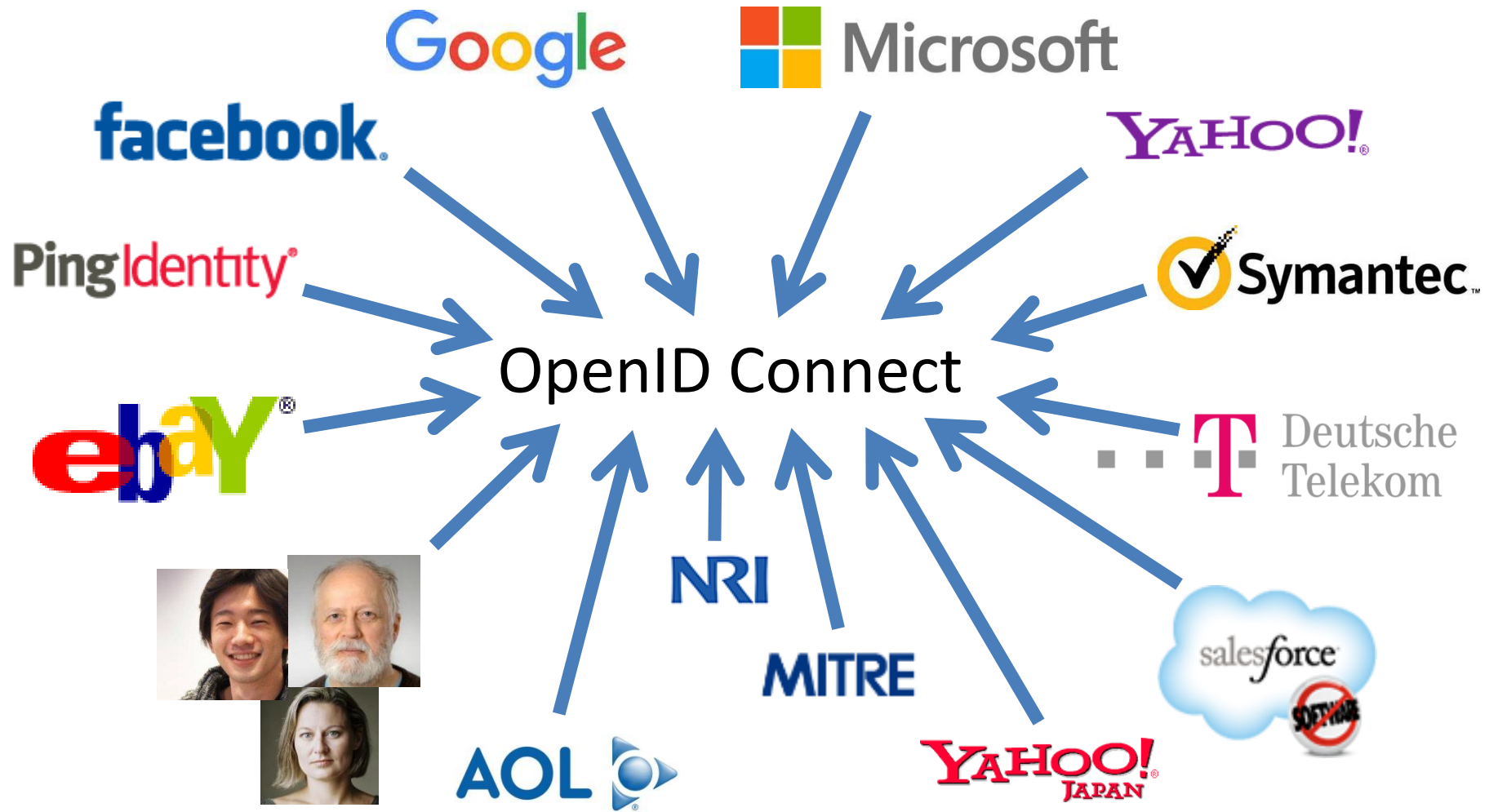# Introduction to OpenID Connect

April 16, 2024

Michael B. Jones

Self-Issued Consulting

Working Together

What is OpenID Connect?

- Simple identity layer on top of OAuth 2.0
- Enables Relying Parties (RPs) to verify identity of end-user
- Enables RPs to obtain basic profile info
- REST/JSON interfaces → low barrier to entry
- Described at https://openid.net/connect/

You're Almost Certainly Using OpenID Connect! OpenID

- Android, AOL, Apple, AT&T, Auth0, Deutsche Telekom, ForgeRock, Google, GrabTaxi, GSMA Mobile Connect, IBM, KDDI, Microsoft, NEC, NRI, NTT, Okta, Oracle, Orange, Ping Identity, Red Hat, Salesforce, Softbank, Symantec, Telefónica, Verizon, Yahoo, Yahoo! Japan, all use OpenID Connect
  - Many other sites and apps large and small use OpenID Connect
- OpenID Connect is infrastructure
  - Not a consumer brand

OpenID Connect Range

- Spans use cases, scenarios
  - Internet, Enterprise, Mobile, Cloud, Federated, User-Centric
- Spans security & privacy requirements
  - From non-sensitive information to highly secure
- Spans sophistication of claims usage
  - From basic default claims to specific requested claims to collecting claims in multiple formats from multiple sources
- Maximizes simplicity of implementations
  - Uses existing IETF specs: OAuth 2.0, JSON Web Token (JWT), etc.
  - Lets you build only the pieces you need

