OpenID Connect and OAuth in the R&E Community

IAM Online
Wednesday, December 12, 2018

Rachana Ananthakrishnan, Globus
Nathan Dors, University of Washington
Roland Hedberg, Catalogix
Davide Vaglietti, Consortium GARR
Albert Wu, InCommon/Internet2
OpenID Connect and OAuth in the R&E Community

Welcome!

Today’s IAM Online will explore the Trust & Identity initiatives and working group activities shaping the adoption of OpenID Connect (OIDC) and OAuth technologies within and for the research and education (R&E) community, particularly in support of multi-institutional academic collaboration.
Davide
OIDF R&E WG Chair
Consortium GARR

Roland
Software developer
Catalogix

Rachana
Head of Products
Globus

Albert
Federation Service Mgr
InCommon/Internet2

Nathan
Moderator
University of Washington
Objectives

Learn how to help ensure OIDC and OAuth deliver what R&E needs to sustain multilateral federations.

Learn how Internet2, REFEDS, GÉANT, and others are coordinating activities to influence standards.

Learn practical ways to navigate these activities and how and when to get involved.

Learn what actions to plan for in 2019, including how to contribute your time based on interests.
Landscape

In 2018, the FIM4R (Federated Identity Management for Research) initiative identified requirements that warrant further consideration of OIDC and OAuth, including non-web use cases and access delegation.

FIM4R paper categorizes the requirements according to types of constituents, all of which can influence how OIDC and OAuth are deployed:

Home organizations
Federations and eduGAIN
Research community proxies
Research service providers
Software developers
Standards bodies
AARC (Authentication and Authorization for Research Collaboration) Blueprint Architecture provides a reference architecture that enables the integration of identities from SAML-based federations into research communities.
AARC Blueprint Architecture has been adopted by research collaborations as a reference model enabling them to deploy ecosystems of research services and applications, including ecosystems of end services that rely on OIDC and OAuth.

**Landscape**

AARC Blueprint Architecture has been adopted by research collaborations as a reference model enabling them to deploy ecosystems of research services and applications, including ecosystems of end services that rely on OIDC and OAuth.
Landscape

Observers have noticed our large-scale SAML-based federations and related academic collaborations spanning many organizations.

The OpenID Foundation has welcomed the R&E community to help develop the OpenID Connect Federation 1.0 specification into a standard.
**Context**
- Objectives
- Landscape

**Activities**
- Working Groups
- Deliverables
- Impacts

**Perspectives**
- Developer
- Standards bodies
- Research community proxy
- Research service provider
- Federation operator

**Conclusion**
- Summary
- Recommendations

**Davide**
Working Group:
OIDC-OAuth Deployment

Sponsor:
InCommon Technical Advisory Committee

Chair(s):
Nathan Dors

Status:
Active - refining scope and deliverables

Location:
https://spaces.at.internet2.edu/x/jJiTBg
What’s the purpose of the working group?

Broadly, to share information, develop best practices, and guide standardization in support of multi-lateral federation. However, the objectives overlap with other working groups, so the scope is being refined for 2019.

What deliverables will this WG produce?

In 2019, we’re proposing the working group focus on OIDC deployment guides for the GÉANT Shibboleth OIDC Extension and the SATOSA proxy.

How will they impact implementations and R&E constituents?

They'll enable home organizations and others to add OIDC support to their Shibboleth IdPs, and understand the use cases it enables.
Working Group:
OpenID Connect for Research & Education (OIDCre)

Sponsor:
REFEDS

Chair(s):
Niels van Dijk

Status:
Active

Location:
https://wiki.refeds.org/display/GROUPS/OIDCre
What’s the purpose of the working group?

In addition to coordinating OIDC discussions, this year’s work focused on consistent ways to map identifiers and attributes between SAML and OIDC, in the context of attribute exchange in the R&E community.

What deliverables will this WG produce?

Currently, a white paper for implementation of mappings between SAML 2.0 and OIDC in R&E.

How will they impact implementations and R&E constituents?

