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

Editor: Niels van Dijk, SURFnet

Abstract:

Table of Contents

This activity was carried out as part of the OpenID Connect for Research and Education (OIDCre)[1] working group of REFEDS[2]

`

The authors of this paper declare that they have not breached any IPR conditions by contributing material.

[1] https://wiki.refeds.org/display/GROUPS/OIDCre
[2] https://refeds.org/

1. Summary

The goal of this document is to provide a well understood and consistent profile for implementing mappings between the SAML 2.0[3] and OpenID Connect[4] (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[5] of the OIDC core[6] 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.

2. Acknowledgements

This document was the result of multiple consultations and could not have existed without the important input of many, as listed in the section "Authors and contributors".

[3] https://en.wikipedia.org/wiki/SAML_2.0
[4] http://openid.net/connect/
[5] http://openid.net/specs/openid-connect-core-1_0.html#StandardClaims
[6] http://openid.net/specs/openid-connect-core-1_0.html

3. Premise

The assumption in this document is that this recommendation will be implemented in a token translation service or in a proxy implementation which will bridge between the SAML 2.0 protocol and the OIDC protocol. Another use case is where a SAML Identity provider and an OIDC OP that are both front-ends to the same user database. Either will be used in the context of Research and Education.

Within the Research and Education sector, the SAML 2.0 implementations typically combine a number of specifications:

- The (SAML2Int) Interoperable SAML 2.0 Profile, a SAML 2.0 WebSSO Deployment Profile[7]
- The eduPerson Object Class Specification[8]
- The SCHema for ACademia (SCHAC)[9]
- Recommendations from REFEDs, including Research and Scholarship[10]
- SAML V2.0 Subject Identifier Attributes Profile [11]

Whenever a SAML-based solution is used in an international context, the following recommendations from eduGAIN should also be taken into account:

- eduGAIN attribute profile[12]
- eduGAIN Policy Framework SAML 2.0 WebSSO Protocol Profile[13]

With "SAML" we will in the remainder of this document refer to the SAML2 specification and the specific R&E profiles above. We exclude SAML 1.0

[7] https://saml2int.org, new version being developed at https://kantarainitiative.github.io/SAMLprofiles/saml2int.html

[8] http://software.internet2.edu/eduperson/internet2-mace-dir-eduperson-201602.html

[9] https://wiki.refeds.org/display/STAN/SCHAC

[10] https://refeds.org/research-and-scholarship

[11] http://docs.oasis-open.org/security/saml-subject-id-attr/v1.0/saml-subject-id-attr-v1.0.html

[12] https://technical.edugain.org/doc/GN3-11-012%20eduGAIN_attribute_profile.pdf

[13] https://technical.edugain.org/doc/eduGAIN%20SAML%202.0%20WebSSO%20Profile.pdf

specifically.

The authors have added a reference to the Subject Identifier Attributes Profile and added it to the mappings (later on in this document). Reasoning is that even though this standard is still young and has not been implemented broadly yet, its features are a very good match with the scenarios described in this document.

There is currently no specific profile for Research and Education with OIDC. Hence this document will reference the OIDC generic protocol specifications as provided by the OpenID Foundation.

Finally, this document is not describing a formalized implementation standard, nor does it intent to. At the time of writing it was felt that, even though several operators of production platforms were involved in the writing of this document, too little field experience exists to be able to write a standardization document at this time. As such the authors have chosen not to use formal RFC2119 wording throughout the document.

4. Mapping between identifiers in SAML and OIDC

Many implementations need to map identifiers from the SAML protocol into the OIDC protocol, or vise versa. Unfortunately, the definitions of commonly used identifiers in SAML, eduPerson, and OIDC do not align completely. In addition it should be noted that not all identifiers can be used literally between the two protocols, in many cases an identifier received is used as the basis for constructing a new one. In other cases, e.g. stripping the part behind the @ sign may suffice. This is dependent on implementation.

To assess and compare the identifiers, the following properties were taken into account:

- **Non-Reassignable**
  The identifier is not re-assigned according to the specification
- **Opaque**
  The identifier is opaque according to the specification
- **Persistent**
  The identifier is persistent over multiple sessions, according to the specification
- **Targeted**
  The identifier is distinct on a per SP/RP basis, according to the specification
- **Unique**
  The identifier is globally unique by itself, according to the specification. Typically, the identifier is scoped with a DNS domain associated with the issuer.

