
SWAMID
Swedish Academic Identity Federation

Introduktion till SWAMID

SWAMID

- Kort historia:
- Start ca 2003 med Codex och CWAA, WLAN inloggning och NyA
- 2005 startas Swami (SWedish Academic Middleware Initiative)
- 2006/7 ”SWAMID” inklusive eduroam
- 2009 Adobe Connect lanseras som ersättare till Marratech
- 2011 uppdateras SWAMIDs huvudpolicy, blir SUNET-tjänst
- AL1/AL2 – profilerna tas fram

Introduktion till SWAMID

SWAMID

- SWAMID står för:
  Swedish Academic Identity Federation
- - är en SUNET-tjänst
- - drivs av SWAMID Operations
- - styrgrupp, SWAMID Board of Trustees

- Ca 50 identitetsutfärdare
- Över 250 tjänsteleverantörer

SUNET

Introduktion till SWAMID

SWAMID

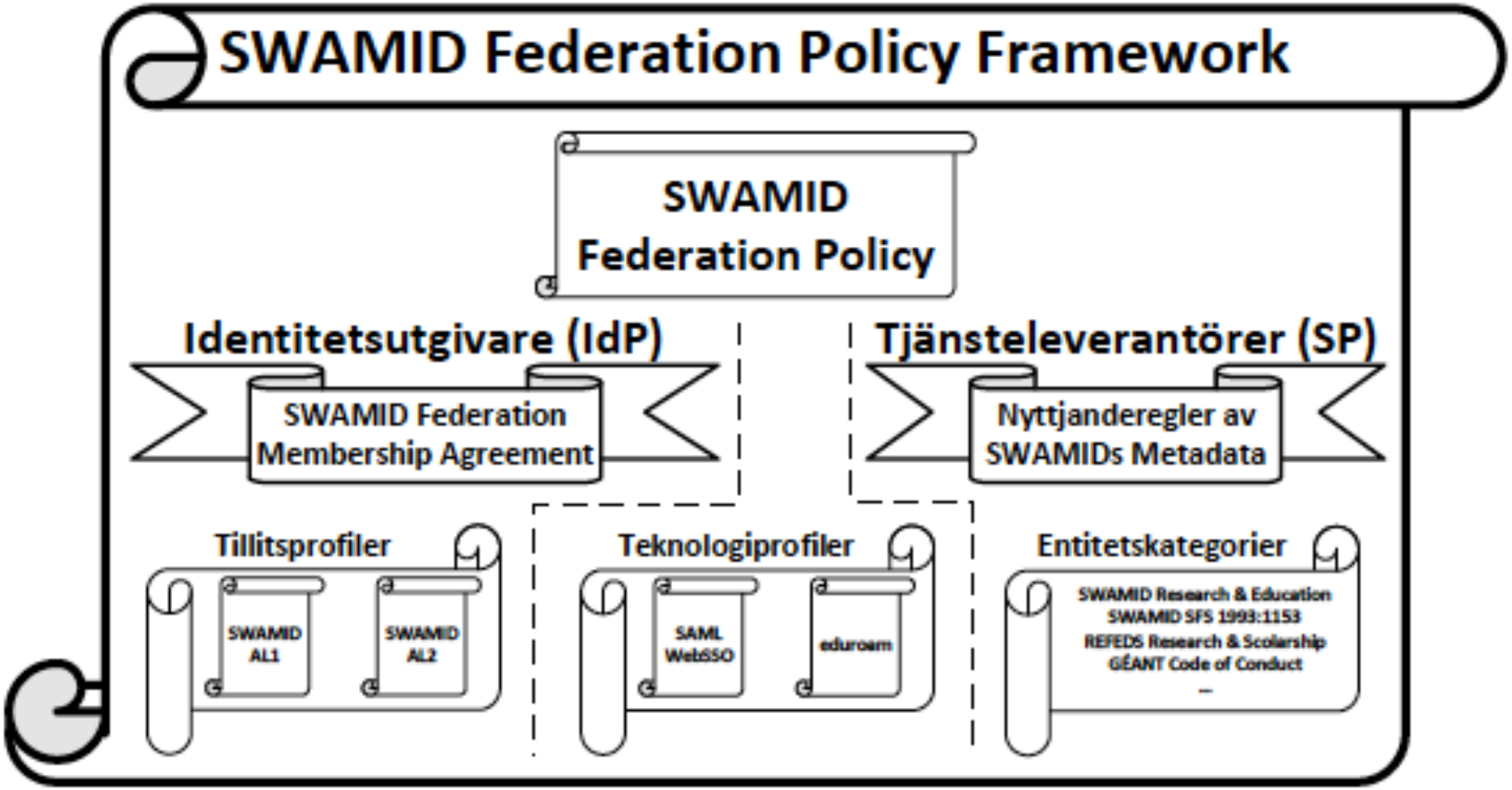
- Två tekniker inom SWAMID-familjen:
  - eduroam för trådlöst internet
  - WebSSO för webb-baserade tjänster (också kallat SAML)
- Samma policy för båda teknikerna
- Samma användare i båda

