Attributes and SAML

At the core, SURFconext is a service that handles attributes. You will need to get yourself acquainted with attributes as soon as you connect a service to SURFconext. An attribute is a characteristic that describes a user. There are quit a few attributes we can provide but we have a minimal disclosure principle. This means only the absolute minimum amount of information needed to make your service work is transferred to your service. When you request a connection to the Production environment, you must specify the attributes needed and motivate them to make us and users understand why you need them. SURFconext Support will review your request and configure an Attribute Release Policy accordingly. If we think you ask to much, we will discuss this with you.

When Identity Providers are asked if they want to connect to your service, they will be informed of the attributes your service requests. The IdP must agree to the release of these attributes to your service.

Attributes in SURFconext

The information below is a carbon copy of our Attributes in SURFconext page as found in the background part of our documentation of SURFconext.

This page will list all the SAML2 attributes that SURFconext and their identity providers have to offer. An attribute is a characteristic that describes a user. It is a 'name:value' pair. The attributes included in the SAML assertion correspond to certain attributes a service provider needs to work properly. In general they are needed to:

- **Convey user information** from the identity provider (IdP) to the service provider (SP)
- **Create an account** for the user at the service provider
- **Authorize** specific services at the service provider

Now, when a user logs in to a service provider, SURFconext sends a SAML assertion to the service provider via the browser of the user, that contains a:

- **User identifier**. All services receive these and are either a **transient** or **persistent NameID** (chosen via SP Dashboard).
- **Additional attributes**. These are optional and per service.

SURFconext's SAML2 implementation adheres to the SAML2int standard 0.2.1.

The header on the link above states that work on saml2int has moved to Kantara Initiative. Until further notice, the SAML2int standard SURFconext adheres to remains at 0.2.1.

Content provider?

For content providers, SURFconext (in consultation with the partnership of the Dutch university libraries and the Koninklijke Bibliotheek (UKB), Hogeschoolbibliotheken (SHB)) applies a separate attribute release policy. The following are allowed:

- Persistent or transient NameID
- schacHomeOrganization
- eduPersonAffiliation

Read our blog for more information (Dutch)

Before you start digging into the theoretical stuff on this page, you might want to start with our 'best practice' page for an introduction to and how attributes are best used.

- User identifiers
- Changing attributes
- Useful links
- Attribute schemas
- Attribute overview
- Detailed attribute descriptions
  - ID

- Surname
- Given name
- Common name
- Display name
- Email address
- uid
- Home organization
- Organization type
- Employee-student number
- Affiliation
- Scoped Affiliation
- Entitlements
- Principal name
- isMemberOf
- Preferred Language
- EduPersonTargetedID
- eduPersonORCID
- eduPersonAssurance
- ECK ID
- SURF CRM ID
- MS AuthnMethodsReferences
- OrganizationalUnitName
- eduID

User identifiers

The user's identity is transmitted in the form of the NameID element. Every IdP must supply a NameID, but for privacy reasons SURFconext will generate a new one, which is duplicated in the attribute eduPersonTargetedID.

To identify a user the Service Provider must use the NameID or eduPersonTargetedID. The NameID is guaranteed to be stable for a fixed user, except in the case of transient identifiers. SURFconext will generate a NameID for each new user. It is unique for the user and specific to the SP, so SP's cannot correlate their received NameID's between each other. There are two types of NameIDs:

- `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent`
  A persistent NameID contains a unique string identifying the user for this SP and is persisting over multiple sessions.
- `urn:oasis:names:tc:SAML:2.0:nameid-format:transient`
  A transient NameID contains a unique string identifying the user for this SP during the session. If the user logs in again, a new transient identifier will be generated.

