Attributen in SURFconext (NL)

Vertaling

Let op! Deze pagina is een vertaling van de Engelstalige pagina Attributes in SURFconext . De Engelstalige pagina is het meest up-to-date, en in het geval dat de Nederlandstalige en de Engelstalige pagina elkaar tegenspreken, is de Engelstalige pagina autoritief.

Lees dus bij voorkeur de Engelstalige versie van deze pagina.

Deze pagina geeft een overzicht van alle SAML2 attributen die SURFconext en hun Identity Providers te bieden hebben. Een attribuut is een kenmerk die een gebruiker beschrijft. Het is een 'naam:waarde' paar. De attributen in de SAML-assertion komen overeen met bepaalde attributen die een serviceprovider nodig heeft om te kunnen werken. In het algemeen zijn ze nodig om:

- **Gebruikersinformatie** van de Identiteitsprovider aan de serviceprovider over te dragen
- **Toegang te krijgen tot een account** bij de serviceprovider
- **Specifieke diensten** toe te staan bij de serviceprovider

Wanneer een gebruiker zich aanmeldt bij een Service Provider, stuurt SURFconext een zogehete SAML-assertion naar de Service Provider via de browser van de gebruiker. Deze bevat:

- Een **User Identifier**. Alle diensten krijgen deze en het bestaat uit een configureerbaar Transiënt- of Persistent NameID.
- **Extra attributen**. Deze zijn optioneel en verschillen per dienst.

De SAML2-implementatie van SURFconext voldoet aan het SAML2int profiel 0.2.1.

In de header op bovenstaande link staat dat het werk aan saml2int is verhuisd naar Kantara Initiative. SURFconext houdt zich tot nader orde aan de SAML2int-profielversie 0.2.1.

Voordat je je gaat verdiepen in de theoretische zaken op deze pagina, loont het om onze 'best practice' pagina (EN) te lezen. Hier krijg je een introductie tot en hoe attributen het beste gebruikt kunnen worden in SURFconext.

Identifiers van een gebruiker

De identiteit van een gebruiker wordt doorgestuurd in de vorm van een element wat het NameID heet. Iedere IdP wordt verplicht een NameID mee te sturen. Vanwege privacy genereert SURFconext een nieuwe NameID en plaatst een kopij daarvan in het attribuut eduPersonTargetedID, maar alleen als het NameIID geconfigureerd is als persistent (dus niet indien het als transient is geconfigureerd).

Wij bevelen sterk aan dat Service Providers het NameID of eduPersonTargetedID gebruiken om gebruikers uniek te identificeren. Het NameID is, in tegenstelling tot bijvoorbeeld het e-mailadres, stabiel en zal niet snel veranderen (uitgezonderd het gebruik van 'transient' identifiers). SURFconext genereert een NameID voor iedere nieuwe gebruiker. Deze is uniek voor de gebruiker en specifiek voor een bepaalde SP. Dit zorgt ervoor dat SP's deze informatie niet kan correleren met andere diensten.

Er zijn twee typen NameId's:

- `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent`
  Een persistent NameID bevat een willekeurige en unieke code om de gebruiker voor deze Service Provider te identificeren. Deze blijft blijft hetzelfde over verschillende sessies.
- `urn:oasis:names:tc:SAML:2.0:nameid-format:transient`
  Deze bevat een willekeurige unieke code om de gebruiker voor deze Service Provider uniek te identificeren tijdens een sessie. Wanneer de gebruikerssessie bij SURFconext verloopt en de gebruiker opnieuw aanmeldt op een dienst, wordt een nieuwe tijdelijke, transiente, NameID gegenereerd.

Opmerking

De attributen NameID (indien geconfigureerd als persistent) en eduPersonTargetedID, wat feitelijk een kopie is van het NameID, zijn onveranderlijk maar dit is zo tot op zekere hoogte. In sommige gevallen kan het zijn dat er door een service provider of een identity provider keuzes gemaakt worden die er voor zorgen dat het NameID toch wijzigt. Het NameID, zoals gebruikt in de SAML assertion naar de service provider bij het aanmelden op de dienst, is een samenstelling van de attributen **uid**, **schacHomeOrganization**, het **Entity ID** van de **service provider** samen met een geheim wat gebruik maakt van een SHA algoritme. Als een instelling of dienstverlener er voor kiest bij een dienst die al in productie is één van deze attributen aan te passen zal het er toe leiden dat SURFconext een nieuw NameID en eduPersonTargetedID gaat genereren. Dit kan tot gevolg hebben dat gebruikers geen toegang meer hebben tot hun profielen bij diensten. Als wij zien dat een instelling dan wel dienstverlener voornemens is één van deze attributen aan te passen zullen wij dit ter sprake brengen en ze wijzen op de gevolgen.

