynamically.
3. **Dynamic Registration**: It defines how clients register with Open ID Providers dynamically.
4. **OAuth 2.0 Multiple Response Types**: It defines several new OAuth 2.0 response types.
5. **OAuth 2.0 Form Post Response Mode**: It defines how to return OAuth 2.0 Authorization Response parameters using HTML form values that are auto-submitted by the User Agent using HTTP POST.
6. **Session Management**: It defines how to manage OpenID Connect sessions, including postMessage-based logout functionality.
7. **HTTP- Based Logout**: It defines an HTTP-based logout mechanism that does not use an OP iframe on RP pages

1.2 OpenID Connect Architecture

The key OpenID Connect terms include End-User, Relying Party (RP), and OpenID Connect Provider (OP), as shown in following figure

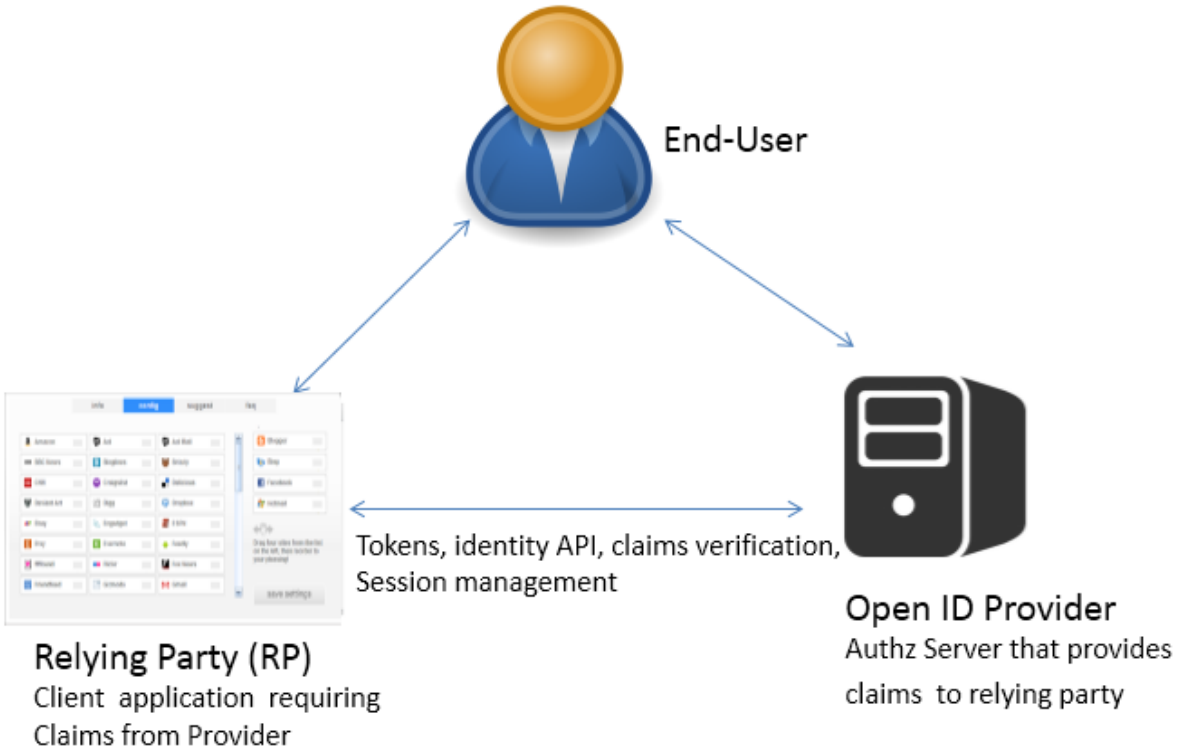

Figure 2: OpenID Connect Architecture

The below diagram depicts flow of information among above mentioned entities.