> **Remark**
>
> The NameID and eduPersonTargetedID, which is basically a copy of the NameID, when set to persistent is unlikely to change and very privacy aware but can change when service providers or identity provider make critical changes. This can cause user profiles for services to be lost. The NameID, as used in the SAML assertion to a service provider when loggin' on, is generated using the **uid**, **schacHomeOrganization**, the **Entity ID** of the **service provider** together with a secret that uses a SHA algorithm. Institutions or services that are in production and change one of these attributes, will cause a new NameID and eduPersonTargetedID to be generated by SURFconext when doing so. This can cause loss of access to profiles at services. We will notify identity providers and service providers when we see a change in one of these attributes to prevent user data being lost.

Changing attributes

As an Identity Provider it is important to realize that changing attributes in production on SURFconext in any way can have an impact on services users have access to. Attributes that you offer to SURFconext are used to create profiles, and data is often linked to them. Changing an attribute in any way can have unwanted results like users that are no longer able to access their valuable data. An example could be to modify the way you fill the email address (amongst others). For example: changing 'student.123456@university.nl' to 'john.doe@university.nl'. Do you plan to do this or do you start a project where this is the case? Contact us and send an email to support@surfconext.nl.

Useful links

- Table with **attributes we recommend our institutions to release**: https://wiki.surfnet.nl/display/surfconextdev/Vereiste+attributen
- Profile Page https://profile.surfconext.nl/ , **showing what attributes are released by your IdP** to SURFconext

- **For new IdP's or for IdP's that upgrade their environment**: system administrators will at some point be asked to share the metadata of their account for analyses. When asked, visit this page and click the 'Mail to SURFconext' button. We will get back to you when we have judged the submitted metadata.This page will also show you the attributes shared and their values.

Attribute schemas

A schema is an abstract representation of an object's characteristics and relationship to other objects.

SURFconext supports two attribute schemas:

- `urn:oid` schema (SAML2.0 compliant)
- `urn` schema (SAML1.1 compliant)

Both can be used to convey the same information (except for the NameID, which is only available in the `urn:oid` schema). By default SURFconext will provide attributes in both schemas as part of the assertion. However it is not recommended to mix the use of the schemas.

Attribute overview

SURFconext supports relaying of the following attributes:

Friendly name	Attribute name	Example
ID	SAML NameID element urn:mace:dir:attribute-def:eduPersonTargetedID urn:oid:1.3.6.1.4.1.5923.1.1.1.10	bd09168cf0c2e675b2def0ade6f50b7d4bb4aae
Surname	urn:mace:dir:attribute-def:sn urn:oid:2.5.4.4	Doe Vermeegen
Given name or first name	urn:mace:dir:attribute-def:givenName urn:oid:2.5.4.42	John Mërgim Lukáš Þrúður
Common name or Full Name	urn:mace:dir:attribute-def:cn urn:oid:2.5.4.3	John Doe Prof.dr. Mërgim Lukáš Vermeegen , PhD.
Display name	urn:mace:dir:attribute-def:displayName urn:oid:2.16.840.1.113730.3.1.241	Dr. John Doe Prof.dr. Mërgim L. Vermeegen , PhD.
Email address	urn:mace:dir:attribute-def:mail urn:oid:0.9.2342.19200300.100.1.3	m.l.vermeegen@university.example.org maarten.'t.hart@uniharderwijk.nl "very.unusual.@.but valid.nonetheless"@example.com mlv@[IPv6:2001:db8::1234:4321]
Organization	urn:mace:terena.org:attribute-def: schacHomeOrganization urn:oid:1.3.6.1.4.1.25178.1.2.9	example.nl something.example.org
Organization Type	urn:mace:terena.org:attribute-def: schacHomeOrganizationType urn:oid:1.3.6.1.4.1.25178.1.2.10	urn:mace:terena.org:schac:homeOrganizationType:int:university urn:mace:terena.org:schac:homeOrganizationType:es:opi

