



SWAMID

Swedish Academic Identity Federation

SWAMID

Identitetsfederationen för
universitet, högskolor och
sektorsmyndigheter

Pål Axelsson, Vetenskapsrådet/Sunet

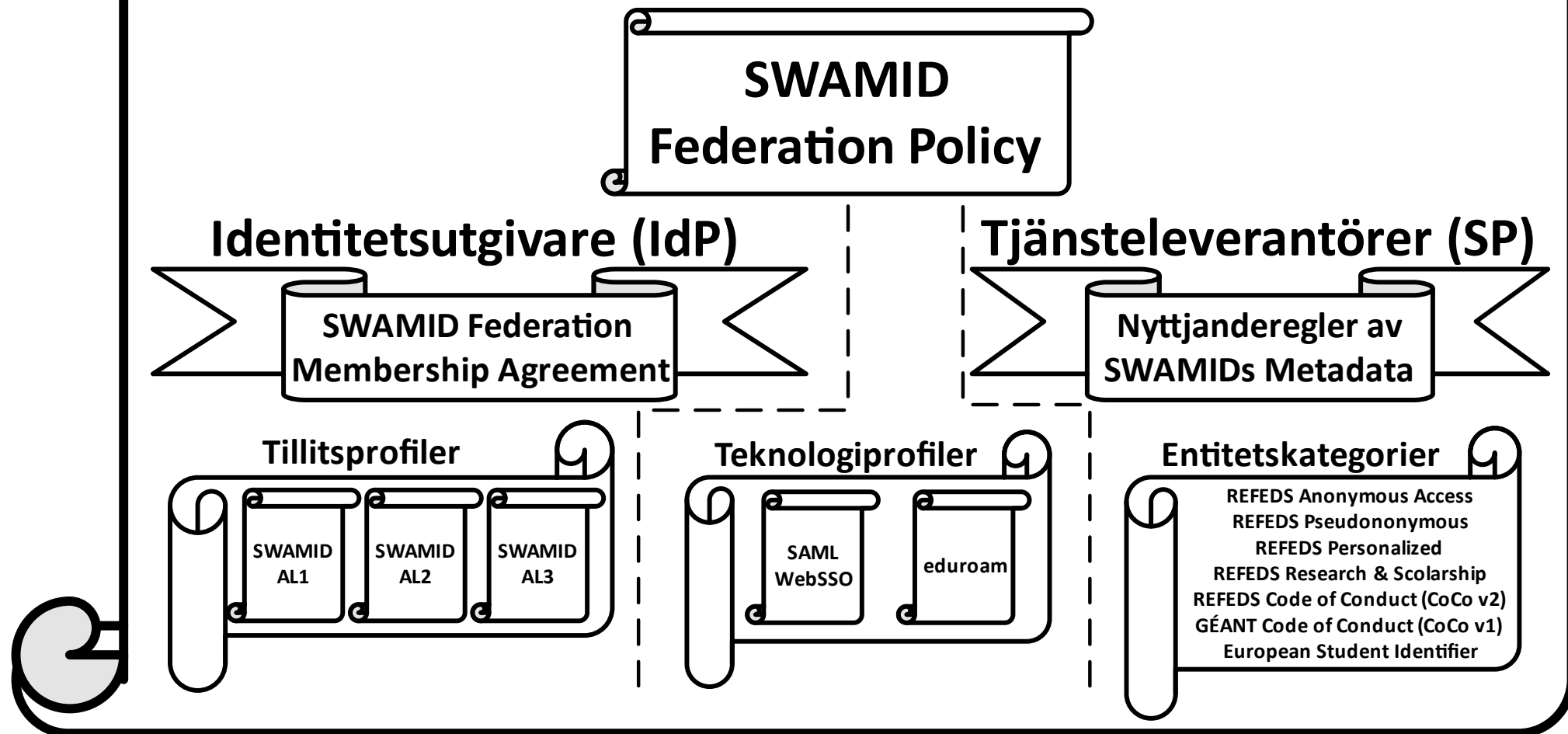
pax@sunet.se



Swedish Academic Identity Federation

- Medlemsdriven federation där alla identitetsutfärdare är anslutna till Sunet
 - Universitet, högskolor, forskningsorganisationer, forsknings- och