OpenID Connect in the R&E World: What is the State of Play?

Maarten Kremers
Technical Product Manager @ SURFnet
Task leader Next Generation T&I development @ GN4-2 Project
OpenID Connect in the R&E World: What is the State of Play?

- A strong and rising interest for using OpenID Connect as a protocol for identification and authentication.
- Given this interest, multiple parties in the R&E Trust & Identity area are working on the adoption and the impact that OpenID Connect has.
- Chartering an R&E working group under the OpenID connect Foundation to consolidate and reinforce the work.
Panel Session

- Nathan Dors, University of Washington
- Roland Hedberg, independent
- Niels van Dijk, SURFnet
- Chris Phillips, CANARIE
InCommon
OIDC-OAuth Deployment Working Group

Nathan Dors, Chair
University of Washington

Sponsor: InCommon Technical Advisory Committee

Website: https://spaces.at.internet2.edu/x/jiTbg

Conference calls: Bi-weekly, Tuesdays, 11am ET

Email: oidc-deploy@incommon.org

Charter / Rationale:
Share information
Develop best practices for deployment, configuration, and use
Guide standardization
Support multilateral federation
Standards & profiles
What standards and profiles do we need to produce useful software implementations and services?

- OIDC Conformance Profiles
- OIDC Discovery
- OIDC Core
- SAM12 OIDC Mapping
- OIDC R&E Profile
- OIDC Federation
- OAuth 2.0
- SAML2 OIDC Mapping
- OIDC Discovery

Software implementation, services, guides
What what software, services, and guides do deployers have to choose from? What guides and training help selection?

- GÉANT Shib OIDC Plugin
- Shib IdP 3.4
- SATOSA
- AppAuth SDK
- JWT Connect OIDC
- mod_oidc
- CAS
- Others...

Deployments & integrations
What's being deployed and how is it integrated? What are typical configurations, customizations, and anti-patterns for different participants/contexts?

- GÉANT, Internet2, NRENs
- Shib IdP 3.4
- SATOSA
- AppAuth SDK
- JWT Connect OIDC
- mod_oidc
- CAS
- Others...

Operating & sustaining
How do deployers operate, improve, coordinate, and advocate for deployments? How are baseline expectations managed?

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

Use, results, outcomes
What were the results of our deployments? What new business needs emerge from real-world use?

- Others...
Status: Active

Pitch:

“Create more value than you capture.”

Plug:
InCommon OIDC-OAuth Deployment WG Meeting
Pacifica Ballroom 4 / 5
4:00pm today
OIDC federation

• **Scope**
  
  • Define a standard for how to do multilateral federations using OpenID Connect
  
  • Present draft available at [https://github.com/rohe/oidcfederation/](https://github.com/rohe/oidcfederation/)
  
  • At least 2 independent implementations
  
  • POCs
Getting Involved

• **Where**
  • OIDF WG lists are main work area
    • R&E WG VC Meetings: to be weekly, TZ friendly for EU and Asia/Pacific
    • REFEDS OIDCre WG on ramp/incubation area for R&E items

• **Passive Participation:**
  • Join OIDF WG list and OIDCre and observe

• **Active Participation**
  • Join OIDF formally and be a voter (*strongly encouraged*)
  • Further steps:
    • Start learning more about OIDC and OAuth2 [https://spaces.at.internet2.edu/x/AluTBg](https://spaces.at.internet2.edu/x/AluTBg)
    • Get involved on activities or projects
    • Participate in prototyping and pilots
Goal

- In a not so distant future OIDC federations have replaced SAML2 federations and people are not lamenting about wanting back the ‘good old days’. 😊
REFEDS OIDCre

White Paper for implementation of mappings between SAML 2.0 and OpenID Connect in Research and Education

Niels van Dijk, SURFnet
REFEDs OIDCre Chair

REFEDS 39 @TechEx2018,
Monday 15th October 2018, Orlando
SAML and OIDC

- We have an ecosystem where SAML and OIDC will be living side to side
- Protocols bring similar, but also unique features, which adds challenges, yet creates opportunities
- Mixed implementation requires a myriad of choices to be answered
- Harmonize on how we implement both protocols side by side
- Answer some questions and capture best practices as we go along
White Paper for implementation of mappings between SAML 2.0 and OpenID Connect in Research and Education

Highlights:
• A discussion on how to map between identifiers used in SAML and OIDC;

• A recommendation for a basic attribute and claims mapping profile, which should be useable with unmodified OIDC clients which implement the standard claims of the OIDC core standard; and,

• A recommendation for an advanced mapping profile, which will leverage the full set of attributes made available by the eduPerson- and SCHAC schema but requires handling additional, (currently) non-standard claims and scopes.

Whitepaper:
Consultation

• The consultation will open on **15th October 2018** and close at **17:00 CET on 26th November 2018**.

• Participants are invited to review and comment on the proposed White Paper for implementation of mappings between SAML 2.0 and OpenID Connect in Research and Education.

• Following the consultation all comments will be taken back to the REFEDS OIDC(re) working group for review and if appropriate the White Paper will then be forwarded to the REFEDS Steering Committee for sign-off and publication on the REFEDS website as per the REFEDS participants agreement.

• Consultation landing page: [https://wiki.refeds.org/display/CON/Consultation%3A+SAML2+and+OIDC+Mappings](https://wiki.refeds.org/display/CON/Consultation%3A+SAML2+and+OIDC+Mappings)
Statement

- With OIDC being such an easy way to deliver and consume identity, what’s the future of SAML and our federations?
OIDF Working Group for OIDC R&E Profile

> **Scope**

- Develop profiles with specific requirements for
  - Security
  - multi-lateral trust
  - interoperability in the R&E sector.
- Specific set of claims and scopes related to R&E.
- Extensions to OpenID Connect entity's metadata.

> **Anticipated Duration**

- ~12-18 months
- commensurate with contributions, effort, running code.

Charter: https://github.com/daserzw/oidc-edu-wg/blob/master/charter.md
Signs of Success

> 1st class multi-lateral trust support in OIDC
  - Ubiquitously supported by platforms
  - Operational capabilities on premises, by vendors, & fed-ops
  - Training offerings to ramp community knowledge.

> Regardless of protocol
  - Interoperability of multi-lateral inter-federation trusts
  - Predictable attribute exchange
  - Parity of trustworthiness of endpoints

> R&E profile must work with existing OIDC libraries

> Stretch goal: User Experience
  - Login once, user is able to access SAML or OIDC resources transparently and simultaneously
Getting Involved

Where
• OIDF WG lists are main work area
• R&E WG VC Meetings: to be weekly, TZ friendly for EU and Asia/Pacific
• REFEDS OIDCre WG on ramp/incubation area for R&E items

Passive Participation:
• Join the OIDF RandE WG list & the REFEDS OIDCre and observe

Active Participation
• Join the OIDF formally and be a voter
• Get involved on activities or projects
• Participate in prototyping and pilots
More information

OIDF R&E WG
• mailinglist: http://lists.openid.net/mailman/listinfo/openid-specs-rande

REFEDS OIDCre
• wiki: https://wiki.refeds.org/display/GROUPS/OIDCre
• mailinglist: https://lists.refeds.org/sympa/info/oidcre