Employee/student number	urn:schac:attribute-def: schacPersonalUniqueCode urn:oid:1.3.6.1.4.1.25178.1.2.14	urn:schac:personalUniqueCode:nl:local:example.edu:employeeid: x12-3456 urn:schac:personalUniqueCode:nl:local:example.nl:studentid: s1234567
Affiliation	urn:mace:dir:attribute-def:eduPersonAffiliation urn:oid:1.3.6.1.4.1.5923.1.1.1.1	employee, student, faculty, member, affiliate, pre-student
Scoped affiliation	urn:mace:dir:attribute-def: eduPersonScopedAffiliation urn:oid:1.3.6.1.4.1.5923.1.1.1.9	student@uniharderwijk.nl employee@uniharderwijk.nl
Entitlement	urn:mace:dir:attribute-def:eduPersonEntitlement urn:oid:1.3.6.1.4.1.5923.1.1.1.7	to be determined per service (see Standardized values for eduPersonEntitlement)
PrincipalName	urn:mace:dir:attribute-def: eduPersonPrincipalName urn:oid:1.3.6.1.4.1.5923.1.1.1.6	piet.jønsen@example.edu not.a@vålîd.émail.addreß
isMemberOf	urn:mace:dir:attribute-def:isMemberOf urn:oid:1.3.6.1.4.1.5923.1.5.1.1	urn:collab:org:surf.nl urn:collab:org:clarin.org
uid	urn:mace:dir:attribute-def:uid urn:oid:0.9.2342.19200300.100.1.1	s9603145 flåp@example.edu
preferredLanguage	urn:mace:dir:attribute-def:preferredLanguage urn:oid:2.16.840.1.113730.3.1.39	nl nl, en-gb;q=0.8, en;q=0.7
ORCID	urn:mace:dir:attribute-def:eduPersonORCID urn:oid:1.3.6.1.4.1.5923.1.1.1.16	http://orcid.org/0000-0002-1825-0097
Assurance	urn:mace:dir:attribute-def:eduPersonAssurance urn:oid:1.3.6.1.4.1.5923.1.1.1.11	`https://refeds.org/assurance/ID/unique`
ECK ID	urn:mace:surf.nl:attribute-def:eckid	https://ketenid.nl/spv1/eacf3765ad342...cf3a11fe9cab2365f95da3e 9965501f7c98e (Attribute made shorter for readability)
SURF CRM ID	urn:mace:surf.nl:attribute-def:surf-crm-id	ad93daef-0911-e511-80d0-005056956c1a

MS AuthnMethodsReferences	http://schemas.microsoft.com/claims
	/authnmethodsreferences
		`urn:oasis:names:tc:SAML:2.0:ac:classes:`
		`PasswordProtectedTransport`
		`http://schemas.microsoft.com/claims/multipleauthn`

OrganizationalUnitName	urn:mace:dir:attribute-def:ou
	urn:oid:`2.5.4.11`
		`ICT Services`
		`Geesteswetenschappen`
		`Facilitair`

eduid	urn:mace:eduid.nl:1.1	658b6b41-7c13-431d-b3b4-663e9077c24c f4c9afe4-b9e1-42bb-92b8-047ac8711e29

Note that not all identity providers might make all attributes available.

(1) eduPerson Object Class Specification (201602): https://wiki.refeds.org/pages/viewpage.action?pageId=44957738

Depricated Attributes

SURFconext considers the attributes **nlEduPersonOrgUnit**, **nlEduPersonStudyBranch** and **nlStudielinkNummer deprecated**. When you register a new SP at SURFconext, these attributes will not be allowed for use with SURFconext. Existing IdP's and SP can use these attributes until further notice.

Detailed attribute descriptions

ID

See User identifiers.

