

Ansluta tjänst till SWAMID

Några få steg...

Vad är SWAMID?

- 50% policy
- 50% förtroende
- 50% teknik
 - metadata
 - discovery

ett, två, tre...

1. Hämta och uppdatera metadata regelbundet
2. Hantera IdP-val för användare
3. Skicka egen metadata till operations

Metadata

Metadata - hjärtat i SWAMID

- Signerad lista på allt som finns i SWAMID
- Permanent URL
 - <http://md.swamid.se/md/swamid-idp.xml>
 - <http://md.swamid.se/md/swamid-idp-transitive.xml>
- Hämta innehållet "tillräckligt" ofta
- All modern programvara sköter detta åt dig
 - Shibboleth
 - SimpleSAMLphp
 - pySAML2

Discovery

Discovery

- Varje tjänst måste lösa discovery-problemet
- SWAMID har lösningar för *vissa* typfall
- Det är bäst att göra discovery *nära* tjänsten

Attribut

Attribut

- Huvudregeln
 - Alla tjänster förhandlar direkt med IdPer om attribut
- Tjänstekategorier
 - Grupper av tjänster med jämförbara egenskaper
 - Används av IdP:er för distribution av attribut
 - Kontakta SWAMID operations

Våra tjänstekategorier

- SFS-1993-1153
 - LADOK
 - NyA
 - CSN
 - konto- & kurs-registrering
 - kontrollerad hantering av personnummer
- Research and Education
 - Lågrisk användning av persondata
 - I huvudsak forskning och utbildning
 - epost, namn, affiliering, organisation

Processen...

1. Skicka beskrivning av tjänsten till operations med fokus på hur persondata hanteras och be om kategori.
2. SWAMID operations behandlar ansökan
3. Tjänsten märks upp i SWAMID metadata
4. IdPer som använder tjänstekategorier skickar attribut.

Och glöm inte...

Skicka tjänstens metadata till SWAMID!

operations@swamid.se

Discovery - några typfall

Typfall 1: Öppen molntjänst

- Alla användare i en stor hög
- Exempel
 - Adobe Connect
 - SUNET mailfilter
- Använd en "vanlig" discovery-tjänst

Typfall 2: SaaS utan kund-till-kund

- Alla kunder har en egen URL
 - kund1.example.com
 - kund2.example.com
- kund1 använder inte resurser från kund2
- Konfigurera IdP för varje kund
- Exempel: DiVA

Typfall 3: SaaS med kund-till-kund

- Alla kunder har en egen URL
 - kund1.example.com
 - kund2.example.com
- kund1 använder resurser från kund2
- Normal identitetsväljare med puff för kundens normala IdP
- Exempel: Box, SUNETs survey-tjänst (?)

Typfall 4: Fattigmans-SSO

- Två eller flera tjänster ska upplevas som en
- Exempel: Portal+LMS, LTI (på förslag)
- Gör discovery vid första inloggning
- Spara entityID för IdPn och använd i länkar till kopplade tjänster

SWAMID Discovery - nu och framtid

- Gårdagens
 - <https://wayf.swamid.se/discovery/WAYF>
 - Funkar bara med SAML1 - **SLUTA ANVÄNDA NU**
- Dagens
 - <https://ds.swamid.se/discovery/DS>
 - Dålig men välkänd användarupplevelse
- Morgondagens (Testa nu!)
 - <https://ds.swamid.se/ds> (inklusive interfederation)
 - <https://ds.swamid.se/swamid>
- Nästa generation (Q2 2013)
 - Google Accountchooser
 - HTML5

Lite Demos

- <https://sites.google.com/site/oidfacwg/cdsdemo>
- <https://sp-test.swamid.se>

Shibboleth...

I shibboleth2.xml

```
<SessionInitiator type="Chaining" Location="/DS" id="DS" relayState="cookie">
  <SessionInitiator type="SAML2" defaultACSIndex="1" acsByIndex="false"
    template="bindingTemplate.html"/>
  <SessionInitiator type="Shib1" defaultACSIndex="5"/>
  <SessionInitiator type="SAMLDS" URL="https://ds.sunet.se/discovery/DS"/>
</SessionInitiator>
```

I din HTML

```
<a href="/Shibboleth.sso/DS?target=/some/login/handler">Login</a>
```

```
<a href="/Shibboleth.sso/DS?entityID=$entityID">Login (fattigmans-SSO)</a>
```