SWEDISH STANDARDS INSTITUTE

Datum
2017-06-09

Referens
TK 450 AG04
Elevinformation

Kontaktperson SIS:
Jolanta Wallström
jolanta.wallstrom@sis.se

Attributprofil för Skolfederation

Detta dokument förtecknar en federationsgemensam vokabulär bestående av attribut för att beskriva uppgifter om vad som inom Skolfederation kallas en Användare. Dokumentet är framtaget av SIS/TK 450 IT standarder för lärande, arbetsgrupp 4.

Datum	Version	Beskrivning	Ansvarig
2015-01-22	2.3	Infört Revisionshistorik.	Robert Sundin
2015-01-22	2.3	Ändrat definition av attributet norEduOrgUnitUniqueIdentifier från SCB-kod till skolenhetskod.	Robert Sundin
2015-03-10	Utkast 3.1	Redaktionella förändringar.	SIS TK 450 AG04
2015-03-10	Utkast 3.1	Indelningen av attribut i kategorierna "Bas", "Standard" och "utökade" är borttagen.	SIS TK 450 AG04
2015-03-10	Utkast 3.1	Attribut borttaget: eduCourseOffering	SIS TK 450 AG04
2015-03-10	Utkast 3.1	Nytt attribut: sisOrgDepartment	SIS TK 450 AG04
2015-03-10	Utkast 3.1	Nytt attribut: ou	SIS TK 450 AG04
2015-03-10	Utkast 3.1	Nytt attribut: eduPersonScopedAffiliation ersätter eduPersonAffiliation	SIS TK 450 AG04
2015-06-01	Utkast 3.1	Attribut borttaget: ou	SIS TK 450 AG04

2015-06-01	Utkast 3.1	Nytt attribut: sisSchoolUnitCode ersätter norEduOrgUnitUniqueIdentifier	SIS TK 450 AG04
2015-06-01	Utkast 3.1	Kod för förskola är under utredning	SIS TK 450 AG04
2015-06-01	3.1	Publicering av version 3.1	SIS TK 450 AG04
2015-12-15	Utkast 4.0	Nytt attribut: *eduPersonEntitlement*	SIS TK 450 AG04
2016-02-02	Utkast 4.0	Attribut borttaget: postOfficeBox	SIS TK 450 AG04
2016-03-08	Utkast 4.0	Attribut borttaget: eduCourseMember	SIS TK 450 AG04
2016-03-08	Utkast 4.0	Nytt attribut: *sisSchoolCourseStudent*	SIS TK 450 AG04
2016-03-08	Utkast 4.0	Nytt attribut: *sisSchoolCourseTeacher*	SIS TK 450 AG04
2016-05-13	Utkast 4.0	Nytt attribut: *sisSchoolCareOfName*	SIS TK 450 AG04
2016-06-09	4.0	Publicering av version 4.0	SIS TK 450 AG04
2017-06-09	4.1	Korrigering av sisOrgDepartment (från 1.2.752.194.10.3 till 1.2.752.194.10.2.3)	SIS TK 450 AG04

Innehållsförteckning

Syfte med detta dokument

Detta dokument förtecknar en federationsgemensam vokabulär bestående av attribut för att beskriva uppgifter om vad som inom Skolfederation kallas en Användare. Dokumentet är framtaget av SIS/TK 450 IT standarder för lärande, arbetsgrupp 4.

Dokumentet är tänkt att användas på följande sätt:

- För att lista de attribut som kan ingå i en teknisk överenskommelse mellan huvudman och tjänsteleverantör.
- För att hålla en tydlig definition av attributens innebörd.
- För att anvisa hur information ska kodas.

Krav

1. När en viss uppgift om en Användare behöver kunna presenteras för en e-tjänst och det i detta dokument finns ett attribut för denna uppgift ska det attributet användas. Andra representationer för samma uppgift ska med andra ord inte användas.

2. Representationen av attribut ska följa deploymentprofilen http://saml2int.org. Det innebär bland annat att *NameFormat* ska vara urn:oasis:names:tc:SAML:2.0:attrname-format:uri, t.ex. ska *urn:oid:0.9.2342.19200300.100.1.3* användas som namn för attributet e-post (alltså inte *mail*).

