Enabling Scalable Multi-lateral Federations with OpenID Connect

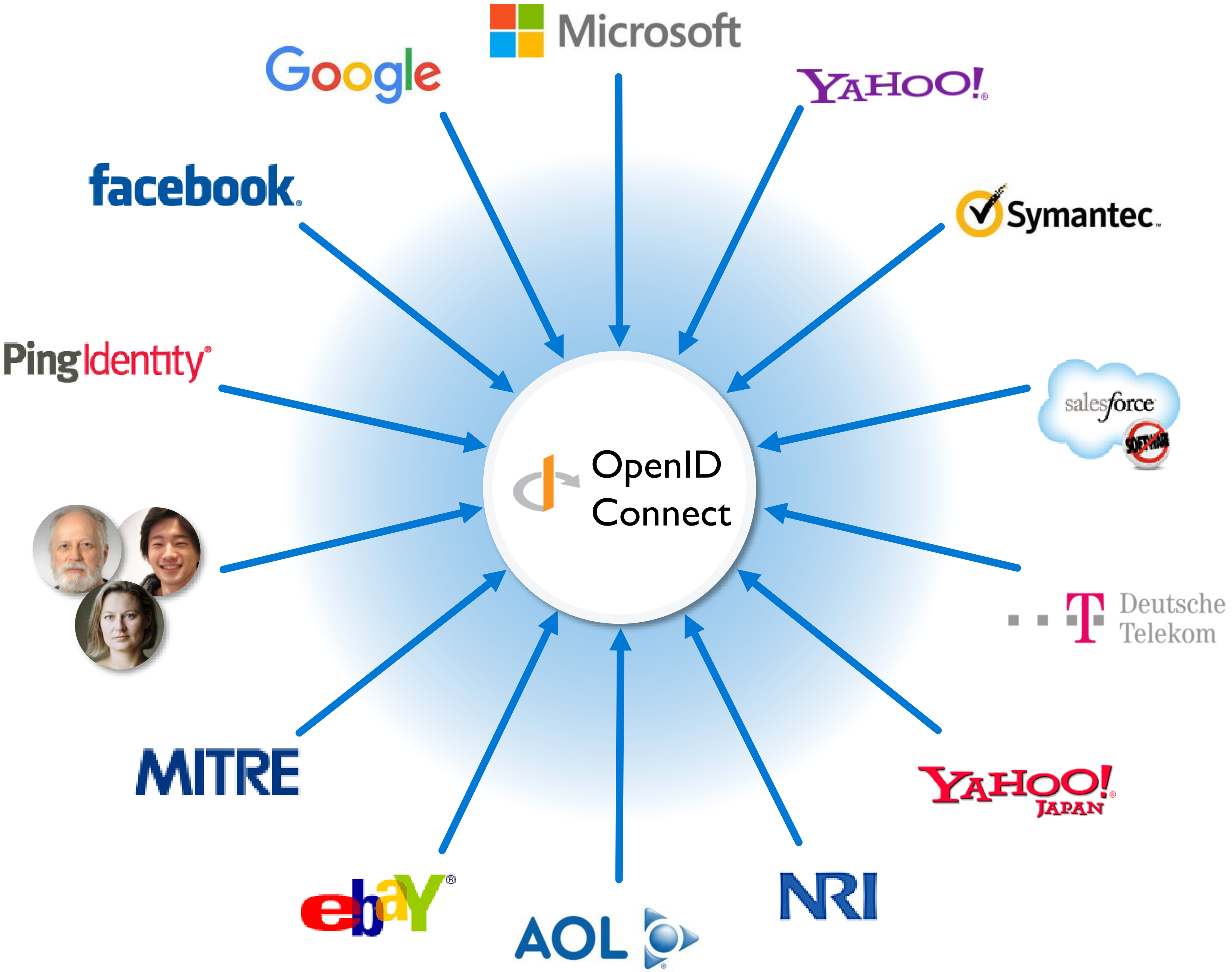
Michael B. Jones

Identity Standards Architect

Microsoft Corporation

With significant contributions from Roland Hedberg

WORKING TOGETHER



You’re Almost Certainly Using OpenID Connect!

If you log in with Android, Apple, AOL, Deutsche Telekom, eBay, Gigya, GSMA, Google, Janrain, KDDI, Microsoft, NEC, NTT, Okta, PayPal, Salesforce, Softbank, Symantec, Verizon, or Yahoo! Japan, you’re already using OpenID Connect.

