Pseudonym identifierare

Detta är en guide för hur man sätter upp sk pseudonya identifierare för Shibboleth IdP:n. Instruktionerna är baserade på en Ubuntu eller debian-baserad Linux men motsvarande bör funka även på andra unix-varianter och Windows. Instruktionerna är baserade på https://www.switch.ch/aai/docs/shibboleth/SWITCH/2.1/idp/install-idp-2.1-debian.html#shibboleth-idp och https://spaces.internet2.edu/display/SHIB2/IdPPersistentNameIdentifier.

En pseudonym identifierare är en permanent, anonym identifierare som är unik för en kombination av IdP, SP och användare. En sådan identfierare kan inte användas för att korrelera information mellan SPer och innehåller heller inte någon persondata. En pseudonym identifierare är oftast lämplig att lämna ut till alla SPer.

> SWAMID rekommenderar att alla IdPer lämnar ut pseudonymer som SAML 2.0 NameID samt som attribut av typen eduPersonTargetedID till alla SPer.
> Instruktionerna nedan åstadkommer precis detta.

Det finns två sätt att skapa pseudonyma identiferare: antingen genom att beräkna en hash-funktion över ett antal ingångsvärden (bla användarens lokala användarnamn, SPns entityID och en unik nyckel) eller genom att lagra en sk UUID i en databas. Båda alternativen har för och nackdelar:

- Beräknade identifierare
  - är mycket enkelt att komma igång med.
  - kan inte hantera att en SP eller IdP byter entityID
  - kan inte hantera att en användare byter uid (sAMAccountName)
  - är deprekerade i shibboleth och kan vara svårt att få att fungera i en modern version
- Lagrade identifiera
  - kräver en databas på IdPn
  - stödjer revokering av identifierare
  - kan hantera att en SP eller IdP byter entityID
  - kan hantera att användare byter uid (sAMAccountName)

Det finns vissa möjligheter att börja med en beräknad identifierare och sedan migrera till en lagrad men eftersom shibboleth numera i princip inte längre stödjer beräknade identifierare är valet ganska enkelt. Vi rekommenderar att man i det enklaste fallet med en IdP som inte ingår i ett kluster kör en mysqld på samma server som kör IdPn så att man inte introducerar ytterligare beroenden. Se dock till att denna mysqld inte är öppen för världen för att undvika evt säkerhetsproblem.

- Beräknad pseudonym identifierare
- Lagrad pseudonym identifierare (**rekommenderad**)