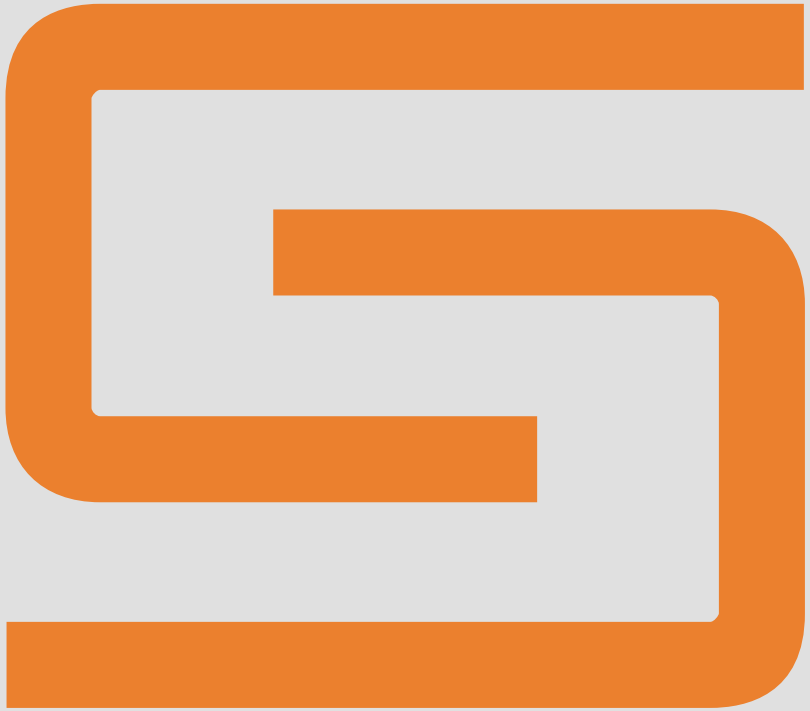
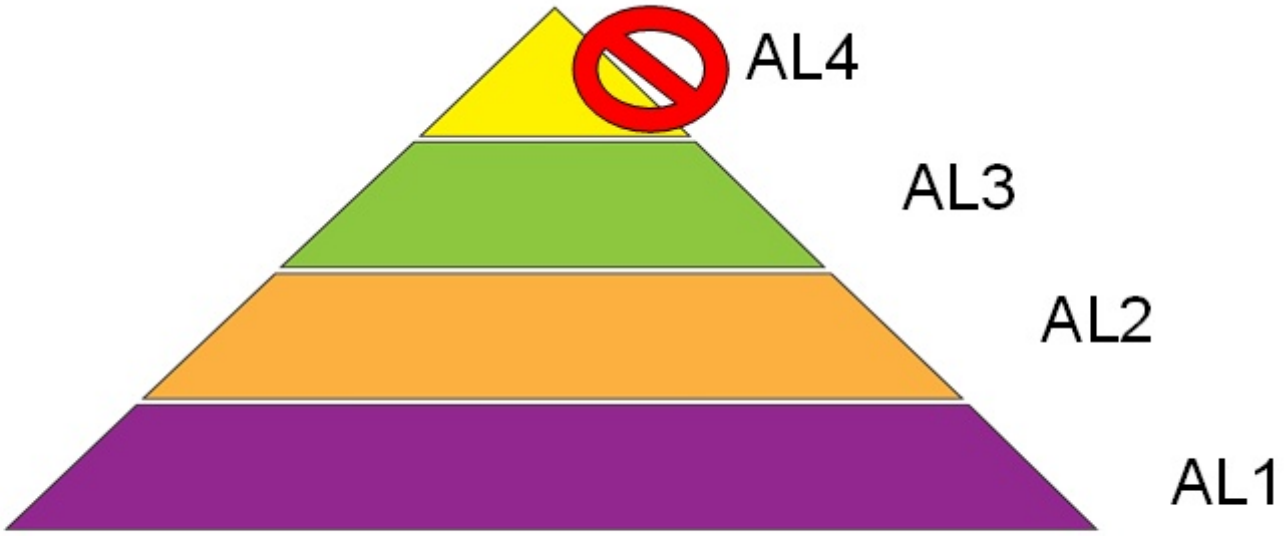


SUNET

Vad är SWAMID AL2?



