SWAMID Identity Management Practice Statement Karolinska Institutet

Universitetsförvaltningen, 2023-06-01

Susanne Torell

Karolinska Institutet

Karolinska Institutet

SWAMID Identity Management Practice Statement

Innehåll

Diarienummer	Dnr föreg. version:	Beslutsdatum:	Giltighetstid:
2-1893/2022	2-1729/2019	Beslutsdatum	Giltighetstid

Beslut:
Beslut

Dokumenttyp:
Dokumenttyp

Handläggs av avdelning/enhet:
UF IT-avdelningen

Beredning med:
Beredning med

Revidering med avseende på:
Uppdaterat dokument för KI uppfyller utökad tillitsnivå SWAMID AL2

Revisionshistorik

Datum	Versions nr	Kommentar	Reviderad av
2022-04-15	0.1	SWAMID AL1 2-1729/2019 Dokument för SWAMID AL2 skapat	Susanne Torell
2022-11-28	1.0	SWAMID AL2 2-1893/2022	Susanne Torell
2023-06-01	2.0	SWAMID AL2 komplette-ring med autentisera konto mha Svenskt e-legitimat-ion på tillitsnivå 3 (avsnitt 5.2)	Susanne Torell

1. Inledning

Karolinska Institutet (KI) är ett av världens ledande medicinska universitet. KI är, tillsammans med bland annat många andra svenska lärosäten, medlem i SWAMID:s federation för att på ett säkert och enkelt sätt kunna ge sina anställda, anknutna och studenter tillgång till IT-resurser

KI uppfyller sedan 2019 tillitsnivå SWAMID AL1. Syftet med dokumentet är att beskriva att KI uppfyller utökad tillitsnivå SWAMID AL2.

4. Organisational Requirement

The purpose of this section is to define conditions and guidance regarding participating organizations responsibilities.

4.1 Enterprise and Service Maturity

This subsection defines the organization and the procedures that govern the operations of the identity provider.

Karolinska Institutet, organisationsnummer 202100-2973 är en statlig forsknings- och utbildningsmyndighet vilket gör att lärosätets verksamhet regleras i lagar, förordningar och regleringsbrev. De viktigaste lagarna och förordningarna som styr universitetets/högskolans arbete är regeringsformen (SFS 1974:152), tryckfrihetsförordning (SFS 1949:105), myndighetsförordningen (SFS 2007:515), högskolelagen (SFS 1992:1434) och högskoleförordningen (1993:100). Regleringsbrevet utställs årligen av regeringen och styr universitetets uppdrag under ett kalenderår. I övrigt följer lärosätet Sveriges övriga lagar och förordningar.

Lärosätets Identitet- och behörighetssystem IDAC och informationsförsörjningskatalog IKAT innehåller uppgifter om lärosätets organisation samt personuppgifter om alla som är verksamma vid lärosätet. Med avseende på detta måste särskild hänsyn till behandling av personuppgifter tas. Allmänna dataskyddsförordningen (EU2016/679) med tillhörande svensk lagstiftning som reglerar behandlingen av personuppgifter samt hantering av personer med behov av skyddade personuppgifter.

Studenters personuppgifter hämtas ur lärosätets studiedokumentationssystem Ladok och därför gäller även förordning (SFS 1993:1153) om redovisning av studier m.m. vid universitet och högskolor för hanteringen av studenters personuppgifter. Anställdas personuppgift0er hämtas från lönesystemet Primula och övriga anknutnas uppgifter från systemet UBW Anknutna.

Som statlig myndighet arbetar lärosätet även med ledningssystem för informationssäkerhet enligt Myndigheten för samhällsskydd och beredskaps gällande ”Föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter”.

KI:s Ledningssystem för informationssäkerhet:
https://medarbetare.ki.se/informationssakerhet
https://staff.ki.se/information-security

Instruktioner om hur olika typer av avfall ska sorteras på KI
https://medarbetare.ki.se/kallsortering-av-avfall
https://staff.ki.se/waste-management

Rutiner för hantering av farligt avfall i form av elektronikskrot och uttjänad lagringsmedia finns beskrivna hos internt hos IT-avdelningen.
4.2 Notices and User Information

The Member Organisation provides an Acceptable Use Policy (AUP) and a Service Definition including a Privacy Policy (PP) for the organisation Subjects. These policies are needed to fulfil the SWAMID Policy and the Swedish legislation including the General Data Protection Regulation (EU) No 679/2016.

