2021-02-09 R&S 2.0 Notes

Attendees
- Heather Flanagan
- Nicole Harris
- Christos Kanellopoulos
- Miroslav Milinovic
- Alan Buxey
- Björn Mattsson
- Scott Cantor
- Andrew Morgan
- Robert Smith
- Peter Brand
- Licia Florio
- Pål Axelsson
- Marina Adomeit

Pre-reading
- schacHomeOrganization (from SCHAC 1.5.0):

  Specifies a person’s home organization using the domain name of the organization. Issuers of schacHomeOrganization attribute values via SAML are strongly encouraged to publish matching shibmd:Scope elements as part of their IDP's SAML metadata. Relaying Parties receiving schacHomeOrganization values via SAML are strongly encouraged to check attribute values against the Issuer's published shibmd:Scope elements in SAML metadata, and may discard any non-matching values.

  Draft spec for R&S 2.0

Agenda
- Recap of consensus so far
  - The FAQ will be revised to offer clarity on the term "affiliation" (see Research and Scholarship FAQ) and editorial changes made to the spec to make it more clear (see https://docs.google.com/document/d/1xXMvMV2_iYZBcejVrIlIABrp7TkTk7Tu9sRcpY22g/edit)
  - eduPersonScopedAffiliation will become a required value
  - R&S will require privacy statements
  - Encouraging the use of eduPersonAssurance requires further discussion with the Assurance Working group
  - subject-id should be listed as the new identifier, but the spec would include migration requirement where ePPN would be passed, regardless of reassignment status
- review of Draft R&S 2.0 text
- schacHomeOrganization - include in the R&S bundle or not?
- Next steps

Notes
- Recap of consensus so far
  - The FAQ will be revised to offer clarity on the term "affiliation" (see Research and Scholarship FAQ) and editorial changes made to the spec to make it more clear (see https://docs.google.com/document/d/1xXMvMV2_iYZBcejVrIlIABrp7TkTk7Tu9sRcpY22g/edit)
  - eduPersonScopedAffiliation will become a required value
  - R&S will require privacy statements
  - Encouraging the use of eduPersonAssurance requires further discussion with the Assurance Working group
  - subject-id should be listed as the new identifier, but the spec would include migration requirement where ePPN would be passed, regardless of reassignment status
- review of Draft R&S 2.0 text
  - We do need more feedback on the mapping of eduPerson-defined attribute names to OIDC that Scott used in the spec; these will be the defaults in Shibboleth. There is no standard that covers this; deployers of the Shibboleth software can remap this as they want. The research community is talking about having their own mapping.
    - Christos will reach out to Niels and other OIDC deployers to share this direction and get feedback. Suggestions from the mailing list.
  - More may be needed to be clearer about the OIDC sub-claim since those could be public/shared or private/pairwise in OIDC
  - Will we lose traction as we encourage migration? Or will we see organizations stay at v1? Past track record suggests we’d need traction from the fed ops to encourage adoption. The OIDC detail may be a way to encourage adoption since it’s missing today.
  - Regardless, this will require SPs to re-map identifiers (ePPN, subject-id) and if an organization can’t do that, then there are other issues.
  - Would people support both versions at the same time? Yes, but there is still the re-map challenge. An IdP can assert both by supporting each category's requirements (same as always, e.g. with supporting R&S and CoCo at the same time).
What would the transition look like? Do we have a cut off date? Or do we say this is what R&S is (not two versions) and tell people they need to migrate over a set period. Given we have two version of the spec maybe thinking of this as a migration isn’t right at all. There are two different sets of requirements; they do overlap significantly, but they are different. If an SP says they support v1 and v2, and they are saying to send both because they’re in the middle of the migration, then they drop v1 and say they only want the one identifier. Maybe the versions themselves are enough to be a signal for what stage of migration the systems are in so we don’t have to call out backwards compatibility support in the v2 specification. This would also allow us to remove some of the time limitations stated in the v2 draft. This means ePPN and targeted ID would both be removed from v2.

Poll: We should not include migration details in the v2 spec. We do need migration information, though, it just shouldn’t be in the spec itself. Agreement that putting dates and timelines in the spec should be avoided.

- Scott will update the spec to remove some of that migration detail
  - Scott has made the changes as discussed so far, and also included a proposal on how to incorporate SAML and OIDC concrete attribute definitions. This was something done before, but there were concerns that people would have difficulty tying in the abstract attribute information with the specific attribute details in the various protocol sections.
  - No substantive changes to the SAML section beyond the subject-id addition; has not included pairwise-id as that may be too large a change.
  - Also made minor changes to requirements for SP and IdP to help support migration.
  - The OIDC section is somewhat a placeholder; needs review and references (OIDC Core)

Discussion

- Do we need a dispute resolution process in the spec itself (it exists in the supporting docs)? We can perhaps point to it, but don’t include the details in the spec
  - Poll: Yes, 30%; No, 70%; Need more info, 0%

- schacHomeOrganization - include in the R&S bundle or not?
  - Christos has the requirement to know what organization as user is coming from. Scopes from scoped eduPerson attributes may not give the necessary “assurance”. In one collaboration, this is used to construct the user id. We would need to be able to say that scope always maps to the domain of the organization. There is a complication that most organizations have more than one domain name (though that affects attributes “scopes” equally as sHO).
  - Scope is similar to sHO, and there are some situations where there is a school may have departments with their own domain name (e.g., harvard.edu has a central IdP, but Harvard Business School (hbs.edu) is part of Harvard and has its own domain name)
  - the subject-id is scoped in SAML: you will likely get the “one true public suffix” that the organization uses from that in most cases
  - Organizational identity has been an issue for a long time now (DNS domains are just a stand-in for solving the real problem)
  - What is the extent of the use case that having this would impact? Does every IdP in the world need to start supporting SCHAC to solve this for the given set of SPs? The growth of eduID systems may see the requirement for this grow. If we can put in R&S that the scope represents the organization, then it doesn’t need to be sHO.
  - Many academic federations, including the largest one on the planet (UKF) that also has the most publishers registered, have been using the scope from ePSA as a contract identifier of sorts (to manage access to institutionally licensed resources) for a long time now. The claim that the “scope” portion of ePSA (or of other attributes defined as “scoped”) does not properly identify those institutions seems unfounded that way.

- Next steps
  - Focus on the OIDC section
  - Come back to the need for organization info (scope? schacHomeOrganization?) if not resolve on the list

Action items

- Christos Kanellopoulos will reach out to Niels and other OIDC deployers to share the proposed 2.0 OIDC attribute direction and get feedback.
- Scott Cantor will update the draft spec to remove migration detail