



Shibboleth IdP i Windows

Att installera en Shibboleth Identity Provider i Windows med koppling till Active Directory

<https://wiki.swamid.se/display/SWAMID/Shibboleth-IdP+on+Windows>



Fredrik Åslund

- Anställd på Umeå universitet
 - Systemadministratör NyA-utveckling
 - Systemadministratör Ladok3-utveckling
- SWAMID Operations
 - Metadatanhantering
 - IdP/SP-stöd
 - Policyarbete
- fredrik.aslund@umu.se
- operations@swamid.se

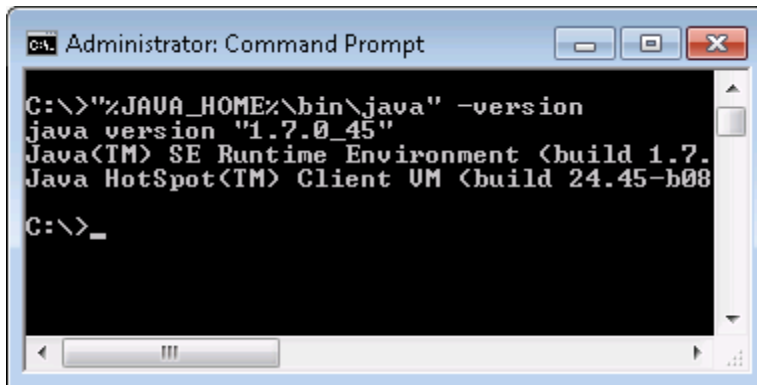


Shibboleth IdP i SWAMID

- 51 IdP:er
 - 45 Shibboleth
 - 29 Linux
 - 9 Windows
 - 7 Okänt operativsystem
 - 4 ADFS
 - 2 SimpleSAMLphp

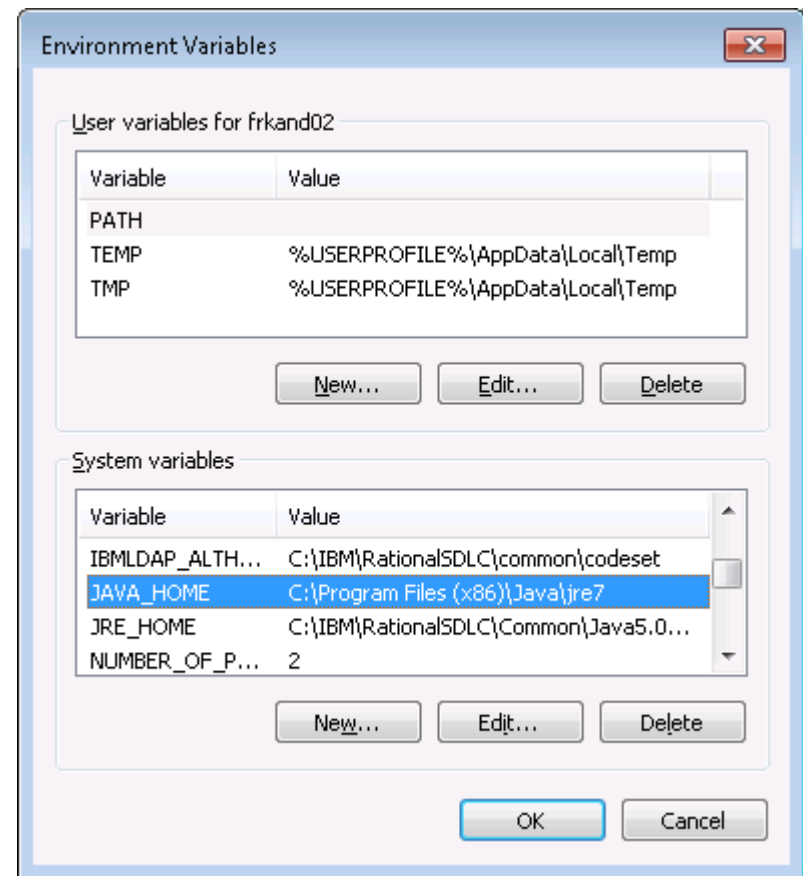
Installera Java

- Installera Java JRE 32-bit
 - www.java.com
- Konfigurera JAVA_HOME



```
C:\> "%JAVA_HOME%\bin\java" -version
java version "1.7.0_45"
Java(TM) SE Runtime Environment (build 1.7.0_45-b08)
Java HotSpot(TM) Client VM (build 24.45-b08)

C:\> _
```



