SWAMID Assurance How-To

The formal SWAMID Policy is available at SWAMID Policy in the wiki, linked in the assurance profile headers below.



Information under this section is in Swedish due to that SWAMID Identity Providers are institutions of the Swedish Higher Educational Sector.

I identitetsfederationen SWAMID är tillit till att universitet, högskolor och andra organisationer hanterar användare och inloggningar tillräckligt bra grunden för att tjänsteleverantörer ska lita på att det är rätt användare som loggar in. För att definiera vad som är tillräckligt bra i SWAMID finns tre tillitsprofiler, SWAMID AL1, SWAMID AL2 och SWAMID AL3.

- SWAMID Identity Assurance Level 1 Profile (SWAMID AL1)
- SWAMID Identity Assurance Level 2 Profile (SWAMID AL2)
- SWAMID Identity Assurance Level 3 Profile (SWAMID AL3)
- SWAMID AL1, SWAMID AL2 eller SWAMID AL3?
- Ansöka om att bli godkänd för tillitsprofil inom SWAMID
    - Mallar för bästa praxis
- Att signalera tillitsprofilerna vid attributrelease

SWAMID Identity Assurance Level 1 Profile (SWAMID AL1)

Tillitsprofilen SWAMID AL1 innebär tre saker:

1. Att det är en person som innehar och använder kontot, detta kallas även för ***obekräftad användare***.
2. Informationen knuten till kontot är oftast uppgiven av och ansvaras för av användaren själv.
3. Lärosätets identitetshanteringssystem uppfyller minst kraven i SWAMID AL1.

För att en medlem ska bli godkänd som identitetsutfärdare för tillitsprofilen SWAMID AL1 krävs en tillitsdeklaration genom Identity Management Practice Statement (IMPS) tillsammans med tillgång till eventuella dokument som hänvisats till. SWAMID kontrollerar undertecknad SWAMID AL1 check list (finns på länk i rubriken) tillsammans med tillitsdeklarationen innan godkännande.

SWAMID Identity Assurance Level 2 Profile (SWAMID AL2)

Tillitsprofilen SWAMID AL2 innebär tre saker:

1. Utökning av SWAMID AL1.
2. Ställer högre krav på att lärosätet vet vem personen är som innehar och använder kontot, detta kallas även för ***bekräftad användare***.
3. Lärosätet ansvarar för personinformationen till skillnad från i SWAMID AL1.

För att en medlem ska bli godkänd som identitetsutfärdare för tillitsprofilen SWAMID AL2 krävs en tillitsdeklaration genom Identity Management Practice Statement (IMPS) tillsammans med tillgång till eventuella dokument som hänvisats till. SWAMID genomför en granskning av tillitsdeklarationen innan godkännande.

SWAMID Identity Assurance Level 3 Profile (SWAMID AL3)

Tillitsprofilen SWAMID AL3 innebär tre saker:

1. Utökning av SWAMID AL2.
2. Ställer högre krav på att lärosätet vet vem personen är som innehar och använder kontot, detta kallas även för ***verifierad användare***.
3. Inloggning måste alltid ske med multifaktor.

För att en medlem ska bli godkänd som identitetsutfärdare för tillitsprofilen SWAMID AL3 krävs en tillitsdeklaration genom Identity Management Practice Statement (IMPS) tillsammans med tillgång till eventuella dokument som hänvisats till. SWAMID genomför en utökad granskning av tillitsdeklarationen innan godkännande.

SWAMID AL1, SWAMID AL2 eller SWAMID AL3?

De flesta tjänster har bara behov av tillitsprofil SWAMID AL1 men vissa verksam-hetskritiska tjänster kräver för all, eller viss, användning att användaren är en bekräftad användare, dvs. tillitsprofil SWAMID AL2. En god rekommendation är att system som ger användaren tillgång till personuppgifter om användaren själv eller om andra personer bör kräva konton som minst uppfyller SWAMID AL2. För system med känsliga personuppgifter, annan känsliga data eller där myndighetsbeslut genomförs rekommenderas att SWAMID AL3 används för att säkerställa att det är rätt användare som har tillgång.

Alla användare vid ett lärosäte behöver inte uppfylla samma tillitsprofil så länge som inloggningstjänsten via s.k. attributrelease kan signalera till aktuell tjänst vilken tillitsprofil som användaren har. Ett lärosäte kan bli godkänt för att intyga att enskilda användare uppfyller:

- SWAMID AL1, SWAMID AL2 och SWAMID AL3,
- SWAMID AL1 och SWAMID AL2 eller
- endast SWAMID AL1.

Ansöka om att bli godkänd för tillitsprofil inom SWAMID

För att en medlemsorganisation ska bli godkänd att signalera en viss tillitsprofil för en användare vid inloggning i tjänst måste medlemmen först se till att organisationen blir godkänd för aktuell, eller högre, tillitsprofil. För att bli godkänd måste medlemmen skriva en tillitsdeklaration, en. Identity Management Practice Statement, för att visa att medlemsorganisationen uppfyller kraven i aktuell tillitsprofil. Observera att alla användare i medlemsorganisationen inte behöver uppfylla aktuell tillitsprofil så länge som aktuell nivå kan säkerställas med attributrelease.

Mallar för bästa praxis

- SWAMID template Identity Management Practice Statement (IMPS) - v2.0
- SWAMID template Acceptable Use Policy
- SWAMID template Password Policy
- SWAMID template Kontroll av legitimationshandling
- SWAMID template Service Definition
- SWAMID template Identity Provider Privacy Policy

Att signalera tillitsprofilerna vid attributrelease

Identitetsutfärdare registrerade i SWAMID förväntas informera tjänster om vilken eller vilka tillitsprofiler som användaren är godkänd för i samband med inloggning om detta begärs via entitetskategorier. Alla identitetsutfärdares registrerade i SWAMID har markering i metadata om vilka tilltisprofiler de uppfyller. Internationellt används REFEDS Assurance Framework (RAF), se Release of assurance statements in the attribute eduPersonAssurance based on SWAMID Identity Profiles för mappning av SWAMIDs tillitsprofiler till REFEDS Assurance Framework.