Research and Education profiles for OpenID Connect

Davide Vaghetti, OIDF R&E WG (chair), eduGAIN, GARR
Maarten Kremers, OIDF R&E WG, GN4-3 WP5 Task 4 (lead), SURFnet

Tallinn, June 19th 2019

The OIDF Research and Education working group

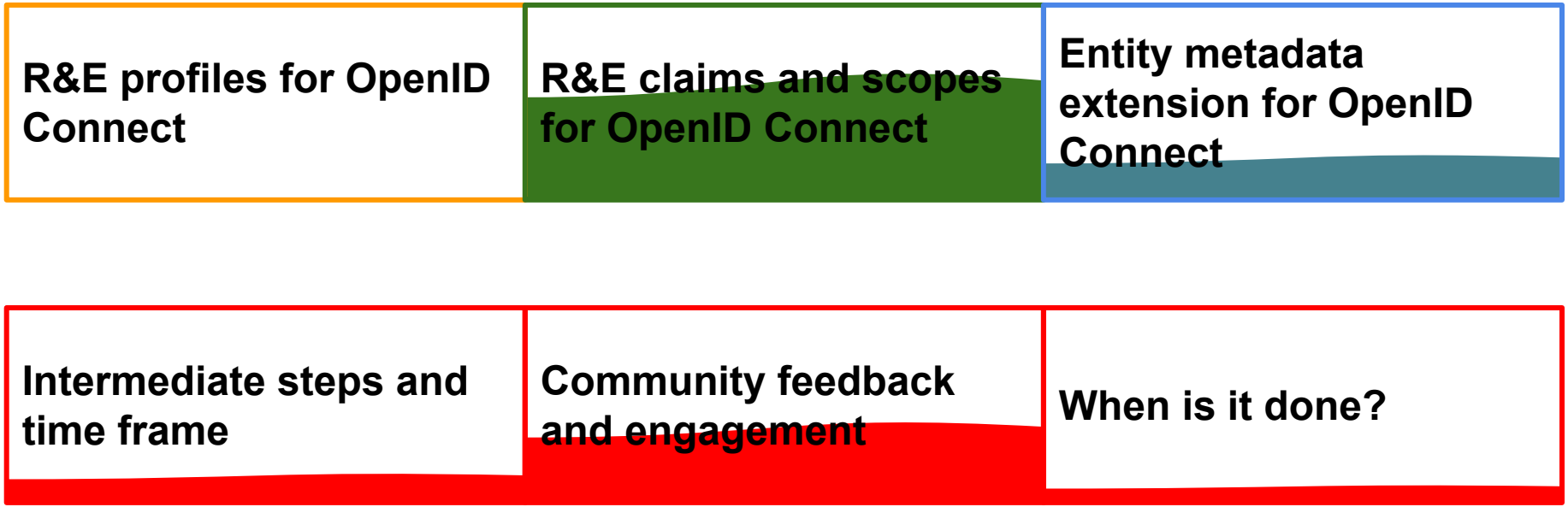
- Research and Education sector has been doing IAM and FIM (Federated Identity Management) for many years.
- Standards, specifications and profiles has been created around two major technologies: LDAP and SAML.
- Meet the raising demand for OIDC and OAuth2 in the current R&E IAM and FIM landscape.
- We want to work with the industry to create a set of specs and profiles that will ease the use of OIDC and OAuth2 in the R&E sector.

Work planning: specifications, schedule, commitment

R&E profiles for OpenID Connect	R&E claims and scopes for OpenID Connect	Entity metadata extension for OpenID Connect

Intermediate steps and time frame	Community feedback and engagement	When is it done?

Work done so far



Entity metadata extension for OpenID Connect

Why we need to extend the OIDC entities metadata?

- **No way to specify contact types**: `contacts` is a simple list/array of string, while in R&E we have administrative, technical contact types plus a security incident response one.
- **No entity tagging**, or to declare that an entity belong to a specific category, nor that an entity supports and recognizes an entity category.
- Implementing the most common policy frameworks used in the R&E federated identity context [R&S EC, CoCo, SIRTFI] relying on existing OIDC metadata is challenging, if possible anyway.
- The final target is to extend the set of claims used to describe entities in a standard and community blessed way --- not just the R&E community.

Entity metadata extension for OpenID Connect

Work done so far

- Considered two different approaches:

    1. An extension claim that will host a structured JSON Object.
    2. Create new claims as they are currently needed to implement the R&E policy frameworks.