Användarvillkor (ansvarsförbindelse) signeras av den som anställs på KI. Detta gäller även personer som anknyts.
https://medarbetare.ki.se/media/31585/download

Studenter godkänner användarvillkor i samband med att de aktiverar sitt konto. https://kib.ki.se/datorer-it/anvanda-kis-datorer-datorprogram/regler-och-riktlinjer-datoranvandning

Acceptans av användarvillkoren sker första gången användaren loggar in och i samband med förnyelse en gång per år. En flagga finns sparad i IdP:n om användaren har godkänt villkoren. När t ex policy för lösenord ändras så kommuniceras detta primärt via e-post samt publika webb-platser. I samband med förändrad policy så får användaren god-känna/avböja på nytt.

Privacy policy och Tjänstedefinition finns beslutade och publicerade på KI:s internwebb Medarbetarportalen

Privacy Policy
https://medarbetare.ki.se/policy-for-hantering-av-personuppgifter-inom-ramen-for-identitetsutgivaren-identity-provider-idp
https://staff.ki.se/rules-and-regulations-for-the-management-of-personal-information-within-the-identity-provider-idp

Tjänstedefinition
https://medarbetare.ki.se/tjanstebeskrivning-saml2-websso-identitet-sutgivare
https://staff.ki.se/service-definition-saml2-websso-identity-provider

Samlingssida om GDPR på KI
https://medarbetare.ki.se/gdpr
https://staff.ki.se/gdpr-at-ki

Länkar till Integritetsskyddspolicy finns på samlingssidan för GDPR
https://medarbetare.ki.se/integritetsskyddspolicy
https://staff.ki.se/data-protection-policy

4.3 Secure Communications

This subsection defines how clear text passwords, private keys and shared secrets must be protected to obtain operational security.

Identitetshanteraren hämtar data från LDAP och Active Directory (AD). SSL/TLS används för detta ändamål. Lösenordet lagras krypterat enligt AD standard. All kryptering sker med 2048-bitars nycklar.

Filerna är skyddade med operativsystemets inbyggda filrättighetssy-stem och endast utsedda administratörer har tillgång till dessa förutom tjänsten själv.

För åtkomst loggar utsedd administratör in till elektronisk lösenordshanterare med sitt personliga administratörskonto för att erhålla lösenord.

Alla administratörer av identitetshanteraren utses av Administrativ chef eller ansvarig för identitetshanteraren.

4.4 Security-relevant Event (Audit) Records

This section defines the need to keep an audit trail of relevant systems.

Identitet- och behörighetssystemet IDAC loggar alla förändringar som sker på en identitet och de som är äldre än ett år rensas löpande. Detta innefattar mejlbyten, namnbyten och all annan innan information som kan ses på identitetskortet i systemet. Systemet loggar ändringar på sina dataobjekt, vilket innebär att det finns historik på organisationer och grupper. Mejlutskick loggas med undantag för de mejl som innehåller lösenord, dessa sparas ej. Loggarna har tidstämpel och med information om vem som har utfört förändringen. I de fall där förändringar importeras från HR-system (källsystem) står identitet- och behörighetssystemets servicekonto som användare.

Inloggningar loggas i Shibboleth samt skickas till KI:s centrala IT-säkerhetsloggserver. KI:s centrala IT-säkerhets loggserver hanterar användare, datorer och beteenden.

Auditloggning sker även i den centrala identitetshanteraren. Tidstämpel för alla lösenordsbyten loggas.

5. Operational Requirements

5.1 Credential Operating Environment

The purpose of this subsection is to ensure adequate strength of Subject credentials, such as passwords, and protection against common attack vectors.

Följande förenklade sammanfattade regler för lösenordshantering gäller för alla IT-tjänster och system (applikationer) vid Karolinska Institutet.