Surname

urn:mace	urn:mace:dir:attribute-def:sn
urn:oid	urn:oid:2.5.4.4
Multiplicity	single-valued
Data type	UTF8 string (unbounded)
Description	The surname of a person (including any words such as “van”, “de”, “von” etc.) used for personalization; this can be a combination of existing attributes.
Examples	Vermeegen Valk, van der
Notes	

Given name

urn: mace	urn:mace:dir:attribute-def:givenName
urn:oid	urn:oid:2.5.4.42
Multiplicity	single-valued
Data type	UTF8 string (unbounded)
Description	Given name, also known as a first name, forename or Christian name / “name known by”; combinations of title, initials, and “name known by” are possible.
Examples	Jan Klaassen Mërgim K. Lukáš Þrúður
Notes	Words such as “van”, “de”, “von” must not be in this attribute, but in Surname.

Common name

urn: mace	urn:mace:dir:attribute-def:cn
urn: oid	urn:oid:2.5.4.3
Multiplicity	multi-valued
Data type	UTF8 string (unbounded)

Description	Full name.
Examples	Prof.dr. Mërgim Lukáš Vermeegen , PhD.
Notes	For example, a typical name of a person in an English-speaking country comprises a personal title (e.g. Mr., Ms., Rd, Professor, Sir, Lord), a first name, middle name(s), last name, generation qualifier (if any, e.g. Jr.) and decorations and awards (if any, e.g. CBE).

Display name

urn:mace	urn:mace:dir:attribute-def:displayName
urn:oid	urn:oid:2.16.840.1.113730.3.1.241
Multiplicity	single-valued
Data type	UTF8 string (unbounded)
Description	Name as displayed in applications
Examples	Prof.dr. Mërgim Lukáš Vermeegen , PhD.
Notes	• This attribute can typically be changed by the end-users themselves, and is therefore not very suitable for identification.

Email address

urn:mace	urn:mace:dir:attribute-def:mail
urn:oid	urn:oid:0.9.2342.19200300.100.1.3
Multiplicity	multi-valued
Data type	RFC-5322 address (max 256 chars)
Description	e-mail address; syntax in accordance with RFC 5322
Examples	m.l.vermeegen@university.example.org "very.unusual.@.unusual.com"@example.com mlv@[IPv6:2001:db8::1234:4321]; the

Notes	• Multiple email addresses are allowed. However, there's no clear strategy for SP's on how to interpret multiple addresses (use both? pick one? ask user to pick one?); the SP should devise a strategy that makes sense within the context of the application. As an IdP, in the interest of interoperability, it's advisable to avoid sending multiple addresses where possible. • An email address is not necessarily the email address of this person at the institution. • Do not use this attribute to uniquely identify a user. Use the NameId instead. • A user's email address may change over time, or an IdP may allow a user to change this value themselves. This makes that attribute unsuitable for authentication and authorization purposes.

uid

urn:mace	urn:mace:dir:attribute-def:uid
urn:oid	urn:oid:0.9.2342.19200300.100.1.1
Multiplicity	single-valued (multi-valued in the specification, but within SURFconext only 1 value is allowed)
Data type	UTF8 String (max 256 chars); use of spaces and @-characters is discouraged.
Description	The unique code for a person that is used as the login name within the institution.
Examples	s9603145 piet flåp@example.edu (See note below)
Notes	• The uid is *not* a unique identifier for SURFconext users. Uid values are at most unique for each IdP. • Ideally the uid is not only a login name/code but also an identifier that is guaranteed as being unique within the institution over the course of time. At the moment, there is no such guarantee. • Use the NameId for unique identifiers in SURFconext rather than uid. • Use the eduPersonPrincipalName attribute if a human-readable unique identifier is required • A uid may contain any unicode character. E.g., "`org:surf.nl:joe von stühl`" is a valid uid. • SURFconext translates @-characters in the uid to underscores before constructing the NameID. flåp@example.edu translates to flåp_example.edu.

