Consultation: SAML2 and OIDC Mappings

Consultation Closed

Please note this consultation is now closed

Background

The goal of this REFEDS White Paper for implementation of mappings between SAML 2.0 and OpenID Connect in Research and Education is to provide a well understood and consistent profile for implementing mappings between the SAML 2.0 and OpenID Connect (OIDC) protocols, in the context of use cases in Research and Education.

It describes how to map identifiers and commonly used attributes into scopes and claims for use with the OIDC protocol, and vice versa.

The document contains three main sections:

- 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.

The White Paper has been prepared by the REFEDS OIDCre Working Group and is now being made available for public consultation according to the REFEDS Participants Agreement.

Overview

The consultation was open from 15th October 2018 untill 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.

The document for the consultation is available as an attachment to this page. Background on the OIDC(re) Working Group is available. All comments should be made on: consultations@lists.refeds.org or added to the change log below. Comments posted to other lists will not be included in the consultation review.

Change Log

Change Log for the SAML2 and OIDC Mappings.

Number	Line / Reference	Proposed Change or Query	Proposer	Resolution
1	N/A	The PDF appears to lack line numbers, so that may complicate the feedback here.	Scott Cantor Fixed Scott Cantor - my bad, sorry (NH).	Resolved
2	L99, End of pg 4	Nit, suggest you s/SAML 1.0/SAML 1.0 and 1.1 for completeness.	Scott Cantor	
3	L113, Page 5	Nit, s/intent/intend	Scott Cantor	
4	Footnote 15	Nit, s/subjected/subject	Scott Cantor	
5	Line 169	I think the "spirit" of pairwise IDs in SAML would make it improper to just forward them into the Internet as an OIDC claim. They were always intended by the original Liberty work as "secret" in some sense and not to be shared gratuitiously, so I think turning a pairwise ID into a non-pairwise ID through a proxy is not really appropriate unless the proxy is "inward" facing. I don't think the document is presuming that though. If the intent here is rather that the proxy be stateful and do a mapping from the inbound SAML value to an outbound pub claim, that isn't coming across as clearly as perhaps intended. It may be a similar question in the opposite direction but I don't claim to speak for the "intent" behind the pairwise nature of the sub claim in OIDC, whereas I can speak for what the intent was in SAML.	Scott Cantor	
6	Line 211	Nit, s/taking/taken	Scott Cantor	

7	Line 337	Those are not in any sense "SAML Attribute names" as used by our community so I would suggest the mapping be limited to eduPerson/etc. and OIDC and leave the SAML part out of it. Essentially if you can deduce that a SAML Attribute corresponds to a given LDAP/X.500 Attribute Type, then your mapping can transit that hop and leave the SAML part implied. I disagree with string-based attribute names in a pretty deep way but if you're going to do that, I would just leave the non-string naming in SAML off to the side.	Scott Cantor	
9	footnote 15, P7	Nit, s/the the/the	Alan Buxey	
10	L34, P1	Define Research and Education - s/R&E/Research and Education (R&E)/	Alan Buxey	
11	L35, P2	s/R&S/Research and Scholarship (R&S) (then remove eventual definition bracket mention from L435, P21)	Alan Buxey	
12	L103, P5	s/. Reasoning is that/ because/	Alan Buxey	
13	Section 8	Please also include voPerson attributes, which I believe can be mapped just like eduPerson attributes.	James Alan Basney	
14	L277	'In addition it is discouraged to base preferred_username on a SAML attribute.' Can a small explanation be provided? Is it just discouraged to based it on an eduPerson attribute?	Patrick Radtke	
15	L279-L302	I'm unsure if these rules to determine email_verified would work across all schools. Specifically, a previous university employer of mine asserted for mail whatever the user entered in their profile, even if it was the email address of another user at the university. The IdP certainly wasn't asserting an email that has been verified to be in control of the end user, or validated in anyway. I'm not sure if this case is an anomaly or widespread, but since *email_verified* is not a required claim why guess at it's value? Or if you need to guess then perhaps if mail == eppn (which is quite common) and the eppn scope check is valid then assert true? otherwise you don't really know the institutional rules for how email addresses are picked, or what assumptions a downstream RP is making about email address and matching to existing accounts by email address and what security holes can occur.	Patrick Radtke	
		As part of the consultation a face to face session was held at Internet2 TechEx 2018 ACamp on Oct. 19, 2018. Notes from this meeting can be found here: https://docs.google.com/document/d/1cGuVn3k0-lJ3BzSvACm1gCk_MMftYyTKRxvwpqfpStI/edit	Niels, on behalf of ACamp participants	