

INTERNET   
STIFTELSEN

# Internetstiftelsens Tekniska Federationsforum

Tekniska nyheter och diskussion

13:02-14:30, 8 september 2022

# Syfte

- Att från federationsoperatörens håll presentera tekniska nyheter avseende Internetstiftelsens federationer
- Att samla in synpunkter och frågor från omvärlden
- Nätverksbyggande

# Om ITFF

- Forumet är i form av ett "öppet hus" med teknisk inriktning
- Ett forum för både Skolfederation och Sambi
- Typiskt ingen fast agenda eller minnesanteckningar
- Alla är välkomna – medlemmar som icke-medlemmar, leverantörer, integratörer, konsulter

# Agenda

- Dagens fokus: EPPN
- ~~Nyheter från federationsoperatören~~
- Diskussion och frågestund

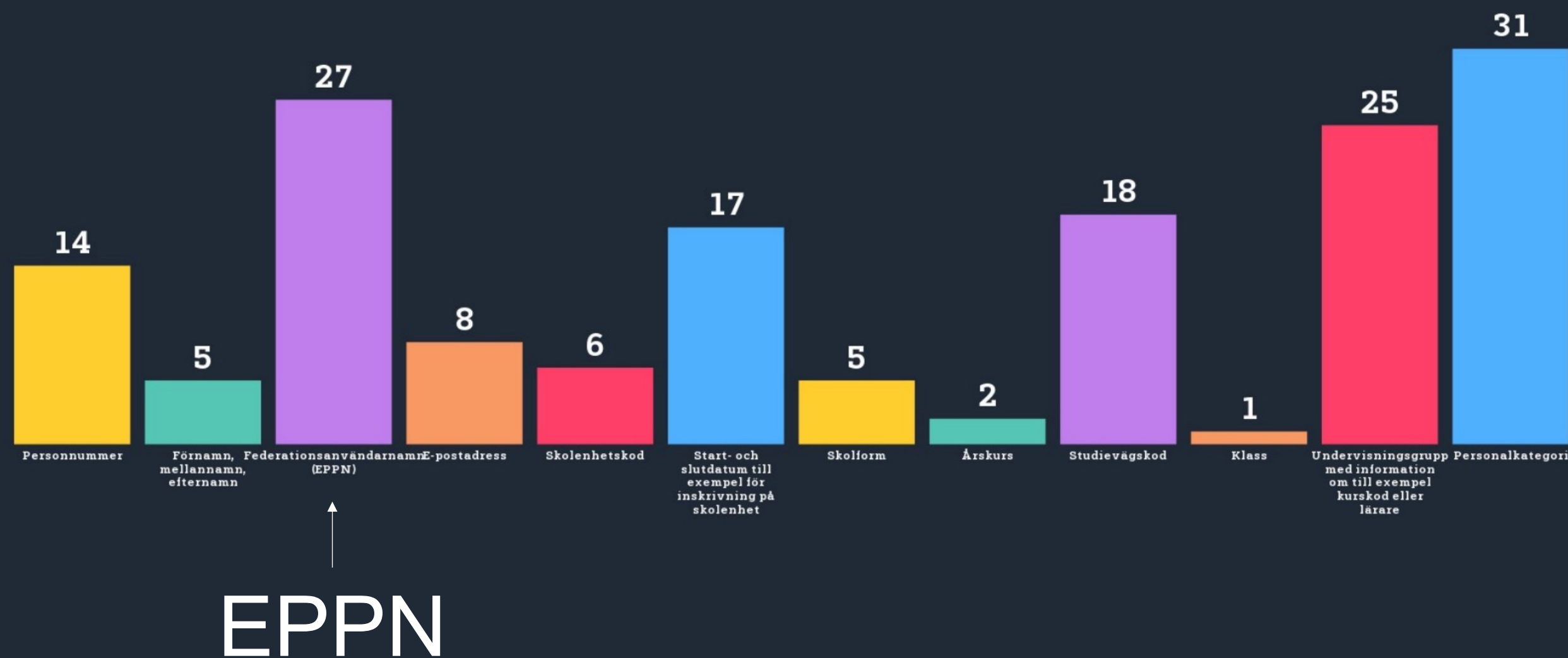


**Allt du behöver veta om EPPN**

# Varför ska vi prata om EPPN?

Från 27/10 2021  
”Förberedelser för DNP”

**Vilka uppgifter tror du skulle orsaka problem?** (vid sammanställning av uppgifter som behövs för DNP)



INTE  
STIF

“Federationsidentifieraren (EPPN) formas inte enligt Skolverkets instruktioner”  
- erfarenheter från Skolverkets försökverksamhet våren 2021