Home organization

urn:mace	urn:mace:terena.org:attribute-def:schacHomeOrganization
urn:oid	urn:oid:1.3.6.1.4.1.25178.1.2.9
Multiplicity	single-valued
Data type	RFC-1035 domain string. The domain MUST be a secondary-level domain that is under control by the institution. Preferably, the institution's main domain name should be used.
Description	The user's organization using the organization's domain name; syntax in accordance with RFC 1035.
Examples	uniharderwijk.nl example.nl

Notes	• In the past, SURFconext used to send the home organization in the attribute urn:oid:1.3.6.1.4.1.1466.115.121.1.15, which was incorrect. Since 2013, the correct oid urn:oid:1.3.6.1.4.1.25178.1.2.9 is in use. For reasons of compatibility, the old (wrong) key is still sent. It will be removed in the near future. • Matching values against this attribute should be case-insensitive, i.e. the values "uniharderwijk.nl" and "UniHarderwijk.nl" should be considered equal. For Interoperability reasons however we require lower-case values as specified above in SURFconext. • It is desirable to have the same value for all your users. • SURFconext will store the allowed value for your institution in our configuration so we can check that no illegal values are being sent.

Organization type

urn:mace	urn:mace:terena.org:attribute-def:schacHomeOrganizationType
urn:oid	urn:oid:1.3.6.1.4.1.25178.1.2.10
Multiplicity	single-value
Data type	RFC-2141 URN (see Schac standard)
Description	designation of the type of organization as defined on https://wiki.refeds.org/display/STAN/SCHAC+Releases?preview=/44957731/128909315/SCHAC%2B1.6.0-final.pdf
Examples	urn:mace:terena.org:schac:homeOrganizationType:int:university urn:mace:terena.org:schac:homeOrganizationType:es:opi
Notes	• Attribute values are registered by Géant on https://wiki.refeds.org/display/STAN/SCHAC+Releases • In practice, this attribute is not/hardly used by IdP's or SP's • Please contact support@surfconext.nl if you would like to use this attribute

Employee-student number

urn:mace	urn:schac:attribute-def:schacPersonalUniqueCode
urn:oid	urn:oid:1.3.6.1.4.1.25178.1.2.14
Multiplicity	multi-value
Data type	RFC-2141 URN (see SURF uri registry)
Description	The user's student, employee, and/or member id as used in the university's internal systems. Also used for the Erasmus Student Identifier for international student exchange.
Examples	urn:schac:personalUniqueCode:nl:local:example.edu:employeeid:x12-3456 urn:schac:personalUniqueCode:nl:local:example.nl:studentid:s1234567 urn:schac:personalUniqueCode:int:esi:example.nl:123321
Notes	• Attribute values are registered by SURF as shown on this page. • Please contact the SURFconext support team if you would like to use this attribute as an SP, or if you would like to provide it as an IdP. • This attribute's main use is for matching user accounts to the university's internal systems • It is also used in the Erasmus+ student exchange program. See Toevoegen European Student Identifier aan instellingssystemen.

Affiliation

urn:mace	urn:mace:dir:attribute-def:eduPersonAffiliation
urn:oid	urn:oid:1.3.6.1.4.1.5923.1.1.1.1
Multiplicity	multi-valued
Datatype	UTF8 String (only the values enumerated below are allowed)
Description	Indicates the relationship between the user and his home organization (institution). The following values are permitted within SURFconext: • `student` — A person enrolled at an institution, an external student or course participant. • `employee` — A person with a position at or labor agreement with an institution. • ~~`staff`~~ — ~~All academic staff and teachers.~~ (*deprecated*; do not use in new deployments) • `faculty` — A person whose primary role is teaching or research. (Commonly called WP at Dutch universities. Please note, PhD *students* are also perfectly allowed to carry this value.) • `member` — Anyone that holds at least one of the above affiliations is also a member. • `pre-student` — A person who has registered to start studying, but is not yet a full student. See this page (Dutch only) for more information about pre-students and the terms and conditions under which such users are allowed access. Pre-students will never be allowed access to service providers without prior consent from the service provider. • `affiliate` — A person who is authorized by the Institution, pursuant to the lenience model concluded by the Institution, to use the Service. Note: only the above mentioned values are allowed within SURFconext. Use the definitions mentioned to determine *which* affiliation a user gets. If you have doubts whether a user (fully) fits the definition, please use common sense.
Examples	see above
Notes	• Any user who has the affiliation `student`, `employee`, or `faculty`, should also have the value `member`. • Identity Providers might internally use additional values for the affiliation attribute, such as `alum`. Per SURFconext policy, the IdP may not allow such users to access SURFconext. Other values mentioned in the eduPerson specification include `library-walk-in`. This value is not currently used within SURFconext. • According to the eduPerson specification, the values of this attribute are case insensitive; for Interoperability reasons however, we require lower-case values as specified above in SURFconext. • The document REFEDS eduPerson(Scoped)Affiliation usage comparison is useful to determine the usefulness of values in an international context.