utbildningsnära myndigheter, Kungliga biblioteket och statliga kulturarvsinstitutioner
- En användare vid en organisation kan logga in i tjänst i en annan organisation
- 63 organisationer är medlemmar
 - >90 000 anställda
 - >400 000 studenter
- >750 tjänster är registrerade i SWAMID
- 15 år 2022

SWAMID Federation Policy Framework

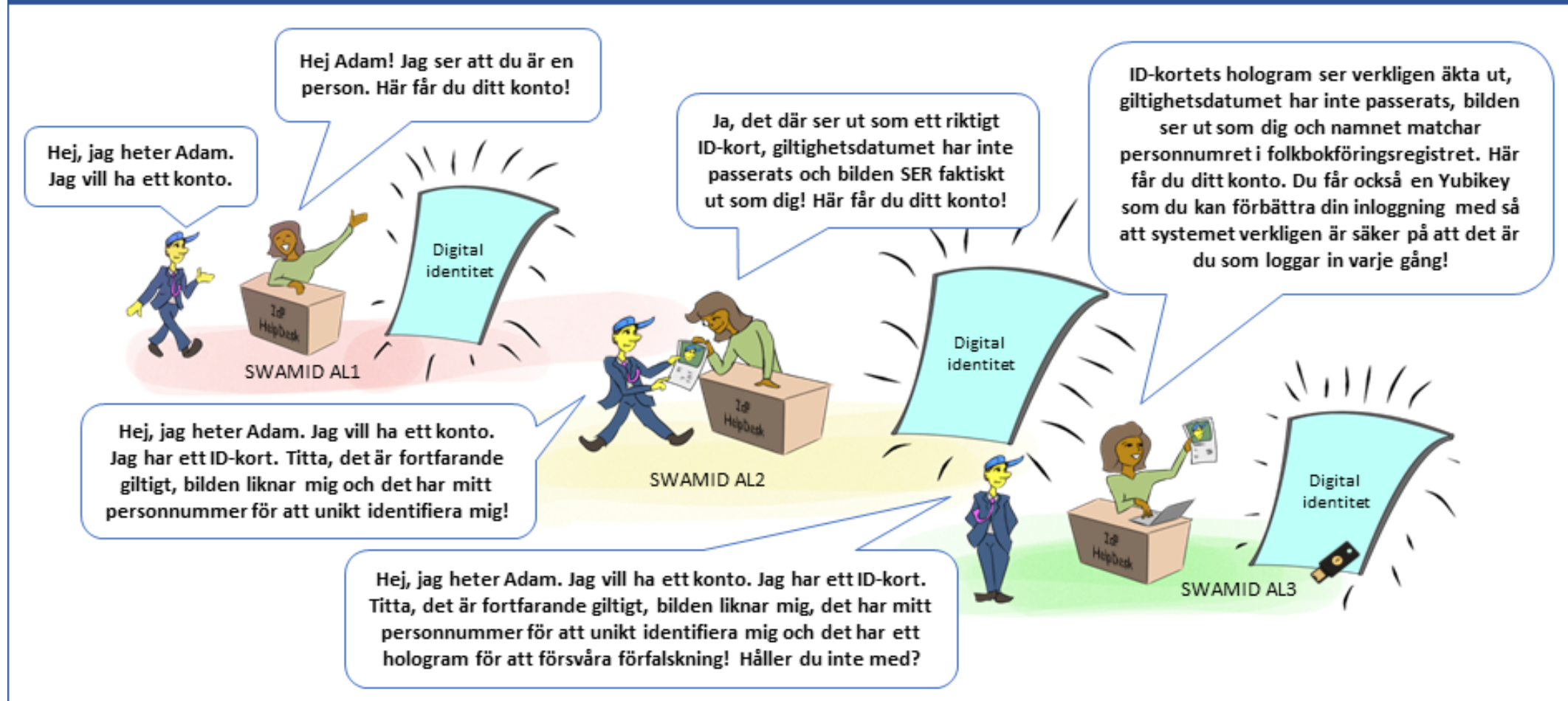


Vem får registrera en tjänst i SWAMID?

