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

Version 1.1, Feb 14, 2024

Editor: Niels van Dijk, SURF (niels.vandijk@surf.nl)

This activity was originally carried in out in 2018 as part of the OpenID Connect for Research and Education (OIDCre)[1] working group of REFEDS[2], and was revised as part of the REFEDs Verifiable Credentials working group in 2024/2025

DOI

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

WORKING AREA
(To be resolved/deleted in final document)

Thoughts:

1. Peter Gietz: Create JSON objects?
2. Peter Gietz: Add JSON schema for eduperson/voPerson/ and may be even SCHAC
3. Peter Gietz: work ongoing/started on eduPerson and voPerson schema in the context of SCIM
4. Niels van Dijk: Propose to drop the reference “OIDC Claims” and just refer to “Claims”

Idea for document layout:

5. ~~Generic section describing the mapping objects and JSON schema~~
6. ~~Followed by Protocol specific implementation guidance for SAML, OIDC, SCIM and VCs~~

Take into account:

7. For VCs we need to consider the VCs must also be useful/understandable for folks outside of the community and we may need to at some point register the schema in EU/Gov schema

Earlier comments:

8. https://wiki.refeds.org/display/CON/Consultation%3A+SAML2+and+OIDC+Mappings
9. https://docs.google.com/document/d/1cGuVn3k0-IJ3BzSvACm1gCk_MMftYyTKRxvwpqfpStI/edit?tab=t.0

References:

- OIDC4VC: https://openid.net/wordpress-content/uploads/2022/06/OIDF-Whitepaper_OpenID-for-Verifiable-Credentials-V2_2022-06-23.pdf
- OpenID for Verifiable Credential Issuance - draft 15 (19 December 2024): https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html
- OpenID for Verifiable Presentations - draft 27
- https://openid.net/specs/openid-4-verifiable-presentationccccccciduvghfdhcniufjvffekvrnfbtgiclrhggudcd
- s-1_0.html
- W3C VC: https://www.w3.org/TR/vc-data-model-2.0/

- AARC GO56: https://docs.google.com/document/d/1jO1X7GSXWf_R604j5LXinr37ZUf96YVdIXSvjpS_Vyk/edit?tab=t.0#heading=h.s7slh698ji4x

Summary

Many protocols make use of so-called claims, for example OpenID Connect (OIDC)[3], Verifiabled Credentials (VC)[4] and the System for Cross-domain Identity Management (SCIM) [5] standard.

Historically, research and education have developed schema in support of their SAML based identity and access management systems and identify federations. Schema like eduPerson, SCHAC and voPerson are used to describe the semantics of the SAML messages used for authentication and authorization.

Goal of this document is to provide a consistent set of profiles for implementing and mapping the semantics as described in the schemas, and claims based protocols, in the context of use cases in Research and Education.

Since the introduction of this paper in 2018, it has seen broad implementation, among others in Shibboleth OP and SimpleSAMLphp as well as in several so called “Research AAI platforms” services such as eduTEAMS, CILogin, EGI Checkin and SURF Research Access Management.

Primary reason for the revisit of this document in 2024 is the introduction of Verifiable Credentials (VCs) and the request to add a profile for SCIM. The REFEDs Verifiable Credentials working group was started in the summer of 2024 to revise this document and take it into formal consultation within the REFEDs community.

[3] https://openid.net/specs/openid-connect-core-1_0.html
[4] https://www.w3.org/TR/vc-data-model-2.0/
[5] https://scim.cloud/

Version History

Version	Date	Comments
1.0	June 27, 2018	• Initial release
1.1	Feb 14, 2024	• Added ToC, • Fixed spelling errors, • Added Version History, License and DOI

Table of Contents

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"

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[6]
- The eduPerson Object Class Specification[7]
- The SCHema for ACademia (SCHAC)[8]
- Recommendations from REFEDs, including Research and Scholarship[9]
- SAML V2.0 Subject Identifier Attributes Profile [10]
- voPerson [11]

Most of this schema originates from LDAP schema[12].

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[13]
- eduGAIN Policy Framework SAML 2.0 WebSSO Protocol Profile[14]

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 and SAML 1.1 specifically.

