



SWAMID

Swedish Academic Identity Federation

Identitetshantering 101

Identitet i en federerad miljö

Sunetdagarna våren 2025

**Bra identitetshantering är
en förutsättning för god
informationssäkerhet!**

Identitetshantering, vad behövs?

- Tekniska kärnsystem för identitetsadministration
- Källsystem för personinformation
- Tekniska system för inloggning i tjänster
- Tillit till att rätt person loggar in
- Processer och rutiner
- Service desk med stöd för identitetshantering

Tekniskt kärnsystem

- I centrum för identitetshantering och inloggning finns alltid en teknisk kärnkomponent normalt sätt kallad katalogtjänst
- Katalogtjänsten innehåller all information som behövs för att en användare ska få tillgång till en tjänst
- Exempel på nyckelfärdiga katalogtjänster är Active Directory och Microsoft Entra ID

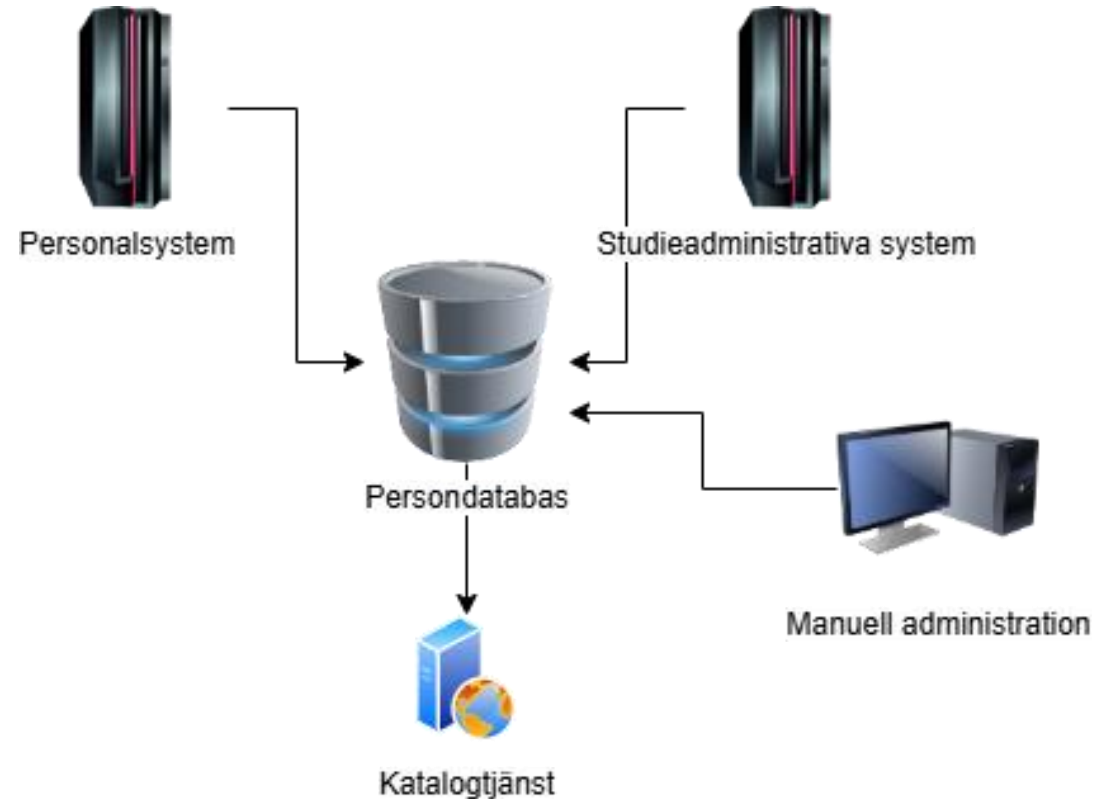
Administrativt kärnsystem

- Många organisationer har ett egenutvecklat försystem till katalogtjänsten, kallas ofta för persondatabas
 - Persondatabasen kan vara sammanbyggd med katalogtjänsten
- Katalogsystem är ofta färdiga nyckelsystem som behöver födas med sammanställd och strukturerad information
- Persondatabasen är verktyget som automatiskt hämtar och sammanställer information från verksamhetsadministrativa system
- Personer kan också registreras manuellt

Källsystem för personinformation

- Uppgifter om anställd personal hämtas personalsystemet
- Uppgifter om studenter hämtas från studieadministrativa systemet (oftast Ladok)
- Uppgifter om övriga personer som behöver kunna logga in i tjänster registreras och underhålls manuellt i persondatabasen