They help developers resolve differences between OIDC and existing schemas like eduPerson and SCHAC, and provide implementations with configurations required by deployers in R&E.
Working Group:
Research & Education (R&E)

Sponsor:
OpenID Foundation (OIDF)

Chair(s):
Davide Vaghetti

Status:
Active

Location:
https://openid.net/wg/rande/
Working Group:
OIDF R&E

What's the purpose of the working group?

Develop a set of profiles and standards for OIDC that take into account the needs and current practices of IAM and FIM in the R&E sector; and to do so within the primary standards body developing standards for OIDC.

What deliverables will this WG produce?

At least three specifications are planned:

- One (or more) general OIDC profiles for the R&E sector that set standards for use of OIDC in terms of security, interoperability, and client requirements
- OIDC claims and scopes to be used in the R&E sector
- Entity metadata extension standard for OIDC
Working Group:
OIDF R&E

How will they impact implementations?

By specifying how to represent an R&E persona with OIDC, creating a profile to limit the number or options in the use of the protocol and creating a standard way to extend entity metadata, this WG will impact implementations in terms of:

- Ease of adoption
- Interoperability
- Security
- Baseline expectations and requirements

How will they impact R&E constituents?

This WG has been created inside the OpenID Foundation to let R&E communities and entities to work more closely with industry and vendors. This will help in creating better software and solutions that will cover the needs of the R&E sector, and expose other sectors to some of our practices.
Working Group:
Federation 2.0

Sponsor:
REFEDS

Chair(s):
Tom Barton and Judith Bush

Status:
Call for participation is open - initial meeting in January

Location:
https://wiki.refeds.org/display/GROUPS/Federation+2.0
Working Group:
REFEDS Federation 2.0

What’s the purpose of the working group?
To review the lessons we’ve learned from building and sustaining federations, and to consider how federation needs to evolve to support research and education.

What deliverables will this WG produce?
- Gather, analyze, and synthesize input from a wide range of sources and perspectives
- Articulate the value of R&E federation across constituencies and stakeholders
- Identify potential changes that may increase that value
- Recommend actions that R&E Federations and others can take to increase their value
**Working Group:**
REFEDS Federation 2.0

**How will they impact implementations?**

Too soon to say. This working group will evaluate several contingencies and potential changes to R&E federations, and the impact on implementations isn't known yet.

**How will they impact R&E constituents?**

Similarly, impacts depend on the recommendations. Actions undertaken could be substantial for eduGAIN, R&E federations, and other constituencies.
Roland Hedberg
Perspective(s): developer, standards bodies

Developers contribute to and draw from the work of standards bodies and their working groups.

Which of the aforementioned OIDC-OAuth working groups are you participating in and why?

All the above because so far they have been dealing with different pieces of the puzzle.

What’s the status of the OpenID Connect Federation standard?

It’s hard to say. The major parts I think are accepted but as always the devil is in the details.

The engine is there but some of the behavior is not nailed down.
What other OIDC and OAuth standards and profiles should the R&E community be aware of?

- The OIDF HEART and iGov profiles.
- OAuth PoP access token/token binding
- OAuth Distributed oauth/resource indicators

The IETF OAuth working group has decided clients SHOULD NOT use the “implicit” grant.

How significant is this to the development of secure implementations in the R&E community?

I think the R&E community would do well to stay away from “Implicit” grant.
In early 2018 you implemented your 2nd OIDC relying party library and lamented on Twitter that tests against a number of identity providers showed they had non-standard implementations.

Unfortunately a number of big identity providers seems to think they are above such mundane things as standards.

In 2018, the OpenID Certification program won the IDnext Identity Innovation Award. How do certification programs help developers?

A number of developers are using the test suite as an addition to their unit tests.

What can the R&E community learn from this program and apply to our activities in 2019?

Never ever buy or use anything that is not certified!!!
Developers also rely on feedback from those who deploy and use their software implementations.

In 2019, what OIDC and OAuth software projects will be the most relevant to the R&E community?

The JWTConnect RP libraries, the SATOSA proxy, and the GÉANT Shibboleth OIDC Extension.