Table 1 compares identifiers as they are described in the SAML, eduPerson, and OIDC specifications. Based on the identifier properties, a mapping can be made on what would be compatible implementations, going between OIDC and SAML eduPerson.

In Table 1 the following symbols are used:
❎ identifier does not match property
✅ identifier matches property
❓ identifier may match property, but is implementation dependent.

Identifier	**Properties**				
	Non-Reassignable	Opaque	Persistent	Unique	Targeted
eduPersonPrincipalName (ePPN)	✗	✗ ?[14]	✓	✓	✗
eduPersonUniqueId (ePUID)	✓	✓	✓	✓	✗
eduPersonTargetedID (ePTID) and/or SAML2 persistent NameID	✓	✓	✓	✓[15]	✓
SAML2 transient NameID	✗	✓	✗	✗	✗
SAML subject-id	✓	✗ ?	✓	✓	✗
SAML pairwise-id	✓	✗ ?	✓	✓	✓
OIDC public sub	✓	✗	✓	✓	✗
OIDC pairwise sub	✓	✓[16]	✓	✓	✓

Table 1: Identifier properties as described in the SAML 2.0, eduPerson, and OIDC specifications

[14] Technically eduPersonPrincipalName may be used in an opaque way, however, this is not common and may be unfriendly to end users as ePPNs may be displayed to end users.

[15] This identifier is made unique by concatenation of the entityid of the issuer, the the entityid of the target and the subjected.

[16] A Pairwise sub may also provide the same sub for "a group of Web sites under single administrative control".

5. SAML to OIDC

In this scenario, SAML identifiers need to be mapped into OIDC sub (subject) claims.

Mapping eduPerson/SAML ➡️ OIDC public sub claim

Table 1 shows SAML identifier compatibility for creating an OIDC public sub out of various SAML based identifiers.

Based on the comparison from Table 1, the best match for mapping SAML 2.0 or eduPerson identifier attributes to an OIDC public sub is to use ePTID, a SAML2 persistent NameID, the SAML pairwise-id, ePUID or SAML subject-id . Even though these identifiers present unique, per SP identifiers, this document assumes a single proxy (SP) to take care of the token translation, hence it will have a suitable (single) identifier to create a public sub.

In case a suitable profile is used, which ensures non-reassignment, for example the Research and Scholarship Entity Category, an ePPN may also be used in case no ePTID is also received.

Mapping eduPerson SAML ➡️ OIDC pairwise sub claim

Again Table 1 describes SAML identifiers compatibility for creating an OIDC pairwise claim out of various SAML based identifiers.

Based on the comparison from Table 1, the best match for SAML 2.0 or eduPerson identifier attributes as a basis for creating an OIDC pairwise sub is to use ePUID, ePTID, a SAML2 persistent NameID, or a subject-id or pairwise-id. As OIDC pair-wise sub requires unique per RP identifiers, an implementation must create a per RP identifier. Please note that the OIDC specification section "Pairwise Identifier Algorithm"[17] has specific recommendation on how a pairwise sub should be created.

ePPN (or the combination of ePPN and ePTID) may be used as the basis for creating an OIDC pairwise sub, but *only* if non-reassignment is guaranteed. This could be the case when the implementation supports the Research and

[17] http://openid.net/specs/openid-connect-core-1_0.html#PairwiseAlg

Scholarship Entity Category[18]. In addition, the resulting identifier must be made both opaque and unique by the proxy.

[18] https://refeds.org/category/research-and-scholarship

6. OIDC to SAML

Mapping OIDC public sub claim ➡️ SAML

Table 1 also shows SAML identifiers that can be created from an OIDC public claim.

Taking into account Table 1, an ePTID, SAML2 persistent nameID, or SAML pairwise-id may be created from an OIDC public sub, if the implementation takes into account generating unique identifiers per SP on the SAML side of the implementation. Alternatively, an ePUID or subject-id could be created. A non-reassignable ePPN may be created from a public sub as well. Consideration concerning anonymity and global uniqueness should be taking into account when assessing which identifier to use.

If the SAML identifier requires a scope to be added, it is suggested the identifier is scoped to the domain of the proxy performing the translation.

A SAML2 transient nameID may be created if the proxy takes care of all the transient properties required for this identifier.

