



SWAMID

Swedish Academic Identity Federation

Swamid TNG och samspelet med digitala plånböcker

Sunetdagarna våren 2025

Framtiden för digital identitet

- SWAMID har funnits i 18 år och det digitala identitetslandskapet har förändrats mycket under denna tid
- EUs digitala e-legitimationer kommer på sikt ersättas med digitala identitetsplånböcker

Swamid TNG

(The next generation)

SAML och framtiden

- Sedan Swamid skapades 2006-2007 har tekniken multilateral SAML använts
- Multilateral SAML utvecklades som en påbyggnad till SAML inom högre utbildning i USA ett par år tidigare
- I traditionell SAML konfigurerades en bilateral teknisk koppling mellan varje tjänst och identitetsutfärdare
- I multilateral SAML används en federativmiljö där metadata för identitetsutgivare och tjänster utbyts via gemensam administration av metadatasamlingar
- Av olika tekniska anledningar är det dags att ersätta SAML
 - SAML kommer inte att försvinna på kort sikt utan gradvis ersättas

Framtidens federationsteknologi

- Swamid och ett antal andra akademiska identitets-federationer, inkl. eduGAIN, undersöker nu framtidens federationsteknologier, två alternativ för underliggande inloggningsstandard:
 - OpenID Connect (inkl. OAuth 2.0)
 - Digital akademisk plånbok
- Som federationsteknologi som binder ihop den underliggande tekniken föreslås OpenID Federation för båda två

OpenID Connect

- OpenID Connect är en mogen standard som används av många parter vilket gör att vi börjar med denna
- Traditionellt har man sagt att OpenID Connect är enkelt men med tiden har även denna standard blivit komplex
- Precis som för SAML är OpenID Connect i grunden en bilateral teknik där konfiguration sker direkt mellan OpenID Provider (OP) och OpenID Relying Parties (RP)

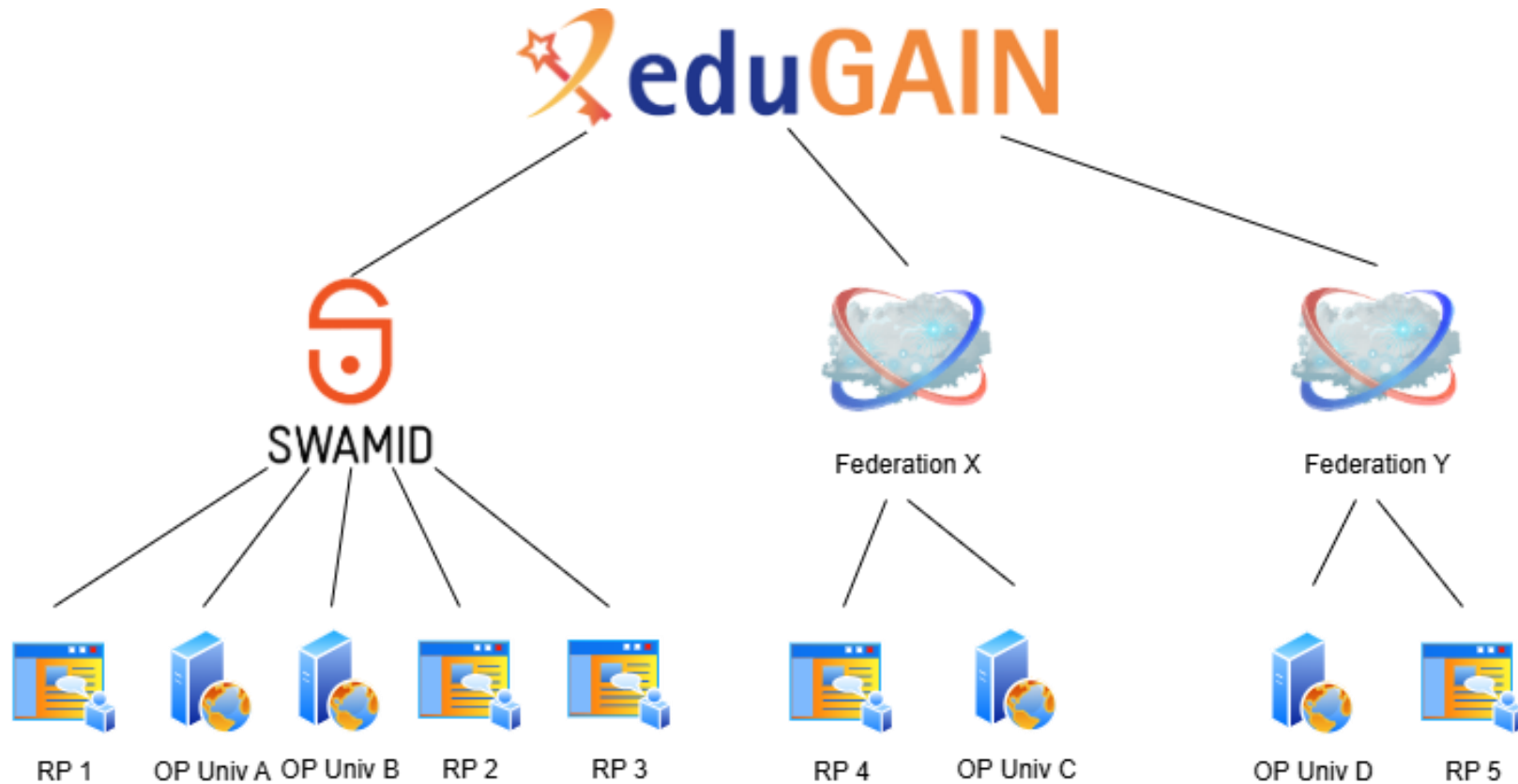
OpenID Federation the new kid...

