OpenID Connect

Muhammad **Rizwan** Asghar
The University of Auckland
September 24, 2015

For template of slides,
thanks to kingsoftstore.com

Overview

- Open ID Connect is an identity layer built on the top of OAuth 2.0
- It provides an open standard for interoperability
- Specifications launched on February 26, 2014
- Free

Why OpenID Connect

- Lack of notion of identity management in OAuth 2.0
- No support of native applications in OpenID

Basic Purpose

- It enables clients to verify the identity of End-Users
- End-Users are identified based on authentication performed by an Authorisation Server
- It also enables clients to obtain information about End-Users

OpenID Connect

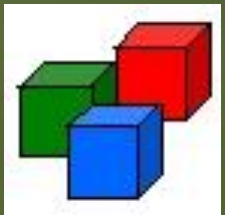
- For developing Internet identity ecosystems that are
  - Secure
  - Flexible
  - Interoperable
- It offers not only authentication but also authorisation
- It supports a variety of use cases

Main Building Blocks

- OpenID 
- OAuth 2.0 

- TLS/SSL 

Roles

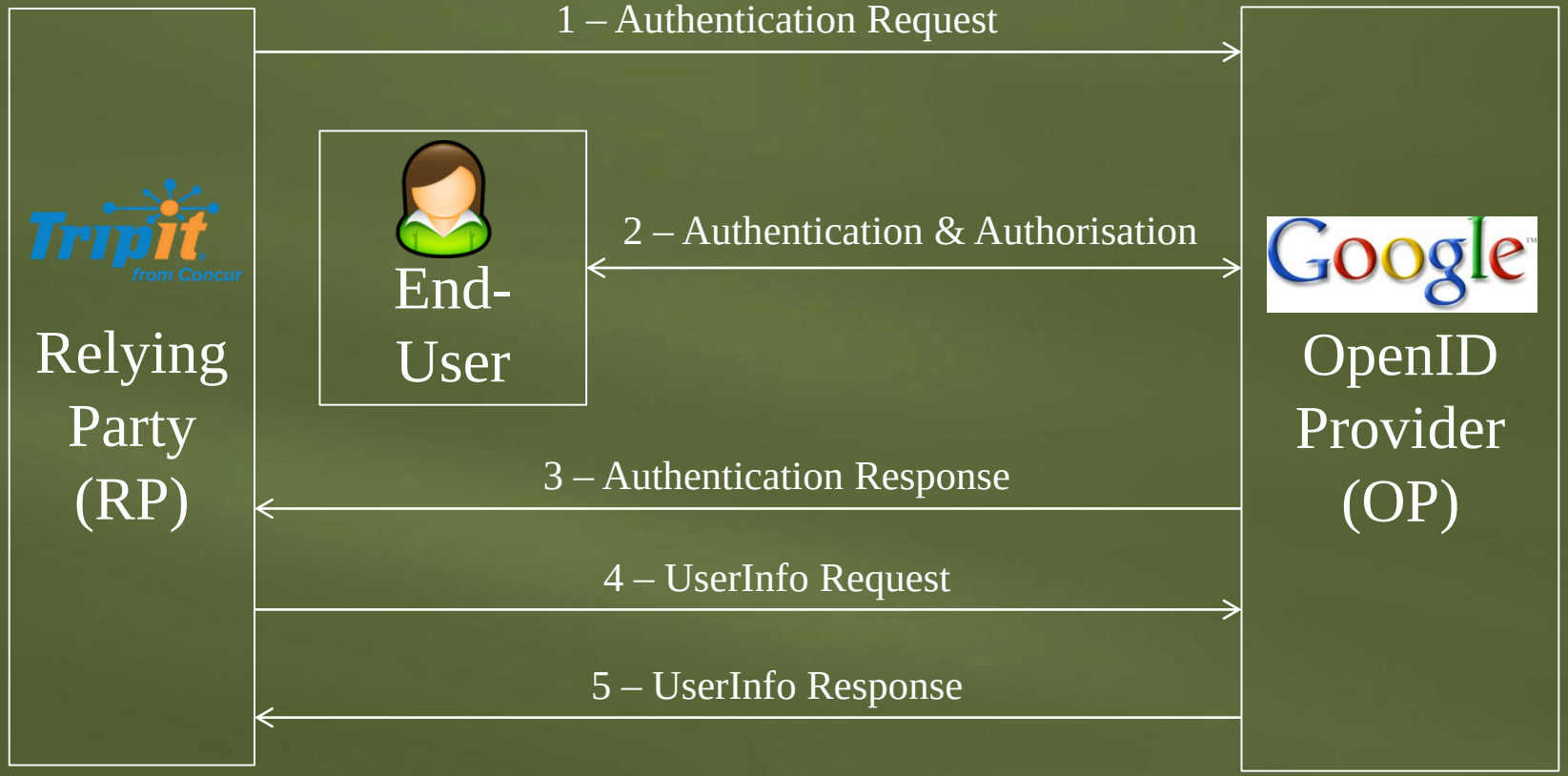


- OpenID Provider (OP)
  - It offers authentication/authorisation
- Relying Party (RP)
  - A client that requires authentication and authorisation
- End-User
  - A human participant who gets authenticated and provides authorisation

OP Examples

- Google
- Microsoft
- Running own OPs on
  - Web sites
  - Personal devices
    - E.g., mobile phones and tablets

