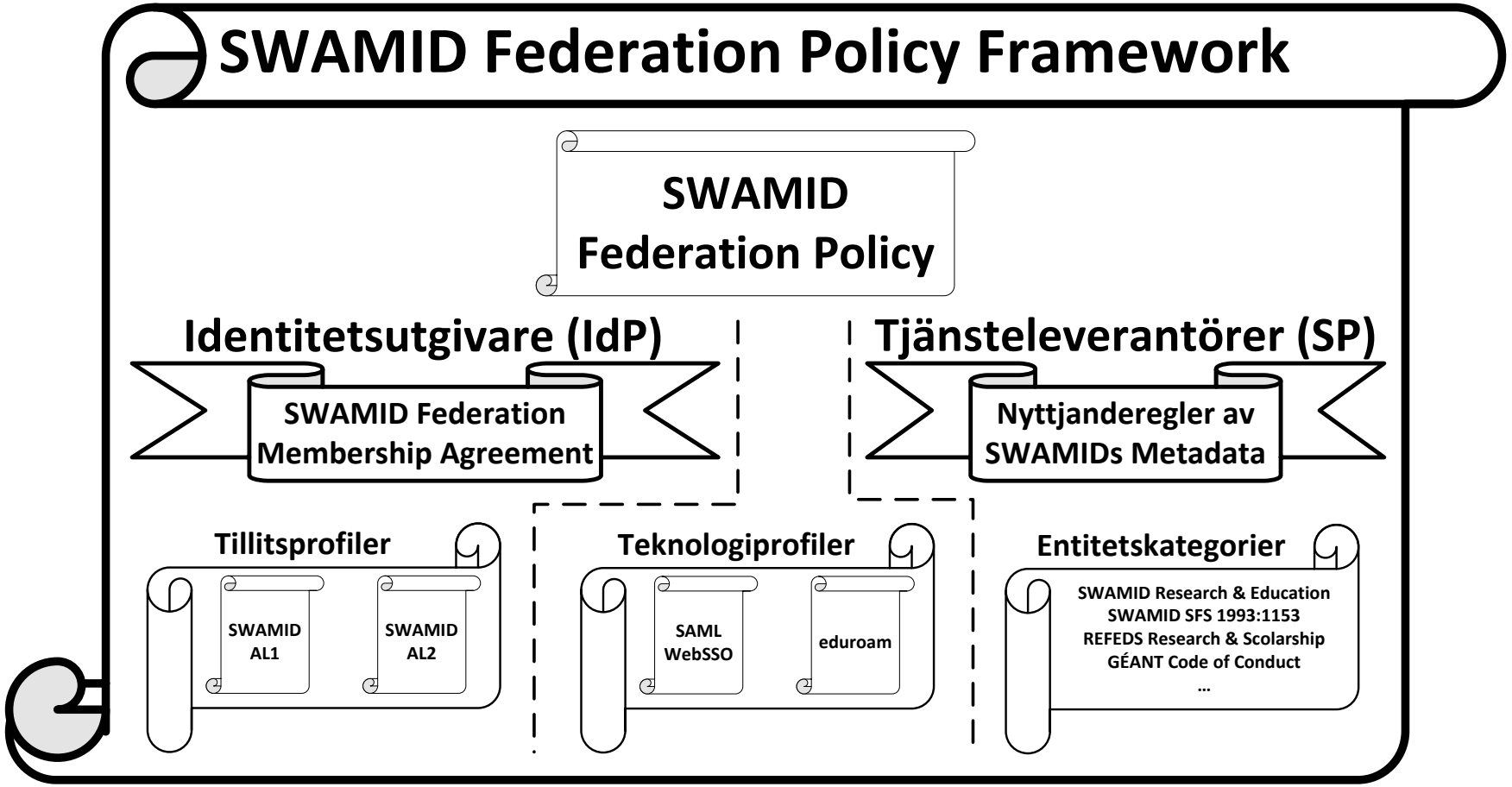
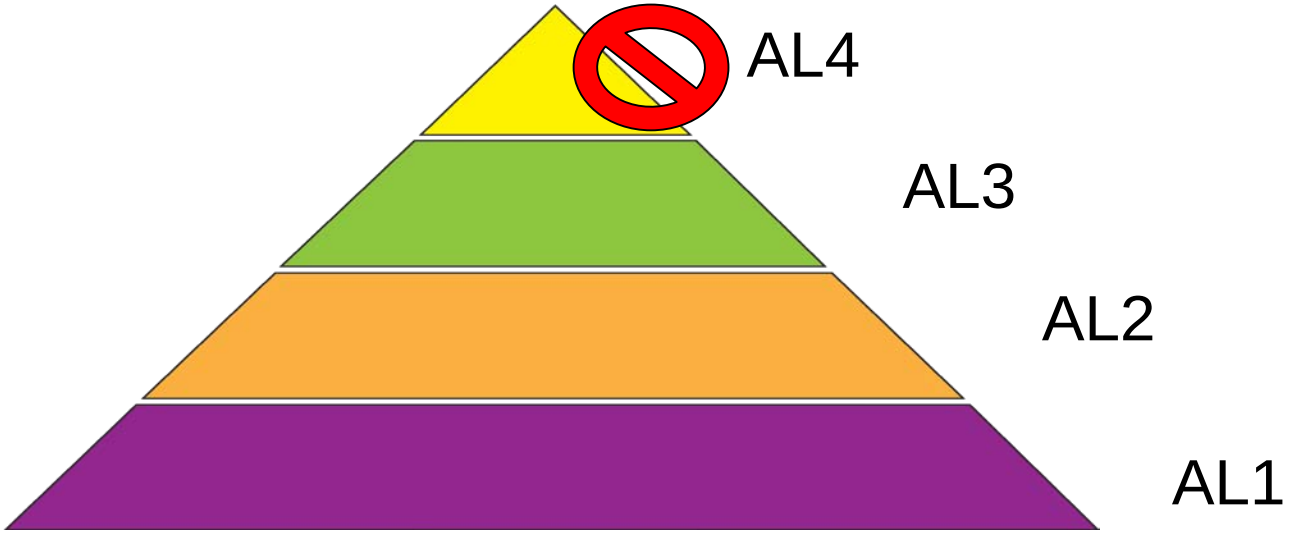
Vad skiljer SWAMID AL1 och SWAMID AL2?