The authors have added a reference to the Subject Identifier Attributes Profile, and added it to the mappings (later on in this document). Because even though this standard is still young

---

[6] https://saml2int.org, new version being developed at https://kantarainitiative.github.io/SAMLprofiles/saml2int.html
[7] http://software.internet2.edu/eduperson/internet2-mace-dir-eduperson-201602.html
[8] https://wiki.refeds.org/display/STAN/SCHAC
[9] https://refeds.org/research-and-scholarship
[10] http://docs.oasis-open.org/security/saml-subject-id-attr/v1.0/saml-subject-id-attr-v1.0.html
[11] https://refeds.org/specifications/voperson
[12] https://datatracker.ietf.org/doc/html/rfc4519, https://datatracker.ietf.org/doc/html/rfc2798
[13] https://technical.edugain.org/doc/GN3-11-012%20eduGAIN_attribute_profile.pdf
[14] https://technical.edugain.org/doc/eduGAIN%20SAML%202.0%20WebSSO%20Profile.pdf

and has not been implemented broadly yet, its features are a very good match with the scenarios described in this document.

Currently, there is no specific profile for Research and Education with OIDC. Therefore, this document references the generic OIDC protocol specifications provided by the OpenID Foundation.

It is important to note that this document does not describe a formalized implementation standard, nor does it intend to. At the time of writing, it was determined that despite the involvement of several operators of production platforms, there is insufficient field experience to create a standardization document. Consequently, the authors have chosen not to adopt the formal RFC2119 terminology throughout the document.

Mapping between attributes and claims

This section describes mapping attributes from eduPerson, eduMember, voPerson, SCHAC, and the SAML V2.0 Subject Identifier Attributes Profile (further reference as “schema”) into claims.

Mapping guidelines

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, when transforming a schema name to a claim name:

- 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, underscores are used to separate words.

The reverse is applied to move from claim to schema.

By retaining the schema name as part of the claim, the OIDC requirement on collision-resistant names for claims[15] 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 follows:

A schema attribute	**COIDC claim**
eduPersonFoo	eduperson_foo
SchacFooBar	schac_foo_bar
voPersonFoo	voperson_foo

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

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

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

claim name	**schema name**
eduperson_affiliation	eduPersonAffiliation
eduperson_entitlement	eduPersonEntitlement
eduperson_principal_name	eduPersonPrincipalName
eduperson_scoped_affiliation	eduPersonScopedAffiliation
eduperson_assurance	eduPersonAssurance
eduperson_unique_id	eduPersonUniqueId
eduperson_orcid	eduPersonOrcid
edumember_is_member_of	isMemberOf
schac_home_organisation	schacHomeOrganisation
schac_personal_unique_code	schacPersonalUniqueCode
voperson_external_id	voPersonExternalID
voperson_scoped_affiliation	voPersonScopedAffiliation
voperson_external_affiliation	voPersonExternalAffiliation or eduPersonScopedAffiliation

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

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[16] once sufficient consensus has been reached.

Research and Education (R&E)&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[17] was submitted to the OIDC foundation and it was accepted on Sept 27, 2018. It is the inte nt that this document becomes one of the deliverables within the R&E Working group.

Research and Scholarship (R&S)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[18]. 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.

Formalised 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 standardisation document at this time. It is recommended to determine at some point in time whether a formal standardisation document is needed to further standardise the combined use of SAML2 and OIDC.

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

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)
- Nicole 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[19], 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[20] project, a project that has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 730941.

[19] https://www.geant.org/Projects/GEANT_Project_GN4
[20] https://aarc-project.eu/

Technology profiles

Mapping between SAML and OIDC

Use cases

- Multi protocol IdP/OP (e.g. Shibboleth IdP, SimpleSAMLphp), using the same authentic source
- Proxy deployment, bridging between protcols

Identifiers

Many implementations need to map identifiers from the SAML protocol into the OIDC protocol, or vice 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)	✗	✗ ? [21]	✓	✓	✗
eduPersonUniqueId (ePUID)	✓	✓	✓	✓	✗
eduPersonTargetedID (ePTID) and/or SAML2 persistent NameID	✓	✓	✓	✓ [22]	✓
SAML2 transient NameID	✗	✓	✗	✗	✗
SAML subject-id	✓	✗ ?	✓	✓	✗
SAML pairwise-id	✓	✗ ?	✓	✓	✓
OIDC public sub	✓	✗	✓	✓	✗
OIDC pairwise sub	✓	✓ [23]	✓	✓	✓
voPerson Unique Identifier (voPersonID)	✓ ?	✓ ?	✓ ?	✓	✗

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

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.