Numerous Awards

- OpenID Connect won 2012 European Identity Award for Best Innovation/New Standard
  - https://openid.net/2012/04/18/openid-connect-wins-2012-european-identity-and-cloud-award/
- OAuth 2.0 won in 2013
- JSON Web Token (JWT) & JOSE won in 2014
- OpenID Certification program won 2018 Identity Innovation Award
- OpenID Certification program won 2018 European Identity Award

Presentation Overview

- Introduction
- Design Philosophy
- Timeline
- A Look Under the Covers
- Overview of OpenID Connect Specs
- More OpenID Connect Specs
- OpenID Certification
- Resources

Design Philosophy

OpenID

Keep Simple Things Simple

Make Complex Things Possible

単純

Keep Simple Things Simple

OpenID

UserInfo Endpoint for simple claims about user

Designed to work well on mobile phones

How We Made It Simple

- Built on OAuth 2.0

- Uses JavaScript Object Notation (JSON)

- Lets you build only the pieces that you need

- *Goal: Easy implementation on all modern development platforms*

Make Complex Things Possible

OpenID

Encrypted Claims

Aggregated Claims

Distributed Claims

Key Differences from OpenID 2.0

- Support for native client applications
- Identifiers using e-mail address format
- UserInfo Endpoint for simple claims about user
- Designed to work well on mobile phones
- Uses JSON/REST, rather than XML
- Support for encryption and higher LOAs
- Support for distributed and aggregated claims
- Support for session management, including logout
- Support for self-issued identity providers

OpenID Connect Timeline

- Artifact Binding working group formed, March 2010
- Major design issues closed at IIW, May 2011
  - Result branded "OpenID Connect"
- 5 rounds of interop testing between 2011 and 2013
  - Specifications refined after each round of interop testing
- Won Best New Standard award at EIC, April 2012
- **Final specifications approved, February 2014**
- Errata Set 1 approved, November 2014
- OpenID Connect Certification launched, April 2015
- OpenID Federation work begun, July 2016
- OpenID Certification program won awards in March 2018 and April 2018
- Logout specifications became Final, September 2022
- Numerous extension specs under way, including for Verifiable Credentials, 2019-present
- Errata Set 2 approved, December 2023
- OpenID Connect submitted to ISO for publication as PAS specifications, January 2024

A Look Under the Covers

- ID Token
- Claims Requests
- UserInfo Claims
- Example Protocol Messages

ID Token

- JSON Web Token (JWT) representing logged-in session
- Claims:
  - `iss` – Issuer
  - `sub` – Identifier for subject (user)
  - `aud` – Audience for ID Token
  - `iat` – Time token was issued
  - `exp` – Expiration time
  - `nonce` – Mitigates replay attacks

ID Token Claims Example

```json
{
 "iss": "https://server.example.com",
 "sub": "248289761001",
 "aud": "0acf77d4-b486-4c99-bd76-074ed6a64ddf",
 "iat": 1311280970,
 "exp": 1311281970,
 "nonce": "n-0S6_WzA2Mj"
}
```

OpenID

Claims Requests

- Basic requests made using OAuth scopes:
  - `openid` – Declares request is for OpenID Connect
  - `profile` – Requests default profile info
  - `email` – Requests email address & verification status
  - `address` – Requests postal address
  - `phone` – Requests phone number & verification status
  - `offline_access` – Requests Refresh Token issuance
- Requests for individual claims can be made using JSON "`claims`" request parameter

UserInfo Claims

OpenID

- `sub`
- `name`
- `given_name`
- `family_name`
- `middle_name`
- `nickname`
- `preferred_username`
- `profile`
- `picture`
- `website`

- `gender`
- `birthdate`
- `locale`
- `zoneinfo`
- `updated_at`
- `email`
- `email_verified`
- `phone_number`
- `phone_number_verified`
- `address`

UserInfo Response Example

```
{
 "sub": "248289761001",
 "name": "Jane Doe",
 "given_name": "Jane",
 "family_name": "Doe",
 "email": "janedoe@example.com",
 "email_verified": true,
 "picture": "https://example.com/janedoe/me.jpg"
}
```

Authorization Request Example

OpenID

```
https://server.example.com/authorize
  ?response_type=id_token%20token
  &client_id=0acf77d4-b486-4c99-bd76-074ed6a64ddf
  &redirect_uri=https%3A%2F%2Fclient.example.com%2Fcb
  &scope=openid%20profile
  &state=af0ifjsldkj
  &nonce=n-0S6_WzA2Mj
```

Authorization Response Example

OpenID

```
HTTP/1.1 302 Found
Location: https://client.example.com/cb
  #access_token=mF_9.B5f-4.1JqM
  &token_type=bearer
  &id_token=eyJhbGzI1NiJ9.eyJz9Glnw9J.F9-V4IvQ0Z
  &expires_in=3600
  &state=af0ifjsldkj
```

UserInfo Request Example

```
GET /userinfo HTTP/1.1
Host: server.example.com
Authorization: Bearer mF_9.B5f-4.1JqM
```

