eduPersonPrincipalName (ePPN)

Stefan Halén

stefan.halen@internetstiftelsen.se

Vad är ePPN

ePPN är en standardiserad globalt unik identifierare som används för att representera en användare i federationer. ePPN är ett attribut som har använts inom akademiska och forskningssammanhang i 20 år. Det är väldefinierat och accepterat.

ePPN

<användarnamn>@<scope>

<användarnamn>: En sträng som identifierar användaren. Den måste vara unik inom sin organisation, vara beständig och får inte återanvändas.

@: Separerar delarna.

<scope>: I Skolfederation måste detta vara ett av organisationen ägt publikt domännamn t.ex. iis.se eller swefed.se.

Exempel: be56js23f@iis.se

Scope – en del av ePPN

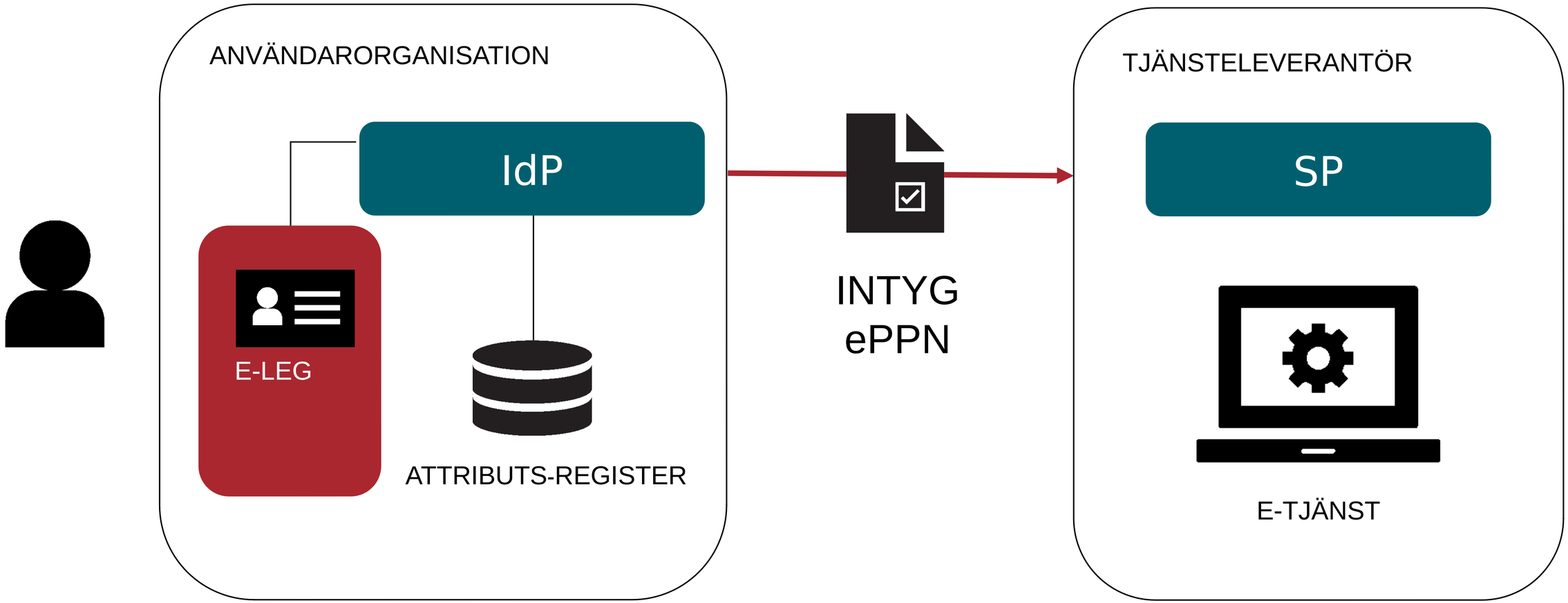
- Scope är en kontrollfunktion som binder attribut till den utfärdande organisationen.
- Scope används för att förhindra sammanblandning av identiteter
- Utan scope kommer tjänsten att uppfatta Kalle från Lerum och Kalle från Borås som samma person.

