Sunet dagarna

Vad är på gång inom SWAMID?

SWAMID

SWAMID är en av de bästa i eduGAIN-klassen men...

SWAMID

Vad gör oss en av de goda?

- SWAMID ses idag internationellt inom eduGAIN som en pålitlig identitetfederation som uppfyller de grundläggande krav på säkerhet, äkthet, noggrannhet och interoperabilitet som förväntas
- I princip alla identitetsutgivare inom SWAMID fungerar idag väl vid inloggning i internationella forsknings-infrastrukturer, e-infrastrukturer och studentsystem
  - Det vi i Sverige är duktiga generellt på är att ge våra användare tillgång till tjänsterna via lämplig attributrelease

SWAMID

Vad kan vi bli bättre på?

- Multifaktorinloggning via specifikationen REFEDS MFA
  - Stöd finns i samtliga tillitsprofiler i SWAMID men kräver lokal implementation i både processer och teknik
- Tillitsnivå hög enligt REFEDS Assurance Framework (RAF)
  - SWAMID AL3 uppfyller kraven för RAF High
- Stödja incidenthanteringsramverket SIRTFI
  - eduGAIN kommer troligtvis införa krav på detta i nära framtid

- eduID Connect kan hjälpa till med att hantera de två första punkterna

SWAMID

Vad händer eller har hänt i år...

SWAMID

Uppgradering av Shibboleth IdP

- Shibboleth Identity Provider v4 är end-of-life
- Ny modell för stöd från SWAMID Operations
  - Inledande Webinar om vad som behöver göras
  - Webinarer spelas in utan deltagare och publiceras
  - Påminnelse med jämna mellanrum både via Sunets månadsbrev och till saml-admins
  - Öppna frågestunder under lång tid
- Alla utom 2 organisationer har genomfört uppdateringen!
- TACK för bra arbete…

SWAMID

Uppdatering av SWAMIDs tillitsprofiler

- SWAMID Operations har jobbat med att ta fram förslag till uppdaterade tillitsprofiler
- Målet med uppdateringen är att göra tillitsprofilerna mer tydliga och i vissa delar enklare krav
- Förslaget finns tillgängligt på Översyn av SWAMIDs tillitsprofiler 2024 - Sunet Wiki
- Nästa pass 10.00—10.45 presenterar förslaget
- Konsultation öppen till och med 30 november

SWAMID

metadata.swamid.se

- Swamid-Testing har plockats bort

- 1:a sidan ger nu möjlighet att göra ”Validate” för flera entiteter på en gång.
- MDQ länk på respektive entitet

SWAMID

metadata.swamid.se - Validering

- AttributeAuthority
- Storlek på bilder
  - Klagar om de inte stämmer
- Algoritmer
- SAML1
  - Giltiga Bindings

SWAMID

metadata.swamid.se

Nya val på sidan för entityID

- Annual Confirmation
- Remove SAML1 support
- Remove Obsolete Algorithms

SWAMID

metadata.swamid.se

Nya menyposter

- RAF Statistics
- Members

SWAMID

metadata.swamid.se

Påminnelsebrev via e-post

- Metadata behöver valideras
- Något certifikat är på väg att löpa ut / har löpt ut
- Glömt att skicka pending mail till Operations ?
- Glömt kvar i Drafts?

- Nästa år - Påminnelse om att IMPS:en behöver kontrolleras

SWAMID

release-check.swamid.se

- Inget hänt sedan 2023 ☺
- Men… Komihåg att köra testena minst en gång per år, t.ex. i samband med den årliga valideringen av metadata

Hämta metadata via MDQ

- SP / Shibboleth

```
<MetadataProvider type="MDQ”
        id="mdq.swamid.se”
        ignoreTransport="true”
        cacheDirectory="mdq.swamid.se"
        baseUrl="https://mds.swamid.se/">
        <MetadataFilter type="Signature”
                certificate="md-signer2.crt"/>
        <MetadataFilter type="RequireValidUntil"
                maxValidityInterval="2419200"/>
</MetadataProvider>
```

SWAMID

Hämta metadata via MDQ

- IdP / Shibboleth

```
<MetadataProvider id="DynamicEntityMetadata"
        xsi:type="DynamicHTTPMetadataProvider"
        connectionRequestTimeout="PT2S"
        connectionTimeout="PT2S"
        socketTimeout="PT4S">
    <MetadataFilter xsi:type="SignatureValidation" requireSignedRoot="true"
          certificateFile="%{idp.home}/credentials/md-signer2.crt" />
    <MetadataFilter xsi:type="RequiredValidUntil" maxValidityInterval="P14D"/>
    <MetadataQueryProtocol>https://mds.swamid.se/</MetadataQueryProtocol>
</MetadataProvider>
```