Scoped Affiliation

urn:mace	urn:mace:dir:attribute-def:eduPersonScopedAffiliation
urn:oid	urn:oid:1.3.6.1.4.1.5923.1.1.1.9
Multiplicity	multi-valued

Data type	UTF8 String of the form affiliation@domain (see below)
Description	Indicates the relationship between the user and the domain of his home organization. The affiliation part must be one of the allowed values of the eduPersonAffiliation attribute (see definition right above). The value is the role of the user and the domain name of the organisation. eduPersonScopedAffiliation can hence be defined as: <eduPersonAffiliation> "@" <schacHomeOrganization>. Just like eduPersonScopedAffiliation, this is a multi valued attribute. The domain part must be the schacHomeOrganization of the user (or a subdomain thereof).
Examples	`student@uniharderwijk.nl` `faculty@uniharderwijk.nl`
Notes	• This attribute is primarily a different way to convey the same information as is contained in eduPersonAffiliation and schacHomeOrganization. It's recommended to release this attribute next to eduPersonAffiliation and schacHomeOrganization, because some SP's ask for this attribute instead of the two separate ones. • If desired, this attribute can be used to describe the role of the user within a specific faculty, field, study or department that the user is part of. Because the attribute is multi-valued, a user can be a student at one and an employee at another department.

Entitlements

urn:mace	urn:mace:dir:attribute-def:eduPersonEntitlement
urn:oid	urn:oid:1.3.6.1.4.1.5923.1.1.1.7
Multiplicity	multi-value
Data type	RFC-2141 URN
Description	entitlement; custom URI (URL or URN) that indicates an entitlement to something.
Examples	`urn:mace:terena.org:tcs:personal-admin` `urn:mace:surf.nl:surfdomeinen.nl:role:dnsadmin`
Notes	• This attribute can be used to communicate entitlements, roles, etc, from identity providers to services, which can be used, for example, for authorization. • The values of this attribute are scoped to the identity provider that is authoritative for the attribute. • Formatting rules apply: See also the SURFconext entitlement name-spacing policy.

Principal name

urn:mace	urn:mace:dir:attribute-def:eduPersonPrincipalName
urn:oid	urn:oid:1.3.6.1.4.1.5923.1.1.1.6

Multiplicity	single-valued
Data type	UTF8 String of the form `user@scope`
Description	Unique identifier for a user.
Examples	piet.jønsen@example.e not.a@vålîd.émail.addreß
Notes	• This is a scoped identifier for a person. It should be represented as user@scope, where user is a name-based identifier for a person. The scope part of the attribute must be part of an administrative domain of the identity system where the identifier was created and assigned. An IdP can have multiple scopes, e.g. piet@student.hartingcollege.nl or piet@hartingcollege.nl. These Piet's are different persons and are scoped under the administrative domain of e.g. hartingcollege.nl were the scope was defined. • It is common that schacHomeOrganization is used for the scope, if no other scopes are defined. • Although this value resembles an email address, it MUST NOT be used as an email address. In many cases mail cannot be delivered to this "address". • Even though this value uniquely identifies a user, it is not guaranteed that it is persistent over sessions (even though it usually is). • It is preferred to not use this to uniquely identify users. Use the NameId instead. • SURFconext will store the allowed domain part for your institution in our configuration so we can check that no illegal values are being sent.