Instalera Shibboleth-IdP

- <http://shibboleth.net/downloads/identity-provider/latest/>
- shibboleth-identityprovider-2.4.0.msi



Installera Shibboleth-IdP

- Konfigurera dns-namn, scope och koppling till LDAP/AD

Shibboleth IdP 2.4.0 IdP Details Setup

The installer for Shibboleth IdP 2.4.0 needs to know various details about this machine, the Active Directory Domain and the scope (Security Domain) that the IdP will assert.

What is the DNS Name of this host ?

Use the default port values unless you are deploying on a machine with a web server already installed

Browser facing port

Shibboleth facing port

What is the name of the Active Directory Domain that this IdP will serve ?

What scope will this IdP assert ?

Wise Installation Wizard...

< Back Next > Cancel

Shibboleth IdP 2.4.0 LDAP Setup

The Shibboleth IdP 2.4.0 installer needs information about the LDAP connection.

The Shibboleth IdP 2.4.0 Installer needs the DNS name or IP Address and also the port number of the Active Directory Server to use. The port number is usually 389, or 3268 for the GC.

Active Directory Server (GC if you have a forest)

Port

The installer also needs a username and password to allow it to query attributes.

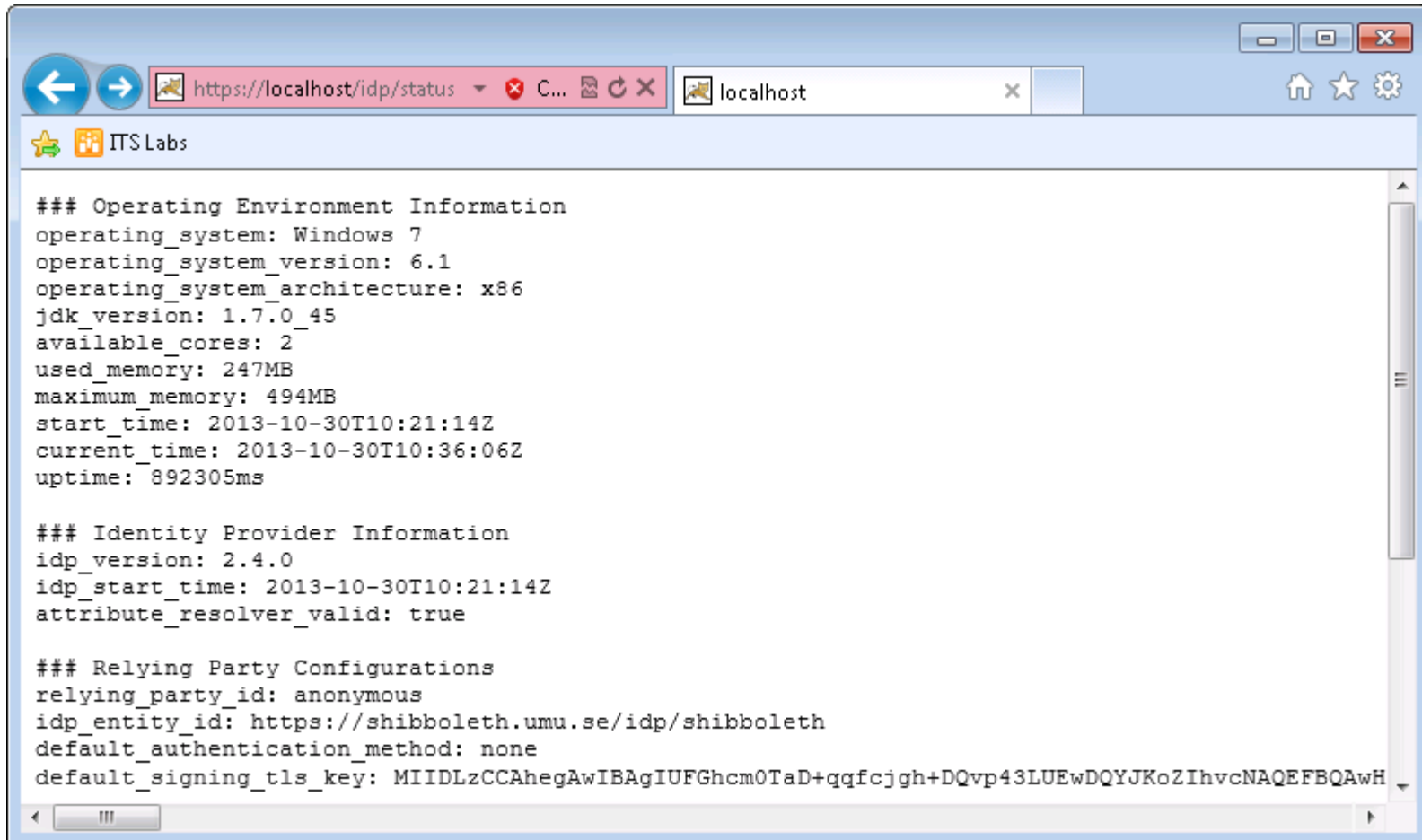
Username (no domain)

