eduID

Hans Nordlöf

hanor@sunet.se

Vad händer inom eduID

- Nytt gränssnitt för användarna
- Proofing via registrerat mobiltelefonnummer
- eduID MFA
- IdP as a service via eduID (pilotprojekt?)

Nytt användargränssnitt

Ny logga

Bekräfta identitet med registrerat mobiltelefonnummer

- Sedan i går finns det möjlighet att använda ett registrerat mobiltelefonnummer för att bekräfta identiteten som AL2
- Detta tillsammans med ”Min myndighetspost” fungerar för de flesta svenskar.
- Det finns enligt våra undersökningar en stor grupp mellan 18-21 år som bor hemma och har telefonen registrerad hos en förälder. Vi har ett godkänt scenario för dessa (där föräldrarna har s.k. särskilt försörjningsansvar). Det innefattar att den förälder som är registrerad som ägare träder fram som ”vittne” att den sökande personen är rättmätig innehavare av mobiltelefonnumret. Skall vi aktivera möjligheten?
- När det gäller personer under 18, accepteras automatiskt att vårdnadshavare (kontroll mot navet) är registrerad ägare

Höjd säkerhet

- SWAMID tar fram en teknisk profil som möjliggör att stödja implementationen av multifaktorautentisering både för IT-tjänster inom lärosätet och för federerade IT-tjänster som används mellan lärosäten.
- Denna tekniska profil används som ett komplement till tillitsnivån SWAMID AL2
- Saknas idag kända intressenter som efterfrågar höjd säkerhet för SWAMID AL1

Användningsområden

	Låga krav på information om individen	Höga krav på information om individen
Normala krav på säker användning av kontot	SWAMID AL1 + lösenord	SWAMID AL2 + lösenord
Höga krav på säker på säker användning av kontot		SWAMID AL2 + MFA

