SUNET

SWAMID AL2

Vad är SWAMID AL2 och vad innebär detta för mitt lärosäte?

Tillitsnivåer i SWAMID

SUNET

SWAMID AL1 – Obekräftad användare

- Kontot innehas av ***en person***
- Används när information är ***kopplat till ett konto*** (t.ex. egengenererad information), t.ex. e-postadress

SWAMID AL2 – Bekräftad användare

- Kontot innehas av ***en identifierad person***
- Används när information är ***kopplad till en person***, t.ex. personnummer och studieuppgifter i Ladok

SWAMID AL1

- Införande att SWAMID AL1 påbörjades vintern 2014/2015

- 13 lärosäten är idag godkända för AL1
- 1 lärosäte ligger för beslut hos SWAMID Board of Trustees

- Kraven på årlig revision i AL1 kommer att ändras till årlig självkontroll i samband med att SWAMID AL2 införs

SWAMID AL2

SUNET

- SWAMID AL2 är på remiss inför beslut i SWAMID Board of Trustees (SWAMID BoT) november 2015
- SWAMID AL2 är en påbyggnad på SWAMID AL1
- Sammanfattning av skillnaderna mellan AL1 och AL2:
  - Godkännande och revisionsförfarande skiljer
  - Högre krav på vem som innehar och använder användarkontot
  - Högre krav på lösenord, lösenordbyte och lösenordsåterställning
  - Högre krav på hantering av attribut
  - Högre krav på krypterade anslutningar och loggning

Vad betyder en inloggning med SWAMID AL2?

SUNET

- Den inloggade användaren är ***kopplad till den aktuella medlemsorganisationen*** i SWAMID
- Den inloggade användaren är en ***identifierad person***
- Den inloggade användaren har en ***unik permanent identifierare*** som inte får återanvändas för annan användare

Godkännande och revisions-förfarande för AL2

- Identity Management Practice Statement (IMPS) ska beskriva hur medlemsorganisationen uppfyller alla delar av AL1 och AL2, inkl. identitetsprocesserna
- SWAMID Operations, eller någon annan part godkänd av SWAMID BoT, genomför granskning av IMPS och rekommenderar SWAMID BoT ett beslut
- Medlemsorganisationen måste årligen meddela att IMPS är fortfarande aktuell
- Vid förändring av IMPS ska den skickas in för förnyad granskning och godkännande

Högre krav på vem som innehar och använder användarkontot i AL2

- Kontoinnehavare måste unikt identifieras
  - Online med hjälp av inloggning med ett personligt konto som har tillitsnivå som motsvarar SWAMID AL2 eller högre
  - Personligt besök i servicedisk med uppvisande av legitimation som uppfyller Skatteverkets regler för godkända id-handlingar samt motsvarande giltiga pass (ICAO Doc 9303), nationella identitetskort inom EU/EES (EU-förordning 2006/562/EG) eller körkort inom EU/EES (EU-direktiv 2006/126/EG)
  - Utskick av tidsbegränsad engångskod till folkbokföringsadress
  - Utskick av tidsbegränsad engångskod till adress på hushållsräkning där namn överensstämmer med namn på kopia av giltig identitetshandling
  - Eller annat motsvarande sätt att identifiera personen

Högre krav på lösenord, -ordbyte och –återställning i AL2

- Krav på att lösenord måste ha en viss komplexitet som motsvarar rekommenderad nivå i AL1
  - Exempel 1: 8 teckens lösenord med stora och små bokstäver samt minst en siffra eller ett specialtecken är OK
  - Exempel 2: 8 teckens komplexa lösenord i Active Directory är OK
- Lösenord skall ha ett bäst före datum, maximalt två år kan vara lämpligt
- Vid återställning av lösenord ska motsvarande rutiner användas som för personidentifiering enligt SWAMID AL2 alternativt en delad engångskod till två i förväg verifierade källor, t.ex. SMS och e-post

Ersätta lösenordsinloggning med multifaktorsinloggning

SUNET

- Istället för inloggning med lösenord på AL2-nivå får två eller fler faktorer användas vid inloggning om de ger motsvarande säkerhet
  - Exempel 1: Inloggning med användarid och lösenord på AL2-nivå kombinerat med Yubikey eller motsvarande
  - Exempel 2: Inloggning med användarid och lösenord på AL2-nivå kombinerat med Google Authenticator, Microsoft Authenticator eller motsvarande där medlemsorganisationen kopplat andra faktorn till individen
  - Exempel 3: PKI-baserad inloggning på kort med pinkod

- Mer information i presentation morgon…

Högre krav på hantering attribut i AL2

SUNET

- Alla attribut som Identity Provider skickar till Service Provider ska medlemsorganisationen ha kontroll över samt ta ansvar för
- Användaren får inte ändra attributvärden själv utan att organisationen verifierar att ändringen är korrekt

Högre krav på krypterade anslutningar och loggning i AL2

- Krav på att all kommunikation in till och mellan ingående komponenter i identitetssystemet är säker och krypterad
  - Det är inte ok med endast skyddade men okrypterade interna ”svarta” nät mellan komponenter som ligger på olika servrar även om de är i samma datorhall
- Krav på att alla relevanta säkerhetshändelser i Identity Provider och underliggande komponenter loggas och sparas på ett säkert sätt

Diskussion

SUNET

- Är kraven på rätt nivå?
- Vad är en realistisk tidplan för införande?
- Vad behöver tydliggöras?
- Behövs det ytterligare alternativ för hur man identifierar en användare eller täcker vi befintliga rutiner på lärosäten?