- Lösenord är personliga och får inte delas med annan

- Lösenord ska bestå av minst 10 tecken[1]
- Lösenord ska vara sammansatt av både bokstäver, siffror och specialtecken
- Lösenord får inte vara knutet till personlig information som till exempel namn, personnummer, telefonnummer eller användarnamn
- Lösenord får inte återanvändas utanför KI
- Ytterligare autentiseringsverktyg, exempelvis OTP-enheter, inloggningskort, säkerhetsnycklar, autentiseringsappar m.m. är personliga och får inte delas med annan.

Lösenordsregelverket för Karolinska Institutet finns publicerat på KI:s internwebb Medarbetarportalen
https://medarbetare.ki.se/konton-och-losenord
https://medarbetare.ki.se/media/107535/download

Tvåstegsverifiering/MFA är obligatoriskt på KI. Det innebär att inloggning sker i två steg: med hjälp av användarnamn och lösenord, samt push notis med nummer matchning via Microsoft Authenticator appen. Microsoft Authenticator appen är av typen ”a Single-Factor Cryptographic Software”.

KI signalerar för närvarande inte tvåstegsverifiering/MFA vid inloggningar inom SWAMID.

Om ett konto har kompromettерats finns fastställda rutiner för att stänga av kontot, se avsnitt 5.4

All kommunikation sker krypterat via SSL/TLS eller motsvarande, vilket innebär att KI följer SWAMID:s krav.

KI hanterar system, interna nät och servrar på ett säkert sätt med implementerade skyddsmekanismer samt hanteras enligt fastställda rutiner.

5.2 Credential Issuing

The purpose of this subsection is to ensure that the Identity Provider has control over the issuing process including issuing of credentials and binding of other information to the Subject. Furthermore, the Identity Provider and its Subjects must be uniquely identified.

[1] För andra typer av konton än personliga användarkonton gäller andra krav

De användarnamn (KIID) som Karolinska Institutet skapar i KI:s centrala Identitet- och behörighetssystem IDAC hör till domänen ki.se som KI äger. Vid federation kompletteras användarnamnet med KI:s domännamn, enligt formatet <KIID>@ki.se. Användarnamnet blir därmed globalt unikt även utanför KI:s domän. KI har ett globalt unikt EntityID för vår SAML2-identitetshanterare.

Användarnamnet (KIID) återanvänds inte, med undantag om det är en identitet med samma personnummer som återvänder till KI inom 10 år. Personen kan då få tillbaka samma användarnamn.

En användare kan ha flera konton, beroende på funktion/roll. Det kan handla om en användare som är både anställd/anknuten/doktorand och student på grundnivå. Användaren kan välja vilket konto som ska användas genom att ange specifika användarnamnet som medarbetare eller som student.

Captcha och engångslösenord/aktiveringskoder används för att aktivera konton för studenter. Detta kan också ske, mot uppvisande av giltig ID-handling, via Student IT.

I Identitets- och behörighetssystem IDAC går det inte att registrera information om medarbetare eller student och på sätt skapa upp ett konto. All information om medarbetare och student flödar från källsystemen till Identitet- och behörighetssystem IDAC. De personliga identifierarna för ett konto är personnummer, samordningsnummer, passnummer eller interims personnummer från Ladok.

Medarbetare (anställda, anknutna och doktorander) får sitt användarnamn (KIID), e-postadress och lösenord utdelat av administratörer på respektive institution. I samband med utlämnandet, så kontrolleras kontot i Identitet- och behörighetssystem IDAC. Administratören skriver ut ett papper med användaruppgifter i användarens närvaro som denna får med sig. Kontot blir aktivt först vid startdatumet för anställningen/anknytningen. Kontots tillitsnivå är SWAMID AL1.

Vid aktivering av studentkonto är identifierarna personnummer, e-postadress eller användarnamn (KIID). Studenter får en aktiveringskod som endast kan användas en gång och är tidsbestämd. Koden

distribueras till folkbokföringsadress eller lämnas ut mot giltig ID-handling i Student IT. Studenter kan även aktivera sitt KI-konto via antagning.se eller eduID. Kontots tillitsnivå är SWAMID AL1.

