2021-01-22 R&S 2.0 Notes

Attendees

- Andrew Morgan
- Adam Snook
- BjOrn Mattsson
- Alan Buxey
- Alex Stuart
- Bas Zoetekouw
- Christos
- David St Pierre Bantz
- Jens Jensen
- Jri Pavlik
- Miro
- Scott Cantor
- Nicolas Liampotis
- Heather Flanagan

Agenda

Recap

- Consensus achieved within the working group on the following items (noting that all spec changes will need to go through the full community consultation process before being finalized)
    - 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_tYZBcejfVrItLlABprC7TkkTu9sRcpY22jg/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
- Notes capturing the above can be found in 2020-12-17 - Notes, 17 December 2020 R&S call and 2020-12-03 Notes 3 December 2020 R&S call

Identifier issue

From R&S 1.3

> where *shared user identifier* is a persistent, non-reassigned, non-targeted identifier defined to be either of the following:
>
> 1. `eduPersonPrincipalName` (if non-reassigned)
> 2. `eduPersonPrincipalName` + `eduPersonTargetedID`

From the eduPerson (202001)

> *NOTE: eduPersonTargetedID is DEPRECATED and will be marked as obsolete in a future version of this specification. Its equivalent definition in SAML 2.0 has been replaced by a new specification for standard Subject Identifier attributes [https://docs.oasis-open.org/security/saml-subject-id-attr/v1.0/saml-subject-id-attr-v1.0.html], one of which ("urn:oasis:names:tc:SAML:attribute:pairwise-id") is a direct replacement for this identifier with a simpler syntax and safer comparison rules. Existing use of this attribute in SAML 1.1 or SAML 2.0 should be phased out in favor of the new Subject Identifier attributes."*

Issues Raised on Previous Calls

1. One of the reasons R&S supports ePPN and ePTID is that it was targeting applications that were broken because they only allow for a single identifier to identify an individual (the “one field for everything” approach). That’s why ePPN was the chosen identifier, because it was traditionally a user-friendly identifier and so suitable for the one-size-fits-all use case, as long as you ignore reassignment. ePTID was added to address reassignment. Those applications failed miserably if they only had ePTID.

   Is this still an issue? Do we still need to support the one-size-fits-all approach? If we can chose a common, opaque identifier, with an understanding that you want the additional personalization, we can do that.

    - One opinion: time is right to do this, and R&S is the right place to do this first.
    - Second opinion: this is a question for the SP. Are they ready for R&S to move to a more opaque identifier? There’s no incentive for an IdP to make their identifier better unless there’s a demand by the SPs.

        - Based on the responses from the SPOG list, SPs do not handle identifier reassignment in any standardized manner. The level of automation in responding to this seems to depend entirely on the size of the SP and how big their IT budget is
2. Providing a migration path for changes in R&S

Notes

If the requirement is to have an single identifier that is user friendly and able to route email, then there are no changes we can make here, and we need to convince people to not reassign it. There is also concerns that it will be too difficult to change this because of existing implementations, because implementations will need to re-key. If we are going to change it, we do have a clear target to move to.

Note that we are also seeing a number of services moving to OIDC, and they are relying on "sub". We can make a similar change to rely on a subject ID.

Poll one: replacing both ePPN and ePTID with a common, opaque identifier: 57%, yes; 36%, no; 7%, more info

- biggest concern is the migration; if ePPN works in place, then why should they change it?

If we focus on the "ePPN+ePTID" can we change that to a SAML subject identifier?

- the primary identifier is ePPN, and it should never be reassigned
- the purpose of the R&S language is to provide a non-targeted, non-redirected attribute
- we do need a correlatable identifier
- subject-id is a better choice for our purposes

What can our migration path look like?

- old services can continue to use ePPN, but new services can use public - this does not encourage existing SPs and IdPs to actually migrate
- we need to be clear on goal state and offering that migration path as to what's expected

Targeted vs non-targeted

- Privacy policies are a requirement, and we are restricting who can use R&S, so we shouldn't have to worry about non-targeted identifiers.
- Alternatively, if you do want to allow for non-targeted, that can be signaled in the subject-id; this could be signaled in the spec, but it would be a bit more complicated

Poll two: R&S 2.0 should offer ePPN if not reassigned as one option, and SAML subject-id as the second option: 71%, yes; 29% no

- 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

Poll three: 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: 69%, yes; 15%, no; 15% need more info

- one concern about the "regardless of reassignment status"; would prefer to keep what we do today, AND require subject-id
- another concern is that we should accommodate subject-id and pairwise-id

Action item

- [x] Scott Cantor and Heather will work on draft text to model the above change (see Poll three) and bring that back to the next call

For our next call:

- schacHomeOrganization - include in the R&S bundle or not?
- review of draft R&S 2.0 text