What kinds of deployments and what type of feedback will be useful to these projects?

No software is done, it is honed and refined based on user experience.

Which is more important to developers: conformance tests or deployment guides?

Depends on type of developer.
Roland Hedberg
Perspective(s): developer, standards bodies

If you could travel into the future a few years to collect data on OIDC deployments, what would you want to observe and learn from the future to apply to what we’re doing in 2019.

- Special case federations
- Authorization services
- SAML out - OIDC/OAuth2 in
Rachana Ananthakrishnan
Perspective(s): research community proxy, research service providers

Globus Auth provides foundational IAM services to research communities
- OIDC Provider
- OAuth 2.0 Authorization service
- Federated logins
- Single hosted scalable instance

Use cases
- User login to applications
- Apps accessing services on behalf of users
- Services accessing services
- Service access as itself

Some metrics
- Federated identity providers: 500+
- Registered applications: ~1100
- Registered services: ~60
Rachana Ananthakrishnan
Perspective(s): research community proxy, research service providers

Why are open standards and the sustaining activities of federations key?

R&E is unique: collaboration across organizational security boundaries
- Accepted and trusted standards are pivotal to interoperability; enables business functions

Need end-to-end trust and communication
- E.g. User authorization error due to ePTIDs change?! What does it take to solve that?

Attributes are key
- Authorization policies often rely on ePPN
- For scale, other attributes are required in policy (e.g. provide access to all staff)
Rachana Ananthakrishnan
Perspective(s): research community proxy, research service providers

Federated logins
- InCommon IdPs via CILogon
- Project/division options: XSEDE, Argonne Leadership Computing Facility etc.
- Others: ORCID, Google.
- Globus Auth acts as proxies and issues tokens to applications and services

Baseline expectations
- Research and Scholarship attributes
  - Persistent, non-reassigned, non-targeted identifier, Name, Email, ePPN
- For other Identity Providers
  - No enforced requirement
  - Since authorization is managed by resource owner, they manage the trust relationship
Building applications
- Libraries and client tools, e.g. PyOIDC, OAuthLib
- Use of supported client code e.g. Atlassian products, Apache, etc
- Discovery of scopes

It is not all about browsers
- Native application/command line applications
- Automation and long running tasks
- Use of Service accounts

Supported grants
- Authorization code grant
- Client credentials grant
- Native app grant
- Implicit grant*

Rachana Ananthakrishnan
Perspective(s): research community proxy, research service providers
Rachana Ananthakrishnan
Perspective(s): research community proxy, research service providers

Securing services
- Register service
- Custom scopes
- Discovery of scopes

Service to service
- Dependent tokens
- User facing consents for the tree

User authorization at the service
- Identity, security context provided
- Authorization policy stored and managed by the service
How does Globus translates the capabilities of OIDC and OAuth into a useful set of features for customers?

- End users
- Developers
- Patterns and solutions
- Training and outreach
Rachana Ananthakrishnan  
Perspective(s): research community proxy, research service providers

Globus aims to streamline the onboarding of customers and their services into its ecosystem.

- Lots of outreach & training - patterns, examples, guides, sample code

In 2019, what changes, resources, and sustaining activities will help Globus customer integrations:

- Home organization (IdP) adoption of OIDC
- Community-supported libraries and tools
- “Common” ways of handling tokens
Albert Wu
Perspective(s): Federation operator

Readying InCommon Federation for OIDC/OAuth

InCommon Federation is about engendering trust and interoperability on a global scale.

Its goal is to streamline and simplify research and scholarly collaboration.

Engendering trust and interoperability is not protocol dependent.

SAML is a technical protocol Federations use to convey trust today.

InCommon Federation and SAML need not be synonymous.
### Albert Wu  
**Perspective(s): Federation operator**

**Readying InCommon Federation for OIDC/OAuth**

**As a Federation Operator:**

- Core sustaining federation activities are not specific to supporting SAML
  - Governance
  - Policy & Practices
  - Evolving infrastructure to be multi-protocol friendly
- Engaging international R&E, industry, and IDM community to foster common standards
  - Reduce duplication of efforts
  - Improve interoperability
  - Learn from deploying SAML - agreeing on the meaning of vocabulary is important to scaling interoperability
- Resource is limited. We need your participation to prioritize.