SWAMID

Kontrollera tillitsnivå i en applikation som inte har stöd för det

Problem:

- Inloggningslogik kan vara svår att implementera i en befintlig applikation
- Det är svårt att införa förändringar i tredjepartsapplikationer, t.ex. Atlassian Confluence, Primula

SWAMID

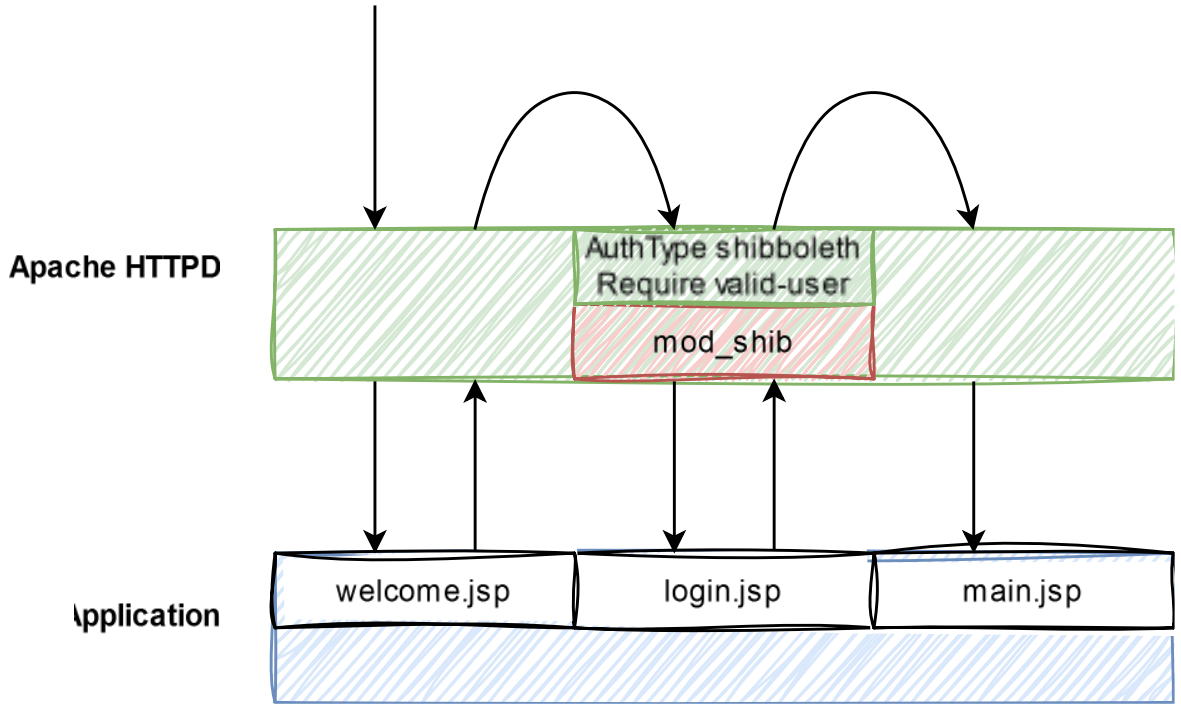
Kontrollera tillitsnivå i en applikation som inte har stöd för det

Lösning:

- Lägg logiken utanför applikationen – i en egen applikation
- Styr kraven på AL2 i Shibboleth Service Provider (shibboleth2.xml)
- Liten eller ingen påverkan på applikationen