3. I en överenskommelse mellan huvudmannen och tjänsteleverantören ska avgöras vilka attribut som presenteras för tjänsteleverantören. Personuppgiftsbiträdesavtal samt ytterligare kravställning ska också ingå i överenskommelsen. Ytterst är det huvudmannen som har ansvaret för vilka uppgifter som tillgängliggörs och till vem. Läs mer på http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/skolor/checklista-for-hantering-av-personuppgifter/.

Rekommendationer

1. En minimalistisk princip ska gälla så att inte fler attribut än nödvändigt presenteras för en tjänst.

2. Det finns inget krav på att samtliga attribut behöver finnas och kunna levereras för att en huvudman ska få vara med i federationen.

3. Ett av syftet med Skolfederation är att inte exponera personuppgifter mer än nödvändigt. Olika attribut har olika potential att exponera personuppgifter. Vissa utgör normalt ingen risk för integriteten och kan därför ingå i alla intyg medan andra kan innehålla uppgifter som är av känsligare art. Attribut bör därför inte användas utan en noggrann prövning av säkerhet och personuppgiftshantering. Vid prövningen ska en samlad bedömning göras av det som tillgängliggörs.

Vokabulär

Attributen i denna vokabulär ska kunna användas för att ange uppgifter om en Användare, definierad som *den fysiska person som har tilldelats en identitet i Skolfederation*.

För varje attribut nedan anger rubriken en benämning som bör användas i löpande text för att beteckna den uppgift som attributet representerar. Därefter följer namnet och representationen av attributet, en förklarande text och eventuellt ett exempel.

NameID

Enligt den deploymentprofil som Skolfederation använder (http://saml2int.org) så ska en IdP alltid ha förmågan att sätta ett transient-id som NameID och eventuellt, som ett alternativ därtill, istället använda ett persistent-id. Andra format avrådes. Transient-id är ett engångs-Id för användaren, som gäller *bara* för en specifik inloggning. Persistent-id är ett icke spårbart, men över tid persistent, ID för användaren i relation till just en viss IdP och en viss SP. Se deploymentprofilen för detaljer.

Det är bra att förstå att en SP inte nödvändigtvis måste förlita sig på NameID som unik identifierare för en användare. Ett vanligt undantag att SP:n hellre använder ett attribut som en spårbar identifierare, såsom eduPersonPrincipalName (eppn) som är gemensam för flera tjänster. Det är personuppgiftsombudets ansvar att bedöma om det är rimligt att tjänsten har behov av spårbara identifierare.

Attribut

Personnummer

norEduPersonNIN (urn:oid:1.3.6.1.4.1.2428.90.1.5)

Svenskt personnummer, tilldelat personnummer eller Skatteverkets samordningsnummer för Användaren.

Ska anges med 12 siffror utan separatorer.
Exempel: 200112240123

Samordningsnummer ska anges med 12 siffror utan separator. Födelsedagen adderas med talet 60, det vill säga någon född den 24 i en månad får talet 84 som dag.
Exempel: 200112840123

Födelsedatum

norEduPersonBirthDate (urn:oid:1.3.6.1.4.1.2428.90.1.3)

Användarens födelsedatum, angivet på formen *yyyymmdd*.
Exempel: 20010104.

Kön

schacGender (urn:oid:1.3.6.1.4.1.25178.1.2.2)

Legalt kön hos Användaren.
Det kodas med 0 – för okänt, 1 – för man, 2 – för kvinna och 9– för ospecificerat eller ej tillämpbart.

Användaridentifierare

eduPersonPrincipalName (urn:oid:1.3.6.1.4.1.5923.1.1.1.6)

Den identifierare som ska användas för att identifiera användaren i skilda e-tjänster. Identifieraren ska vara en spårbar, persistent och globalt unik sträng.