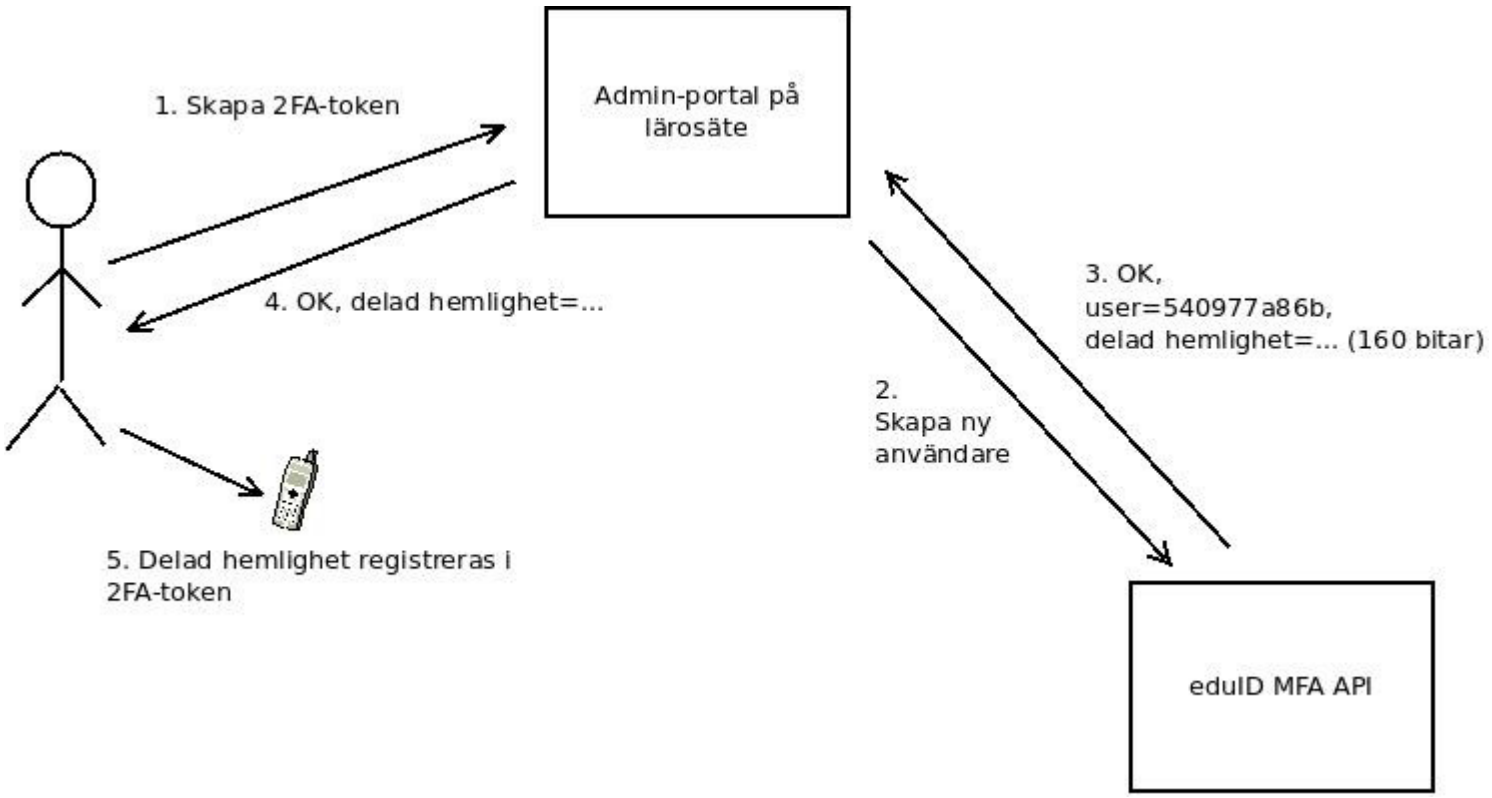
Multifaktorautentisering

- En gemensam standard för hur IT-tjänster kan signalera krav på användandet av en andra faktor (smartphone-appar eller USB-nyckel) för höjd säkerhet
- Rekommendationer för vilka tekniker som kan användas och krav på hur de bör implementeras
- Stöd för att lagra extra faktor i eduID för användande antingen som komplement till lokal IdP eller tillsammans med eduID