Many other sites and apps large and small also use OpenID Connect.

Not a consumer brand

Rather, very widely deployed, simple, secure identity infrastructure

What has OpenID Connect Achieved?

Widely used for:

- Web apps
- Native apps
- Enterprise apps
- Cloud apps
- Financial apps

Over 160 certified deployments at https://openid.net/certification

Available for essentially all modern development platforms

Increasingly preferred by developers over SAML

Numerous Awards

- OpenID Connect won 2012 European Identity Award for Best Innovation / New Standard
- 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

eic
2018
12TH EUROPEAN IDENTITY & CLOUD CONFERENCE
European Identity & Cloud Award 2018

A Microsoft Perspective

At Identiverse in 2019, Alex Simons – Microsoft's VP of Identity Program Management, reported:

- Over 95% of all Azure Active Directory (Azure AD) authentications use OpenID Connect
- We're doing over 20 billion authentications per day

But what about Research and Education?

Research and Education sector has numerous large-scale identity federations

- Many national and regional federations
  - Such as SWAMID in Sweden and InCommon in the United States
  - Some have thousands of sites
- Inter-federations among dozens of federations, such as eduGAIN

These allow identities from any federation member to be used at relying parties from any federation member

- For instance, using a University of Washington account at CERN

BUT… today these are nearly all based on SAML 2

- Mostly using Shibboleth software

Significant OpenID Connect Interest in Research and Education Sector

Research and Education OpenID Working Group

- https://openid.net/wg/rande
- Profiling OpenID Connect for use in R&E applications
- Including mapping EduPerson schema to OpenID Connect claims

Multiple OpenID Connect implementations for R&E world:

- University of Chicago Shibboleth Plug-in was an early implementation
- GÉANT OpenID Connect Shibboleth Plug-In
  - Now supported and distributed with Shibboleth software

Federation using OpenID Connect

Rest of this presentation describes how Federation is being achieved natively with OpenID Connect

OpenID Connect Federation specification

- https://openid.net/specs/openid-connect-federation-1_0.html
- Enables establishment and maintenance of scalable multi-lateral federations using OpenID Connect

Incorporates lessons learned from SAML-based federations

- Defines hierarchical JSON-based metadata structures for federation participants

Establishing Trust within a Federation

How do a Relying Party and an Identity Provider know that they're in the same federation?

- Important for trust, liability, accountability, and reliability

Shibboleth/SAML approach:

- Federation Operator polls participants for their metadata, concatenates it into a huge flat file, and distributes it to all nightly
- In production use, but brittle and not scalable
  - SAML world developing Metadata Query protocol to try to move away from this

New OpenID Connect Federation approach:

- Hierarchical metadata:
  - Organizations publish metadata about themselves
  - Federation Operators publish metadata about orgs
- Scalable, maintainable