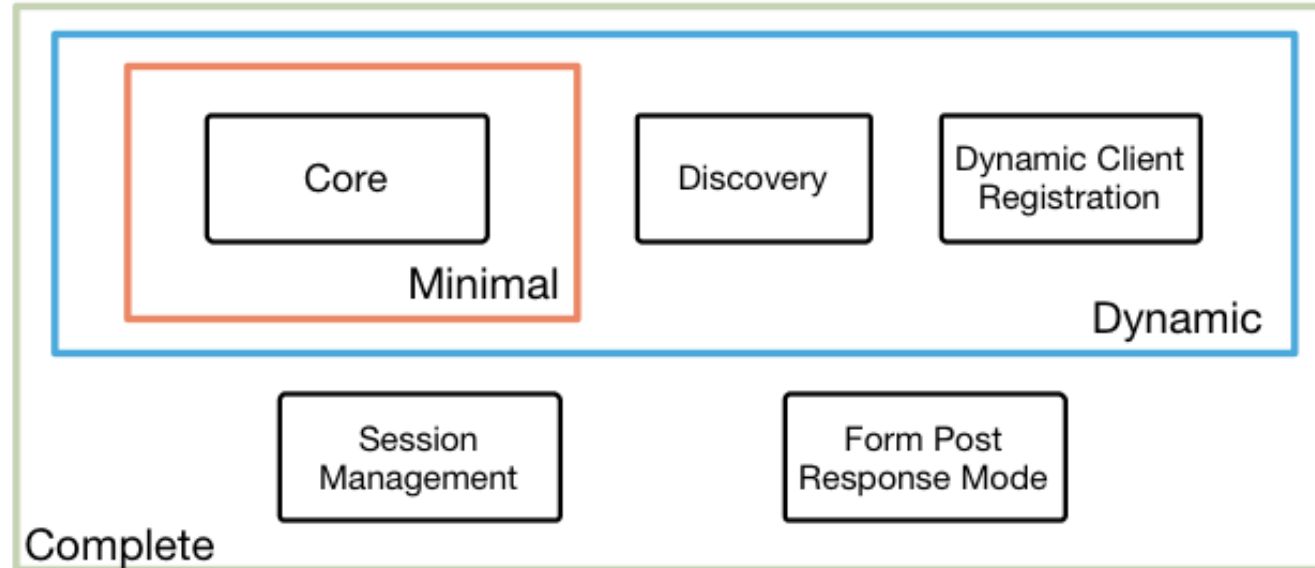# Original Overview of Specifications

OpenID

OpenID Connect Protocol Suite

4 Feb 2014
http://openid.net/connect

OpenID 2.0 to OpenID Connect Migration (Additional Final Specification)

- Defines how to migrate from OpenID 2.0 to OpenID Connect
  - Has OpenID Connect identity provider also return OpenID 2.0 identifier, enabling account migration
- https://openid.net/specs/openid-connect-migration-1_0.html
- Completed April 2015
- Google shut down OpenID 2.0 support in April 2015
- AOL, Yahoo, others have replaced OpenID 2.0 with OpenID Connect

OAuth 2.0 Form Post Response Mode (Additional Final Specification)

- Defines how to return OAuth 2.0 Authorization Response parameters (including OpenID Connect Authentication Response parameters) using HTML form values auto-submitted by the User Agent using HTTP POST
- A "form post" binding, like SAML and WS-Federation
  - An alternative to fragment encoding
- https://openid.net/specs/oauth-v2-form-post-response-mode-1_0.html
- Completed April 2015
- In production use by Microsoft, Ping Identity

RP-Initiated Logout

- Enables RP to request that OP log out end-user
  - https://openid.net/specs/openid-connect-rpinitiated-1_0.html
  - Content recently split out of Session Management spec
- Can be used with all OP-Initiated Logout methods
- Not affected by browser privacy changes
  - (unlike some of the OP-Initiated Logout methods)
- *Final Specification as of September 2022*

OP-Initiated Logout

- Enables OP to request that RPs log out end-user's sessions with the OP
- Three approaches specified by the working group:
  - Session Management
    - https://openid.net/specs/openid-connect-session-1_0.html
    - Uses HTML5 postMessage to communicate state changes between OP and RP iframes
  - Front-Channel Logout
    - https://openid.net/specs/openid-connect-frontchannel-1_0.html
    - Uses HTTP GET to load image or iframe, triggering logout (similar to SAML, WS-Federation)
  - Back-Channel Logout
    - https://openid.net/specs/openid-connect-backchannel-1_0.html
    - Server-to-communication not using the browser (so can be used by native applications)
- All support multiple logged-in sessions from OP at RP
- Session Management & Front-Channel Logout affected by browser privacy changes
- *Final Specifications as of September 2022*

`unmet_authentication_requirements` Specification

- OpenID Connect Core Error Code unmet_authentication_requirements
  - https://openid.net/specs/openid-connect-unmet-authentication-requirements-1_0.html

- **Defines** `unmet_authentication_requirements` **error code**

- Enables OP to signal that it failed to authenticate the End-User per the RP's requirements

- *Became Final in November 2022*

`prompt=create` Specification

- Initiating User Registration via OpenID Connect specification
  - https://openid.net/specs/openid-connect-prompt-create-1_0.html
- Requests enabling account creation during authentication

- *Became Final in December 2022*

Tenth Anniversary of OpenID Connect OpenID

- OpenID Connect specifications were approved in February 2014
- Three celebrations are being held
    - January 2024 at Japan OpenID Summit in Tokyo
    - May 2024 at Identiverse in Las Vegas
    - June 2024 at EIC in Berlin
- Presentations from first celebration published at https://self-issued.info/?p=2481
- During the celebrations, we are sharing our perspectives on
    - How we developed OpenID Connect
    - Why it succeeded
    - Lessons we learned along the way
- Lessons learned
    - "Keep simple things simple"
    - Repeated interop testing and incorporating resulting feedback from developers was critical
    - Certification enables an ecosystem of interoperable implementations

Exciting time for OpenID Connect!