---

[21] 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

[22] This identifier is made unique by concatenation of the entityid of the issuer, the the entityid of the target and the subjectid

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

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-resignment, for example the Research and Scholarship Entity Category, an ePPN may also be used in case no ePTID is also received.

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

Table 2

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"[24] has specific recommendations 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-reassignability is guaranteed. This could be the case when the implementation supports the Research and Scholarship Entity Category[25]. In addition, the resulting identifier must be made both opaque and unique by the proxy.

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

Table 3

[24] http://openid.net/specs/openid-connect-core-1_0.html#PairwiseAlg
[25] https://refeds.org/category/research-and-scholarship

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

And 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.

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.

Basic profile: Creating standard claims using attributes

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 [26] 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[27]. 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 or subject-id
	name	displayName
	given_name	givenName
	family_name	sn (surname)
email	email	mail[28]
	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.

[26] https://openid.net/specs/openid-connect-core-1_0.html#Claims
[27] https://refeds.org/category/research-and-scholarship
[28] 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

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 email address has been verified; otherwise false. When this Claim Value is true, this means that the OP took affirmative steps to ensure that this email 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 entity's SAML metadata.

As in such a 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.

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.

Standard claims

To request standard 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[29] 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.

[29] https://wiki.refeds.org/display/ENT/Guidance+on+justification+for+attribute+release+for+RandS

Unfortunately however, OIDC currently lacks the mechanisms to signal Entity Categories, such 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.

Requesting individual Claims

Individual Claims can be requested using the claims request parameter[30]. The use of the claims parameter is further described in the OIDC specification, section "Requesting Claims using the "claims" Request Parameter"[31].
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 recommended to also implement support for non-standard Scopes.

Requesting non-standard Scopes

The OIDC specification defines a number of standardised, optional scopes which can be used to request that specific sets of information be made available as Claim Values.[32] Unfortunately there is no standardised 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 sopes.

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.

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

[30] http://openid.net/specs/openid-connect-core-1_0.html#Claims
[31] http://openid.net/specs/openid-connect-core-1_0.html#ClaimsParameter
[32] http://openid.net/specs/openid-connect-core-1_0.html#ScopeClaims

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

Verifiable Credentials

Introduction

A Verifiable Credential (VC) is a digital version of a physical credential (e.g., a passport, driver's license, or diploma) that is cryptographically secure, tamper-proof, and verifiable. It follows the W3C Verifiable Credentials Data Model[33] and consists of three main components: the metadata, the subject data and the proofs.

Credential Metadata

This includes general information about the credential itself, such as:

- Type: Specifies the kind of credential (e.g., "VerifiableCredential", "UniversityDegreeCredential").
- Issuer: The entity that issued the credential (e.g., a university, government agency).
- Issued Date: When the credential was issued.
- Expiration Date (Optional): When the credential expires, if applicable.

It should be noted that the Credential Type is used in multiple ways throughout the lifecycle of a credential:

- The credential type may be used as the identifier for json schema definition to describe the content, structure, data types, and expected constraints within the VC. This helps ensure the consistency and integrity of JSON data.
- The credential type may trigger specific behaviour in a wallet, e.g. to allow for specific graphical presentation of parts of the credential data to a user. For example the OpenBadges v3 specification may contain values expressed in Markdown
- The credential type may be used by a verifier to request specific VCs or parts thereof, see e.g. https://openid.net/specs/openid-4-verifiable-presentations-1_0.html#appendix-B.1.1
- Credential Types currently do not have any collision protection. Anybody can create a ”voPersonCredential” with a set of claims to their liking. To avoid name collision we should use an URI here. As REFEDs is already authoritative for the eduPerson, SCHAC and voPerson Schema, it seems logical to let these land there.

