SWAMID WebSSO FAQ

Hur får jag in min IdP i listan på swamid.se?

Listan på IdP:er/organisationer på md.nordu.net utgörs av de organisationer som är medlemmar i SWAMID samt organisationer som SWAMID har avtal med. För att synas måste förutom medlemskap krävs det att organisationen har skickat information om sin IdP till operations@swamid.se. Inkludera namnet på IdP:n (tex https://idp.example.com/identity) samt det certifikat som används för att skydda attribut-release, vanligen specat i idp.xml. Om din organisation inte är medlem i SWAMID finns information om hur ni blir det på http://www.swamid.se/11/policy/swamid-2.0.html.

Kan man inte använda CAS eller någon annan Enterprise SSO istället?

Jovisst men då tappar man möjligheten att kommunicera mellan organisationer. Dessa teknologier har sin plats som SSO-lösningar inom en organisation och fungerar bra som login-lösningar för shibboleth men om man vill skicka attribut mellan organisationer eller undvika att göra sin applikation beroende av någon specifik användardatabas (tex LDAP) så är en SAML-baserad identitetsfederation enda praktiska alternativet idag.

Behövs en SSO-lösning ändå?

Nej. Shibboleth kan fungera som SSO-lösning inom en organisation helt enkelt genom att man sätter upp en intern federation. Det finns verktyg på https://wiki.shibboleth.net/confluence/display/SHIB/Contributions som underlättar arbetet med att sätta upp en lokal federation. Om man har en existerande SSO-lösning (tex CAS) så duger den gott som inloggnings-bakända för shibboleth.

Vad är det för skillnad mellan SAML, OAuth och OpenID?

- SAML - protokollet som bär information om användare och attribut inom en federation.
- OAuth - ett protokoll för delegering av behörigheter mellan applikationer.
- OpenID - Används för att autenticera slutanvändare, dvs kan ses som en "personlig" IdP.
- OpenID Connect - Nästa generations protocol, ibland kallat "SAML 3".

Hur sätter jag upp en intern federation?

En federation är i princip bara en metadatafil som hålls synkroniserad mellan alla medlemmar. Skapa och underhåll en metadatafil och sätt upp en discovery-tjänst någonstans så är du igång. Det är rekommenderat att lagra certifikat i metadatafilen (jämför hur swamids metadata ser ut) istället för externt eftersom man då undviker många problem med certifikatvalidering.

Hur kommer jag enklast igång?

Börja med att skaffa dig en identitet på ProtectNetwork - där får du en gratisinloggning som fungerar på de test och demo-tjänster som finns i SWAMID idag. Det ger dig möjlighet att börjat prova shibboleth. På testshib.org finns det också bra verktyg för att testa själva installationen.

Hur testar jag om min identitet fungerar?

Välj till någon av demotjänsterna, förslagsvis https://sp.swamid.se eller https://sp-test.swamid.se. Om allt fungerar så ska du åtminstone se din identitet i eppn-fältet. Beroende på vilka attribut som din IdP släpper ut så ser du även andra fält.

Vad betyder 'scope'?

Scope är ett shibboleth-begrepp som betyder 'administrativ domän'. Vissa attribut som skickas från en IdP till en SP har ett scope som anger vilken domän/organisation som utfärdat värdet. Ett exempel på användningen av scope är attributet eduPersonPrincipalName som ofta mappas till användaridentiteter i IdP:n. För att det inte ska bli kollision mellan identiteter mellan olika organisationer används scoping. I SAML representeras scope som ett attribut på <AttributeValue/>-element men scope visas ofta med @-notation som tex nissehult@example.com - där example.com är scope. I detta exempel är nissehult användarnamnet på en användare från en IdP som har scope example.com (kanske heter idp:n https://idp.example.com/identity men det är långt ifrån säkert).

