

SWAMID BoT 2021-03-11

Agenda för SWAMID BoT 2021-03-11 10.00

Plats: Videomöte, Zoom

Agenda

Välkommen (VN)

Fastställande av dagordning (VN)

Beslut om extra rutin för verifiering av användare på AL2-nivå (PA)

Beslut om ansökningar om godkännande av tillitsnivåer (PA)

Beslut om deltagande i interfederationen FIDUS (PA)

Information om det pågående policyarbetet (PA)

Information om det pågående arbetet med att byta modell attributrelease i SWAMID (PA)

Diskussion om information riktad till IT-chef/motsv om SWAMID (VN)

Övriga frågor (VN)

Nästa möte (VN)

Avslutande (VN)

Protokoll

Plats

Videomöte i Zoom

Närvarande

- Valter Nordh (VN)
- Mauritz Danielsson
- Magnus Höglund
- Jan Nordin
- Per Zettervall
- Ann Amling
- Per-Olov Hammargren
- Sverker Holmgren
- Hans Wohlfart

Frånvarande

Adjungerade

- Pål Axelsson (PA)

Välkommen (VN)

Valter öppnar mötet och hälsar alla välkomna.

Fastställande av dagordning (VN)

Dagordningfastställs.

Beslut om extra rutin för verifiering av användare på AL2-nivå (PA)

Rutin för identifiering via videosamtal

Bakgrund

Det har länge funnits önskemål ifrån SWAMIDs medlemmar att skapa en rutin som möjliggör att kunna identifiera användare som ej fysiskt befinner sig på plats i organisationens lokaler. Under 2020 inträffade en pandemi vilket har aktualiserat behovet. SWAMID Operations har därför tagit fram ett förslag för godkännande av SWAMID Board of Trustees för vad som skulle kunna vara en rimlig nivå för identifiering som uppfyller avsnitt 5.2.5, punkt 8 för SWAMID Identity Assurance Level 2 Profile (SWAMID AL2) för att möjliggöra kontoaktivering på distans. Observera att denna rutin inte är lämplig att använda för studenter!

Definitioner

Kontoadministratör - Administratör hos medlemsorganisationen som har teknisk tillgång till att administrera konton i medlemsorganisationens identitets- och behörighetssystem, antingen via tekniska gränssnitt alternativt via en speciellt avsedd applikation för detta. Kontoadministratören ska ha möjligheten att autentisera sig enligt SWAMID AL2.

Betrodd part - Anställd medarbetare hos medlemsorganisationen med möjlighet att autentisera sig enligt SWAMID AL2.

Kontoinnehavare - Fysisk person (benämnd Subject enligt tillitsprofilen) som ska få eller har fått ett konto hos medlemsorganisation och ska identifieras.