Begrepp inom identitetsfederationer

SWAMID

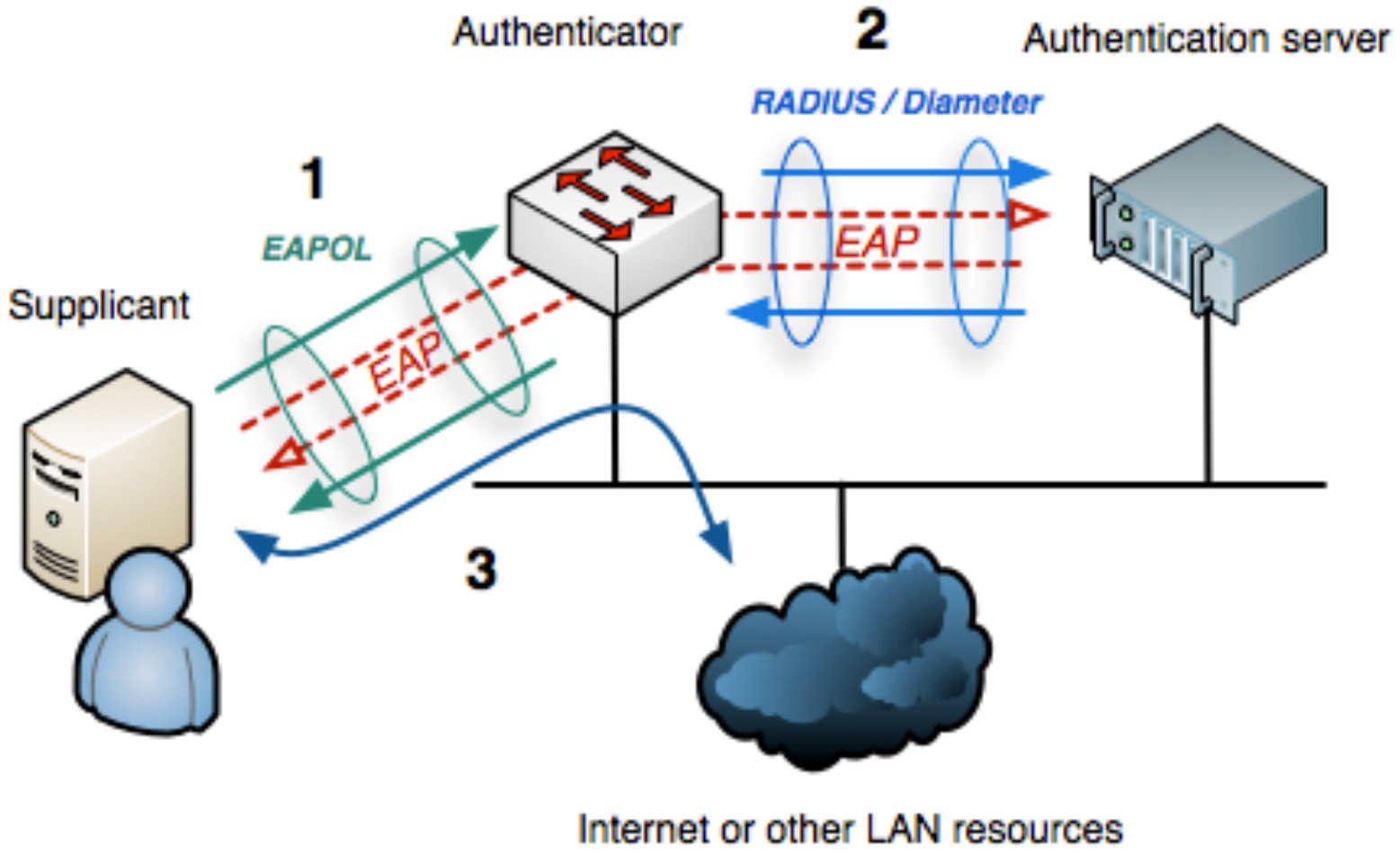
- **IdP** - Identity Provider - Identitetsutfärdare
- **SP** - Service Provider - Tjänsteleverantör
- **DS** - Discovery Service - Anvisningstjänst
- **Radius** – Protokoll för autentisering inom eduroam
- **Federationspolicy** – Dokument som beskriver vad IdP:er och SP:ar skall uppfylla för att vara med i federationen
- **Tillitsramverk** – beskrivning av hur en IdP skall vara organiserad för att på olika nivåer kunna ge SP:ar förtroende för uppgifter
- **Tillitsnivåer** – olika nivåer som innebär att man kan tala om hur väl en IdP vet vem som verkligen använder ett konto

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
...