Use of Hierarchical Metadata

Hierarchical metadata is an online graph data structure

Each federation participant publishes self-signed metadata about itself

Leaf members are at bottom of trust hierarchy

- Relying Parties
- Identity Providers

Organizations publish signed metadata about the members that belong to them

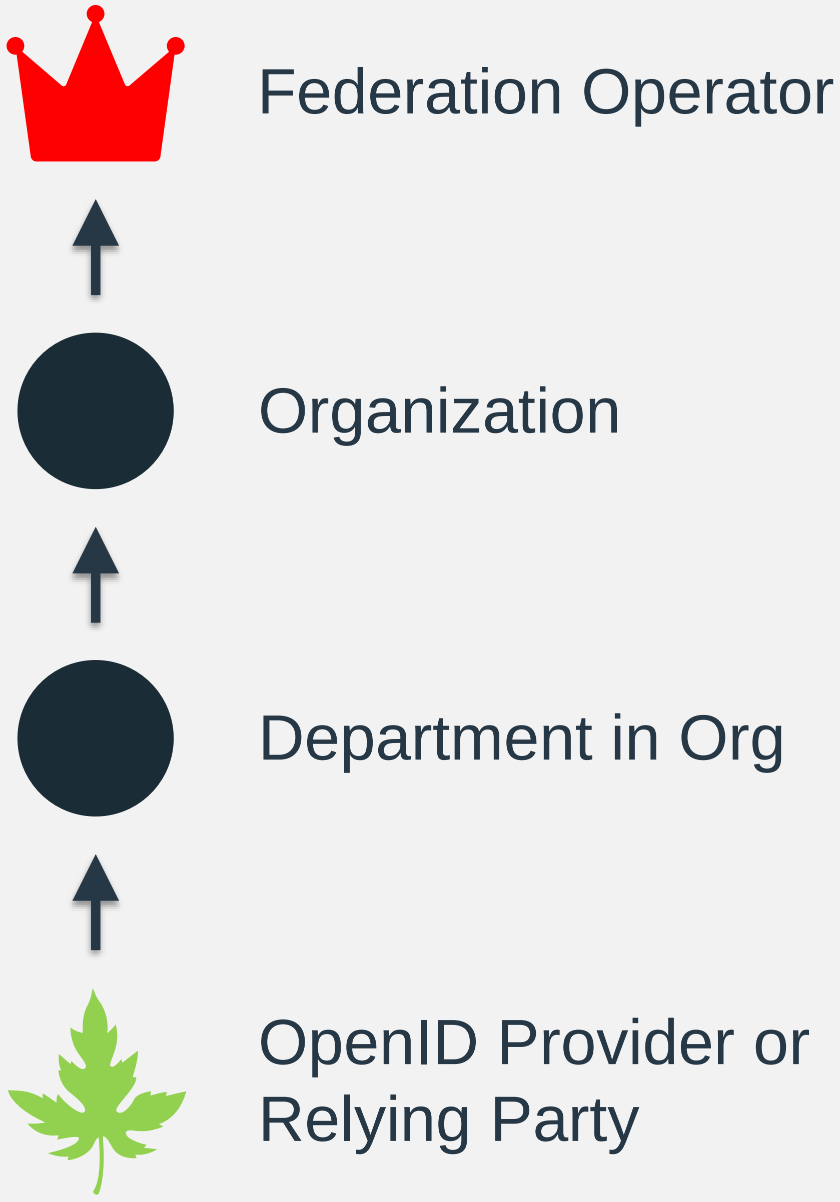
- Orgs may be multi-tiered, such as for departments within a university

Federation operators publish signed metadata about orgs

Inter-federations publish signed metadata about federations

Trust Chains

- Participants follow metadata trust chains from leaves up to common roots, verifying signatures
- Participants are members of a federation if a common trusted root is found
- Participants can be members of multiple federations



Federation Operator

Organization

Department in Org

OpenID Provider or Relying Party

Metadata Representation

Each metadata statement is a signed JSON Web Token (JWT)

- These are called ***Entity Statements***

They make statements about:

- The entity itself
- Keys used by the entity
- Policies applied to subordinates of the entity
- Other entities up the trust chain that they are willing to trust
  - This is how trust chains are followed up to federation roots