Krav på rutin

1. Själva identifieringen ska ske via ett treparts videosamtal med kontoadministratör, betrodd part samt kontoinnehavare närvarande.
2. Organisationen måste ha rutiner på plats, t.ex. via arbetsordningen, för att minimera kontoadministratörens eventuella beroendeställning gentemot betrodd part och kontoinnehavare.
3. Kontoinnehavare ska vara känd sedan tidigare för betrodd part. Följande relationer är exempel på vad som avses med känd för denna rutin:
 - a. Betrodd part är ansvarig chef för kontoinnehavarens organisatoriskt.
 - b. Betrodd part har varit del i att genomföra anställningsintervjuer eller motsvarande i samband med en nyanställning och därigenom träffat kontoinnehavaren ifråga ett antal gånger via videosamtal.
 - c. Betrodd part och kontoinnehavaren har arbetat tillsammans i t.ex. forskningssamarbeten mellan lärosäten och därigenom träffat kontoinnehavaren vid upprepade tillfällen innan videosamtalet för identifiering sker.
4. Kontoinnehavare ska bifoga en kopia av godkända identitetshandlingar (enligt avsnitt 5.2.5 punkt 4 eller 5 i SWAMID AL2) till kontoadministratören i förväg, antingen i elektronisk form alternativt som papperskopia. Kopien ska vara en komplett kopia där all information på den aktuella identitetshandlingen är fullt läsbar. Kontoadministratören ska därmed kunna granska kopian i förväg för att säkerställa att rätt information finns tillgänglig och är läsbar.
5. Kontoinnehavaren ska vid videosamtalet uppvisa den aktuella identitetshandlingen så att kontoadministratören kan verifiera den inskickade kopians likhet samt överensstämmelse med person i videosamtalet.
6. Förnamn, efternamn och personnummer (födelsedatum om person utan svenskt personnummer) ska stämma överens med medlemsorganisationens eventuella förregistrerad information gällande kontoinnehavaren. Denna information behövs även för att vid ett senare tillfälle kunna göra en riskbedömning i samband med en lösenordsåterställning.
7. Betrodd part ska under videosamtalet
 - a. intyga att kontoinnehavaren är personen som identitetshandlingarna är utställda till enligt betrodd parts bästa kännedom.
 - b. kunna autentisera sig enligt SWAMID AL2 på ett sätt som kontoadministratören kan verifiera, exempelvis genom
 - i. att betrodd part via en kontohanteringsportal, under autentisering som uppfyller SWAMID AL2, kvitterar ut en tidsbegränsad engångskod som via samma kontohanteringsportal ger kontoadministratören en bekräftelse på att det är betrodd part som kvitterat ut engångskoden.
 - ii. att kontoadministratören i samband med videosamtalet via en kontohanteringsportal kvitterar ut en tidsbegränsad engångskod som betrodd part, under autentisering som uppfyller SWAMID AL2, i samma kontohanteringsportal anger (efter att fått engångskoden uppläst av kontoadministratören) och att kontoadministratören därmed i samma kontohanteringsportal får bekräftelse på att det är betrodd part som angett engångskoden.
8. Kontoaktiveringsuppgifter ska distribueras ifrån kontoadministratör till kontoinnehavare på ett tillräckligt säkert sätt, exempelvis genom att läsa upp en tidsbegränsad engångskod för kontoinnehavaren i videosamtalet eller distribuera engångskod via videosamtalets chat-funktion.

Beslut: SWAMID Board of Trustees ställer sig bakom att ovanstående rutin för personverifiering via videosamtal kan användas för SWAMID AL2.

Beslut om ansökningar om godkännande av tillitsnivåer (PA)

• Rymdstyrelsen ansöker om godkännande för uppfyllande av SWAMID AL2

Efter granskning anser SWAMID Operations att kraven uppfylls och rekommenderar SWAMID Board of Trustees att godkänna ansökan.

Beslut: SWAMID Board of Trustees godkänner Rymdstyrelsens ansökan om godkännande för tillitsnivå SWAMID AL2.

• Ersta Skönda Bräcke Högskola ansöker om godkännande för uppfyllande av SWAMID AL2

Efter granskning anser SWAMID Operations att kraven uppfylls och rekommenderar SWAMID Board of Trustees att godkänna ansökan.

Beslut: SWAMID Board of Trustees godkänner Ersta Skönda Bräcke Högskolas ansökan om godkännande för tillitsnivå SWAMID AL2.

• Försvarshögskolan ansöker om förnyat godkännande för uppfyllande SWAMID AL2

Efter granskning anser SWAMID Operations att kraven uppfylls och rekommenderar SWAMID Board of Trustees att godkänna ansökan. Försvarshögskolan har lagt till nya rutiner på AL1-nivå för att hantera effekterna av pandemin.

Beslut: SWAMID Board of Trustees godkänner Försvarshögskolans ansökan om förnyat godkännande för tillitsnivå SWAMID AL2.

- **Lunds universitet ansöker om förnyat godkännande för uppfyllande SWAMID AL2 samt bibehållen SWAMID AL2-MFA-HI**
Efter granskning anser SWAMID Operations att kraven uppfylls och rekommenderar SWAMID Board of Trustees att godkänna ansökan. Lunds universitet har lagt till ny rutin för videomöte för kontoutdelning för anställda för att hantera effekterna av pandemin.

Beslut: SWAMID Board of Trustees godkänner Lunds universitets ansökan om förnyat godkännande för tillitsnivå SWAMID AL2.