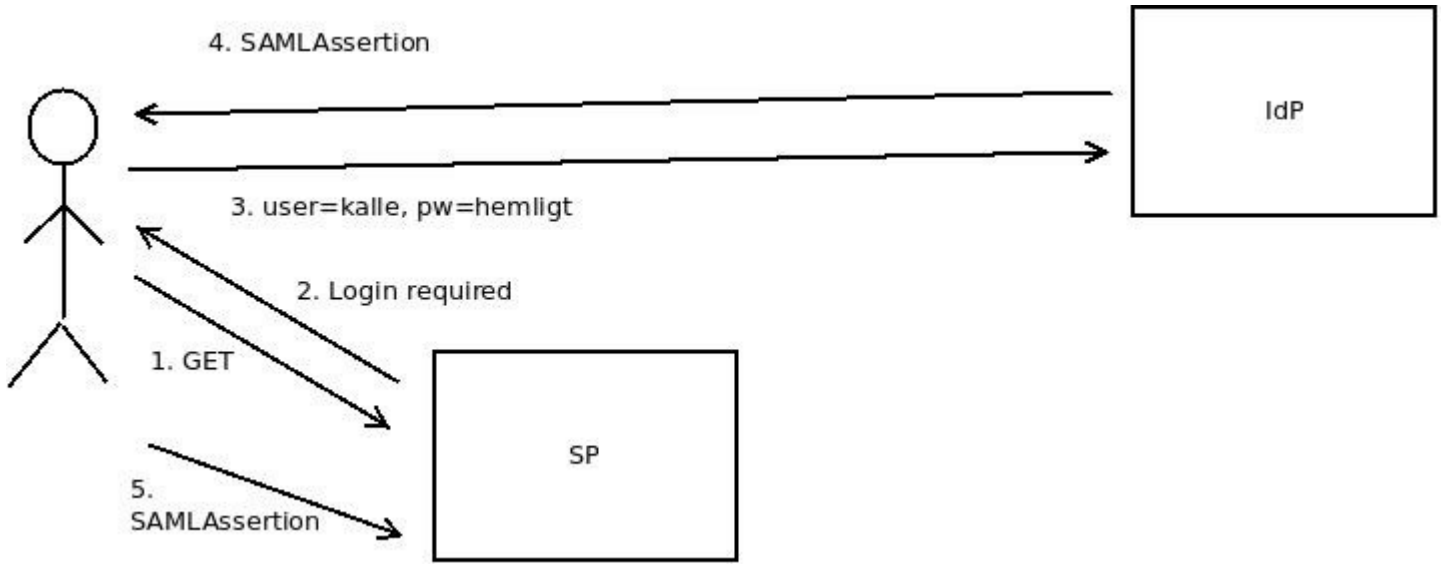
eduID tvåfaktor API för IdP eller SP

- Ger ett lättanvänt interface för tvåfaktorsautentisering (JOSE)
- OATH TOTP HMAC-SHA-1 (sex eller åtta siffrors koder)
- Tidsbaserat, koder giltiga 30+30 sekunder
- FIDO U2F senare, om det verkar vettigt
- Anonyma ”användare” skapas hos eduID
- eduID svarar JA eller NEJ baserat på uppgiven kod

