SWAMID

Swedish Academic Identity Federation

Från A-Ö för att ansluta en tjänst till SWAMID

Fredrik Domeij, SWAMID Operations
fredrik.domeij@umu.se
2021-04-22

SWAMID

Innehåll

- Övergripande om SAML och federationer
- Service Provider-programvara – val och konfiguration
- Bygga en bra tjänst i SWAMID
- Tjänsten i federationen

SWAMID

Övergripande om SAML och federationer

- Identity Provider (IdP), eller identitetsutfärdare
  - Inloggningstjänst för användare
  - Kopplad till bakomliggande katalogtjänst med alla attribut för användare (användarnamn, lösenord, epost-adress osv)
- Service Provider (SP)
  - Tjänsterna som användare vill logga in på
- Discovery Service (DS)
  - Tjänst som hjälper användare hitta sin egen IdP i federationen för inloggning i en tjänst

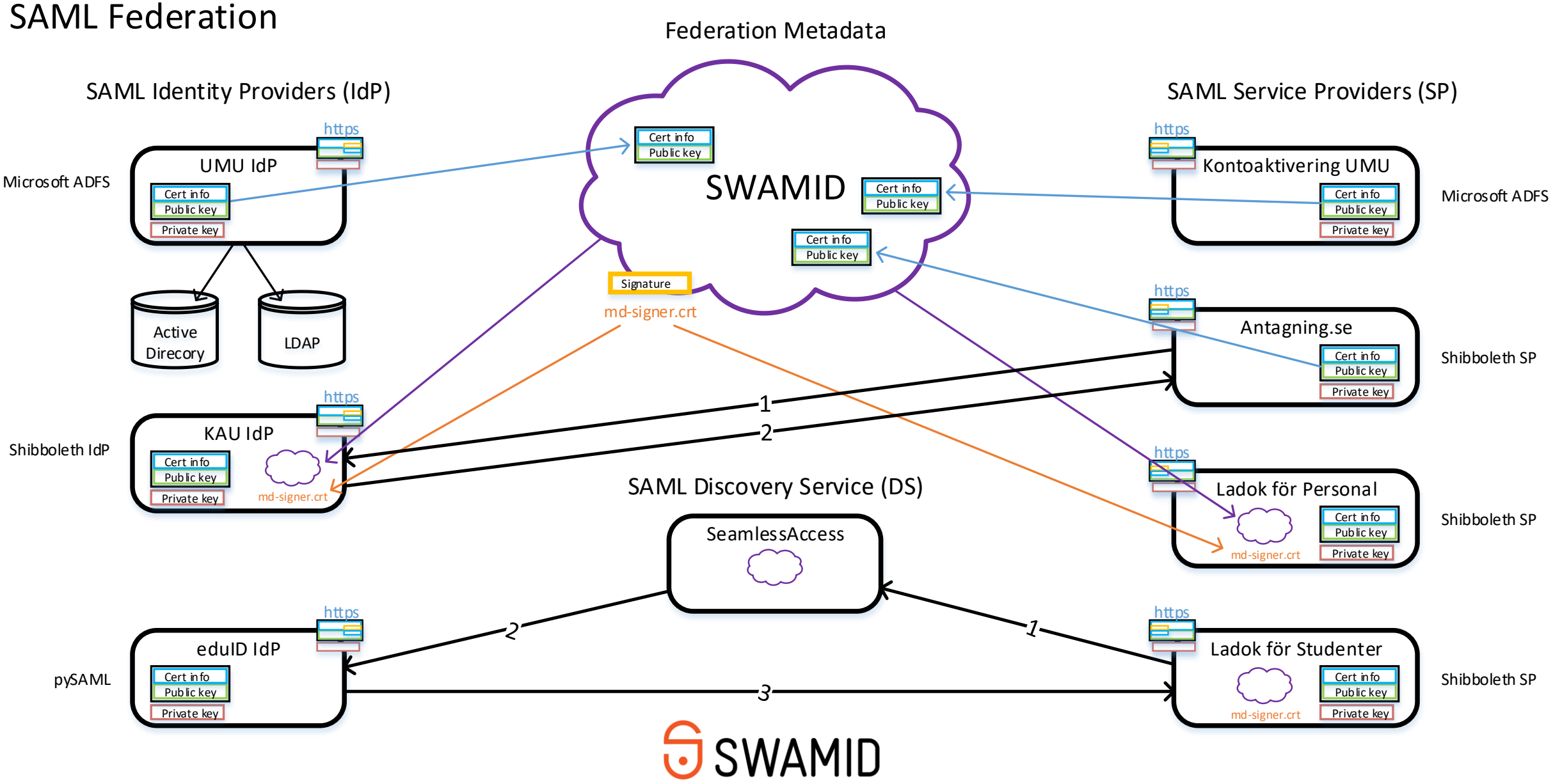
SWAMID

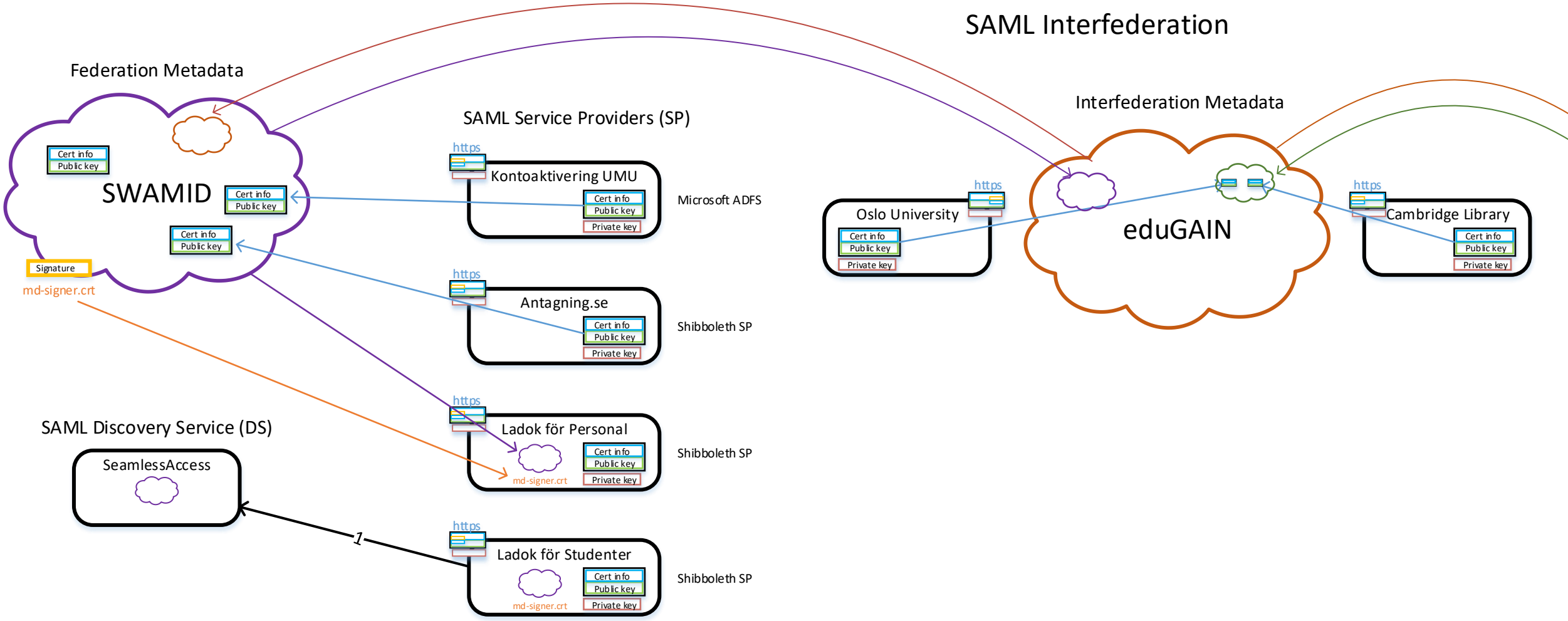
Övergripande om SAML och federationer

- Federation (SWAMID, Feide, Haka, WAYF, InCommon, …)
  - Metadata för flera identitetsutfärdare/tjänster
    - Namn
    - SAML-webbadresser för inloggning och attribut
    - Certifikat
    - Signeras av federationens signeringscertifikat
- Interfederation (eduGAIN, 27 federationer)
  - Metadata för flera federationer