Mapping OIDC pairwise sub claim ➡️ SAML

It comes to no surprise that Table 1 also describes SAML identifiers that can be created from an OIDC pairwise claim.

An OIDC pairwise sub claim can be mapped to a SAML2 persistent NameID, SAML pairwise-id, or ePTID while retaining all characteristics. All other identifiers may be created on the basis of a pairwise sub, but this will result in the loss of one or more properties.

Special considerations should be made in case the pairwise character of the identifier should be retained, for example in the case of a proxy for whom any pairwise identifier received is de facto not pairwise anymore.

7. Examples

For example, consider the following ID token:

A sample ID token

```
{
 "iss": "https://server.example.com",
 "sub": "24400320",
 "aud": "s6BhdRkqt3",
 "nonce": "n-0S6_WzA2Mj",
 "exp": 1311281970,
 "iat": 1311280970,
 "auth_time": 1311280969,
 "acr": "urn:mace:incommon:iap:silver"
}
```

Suppose the sub claim in the above ID token is a pairwise sub claim, then that claim can be mapped to the following SAML2 persistent NameID:

A SAML2 Persistent NameID

```
<saml2:NameID
  Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
  NameQualifier="https://server.example.com">
  24400320
</saml2:NameID>
```

Note that the saml2:NameID/@SPNameQualifier XML attribute has been omitted.

8. Basic attribute to claims mapping profile

The basic profile proposes to create an implementation that would allow an unmodified OIDC client to receive claims based on SAML attributes through the proxy. This would allow an existing SAML based Identity federation to add a proxy to onboard OIDC RPs, which seems the most common scenario at the time of writing.

As the basis for the basic profile, the standard claims as described in the OIDC specification[19] are used, with a "*shared user identifier*" and a straightforward mapping from eduPerson attributes.

This profile shares the spirit of the "R&S attribute bundle" as described in the Research and Scholarship Entity Category definition[20]. As such we choose not to support all possible claims of the profile scope nor all possible (eduPerson) attributes.

The recommended mapping is shown in Table 2.

OIDC Scope	**OIDC claim**	**eduPerson attribute**
profile	Public sub	eduPersonPrincipalName (if non-reassigned) or eduPersonTargetedID
	name	displayName
	given_name	givenName
	family_name	sn (surname)
email	email	mail[21]

[19] https://openid.net/specs/openid-connect-core-1_0.html#Claims
[20] https://refeds.org/category/research-and-scholarship
[21] As mail may be multi valued, it is left to the implementer to choose which address needs to go into the single valued email claim

	email_verified	See below

Table 2: Recommended basic mapping profile of SAML attributes into OIDC claims

Supporting the profile scope

When mapping SAML attributes to OIDC claims it is recommended to follow the mapping as presented in Table 2. The profile however has additional claims available. This document does not make any recommendation on the use of these claims.

One should note however, very few entities in this sector will likely be willing or able to share claims like profile, picture, website, gender, birthdate as educational institutions either do not collect these data, or consider this to be too privacy sensitive to be released.

In addition it is discouraged to base preferred_username on a SAML attribute.

Using email_verified

OIDC has a claim called email_verified, which is defined as: "true if the End-User's e-mail address has been verified; otherwise false. When this Claim Value is true, this means that the OP took affirmative steps to ensure that this e-mail address was controlled by the End-User at the time the verification was performed. The means by which an e-mail address is verified is context-specific, and dependent upon the trust framework or contractual agreements within which the parties are operating."

It is up to the implementor to select which email address is to be provided through the mail claim in case multiple values are available. For the email address provided, it is recommended to set the email_verified claim to "true" if the email address that is being provided in the claim was:

- Provided by the Institutional Identity Provider as part of the SAML assertion, and
- The domain part of the email address is a (sub) domain of the institution
- The domain of the email is validated by the implementation based on the <shibmd:Scope> element from the entities

SAML metadata.

As in such case it may be assumed the email service being used is under direct administrative control of the Institution, and the requirements for setting email_verified to "True" have been fulfilled.

8. Advanced profile

The advanced profile provides a more elaborate profile for mapping SAML attributes from the eduPerson and SCHAC schemas to OIDC. This may however require the RP to create a custom implementation to be able to consume all claims.