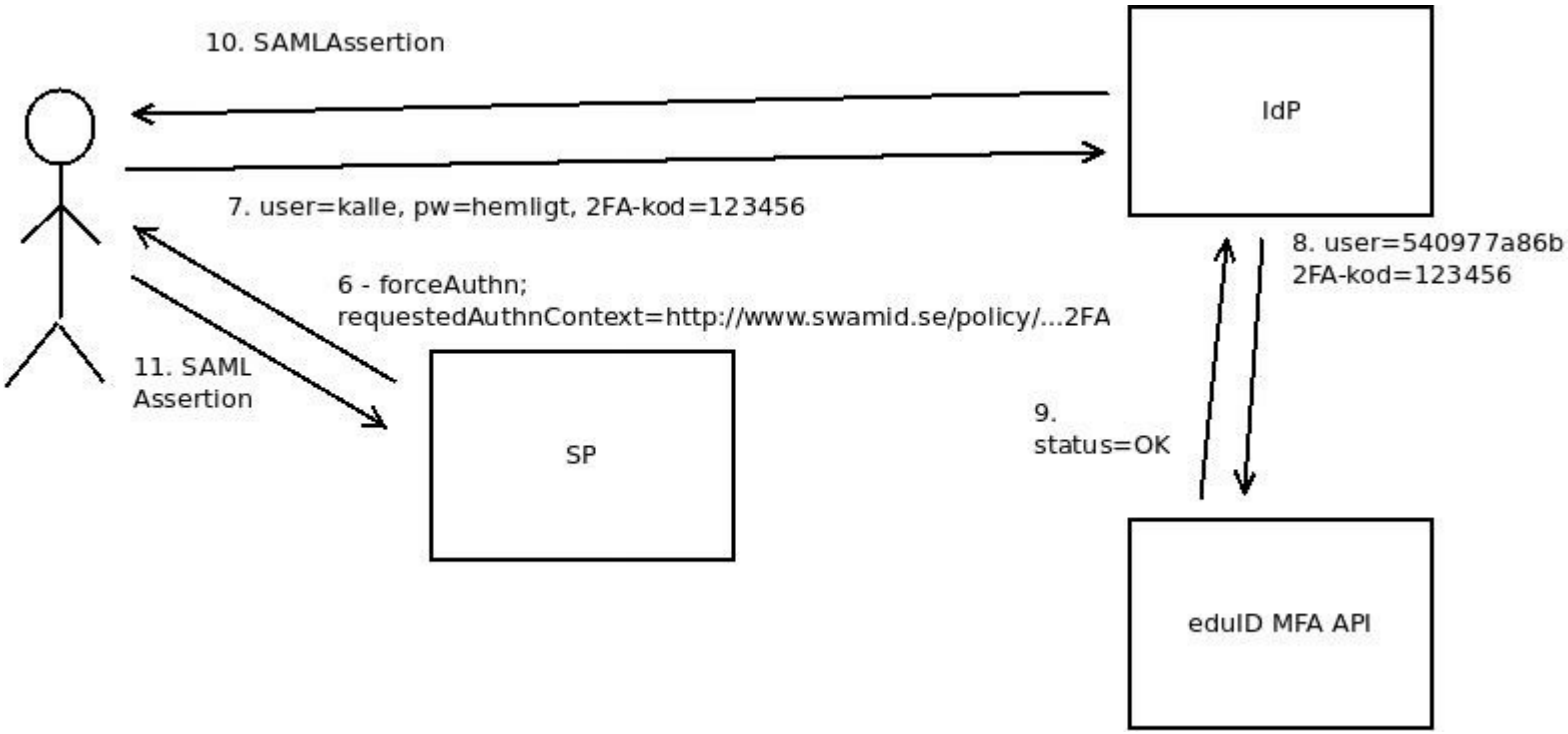
Så kan det göras



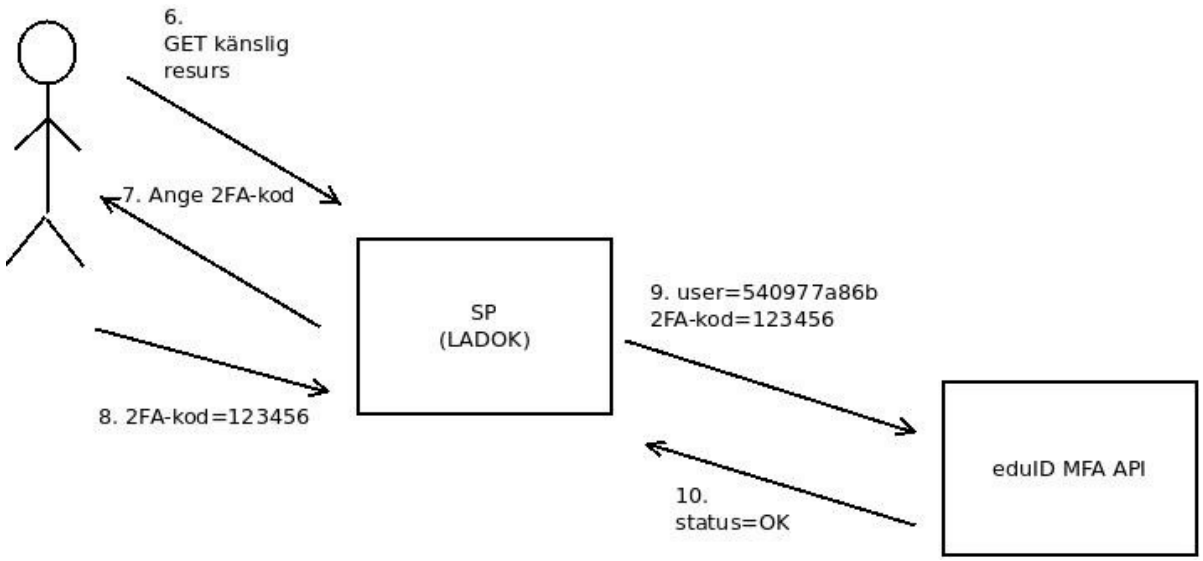
Vanlig SAML2-inloggning