- Standarden för OpenID Federation (OIDF) närmar sig godkännande
- OIDF byggs som ett träd med flera nivåer där
 - eduGAIN är trädstammen
 - nationella identitetsfederationer, t.ex. Swamid, är grenarna som utgår från stammen
 - Ops och RPs kan såsom löv antingen sitta direkt på dessa grenar eller på lärosätens/organisationers ev. egna undergrenar

Tillit i OpenID Federation

- Grundläggande teknisk tillit i OpenID federation
 - Trädet är säkrat genom att en överliggande entitet (gren eller stam) signerar underliggande entitet (stam eller löv)
 - Stammen är en så kallad Trust Anchor som alla underliggande entiteter litar på
- Utökad tillit signaleras via signerade Trustmarks
 - Exempel på trustmarks skulle kunna vara medlem i Swamid, uppfyller kraven för specifik tillitsnivå och uppfyller kraven för att få attribut via angiven entitetskategori

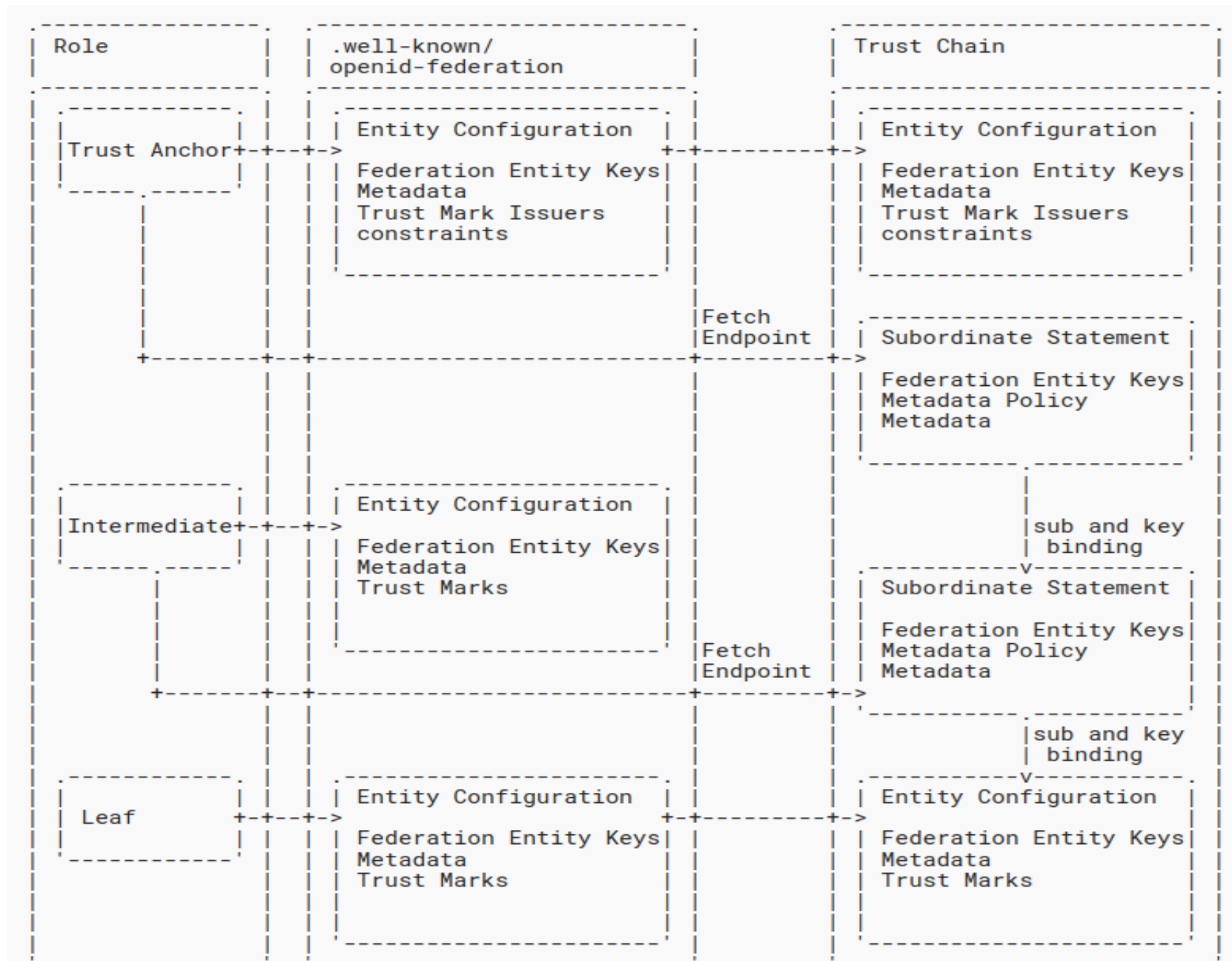
eduGAIN OIDF Tree example





Federation

Entity



eduGAIN OpenID Federation Pilot

- eduGAIN tillsammans med ett fåtal nationella federationer kommer under 2025 genomföra en begränsad pilot för att få erfarenhet av OpenID Federation
 - Swamid är en av dessa federationer
- Målet med piloten är
 - Att lära känna federationsteknologin
 - Att testa den i "verkligheten"
 - Att få erfarenhet så att vi kan skriva en teknisk teknologiprofil för OpenID Federation

Vad innebär detta för Swamid nu?

- För er som SWAMID-medlemmar innebär piloten inte något särskilt mer än att ni kommer få höra mer om den nya standarden och får möjlighet att frivilligt testa om ni vill
- OIDC-klienter behöver få stöd OIDF
 - Utveckling av OpenID Provider (OP) med stöd för OIDF
 - Protokollsproxy för översättning SAML IdP tas fram för piloten
 - Shibboleth kommer med en plugin senare under året
 - Utveckling OIDF-stöd i OpenID Relying Parties (RP)
- Federationsadministrativa verktyg behöver tas fram

The eduGAIN OpenID Connect Profile



TRUST is based on trust chains with eduGAIN as primary Trust Anchor, and the national academic Federations as Intermediates and Entities as Leaves



ENTITY VALIDATION is based on the eduGAIN Trust Mark. Only validated entities can be part of trust chains with eduGAIN as Trust Anchor



ENTITY RESOLUTION is provided by a resolver endpoint at federation and inter-federation level that provides metadata about entities

Akademisk identitetsplånbok