* represents reference sites

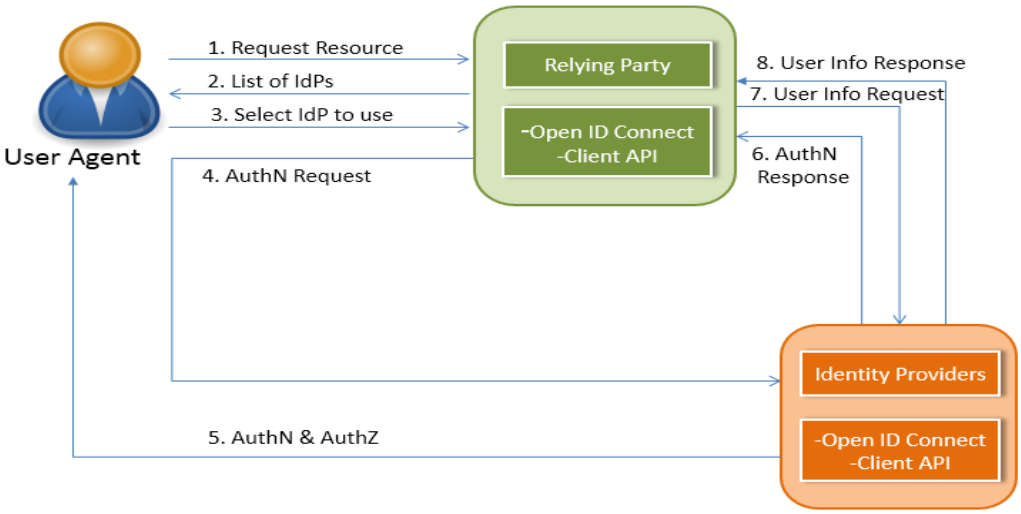

Figure3: Information flow in Open ID Connect

1. End user requesting resource from service provider which acts as Relying party.
2. Relying party respond back with list of identity providers (Open ID Connect is designed such that the users are able to select their preferred identity provider, also known as OpenID Providers which renders the authentication challenge and gains user approval before sharing user attributes.)
3. User selects preferred identity provider.
4. User's authentication request is redirected to selected identity provider and user receives authentication challenge from Identity Provider.
5. User fills in his/her credentials for authentication and authorization.
6. OpenID provider sends user authentication response back to service provider which is referred as relying party.
7. The relying party can request additional profile attributes from OpenID provider.
8. OpenId provider respond back with requested user attributes.

Finally the protected resource is sent back to end user.

2. OpenID Connect Use cases [3*]

- **Non-web Federation:** Open ID Connect supports non web based clients like mobile devices, product API's thus it provides a federation mechanism to other non-web based platforms where SAML concept cannot be used. Since mobile interface increasing its popularity among end users, this standard could widely be accepted in near future.
- **Provisioning Revisited:** Open ID Connect supports session management and an OAuth style back channel communication based on access tokens. There are a number of provisioning scenarios and provisioning mechanisms where SAML, JIT provisioning and SPML interfaces cannot be used. OpenID Connect can be considered as better provisioning standard here.
- **Level of assurance service:** Open ID Connect can be used for supporting Step-up Authentication-as a-Service. OpenID Connect allows an authentication context reference to be passed in requests and responses, just like SAML. The service might be of interest to a wider audience if it supports both SAML and OpenID Connect.
- **Automation of services:** OpenID Connect automates some of the manual work that authentication services of past have relied on the admin to manage by hand. For example, dynamic Identity provider discovery and client registration automates the solution and require less developer interaction.

* represents reference sites

- **Extendable by complimentary profiles:** Many efforts are underway to build on the strong foundation of OpenID Connect. How devices share sessions, how OpenID Providers and relying parties can collaborate using multi-party federation metadata, how OpenID Connect can be leveraged by an authorization protocol like UMA, all of these are examples of how well OpenID Connect can address challenges still unresolved in the industry as of today.

3. Comparison between OpenID Connect, OAuth2.0 and SAML 2.0 [4*]

Aspects	Open ID Connect	OAuth 2.0	SAML 2.0
Underlying Technology	It allows Clients to verify the identity of the End-User based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the End-User in an interoperable and REST-like manner.	It provides and authorization framework to service provider without passing any user identity information	It provides a standard for exchanging authentication and aut horization data between security domains using an XML-based protocol which uses security tokens containing assertions to pass information about a principal between an identity provider and a service provider.
Token Types	It is REST based encapsulating JSON Web Tokens which do not only sign the payload but encrypt the token as well	It uses bearer token (similar to cookies) which do not require a bearer to prove possession of cryptographic key material (proof-of-possession)	It is XML based and supports signing & encrypted certificates
High Security Identity tokens	OpenID connect supports signed and encrypted identity tokens	OAuth 2.0 is an authorization framework does not support identity token	SAML 2.0 also does not support identity token rather it only asserts identity data in token payload
Collects user's consent before sharing attributes	OpenID Connect collects user consent before sharing any user's sensitive information to Service provider	OAuth 2.0 also collects user consent before sharing any user's sensitive information to Service provider	SAML 2.0 does not ask for user consent while sharing user personal information with relying party
Token contains user identity information	Yes, as OpenID connect issues two types of token Identity and access token	OAuth 2.0 does not deal with user identity information	SAML 2.0 token does not contain identity information rather XML payload can be enriched with user attributes
Distributed & Aggregated Claims	OpenID Connect supports this feature	OAuth 2.0 does not support this feature	SAML 2.0 does not support this feature

* represents reference sites

Dynamic Introductions (client discovery & on-boarding)	OpenID Connect supports this functionality	OAuth 2.0 does not support this functionality	SAML 2.0 does not support this functionality
Session Timeout	OpenID Connect supports this functionality	OAuth 2.0 does not support this functionality	SAML 2.0 does not support this functionality

4. Future scope of OpenID Connect

OpenID Connect is a standard which provides federation capabilities in flexible environment where various types of clients such as Web based clients and mobile devices operate and exchange information with each other. It also uses a better mechanism to transfer data over unsecure channels which is more secure and light weight. This feature of OpenID Connect makes its capabilities unique among other federation standards available in market.