Den ska bestå av en lokalt unik användaridentifierare, ett ’@’ och en domän. En domän är ofta, men inte nödvändigtvis, samma som organisationens internet-domännamn.
Exempel: kalko@edu.goteborg.se

Förnamn

givenName (urn:oid:2.5.4.42)

Användarens förnamn, med fördel tilltalsnamnet.
Exempel: Valfrid

Efternamn

sn (urn:oid:2.5.4.4)

Användarens efternamn.
Exempel: Lindeman

Visat namn

displayName (urn:oid:2.16.840.1.113730.3.1.241)

Användarens namn så som det ska visas, normalt på formatet *förnamn efternamn*.
Exempel: Valfrid Lindeman

c/o

sisSchoolCareOf (urn:oid: 1.2.752.194.10.2.7)

Namn på person vars adress ska användas för post eller leverans när adressaten är någon annan.
Exempel: Valfrid Lindeman
c/o Sara Andersson

Gatuadress

street (urn:oid:2.5.4.9)

Användarens gatuadress.
Exempel: VETTERSLUNDSGATAN 30 LGH 1303

Postnummer

postalCode (urn:oid:2.5.4.17)

Användarens postnummer.
Ska anges med 5 siffror utan separatorer.
Exempel: 12345

Postort

l (urn:oid:2.5.4.7)

Användarens postort.
Exempel: Tidaholm.

Land

c (urn:oid:2.5.4.6)

Det land i vilket Användaren är bosatt, kodat i enlighet med ISO-3166.
Exempel: SE

Mejladress

mail (urn:oid:0.9.2342.19200300.100.1.3)

En mejladress för att komma i kontakt med Användaren.
Exempel: valfrid.lindeman@example.com

Telefonnummer

telephoneNumber (urn:oid:2.5.4.20)

Användarens telefonnummer i enlighet med ITUs rekommendation E.123.
Exempel: +46 31 123 4567

Mobiltelefonnummer

mobile (urn:oid:0.9.2342.19200300.100.1.41)

Användarens mobiltelefonnummer i enlighet med ITUs rekommendation E.123.
Exempel: +46 70 123 4567

Vårdnadshavares barn

sisLegalGuardianFor (urn:oid: 1.2.752.194.10.2.1) Flervärt värde.

Barn som Användaren är juridisk vårdnadshavare för. Barnet identifieras med personnummer, samordningsnummer eller tillfälligt personnummer.

Ska anges med 12 siffror utan separatorer.
Exempel: 201412240123

Årskurs

sisSchoolGrade (urn:oid:1.2.752.194.10.2.2)

Den årskurs som en Användare, i praktiken en elev, går i.
Den ska kodas med F för förskolan, 0-10 för grundskolan, 11-14 för gymnasiet och V för vuxenutbildning.

Organisation

o (urn:oid:2.5.4.10)

Namnet på den organisation som Användaren tillhör.
Exempel: Göteborgs stad

Huvudman

norEduOrgNIN (urn:oid:1.3.6.1.4.1.2428.90.1.12)

Organisationsnumret för den skolhuvudman som Användaren är associerad med.
Exempel: 212000-1355

Förvaltning

sisOrgDepartment (urn:oid:1.2.752.194.10.2.3) Flervärt värde.

Används för att beskriva Användarenstillhörighet till kommunal förvaltning, stadsdel eller motsvarande organisatorisk enhet i syfte att kunna styra Användarens tillgång till resurser.

Skolenhetskod

sisSchoolUnitCode (urn:oid:1.2.752.194.10.2.4) Flervärt värde.

Den skolenhet som Användaren tillhör, i form av den åttasiffriga skolenhetskod som Skolverket tilldelat skolenheten (http://www.scb.se/skolreg/).
Exempel: 14801860

Roll i undervisningsorganisation

eduPersonScopedAffiliation (urn:oid:1.3.6.1.4.1.5923.1.1.1.9) Flervärt värde.

Detta attribut fasas ut från Attributprofilen under 2016.

Attributet avser den eller de roller som användaren har i förhållande till organisationen. Om användaren har flera roller i organisationen så kan det vara den roll som användaren på något sätt aktivt valt att agera som, eller, om användaren inte valt, så kan det vara samtliga roller. Attributet är flervärt. Varje värde anges med en av de giltiga koderna, ett ’@’ och en säkerhetsdomän. En säkerhetsdomän är ofta, men inte nödvändigtvis, samma som organisationens internetdomän.