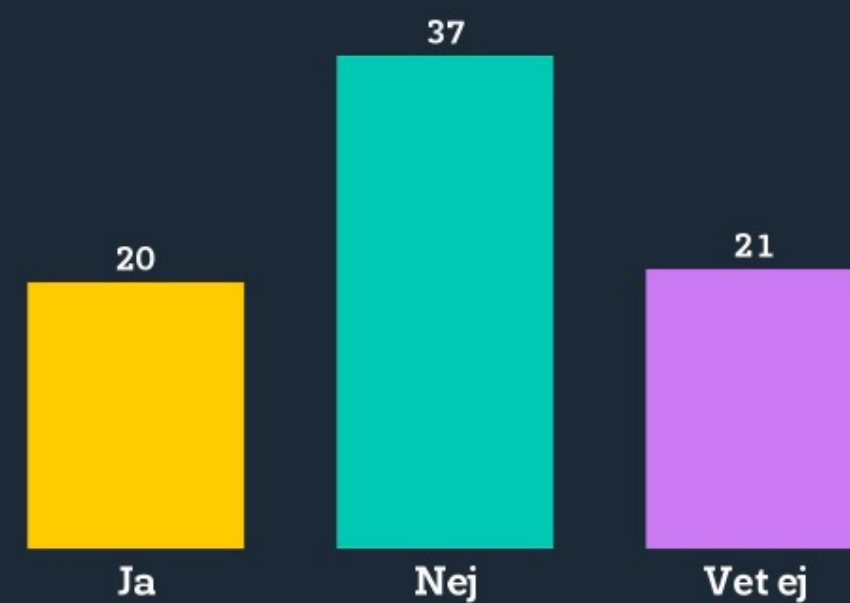
# Varför ska vi prata om EPPN?

Från 11/5 2022

”Planering inför DNP”

Har ni bestämt hur ni kommer att utforma er lösning för att hantera EPPN (eduPersonPrincipalName)?

INTERNET  
STIFTELSEN



78

Om ja på förra frågan om EPPN: Kommer det att vara en pseudonym eller kommer användarens namn att kunna utläsas?

INTERNET  
STIFTELSEN



73

Blandade citat från våra seminarier

“Vi gjorde misstag att konstruera EPPN med för- och efternamn vilket inte fungerar när det finns flera användare/elever med samma namn.”

“ vet inte hur det ligger till gällande EPPN”

” Undrar över EPPN”

“Fortfarande en del otydligheter, särskilt vad gäller EPPN”

“Den unika EPPN är en utmaning. Här behövs mer information.”

# Varför ska vi prata om EPPN?

Vi vill...

- gå på djupet och prata om attributet utifrån Skolfederations perspektiv
- Släppa ut lite luft från den kanske lite väl uppblåsta ballongen EPPN, eller:





# Vad är EPPN?

- Ett attribut som används för identifiering av användare i Skolfederation, i högskolevärlden, och till DNP
- När användaren loggar in till en tjänst via skolans IdP, kan attributet skickas i inloggningsintyget
- Tjänster använder sedan attributet för att identifiera användaren, ex koppla till befintlig profil i tjänsten

Ibland benämns EPPN  
”federationsanvändarnamn”

Vi tycker det är något missvisande,  
användaren ska inte behöva känna till  
sitt EPPN, och inte logga in med det  
som användarnamn. Användaren har  
redan ett användarnamn.

EPPN är ett identifierande attribut –  
det har ingenting att göra med  
användarnamn :-)

# Vad är EPPN?

EPPN ser ut som följande:

**användaridentifierare + @ + säkerhetsdomän**

Användaridentifieraren kan vara nästan vad som helst så länge den är:

- unik inom den egna organisationen, och
- persistent

Det vill säga: dela inte ut redan använda EPPN till nya användare

# Vad är EPPN?

EPPN ser ut som följande:

användaridentifierare + @ + **säkerhetsdomän**

En unik säkerhetsdomän gör att den lokala användaridentifieraren blir **globalt unik**

Minskar risken för identitetskrockar. Ofta finns samma användar-ID i flera organisationer – vilken Kalle är det som loggar in?

# Vad är EPPN?

EPPN ser ut som följande:

användaridentifierare + @ + säkerhetsdomän

För säkerhet anges skolans säkerhetsdomän(er) i något som kallas **Scope** i IdP-metadata. Scope knyter en säkerhetsdomän till en IdP.

Risken för identitetskrocker minimeras – en tjänst ska inte acceptera intyg från en skola som har angivit ett felaktig EPPN – validering görs mot metadata.