Example Entity Statement Body

Statement by Norwegian federation Feide about Norwegian university NTNU

Includes statement that eduGAIN inter-federation is above in the trust chain

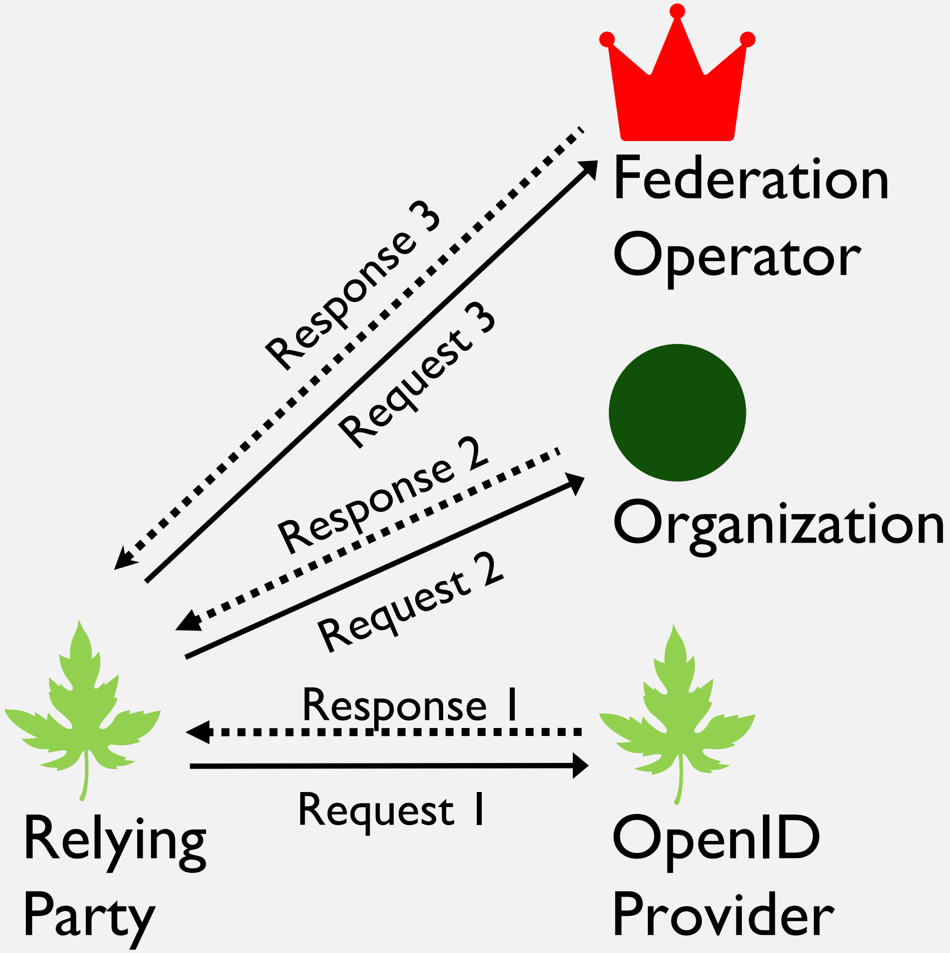
```
{
 "iss": "https://feide.no",
 "sub": "https://ntnu.no",
 "iat": 1516239022,
 "exp": 1516298022,
 "jti": "7l2lncFdY6SlhNia",
 "metadata_policy": {
    "openid_provider": {
      "issuer": {"value": "https://ntnu.no"},
      "organization_name": {"value": "NTNU"},
      "id_token_signing_alg_values_supported":
        {"subset_of": ["RS256", "RS384", "RS512"]},
   }
 },
  "jwks": {
    "keys": [
      {
        "e": "AQAB",
        "kid": "key1",
        "kty": "RSA",
        "n": "pnXBOusEANuug6ewezb9J_...",
        "use": "sig"
      }
    ]
  },
  "authority_hints": [
    "https://edugain.org/federation"
  ]
}
```

Following Trust Chains

Self-signed entity statement is first entity in trust chain

1. From the claim `authority_hints`, pick superior entity
2. Get superior's self-signed entity statement (using `.well-known`) and superior's view of subordinate (using Federation API)
3. Add to the trust chain

Repeat until the superior is a trusted trust anchor



OASIS STANDARD SAML

vs.

OpenID Connect

Appearing in a metadata file means you are part of a federation

Entities with trust chains up to the same trust anchor belong to the same federation

OASIS STANDARD SAML

vs.

OpenID Connect

An entity’s complete metadata set must be accepted by the federation operator for the entity to be allowed into the federation

The federation operator defines what is acceptable

Praise for the OpenID Connect Federation Approach

> “Given all my experience, if I were to redo the metadata handling today, I would do it along the lines in the OpenID Connect Federation specification.”

Scott Cantor

Shibboleth Author

identiverse® 2020

Policy Language for Entity Statements

Operators Defined

subset_of

one_of

superset_of

add

value

default

essential

Path length/name restrictions

Trust/certification marks

Applying Metadata Policies

Policies applied top-down from root to leaves of trust chain

Policies higher in the chain override those lower in the chain

For instance, a Federation Operator might specify that only a particular set of signing algorithms may be used

- Policies are applied to all entities in the federation

OASIS STANDARD SAML

vs.

OpenID Connect

It is rare that an entity belongs to more then one federation. Given eduGAIN, it is actually recommended that an entity only belong to one.

There is no drawback to belonging to multiple federations.

OASIS STANDARD SAML

vs.