What's next?

- Cannot work it in parallel with the other spec, so it has been paused until the R&E claims and scopes spec is published.

R&E claims and scopes for OpenID Connect

What we need to define

- Affiliation, groups and role information.
- A set of claims and scopes to specifically support the schemas and the specifications currently employed in R&E:
  - eduPerson.
  - SCHAC.
  - Research and Scholarship Entity Category attributes set.
- User identification use cases tailored to R&E.

R&E claims and scopes for OpenID Connect

Registered claims

IANA JSON Web Token Claims registry

Public claims

collision-resistant namespace:

- Domain names
- Object Identifiers
- URN

Private claims

Specific agreements between provider and relying party.

R&E claims and scopes for OpenID Connect

- Started leveraging the REFEDS OIDCre SAML-OIDC mapping white paper:
  https://wiki.refeds.org/x/BYBRAg

- Drafted synthetic ways to represent an OIDC public identifier for account linking, two proposals:
  - as a string: `iss!sub`
  - as a compact JWT:
    `{ “iss”:”https://donotoverload.this”, “sub”:”compact JWT”}`

- Drafted use cases for user identifiers:
  - targeted identifier (i.e. pair-wise).
  - globally unique identifier.

  IMPORTANT: The `sub` claim format need to be specified.

Defining a set of claims to match the R&S EC attributes set

OIDC claim	Required	Notes	SAML Equivalent (if exists)
`name`	Required if `given_name` and `family_name` are not provided		[eduPerson, RFC2798] displayName
`given_name`	Required, along with `family_name`, if `name` is not provided		[eduPerson, RFC4519] givenName
`family_name`	Required, along with `given_name`, if `name` is not provided		[eduPerson, RFC4519] sn (surname)
`email`	Required	Note that SAML mail may be multi-valued, while OIDC is single valued as pointed out in OIDCre doc footnote 21.	[eduPerson, RFC4524] mail
`email_verified`	Optional		
`eduperson_scoped_affiliation`	Optional	(This is a bit long)	[eduPerson] eduPersonAffiliation
`sub`	Required	It MUST be a public subject_type. It MUST be coupled with the `iss` to work as a *shared user identifier*	[subjid] OASIS SAML Subject Identifiers
`iss`	Required		

R&E claims and scopes for OpenID Connect

Interesting spin-off discussions

- *Where should I get my claims?*
  - ID Token vs userinfo endpoint.
- *OIDC missing subject type:*
  - The case for an OIDC ephemeral subject.

All you need is ID Token

The WLCG community expressed the needs for an ID Token filled up with all the needed claims to represent the users in order to:

- **avoid a second call** to the userinfo endpoint to retrieve the claims.
- have **all the authorization information in the ID Token** (scope) and use it as a **bearer token** with unregistered resources.

At the same time **the ID Token MUST be kept small**, and possibly **less than 2048 bytes**, which appears to be the hard limit of some implementations.

The WLCG community also defined two additional claims to deal with `group` and to start `ver`(sioning) the tokens.

The case for an OIDC ephemeral ID

WHY: There are use cases for an ephemeral or transient identifier.

WHAT: OpenID Connect has only **stable** (read persistent) subject types:

- `public`, same sub for all RPs.
- `pairwise`, a unique sub per RP.

HOW: We are drafting a proposal to add a **new subject type** to define an ephemeral identifier in OIDC.

WHERE: The discussion is happening on the A/B Connect mailing list.

R&E claims and scopes for OpenID Connect

What's next?

1. Publish a complete draft of the specification by the end of the summer.
2. Ask for feedbacks and comments in two main places: inside the OpenID Connect community, and in the REFEDS and eduGAIN communities.
3. Implement the due changes to the specification.
4. Repeat points 2 and 3 in short cycles (as per the charter).
5. Publish the draft.

WG tools: repositories, wikis, trackers

https://github.com/daserzw/oidc-edu-wg/

References

- The R&E WG web-page on the OpenID Foundation site
  https://openid.net/wg/rande
- R&E WG presentation at OIDF Workshop at VMWare (Oct 22 2018):
  https://bit.ly/2JPT30Z
- Wrap-up of R&E OIDC Panel Session at Internet2 TechEx 2018:
  https://bit.ly/2SUPDOC
- Who proposed this working group and why:
  https://bit.ly/2PNu8Az

QUESTIONS?

davide.vaghetti@garr.it

GÉANT

Networks · Services · People

www.geant.org