- More happening than at any time since original specs created
- I'll give you a taste of the exciting work happening…

OpenID Federation Specification

- OpenID Federation specification
  - https://openid.net/specs/openid-federation-1_0.html
- Enables trust establishment and maintenance of multi-party federations
  - Applying lessons learned from large-scale SAML federations
  - Can be used for OpenID Connect, OAuth 2.0 deployments
- Recently renamed from "OpenID Connect Federation" to reflect broader role
  - Can be and is used both with and without OpenID Connect
- Defines hierarchical JSON-based metadata structures for participants
- Three interop events were held in 2020
- In production use in Italy, Australia, Sweden
- Have already resolved most open issues
  - *Last Implementer's Draft planned in this quarter*
  - *Then advancement to Final status later this year*

OpenID for Verifiable Credentials

- Family of three specs enabling use of identities that you hold
- Uses the three-party Issuer/Holder/Verifier model
  - An Issuer creates a Verifiable Credential for you to hold
  - You hold it in a Wallet
  - You present it to a Verifier
- Credential format agnostic
  - Can be used w/ W3C VCs, ISO Mobile Driving Licenses (mDL), SD-JWTs, etc.
- Has good privacy properties
  - Issuer doesn't know when/where you're using the credential
- See https://openid.net/openid4vc/

OpenID for Verifiable Credential Issuance ⬡ OpenID

- OpenID for Verifiable Credential Issuance specification
  - https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html
- Specifies how to issue Verifiable Credentials to Holder/Wallet
- Based on OAuth 2.0
- Credential format agnostic
  - For example, can use with ISO Mobile Driving Licenses (mDL)
- Includes issuer-initiated flow
- *First Implementer's Draft approved this month*

OpenID for Verifiable Presentations

- OpenID for Verifiable Presentations specification
  - https://openid.net/specs/openid-4-verifiable-presentations-1_0.html
- Defines how to present Verifiable Presentations to a Verifier
- Based on OAuth 2.0
- Credential format agnostic
  - For example, can use with ISO Mobile Driving Licenses (mDL)
- Second Implementer's Draft approved May 2023
- *Actively working towards third Implementer's Draft*

Self-Issued OpenID Provider V2

- OpenID Connect Core defined Self-Issued OpenID Provider (SIOP) functionality
  - Lets you be your own identity provider (rather than a third party)
- Self-Issued OpenID Provider v2 specification
  - https://openid.net/specs/openid-connect-self-issued-v2-1_0.html
  - Extends initial SIOP functionality to include DIDs as subjects
- Credential format agnostic
- SIOP being used with ISO Mobile Driving Licenses (mDL)
- Implementer's Draft approved February 2022
  - *Actively working towards second Implementer's Draft*

Native SSO Specification

- OpenID Connect Native SSO for Mobile Apps specification
  - https://openid.net/specs/openid-connect-native-sso-1_0.html
- Enables Single Sign-On across apps by the same vendor
- Assigns a device secret issued by the Authorization Server
- Deployed by AOL

- *Became an Implementer's Draft in December 2022*

Second Errata Set

- Edits were performed to address outstanding errata issues
  - Updates to Core, Discovery, Registration, and Backchannel Logout
- Errata updates do not change the meaning of the specs
- Second Errata Set published December 2023

ISO Publicly Available Submission (PAS) for OpenID Connect

Submission of OpenID Connect specs for republication by ISO/IEC JTC 1

- Will enable use of OpenID Connect in jurisdictions requiring specs by treaty organizations
- Submission accepted, January 2024
- No changes were made to the submitted specifications, other than adding ISO title pages
- ISO spec numbers assigned, February 2024
    - ISO/IEC CD 26131: Information technology — OpenID Connect Core 1.0
    - ISO/IEC CD 26132: Information technology — OpenID Connect Discovery 1.0
    - ISO/IEC CD 26133: Information technology — OpenID Connect Dynamic Client Registration 1.0
    - ISO/IEC CD 26134: Information technology — OpenID Connect RP-Initiated Logout 1.0
    - ISO/IEC CD 26135: Information technology — OpenID Connect Session Management 1.0
    - ISO/IEC CD 26136: Information technology — OpenID Connect Front-Channel Logout 1.0
    - ISO/IEC CD 26137: Information technology — OpenID Connect Back-Channel Logout 1.0
    - ISO/IEC CD 26138: Information technology — OAuth 2.0 Multiple Response Type Encoding Practices
    - ISO/IEC CD 26139: Information technology — OAuth 2.0 Form Post Response Mode
- Publication as ISO specs expected after five-month ISO balloting period