Claims (Subject Data)

This contains the actual information about the subject (the person or entity to whom the credential belongs), such as:

- Subject Identifier: A unique identifier for the subject (e.g., a decentralized identifier "did:example:123").

[33] https://www.w3.org/TR/vc-data-model-2.0/

- Attributes: Information about the subject (e.g., "name": "Alice", "degree": "BSc in Computer Science").
- Schema Definition: A standard way to interpret the claims.

Proofs (Cryptographic Signature)

This ensures the credential is authentic and tamper-proof. It includes:

- Digital Signature: Cryptographic proof issued by the issuer to verify authenticity.
- Proof Type: The method used for signing (e.g., JSON Web Signature (JWS), Linked Data Proof).
- Revocation Mechanism (Optional): A way to check if the credential has been revoked.

Figure X provides an overview of the technical representation of a VC when presented in JSON format with the above components.


```
{
  "@context": ["https://www.w3.org/2018/credentials/v1"],
  "id": "http://example.edu/credentials/123",
  "type": ["VerifiableCredential", "UniversityDegreeCredential"],
  "issuer": "https://example.edu",
  "issuanceDate": "2023-06-01T12:00:00Z",
  "credentialSubject": {
          "id": "did:example:456",
          "name": "Alice",
          "degree": "Bachelor of Science in Computer Science"
  },
  "proof": {
          "type": "Ed25519Signature2020",
          "created": "2023-06-01T12:00:00Z",
          "proofPurpose": "assertionMethod",
          "verificationMethod": "https://example.edu/keys/1",
          "jws": "eyJhbGciOiJFZERTQSJ9..."
  }
}
```


Figure X: Example JSON Representation of a Verifiable Credential

Wallet ecosystem

The VC is a stand-alone, atomic credential, meaning it can be viewed and verified on its own. As such it could be used in a similar way as e.g. a digitally signed PDF document, and might be shared via e.g. email or social media.

VCs are also an integral part of the wallet ecosystem, where VCs are transported between Issuers, Holder Wallets and Verifiers.

Figure X shows the relation between various entities in the wallet ecosystem as described by the W3C VC data model[34].

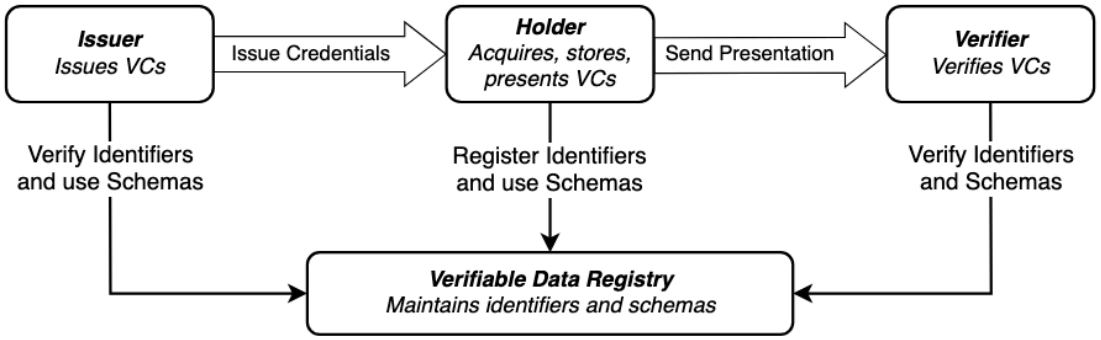


Figure X: The roles and information flows forming the basis for exchange of Verifiable Credentials.

A commonly used protocol for the issuance of the credentials is the OpenID4VCI[35] specification. The presentation of the credential by the wallet towards the verifier is done using the OpenID4VP[36] specification.
The OpenID4V* specifications are not limited to the use of VCs, also credential formats like mDOC are supported.