När en SP tar emot attribut med scope så kan SP:n filtrera baserat på scope (tex för att bara tillåta användare från organisationer SP:n har kontrakt med). Exempelvis kan ett SAML-response för nissehult innehålla följande (exemplet är baserat på SAML1 men för SAML2 ser det ungefär likadant ut):

```
<Attribute AttributeName="urn:mace:dir:attribute-def:
eduPersonPrincipalName" AttributeNamespace="urn:mace:shibboleth:1.0:
attributeNamespace:uri">
<AttributeValue Scope="example.com">nissehult</AttributeValue>
</Attribute>
```

Kan en SP/IdP vara medlem i mer än en federation?

Tekniskt är en federation bara en metadatafil som hålls synkroniserad mellan alla entiteter (SP och IdP) som ingår i federationen. Både SP:n och IdP:n stödjer att man pekar ut flera olika metadatafiler.

Hur väljer jag vilka attribut som skickas?

Detta styrs genom sk "attribute release policy". I default-installationen av shibboleth 1.x finns det i filen idp.xml ett <ReleasePolicyEngine>-element som innehåller konfiguration av en fil-baserad attribute-policy-motor. Denna använder xml-filer som lagras på IdP:n. Filen site.arp.xml innehåller inställningar som gäller för alla användare. Dessutom kan man ha filer för individuella användare. I normalfallet så är det SP:n och IdP:n som kommer överens om vilka attribut som ska skickas men det kan vara intressant att låta användaren få kontroll över vissa detaljer. Vill man låta sin användare få kontroll över attributen finns det verktyg på https://spaces.internet2.edu/display/SHIB/Contributions som kan vara intressanta.

Hur använder jag attribut från en IdP?

Attribut från IdP:n exponeras i SP:n som HTTP request headers. I java (tex) kan man komma åt dom med HttpServletRequest#getHeader. Namnet på headern styrs av SP-konfigurationsfilen AAP.xml. Ett specialfall är eduPersonPrincipalName som normalt exponeras som REMOTE_USER (dvs HttpServletRequest#getRemoteUser i java).

Hur kollar jag om någon är inloggad?

Genom att kolla om REMOTE_USER inte är tomt. Detta beror på om eduPersonPrincipalName skickas från IdP. Om inte så kan man titta på headern SHIB_IDENTITY_PROVIDER som innehåller identifieraren för den IdP som användaren loggat in på.

Hur initierar jag en inloggning från min applikation?

Normalt sker detta genom att användaren följer en länk som triggar en sk session initiator. Sådana styrs av <SessionInitiator>-element i shibboleth.xml. Varje SI pekar antingen ut en IdP direkt eller en WAYF-tjänst (för någon federation). Det är vanligt att man lägger ut minst 2 SI-länkar: en för den "lokala" IdP:n (tex skolans egna) och en till WAYF:en för federationen.

Det står ';'-tecken i attributvärden! Vad betyder detta?

Attributet är flervärt. Värden separeras med ';'.

Vilka certifikat behövs?

Certifikat används på två ställen: dels för att skydda kommunikationen mellan användaren och IdP:n (resp SP:n) och dels för att skydda transporten av attribut mellan IdP:n och SP:n. För skydd av kommunikation mellan användaren och webbapplikationerna som vänder sig till användare (tex IdP:ns inloggningsdel eller en webapplikation som använder shibboleth för authenticering) kan man använda vilket certifikat som helst. Det finns ingen policy som styr valet - swupki eller kommerciella certifikat går lika bra.

För kommunikationen mellan IdP och SP används i SWAMID certifikat som publiceras i metadata för federationen. Dessa kan vara självsignerade eller vanliga certifikat men valideringen av dessa certifikat sker genom att de jämförs med certifikatet i metadata och inte baserat på hela kedjan upp till ett trustankare. Det betyder att man kan använda vilket certifikat som helst, även det vanliga tls certifikatet

Varför ska jag bry mig om Kalmar Unionen?

Kalmar Unionen är en samverkan mellan de nordiska ländernas forsknings-federationer. SWAMID ingår i Kalmar Unionen. Via Kalmar Unionen går det att publicera och komma åt tjänster mellan de nordiska länderna.

Varför ska jag bry mig om eduGAIN?

eduGAIN är liknande Kalmar Unionen en samverkan mellan de primärt de Europeiska ländernas forsknings-federationer. SWAMID ingår i eduGAIN.