isMemberOf

urn:mace	urn:mace:dir:attribute-def:isMemberOf
urn:oid	urn:oid:1.3.6.1.4.1.5923.1.5.1.1
Multiplicity	multi-valued
Data type	RFC-2141 URN
Description	Lists the collaborative organizations the user is a member of.
Examples	`urn:collab:org:surf.nl`
Notes	• Attribute values are URIs (URN or URL) • The only currently supported value is `urn:collab:org:surf.nl`, which indicated that the user's home institution is a member of SURF • In the future, this can be used to determine membership of non-institutional collaborative organizations. • This attribute is generated by SURFconext and is available to SP's; it should not be set by IdP's.

Preferred Language

urn:mace	urn:mace:dir:attribute-def:preferredLanguage
urn:oid	urn:oid:2.16.840.1.113730.3.1.39
Multiplicity	single-valued
Data type	RFC2798 BCP47
Description	a two-letter abbreviation for the preferred language according to the ISO 639 language abbreviation code table; no subcodes.
Examples	nl en
Notes	Used to indicate an individual's preferred written or spoken language. This is useful for international correspondence or human-computer interaction. Values for this attribute type MUST conform to the definition of the Accept-Language header field defined in RFC 2068 with the exception that the value "`:`" should be omitted.

EduPersonTargetedID

urn:mace	urn:mace:dir:attribute-def:eduPersonTargetedID
urn:oid	urn:oid:1.3.6.1.4.1.5923.1.1.1.10
Multiplicity	single-valued
Data type	UTF8 string (unbounded)
Description	The attribute eduPersonTargetedID is a copy of the *persistent* Subject -> NameID, which is generated by SURFconext itself. When an Identity Provider provides the eduPersonTargetedID itself, it is always overwritten by SURFconext.

Examples	<saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent">bd09168cf0c2e675b2def0ade6f50b7d4bb4aae</saml:NameID>
Notes	This attribute is created because the Subject -> NameID itself is not part of the SAML v2.0 attribute list and therefore only is available for an application if the local SAML implementation explicitly supports this. Within SURFconext the Subject -> NameID is explicitly copied into the `eduPersonTargetedID` attribute, including XML, in order for the identifier to be used like any other attribute, but only when NameID is configured to be persistent (as the eduPerson definition of eduPersonTargetedID requires it to be persistent)

eduPersonORCID

urn:mace	urn:mace:dir:attribute-def:eduPersonOrcid
urn:oid	urn:oid:1.3.6.1.4.1.5923.1.1.1.16
Multiplicity	multi-valued (see remark below)
Data type	URL, registered with ORCID.org
Description	The ORCID is a persistent digital identifier that distinguishes the account holder from every other researcher. Through integration in research workflows such as manuscript and grant submission, the ORCID identifier supports automated linkages between the account holder and his/her professional activities ensuring that the account holder's work is recognized. Values MUST be valid ORCID identifiers in the ORCID preferred URL representation, i.e. http://orcid.org/0000-0002-1825-0097
Examples	`http://orcid.org/0000-0002-1825-0097` `http://orcid.org/0000-0001-9351-8252`
Notes	Although the attribute is in theory multi-valued, in practice it probably makes sense that it has no more than one value.

eduPersonAssurance

urn:mace	urn:mace:dir:attribute-def:eduPersonAssurance
urn:oid	urn:oid:1.3.6.1.4.1.5923.1.1.1.16
Multiplicity	multi-valued
Data type	URL
Description	Set of URIs that assert compliance with specific standards for identity assurance.
Examples	`https://refeds.org/assurance/ID/unique` `https://refeds.org/assurance/IAP/medium`
Notes	Assertion by the home institution about specific aspects of identity proofing or authentication strength, according to the standards as outlined in REFEDS Assurance Framework. For institutions, more information is available at Vrijgeven van eduPersonAssurance.