  - Signeras av interfederationens signeringscertifikat
- REFEDS – the Research and Education FEDerations group
  - Samordnar frågor kring identitetsfederationer inom forskning och utbildning

SWAMID

SAML Federation



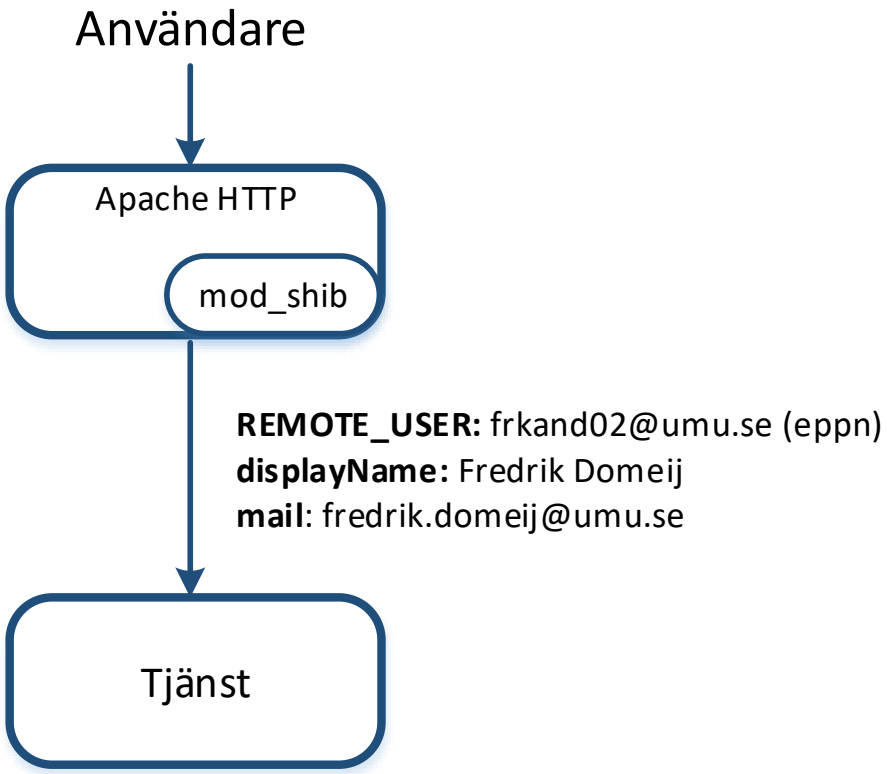

SAML Interfederation
Federation Metadata
SAML Service Providers (SP)
Interfederation Metadata
SWAMID
Cert info
Public key
Signature
md-signer.crt
https
Kontoaktivering UMU
Private key
Microsoft ADFS
Antagning.se
Shibboleth SP
Ladok för Personal
Ladok för Studenter
SAML Discovery Service (DS)
SeamlessAccess
1
Oslo University
eduGAIN
Cambridge Library