Veranderen van attributen

Als Identity Provider is het belangrijk je te beseffen dat het veranderen van attributen in productie op SURFconext op wat voor manier ook invloed kan hebben op de diensten waar gebruikers toegang toe hebben. Attributen die je aan SURFconext aanbiedt, worden gebruikt om profielen aan te maken, waaraan vaak gegevens worden gekoppeld. Het veranderen van een attribuut kan ongewenste resultaten hebben, zoals gebruikers die geen toegang meer hebben tot hun waardevolle gegevens. Een voorbeeld hiervan is het aanpassen van de manier waarop je (onder andere) het e-mailadres invult. Bijvoorbeeld: het wijzigen van 'student.123456@university.nl' in 'john.doe@university.nl'. Bent je van plan dit te doen of start je een project waar dit het geval is? Neem dan contact met ons op en stuur een e-mail naar support@surfconext.nl.

Links

- Tabel met **attributen die we onze instellingen aanbevelen om vrij te geven** https://wiki.surfnet.nl/display/surfconextdev/Vereiste+attributen
- Profiel pagina https://profile.surfconext.nl/ , **laat zien welke attributen er door uw IdP worden doorgegeven** aan SURFconext
- **Voor nieuwe IdP's of voor IdP's die hun omgeving upgraden:** systeembeheerders worden op enig moment gevraagd de metadata van hun account te delen voor analyses. Ga dan naar deze pagina en klik op de 'Mail to SURFconext' knop. We nemen contact met u op wanneer we de ingediende metadata hebben beoordeeld. Deze pagina toont u ook de gedeelde attributen.

Attributenschema's

Een attributenschema is een abstracte representatie van de karakteristieken van een object, en de relatie tot andere objecten.

SURFconext ondersteunt twee attributen schema's:

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

Beiden kunnen worden gebruikt om dezelfde informatie uit te drukken. De uitzondering hierop is het NameID, deze is enkel beschikbaar binnen het urn:oid schema. Standaard geeft SURFconext de attributen door in beide schema's als onderdeel van de assertion. Desalniettemin wordt het door elkaar gebruiken van de schema's afgeraden.

Attributenoverzicht

SURFconext ondersteunt het vrijgeven van de volgende attributen:

Omschrijving	Attribuutnaam	Definitie	Data type	Voorbeeld
ID	(NameID) urn:mace:dir:attribute-def: eduPersonTargetedID urn:oid:1.3.6.1.4.1.5923.1.1.1.10	eduPerson (1)	UTF8 string (unbounded)	bd09168cf0c2e675b2def0ade6f50b7d4bb4aae
Surname	urn:mace:dir:attribute-def:sn urn:oid:2.5.4.4	X.520	UTF8 string (unbounded)	Vermeegen
Given name or first name	urn:mace:dir:attribute-def: givenName urn:oid:2.5.4.42	X.520	UTF8 string (unbounded)	Mërgim Lukáš Þrúður
Common name or Full Name	urn:mace:dir:attribute-def:cn urn:oid:2.5.4.3	X.520	UTF8 String (unbounded)	Prof.dr. Mërgim Lukáš Vermeegen , PhD.
Display name	urn:mace:dir:attribute-def: displayName urn:oid: 2.16.840.1.113730.3.1.241	RFC2798	UTF8 String (unbounded)	Prof.dr. Mërgim L. Vermeegen , PhD.
Email address	urn:mace:dir:attribute-def:mail urn:oid: 0.9.2342.19200300.100.1.3	RFC4524	RFC-5322 address (max 256 chars)	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	Schac	RFC-1035 domain string	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	Schac	RFC-2141 URN see Schac standard	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	Schac	RFC-2141 URN see SURFnet registry	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	eduPerson (1)	Enum type (UTF8 String)	employee, student, faculty, member, affiliate, pre-student (staff is niet meer in gebruik; library-walk-in, alum zijn niet toegestaan)
Scoped affiliation	urn:mace:dir:attribute-def: eduPersonScopedAffiliation urn:oid:1.3.6.1.4.1.5923.1.1.1.9	eduPerson (1)	UTF8 String user@domain	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	eduPerson (1)	RFC-2141 URN Multi-valued	Wordt gedefineerd per dienst (zie Standardized values for eduPersonEntitlement)
PrincipalName	urn:mace:dir:attribute-def: eduPersonPrincipalName urn:oid:1.3.6.1.4.1.5923.1.1.1.6	eduPerson (1)	UTF8 String user@scope	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	eduMember	RFC-2141 URN Multi-valued	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	RFC4519	UTF8 String (max 256 chars)	s9603145 flåp@example.edu
preferredLanguage	urn:mace:dir:attribute-def: preferredLanguage urn:oid:2.16.840.1.113730.3.1.39	RFC2798 BCP47	List of BCP47 language tags	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	eduPerson (1)	URL registered with ORCID.org	http://orcid.org/0000-0002-1825-0097
ECK ID	urn:mace:surf.nl:attribute-def: eckid	SURF / Edu-K	URL zoals gedefinieerd door Edu-K	https://ketenid.nl/spv1/eacf3765ad342...cf3a11fe9cab2365f95da3e9965501f7c98e (Attribuut korter gemaakt voor de leesbaarheid)
SURFCRM ID	`urn:mace:surf.nl:` `attribute-def:`surf-crm-id	SURF	GUID van de aangesloten instelling zoals in SURF CRM	ad93daef-0911-e511-80d0-005056956c1a

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

Verouderde attributen

SURFconext beschouwt de attributen **nlEduPersonOrgUnit** , **nlEduPersonStudyBranch** en **nlStudielinkNummer** als **verouderd**. Deze worden niet meer toegepast bij nieuw op te voeren SP's in SURFconext. Als je al een IdP of SP bij SURFconext hebt geregistreerd die gebruik maakt van deze attributen kunnen deze tot nader order gebruikt worden.

Gedetailleerde beschrijvingen van de attributen

ID

Zie de paragraaf Identifiers van een gebruiker.

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)
Omschrijving	De achternaam van een gebruiker (Inclusief woorden als “van”, “de”, “von” etc.) en wordt gebruikt voor personalisatie; dit kan een combinatie zijn van bestaande attributen.
Voorbeeld	Vermeegen
Opmerking	

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)
Beschrijving	Voornaam / 'name known by'; combinatie van titel, initialen, en 'name known by' zijn mogelijk.
Voorbeeld	Jan Klaassen Mërgim K. Lukáš Þrúður
Opmerking	

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)
Omschrijving	Volledige naam.
Voorbeeld	Prof.dr. Mërgim Lukáš Vermeegen , PhD.
Opmerking	Bijvoorbeeld: een gebruikersnaam in een Engelssprekend land bevat een persoonlijke titel (bijvoorbeeld dhr., mw., professor, mijnheer, Lord), een voornaam, 2e (en verdere) naam, achternaam, kwalificatie van de generatie (als die er is, bijvoorbeeld Jr.) en onderscheidingen en prijzen (als die er zijn; bijvoorbeeld een onderscheiding Commander of the Order of the British Empire, 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)
Omschrijving	Naam zoals weergegeven in applicaties.

Voorbeeld	Prof.dr. Mërgim Lukáš Vermeegen , PhD.
Opmerkingen	Mogelijkerwijs kunnen gebruikers zelf invloed hebben op deze waarde. Daarom is deze niet geschikt voor identificatie.