When using VCs, these can be represented using different serialization formats to ensure interoperability, security, and ease of verification. The most common formats include:

- VC_JWT (Verifiable Credential as a JSON Web Token)
- LD_JWT (Linked Data JSON Web Token)
- SD_JWT (Selective Disclosure JSON Web Token)

Each format has unique characteristics and is suited for different use cases. Chapter XYZ will further discuss the practical implications.

Use cases

Presenting Academic Identity

One of the key features of the European EUDI Wallet programme is the delivery of government issued PIDs which should provide a base government issued high assurance identity, and a trusted ecosystem where credentials, also outside of governmental use cases, may be exchanged. However, due to the high assurance attached to the use of government ID, this ecosystem likely also has high technical and organisational requirements.
Many use cases in research and education however do not require a high assurance identity, as can be concluded from the fact that the sector has been working with institutional identity for the better part of 20 years. It is therefore likely such institutional identity will also be able to facilitate many of the sectoral use cases, both nationally and internationally. Furthermore, the government

[34] https://www.w3.org/TR/vc-data-model-2.0/
[35] https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html
[36] https://openid.net/specs/openid-4-verifiable-presentations-1_0.html

ID may not hold all user credentials we need in the R&E sector, like e.g. email address is not included in the PID set.

A sectorial identity, preferably containing a persistent identifier derived from the government identity, would be a good way to support many of the use cases in our sector. To support as many use cases as possible, and yet release as little personal data as possible, adopting a VC equivalent of the REFEDs Personalized Entity category[37] seems like a good basis for a generic academic base identity. This would mean creating VCs that replicates the functionality of the REFEDS Personalized Entity category attribute bundle, ensuring privacy while meeting the needs of research and education use cases.

This identity can then be augmented with additional context specific identifiers like ORCID or MyAcademicID, be used as the identity part of badges and micro-credentials, and serve as the base identity for research to add additional VCs in the context of their research communities

Presenting learning and education outcomes

In today's education, there is a need to present credentials such as diploma, courses and skills across borders of an institution and country. This can include transcript of records, microcredentials or badges in order to support use cases such as access to other education experiences (including mobility or at alliance partners), applying for jobs or getting registered into (or staying in) professional registers.

Important to note is that this use case will likely be mandatory for EU Member states to support. The European Digital Identity Regulation (Regulation (EU) 2024/1183), also known as eIDAS 2.0, in its Annex VI, requires a support of a set mandatory attributes, part of which are educational qualifications, titles and licences.
Next to the formal educational qualifications there is an increasing demand for using so called “micro-credentials”[38] which signal the results of following a small volume of learning. In many cases these micro-credentials are not formally established.

Presenting entitlements, group membership or resources capabilities

The AARC Blueprint Architecture[39] defines the building blocks for an AAI solution catering the needs of access to research infrastructures. AARC BPA is clear that the research infrastructures are the ones in charge of assigning information about rights of user access, and based on this information making authorisation decisions. In today's research infrastructure landscape, collaborations of distributed research infrastructures that tend to federate their resources, make a promise of more complex use cases to emerge. While one entity can act as the one assigning the rights to the users, other entities may grant access based on that information. These use cases can be even more complex when it is not simply an access right information that needs to be communicated, but also potentially resource capacities that are assigned, such as in the case of federating HPC resources. Access to sensitive data, such as for example genetic data in Life Science research, where one authority gives permission to access the data managed by other authorities is another advanced use case.
Digital credentials that can hold a rich set of data describing user rights and resources being made available to the users, can be used to exchange this information instead of creating complex data exchange infrastructures.

---

[37] https://refeds.org/category/personalized

[38] https://education.ec.europa.eu/sites/default/files/2022-01/micro-credentials%20brochure%20updated.pdf

[39] https://aarc-community.org/architecture/

Identifiers

Protocol identifiers

- Holder key
- Wallet key
- OpenID4VCI
- OpenID4VP
- Vc id
- Issuer
- credentialType
- credentialSubject ID
- Other identifiers

Claims

Any credential issued into a wallet is in essence a copy of the source attribute as it was held by the issuer. For many credentials that is of course the whole idea of the credential release. However the very nature of VCs main change some of the properties of the claims as compared to the way these can

Table 1 shows various common identifiers as currently in use in R&E when using SAML or OIDC. If we want to use these identifiers within the Verifiable Credentials, we must take into account how the properties of these verifiers change when these would become part of a VC.