OpenID Connect

There is no metadata negotiation

The RP proposes and the OP decides, subject to applicable policies from the trust chain

Client Registration Methods

Explicit

- Client performs standard OpenID Connect Dynamic Client Registration
- OP responds with an entity statement about the RP with metadata policy
- RP provides the OP with its self-signed entity statement in the client registration request
- Requires OP to keep state about the registered client

Automatic

- Client preforms no advance client registration. Instead, it sends an authorization request with `client_id` == `entity_id` using either:
    - a signed JWT Authorization Request (JAR)
    - a Pushed Authentication Request (PAR) using one of three client authentication methods
- OP fetches the RP's self-signed entity statement
- Doesn't require OP to keep state about the client

OpenID Connect Federation Past

First Implementer's Draft Approved, August 2018

Second Implementer's Draft Approved, January 2020

Spec refined based on discussions at multiple federation events

- NORDUnet, September 2017
- SURFnet, December 2018
- TNC/REFEDS, June 2019
- Internet2/REFEDS, December 2019
- OpenID Japan Workshop, January 2020

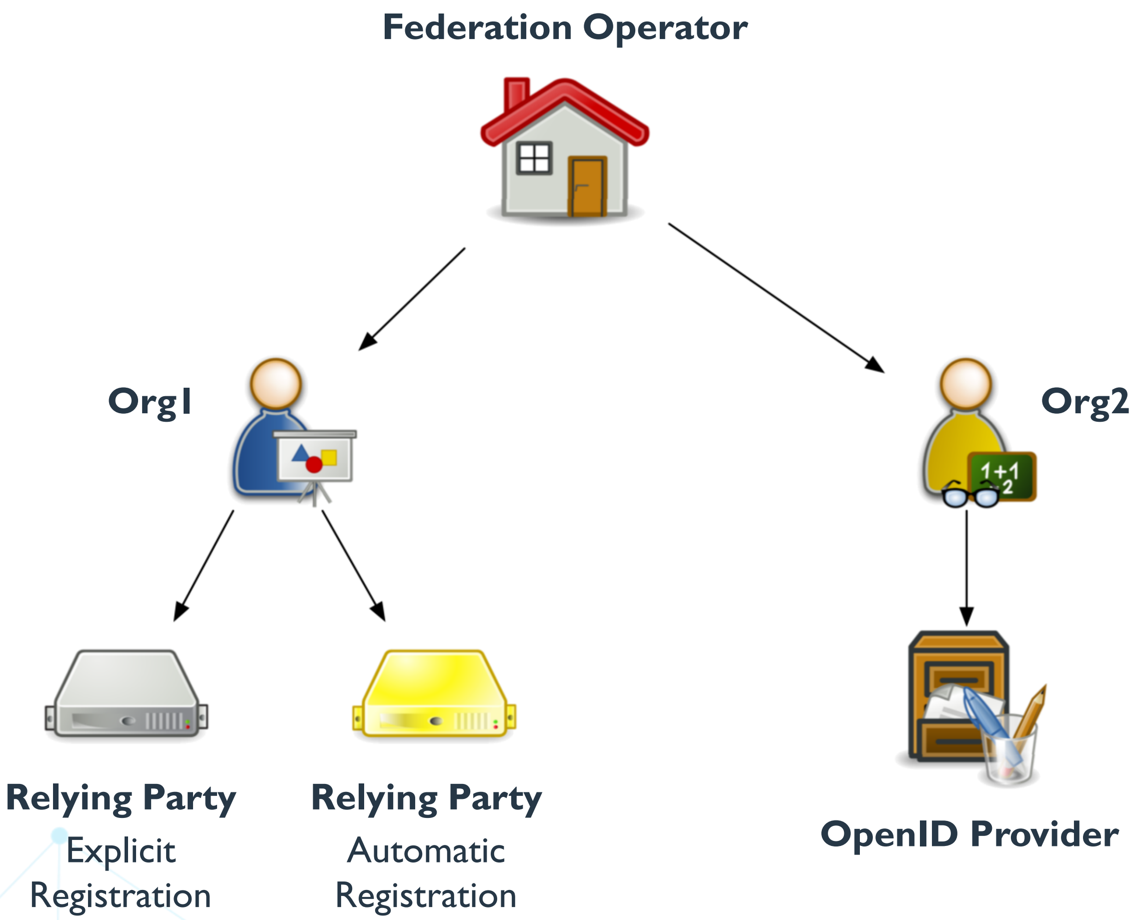
Hackathon with interop testing among multiple implementations

- Internet2/REFEDS, December 2019

First 2020 Federation interop testing event

- June 2020 (virtual)
- Spec updated to incorporate feedback from interop, July 2020