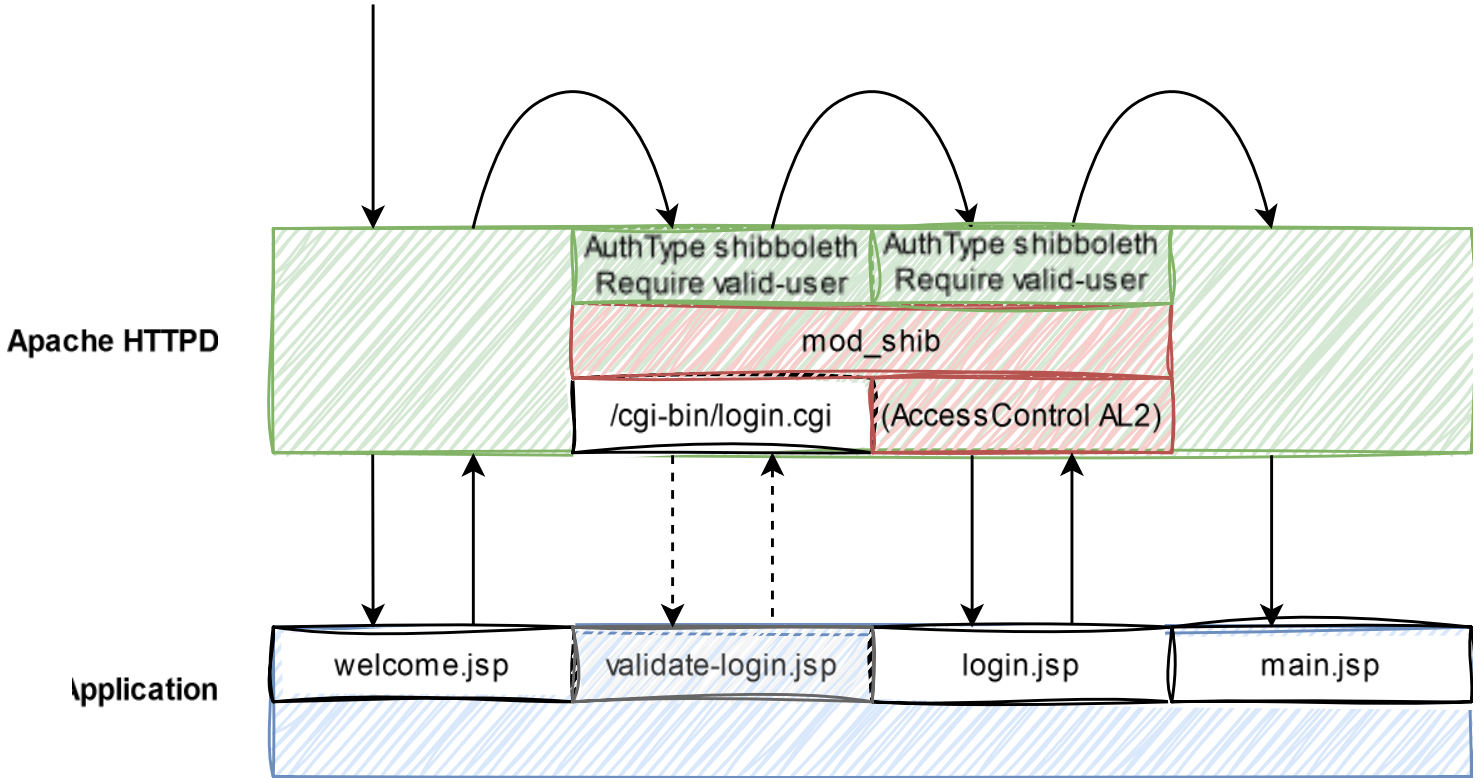
SWAMID

Normalt inloggningsflöde



SWAMID

Modifierat inloggningsflöde



SWAMID

Nya krav för inloggning efter 2025-01-01

Du har loggat in i Confluence med en obekräftad användare från **Umeå universitet**.

För att kunna logga in efter **2025-01-01** behöver du en bekräftad användare, även kallad SWAMID AL2.