Email-adres

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)
Omschrijving	e-mailadres; syntax in overeenstemming met RFC 5322
Voorbelden	m.l.vermeegen@university.example.org "very.unusual.@.unusual.com"@example.com mlv@[IPv6:2001:db8::1234:4321];
Opmerkingen	• Meerdere e-mailadressen zijn toegestaan. Echter, er is geen evidente strategie voor SP's over hoe hiermee om te gaan (beide gebruiken? één kiezen? de gebruiker vragen er één te kiezen); de SP zal een strategie moeten bedenken die past binnen de context van de applicatie. Als IdP is het, voor de interoperabiliteit, aan te raden om het sturen van meerdere waarden in dit attribuut te vermijden waar mogelijk. • Het e-mailadres hoeft niet noodzakelijk het e-mailadres van de gebruiker bij de organisatie te zijn. • Gebruik dit attribuut niet om een gebruiker uniek te identificeren. Gebruik daarvoor het NameID. • Het e-mailadres van een gebruiker kan na verloop van tijd veranderen, of je kunt een gebruiker toestaan om deze zelf te veranderen. Dit maakt het attribuut ongeschikt voor authenticatie- en autorisatiedoeleinden.

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 de specificatie, maar in SURFconext is slechts 1 waarde toegestaan)
Data type	UTF8 String (max 256 chars); gebruik van spaties en @-characters wordt afgeraden

Omschrijving	De unieke code voor een persoon, die als inlognaam wordt gebruikt binnen een organisatie.
Voorbeelden	s9603145 piet flåp@example.edu
Opmerkingen	• Het uid is geen unieke identifier voor gebruikers van SURFconext. Uid-waarden zijn hoogstens uniek voor elke Identity Provider. • In het ideale geval is de uid niet alleen een inlognaam/-code, maar ook een identifier die gegarandeerd uniek is binnen een organisatie. Op dit moment is zo'n garantie er echter niet. • Gebruik liever het NameID voor unieke identifiers binnen SURFconext dan het uid. • Gebruik het eduPersonPrincipalName-attribuut als een door mensen leesbare unieke identifier nodig is. • Een uid kan elk unicodeteken bevatten. Bijvoorbeeld: '`org:surfnet.nl:joe von stühl`' is een geldig uid. • SURFconext vertaalt @-tekens in het uid naar underscores voordat het NameID op basis hiervan gevormd wordt.

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. Dit MOET een secondary-level domein zijn die in beheer is van de instelling. Bij voorkeur wordt de hoofd-domeinnaam van de instelling gebruikt.
Omschrijving	The user's organization using the organization's domain name; syntax in accordance with RFC 1035.
Voorbeelden	uniharderwijk.nl example.nl
Opmerkingen	• In het verleden stuurde SURFconext ooit de 'home organization' in het attribuut `urn:oid:1.3.6.1.4.1.1466.115.121.1.15`, wat incorrect was. Sinds 2013 is het correcte oid `urn:oid:1.3.6.1.4.1.25178.1.2.9` in gebruik. Om redenen van compatibiliteit wordt de oude (verkeerde) string ook nog steeds opgestuurd. Deze wordt in 2020 verwijderd. • Het is wenselijk dat dit een vaste waarde is die hetzelfde is voor alle gebruikers van de organisatie. • Waarden die met dit attribuut overeen moeten komen mogen niet hoofdlettergevoelig zijn, d.w.z. de waarden "uniharderwijk.nl" en "UniHarderwijk.nl" moeten als gelijk worden beschouwd. Om Interoperabiliteitsredenen schrijft SURFconext kleine letters voor, zoals hierboven gespecificeerd. • SURFconext slaat in zijn configuratie op welke waarde de instelling gebruikt, om bij te kunnen houden als er afwijkende waarden gestuurd worden.

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 (Zie Schac standard)
Omschrijving	Naam van het type organisatie zoals gedefinieerd op http://www.terena.org/registry/terena.org/schac/homeOrganizationType
Voorbeelden	urn:mace:terena.org:schac:homeOrganizationType:int:university urn:mace:terena.org:schac:homeOrganizationType:es:opi
Opmerkingen	• Attributen worden geregistreerd door Terena op http://www.terena.org/registry/terena.org/schac/homeOrganizationType • Dit attribuut wordt doorgaans weinig gebruikt. • Neem contact op met support@surfconext.nl als je gebruik wilt maken van dit attribuut.