Attribute Mapping

The advanced profile retains the mappings as presented in the basic profile, but adds a direct, literal mapping from attributes from eduPerson, eduMember and SCHAC into claims. As a general rule of thumb, to map the attributes an attempt was made to match common semantics of both protocols as much as possible. In some cases a straightforward mapping of the attribute or claim value is not possible, and will have to be left to the implementer.

Therefore, going from SAML to OIDC:

- an underscore is used to separate words that would normally have a space in natural language;
- the schema prefix of the attribute is retained, presented in lower case and separated by an underscore, and
- camel case is converted into lower case, and again using underscores to separate words.

To move from OIDC to SAML, the reverse is applied.

By retaining the SAML schema name as part of the claim, the OIDC requirement on collision-resistant names for claims[22] is met, whereas attributes without a collision-resistant name are to be mapped in accordance with the Basic profile.

With this, a mapping of attributes to claims will be as following:

[22] http://openid.net/specs/openid-connect-core-1_0.html#AdditionalClaims

SAML attribute	**OIDC claim**
eduPersonFoo	eduperson_foo
SchacFooBar	schac_foo_bar

Table 3: Generic example for mapping between SAML attributes and OIDC claims

Other attributes can be mapped in a similar fashion. Table 4 presents a number of examples for mapping commonly used attributes to OIDC Claims.

OIDC claim name	eduPerson or SCHAC name
eduperson_affiliation	eduPersonAffiliation
eduperson_entitlement	eduPersonEntitlement
eduperson_principal_name	eduPersonPrincipalName
eduperson_scoped_affiliation	eduPersonScopedAffiliation
eduperson_targeted_id	eduPersonTargetedID
eduperson_assurance	eduPersonAssurance
eduperson_unique_id	eduPersonUniqueId
eduperson_orcid	eduPersonOrcid
edumember_is_member_of	isMemberOf
schac_home_organisation	schacHomeOrganisation
schac_personal_unique_code	schacPersonalUniqueCode

Table 4: Examples of mapping commonly used eduPerson and SCHAC attributes to OIDC claims

Requesting claims

Due to data protection regulations, like e.g. GDPR in the EU, it is common to apply the principle of minimal disclosure: to send as little personal data as possible given the functional scope of the requesting application.

Basic profile

To request claims through the Basic profile, the profile and email scopes may be used. This allows for requesting a consistent set of attributes.

Earlier work from REFEDs around the Research and Scholarship Entity Category[23] has identified the entity category that provides for consistent attribute release through the definition of a set of commonly supported and consumed attributes typically required for effective use of R&S services. The attributes chosen represent a privacy baseline such that further minimization achieves no particular benefit. Thus, the minimal disclosure principle is already designed into the category.

When an entity implements the Basic profile as described in this document, the personal data that will be transferred closely resembles the information transferred as part of the Research and Scholarship Attribute Bundle. Unfortunately however, OIDC currently lacks the mechanisms to signal Entity Categories, such as as e.g. Research or Scholarship, to relying parties. It is therefore left up to the discretion of the implementer of the token translation service to decide if the requirements around purposeful use are met.

Advanced profile

To request specific, individual claims, the OIDC protocol supports both the use of requesting individual claims as well as the ability to request non-standard Scopes.

Requesting individual Claims

Individual Claims can be requested using the claims request parameter[24]. The use of the claims parameter is further described in the OIDC specification, section "Requesting Claims using the "claims" Request Parameter"[25]. Unfortunately however, given that this mechanism is optional in the specification, support for the capability to handle claim requests in this way is rather rare in existing Relying Party software products. It is therefore

[23] https://wiki.refeds.org/display/ENT/Guidance+on+justification+for+attribute+release+for+RandS
[24] http://openid.net/specs/openid-connect-core-1_0.html#Claims
[25] http://openid.net/specs/openid-connect-core-1_0.html#ClaimsParameter

recommended to also implement support for non-standard Scopes.

Requesting non-standard Scopes

The OIDC specification defines a number of standardized, optional scopes which can be used to request that specific sets of information be made available as Claim Values.[26] Unfortunately there is no standardized way of registering additional Scopes beyond what is defined in the specification. It is however possible and allowed for an OP to support non-standard Scopes. And for most of the Relying Party software, requesting (additional) scopes is part of the configuration of the software, which makes it trivial to support additional scopes.