SWAMID

Service Provider-programvara – val och konfiguration

SWAMID

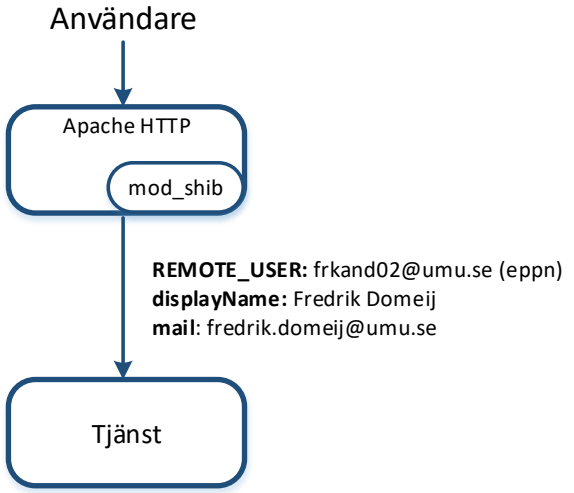
Service Provider-programvara – val och konfiguration



SWAMID

Service Provider-programvara – val och konfiguration

- Val av webbserver (TLS-terminering, SP environment)
  - Apache HTTP Server
  - Microsoft IIS
  - Python
- Val val SP-programvara
  - Shibboleth (66% i SWAMID)
  - SimpleSAMLphp (9%)
  - PySAML (2%)
  - ADFS (2%)
  - Annat (21%)
- Stöd vid installation och konfiguration på https://wiki.swamid.se



SWAMID

Service Provider-programvara – val och konfiguration

- entityID – unik identifierar i federationen
  - Exempel https://www.student.ladok.se/student-sp
- Internt SAML-certifikat
  - Bör vara giltigt i minst 10 år
  - Self-signed
  - Trust ligger inte i certifikaten utan i signering av federationsmetadatan
  - Vid byte tas det gamla certifikatet bort från metadatan

SWAMID

Service Provider-programvara – val och konfiguration

- Resolving av attribut
  - Användarattribut
    - eduPersonPrincipalName, namn, epost
    - assurance, affiliation, entitlements
    - Personnummer, ORCID
  - IdP-attribut (Meta-attribut)
    - Assurance-certification (SWAMID AL1/AL2/AL3)
    - errorURL
  - Exempel finns på https://wiki.swamid.se

SWAMID

Bygga en bra tjänst i SWAMID

SWAMID

Bygga en bra tjänst i SWAMID

- Val kring inloggning – Krav på Assurance Level

Tillitsnivå	**Vad vet vi**	**Lägsta identifieringsnivå**	**Attribut**	**MFA**
SWAMID AL1	En person	Har klarat en CAPTCHA	Självuppgivna	Tillåts
SWAMID AL2	Bekräftad person	Har fått PIN-kod till sin folkbokföringsadress	Kontrollerade mot andra system, ex. personnummer	Tillåts
SWAMID AL3	Verifierad person	Har uppvisat legitimation för betrodd part	Kontrollerade mot andra system, ex. personnummer	Alltid

SWAMID

Bygga en bra tjänst i SWAMID

- Val kring inloggning - Autentisering
  - Normalt lösenordsinloggning (ofta implicit eller explicit Single sign-on)
  - Tvåfaktorsinloggning (MFA)
    - SWAMID AL1: Skyddar det egna kontot
    - SWAMID AL2: MFA kopplad under AL2-inloggning
    - SWAMID AL3: MFA utdelad under uppvisande av legitimation
    - Värde på AL1/AL2-nivå - Hög sannolikhet att det är samma person som loggar in varje gång
  - ForceAuthn
    - En tjänst kan begära att en inloggningstjänst tvingar en inloggning (inaktiverar SSO)
  - Step-up
    - Höjning av autentisering efter inloggning
    - Tvinga MFA när något extra viktigt ska göras (”signering”)