Protocol identifiers

How to satisfy Anoymous, Pseudonoumous, Personalized

Wallet ecosystem identifiers

Holder key
Wallet key
OpenID4VCI
OpenID4VP

Identifiers

Targeted identifiers
Claims holding identifiers which previously were transient or targeted, like pairwise-id should be avoided as one these lose their transient or targeted property once these are embedded into a VC.

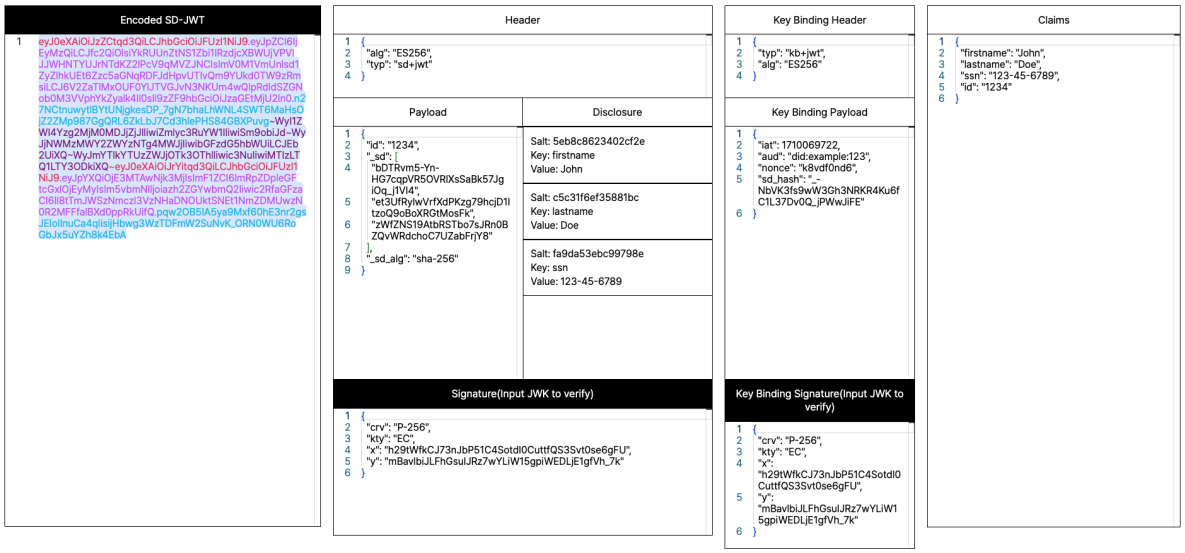
Persistent Identifiers
Claims holding (long lived) persistent identifiers like eduPersonPrincipleName or eduPersonUniqueId have been should be avoided as one these lose their transient or targeted property once these are embedded into a VC.

Entitlements

VC schema

- VC_JWT
- LD_JWT
- SD_JWT

SD_jwt example https://www.sdjwt.co/



Examples

SCIM

Introduction

The System for Cross-domain Identity Management is an open standard protocol[40] that enables the creation, modification and deletion of users' accounts in cloud applications and services. SCIM contributes to automatise users provisioning and deprovisioning across several applications and platforms. It works with a resource as a common denominator - that includes id, externalID and meta as attributes - from which SCIM objects derive.

RFC7643 defines the User, Group and EnterpriseUser that extends common attributes.

SCIM provides a REST API for the manipulation of the resources (Create, Read, Replace, Delete, Update, Search, Bulk).

To explore features and attributes, SCIM provides a discovery service with three end-points[41]:

GET /ServiceProviderConfig
Specification compliance, authentication schemes, data models.

GET /ResourceTypes
An endpoint used to discover the types of resources available.

GET /Schemas
Introspect resources and attribute extensions

Use cases

Identifiers

Schema

Examples

[40] https://datatracker.ietf.org/doc/html/rfc7644
https://scim.org/
[41] https://scim.org