June 2020 Federation Interop: Test Setup



Federation Operator

Org1

Org2

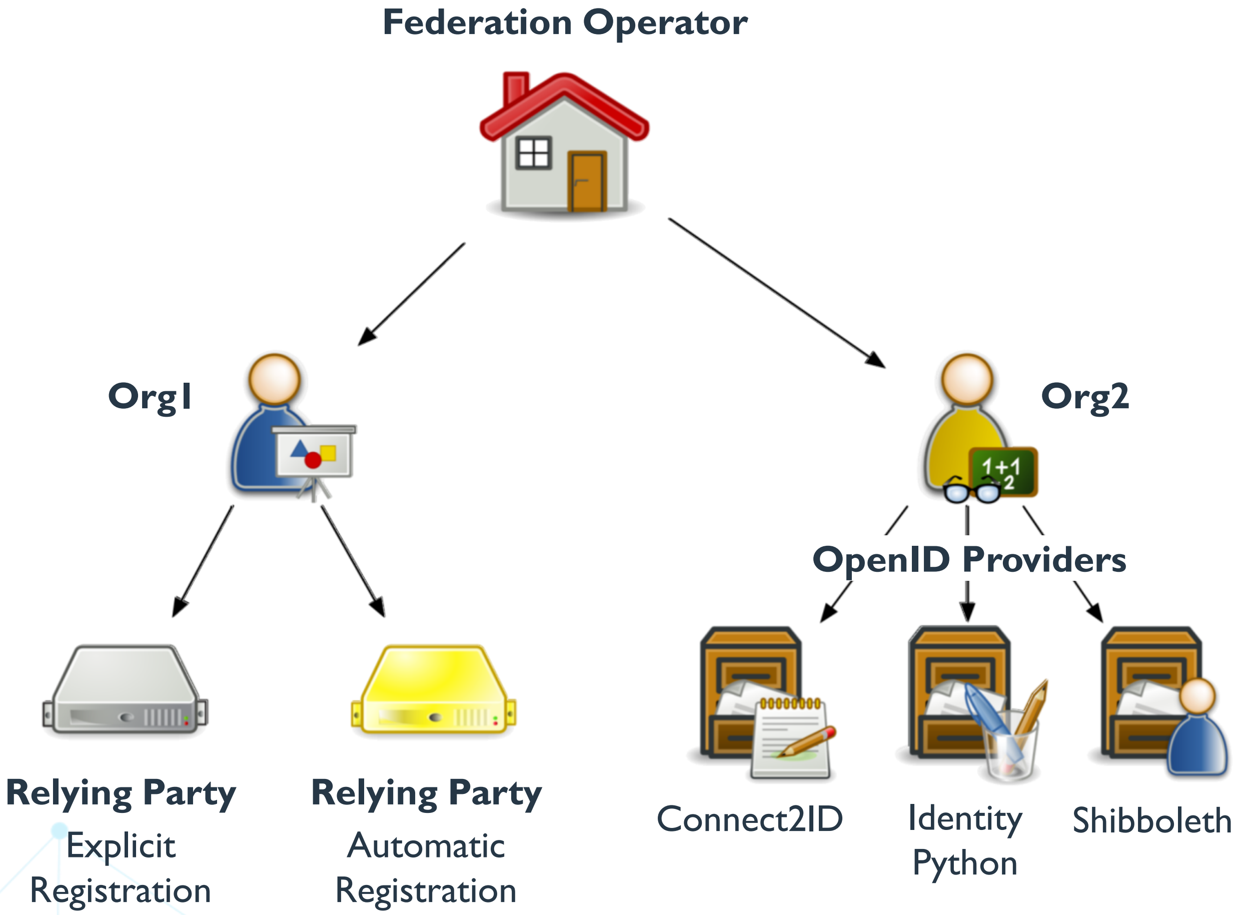
Relying Party
Explicit
Registration

Relying Party
Automatic
Registration

OpenID Provider

identiverse®
2020

June 2020 Federation Interop: Test Setup



Federation Operator

Org1

Org2

OpenID Providers

Relying Party
Explicit
Registration

Relying Party
Automatic
Registration

Connect2ID

Identity
Python

Shibboleth

June 2020 Federation Interop: Goal

Successfully complete negotiation process between OpenID Connect Providers (OPs) and Relying Parties (RPs)

Explicit Client Registration Steps

- Provider Info Discovery
- Client Registration
- Authorization Request
- Token Request
- UserInfo Request

Automatic Client Registration Steps

- Provider Info Discovery
- Authorization Request
- Token Request
- UserInfo Request