Kalle



Användar-  
katalog

Skola 1



IdP

### Metadata

```

<md:EntityDescriptor entityID="https://skola1.se/idp">
  <md:Extensions>
    <shibmd:Scope regexp="false">skola1.se</shibmd:Scope>
  </md:Extensions>
  ...
</md:EntityDescriptor>

```

Skola 2



IdP

```

<md:EntityDescriptor entityID="https://skola2.se/idp">
  <md:Extensions>
    <shibmd:Scope regexp="false">skola2.se</shibmd:Scope>
  </md:Extensions>
  ...
</md:EntityDescriptor>

```



Skolfederation  
MD-register



Kalle



Användar-  
katalog



Kalle




Användar-  
katalog

Skola 1



IdP

```
<saml:Attribute Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
  FriendlyName="eduPersonPrincipalName">
  <saml:AttributeValue>
    kalle@skola1.se
  </saml:AttributeValue>
</saml:Attribute>
```




Intyg

*"Får IdP ställa ut EPPN med angiven säkerhetsdomän?"*



SP



Skolfederation  
MD-register

```
<shibmd:Scope regexp="false">
  skola1.se
</shibmd:Scope>
```

Skola 2




IdP



Intyg

```
<saml:Attribute Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
  FriendlyName="eduPersonPrincipalName">
  <saml:AttributeValue>
    kalle@skola1.se
  </saml:AttributeValue>
</saml:Attribute>
```



```
<shibmd:Scope regexp="false">
  skola2.se
</shibmd:Scope>
```