SWAMID


SWAMID Federation Policy Framework
SWAMID
Federation Policy
Identitetsutgivare (IdP)
SWAMID Federation
Membership Agreement
Tjänsteleverantörer (SP)
Nyttjanderegler av
SWAMIDs Metadata
Tillitsprofiler
SWAMID
AL1
SWAMID
AL2
Teknologiprofiler
SAML
WebSSO
eduroam
Entitetskategorier
SWAMID Research & Education
SWAMID SFS 1993:1153
REFEDS Research & Scolarship
GÉANT Code of Conduct
...

Tillitspyramiden



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.

SWAMID AL1 eller SWAMID AL2?

Alla användare vid ett lärosäte behöver inte uppfylla samma tillitsprofil så länge som inloggningstjänsten via s.k. attributrelease kan signalera till aktuell tjänst vilken tillitsprofil som användaren har. Ett lärosäte kan bli godkänt för att intyga att enskilda användare uppfyller:

- SWAMID AL1 och SWAMID AL2,
- endast SWAMID AL1 eller
- ingen av dem.

Aktuell medlemsstatus

- SWAMID har 58 medlemmar

  Universitet, högskolor, forskningsråd och närliggande myndigheter

- 2 medlemmar är godkända för SWAMID AL1 och SWAMID AL2

  Lunds universitet och Uppsala universitet

- 15 medlemmar är godkända för SWAMID AL1

  Chalmers tekniska högskola, Göteborgs universitet, Högskolan Dalarna, Högskolan i Gävle, Högskolan Kristianstad, Jönköping University, Kungliga Konsthögskolan, Luleå tekniska universitet, Mittuniversitetet, Röda Korsets Högskola, Sophiahemmet Högskola, SUNET med eduID, Sveriges lantbruksuniversitet, Umeå universitet och Örebro universitet.