SWAMID

Bygga en bra tjänst i SWAMID

- Implementering av identifierande attribut/användarnamn i tjänsten
  - eduPersonPrincipalName (exvis frkand02@umu.se) är unikt och återanvänds ej inom SWAMID
  - Arbete pågår inom REFEDS för att hitta något som fungerar bra globalt (subject-id respektive pairwise-id)
- Hantering av inloggningssession
  - Alternativ 1: Hela tjänsten skyddas av SAML-inloggning
    - Enkel implementation (alla attribut följer med vid varje request)
  - Alternativ 2: Sessionsinloggningssida
    - Möjliggör fler inloggningsmetoder (lokal inloggning, svensk e-legitimation osv)
  - Lita inte på Single Logout, uppmana användaren att stänga webbläsaren

SWAMID

Bygga en bra tjänst i SWAMID

- Begäran av attribut från IdP:erna (entitetskategorier)
  - En markering i metadata på tjänster för att möjliggöra automatiserad skalbar minimerad attributrelease
  - REFEDS Research and Scholarship
    - Tjänster som har som syfte att stödja forskning och utbildning
    - Standardrelease
      - eduPersonPrincipalName (eppn)
      - E-post
      - Namn
      - assurance (SWAMID AL1/AL2/AL3)
      - affiliation (student, employee etc)

SWAMID

Bygga en bra tjänst i SWAMID

- Begäran av attribut från IdP:erna (entitetskategorier)
  - GÉANT Dataprotection Code of Conduct
    - Öppen för alla
    - Privacy-policy krävs av tjänsten (som bland annat deklarerar att GDPR följs)
    - Begäran av attribut (minimalitetsprincipen)
      - eduPersonPrincipalName
      - E-post
      - Namn
      - assurance
      - affiliation
      - Personnummer
      - ORCID (forskar-id)
  - Mer information på https://wiki.swamid.se

