SWAMID

Är alla användaridentiteter lika värda?

Några termer vi använder ofta

- Vad är en **användare**?
  - Det är en person, en mängd personer eller en sak (dator, skrivare eller något annat)
- Vad är en **användaridentitet**?
  - Det är något som unikt identifierar en användare i ett eller flera system
- Vad är en **federerad användare**?
  - Det är en användare som kan använda användar-identitet vid egen organisation för att komma åt tjänster i eller utanför sin egen organisation

Introduktion till förtroendenivå

- I en identitetsfederation som SWAMID är tillit eller förtroende det viktigaste!
- Hur vet jag att identitetsutfärdarna (universiteten och högskolorna) och federationen (SWAMID) hanterar användare och tekniska system på ett bra och korrekt sätt efter mina behov som tjänsteleverantör?
- Svaret är förtroendenivåer!

Definition av förtroendenivå

- Förtroendenivå är ett tal mellan 1 och 4, där 4 är bäst, som beskriver hur mycket vi kan lita på att en användare är den han/hon utger sig för att vara

- Förtroendenivå heter på engelska
  - Level of Assurance (LoA) alt.
  - Assurance Level (AL)

Bedömning av förtroendenivå

- Förtroendenivån för en användare bedöms på
  - användaridentitetens livscykel,
  - inloggningstoken (t.ex. användarid och lösenord och smart card),
  - hur inloggningstoken skapas och administreras,
  - vilka protokoll som används vid inloggningen och
  - hur resultatet av inloggningen inkl. attribut överförs till tjänsten
- Varje område får en förtroendenivå och minsta nivån är den sammanvägda

SWAMID och förtroendenivåer

- I SWAMID 2.0 finns idag endast en basnivå (Basic Identity Assurance Profile v1.0) som inte går att koppla till en definierad förtroendenivå.
- Lärosätena deklarerar idag genom ett Identity Management Practice Statement vid ansökan till SWAMID 2.0 hur de hanterar användar-identitetens livscykel med en egen bedömning av LoA-nivå. (http://wiki.swamid.se/pages/viewpage.action?pageId=31201529)

SWAMID och förtroendenivåer

- Arbete pågår för att i SWAMID skapa
  - Identity Assurance Level 1 Profile (AL1) och
  - Identity Assurance Level 2 Profile (AL2)
- Dessa bägge nya profiler kommer på sikt att ersätta dagens Basic Identity Assurance Profile
- Förberedelsearbetet inkl. införandebeslut av SWAMID Bord of Trustees beräknas vara klart under våren 2013.
- Teknisk implementation påbörjas hösten 2013

Enkla exempel

- Användare på Google, Microsoft (Windows Live) eller Facebook motsvarar LoA1
- Svensk e-legitimation i nuvarande form är ungefär LoA3
- Obekräftad användare i NyA är ungefär LoA1 (webbregistrering)
- Bekräftad användare i NyA är ungefär LoA2 (aktiveringskod skickad till folkbokföringsadress efter webbregistrering)

Andra inloggningsmöjligheter

- Ibland vill man ge externa användare som inte finns i den svenska universitetets och högskole-sektorn tillgång till något av våra system.
  - Om systemet kräver hög förtroendenivå och inloggningar får kosta pengar använd Svensk E-legitimation 2.0
  - Om användarna finns bland europeiska lärosäten anslut till eduGAIN via SWAMID
  - Om användarna finns i den svenska skolsektorn anslut tjänsten även Skolfederationen
  - Om låg förtroendenivå behövs använd Google, Windows Live och Facebook (mer i eftermiddag)

Byta från lokal inloggning/CAS till SAML2

- Inloggning via SAML2 är ofta svårare att införa än inloggning mot lokala konton eller CAS.
- CAS kräver antingen en färdig modul eller att man inkluderar 10-20 rader kod.
- SAML2 kräver en särskild modul samt registrering i federations metadata.
  - Befintlig applikation behöver ofta även anpassas för att klara inloggningar från olika identitetsutgivare.
- Det kan vara bra att ha en CAS-proxy, dvs CAS använder SAML2 IdP för inloggningen.