I SWAMIDs teknologiprofil för SAML WebSSO definieras att en tjänst kan registreras av

- medlemsorganisation
- ägare av en tjänst som har avtal/överenskommelse med minst en medlem
- myndighet som har en tjänst som används av minst en medlem
- ägare av en tjänst som tillhandahålls utan avtal/överenskommelse men som används för att genomföra eller samarbeta inom forskning eller utbildning

SWAMID's tillitsnivåer



Det identitetsfederativa dilemmat

- **Tjänster behöver information om användarna för att kunna låta dem logga in men identitetsutfärdarna vill vara i kontroll över vilka personuppgifter en tjänst får tillgång till**
- Detta hindrar ofta användare att logga in i de tjänster de behöver för att kunna genomföra sitt arbete eller sina studier
- De som hindras i inloggningen tar ofta inte kontakt med helpdesk/support utan försöker hitta andra mindre säkra vägar in i tjänsten

Entitetskategorier för attributrelease

- I SWAMID används entitetskategorier för att underlätta attributrelease från identitetsutfärdare till tjänst
 - Kortfattat är det en markering i tjänstens metadata att de behöver definierade attribut från identitetutgivaren
- Entitetskategorierna används för att både förenkla och minimera överföringen av personuppgifter till en tjänst

Vilka entitetskategorier används?

- REFEDS Anonymous Access Entity Category
 - Endast organisationsinformation, ingen personifiering genom användaridentifierare
- REFEDS Pseudonymous Access Entity Category
 - Organisationsinformation samt personifiering baserat på en tjänstespecifik pseudonym användaridentifierare
- REFEDS Personalized Access Entity Category
 - Organisationsinformation samt personifiering baserat på en organisationsunik användaridentifierare, namn och e-postadress

Vilka entitetskategorier används?

- REFEDS Data Protection Code of Conduct Entity Category
 - Överföring av specifika personuppgifter som inte ingår i anonymous, pseudonymous och personalized, t.ex. personnummer
 - Kräver att tjänsten tydligt beskriver för användaren vilka personuppgifter som behövs och varför
- REFEDS Research and Scholarship Entity Category (R&S)
 - En äldre version av personalized med begränsningen genomföra eller samarbeta inom forskning eller utbildning
- European Student Identifier Entity Category
 - Används för europeiskt studentutbyte

Interfederation i Sverige och världen

- Interfederation är en federation av federationer
- En användare vid en organisation i en federation kan logga in i tjänst i annan federation
- SWAMID är medlem i två interfederationer
 - FIDUS – Skolverkets interfederation för myndighetstjänster riktade till skolhuvudmän i grund- och gymnasieskola samt vuxenutbildning
 - eduGAIN - Akademiska identitetsfederationer runt om i världen.
 - >80 deltagande federationer
 - >5 200 identitetsutfärdare inom forskning och utbildning
 - >3 500 tjänster exporteras till eduGAIN från deltagande federationer

Standardisering av identitetsfederation

- Federationsprotokollet SAML standardiseras av OASIS
 - [FrontPage - SAML Wiki \(oasis-open.org\)](https://frontpage.saml-wiki.org/)
- Federationsprotokollet OpenID Connect Federation standardiseras av OpenID Foundation
 - Ej ännu klar men finns i draft
 - https://openid.net/specs/openid-connect-federation-1_0.html
- REFEDS (the Research and Education FEDerations group) skapar interoperabilitetsstandarder för att förenkla för federationer, identitetsutfärdare och tjänster att samverka
 - <https://refeds.org/specifications>



SWAMID

Swedish Academic Identity Federation