Bekräfta din användare vid Umeå universitet

Fortsätt till Confluence

New requirements for signing in as of 2025-01-01

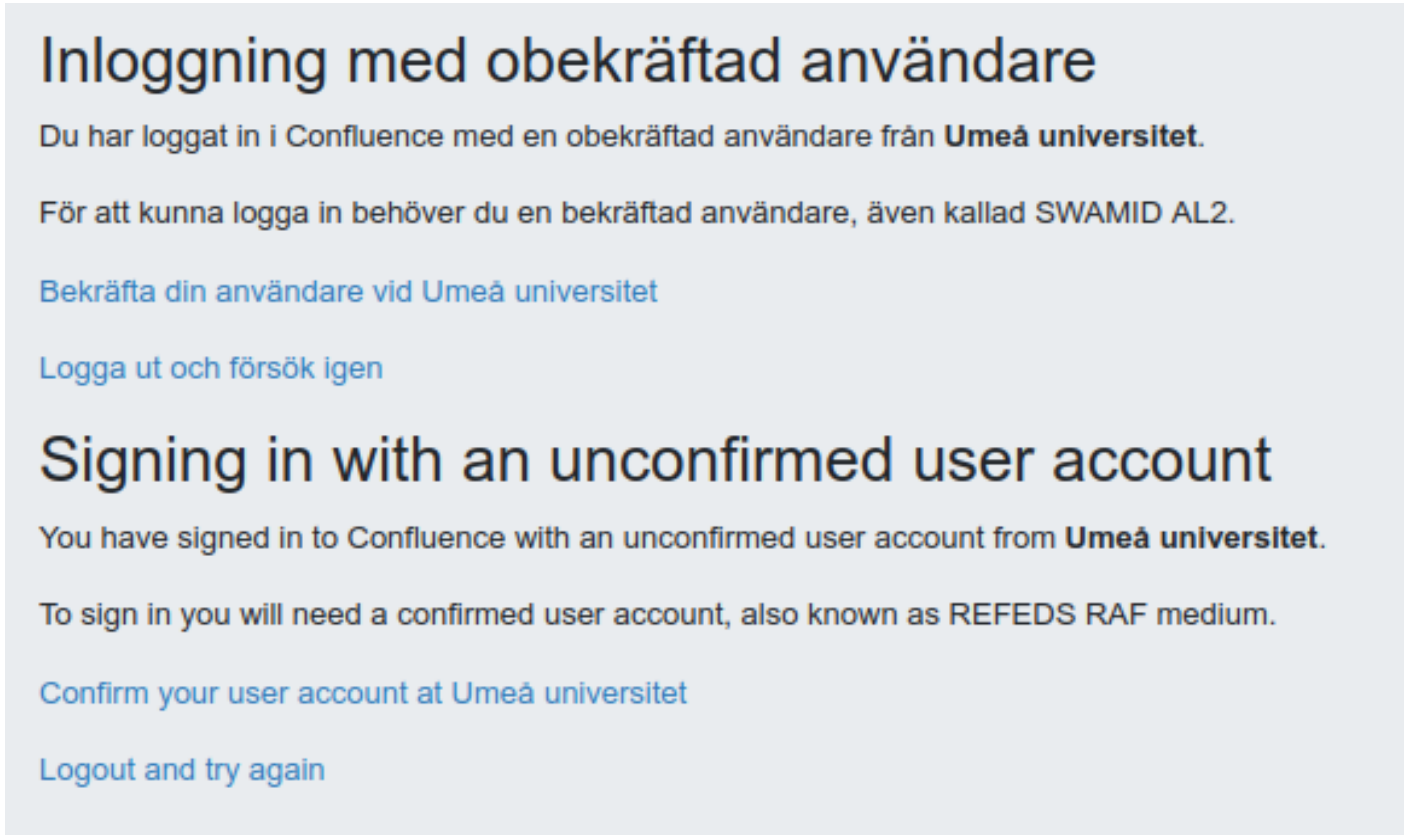
You have signed in to Confluence with an unconfirmed user account from **Umeå universitet**.

To sign in after **2025-01-01** you will need a confirmed user account, also known as REFEDS RAF medium.

Confirm your user account at Umeå universitet

Continue to Confluence

SWAMID



Implementationsdetaljer finns på SWAMIDs wiki, https://wiki.sunet.se/x/PIMADQ

SWAMID

Vad händer nästa år?

SWAMID

Ny federationsteknologi

- SWAMID är idag en identitetsfederation som enbart använder SAML WebSSO för webbaserad inloggning
- SAML utvecklas inte längre och behöver därför på sikt bytas ut
- OpenID Connect over OpenID Federation är ersättaren
- På mycket längre sikt kommer dagens federativa inloggning troligtvis att få ett komplement i en federerad akademisk identitetsplånbok

SWAMID

OpenID Connect over OpenID Federation

- SWAMID kommer att tillsammans med eduGAIN och andra medlemsfederationer ta fram en implementationsprofil
- Shibboleth kommer under 2025 få stöd för federationsteknologin, har redan stöd för OpenID Connect
- SWAMID kommer att undersöka om vi kan bygga ett ADFS Toolkit för den nya federationsteknologin
- För att alla ska kunna börja nyttja den nya federations-teknologin kommer en tillfällig federationsbrygga mellan SAML WebSSO och OIDC over OIDfed byggas

SWAMID

eduGAIN – SIRTFI

- Security Incident Response Trust Framework for Federated Identity (Sirtfi)
- En basnivå för incidenthantering vid federativ inloggning
- eduGAIN kommer med största sannolikhet att införa krav på att SIRTFI stöds av alla inom eduGAIN i två steg
  - Steg 1 är att alla identitetsutgivare och tjänster säkerhetskontakt måste finnas i metadata, incidenthanteringsprocess måste finnas (SWAMID) samt att Traffic Light Protocol (TLP) kan hanteras
  - Steg 2 är fullständigt krav på SIRTFIv2

SWAMID

eduGAIN – Privacy Policy

- eduGAIN kommer med största sannolikhet att införa krav på att Privacy Policy publiceras av alla inom eduGAIN
- SWAMID har redan krav genom teknologiprofilen på att alla ska ha en privacy policy men SWAMID Operations kommer att kontrollera innehållet
- SWAMIDs exempelmallar finns på wikin
  - SWAMID template Service Definition - Sunet Wiki
    - Inkluderar numera Privacy Policy för identitetsutgivare
  - Service Provider Privacy Policy Template - Sunet Wiki

SWAMID

SWAMID

Swedish Academic Identity Federation