<table>
<thead>
<tr>
<th>Governance</th>
<th>For SAML</th>
<th>For OIDC/OAuth</th>
<th>Federation Role</th>
</tr>
</thead>
</table>
|            | ● By community, for community  
|            | ● Represented by InCommon and eduGAIN Steering + advocates such as FIM4R  
|            | ● Technology neutral |                  | Manage |
| Policy & Practices | ● Baseline Expectations  
|                      | ● SIRTFI  
|                      | ● Operations Agreements  
|                      | ● Privacy, Consent |                  | |
| Infrastructure & Tooling | ● Scalable, global endpoint discovery  
|                        | ● Metadata exchange  
|                        | ● System monitoring  
|                        | ● IDP/OP, SP/RP, Access Management Software |                  | Develop (in collaboration); Operate |
| Protocol (Grammar) | SAML | OIDC  
|                      | OAuth  
|                      | OIDC Federation |                  | Facilitate |
| Claims, Scopes, Entitlements (Meaning) | eduPerson  
|                           | SCHAC | OIDC Profile for eduPerson |
|                           | SAML2Int | | |
Albert Wu
Perspective(s): Federation operator

InCommon Federation
Engagements in OIDC/OAuth for R&E Development

- Need a root of trust
  - Protocol: (Roland’s / Andreas’ OIDC Federation work)
  - Policy/Practice: Federation 2.0 WG? Others?
- Need to map attributes / schemas / entity attributes into:
  - Claims, Metadata statements
  - Scopes
  - Some way to represent group membership or entitlements
    - REFEDS OIDCre, OIDF R&E? Others?
- Need an operational model that comes out of our experience running federations, combined with Roland and Andreas’ work
- Need translation between SAML and OIDC claims
  - REFEDS OIDCre WG
Albert Wu
Perspective(s): Federation operator

Suggestion for home organizations (IdPs)

● Participate in key working groups
  ○ REFEDS Federation 2.0 WG
  ○ OIDF R&E WG
  ○ OIDCre WG

● Ready your IAM data management and governance practices, e.g.,
  ○ Do you have a scalable strategy for managing non-human subjects and system-to-system access in a cloud-centric, API-driven, IoT ecosystem?
  ○ Do you have a source of persistent, non-reassigned, consistent-for-each-subject identifier?

● Attempt a view from a different perspective:
  ○ What do your researchers need?
  ○ What does your applications community need?

● Share your success (and challenges). Interoperable solutions only appear if we work together.
Albert Wu
Perspective(s): Federation operator

Suggestion for research service providers

- Be heard: engage in FIM4R and similar advocacy groups
- Participate in key working groups
  - REFEDS Federation 2.0 WG
  - OIDF R&E WG
  - OIDCre WG
- Proxies address near term needs. Don’t stop there. Without your voice, the federation won’t evolve to meet your needs.
- Share your success (and challenges). Interoperable solutions only appear if we work together.
Context
- Objectives
- Landscape

Activities
- Working Groups
- Deliverables
- Impacts

Perspectives
- Developer
- Standards bodies
- Research community proxy
- Research service provider
- Federation operator

Conclusion
- Summary
- Recommendations
Research communities and research service providers are successfully using OIDC and OAuth.

Some are doing so through research community proxies, platforms and ecosystems like Globus, and architectures based on the AARC Blueprint Architecture.
Summary

In today’s IAM Online, you’ve heard about the working group activities shaping the adoption of OIDC and OAuth within and for the R&E community, including development of new standards for trust and scalable multi-lateral federations… Now it’s over to you!

OpenID Foundation R&E WG
Next meeting: Monday, December 17

OIDC-OAuth Deployment WG
Next meeting: Tuesday, December 18

REFEDS OIDCre WG
Email list is active.