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 (zie SURFnet registry)
Omschrijving	Het interne studentnummer, medewerkernummer of persoonsnummer van de gebruiker.
Voorbeelden	urn:schac:personalUniqueCode:nl:local:example.edu:employeeid:x12-3456 urn:schac:personalUniqueCode:nl:local:example.nl:studentid:s1234567
Opmerkingen	• De prefix van de attribuutwaarden wordt door SURFnet geregistreerd op urn:schac:personalUniqueCode:nl:* • Neem s.v.p. contact op met het SURFconext-team als u dit attribuut als IdP of SP wilt inzetten. • De primaire toepassing is het matchen van accounts tegen interne administratiesystemen van studenten en medewerkers.

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
Data type	UTF8 String (only the values enumerated below are allowed)

Beschrijving	Geeft de relatie aan tussen de gebruiker en zijn instelling. De volgende waarden zijn toegestaan binnen SURFconext: • `student` — een bij de Instelling ingeschreven student, extraneus of cursist. • `employee` — een persoon met een aanstelling dan wel een arbeidsovereenkomst bij de Instelling. • ~~`staff` — Alle academische staf (wetenschappelijk personeel, of WP) en docenten~~. (*deprecated* (verouderd); niet gebruiken in nieuwe gevallen) • `faculty` — Persoon wiens primaire taak onderwijs geven of onderzoek doen is (bij universiteiten vaak aangeduid als WP. Let op, doctoraal *studenten* mogen ook deze waarde krijgen.) • `member` — Iedereen die tenminste één van de bovenstaande waardes heeft is automatisch ook member. • `pre-student` — een voorinschrijver, die zich bij een instelling heeft ingeschreven om te gaan studeren maar nog niet een volwaardige student is. Zie deze pagina voor meer informatie over de voorwaarden waaronder voorinschrijvers toegang kunnen krijgen tot SURFconext. SURFconext laat voorinschrijvers nooit toe tot SPs zonder voorafgaande toestemming van de dienstverlener. • `affiliate` — een persoon die anderszins in het kader van de taakuitvoering van de Instelling geautoriseerd is om de dienst te gebruiken Gebruik de bovenstaande voorbeelden om vast te stellen welke waarde een gebruiker krijgt. Indien de definities niet toereikend zijn, gebruik gezond verstand.
Voorbeelden	Zie beschrijving
Opmerkingen	• Alle gebruikers die als affiliation `faculty`, `employee` or `student` hebben, moeten ook de waarde `member` hebben. • Identity Providers kunnen intern aanvullende waarden gebruiken voor het affiliation-attribuut, zoals `alum`. Volgens het beleid van SURFconext mogen deze gebruikers geen toegang krijgen tot SURFconext (dit dient de IdP zelf af te dwingen). • Een andere waarde die in de eduPerson-standaard worden genoemd is `library-walk-in`. Deze waarde wordt niet gebruikt in SURFconext. • Volgens de eduPerson-standaard zijn de waarden van dit attribuut niet hoofdlettergevoelig. Vanwege compatibiliteit eisen wij in SURFconext echter bovenstaande waarden met kleine letters. • Zie REFEDS eduPerson(Scoped)Affiliation usage comparison voor een vergelijk van de waardes in internatiationale conext.

Scoped Affiliation

urn: mace	urn:mace:dir:attribute-def:eduPersonScopedAffiliation
urn: oid	urn:oid:1.3.6.1.4.1.1466.115.121.1.15
Multiplicity	multi-valued
Data type	UTF8 String of the form affiliation@domain (zie onder)
Beschrijving	Beschrijft de relatie tussen de gebruiker en het domein van zijn thuisorganisatie. Het affiliation-gedeelte moet een van de toegestane waarden van het eduPersonAffiliation attribuut zijn (zie direct hierboven). De waarde is de rol van de de gebruiker en de algemene domeinnaam van de instelling. Feitelijk kan eduPersonScopedAffiliation dus gedefinieerd worden als: <eduPersonAffiliation> "@" <schacHomeOrganization>. Dit attribuut is net als eduPersonAffiliation meerwaardig. Het domein-gedeelte moet de schacHomeOrganization van de gebruiker zijn (of een subdomein ervan).
Voorbeelden	`student@uniharderwijk.nl` `faculty@uniharderwijk.nl`

Opmerkingen	• Dit attribuut is primair een andere manier om de informatie uit eduPersonAffiliation en schacHomeOrganization door te geven. Het wordt aangeraden dit attribuut te voeren naast eduPersonAffliation en schacHomeOrganization, omdat sommige SPs in plaats van die twee losse attributen, dit attribuut vragen. • Dit attribuut kan indien gewenst ook gebruikt worden om die rol binnen een faculteit, veld, studie, afdeling waar de gebruiker mee verbonden is te beschrijven. Omdat het attribuut meerwaardig is, kan een gebruiker zowel student bij de ene als medewerker van de andere afdeling zijn.