Förändringar i SWAMID AL1 efter beslut 2016-02-05

Förändringar i SWAMID AL1 IMPS

- Identity Management Practice Statement (IMPS) får samma formkrav som i SWAMID AL2
- IMPS ska beskriva hur alla delar av SWAMID AL1 uppfylls
- SWAMID har tagit fram en IMPS-mall som gäller både SWAMID AL1 och SWAMID AL2
  - Finns på sidan SWAMID Identity Assurance i Wikin

Förändringar i SWAMID AL1 Revision

- Granskning av extern part ersätts med initial egengranskning som rapporteras i särskild checklista för SWAMID AL1 tillsammans med IMPS
- Vid förändringar som påverkar processer och system för identitetshantering ska ny egengranskning genomföras och rapporteras
- Årligen genomförs egenkontroll som rapporteras till SWAMID Operations för att säkerställa att kraven i SWAMID AL1 fortfarande uppfylls på samma sätt som tidigare
- Inget särskilt krav på diarieföring av egengranskningen

Förändringar i SWAMID AL1
Övriga förändringar

- Inga nya krav förutom formkraven på IMPS!
- Duplicerade avdelningar om kryptering ersatt med endast ett krav om säkra och krypterade anslutningar (4.3.3)
- Guidance omskrivna på flera ställen för att de ska bli tydligare
- Numrering av avsnitt och krav är harmoniserad med SWAMID AL2 vilket gör att samma IMPS-mall kan användas

SWAMID

Skillnader mellan

SWAMID AL1 och SWAMID AL2

https://wiki.swamid.se/display/SWAMID/SWAMID+AL1+vs+SWAMID+AL2

Avsnitt 2 – Sammanfattning

AL1

Användaren

- är en person och inte en robot eller annan programvara,
- är med *stor sannolikhet* verksam vid medlemsorganisationen,
- är med *stor sannolikhet* identifierad med en unik permanent teknisk identifierare samt
- att användarinformationen är korrekt ansvarar användaren själv för.

AL2

Användaren

- är en identifierad och verifierad person,
- är verksam vid medlemsorganisationen,
- är identifierad med en unik permanent teknisk identifierare samt
- att användarinformationen är korrekt ansvarar medlemsorganisationen för.

Avsnitt 3.2 – Revision

AL1

Medlemsorganisationen genomför egengranskning att de uppfyller SWAMID AL1 och rapporterar detta till SWAMID genom Identity Management Practice Statement med tillhörande checklista.

AL2

SWAMID genomför granskning mot SWAMID AL2 baserat på av medlemsorganisationen insänd Identity Management Practice Statement.

Avsnitt 4.4 – Loggning

AL1

Saknar krav för generell loggning för identitetsmiljön hos medlems-organisationen. Särskilda krav finns senare i tillitsprofilen, bla. att lösenordsändringar skett.

AL2

Krav finns för generell loggning av identitetsmiljön hos medlems-organisationen. Särskilda krav finns senare i tillitsprofilen, bla. att lösenordsändringar skett.

Alla relevanta säkerhets-händelser på IdP och övriga identitetshanteringsystem ska tillsammans med tidsstämpel loggas. Dessa loggar ska hanteras på ett säkert sätt.

Avsnitt 5.1.1 – Lösenord

AL1

Tillåter lösenord med låg kvalité, i praktiken endast fem teckens pinkod.

SWAMID rekommenderar att ni använder samma lösenordskrav i AL1 som krävs i AL2. Detta underlättar övergång mellan tillitsnivåer.

AL2

Kräver lösenord med högre kvalité, i praktiken komplext lösenord med minst åtta tecken.