ECK ID

urn:mace	urn:mace:surf.nl:attribute-def:eckid
urn:oid	-
Multiplicity	single-valued
Data type	URL as specified by Edu-K, all-lowercase
Description	Educatieve Content Keten Identifier (ECK ID) is a pseudonymous identifier for access to content for primary, secondary and vocational education.
Examples	• https://ketenid.nl/spv1/eacf3765ad342feb5f65c2bf8194b4ccc3d68cec3c01d3c260636747a2b06d092fcc3a8d655bbdc4ae7d815ed005cf3a11f e9cab2365f95da3e9965501f7c98e • https://ketenid.nl/201703/1a5c9c7203901866532c2d72ce056e1d29cacc70836fe2bc3a517f3f9a53eed3d77ef370ad6dcf80b3f34ced1c547c7d2e679e8e47002355f938213b3656b206
Notes	This attribute may only be used for “the access to and use of digital learning resources or the digital administration of tests and exams”. For more information see https://www.eck-id.nl (Dutch). Also, if you query this claim information from an external data stores, such as an Enterprise Active Directory, Lightweight Directory Access Protocol (LDAP) directories or a Microsoft SQL Server, you can also define custom attribute stores to query the ECK ID claim from external data stores. Read this Microsoft blog to get to know more.

SURF CRM ID

urn:mace	urn:mace:surf.nl:attribute-def:surf-crm-id
urn:oid	urn:oid:1.3.6.1.4.1.1076.20.100.10.50.2
Multiplicity	single-valued
Data type	Microsoft GUID
Description	GUID of the organization to which the IdP belongs, as used in the SURF CRM.
Examples	ad93daef-0911-e511-80d0-005056956c1a
Notes	• SURF specific and only to be used by SURF SPs that have to interface with the SURF CRM. • Only to be used after consultation with SURF. • This attribute is linked by SURFconext and is available to SP's; it should not be set by IdP's.

MS AuthnMethodsReferences

Name	http://schemas.microsoft.com/claims/authnmethodsreferences
Multiplicity	multi-valued
Data type	URI
Description	The AuthnContext-referenties involved in authenticating the current user on their home IdP.
Examples	`urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport` `http://schemas.microsoft.com/claims/multipleauthn`
Opmerkingen	• Exclusively for use between IdPs and SURFconext; not available to SPs. • Used when the institution has a Microsoft ADFS IdP, to communicate the used MFA method to SURFconext. Not needed or useful when this functionality is not used by the institution in question. • No other uses. For comparable but more generic SAML 2.0-functionality, see the AuthnContextClassRef sent in each assertion.

OrganizationalUnitName

urn:mace	urn:mace:dir:attribute-def:ou
urn:oid	urn:oid:`2.5.4.11`
Multiplicity	multi-valued
Data type	UTF-8 string
Description	Indicates the department, team, or faculty with which the user is associated within the issuing institution. This attribute is multi-valued, so multiple departments, teams or faculties can be listed
Examples	• `ICT Services` • `Industrial Engineering & Innovation Sciences` • `Facility Management Center`
Notes	• The values of this attribute are scoped to the identity provider that is authoritative for the attribute. • Content is by definition institution-specific. It has no other meaning other than agreed upon between SP and IdP.

eduID

urn:mace	urn:mace:eduid.nl:1.1
Multiplicity	single-valued
Data type	UTF-8 string
Beschrijving	Targeted unique eduID-identifier for a user
Voorbeelden	658b6b41-7c13-431d-b3b4-663e9077c24c f4c9afe4-b9e1-42bb-92b8-047ac8711e29
Opmerkingen	• This is a targeted identifier for a person. • It will preferbly be formatted as a version 4 UUID. • An eduID-identifier exists independent of an educational institution. • The eduID-identifier is meant for services where an institution-independent account is useful, or when data on a user needs to be exchanged between institutions.