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
Beschrijving	rechten; een URI (URL of URN) die aangeeft welke rechten een gebruiker heeft.
Voorbeelden	`urn:mace:terena.org:tcs:personal-admin` urn:x-surfnet:surfdomeinen.nl:role:dnsadmin
Opmerkingen	• Dit attribuut kan gebruikt worden om rechten, rollen, enzovoort van Identity Providers door te geven aan diensten, zodat ze bijvoorbeeld gebruikt kunnen worden voor autorisatie. • De Identity Provider bepaalt doorgaans de waarde ervan • De waarde dient te voldoen aan een gestandaardiseerd formaat, zie 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 `voor een gebruiker in de vorm user@scope`

Beschrijving	Unieke identifier voor een gebruiker
Voorbeelden	piet.jønsen@example.edu not.a@vålîd.émail.addreß
Opmerkingen	• Dit is een scoped identifier voor een persoon. Het moet worden weergegeven als user@scope, waarbij de gebruiker een naamgebaseerde identificatiecode voor een persoon is. De scope moet deel uitmaken van het administratief domein van het identiteitssysteem waar de identifier werd aangemaakt en toegewezen. Een IdP kan meerdere scopes hebben, bv. piet@studenthartingcollege.nl of piet@ hartingcollege .nl. Deze Pieten zijn verschillende personen die scopes meekrijgen die geregistreerd zijn door hartingcollege.nl. • Het is gebruikelijk om schacHomeOrganization te gebruiken als scope, als er geen andere scopes zijn gedefinieerd. • Deze waarde lijkt op een e-mailadres maar wordt **NIET** gebruikt als e-mailadres. Meestal kan e-mail niet aan dit 'adres' gestuurd worden. • Hoewel deze waarde een gebruiker uniek identificeert, is het niet gegarandeerd dat de waarde ervan in alle gevallen vast blijft. Gebruik dit attribuut daarom liever niet om gebruikers uniek te identificeren. Gebruik in plaats daarvan het NameID. • Het domein-deel dient een door de instelling gecontroleerd domein te zijn, liefst hetzelfde als of een subdomein van de schacHomeOrganization. • SURFconext neemt in zijn configuratie op welk domein-deel gebruikt mag worden door de instelling zodat afwijkende waarden gesignaleerd kunnen worden.

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
Beschrijving	Somt de samenwerkende organisaties op waarvan de gebruiker lid is.
Voorbeeld	`urn:collab:org:surf.nl`
Opmerkingen	• Attribuutwaarden zijn URI's (URN of URL). • De enige waarde die momenteel ondersteund wordt, is urn:collab:org:surf.nl, die aangeeft dat het thuisnetwerk van de gebruiker lid is van SURFnet. • In de toekomst kan dit attribuut gebruikt worden om te bepalen of een gebruiker lid is van een samenwerkingsorganisatie. • Dit attribuut wordt gegenereerd door SURFconext en is beschikbaar voor SP's. IdP's moeten dit attribuut niet zetten.

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
Beschrijving	Een afkorting van 2 letters voor de voorkeurstaal volgens de ISO 639 codetabel; geen subcodes.
Veerbeelden	nl en
Opmerkingen	Wordt gebruikt om aan te geven aan welke geschreven of gesproken taal de gebruiker de voorkeur geeft. Dit is nuttig voor internationale correspondentie of mens-computer-interactie. Waarden voor dit attribuuttype MOETEN overeenkomen met de definitie van het 'Accept-Language header field' in RFC 2068, met 1 uitzondering: de waarde ':' moet worden weggelaten.