AL1: Vet att det är en person (obekräftad). Personuppgifterna är självuppgivna.
- Exempel: Facebook och Google

AL2: Vet vem personen är (bekräftad). Uppgifterna är delvis hämtade från annan källa.
- Exempel: Universitet eller högskola.

AL3: Vet mycket väl vem personen är (verifierad). Personen har uppvisat legitimation och personuppgifter är delvis hämtade från annan källa.
- Exempel: Svensk E-legitimation.

Hur är det med BankID?

- Identitetsväxling
- Kostnad (idag 17 öre/inloggning) -> 170MSEK/år?
- De flesta, men inte alla kan få/har BankID

- BankID vill inte vara leverantör enligt våra behov…
  SUNET/VR utkastade från Mina Meddelanden
  UHR fått nej..
  BTH fått nej..
  …

Vad är SWAMID AL2? – del 2

- Vad betyder AL2? Vi vet (med hög rimlighet) att det är rätt person
- Genom SWAMID AL2 uppnår vi en gemensam nivå kring hur vi som lärosäten hanterar och dokumenterar vår identitetshantering.
- SWAMID AL2 har även krav och riktlinjer på den tekniska driften på identitetshanteringssystemen.
- SWAMID AL2 och kommande svensk personuppgiftslagstiftning (GDPR, avsnitt 2 artikel 32 och motiverat i skäl 83)

Mer om SWAMID AL2?

- Måste alla vid ett lärosäte vara SWAMID AL2?
- NEJ. Bara de som har behov.
- Finns alternativ i form av eduID

Ännu säkrare inloggning, eller MFA

- Två-faktor - dvs lösenord plus något mer (tänk BankID eller liten dosa)

- Finns tre varianter, lärosätet hanterar det själv, SUNET genom eduID eller genom statlig e-legitimation (kommande lösning).

eduID och MFA

- eduID har sedan tidigare ett API för TOTP (typ google eller microsoft authenticator)
- För tillfället bygger vi möjlighet att registrera en andra faktor baserad på U2F från FIDO Alliance
- Vi undersöker möjligheten att använda e-legitimation (typ mobilt bankID) som tvåfaktor

Vikten av att en andra faktor är oberoende av den första faktorn

- Autentiseringsfaktorerna kan vara av tre slag:

1. Något man vet (typ lösenord)
2. Något man har (typ mobiltelefon, YubiKey)
3. Något man är (typ fingeravtryck, irisscanning)

- En äkta tvåfaktor är två av dessa tre slag, det får inte vara samma
- I SWAMID ställer vi också krav på att vettingprocessen för de två första faktorerna skall vara oberoende

Hur verifierar man innehavet av en nyckel

- I google, microsoft med mera sjävregistrerar man en nyckel när man är inloggad. Det stärker självklart inloggningssäkerheten, men det stärker inte tillitsnivån.
- Inom SWAMID talar vi om att det inte räcker med ett lösenord för att registrera en nyckel, man måste verifera på något annat sätt än via lösenordet.
- Hur löser vi det?

EIDAS

- Eu:s samlade e-legitimationer
- Om man använder sig av svensk e-legitimation måste man från september 2018 acceptera EIDAS
- Det finns problem att vara säker på vem personen egentligen är ur svenskt perspektiv. EIDAS innehåller i bästa fall unik identifierare, Förnamn, Efternamn och födelsetid. Inga personnummer där..

Så, vad syftar SWAMID AL2 till?

- Att vi som sektor får gemensamma och dokumenterade rutiner för hur vi hanterar identiteter.

- Vad krävs?
  Process- och dokumentationsarbete!

Svar och frågor och kontakt!

- SWAMID:

- www.swamid.se - Pål Axelsson pax@sunet.se
- www.eduid.se - Hans Nordlöf hanor@sunet.se
- Alla frågor: Valter Nordh valter@sunet.se