

Överföringsformat för behörighetsinformation på NyA-webben

Innehållsförteckning

Innehållsförteckning	2
1 Inledning	3
1.1 Bakgrund	3
1.2 Referenser	3
1.3 Versionshistorik	3
2 Attribut.....	4
3 Överföringsformat	4
3.1 Behörighetsmodell	4
3.2 GMAI.....	5

1 Inledning

1.1 Bakgrund

NyA-webben ger en användare möjlighet att se uppgifter som finns registrerade i NyA-systemet. Det går det att se uppgifter om en sökandes anmälan, meriter och dokument. Dessutom går det att få listningar och statistik om sökande sammantaget på en institution.

Autentisering sker med en federerad lösning. NyA-systemet lagrar ingen information om användare av NyA-webben, all behörighetsinformation kommer via den federerade inloggningen.

Syftet med detta dokument är att specificera formatet för överföringen av den behörighetsinformation som behövs för NyA-webben.

1.2 Referenser

- [1] General Model for Authorization Information
(<http://www.swami.se/content/1/c6/01/13/67/gmai.pdf>)

1.3 Versionshistorik

Version	Datum	Författare	Kommentar
1	2010-10-25	Jon Larsson	För kommentarer
2	2010-10-26	Jon Larsson	Förtydligat 3.2.4
3	2010-11-26	Jon Larsson	Förtydligat 3.1.2, 3.2 samt 3.2.1
4	2010-12-07	Jon Larsson	Uppdaterat 3.2.3 och 3.2.5
5	2011-01-12	Jon Larsson	Lagt till 2

2 Attribut

För att NyA-webben ska fungera som avsett måste en identity provider som används för inloggning tillhandahålla följande attribut:

eduPersonPrincipalName	Räknas som användarnamn och används vid loggning. En vanlig förkortning på attributet är "eppn".
commonName	Används för att i användargränssnittet visa vem som är inloggad. En vanlig förkortning på attributet är "cn".
eduPersonEntitlement	Detta attribut innehåller behörighetsinformation beskriven under punkt 3 i detta dokument.

3 Överföringsformat

Vid inloggning sker en översättning av den information som kommer från den federerade inloggningen till den behörighetsmodell som gäller för NyA-webben. Behörighetsinformationen kommer från en identity provider serialiserat i GMAI-formatet, se ref [1].

3.1 Behörighetsmodell

Behörighetsmodellen för en inloggad användare på NyA-webben innehåller följande:

- En eller flera roller
- Ett lärosäte
- Ingen, en eller flera institutioner, tillhörande organisationen

3.1.1 Roll

Rollerna är inbördes oberoende, det finns inget nivåbegrepp som det gör för Expertklienten. I nuläget används två roller:

- Institutionsanvändare - utdata (för att skapa listor och statistik)
- Basanvändare (för att titta på info, meriter, anmälningar och dokument för sökande)

3.1.2 Lärosäte

Vissa funktioner är begränsade till det lärosäte som den inloggade användaren tillhör. I nuläget är det funktionerna för att skapa listor och statistik. En användare kan bara skapa listor och statistik som rör anmälningsalternativ på det egna lärosätet.

Däremot är funktionen för att titta på info, meriter, anmälningar och dokument för sökande oberoende av användarens lärosäte. En användare kan se den informationen för alla sökande oavsett vilken antagningsomgång och anmälningsalternativ de sökt till.

3.1.3 Institution

I nuläget används inte användarens institutioner för behörighetskontroll, utan används endast för att begränsa möjliga val i gränssnittet.

3.2 GMAI

GMAI-informationen hämtas från attributet "eduPersonEntitlement". Detta kan ha flera värden för en användare, och vart och ett av dessa mappar mot en roll i behörighetsmodellen. Det generella formatet för ett GMAI-attribut är

```
urn:mace:swami.se:gmai:<application>:<role>(:<scopeDenominator>=<scopeValue>)*
```

Se [1] för mer information.

För NyA-webben är formatet

```
urn:mace:swami.se:gmai:nya-dw:<id för roll>:o=<id för  
lärosäte>;norEduOrgUnitUniqueNumber=<id för institution>
```

3.2.1 Id för roll

Id för roll kan vara

- department (Institutionsanvändare - utdata)
- base (Basanvändare)

3.2.2 Id för lärosäte

Detta id måste svara mot ett giltigt id i NyA-systemet. Värdet är obligatoriskt.

3.2.3 Id för institution

Det går att ange flera institutioner genom att skicka flera GMAI-attribut med samma roll och lärosäte, men olika id:n för institution. Dessa id:n måste vara giltiga i NyA-systemet.

3.2.4 Översättning av GMAI-attribut till behörighetsmodell

Attribut för endast ett lärosäte beaktas vid översättning. Utifrån dessa attribut får användaren följande behörighetsmodell:

- De roller som angetts
- Det lärosäte som angetts
- Unionen av de institutioner som angetts i dessa attribut

Det finns i nuläget inget stöd för att välja vilket lärosäte som ska beaktas i det fall att en användare har mer än ett i sina GMAI-attribut. Ett lärosäte bland dessa väljs för översättning till behörighetsmodellen, men det är ospecificerat vilket. Därför rekommenderas att en användare har samma lärosäte på alla sina GMAI-attribut.

3.2.5 Exempel

En användare har följande GMAI-attribut:

- urn:mace:swami.se:gmai:nya-dw:department:o=LU:norEduOrgUnitUniqueNumber=4500
- urn:mace:swami.se:gmai:nya-dw:department:o=LU:norEduOrgUnitUniqueNumber=3011

- urn:mace:swami.se:gmai:nya-dw:base:o=LU

Behörighetsmodellen på NyA-webben blir då

- Roller: Basanvändare, Institutionsanvändare - utdata
- Lärosäte: Lunds universitet (LU)
- Institutioner: 4500, 3011 (Institutioner på LU)