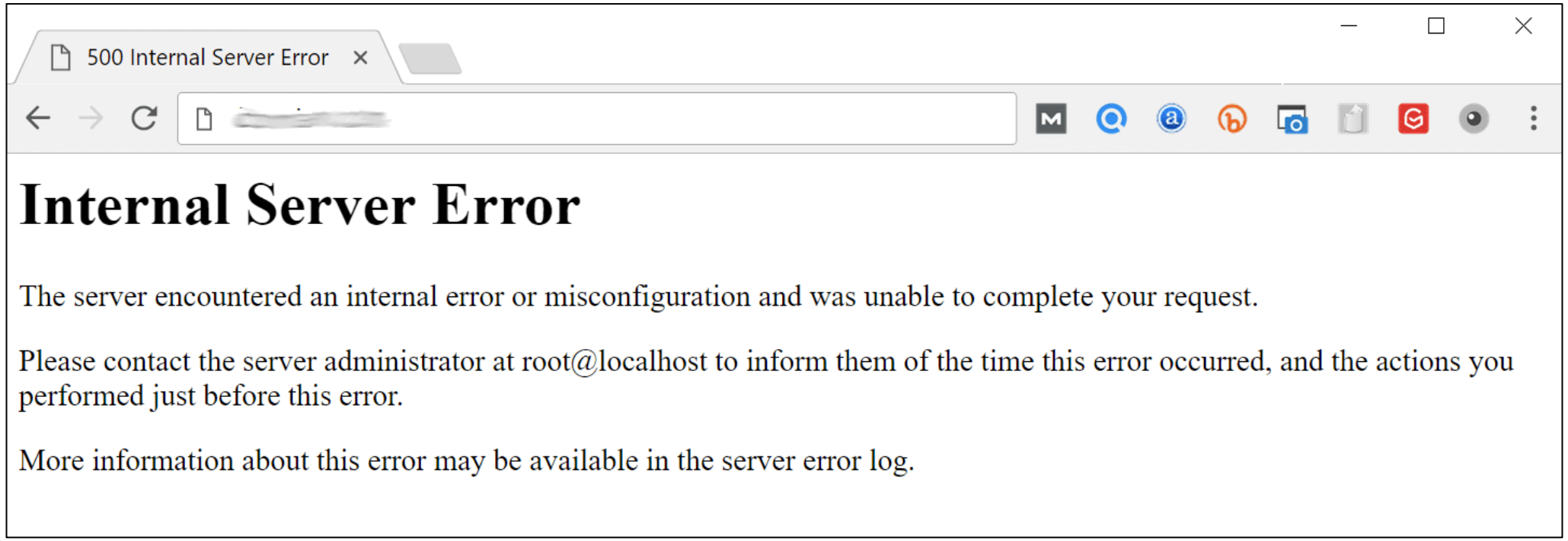
SWAMID

Bygga en bra tjänst i SWAMID

- Hantering av inloggningsproblem - errorURL
  - Vanliga inloggningsproblem
    - Problem med identifiering (ex. saknade attribut)
    - Problem med autentisering (ex. misslyckad MFA-inloggning)
    - Saknade behörigheter (affiliation, assurance, entitlements)
    - Andra fel som förväntas vara lösbara för användaren utan inblandning av tjänsten
  - Hjälp användaren!

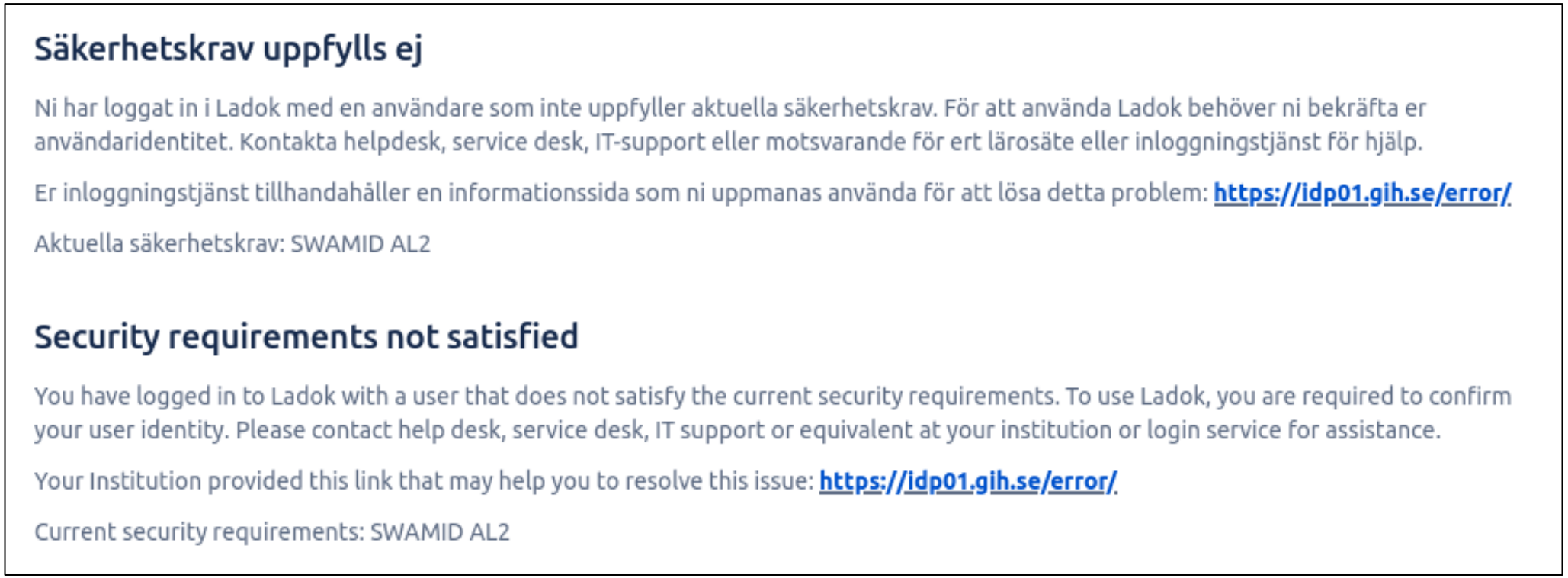
SWAMID

- Att inte hjälpa användaren



SWAMID

- Bättre hjälp – vad är problemet och vad kan användaren göra åt det?