Related OpenID Working Groups

- **M**obile **O**perator **D**iscovery, **R**egistration, & authe**N**tic**A**tion (MODRNA)
  - Mobile operator profiles for OpenID Connect

- Financial-grade API (FAPI)
  - FAPI used for Open Finance in jurisdictions including UK, Australia, Brazil, Saudia Arabia, Norway, Germany, Japan, Canada, & more to come…

- eKYC and Identity Assurance (eKYC-IDA)
  - Defines JWT format for verified claims with identity assurance information

- Digital Credentials Protocols (DCP)
  - Future home of OpenID for Verifiable Credentials (OpenID4VC) specifications

Identity Assurance Specification (Related Work in eKYC-IDA WG)

- OpenID Connect for Identity Assurance
  - https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html
- JWT representation for verified person data
  - Including information about the identity verification performed
  - Enables legal compliance for some use cases
- Moved to eKYC and Identity Assurance working group in 2019
- *Fourth Implementer's Draft approved October 2022*

CIBA Core
(Related Work in MODRNA WG)

- OpenID Connect Client-Initiated Backchannel Authentication (CIBA) Core
  - https://openid.net/specs/openid-client-initiated-backchannel-authentication-core-1_0.html
- Authentication flow with direct Relying Party to OpenID Provider communication without redirects through browser
- Used by FAPI CIBA Profile
- *Became Final in September 2021*

What is OpenID Certification?

- Enables OpenID Connect (and FAPI) implementations to be certified as meeting the requirements of defined conformance profiles
  - Goal is to make high-quality, secure, interoperable implementations the norm
- An OpenID Certification has two components:
  - Technical evidence of conformance resulting from testing
  - Legal statement of conformance
- Certified implementations can use the "OpenID Certified" logo
- *3,532 total certifications to date!*

What value does certification provide?

- Technical:
  - Certification testing gives confidence that things will "just work"
  - No custom code required to integrate with implementation
  - Better for all parties
  - Relying parties explicitly asking identity providers to get certified
- Business:
  - Enhances reputation of organization and implementation
  - Shows that organization is taking interop seriously
  - Customers may choose certified implementations over others

OpenID Connect Certification Profiles OpenID

- Authentication
  - Basic Flow
  - Implicit Flows
  - Hybrid Flows
  - Third Party-Initiated Login Flow
- Discovery (OP Metadata)
- Dynamic Client Registration
- Logout
  - RP-Initiated Logout
  - Session Management
  - Front-Channel Logout
  - Back-Channel Logout
- Form Post Response Mode

OpenID Connect OP Certifications

- OpenID Provider certifications at
https://openid.net/certification/#OPs
  - 616 profiles certified to date for
    160 deployments

- Recent additions:
  - Duende Software, MonoCloud, Myself,
    SAP, Scrive AB, Tiago Cardoso

- Each entry link to zip file with test
logs and signed legal statement
  - *Test results available for public
    inspection*

OpenID Connect RP Certifications

- Relying Party certifications at
  https://openid.net/certification/#RPs
  - 127 profiles certified to date for
    43 deployments

- Recent additions:
  - Echoworx, Erlang Ecosystem
    Foundation, Filip Skokan

Certified Relying Parties

These deployments have been granted certifications for these Relying Party conformance profiles:

Organization	Implementation	Basic RP	RP Implicit	Hybrid RP	Config RP	Dynamic RP	Form Post RP	3rd Party-Init RP
Brock Allen	oidc-client-js 1.3		4-Feb-2017		7-Feb-2017			
Dominick Baier	IdentityModel.OidcClient 2.0	27-Jan-2017			6-Feb-2017			
Damien Bowden	angular-auth-oidc-client 1.0.2		21-Jun-2017		11-Aug-2017			
F5 Networks	BIG-IP 13.1.0 Evergreen	7-Jul-2017						
Thierry Habart	SimpleIdentityServer V1.0.1	17-Jan-2017	17-Jan-2017	17-Jan-2017	17-Jan-2017	17-Jan-2017		
Ilex International	Sign&go 8.0	10-Mar-2020						
Janrain	IDPD 2.6.0	7-Feb-2017						
Roland Hedberg	pyoidc 0.9.4	20-Dec-2016	20-Dec-2016	20-Dec-2016	20-Dec-2016	20-Dec-2016		
Roland Hedberg	oidcrp 0.4.0	16-Apr-2018	16-Apr-2018	16-Apr-2018	16-Apr-2018	16-Apr-2018		
IBM	Open Liberty 18.0.0.4	26-Oct-2018						
IBM	WebSphere Liberty 18.0.0.4	26-Oct-2018						
Tom Jones	TC.AUTHENTICATION 1.0	30-Jun-2017						
Karlsruher Institut für Technologie, SCC	oidcc 1.0.1	2-Feb-2017			2-Feb-2017			
KSIGN	KSign Trust Thing 1.0	2-Jan-2018						
KSIGN	KSign Trust Thing 1.1		3-Oct-2018					
KSIGN	KSign Trust Thing 1.2				10-Oct-2019			
Nomura Research Institute	phpOIDC 2016 Winter	7-Feb-2017	7-Feb-2017	7-Feb-2017	7-Feb-2017	7-Feb-2017		
Nov Matake	openid_connect rubygem v1.0.3	20-Jan-2017						
Ping Identity	PingAccess 4.2.2	26-Jan-2017						
Ping Identity	PingFederate 8.3.1	17-Jan-2017			31-Jan-2017			
Ping Identity	PingFederate 9.2.1	4-Feb-2019			4-Feb-2019		4-Feb-2019	
Filip Skokan	node openid-client ^1.3.0	15-Dec-2016	15-Dec-2016	15-Dec-2016	15-Dec-2016	15-Dec-2016		
Filip Skokan	node openid-client ^2.0.0	12-Apr-2018	12-Apr-2018	12-Apr-2018	12-Apr-2018	12-Apr-2018	29-Jun-2018	
Filip Skokan	node openid-client ^3.0.0	11-May-2019	11-May-2019	11-May-2019	11-May-2019	11-May-2019	11-May-2019	
Manfred Steyer	angular-oauth2-oidc 2.0.5		16-Aug-2017					
ZmartZone IAM	lua-resty-openidc 1.5.1	17-Nov-2017			17-Nov-2017			
ZmartZone IAM	mod_auth_openidc 2.3.1	21-Jul-2017	21-Jul-2017	21-Jul-2017	21-Jul-2017	21-Jul-2017		