Password

Wise Installation Wizard...

< Back Next > Cancel

- Testa status-sidan



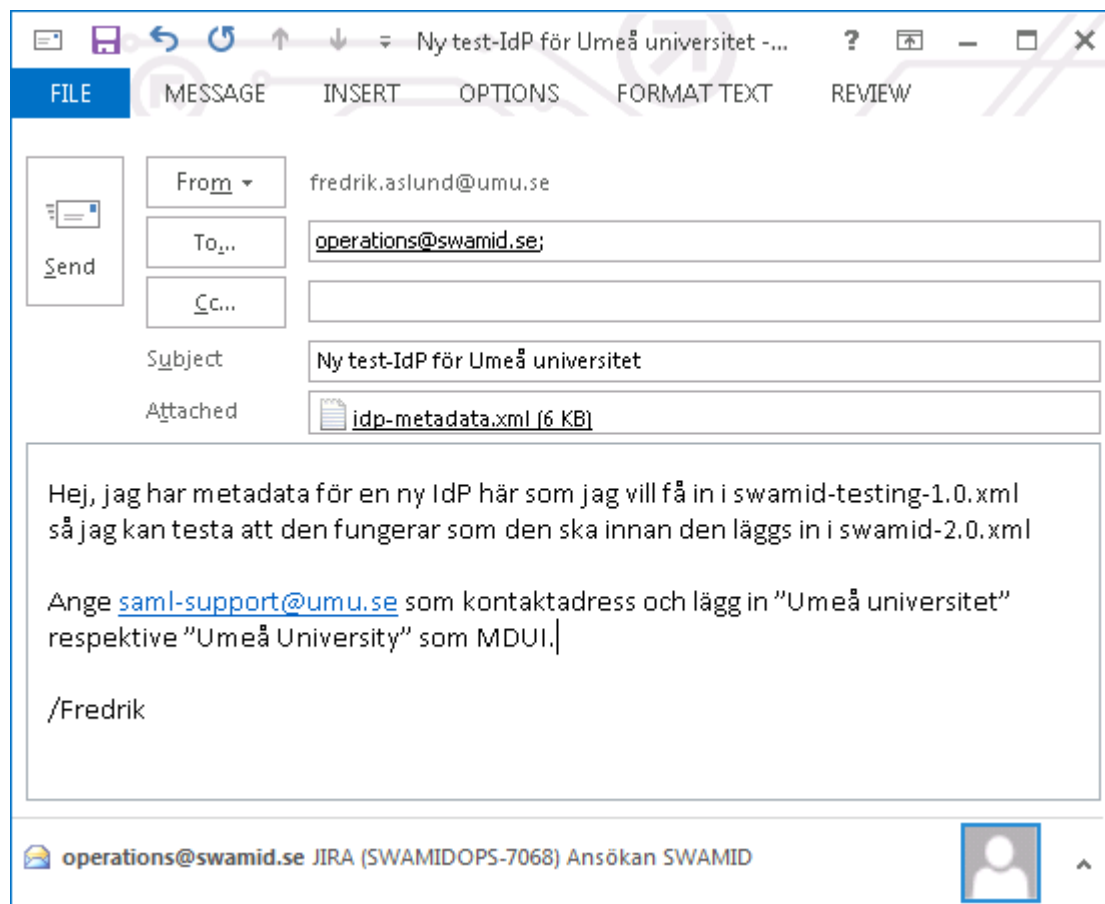
```
### Operating Environment Information
operating_system: Windows 7
operating_system_version: 6.1
operating_system_architecture: x86
jdk_version: 1.7.0_45
available_cores: 2
used_memory: 247MB
maximum_memory: 494MB
start_time: 2013-10-30T10:21:14Z
current_time: 2013-10-30T10:36:06Z
uptime: 892305ms

### Identity Provider Information
idp_version: 2.4.0
idp_start_time: 2013-10-30T10:21:14Z
attribute_resolver_valid: true

### Relying Party Configurations
relying_party_id: anonymous
idp_entity_id: https://shibboleth.umu.se/idp/shibboleth
default_authentication_method: none
default_signing_tls_key: MIIDLzCCAhegAwIBAgIUFGbcm0TaD+qqfcjgh+DQvp43LUEwDQYJKoZIhvcNAQEFBQAwH
```