Säkerhetskrav uppfylls ej

Ni har loggat in i Ladok med en användare som inte uppfyller aktuella säkerhetskrav. För att använda Ladok behöver ni bekräfta er användaridentitet. Kontakta helpdesk, service desk, IT-support eller motsvarande för ert lärosäte eller inloggningstjänst för hjälp.

Er inloggningstjänst tillhandahåller en informationssida som ni uppmanas använda för att lösa detta problem: https://idp01.gih.se/error/

Aktuella säkerhetskrav: SWAMID AL2

Security requirements not satisfied

You have logged in to Ladok with a user that does not satisfy the current security requirements. To use Ladok, you are required to confirm your user identity. Please contact help desk, service desk, IT support or equivalent at your institution or login service for assistance.

Your Institution provided this link that may help you to resolve this issue: https://idp01.gih.se/error/

Current security requirements: SWAMID AL2

SWAMID

- Identitetsutfärdarens egna hjälpsidor

Bekräftad användare krävs

Tjänsten du försökte nå kräver en *bekräftad* användare, även kallad SWAMID AL2.

Identiteter bekräftas oftast genom besök i organisationens servicedesk eller motsvarande under uppvisande av legitimation.

Kontakta din organisation för att bekräfta din användare och försök igen. Om du redan är bekräftad, kontakta din organisation och ange vilken tjänst du försökte nå, eventuella felmeddelande du fick samt, om möjligt, en skärmdump med felmeddelandena inklusive webbadressen högst upp i webbläsaren och motsvarande från denna sida.

IT-Support
E-post: itsupport@gih.se
Telefon: +46812053841

Gymnastik- och idrottshögskolan | Lidingövägen 1 | Stockholm | 08-120 537 00

Teknisk information:

```
ERRORURL_TS: 1607969220 (2020-12-14T18:07:00Z)
ERRORURL_RP: https://www.student.ladok.se/student-sp
ERRORURL_TID: error-5fd7a9c448086
ERRORURL_CTX: http://www.swamid.se/policy/assurance/al2
```

Bygga en bra tjänst i SWAMID

- Hantering av inloggningsproblem - errorURL
  - errorURL – identitetsutfärdarens hjälpsidor
    - Finns för alla identitetsutfärdare i SWAMID sedan mars 2021
    - Innehåller placeholders för att länka användaren till mest lämpad information hos den egna organisationen
    - Beskrivning finns på https://wiki.swamid.se

Tjänsten i federationen

SWAMID

Tjänsten i federationen

- Vem får ansluta en tjänst till SWAMID?
  1. Tjänst som tillhandahålls av medlem i SWAMID
  2. Tjänst med avtal med en eller flera av SWAMIDs medlemmar
  3. Tjänst från svenska myndighet riktad till SWAMIDs medlemmar
  4. Tjänster som uppfyller kraven för REFEDS R&S oavsett entitetskategori
     "Candidates for the Research and Scholarship (R&S) Category are Service Providers that are operated for the purpose of supporting research and scholarship interaction, collaboration or management, at least in part."
  5. Tjänst som får särskilt beslut av SWAMID Board of Trustees

SWAMID

Tjänsten i federationen

- Registrering av metadata
  - Låt Service Provider-programvaran generera metadatan
  - Önskade entitetskategorier
  - MDUI
    - DisplayName, Description, Logo
    - InformationURL, PrivacyStatementURL
  - Organization
    - OrganizationName – Registrerat namn för organisationen som äger tjänsten (organisationsnummer)
    - OrganizationDisplayName – Normalt samma som OrganizationName
    - OrganizationURL – Organisationens webbsida