Certified OpenID Relying Parties for Logout Profiles

These deployments have been granted certifications for these OpenID Relying Party logout conformance profiles:

Organization	Implementation	RP-Initiated RP	Session RP	Front-Channel RP	Back-Channel RP
Roland Hedberg	OIDCrp v.0.6.6	20-Mar-2020	20-Mar-2020	20-Mar-2020	20-Mar-2020

Use of Self-Certification

OpenID

- OpenID Certification uses self-certification
  - Party seeking certification does the testing
  - (rather than paying a 3rd party to do the testing)
- Simpler, quicker, less expensive, more scalable than 3rd party certification
- Results are nonetheless trustworthy because
  - Testing logs are made available for public scrutiny
  - Organization puts its reputation on the line by making a public declaration that its implementation conforms to the profile being certified to

How does OpenID Certification work? OpenID

- Organization decides what profiles it wants to certify to
  - For instance, "Basic OP", "Config OP", and "Dynamic OP"
- Runs conformance tests publicly available at https://www.certification.openid.net/
- Once all tests for a profile pass, organization submits certification request to OpenID Foundation containing:
  - Logs from all tests for the profile
  - Signed legal declaration that implementation conforms to the profile
- Organization pays certification fee (for profiles not in pilot mode)
- OpenID Foundation verifies application is complete and grants certification
- OIDF lists certification at https://openid.net/certification/

What does certification cost?

- Not a profit center for the OpenID Foundation
    - Fees there to help cover costs of operating certification program
- Member price
    - $700
- Non-member price
    - $3500
- New profiles in pilot mode are available to members for free
- Costs described at https://openid.net/certification/fees/

Example Testing Screen

Log from a Conformance Test

OpenID

Test info

Profile: {'openid-configuration': 'config', 'response_type': 'code', 'crypto': 'sign', 'registration': 'static'}
Timestamp: 2015-04-07T02:58:53Z
Test description: Keys in OP JWKs well formed [Config, Dynamic]
Test ID: OP-Discovery-JWKs
Issuer: https://stsadweb.one.microsoft.com/adfs

Test output

```
__After completing the test flow:__
[verify-base64url]
        status: OK
        description: Verifies that the base64 encoded parts of a JWK is in fact base64url encoded and not just base64 encoded
[check-http-response]
        status: OK
        description: Checks that the HTTP response status is within the 200 or 300 range
__X:==== END ====__
```