Katalogtjänst och källsystem



Persondatabasen

- Innehåller rådata om personer och organisationen
- Verksamhetsprocesser för kontoaktivering, -deaktivering och tillitsnivåer hanteras ofta i persondatabasen
- Bearbetad rådata synkroniseras med katalogtjänsten för att skapa och underhålla användarkonton med komplett användarinformation
 - Långsiktigt unik användaridentitet som unikt identifierar en person
 - Utformad för att komma ihåg, delas och skrivas vid inloggning
 - Personuppgifter såsom namn och e-postadresser
 - Rättighets- och organisationsuppgifter såsom tillitsnivå, verksamhetsanknytning och grupptillhörigheter

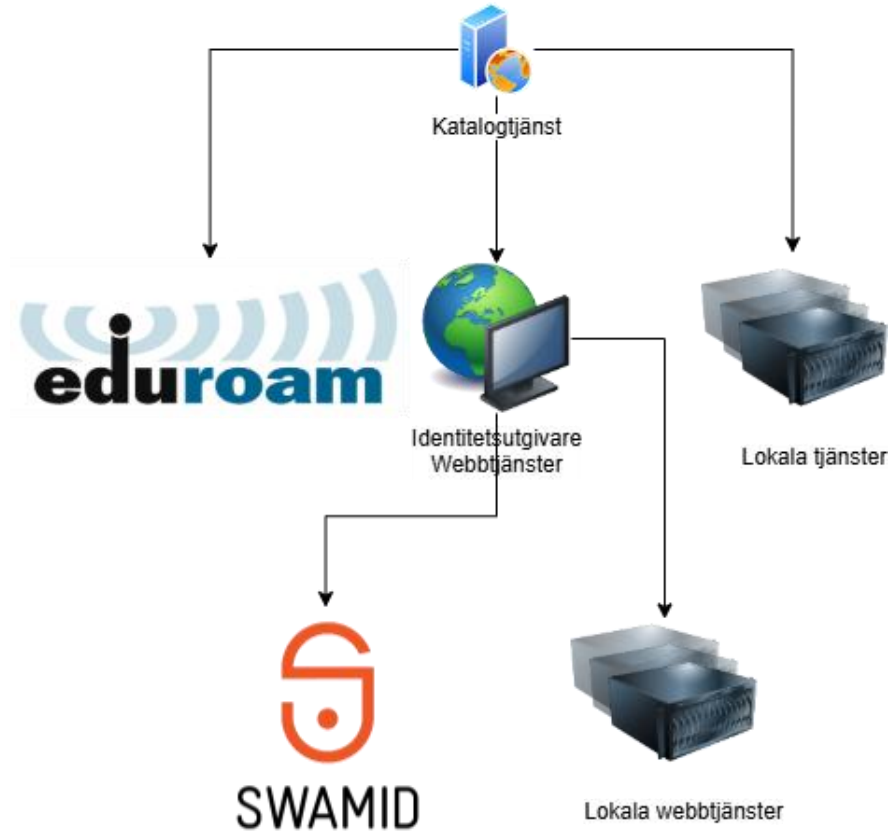
Katalogtjänsten

- Katalogtjänsten kan ha en unik långsiktig teknisk användaridentifierare som inte ska sammanblandas med användaridentifieraren från persondatabasen
 - I Active Directory och Entra ID kallas denna GUID
- Kopplat till katalogtjänsten finns rutiner för utdelning och återställning av inloggningsuppgifter såsom lösenord, passkeys och smartkort
- Katalogtjänsten tillhandahåller rättigheter till tjänster antingen via gruppmedlemskap eller via roller

Inloggning i tjänster

- Interna tjänster vid organisationen är ofta direkt kopplade till katalogtjänsten för inloggning och rättighetsstyrning
 - Kopplingen är ofta byggd på katalogtjänstens interna tjänsteprotokoll
- Webbtjänster använder ofta federerad inloggning vid inloggning
 - Identitetsutgivaren för federerad inloggning är kopplad till katalogtjänsten
 - Antingen är webbtjänsten registrerad i Swamid eller direkt i identitetsutgivaren

Katalogtjänst och anslutna tjänster



Tillit att rätt person loggar in

För att tillit att rätt person loggar in behövs:

- Att organisationen har rutiner och processer för att säkert hantera sin tekniska identitetsinfrastruktur
- Att organisationen har processer som tillräckligt säkerställer att det är rätt person som får tillgång till sitt användarkonto
- Att organisationen använder inloggningsmetoder som delas ut på ett tillräckligt säkert sätt
- Att organisationens inloggningsmetoder är tillräckligt säkra

Behöver vi samma tillit för alla?

NEJ!