Installera Shibboleth-IdP

- Skicka metadata till operations@swamid.se





Installera Shibboleth-IdP

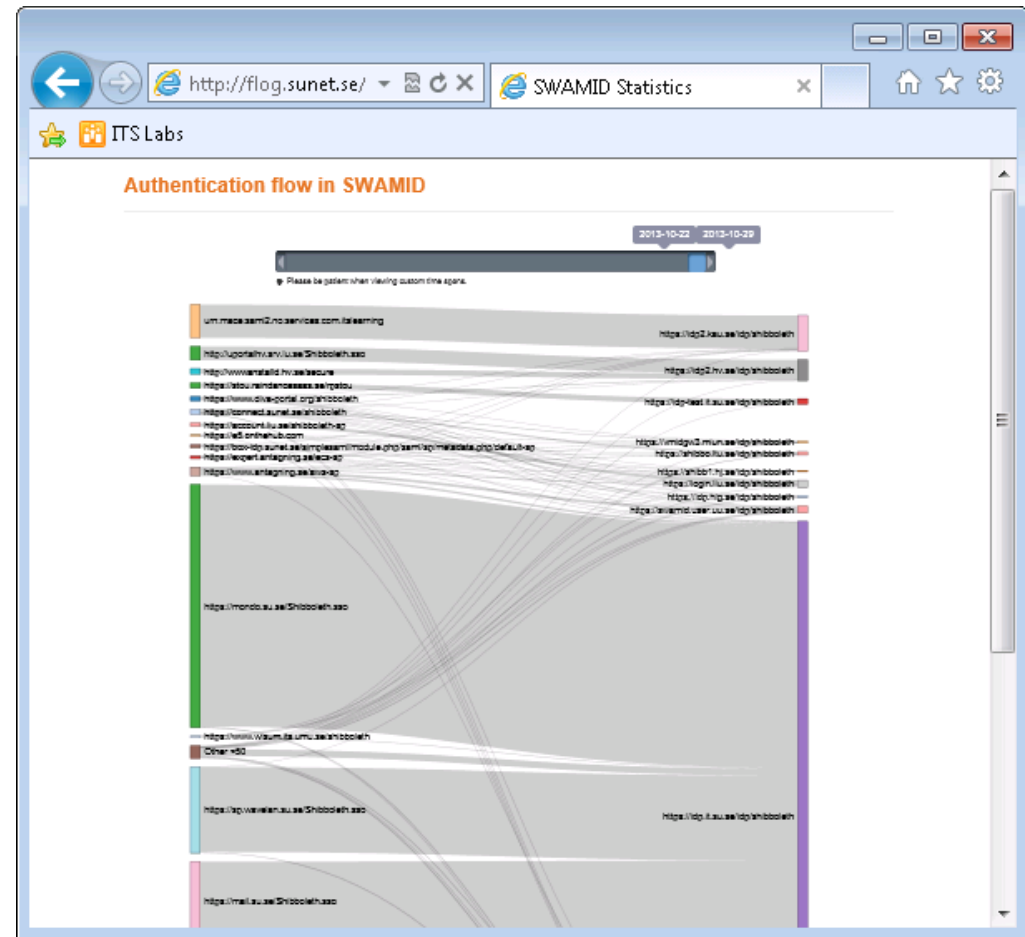
- Konfigurera metadata för att använda SWAMID
 - Hämta ner <http://md.swamid.se/md/md-signer.crt>
 - Verifiera fingerprint via <https://wiki.swamid.se/display/SWAMID/SAML+Metadata+and+Trust>
 - `relying-party.xml`:

```
<!-- SWAMID-METADATA-Trustengine -->
<security:TrustEngine id="swamid-metadata-signer ...">
  <security:Credential ...>
    <security:Certificate>
      C:/Program Files (x86)/Internet2/Shib2Idp/metadata/md-signer.crt
    </security:Certificate>
  </security:Credential>
</security:TrustEngine>

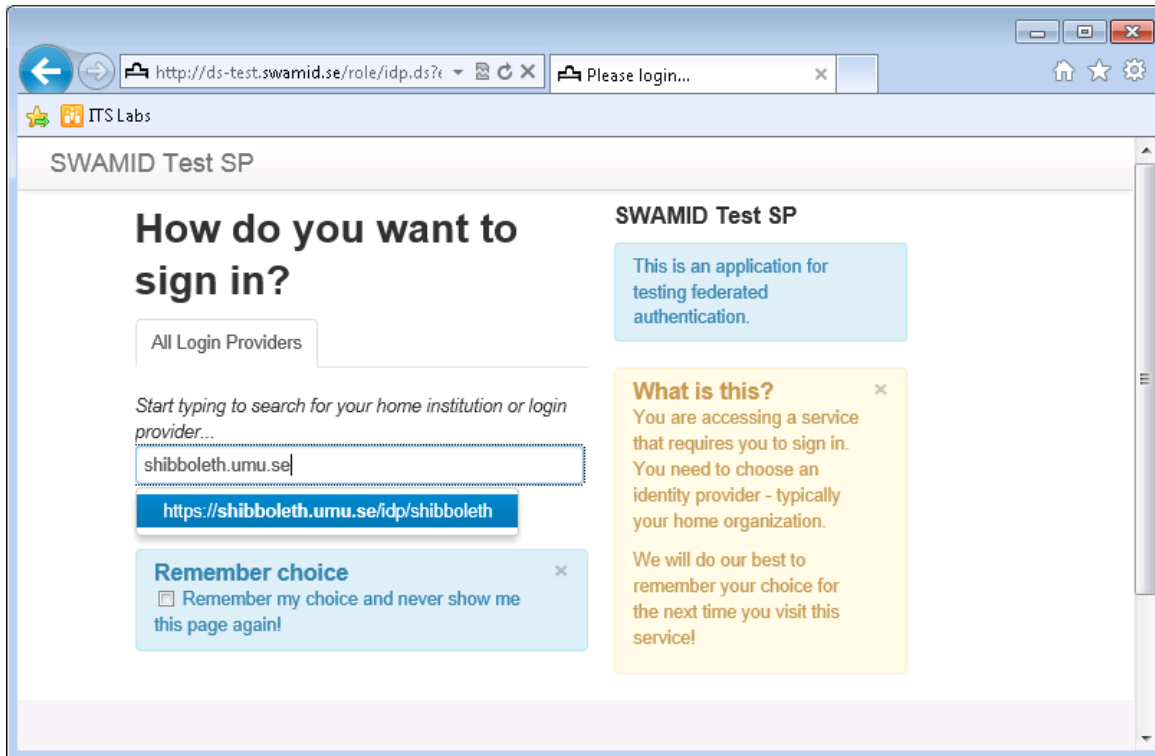
<!-- SWAMID TEST METADATA PROVIDER -->
<MetadataProvider ... metadataURL="http://md.swamid.se/md/swamid-testing-1.0.xml"
  backingFile="C:/Program Files (x86)/Internet2/Shib2Idp/metadata/swamid-testing-1.0.xml">
  <MetadataFilter xsi:type="SignatureValidation" xmlns="urn:mace:shibboleth:2.0:metadata"
    trustEngineRef="swamid-metadata-signer" requireSignedMetadata="true" />
  </MetadataFilter>
</MetadataProvider>
```

- Uppdatera attribute-resolver.xml
 - norEdu* (norEduPerson, norEduPersonOrgUnit, norEduPersonNIN osv)
- Lägg till release av statisk organisationsinformation
 - o (lärosätesnamn), norEduOrgAcronym (lärosäteskod), co (land) osv
- Lägg in attributfilter för entitetskategorier
 - research-and-education
 - code-of-conduct
 - sfs-1993-1153

- Konfigurera f-ticks
 - Hjälper till att generera statistik för användning av IdP:n
 - En anonymiserad loggrad skickas till syslog.swamid.se (IdP, SP, användarhash)
 - Hash av IdP, SP, användarnamn samt bestående randomdata i IdP:n



- <http://sp-test.swamid.se/>
 - Välj ”Logga in via SWAMID Test DS”



SWAMID Test SP

How do you want to sign in?