June 2020 Federation Interop: Results

	OP-c2id		OP-shib		OP-idpy	
	explicit	automatic	explicit	automatic	explicit	automatic
Provider Info Discovery	✓			✓	✓	✓
Client Registration	✗			✗	✓	✓
Authorization Request	✗			✗	✓	✓
Token Request	✗			✗	✓	✓
UserInfo Request	✗			✗	✓	✓

OpenID Connect Federation Future

OpenID Foundation is holding three Federation interop events in 2020

- Much like five interops were held for OpenID Connect
- June 2020 interop was the first of them
- Interop results will be used to improve the specification
- Contact Roland Hedberg roland@catalogix.se to participate
- Join OpenID Federation Interop mailing list
  - https://groups.google.com/forum/#!forum/openid-federation-interop

It's time for feedback from developers and early deployers

- Will you be one?
- Please read (and implement!) the spec and give us your feedback!

OpenID Connect Federation Resources

OpenID Connect Federation Specification

https://openid.net/specs/openid-connect-federation-1_0.html

OpenID Connect Page

https://openid.net/connect

OpenID Connect Working Group Mailing List

https://lists.openid.net/mailman/listinfo/openid-specs-ab

OpenID Blog

https://openid.net

Mike Jones' Blog

https://self-issued.info

Open Conversation

Where would you like to see OpenID Connect Federation used?

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

Please evaluate this session

Your feedback is important to us!

aka.ms/MicrosoftPostSession

More Microsoft sessions

identiverse 2020

Keynotes			
07/01 · 10:00 AM MST	Identity Standards: What's new, what's next?	Alex Simons	aka.ms/identiverse2020/simons
07/15 · 10:00 AM MST	Identity at scale	Sue Bohn	aka.ms/identiverse2020/bohn
Panels			
07/02 · 12:00 PM MST	A Balancing Act: Identity, Privacy, and Security in a Data Sharing Economy	Pamela Dingle	aka.ms/identiverse2020/dingle1
07/21 · 12:00 PM MST	The Skills and Experiences of Identity Practitioners	Pamela Dingle	aka.ms/identiverse2020/dingle2
Masterclasses			
07/24 · 10:00 AM MST	Manage and secure all your apps with identity as the control plane	Jairo Cadena; Jeevan Bisht	aka.ms/identiverse2020/bisht-cadena
08/05 · 12:00 PM MST	Upgrade your apps authentication from AD FS to Azure AD	Luis Leon Plata; Ramiro Calderon	aka.ms/identiverse2020/calderon-plata
Security & Zero Trust			
07/01 · 11:00 AM MST	A Zero Trust approach for today's world	Nitika Gupta	aka.ms/identiverse2020/gupta
07/14 · 12:00 PM MST	Identity Kill Chain · A hacker's eye view of how your systems get pwned	Alex Weinert	aka.ms/identiverse2020/weinert
07/16 · 10:00 AM MST	The science behind detecting compromised Identities	Dana Kaufman	aka.ms/identiverse2020/kaufman
07/28 · 11:00 AM MST	Identity governance for all your users made easier through analytics	Rahul Prakash	aka.ms/identiverse2020/prakash
Decentralized Identity			
06/29 · 12:00 PM MST	Distributed Open Identity · Self-sovereign OpenID · a status report	Preeti Rastogi; Nat Sakimura	aka.ms/identiverse2020/rastogi-sakimura
08/03 · 10:00 AM MST	Meet ION: An open, public, permissionless DID network	Daniel Buchner; Henry Tsai	aka.ms/identiverse2020/buchner-tsai
Boundaryless Identity			
06/23 · 10:00 AM MST	Customers and Partners · Seamless and secure experiences for every relationship	Robin Goldstein	aka.ms/identiverse2020/goldstein
07/07 · 10:00 AM MST	Identity for Firstline Workers · Transforming work for the next 2 billion	Steve Ball	aka.ms/identiverse2020/ball
Standards			
07/09 · 10:00 AM MST	Enabling Attributes of Self in Identity Systems	Bethan Cantrell	aka.ms/identiverse2020/cantrell
07/07 · 12:00 PM MST	Enabling Scalable Multi-lateral Federations with OpenID Connect	Mike Jones	aka.ms/identiverse2020/jones

Thank you.

Join our Identiverse Slack channel
#ask_Microsoft

Michael B. Jones

@selfissued

https://self-issued.info

Bookmark or subscribe

aka.ms/azureadblog

aka.ms/aad

aka.ms/azuread

@azuread

identiverse® 2020