Eduroam och 802.1x

SWAMID



SUNET

eduroam – vad är det?

SWAMID

- eduroam är en federation av IdP:er som kan autentisera en användare. IdPerna till utbildningssektorn eller andra samhällsviktiga organ
- eduroam används främst trådlöst, men inget hindrar att det används även för trådburen trafik
- Med hjälp av en kedja av radiusservrar kan en användare av eduroam autentisera sig mot sin hem-IdP och få en internetaccess var personen än befinner sig i världen
- En eduroam-IdP måste ha en (minst) SP, men en SP behöver inte ha en egen IdP, det räcker med avtal med en IdP inom eduroam

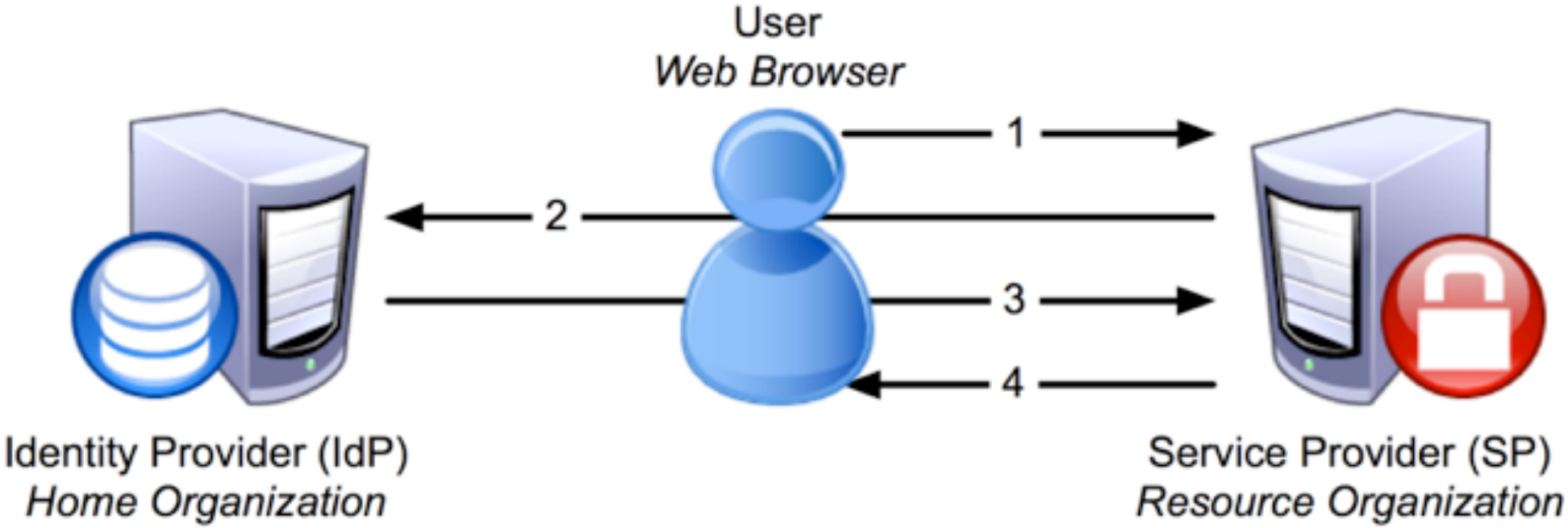
eduroam – hur är det organiserat?

SWAMID

- En toppdomän i varje land. Drivs av SUNET i Sverige
- Varje IdP har radiuskontakt med toppdomänen, som har radiuskontakt med alla nationella domäner utanför den egna
- Vid autentiseringsförfrågan avgörs genom REALM-komponenten i användarnamnet om autentiseringen skall göras av den egna IdP:n eller någon annan. Om det senare är fallet skickas förfrågan vidare till toppdomänen i en kedja av radiusservrar.
- Om autentiseringen hittar rätt så får användaren (supplicant) internetåtkomst