SP vill ha starkare autentisiering via IdP i SWAMID

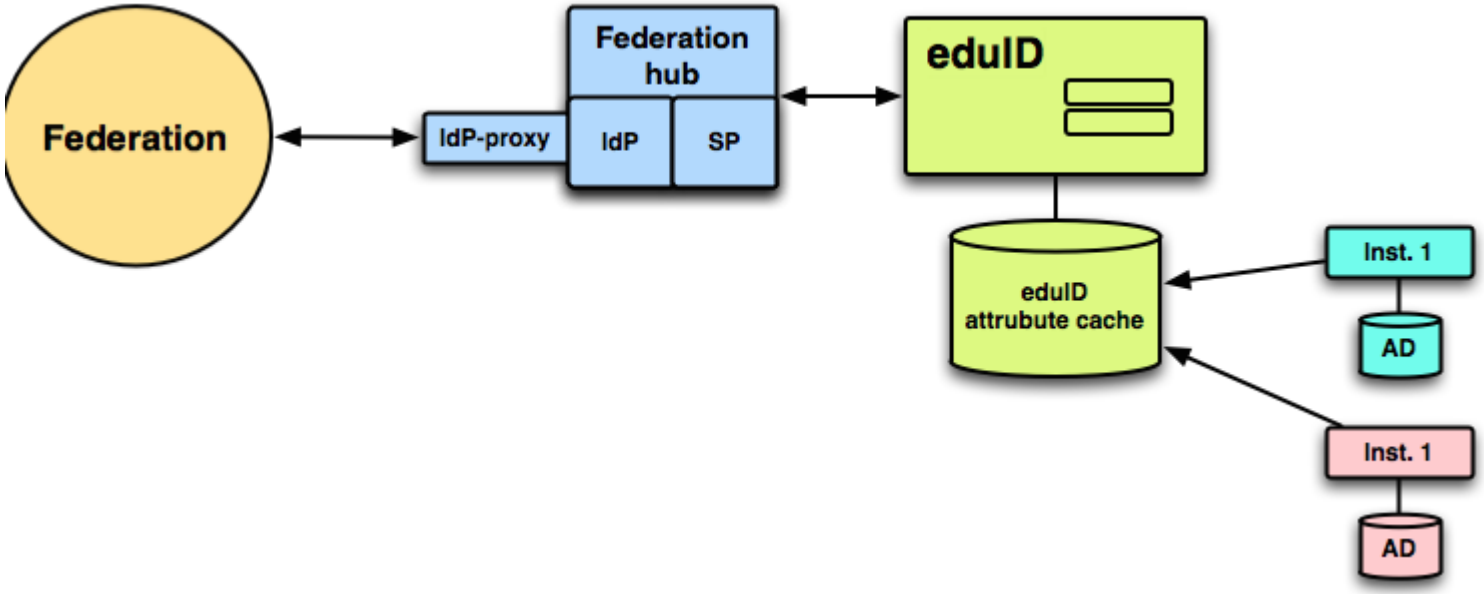


SP använder eduID direkt (Nya Ladok)