Beslut om deltagande i interfederationen FIDUS (PA)

På uppdrag av Skolverket och Regeringen bygger Sunet upp infrastruktur för hur administratörer, lärare och elever på grund- och gymnasieskolor i Sverige ska kunna logga in i den nya digitala tjänsten för nationella prov. De personer som skriver proven finns vis Sveriges universitet och högskolor och behöver också logga in i provtjänsten. Med avseende på detta håller Skolverket på att bygga upp en ny interfederation med Skolverket som huvudman med tänkta medlemmar [Skolfederation.se](https://www.skolverket.se/om-skolverket/interfederation) och SWAMID. Under arbetet har Sunet noga informerat att lärosäten och myndigheter inom vår sektor har tjänster som de vill tillgängliggöra för Sveriges grund- och gymnasieskolor, t.ex. portaler för verksamhetsförlagt utbildning och den nationella betygsdatabasen hos UHR. Vi har fått gehör för detta och SWAMID har hjälpt Skolverket att ta fram en interfederationspolicy som i Skolverkets fall kallas interfederationsramverk beroende intern nomenklatur.

Beslut: SWAMID Board of Trustees ger ett interimistiskt godkänner att SWAMID deltar i interfederationen FIDUS. Det interimistiska beslutet gäller till och med 2021-12-31. Inför ett permanent beslut skall informationsmaterial, konsekvensanalys och övergripande beskrivning tas fram.

Information om det pågående policyarbetet (PA)

Efter dagens beslut är 13 av 64 medlemmar inte godkända för någon tillitsprofil. SWAMID Operations har tagit kontakt med flera av dem för att försöka få igång arbetet. SWAMID Operations tror fortfarande att vi kan vara klara till 2021-12-31.

Följande organisationer är idag inte godkända för någon tillitsprofil:

- Enskilda Högskolan Stockholm
- Handelshögskolan i Stockholm
- Högskolan i Skövde
- Kungliga Musikhögskolan
- Stockholms konstnärliga högskola
- Institut Mittag-Leffler
- KK-Stiftelsen
- Kungliga Biblioteket
- Kungliga Vetenskapsakademien
- NORDUnet
- Stockholm International Peace Research Institute
- Universitets- och högskolerådet
 - [Antagning.se](https://antagning.se) är inte godkänd för någon tillitsprofil
- Vetenskapsrådet inkl. Sunet
 - eduID är godkänd för både SWAMID AL1 och SWAMID AL2

SWAMID Operations tillsammans med SUNET CERT har under januari och februari tagit fram ett förslag på uppdaterade incidenthanteringsrutiner för SWAMID. Dessa bygger på eduGAIN Security Incident Response Handbook som togs fram inom ramen för eduGAIN under förra året. Just nu pågår publik konsultation inom SWAMID för de nya rutinerna och om det inte blir stora förändringar baserat på konsultationen kommer incidentrutinerna upp till beslut på nästa SWAMID Board of Trustees.

SWAMID Operations har påbörjat översynen av teknikprofilen för SAML. Målet med uppdateringen är förutomharmonisering med övriga policydokument så ska det bli tydligare vilka krav som redan idag ställs för registrering med en skillnad. SWAMID Operations vill tydligt införa en begränsning om vilka som har rätt att registrera en tjänst i SWAMID.

Information om det pågående arbetet med att byta modell attributrelease i SWAMID (PA)

SWAMID Operations har beslutat att den 31 mars inte längre gäller för att alla tjänster ska ha flyttat över till de nya entitetskategorierna utan vi flyttar fram det. Översynen av teknikprofilen för SAML kommer innebära att tjänsterna kommer att uppdatera sitt metadata för att göra det mer fullständigt. Vi samordnar förändringen av entitetskategorierna med denna förändring.

Diskussion om information riktad till IT-chef/motsv om SWAMID (VN)

Punkten flyttas till nästa möte.

Övriga frågor (VN)

- Information om förändringar i SWAMID Operations (PA)

Björn Mattson som tidigare varit inlånad till SWAMID Operations från Blekinge Tekniska Högskola är numera anställd vid Sunet för att hantera SWAMIDs infrastruktur och delta i olika federationsprojekt/samarbeten.

Nästa möte (VN)

3 juni 2021 14.40--15.30.

Avslutande (VN)