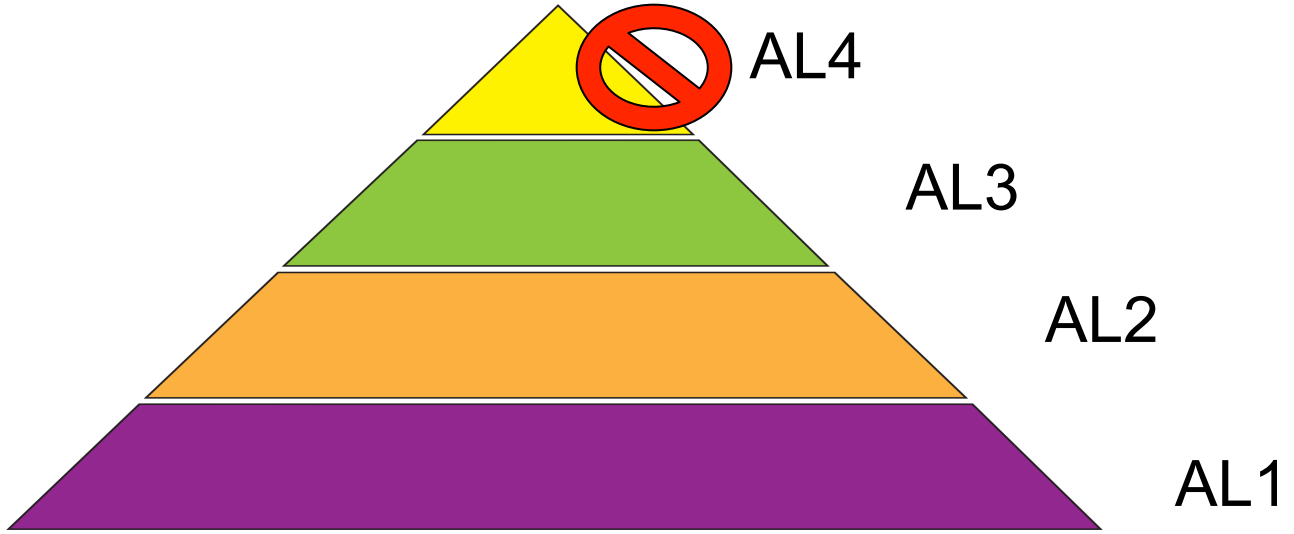
WebSSO - SAML

SWAMID



Tillitspyramiden

SWAMID



AL1: Man vet att det är en person. Personuppgifterna är självuppgivna.
Exempel Facebook
AL2: Man vet ganska väl vem personen är. Uppgifterna är delvis hämtade från annan källa.
Exempel Högskola
AL3: Personen har uppvisat legitimation. Man vet mycket väl vem personen är.
Exempel Svensk E-legitimation

Tillitsnivåer i SWAMID

- Tillitsnivån SWAMID AL1 innebär
  - Att det är en person som innehar och använder kontot, detta kallas även för **obekräftad användare**. Informationen knuten till kontot är oftast uppgiven av och ansvaras för av användaren själv.
  - Lärosätets identitetshanteringssystem uppfyller minst denna tillitsnivå.

Tillitsnivåer i SWAMID

- Tillitsnivån SWAMID AL2 innebär
  - En utökning av SWAMID AL1
  - Att lärosäten vet vem personen är som innehar och använder kontot, användare på denna nivån kallas för **bekräftad användare**.
  - Lärosätet ansvarar för personinformationen till skillnad från SWAMID AL1.
  - Lärosätets identitetshanteringssystem uppfyller minst denna tillitsnivå.

SWAMID AL1 resp SWAMID AL2

- Sammanfattning av skillnaderna mellan AL1 och AL2
  - Godkännande och revisionsförfarande skiljer
  - Högre krav på vem som innehar och använder användarkontot
  - Högre krav på lösenord och lösenordsåterställning
  - Högre krav på hantering av attribut
  - Högre krav på krypterade anslutningar och loggning

Aktivering av konto AL1

SWAMID

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

SUNET

Aktivering av konto AL2

SWAMID

- 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 legitimations-handling enligt SWAMID AL2,
- via brev med tidsbegränsad engångs-kod skickad till folkbokföringsadress,
- via brev med tidsbegränsad engångs-kod till adress på kopia av hushålls-räkning där namnet överensstämmer med namnet på kopia av godkänd legitimationshandling enligt SWAMID AL2 eller
- via annan av SWAMID godkänd motsvarande metod.

Till slut..

SWAMID

- Frågor?

- Hans Nordlöf hanor@sunet.se
- SWAMID: operations@swamid.se

- Länkar:
- sunet.se/swamid
- wiki.swamid.se
- eduroam.se

SUNET