That said, apart from the Research and Scholarship Attribute Bundle which is defined as part of the Research and Scholarship Entity Category, no other logical bundles exist.

It is therefore recommended to support a Scope value *for each* claim from the Advanced Profile by allowing a specific claim to be requested through a Scope with the exact same name. Table 5 provides some examples of how to use standard and nonstandard scopes to request claims.

[26] http://openid.net/specs/openid-connect-core-1_0.html#ScopeClaims

Requested scope(s)	**OIDC claim(s) delivered**
eduperson_foo	eduperson_foo
schac_foo_bar	schac_foo_bar
profile	public sub name given_name family_name
eduperson_targeted_id, eduperson_scoped_affiliation	eduperson_targeted_id, eduperson_scoped_affiliation
profile, email, eduperson_scoped_affiliation	public sub name given_name family_name email email_verified eduperson_scoped_affiliation

Table 5: examples of how to use standard and nonstandard scopes to request sets and individual claims

9. Future Work

Registering Claims

As part of the work for the OIDCre group, the OIDC claims described in the Advanced profile attributes will be registered into the JSON Web Token Claims Registry[27] once sufficient consensus has been reached.

R&E working group in OIDC foundation

At the time of writing this document, work is in progress to create a new R&E working group within the OIDC foundation. A charter proposal[28] was submitted to the OIDC foundation and it has been accepted on Sept 27, 2018. It is the intent that this document becomes one of the deliverables within the R&E Working group.

R&S scope

The REFEDS Research and Scholarship Entity Category (R&S) has been designed as a simple and scalable way for (SAML) Identity Providers to release minimal amounts of required personal data to (SAML) Service Providers serving the Research and Scholarship Community. The R&S Entity Category has two components: a policy part defining which entities are eligible to be tagged as R&S. In addition there is an Attribute Bundle[29]. One of the features that would be very useful is to represent the SAML based R&S attribute bundle also in OIDC. It is therefore proposed to create an R&S scope that would allow a set of claims to be requested by an RP that match equivalent attributes from the R&S attribute bundle. Please note that this scope will not include the *policy* aspects of the REFEDS Research and Scholarship Entity Category. It is envisioned that introduction of this new scope can become part of the above R&E OIDC working group.

[27] https://www.iana.org/assignments/jwt/jwt.xhtml#claims
[28] https://github.com/daserzw/oidc-edu-wg/blob/v1.0.0/charter.md
[29] https://refeds.org/category/research-and-scholarship, section 5

Formalized implementation standard

This document is not an implementation standard. At the time of writing it was felt that, even though several operators of production platforms were involved in the writing of this document, too little field experience exists to be able to write a standardization document at this time. It is recommended to determine at some point in time whether a formal standardization document is needed to further standardize the combined use of SAML2 and OIDC.

10. Authors and contributors

The editor wishes to thank all people and their organisations who have contributed to this document.

- Alejandro Pérez Méndez (Universidad de Murcia)
- Bart Geesink (SURFnet)
- Bradley Beddoes (Australian Access Federation Inc)
- Brendan Bellina (University of California, Los Angeles)
- David Hübner (DAASI International)
- Davide Vaghetti (GARR)
- Heather Flanagan (REFEDs & Spherical Cow Consulting)
- Ioannis Kakavas (GRnet)
- Jim Basney (CILogon)
- José Manuel Macías (RedIRIS)
- Keith Hazelton (University of Wisconsin-Madison & Internet2)
- Leif Johansson (SUNET)
- Maarten Kremers (SURFnet)
- Mark Jones (The University of Texas Health Science Center at Houston)
- Mikael Linden (CSC)
- Mischa Sallé (Nikhef)
- Nick Roy (Internet2)
- Nicolas Liampotis (GRnet)
- Roland Hedberg (Umeå University & SUNET)
- Thomas Lenggenhager (SWITCH)
- Tom Scavo (Internet2)
- Wolfgang Pempe (DFN-Verein)

Parts of this work were supported by the GÉANT project[30], a project that has received funding from the European Union’s Horizon 2020 research and innovation programme under Grant Agreement No. 731122 (GN4-2).

Parts of this work were supported by the AARC2[31] project, a project that has received funding from the European Union’s Horizon 2020 research and

[30] https://www.geant.org/Projects/GEANT_Project_GN4
[31] https://aarc-project.eu/

innovation programme under Grant Agreement No. 730941.