- Denna teknik bygger på samma teknik som EUs kommande digitala identitetsplånbok
- Eftersom EUs identitetsplånbok endast gäller inom EU/EES måste vi ta fram akademisk identitetsplånbok för forskare, lärare och studenter
- Denna teknik är väldigt ny och under utveckling och därför avvaktar vi med att starta arbetet

Uppdatering gällande EUs digitala identitetsplånbok

EUs digitala identitetsplånbok

- EUs digitala identitetsplånbok är en utökning av den s.k. eIDAS-förordningen
- Digital identitetsplånbok för fysiska och juridiska personer, för att på ett säkert sätt kunna begära, erhålla, lagra, välja, kombinera och använda personidentifieringsuppgifter och digitala bevis för autentisering online och offline samt skriva under med kvalificerade elektroniska underskrifter.
- Användare får kontroll på sitt data och kan underteckna med en kvalificerad e-underskrift.
- eIDAS förordningen: <https://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX:02014R0910-20240520>

eIDAS Implementing acts

- EU kommissionen jobbar på att färdigställa eIDAS Implementing acts
 - Ca hälften (av runt 40) är nästan klara.
 - Implementing acts är tänkta att bl.a. peka ut riktningen i form av att definiera vilka standarder som skall användas i utvecklingen av den digitala identitetsplånboken.

Large Scale Pilots - DC4EU

- DC4EU som kör en pilot på utbildningsmeriter (och de andra piloterna) har fått en förlängning och kommer avslutas den 31 Juli, istället för 31 mars som var tänkt från början.
- Efter sommaren kommer resultaten av piloterna att presenteras för de som är intresserade.

Large Scale Pilots - We Build

- Den 1 Augusti kommer nästa iteration av de storskaliga piloterna att dra igång. Det är två piloter istället för fyra denna gång, med mer fokus på organisationsplånboken och affärsintegrering, typ betelningsflöden.
- Sunet och Linköpings universitet är med i We Build och det finns ett användarfall inom We Build som fokuserar på micro-credentials.
- Den andra piloten heter Aptitude men där finns ingen Svensk närvaro.

Svenska digitala identitetsplånboken

- DIGG har fått i uppdrag att ta fram den svenska identitetsplånboken innan slutet på 2026 då eIDAS förordningen skall efterlevas.
- 2026 skall plånboken finnas redo från alla EUs medlemsländer
- Utbildningskvalifikationer skall enligt eIDAS förordningen också vara på plats och kunna släppas till DIGGs plånbok då.