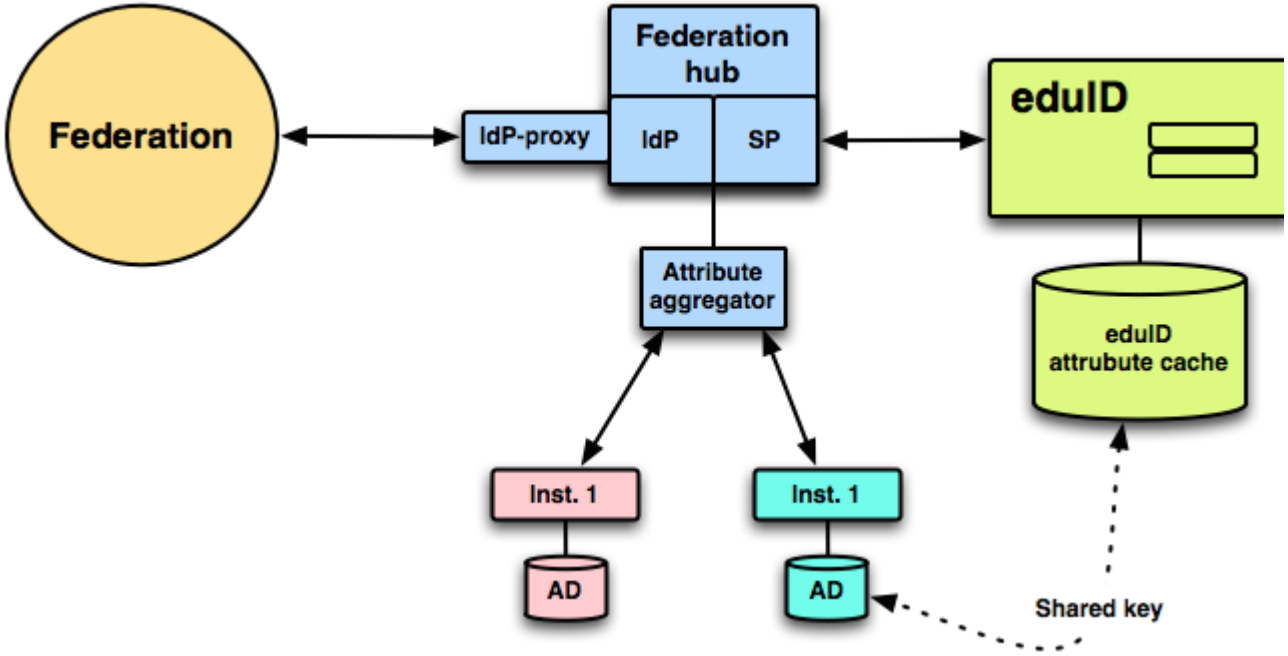


OBS: I detta fall har 2FA-användaren skapats via SP (LADOK), inte via det egna lärosätet.
För att förhindra phishing och andra säkerhetsproblem kan inte organisation A autentisiera med tokens från organisation B.

IdP as-a-service?

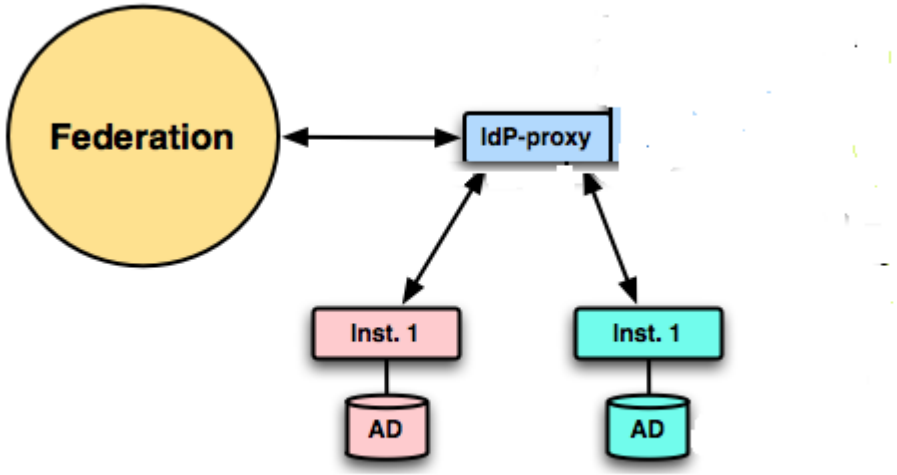


IdP as-a-service?