REFEDS Federation 2.0
Open call - initial meeting in January
Recommendations

Interested in standards development?
Join OIDF R&E WG
Contribute to OIDC specifications

Interested in evolving R&E federations?
Join REFEDS Federation 2.0 WG
Contribute input and ideas

Less time, but want to contribute?
Watch for milestone updates
Provide feedback on draft deliverables
Test OIDC software against your needs
Contribute to deployment guides

Running Shibboleth Identity Provider software?
Upgrade to V3.4.1 or newer
Consider your use cases, web and non-web
Test the GÉANT Shibboleth OIDC Extension
Provide feedback

Have thoughts, questions, or not sure what to do?
Contact CACTI (Community Architecture Committee for Trust and Identity) at cacti-inquiry@internet2.edu.
Thank you!

IAM Online wouldn’t exist without the contributions and participation of this community.

Thanks to today’s gracious presenters, Davide, Roland, Rachana, and Albert. We appreciate each of you and your collective perspectives.

Additional thanks to Internet2 and EDUCAUSE for supporting IAM Online, especially Dean Woodbeck and Emily Eisbruch.

We’re looking forward to more progress in 2019 - Happy New Year!
OpenID Connect and OAuth in the R&E Community

References

AARC (Authentication and Authorization for Research and Collaboration)
https://aarc-project.eu/

FIM4R (Federated Identity Management for Research)
https://fim4r.org/

GÉANT Shibboleth OIDC Extension
https://github.com/CSCfi/shibboleth-idp-oidc-extension

Globus - Platform-as-a-Service
https://www.globus.org/platform

InCommon OIDC/OAuth Deployment Working Group
https://spaces.at.internet2.edu/x/jJiTBg

JWTConnect libraries
https://github.com/openid/jwtconnect.io

OpenID Foundation Research & Education (R&E) Working Group
https://openid.net/wg/rande/

REFEDS Federation 2.0 Working Group
https://wiki.refeds.org/display/GROUPS/Federation+2.0

REFEDS OIDCre (OpenID Connect for Research & Education) Working Group
https://wiki.refeds.org/display/GROUPS/OIDCre

SATOSA Proxy
https://github.com/IdentityPython/SATOSA
Please evaluate today’s session

https://www.surveymonkey.com/r/IAMOnline-Dec2018
January 2019 IAM Online

Per-Entity Metadata Service on the Horizon
This IAM Online will cover the requirements for, status of, and next steps for deployment of the new InCommon Federation metadata service.

January 16, 2019
2 pm ET | 1 pm CT | Noon MT | 11 am PT
### Business needs, use cases, scenarios
What are researchers and research communities trying to do?

<table>
<thead>
<tr>
<th>Activities &amp; working groups</th>
<th>Standards &amp; profiles</th>
<th>Software implementation, services, guides</th>
<th>Deployments &amp; integrations</th>
<th>Operations &amp; sustaining</th>
<th>Use, results, outcomes</th>
</tr>
</thead>
<tbody>
<tr>
<td>What what activities and working groups are needed to support research collaboration? What deliverables will they produce?</td>
<td>What standards and profiles do we need in order to design useful software implementations and services?</td>
<td>What what software, services, and guides do deployers have to choose from? What guides and training help selection?</td>
<td>What's being deployed and how is it integrated? What are typical configurations, customizations, and anti-patterns for different participants/contexts?</td>
<td>How do deployers operate, improve, coordinate, and advocate for deployments? How are baseline expectations managed?</td>
<td>What were the results of our deployments? What new business needs emerge from real-world use?</td>
</tr>
</tbody>
</table>

#### Researchers
- GÉANT, Internet2, NREN
- Home organizations
- Research communities
- Federations
- Research e-infrastructures

#### Research communities
- Baseline expectations
- Code of conduct
- Operational plans
- Assessments
- Processes
- Funding plans
- Others...

#### Others...
- Shib IdP 3.4
- SATOSA
- JWT Connect
- Shib IdP 3.4
- Shib IdP 3.4
- Shib IdP 3.4
- Shib IdP 3.4
- Shib IdP 3.4
- Shib IdP 3.4