Avsnitt 5.2.5 – Aktivering och förändring av tillitsnivå 1(2)

AL1

När ett konto aktiveras för första gången ska användaren verifieras

- **på nätet** med hjälp av ett e-postbrev med tidsbegränsad engångskod som skickas till användarens självuppgivna e-postadress,
- **på nätet** genom att använda inloggning från annan identitetsutgivare som är godkänd för SWAMID AL1 eller SWAMID AL2,

…

AL2

När ett konto aktiveras för första gången, eller då höjning av tillitsnivå görs, ska användaren verifieras

- **på nätet** genom att använda inloggning från annan identitetsutgivare som är godkänd för SWAMID AL2,
- **via besök** i service desk, eller motsvarande, tillsammans med uppvisande av godkänd legitimationshandling enligt SWAMID AL2,

…

Avsnitt 5.2.5 – Aktivering och förändring av tillitsnivå 2(2)

AL1

…

- **via besök** i servicedisk eller motsvarande,
- **via brev** med tidsbegränsad engångskod till självuppgiven postadress eller
- **via annan** av SWAMID godkänd motsvarande metod.

AL2

…

- **via brev** med tidsbegränsad engångskod skickad till folkbokföringsadress,
- **via brev** med tidsbegränsad engångskod till adress på kopia av hushållsräkning där namnet överensstämmer med namnet på kopia av godkänd legitimationshandling enligt SWAMID AL2 eller
- **via annan** av SWAMID godkänd motsvarande metod.

Avsnitt 5.2.8 – Kontohantering

AL1

Kontohandläggare och system som används vid kontohantering måste vara verifierade för SWAMID AL1 eller SWAMID AL2.

Förtydligad vid uppdateringen av SWAMID AL1 i februari 2016.

AL2

Kontohandläggare och system som används vid kontohantering måste vara verifierade för SWAMID AL2.

Avsnitt 5.3.3 – Lösenordsåterställning

AL1

Lösenordsåterställning ska ske med

- någon av metoderna i 5.2.5,
- en kanal uppsatt under tiden som kontot var SWAMID AL1, *t.ex. via ett e-postbrev med tidsbegränsad engångskod till fördefinierad e-postadress*, eller
- ett konto via extern identitetsutgivare som uppfyller SWAMID AL1 eller SWAMID AL2, *t.ex. eduID eller Antagning.se.*

AL2

Lösenordsåterställning ska ske med

- någon av metoderna i 5.2.5,
- två kanaler som används gemensamt och var uppsatta under tiden som kontot var SWAMID AL2, *t.ex. via ett e-postbrev med tidsbegränsad engångslänk till fördefinierad e-postadress samt ett SMS med tidsbegränsad engångskod till fördefinierad mobiltelefon,* eller
- ett konto via extern identitets-utgivare som uppfyller SWAMID AL2, *t.ex. eduID eller Antagning.se.*

Avsnitt 5.3.4 – Tvingande lösenordsbyte

AL1

Inget krav!

AL2

Medlemsorganisationen måste kunna aktivera ett tvingande lösenordsbyte för en enskild användare vid ett särskilt tillfälle. Det räcker inte med att användaren gör en lösenords-återställning.

Krav på att lösenord måste bytas efter viss tid finns inte!

Övriga event under våren 2016

- **SWAMID Workshop: Installera och konfigurera Shibboleth IdP v3**
  - Måndagen och tisdagen den 14-15 mars i Stockholm
  - https://wiki.swamid.se/display/SWAMID/Shibboleth+3+installations-workshop+14-15+Mars+2016
- **SWAMID introduktion på Sunetdagarna**
  - Vad är och hur fungerar SWAMID?
  - Onsdag 13 april på Sunetdagarna i Kristianstad
- **SWAMID Webinar: Shibboleth IdP v3 implementerad med hög tillgänglighet**
  - Torsdagen den 21 april 10.00-11.00 på Connect
  - https://wiki.swamid.se/display/SWAMID/SWAMID+Webinar+2+2016

Frågor och mer information

- SWAMID har nya webbsidor på Sunetwebben
  - https://www.sunet.se/swamid/
- All information om tillitsprofiler är samlad på sidan SWAMID Identity Assurance i Wikin
  - https://wiki.swamid.se/display/SWAMID/SWAMID+Identity+Assurance
- Om ni har frågor till SWAMID Operation skicka e-post till operations@swamid.se