Trace output

```
0.000288 ------------ DiscoveryRequest ------------
0.000299 Provider info discover from 'https://stsadweb.one.microsoft.com/adfs'
0.000305 --> URL: https://stsadweb.one.microsoft.com/adfs/.well-known/openid-configuration
0.426715 ProviderConfigurationResponse: {
  "access_token_issuer": "http://stsadweb.one.microsoft.com/adfs/services/trust",
  "authorization_endpoint": "https://stsadweb.one.microsoft.com/adfs/oauth2/authorize/",
  "claims_parameter_supported": false,
  "claims_supported": [
    "aud",
    "iss",
    "iat",
    "exp",
    "auth_time",
    "nonce",
    "at_hash",
    "c_hash",
    "sub",
    "upn",
    "unique_name",
    "pwd_url",
    "pwd_exp",
    "ver"
  ],
  "grant_types_supported": [
    "authorization_code",
    "refresh_token",
    "client_credentials",
    "urn:ietf:params:oauth:grant-type:jwt-bearer",
    "implicit",
    "password"
  ],
  "id_token_signing_alg_values_supported": [
    "RS256"
  ],
  "issuer": "https://stsadweb.one.microsoft.com/adfs",
  "jwks_uri": "https://stsadweb.one.microsoft.com/adfs/discovery/keys",
  "request_parameter_supported": false,
```

```
  ],
  "issuer": "https://stsadweb.one.microsoft.com/adfs",
  "jwks_uri": "https://stsadweb.one.microsoft.com/adfs/discovery/keys",
  "request_parameter_supported": false,
  "request_uri_parameter_supported": true,
  "require_request_uri_registration": true,
  "response_modes_supported": [
    "query",
    "fragment",
    "form_post"
  ],
  "response_types_supported": [
    "code",
    "id_token",
    "code id_token",
    "token id_token"
  ],
  "scopes_supported": [
    "logon_cert",
    "profile",
    "user_impersonation",
    "aza",
    "vpn_cert",
    "full_access",
    "email",
    "openid"
  ],
  "subject_types_supported": [
    "pairwise"
  ],
  "token_endpoint": "https://stsadweb.one.microsoft.com/adfs/oauth2/token/",
  "token_endpoint_auth_methods_supported": [
    "client_secret_post",
    "client_secret_basic",
    "private_key_jwt",
    "windows_client_authentication"
  ],
  "token_endpoint_auth_signing_alg_values_supported": [
    "RS256"
  ],
  "version": "3.0",
  "webfinger_endpoint": "https://stsadweb.one.microsoft.com/adfs/.well-known/webfinger"
}
0.846957 JWKS: {
  "keys": [
    {
      "alg": "RS256",
      "e": "AQAB",
      "kid": "f-5GWKyaV6fDdnKB7A3b0llXZ0E",
      "kty": "RSA",
      "n": "ygUNL9XXanKy_fQ1X0SMt9LRKpH3Xup1lk5mivaw7thYRPrkGArJezV4x-hfk3Rm9qv6ikBGnTW0lI8FqotLcXmvIBqtbIDfSh59uts1r0QLRUVKS_2Q
      "use": "sig",
      "x5c": [
        "MIIFrjCCBJagAwIBAgIKEzgGLwABAACESDANBgkqhkiG9w0BAQUFADCBgDETMBEGCgmSJomT8ixkARkWA2NvbTEZMBcGCgmSJomT8ixkARkWCW1pY3Jvc29
      ],
      "x5t": "f-5GWKyaV6fDdnKB7A3b0llXZ0E"
    }
  ]
}
0.847706 ==== END ====
```

Result
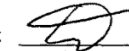
PASSED

Certification of Conformance

OpenID

- Legal statement by certifier stating:
  - Who is certifying
  - What software
  - When tested
  - Profile tested
- Commits reputation of certifying organization to validity of results

OpenID®

CERTIFICATION OF CONFORMANCE
TO OPENID CONNECT CONFORMANCE PROFILE

Name of Entity ("Implementer") Making this Certification: Ping Identity Corporation

Software or Service ("Deployment") Name & Version #: PingFederate Summer 2015 Release

OpenID Connect Conformance Profile: Basic OpenID Provider

Conformance Test Suite Software: op.certification.openid.net as of April 10, 2015

Test Date: April 10, 2015

1. Certification: Implementer has tested the Deployment (including by successfully completing the validation testing using the Conformance Test Suite Software) and verified that it conforms to the OpenID Connect Conformance Profile, and hereby certifies to the OpenID Foundation and the public that the Deployment conforms to the OpenID Connect Conformance Profile as set forth above.

2. Maintenance: If subsequent changes to the Deployment, or other information or testing, indicates that the Deployment is not in conformance, Implementer will either correct the nonconformance (and update this Certification if necessary) or revoke this Certification.

3. Incorporation of Terms: The Terms and Conditions for Certification of Conformance to an OpenID Connect Conformance Profile, located at www.openid.net/certification, are incorporated by reference in this Certification, and Implementer agrees to be bound by such Terms and Conditions.

Implementer's Address Information	
Address:	1001 17th Street, Suite 100
City, State/Province, Postal Code	Denver, CO 80202
Country	USA
Implementer's Authorized Contact Information	
Name:	Brian Campbell
Title:	Distinguished Engineer
Phone:	720.317.2061
Email:	bcampbell@pingidentity.com

Authorized Signature:

Name: Daniel Wossika

Title: Assoc. Gen. Counsel

Date: Apr. 10, 2015

How does certification relate to interop testing?

- OpenID Connect held 5 rounds of interop testing – see http://osis.idcommons.net/
  - Starting over a decade ago!
  - Each round improved implementations and specs
  - By the numbers: 20 implementations, 195 members of interop list, > 1000 messages exchanged
- Recently multiple interop testing rounds for OpenID Connect Federation
- With interop testing, by design, participants can ignore parts of the specs
- Certification raises the bar:
  - Defines set of conformance profiles that certified implementations meet
  - Assures interop across full feature sets in profiles

Can I use the OpenID Certification site for interop testing?

- Yes – please do!
- The OpenID Foundation is committed to keeping the conformance test sites up and available for free to all
- Many projects using conformance testing for regression testing
  - Once everything passes, you're ready for certification!
- Test software is open source using Apache 2.0 license
  - Some projects have deployed private instances for internal testing
  - Available as a Docker container

Favorite Comments on OpenID Certification

- Eve Maler – VP of Innovation at ForgeRock
  - "You made it as simple as possible so every interaction added value."
- Jaromír Talíř – CZ.NIC
  - "We used and still are using certification platform mainly as testing tool for our IdP. Thanks to this tool, we have fixed enormous number of bugs in our platform an even some bugs in the underlying library."
- Brian Campbell – Distinguished Engineer at Ping Identity
  - "The process has allowed us to tighten up our implementation and improve on the already solid interoperability of our offerings in the OpenID Connect ecosystem."
- William Denniss – Google
  - "We have built the RP tests into the continuous-integration testing pipeline for AppAuth."