- Olika tjänster har olika behov av tillit!
- En tjänst behöver endast veta att användaren finns vid organisationen
- En tjänst behöver bara veta att det är en student
- En tjänst behöver få en pseudonymiserad identifierare för att användaren ska kunna spara inställningar
- En tjänst behöver veta vem personen är med hög tillförlitlighet

Användarkontots livscykel

- En viktig del i att ha tillit till ett användarkonto är livscykelprocesserna
- Hur användaren får tillgång till sitt konto inkl. identifiering måste vara väldokumenterat och följa vedertagna metoder
- Definierade säkra processer för byte av och återställning av lösenord och andra inloggningsfaktorer
- Definierade metoder för avstängning och återaktivering av användarkonton vid incidenter
- Definierade rutiner för avveckling av användarkonto

Tillit i Swamid

Tillitsprofilen Swamid Identity Assurance Level 1 Profile innebär:

1. Att det är en person som innehar och använder kontot, detta kallas även för *obekräftad användare*.
2. Att personen som innehar och använder kontot är identifierad med en eller flera unika användaridentifikatorer som aldrig återanvänds.
3. Att personen som innehar och använder kontot är kontaktbar.
4. Att informationen knuten till kontot ofta är uppgiven av och ansvaras för av användaren själv.
5. Att lärosätets/organisationens identitetshanteringsystem uppfyller minst kraven i SWAMID AL1.

Tillit i Swamid

Tillitsprofilen Swamid Identity Assurance Level 2 Profile innebär:

1. Att högre krav ställs på att lärosätet vet vem personen är som innehar och använder kontot, detta kallas även för *bekräftad användare*.
2. Att personen som innehar och använder kontot är identifierad med en eller flera unika användaridentifikatorer som aldrig återanvänds.
3. Att personen som innehar och använder kontot är kontaktbar.
4. Att lärosätet/organisationen ansvarar för personinformationen.
5. Att lärosätets/organisationens identitetshanteringssystem uppfyller minst kraven i Swamid AL2.

Tillit i Swamid

Tillitsprofilen Swamid Identity Assurance Level 3 Profile innebär:

1. Att högre krav ställs på att lärosätet vet vem personen är som innehar och använder kontot, detta kallas även för *verifierad användare*.
2. Att personen som innehar och använder kontot är kontaktbar.
3. Att lärosätet/organisationen ansvarar för personinformationen.
4. Att inloggning alltid måste ske med multifaktor.
5. Att lärosätets/organisationens identitetshanteringssystem uppfyller minst kraven i Swamid AL3.

Tillit via inloggningsmetoder

- Inloggning med enbart lösenord har idag en relativt låg tillit till att det är kontoinnehavaren som loggar in
- Inloggning med enbart en *faktor som du har* t.ex. en passkey eller säkerhetsnyckel utan pinkod är säkrare än lösenord men tilliten är fortfarande låg
- Inloggning med nätfiskeresistent multifaktor ger hög tillit att det är kontoinnehavaren som loggar in
 - Inloggning med *EJ* nätfiskeresistent multifaktor är bättre än enbart lösenord men inte tillräckligt bra för säker användning

Nätfiskeresistent multifaktor

Att en multifaktor är nätfiskeresistent innebär:

- En kombination av något du har och något du vet eller är
- Faktorn som du har måste vara kryptografiskt säker
- Faktorn som du har kan inte bli flyttad, kopierad eller synkroniserad utan skydd av något du vet eller är
- Faktorn som du har måste vara skyddad från nätfiske och socialt bedrägeri
 - TOTP via Authenticator app eller hårdvara är inte nätfiskeresistent

Att tänka på inom Swamid

- Swamids ryggrad är tillit och det arbete ni som har identitetsutfärdare genomför runt detta
- För att få signalera tillitsnivåer och att multifaktorinloggning har genomförts måste detta finnas beskrivet i er inskickade och godkända Identity Management Practice Statement (IMPS)
- Swamid Operations granskar inskickade IMPSer och Swamid Board of Trustees beslutar om godkännande

Överföring av personuppgifter

- Vid inloggning i en Swamidansluten webbtjänst överförs personuppgifter via s.k. attributrelease
- I Swamid finns två sätt att genomföra attributrelease
 - Informerade automatiska eller manuella överföringsregler baserat på entitetskategorier
 - Automatiska beslut är skalbart och har definierade regler för information till användare och organisation runt personuppgifter
 - Manuell konfiguration av identitetsutfärdaren
 - Kräver mycket arbete vid många tjänster och är därför inte skalbart. Hindrar forskare att snabbt få tillgång till tjänster!

Tack!

Frågor och diskussion...