Kalle



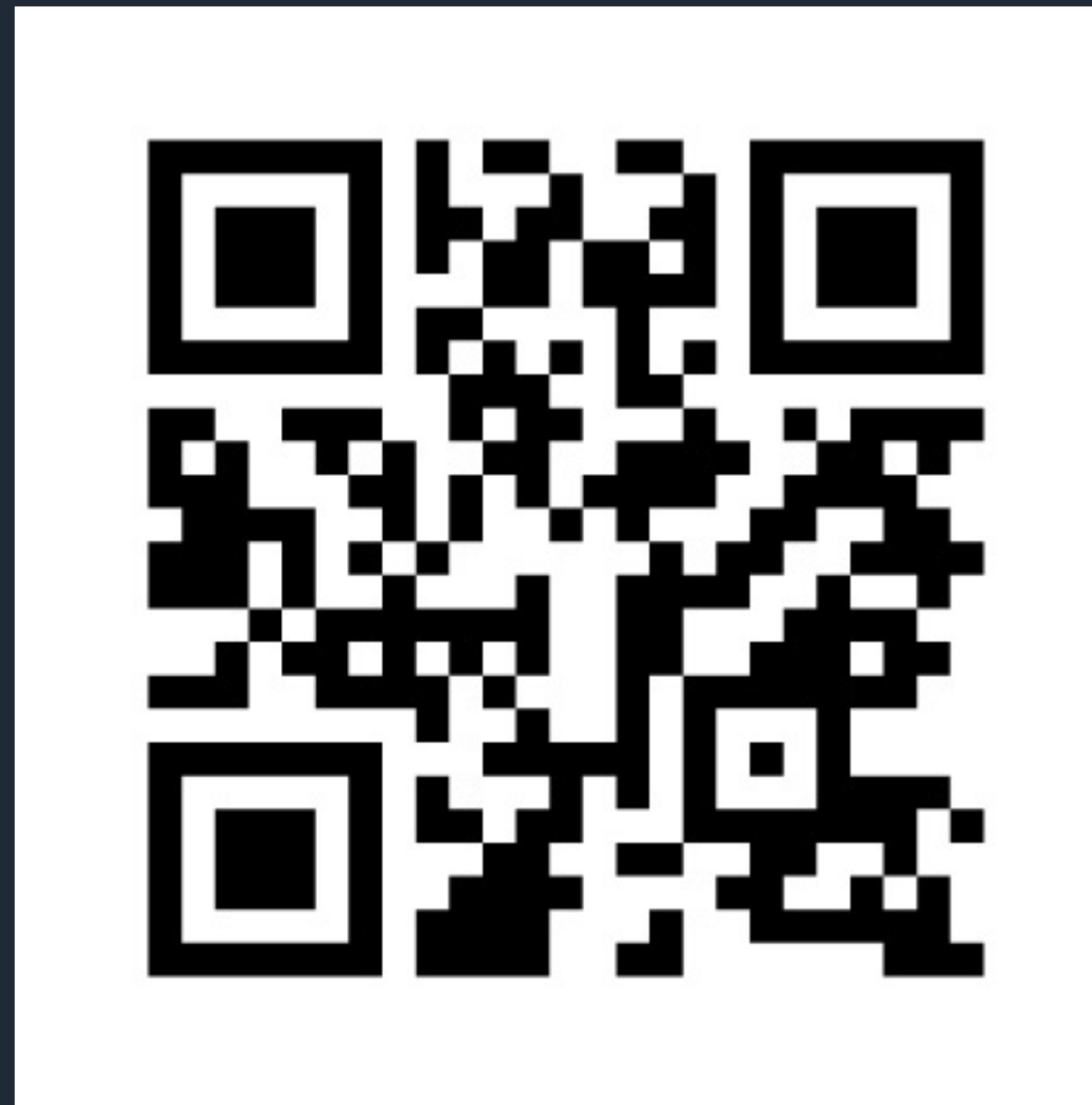
Användar-  
katalog

# EPPN-Menti!

Gå till [menti.com](https://menti.com)

Ange kod: **8936 9028**

Eller scanna QR-kod:



# Vad är EPPN?

EPPN ser ut som en e-postadress – kan jag använda e-post som EPPN?

Nej! Don't do it!

E-postadresser är sällan persistenta. När [lisa.blomdahl@skola.se](mailto:lisa.blomdahl@skola.se) slutar och nästa Lisa Blomdahl börjar så får hon ofta samma e-postadress.

E-postadresser innehåller nästan alltid personuppgifter. EPPN bör vara personuppgiftsfria.

E-post och EPPN har olika användningsområden.



# Vad är EPPN?

I AD så har vi attribut userPrincipalName (UPN)... kan det användas?

Stefan berättar mer om det strax.

# Vad är EPPN?

När ska vi använda EPPN som identifierande attribut?

Så ofta det går, helst alltid!

**integritetsbevarande** – inga personuppgifter om det görs rätt

**säkrast** – tillsammans med Scope det säkraste identifierande attributet

**standard** – ju fler som använder på rätt sätt, desto större nytta

I vissa fall finns användning av andra, ex personnummer för att slå upp information mot Navet, men det kan ofta lösas på andra sätt (ex. så kallad provisionering, överföring av användarinformation via annan kanal).

# Vad är EPPN?

Hur drabbas elever och andra slutanvändare?

Inte alls! De loggar in som vanligt med sitt vanliga användarnamn, de ska inte känna till sitt EPPN.

# Summering - vad är EPPN?

Skolfederations [Attributprofil](#) definierar EPPN på följande vis:

” eduPersonPrincipalName (urn:oid:1.3.6.1.4.1.5923.1.1.1.6)

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

Den ska bestå av en lokalt unik användaridentifierare, ett '@' och en domän, som i det här dokumentet benämns säkerhetsdomän. En domän är ofta, men inte nödvändigtvis, samma som organisationens internet-domännamn.

I det metadata som laddas upp till Skolfederation för en IdP, definieras ett eller flera Scope där värdet är en säkerhetsdomän.

Exempel: användaridentifierare@skolhuvudman.se

Anmärkning: Motsvarighet i SS 12000 är Person/eduPersonPrincipalName

# Exempel på hantering av EPPN

# Frågor?

Ni är varmt välkomna att kontakta oss på [info@skolfederation.se](mailto:info@skolfederation.se) för frågor och synpunkter

# Höstens seminarieserie

## Seminarier ht 2022

Skolfederation fortsätter även under höstterminen att erbjuda seminarier om skolans digitalisering till Sveriges alla skolhuvudmän.

Utöver de tidigare seminarierna riktar vi den här terminen särskilda seminarier till målgrupperna små och medelstora skolhuvudmän som behöver stöd att implementera Skolfederation i sin organisation och förbereda sig för de digitala nationella proven (DNP) som rullas ut under vårterminen 2024.

Små och mellanstora skolhuvudmän som behöver stöd:

[2022-09-14 Införande av Skolfederation](#)

[2022-09-28 Hur lyckas med införande av digitala nationella prov](#)

För alla skolhuvudmän:

[2022-10-12 Hantering av personuppgifter – konsekvensbedömning för digitala läromedel och DNP](#)

[2022-11-09 Hur bidrar samverkan till skolans långsiktiga digitalisering och vilka samverkansmöjligheter finns?](#)

[2022-12-07 Att göra skolans organisation redo för digitala nationella prov \(DNP\)](#)