SWAMID

Tjänsten i federationen

- Registrering av metadata
  - ContactPerson
    - Kontaktuppgifter till tjänsten
    - Bör vara funktionsadresser pga GDPR
    - **administrative** - icketekniska frågor kring tjänsten
    - **technical** - den tekniska driften av tjänsten
    - (**support**) - kontakt för slutanvändare
    - (**security**) - kontakt för säkerhetsincidenter och andra säkerhetsrelaterade ärenden
  - Skicka till operations@swamid.se

SWAMID

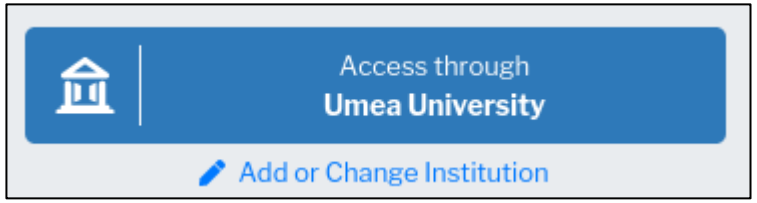
Tjänsten i federationen

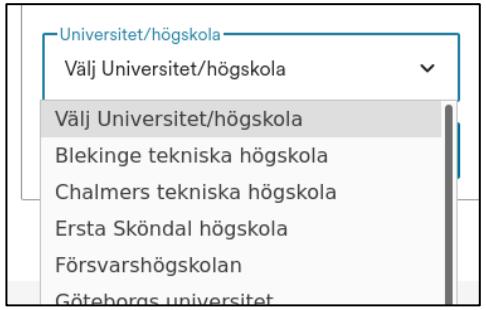
- Val av metadataström
  - Styr från vilka identitetsutfärdare användare kan använda för inloggning
  - Identitetsutfärdare både från SWAMID och eduGAIN
    - https://mds.swamid.se/md/swamid-idp-transitive.xml
  - Identitetsutfärdare endast från SWAMID
    - https://mds.swamid.se/md/swamid-idp.xml
  - Signerade av SWAMIDs signeringscertifikat
    - https://mds.swamid.se/md/md-signer2.crt

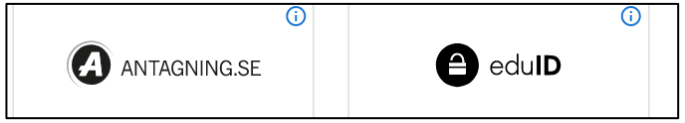
SWAMID

Tjänsten i federationen

- Val av identitetsutfärdare för användare
  - Via discovery-tjänst
    - SeamlessAccess
    - Drar nytta av tidigare val
    - Användare känner igen sig
  - Statisk lista
    - Oberoende av extern tjänst
    - Behöver underhållas, IdP:er byts ut
  - En eller ett fåtal IdP:er
    - Används i många kontoaktiveringstjänster (eduID + Antagning.se)
    - Begränsande, bör kompletteras med Discovery-tjänst för att hjälpa användaren







SWAMID

Tjänsten i federationen

- Hantering av säkerhetsincidenter
  - SWAMIDs incidenthanteringsprocess
  - Sirtfi (Security Incident Response Trust Framework for Federated Identity)
    - Checklista på viktiga säkerhetsområden
    - Ta del av säkerhetsincidenter inom federationen
    - Definierad kontaktväg vid säkerhetsincidenter

SWAMID

Tid för frågor?

Fredrik Domeij, SWAMID Operations
fredrik.domeij@umu.se
2021-04-22

SWAMID

Tack för att ni lyssnat

Fortsättning 10:15

- Vad är på gång inom SWAMID

Ge oss feedback!

- https://sunet.artologik.net/sunet/sunetdagarna2021
- Vad tyckte du om detta pass?
- Vad är ditt intryck av vårens Sunetdagar i sin helhet?
- Har du någon annan åsikt du vill dela med dig av?

Besök oss gärna på After Work i kväll mellan 17.15 och 19.00

- https://www.wonder.me/r?id=19633577-b561-4a16-af71-8fe3fb925884

SWAMID