Tillåtna koder är: *faculty, student, staff, alum, member, affiliate, employee, library-walk-in. member* är tänkt att inkludera alla med en medlemsliknande relation till skolan, det vill säga *employee, faculty, student, staff*. För dessa roller MÅSTE även det gemensamma värdet *member* anges. På samma sätt MÅSTE för *faculty* och *staff* även det gemensamma *employee* anges. Se tabell för en enkel förklaring.

Kodvärdena är ordnade i en hierarkisk struktur enligt nedan.

Roll	**Värde 1**	**Värde 2**	**Värde 3**
Elev	*member@domän*	*student@domän*	
Student	*member@domän*	*student@domän*	
Lärare	*member@domän*	*employee@domän*	*faculty@domän*
Pedagogisk personal	*member@domän*	*employee@domän*	*faculty@domän*
Betygsättande lärare	*member@domän*	*employee@domän*	*faculty@domän*
Hjälplärare	*member@domän*	*employee@domän*	*faculty@domän*
Administrativ personal	*member@domän*	*employee@domän*	*staff@domän*
Övrig personal	*member@domän*	*employee@domän*	*staff@domän*
Frivilligarbetare	*affiliate@domän*		
Elever och studenters förälder eller vårdnadshavare	*affiliate@domän*		
Gästföreläsare	*affiliate@domän*		
Alumni	*alum@domän*		
Tidigare medlem	*alum@domän*		
Annan nyttjare	*library-walk-in@domän*		

Elev i elevgrupp

sisSchoolCourseStudent (urn:oid: 1.2.752.194.10.2.5) Flervärt värde.

Med elevgrupp avses en grupp elever. Elevgrupper kan bestå av exempelvis skolgemensam undervisningsgrupp, klass, ämnesgrupp, kursgrupp eller annan grupp.

Syftet med elevgrupper är att kunna administrera resurser (personal, lokaler, tjänster) i förhållande till en grupp elever.

En elevgrupp identifieraras med en unik URI. Det viktiga är att URI:n är unik, innehåller en domän och en **över tid unik** identifierare för den avsedda gruppen.

Attributet avser elev i en viss elevgrupp.

Elevgruppen ska formateras som 'http://' + säkerhetsdomän + '/' + skolenhetskod + '/' gruppidentifierare.

Notera att gruppidentifieraren måste URL-kodas om den innehåller exempelvis '/', ':' eller andra specialtecken.
Exempel: http://goteborg.se/ 61701709/IDHIDH01-2015%2F16

Lärare för elevgrupp

sisSchoolCourseTeacher (urn:oid: 1.2.752.194.10.2.6) Flervärt värde.

Med elevgrupp avses en grupp elever. Elevgrupper kan bestå av exempelvis skolgemensam undervisningsgrupp, klass, ämnesgrupp, kursgrupp eller annan grupp.

Syftet med elevgrupper är att kunna administrera resurser (personal, lokaler, tjänster) i förhållande till en grupp elever.

En elevgrupp identifieraras med en unik URI. Det viktiga är att URI:n är unik, innehåller en domän och en **över tid unik** identifierare för den avsedda gruppen.

Attributet avser lärare för en viss elevgrupp.

Hur attributet ska kodas är beskrivet i *sisSchoolCourseStudent*.

Tilldelning av resurser

eduPersonEntitlement (urn:oid: 1.3.6.1.4.1.5923.1.1.1.7) Flervärt värde.

Attributet syftar till att beskriva användarens tillgång till resurser. Exempel på resurser är licenser, programvaror, webbtjänster eller fysiska resurser. Resursen definieras som en URN på ett mellan huvudman och tjänsteleverantör överenskommet format. För enklaste identifiering inleds den med ett domännamn som kopplas till tjänsteleverantören.

Attributet är flervärt.
Exempel:
http://xstor.com/contracts/HEd123
http://eduX.se/<skolenhet>#<kurskod>&<roll>