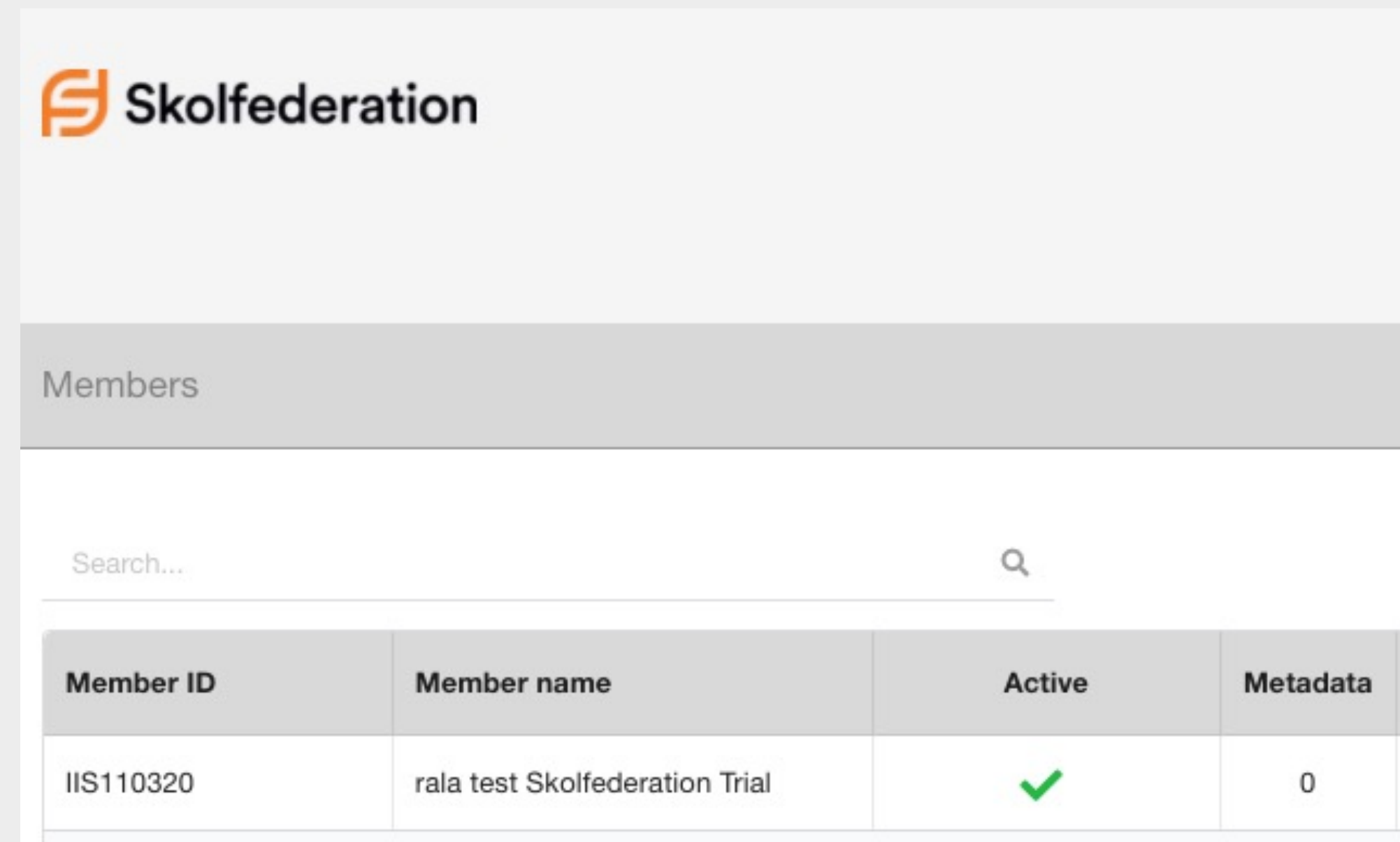
Läs mer och anmäl er  
på [skolfederation.se](https://skolfederation.se)!

# Nästa ITFF

10 november 2022 kl. 13:00-14:30



# Förbättringsförslag eller feedback?



The screenshot shows the Skolfederation website interface. At the top left is the Skolfederation logo. Below it is a grey header bar with the word "Members". Underneath is a search bar with the placeholder text "Search..." and a magnifying glass icon. Below the search bar is a table with the following data:

| Member ID | Member name                    | Active | Metadata |
|-----------|--------------------------------|--------|----------|
| IIS110320 | rala test Skolfederation Trial | ✓      | 0        |

Kontakta oss!

[info@skolfederation.se](mailto:info@skolfederation.se)

[info@sambi.se](mailto:info@sambi.se)

# Diskussion och frågor

*För frågor ni önskar ta i mer privata sammanhang så finns vi på [info@skolfederation.se](mailto:info@skolfederation.se) samt [info@sambi.se](mailto:info@sambi.se) respektive.*