OpenID Connect Flow



Core Endpoints

- Authorisation endpoint
  - Authenticates End-Users and asks for their consent for authorisation
- Token endpoint
  - Returns tokens if the client has been authorised
- UserInfo endpoint
  - Hosts protected resources

Flow Details

1. The RP (client) sends a request to the OP
2. The OP authenticates the End-User and obtains authorisation
3. The OP responds with
   - ID Token and
   - Access Token

Flow Details (2)

4. The RP can send a request with the Access Token to the OP
5. The RP receives Claims about the End-User

Authentication Flows

- Authorisation code flow
- Implicit flow
- Hybrid flow

Authentication Flows

Property	Authorisation Code Flow	Implicit Flow	Hybrid Flow
All tokens returned from the Authorisation Endpoint	No	Yes	No
All tokens returned from the Token Endpoint	Yes	No	No
Tokens not revealed to User Agents	Yes	No	No
Client can be authenticated	Yes	No	Yes
Refresh Token possible	Yes	No	Yes
Communication in one round trip	No	Yes	No
Most communication server-to-server	Yes	No	Varies

Key Artefacts

- ID Token
  - Asserts the user's identity
  - Like a standard identity card that is digitally signed
- Access Token
  - Used to get access to protected resources

ID Token

- Asserts the user identity
  - The unique user identifier
- Specifies the authority
  - The OP URI
- The intended audience
  - The client

ID Token (2)

- May specify how and when the user was authenticated
- Includes issue and expiration dates
- May contain additional information
  - User's name
  - User's email
  - …

ID Token: Example


```
{
  "iss": "https://server.example.com",
  "sub": "24400320",
  "aud": "s6BhdRkqt3",
  "nonce": "n-0S6_WzA2Mj",
  "exp": 1311281970,
  "iat": 1311280970,
  "auth_time": 1311280969,
   ...
}
```

ID Token Security

- Digitally signed
  - Provider's RSA key
  - HMAC issued to the client during registration
- May be encrypted

Claims

- Claim
  - A piece of information asserted about an Entity
- Claim Provider
  - A server that can return Claims about an Entity
- ID Token
  - Claims about the Authentication event

Standard Claims

- Address Claim
  - Street address
  - Locality
  - Region
  - Postal code
  - Country

Claim Types

- Normal Claims
  - Directly asserted by the OP
- Aggregated Claims
  - Asserted by a Claim Provider other than the OP but returned by the OP
- Distributed Claims
  - Asserted by a Claim Provider other than the OP but returned as references by the OP

Normal Claim

- Name
- Given name
- Family name
- Email
- Picture

Adoption

- Implemented worldwide by Internet and mobile companies
  - Google
  - Microsoft
  - Deutsche Telekom
  - Salesforce
  - Ping Identity
  - Nomura Research Institute

Adoption (2)

- Mobile network operators
- Many more …

- It will be built into commercial products
- Implemented in open-source libraries for global deployment

Products

- Google has provided OpenID Connect support since early 2013
- Example
  - Google+ Sign-In
  - Link https://developers.google.com/+/api/openidconnect/

Support

- System-level APIs built into Android
- Browsers
  - Mobile
  - Desktop

Integration with New Authentication Technologies

- To replace password-based authentication, new technologies are in progress
- New technologies can be adopted by OpenID Connect, e.g.,
  - 2-factor authentication
  - Biometrics

What does OpenID Connect Solve

- It lets app/site developers authenticate users without owing/managing their passwords
- Developers know who is connected to their app/site

Benefits

- It provides a standard way to outsource site and application login
- Easy to use
- Easy to implement and deploy
- Reliable and secure
- Efficient
- Interoperable

Consent

- Before sharing personal information with RPs, OPs obtain End-Users' consent

Signing & Encryption

- Signing
  - Asymmetric: RSA or ECDSA
  - Symmetric
- Encryption
  - Asymmetric: RSA
  - Asymmetric: Elliptic curve
  - Symmetric

Security Considerations

- Request disclosure
  - Take appropriate protection measures
- Token manufacture/modification
  - Sign or use secure channel
- Server masquerading
  - A malicious server might masquerade
  - Clients need to authenticate the server

Privacy Considerations

- Personally Identifiable Information in UserInfo response
  - Obtain End-Users' consent
- Data access monitoring
  - Make End Users' UserInfo access logs available to them so that they can monitor who accessed their data

Summary

- OpenID Connect is an identity layer built on OAuth 2.0
- An open standard that provides interoperability
- It supports native and mobile apps
- Enables information sharing
- Data access monitoring


Q&
A

References

- OpenID Connect Core 1.0, http://openid.net/specs/openid-connect-core-1_0.html
- OpenID Connect Work Group, http://openid.net/wg/connect/
- The OpenID Foundation Launches the OpenID Connect Standard, http://openid.net/2014/02/26/the-openid-foundation-launches-the-openid-connect-standard/
- Libraries, http://openid.net/developers/libraries/

References (2)

- Google Identity Cookbook: OpenID Connect, https://developers.google.com/accounts/cookbook/technologies/OpenID-Connect
- Google Accounts Authentication and Authorization: Using OAuth 2.0 for Login (OpenID Connect), https://developers.google.com/accounts/docs/OAuth2Login
- Google+ Platform: People: getOpenIdConnect, https://developers.google.com/+/api/latest/people/getOpenIdConnect