What's new for OpenID Certification? ⟳ OpenID

- Certification program is now financially self-supporting!
  - Open Banking certifications from Brazil and other places got us there
- OpenID4VC certification tests (for OpenID4VP) started
- eKYC-IDA certification tests planned
- OpenID Federation tests planned

OpenID Certification Call to Action

- Test your OpenID Connect and FAPI implementations now
  - And once you're ready, certify!
- Join the OpenID Foundation and/or the OpenID Connect working group

OpenID Connect Resources

- OpenID Connect
  - https://openid.net/connect/
- Frequently Asked Questions
  - https://openid.net/connect/faq/
- OpenID Connect Working Group and Specs Status Page
  - https://openid.net/wg/connect/ and https://openid.net/wg/connect/status/
- OpenID for Verifiable Credentials
  - https://openid.net/openid4vc/
- OpenID Certification Program
  - https://openid.net/certification/
- Certified OpenID Connect Implementations Featured for Developers
  - https://openid.net/developers/certified/
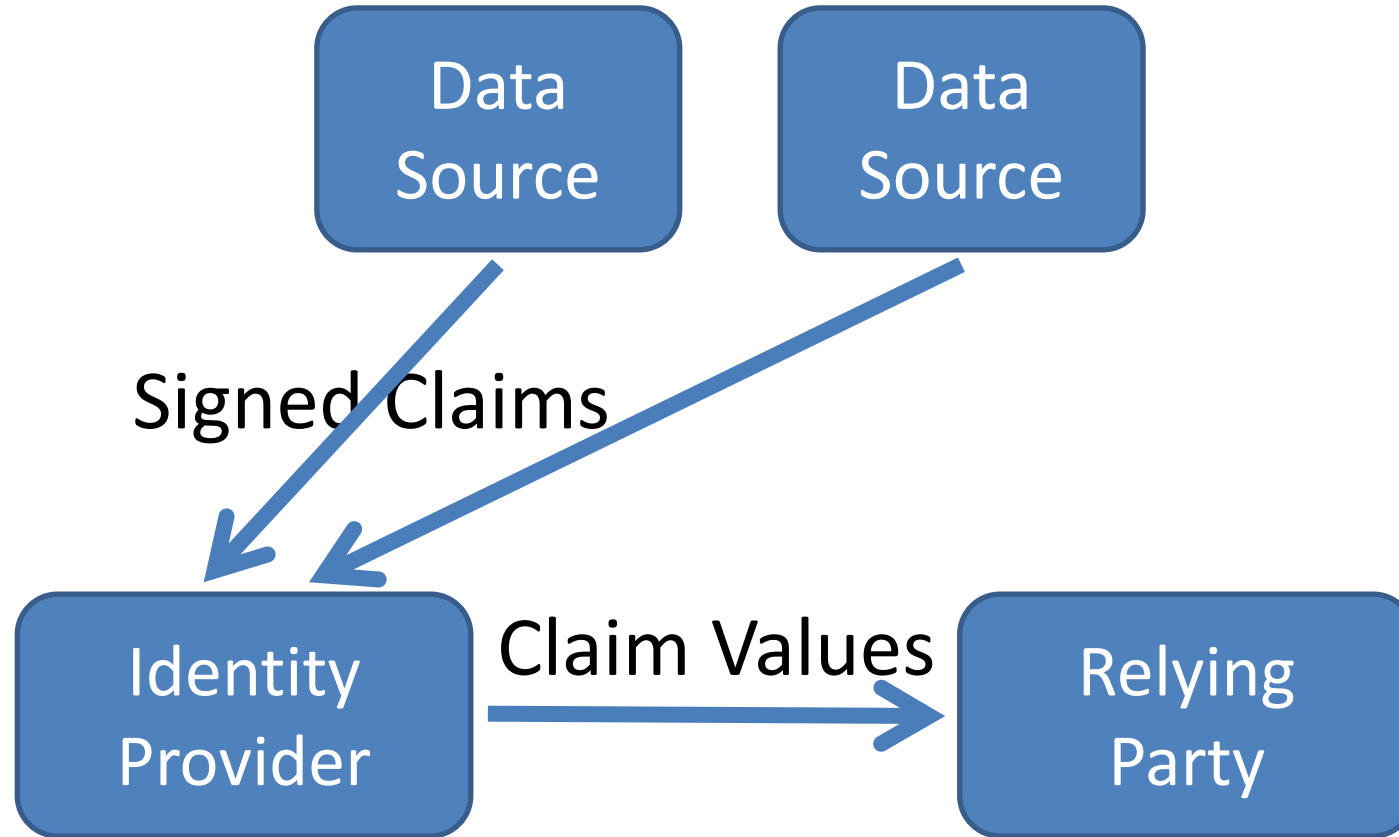- Mike Jones' Blog
  - https://self-issued.info/

Open Conversation

- How are you using OpenID Connect?

- What would you like the working group to know or do?

- *Slides will be posted at https://self-issued.info/*

BACKUP SLIDES

Aggregated Claims