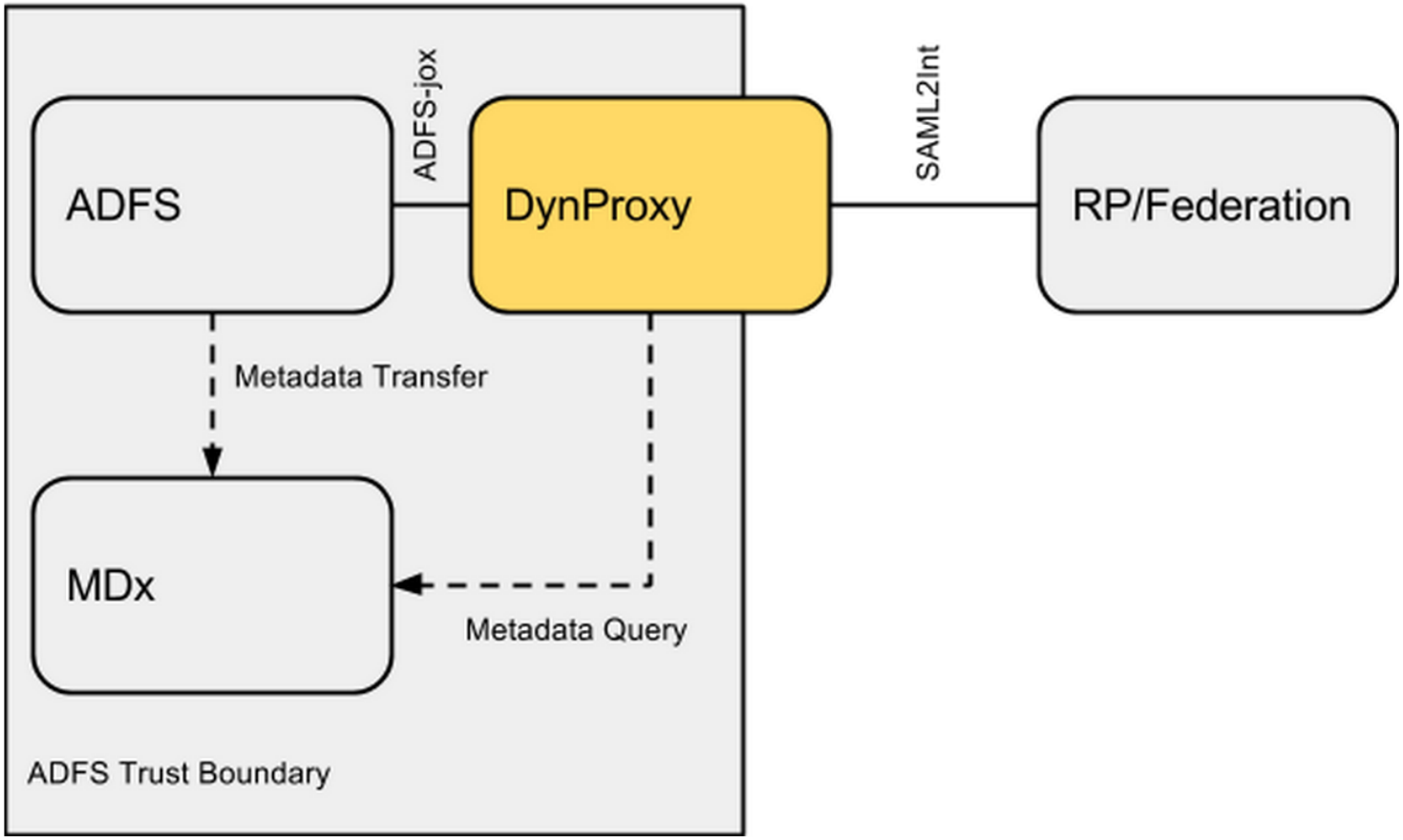


Hosted IdP?

Kan vara en lösning för de som inte har AD i molnet.



Dynamisk ADFS-proxy



SWAMID Dynamisk ADFS-proxy

- Plocka in vilka attribut som helst från ADFS-sidan - default-konfiguration av ADFS ska funka rimligt väl men det ska gå att göra mappning av typen attribut+valfri nameForm -> attribut+oid nameform. Mappning ska i första versionen vara 1-1 - dvs i princip bara omskrivning av attributnamnet. Ta höjd för mer komplex omskrivning.
- Varje ADFS-IdP ska ha en virtuell ändpunkt i “SAML2int-änden”. Konfiguration ska vara dynamisk och vara baserad på metadata query så långt som möjligt.
- Målet ska vara att de flesta ADFS-IdPer ska klara sig med default-inställningar. Det enda som ska behövas är att skicka ADFS-metadata till MDx:en (en pyff bara för detta tror jag) samt releasa alla attribut (eller iaf super-set av alla som behövs på saml2int-sidan) till DynProxy:n. För att “aktivera” en ADFS på saml2int-sidan behövs antagligen någon slags lista på “kända entityIDs”
- Ett sätt att implementera virtuella ändpunkter är att använda sha1(ADFS-entityid) som en del i URLerna (både ändpunkter och entityID) på saml2int-sidan.

Hur går vi vidare?

- eduID har fortfarande fokus på studenter och att ersätta UHR:s användarhantering
- Flera användarfall dyker upp som inkluderar personal och speciella lärosätesbehov
- Diskussion!!!
- Frågor?