
SWAMID
Swedish Academic Identity Federation

SWAMID

Vad händer i SWAMID

Pål Axelsson
SWAMID Operations, SUNET
pax@sunet.se

SUNET

Federationens framgångsfaktorer för förändringar i regelverk eller ny teknik

SWAMID

- Federationsoperatören har gjort ett gediget arbete som är förankrat med federationens medlemmar
- Förändringen måste vara efterfrågad med avseende på
  - ny tjänst som alla vill ha,
  - lagkrav på befintlig tjänst eller
  - omvärldskrav på befintlig tjänst och till sist
  - tjat…

Multifaktorinloggning via SWAMID

I SWAMID finns följande behov av inloggningsskydd

- Lösenord (eller annan enskild faktor)
- Egenregistrerad multifaktor för att skydda sin egen inloggning
  - Inloggning med lösenord vid skapande av andra faktorn
- Personverifierad multifaktor för att säkerställa att det är rätt person som loggar in i tjänsten
  - Identitetskontroll genomförs vid utdelning av multifaktor eller andra faktor

SWAMID

Multifaktorinloggning via SWAMID

- Datainspektionen har ställt krav på säkerinloggning i ett gemensamt system med känsliga personuppgifter
- Anställda på lärosätena vill inte använda privat e-legitimation i tjänsten
- SWAMID tar fram regelverk för användning av personverifierad multifaktor inom federationen inkl. krav på att användaren uppfyller tillitsprofilen SWAMID AL2

SWAMID

Hur begär en tjänst multifaktorinloggning?

- Tjänsten begär i sin inloggningsförfrågan
  - att personverfierad multifaktorinloggning används och
  - att ny inloggning genomförs, dvs. lita inte på SSO
- Tjänsten kontrollerar efter lyckad inloggning
  - att multifaktor har använts för inloggningen,
  - att Inloggningen är ny och
  - att användaren uppfyller kraven för SWAMID AL2

SWAMID

SWAMID och Dataskyddsförordningen

- Individens grundläggande fri- och rättigheter enligt Lissabonfördraget är grunden för DSF
- DSF är inte till för att hindra överföring av personuppgifter utan för att skydda personens integritet
- Federationsteknologin är baserad på minimmalitetsprincipen
  - Vid federationsbaserad inloggning överförs endast personuppgifter för en individ i samband med att individen loggar in i en tjänst
  - Inte fler personuppgifter än nödvändigt förs över, personnummer används bara när behov av identifiering med hjälp av personnummer

SWAMID

Effekter av Dataskyddsförordningen

- SWAMID som federation hanterar inte personuppgifter för annat än kontaktuppgifter i metadata, vi har rekommenderat alla att ha funktionsadresser i sina kontaktuppgifter
- För registrering av entitetskategori för tjänster krävs att tjänsteägaren påvisar vilken laglig grund (DSF artikel 6 paragraf 1) som åberopas för behandlingen
- Både IdP och SP måste ha integritetsmeddelande (privacy notice)
- För personuppgiftsincidenter ska REFEDS SIRTFI användas för informationsöverföring mellan SP och IdP (https://refeds.org/sirtfi)

SWAMID

Active Directory Federation Service

- ADFS kan inte uppdatera metadata automatiskt och kan inte heller hantera entitetskategorier!
- SWAMID har tagit fram ADFSToolkit för att ladda och uppdatera metadata från federationen inkl. hantering av entitetskategorier
- Tillsammans med SWAMIDs systerfederation CAF i Kanada har ADFSToolkit förpackats och publicerats på PowerShell Gallery (https://www.powershellgallery.com/packages/ADFSToolkit/)

SWAMID

Swedish Academic Identity Federation

SWAMID