Varför domännamn som scope

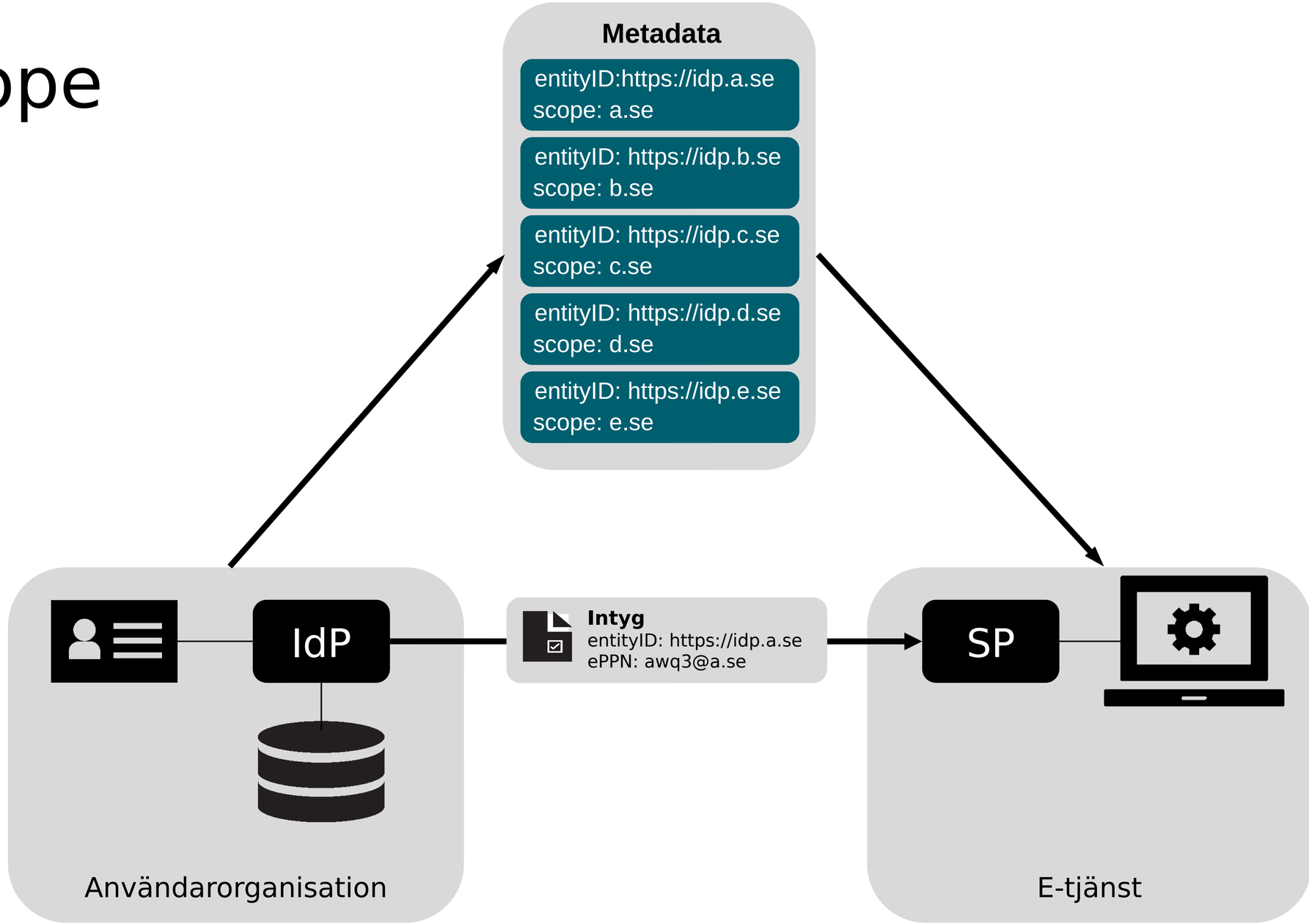
- Ett scope måste vara en globalt unik sträng.

- Domännamn används som scope eftersom DNS är ett hierarkiskt system som garanterar att alla ingående namnrymder är globalt unika och kan härledas till en ägare.

Federerad inloggning



Scope


Metadata
entityID:https://idp.a.se
scope: a.se
entityID: https://idp.b.se
scope: b.se
entityID: https://idp.c.se
scope: c.se
entityID: https://idp.d.se
scope: d.se
entityID: https://idp.e.se
scope: e.se
IdP
Intyg
entityID: https://idp.a.se
ePPN: awq3@a.se
SP
Användarorganisation
E-tjänst

Lösningsexempel

Google Workspace for Education och Microsoft AD

Base36 alfanumerisk sträng

000000 – ZZZZZZ, 36^6 = 2 176 782 336 ePPN

https://wiki.federationer.internetstiftelsen.se/x/kQBMAg

Länkar

Attributprofil: https://www.skolfederation.se/teknisk-information/attribut/

Scope: https://wiki.federationer.internetstiftelsen.se/x/ZwBMAg