All Login Providers

Start typing to search for your home institution or login provider...

shibboleth.umu.se

<https://shibboleth.umu.se/idp/shibboleth>

Remember choice

Remember my choice and never show me this page again!

SWAMID Test SP

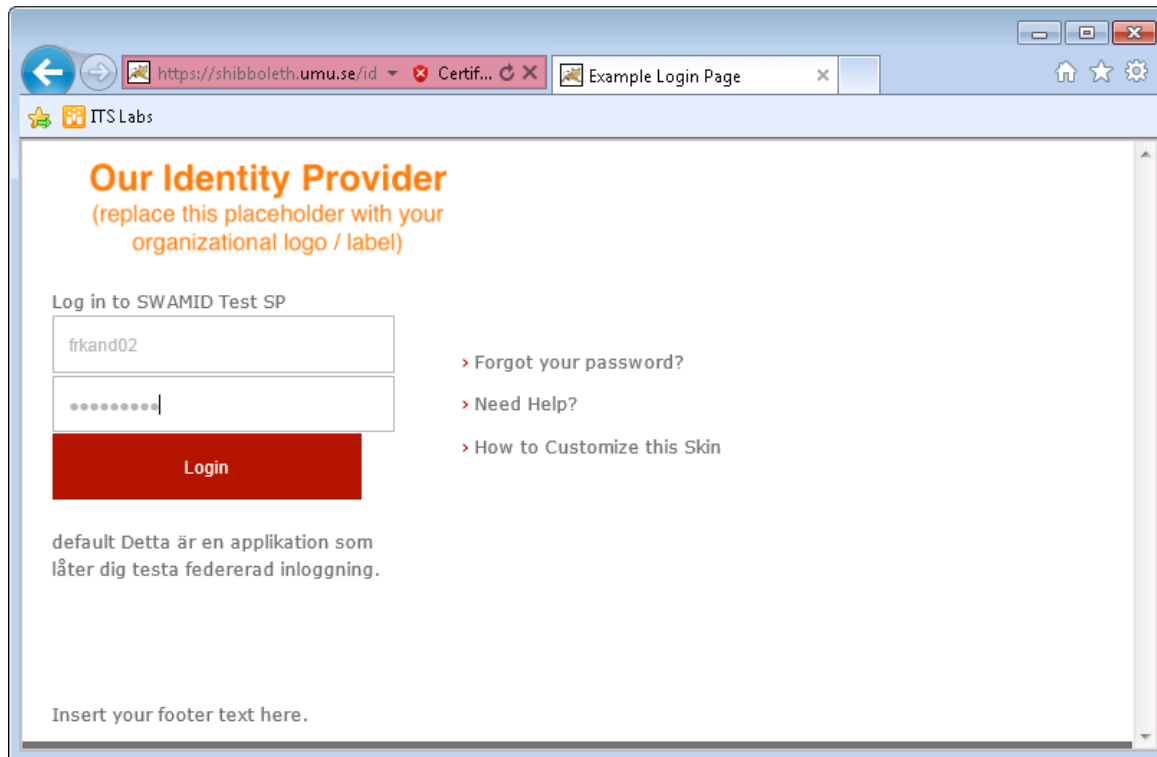
This is an application for testing federated authentication.

What is this?