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)
Beschrijving	Het attribuut eduPersonTargetedID is een kopie van de Subject -> NameID (maar alleen als het NameID is geconfigureerd als persistent) welke door SURFconext zelf wordt gegenereerd. Als een Identity Provider de eduPersonTargetedID zelf zet, wordt deze altijd overschreven door SURFconext.
Voorbeeld	bd09168cf0c2e675b2def0ade6f50b7d4bb4aae
Opmerkingen	Dit attribuut is in het leven geroepen omdat de Subject -> NameID zelf geen onderdeel is van de SAML v2.0-respons en dus niet gebruikt kan worden. Als SURFconext de Subject -> NameID expliciet in het attribuut eduPersonTargetedID plaatst, kun je deze wel gebruiken.

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 (maar zie onder)
Data type	URL, geregistreerd via ORCID.org
Beschrijving	Het ORCID is een persistente digitale identifier die de houder onderscheidt van andere onderzoekers. Via integratie in publicatieworkflows leidt dit tot de herkenning van de juiste onderzoeker bij zijn wetenschappelijke activiteiten. Waarden moeten geldige ORCID identifiers zijn in de ORCID-voorkeursrepresentatie als URL, b.v. http://orcid.org/0000-0002-1825-0097

Voorbeelden	`http://orcid.org/0000-0002-1825-0097`
	
	`http://orcid.org/0000-0001-9351-8252`

Opmerkingen	Zie voor achtergrondinformatie over ORCID: https://www.surf.nl/nieuws/2016/02/orcid-nu-beschikbaar-voor-europese-instellingen.html Het attribuut is in theorie multi-valued, maar in de praktijk lijkt het logisch niet meer dan één waarde mee te geven.

ECK ID

urn:mace	urn:mace:surf.nl:attribute-def:eckid
urn:oid	-
Multiplicity	single-valued
Data type	URL zoals gespecificeerd door Edu-K, geheel in onderkast
Beschrijving	Educatieve Content Keten Identifier (ECK ID) is een pseudonieme identificatie voor toegang tot leermaterialen voor primair, secundair en middelbaar beroepsonderwijs.
Examples	https://ketenid.nl/spv1/eacf3765ad342feb5f65c2bf8194b4ccc3d68cec3c01d3c260636747a2b06d092fcc3a8d655bbdc4ae7d815ed005cf3a11fe9cab2365f95da3e9965501f7c98e
Opmerkingen	Dit attribuut mag alleen gebruikt worden voor *“de toegang tot en het gebruik van digitale leermiddelen of het digitaal afnemen van toetsen en examens”*. Voor meer informatie zie https://www.eck-id.nl. Als u deze claiminformatie ophaalt uit een externe bron, zoals een Enterprise Active Directory, LDAP of een Microsoft SQL-server, kunt u aangepaste 'attribute store' definiëren voor het opvragen van de ECK-ID-claim . Lees dit Microsoft blog om meer te weten te komen.

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
Beschrijving	Het GUID van de organisatie (aangesloten instelling) waar de idp van de gebruiker toe behoort, zoals gebruikt in het SURF CRM.

Voorbeelden	ad93daef-0911-e511-80d0-005056956c1a
Opmerkingen	SURF specifiek en alleen te gebruiken voor SURF-eigen SP's die ook een koppeling hebben met het SURF CRM. Uitsluitend in te zetten na overleg met SURFnet.

MS AuthnMethodsReferences

Name	http://schemas.microsoft.com/claims/authnmethodsreferences
Multiplicity	multi-valued
Data type	URI
Beschrijving	De AuthnContext-referenties die betrokken zijn geweest bij de authenticatie van de betreffende user.
Voorbeelden	`urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport` `http://schemas.microsoft.com/claims/multipleauthn`
Opmerkingen	• Uitsluitend in gebruik tussen IdP's en SURFconext; niet beschikbaar voor SP's. • Bedoeld om indien Microsoft ADFS gebruikt wordt, de gebruikte MFA-methode aan SURFconext te communiceren. Niet nodig of nuttig indien deze functionaliteit niet gebruikt wordt door de betreffende instelling. • Geen andere toepassingen. Voor vergelijkbare maar generieke SAML 2.0-functionaliteit, zie de AuthnContextClassRef die meegestuurd wordt in elke assertion.