Open ID Connect has the support of companies such as Google, Deutsche Telekom, Microsoft, Salesforce and mobile network operators. Some of them are offering its users federated identity options through OpenID Connect. Google, Microsoft, Ping Identity, Nikkei Newspaper, Tokyu Corporation, Yahoo! Japan and Softbank have setup live production environments at their site. Other companies like Deutsche Telekom, AOL and Salesforce have mature deployments of OpenID Connect. Mobile network operators expect OpenID to provide a standard for developing interoperability between the different operators.

Major advantage of OpenID Connect is that it is simple for developers to understand and makes it easy to federate with identity providers. Moreover, it shares only that information which users explicitly tell them to share.

Open ID Connect is poised to enable users to log in through a professional identity provider. The future of Open-ID and federated authentication is bright. There has always been the convenience of making it easier for consumers to sign-up and use the services cheaper and faster to integrate with business partners. However, now Open-ID and equivalents are being offered by vendors with a service that people already use, the authentication is nice side benefit. For companies using Open-ID means that they need not solve the tedious problems of handling registration, login, password reset etc along with getting access to the social graph and getting viral growth by offering users the option logging in via these services. The latter is a compelling reason for supporting Open-ID and why its use will continue to grow.

Following are some of the applications of OpenID Connect for future use:

- **Native SSO**: As the demand for native apps continue to grow due to their ease of use and distribution; this has given rise to an increased demand for default OAuth in native environments. However the onus of managing authentication among the various available native apps lies on the end user. End user must remember login credentials for each and every app, which needs to be re-authenticated. One possible solution in this scenario is increasing the usability of a single sign-on for multiple apps which are published by the same owner. This can be accomplished using OpenID Connect paired with OAuth. Consequently, businesses would then be able to enable and control SSO access to certain enterprise-grade applications, for both web and native apps, as well as for several B2C apps.

- **Mobile Information Management (MIM) and BYOD**: MIM acts as the final step in securing information in mobile devices. The enterprise imposes its management policy directly on the data itself. Business data is secured with the help of security mechanisms and policies which act as constraints while determining how that data can be used. OpenID Connect interacts with a number of identity services which are available in online market and Mobile Network Operators (MNOs) are becoming increasingly aware of this fact. This includes payments and log-in feature. It is believed that OpenID Connect has the power to mitigate pain points which

* represents reference sites

exist within existing services by offering a public key encryption-based authentication framework. Once accomplished, this will transfer the responsibility of identity verification from an average user to an expert service provider. Applying MIM using OpenID Connect is theoretical, and has not yet been proven. However, once adopted, it is believed that it could increase the security of the entire Internet dramatically.

- **Internet of Things**: There is a definite need to distinguish among different connected Things and their identities, as well as a need for a way to authenticate how these Things will collect data. OpenID Connect can enable a 'Thing' to obtain a token to be used in an API call. The user has an active involvement in the issuing of that token, and has the power to impose policies to determine when that token can be used and how his or her data is shared. Because OpenID Connect provides standardized mechanisms by which users can control the sharing of the identity that they use, it is believed that OpenID Connect will become a critical asset in the further development of usable, personalized, and secure Internet of Things applications.

***** represents reference sites

5. References

- http://openid.net/connect/ 2*
- https://blog.surf.nl/wp-content/uploads/2013/04/SURFnet-OpenID-Connect-1.1-.pdf 1*
- http://apicrazy.com/category/identity-management/openid-connect/ 4*
- http://www.ibm.com/developerworks/websphere/library/techarticles/1502_odonnell/1502_odonnell.html
- https://ldapwiki.com/wiki/OpenID%20Connect 3*
- https://www.pingidentity.com/en/resources/articles/openid-connect.html
- http://www.gluu.org/blog/5-reasons-you-need-openid-connect-uma-identity-access-management/
- http://www.gluu.org/blog/10-reasons-openid-connect-will-be-ubiquitous/ 3*
- http://nordicapis.com/3-unique-authorization-applications-of-openid-connect/