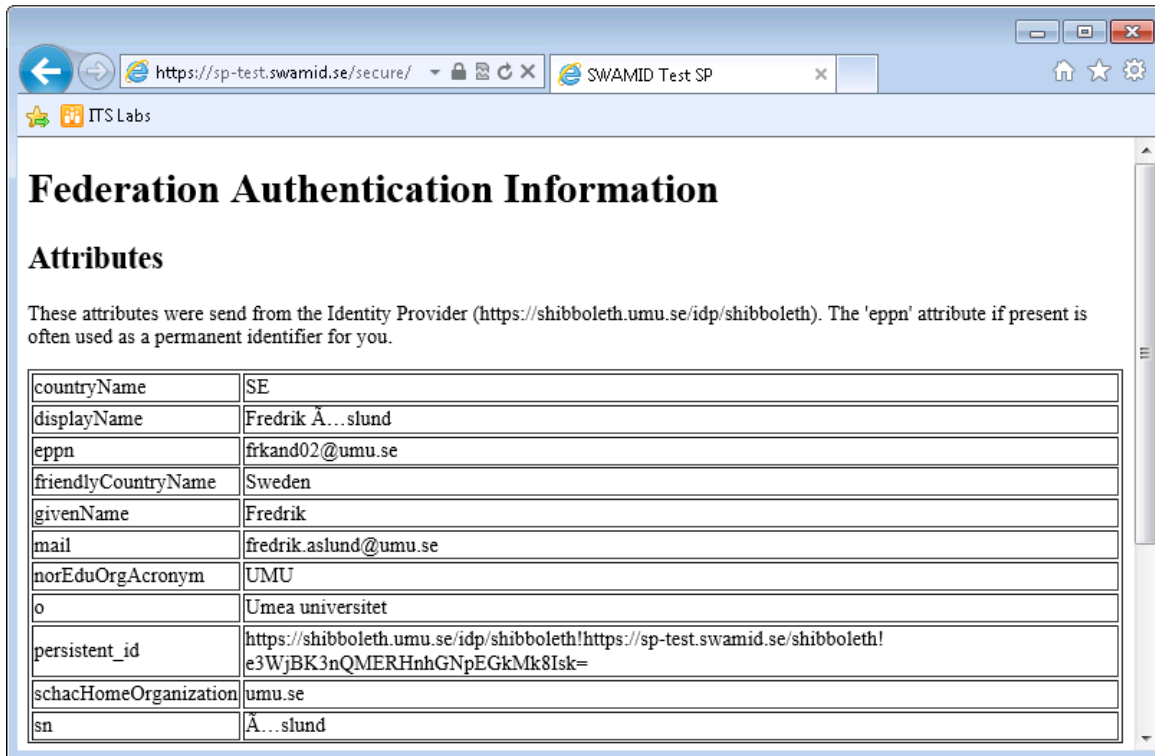
You are accessing a service that requires you to sign in. You need to choose an identity provider - typically your home organization.

We will do our best to remember your choice for the next time you visit this service!

- Logga in med användarkonto i AD/LDAP



- sp-test.swamid.se listar mottagna attribut



The screenshot shows a web browser window with the address bar displaying `https://sp-test.swamid.se/secure/`. The page title is "SWAMID Test SP". The main content area is titled "Federation Authentication Information" and "Attributes". Below the title, there is a paragraph explaining that these attributes were sent from the Identity Provider (`https://shibboleth.umu.se/idp/shibboleth`). The 'eppn' attribute is noted as often used as a permanent identifier. A table lists the following attributes:

countryName	SE
displayName	Fredrik Å...slund
eppn	frkand02@umu.se
friendlyCountryName	Sweden
givenName	Fredrik
mail	fredrik.aslund@umu.se
norEduOrgAcronym	UMU
o	Umea universitet
persistent_id	<code>https://shibboleth.umu.se/idp/shibboleth!https://sp-test.swamid.se/shibboleth! e3WjBK3nQMERHnhGNpEGkMk8Isk=</code>
schacHomeOrganization	umu.se
sn	Å...slund



Anpassa inloggningssida

- Anpassa inloggningssidan
 - `C:\Program Files (x86)\Internet2\Shib2IdPInstall\src\main\webapp\login.jsp`
- Ladda om webbappen
 - `C:\Program Files (x86)\Internet2\Shib2IdPInstall\install.bat`
- Starta om tomcat
 - Kontrollpanelen - Administrative Tools - Services - tomcat6



Till sist...

- Frågor?
 - Fråga oss nu...
 - Skicka epost till SWAMID Operations eller
 - ring någon i SWAMID Operations och fråga!
- Mer information på SWAMIDs Wiki:
 - <https://wiki.swamid.se/display/SWAMID/Shibboleth-IdP+on+Windows>



Nästa SWAMID-workshop

- SWAMID-workshop 10-11 december
- Göteborg eller Stockholm
- Agenda inom de närmaste dagarna
- saml-admins@swamid.se