SWAMID Workshop 3 2017 - Hur blir min organisation godkänd för SWAMID AL1 eller SWAMID AL2?

I identitetsfederationen SWAMID är tillit till att universitet, högskolor hanterar användare och inloggningar tillräckligt bra grunden för att tjänsteleverantörer ska lita på att det är rätt användare som loggar in. Inom SWAMID använder vi oss av tillitsprofiler för att påvisa vilken tillit en tjänsteleverantör kan ha när det gäller att det är rätt person som loggar in i tjänsten. Inom federation finns två tillitsprofiler: SWAMID AL1 för obekräftade användare där uppgifter om användaren kan vara självuppgivna och okontrollerade och SWAMID AL2 där uppgifter om användaren är kontrollerade av användarens hemorganisation.

För att en medlemsorganisation ska kunna signalera en viss tillitsprofil för en användare vid inloggning i en tjänst måste medlemsorganisationen först se till att vara godkänd för minst en av tillitsprofilerna. Medlemsorganisationen måste skriva en tillitsdeklaration (en. Identity Management Practice Statement, förkortat IMPS), för att visa att medlemsorganisationen uppfyller kraven i aktuell tillitsprofil. Denna ska därefter skickas in till SWAMID Operations för granskning och godkännande.

Vi vill därför bjuda in till en workshop där vi som arbetar i SWAMID Operations kan hjälpa er i ert arbeta att skriva en tillitsdeklaration. Vi går igenom och presenterar best practice både ur perspektivet hur man bör tänka vad gäller processer och teknik men även hur man bör dokumentera detta. Vi kan också dela med oss om bra tips på tillvägagångssätt i de fall man behöver justera befintliga identitetslösningar för att uppfylla kraven.

Vi vill också passa på att för tydlighetens skull påminna om att alla användare i medlemsorganisationen inte behöver uppfylla samma tillitsprofil så länge som aktuell nivå kan säkerställas med attributrelease. Detta betyder i praktiken att att alla användare behöver inte uppfylla kraven för SWAMID AL2 även om medlemsorganisationen som sådan är betrodd på denna nivå. Det är fullständigt naturligt att vissa användare som kan använda federativ inloggning genom SWAMID bara uppfyller kraven för SWAMID AL1. Dessa användare kommer då ej att kunna använda tjänster som kräver SWAMID AL2 men kommer kunna använda övriga tjänster (t.ex. eduroam, e-mötestjänster och bibliotekstjänster).

Som en förberedelse inför workshopen rekommenderar vi följande:

- Leta upp länkar eller dokument till organisationens:
  - användarregler,
  - lösenordspolicy,
  - tjänstedefinition för identitetsutgivaren (IdP) eller användarhanteringssystem (IAM) och
  - policy för hantering av personuppgifter för identitetsutgivaren (IdP).
- Gå igenom mallen för IMPS och sammanställ den information som lärosätet har i driftdokumentation, policydokument osv.
  - IMPS-mallen finns under rubriken "Mallar för bästa praxis" på wikisidan SWAMID Identity Assurance.
- Glöm inte att prata med dina kollegor om det finns några frågor du är osäker på.

Om du är osäker om din organisations status när det gäller SWAMIDs tillitsprofiler finns aktuell status på webbsidan över alla medlemsorganisationer i SWAMID, https://www.sunet.se/swamid/medlemmar/.

Syfte	Att deltagarna under dagen har skrivit en tillitsdeklaration och tagit fram en plan för vilka förändringar kring processer och teknik i befintliga identitetslösningar som krävs för att uppnå resp. tillitsnivå
Målgrupp	Process- och teknikansvariga för identitetshanteringstjänsten i resp. medlemsorganisation.
Datum & tid	Onsdagen den 13 december 9.00--16.00
Plats	Sunets kontor på Tulegatan 11 i Stockholm
Anmälan	Anmälan sker, samordnat inom medlemsorganisationen, med e-post till operations@swamid.se.
Deltagarbegränsning	För att arbetet ska bli så effektivt som möjligt är antalet deltagare på workshopen är begränsat till 2-4 medlemsorganisationer med totalt max 10 personer i rummet.

Material:

- Presentation som används under workshopen: SWAMID WS 2016 - Att skriva IMPS.pdf