Användare med tillitsnivå AL1 och AL2 som inte har satt upp tvåstegsverifiering/MFA för sitt konto kan göra det genom att koppla en Microsoft Authenticator-app till sin identitet. Vid koppling loggar användaren in i Microsoft 365 med sitt användarnamn och lösenord och registrerar en Microsoft Authenticator-app enligt guide.

På KI skickas inga lösenord med e-post till den berörde.

Självuppgiven information kan ändras av innehavaren av kontot

Vid behov av att uppgradera tillitsnivå på konto kan användaren använda sig av ett av nedanstående sätt, antingen genom att använda sig självserviceportal eller genom fastställd manuell process.

- Användare som har Svenskt e-legitimation på tillitsnivå 3 kan själv uppgradera sitt identitetskonto till en högre tillitsnivå som en tjänst kräver, genom att gå in på en självserviceportal, ID-Portal (https://idportal.ki.se). Användaren behöver först logga in för att identifiera sig. Efter inloggning ges möjlighet att välja e-legitimation på tillitsnivå 3 för att autentisera sitt konto. Matchning görs på personnummer mellan KI-kontot och autentisering med Svensk e-legitimation. Efter autentisering av kontot flödar information till IdP:n om att användaren är bekräftad enligt SWAMID AL2. Informationen loggas på identitetskortet i Identitet- och behörighetssystem IDAC.

- För de användarna som inte har e-legitimation på tillitsnivå 3 finns det en fastställd manuell process enligt nedan.
  Enligt fastställd process innebär det att medarbetare initierar begäran om utökad tillitsnivå till SWAMID AL2 till sin närmaste chef. Närmaste chefen tar kontakt med HR. HR tar kontakt med medarbetaren, som uppvisar godkända identitetshandlingar (enligt avsnitt 5.2.5 punkt 4 och 5 i SWAMID AL2). HR granskar, tar kopia på identitetshandlingen och signerar kopian samt laddar upp kopian i medarbetarens personakt (HR-arkiv) samt söker fram medarbetaren

och registrerar i Identitet- och behörighetssystem IDAC att medarbetaren är bekräftad enligt SWAMID AL2.

För studenter sker detta förnärvarande i samband med utlämnade av KI-kortet, personligt passerkort för access. Först efter studenten har aktiverat sitt studentkonto kan studenten ansöka om ett KI-kort. KI-kortet lämnas ut mot uppvisande av godkända identitetshandlingar (enligt avsnitt 5.2.5 punkt 4 och 5 i SWAMID AL2). I samband med detta, så söker administratören fram studenten och registrerar i Identitet- och behörighetssystem IDAC att studenten är bekräftad enligt SWAMID AL2.

Uppdatering av tillitsnivån sker genom att använda tjänsten Verifiera användare i Identitet- och behörighetssystem IDAC. Administratören behöver ange i tjänsten vilken användare och dess konto det berör. Information flödar efter registrering till IdP:n om att användaren är bekräftad enligt SWAMID AL2. Informationen loggas på identitetskortet i IDAC.

Om det finns någon anledning att tillitsnivån ska sänkas till SWAMID AL1 så används samma tjänst och flaggan för tillitsnivån tas bort, i och med det så tas också informationen bort från IdP:n.

Kontoadministratörer, institutionsadministratörer och HR-personal som genomför identitetskontroll samt systemadministratörer för identitetshanteraren uppfyller kraven för SWAMID AL2. Ovannämnda process har genomförts för att signalera tillitsnivå SWAMID AL2 samt loggas på dess kontots identitetskort. Tekniska konton exponeras för närvarande inte mot SWAMID.

5.3 Credential Renewal and Re-issuing

The purpose of this subsection is to ensure that Subjects can change their credential and get new credentials when lost or expired.

Förutsättningen för att en användare ska kunna ändra och återställa sitt lösenord är att kontot är aktivt.

En användare kan själv ändra sitt lösenord genom att logga in på Microsoft Office365 (https://office.com) och välja Ändra lösenord.

Användaren behöver uppge sitt gamla lösenord samt uppge ett nytt samt verifiera det.

Har en användare har glömt sitt lösenord, så finns det två vägar beroende på om denne är medarbetare eller student.

- Om användaren en medarbetare (anställd, anknuten eller doktorand) och att det inte går att nollställa sitt lösenord behöver medarbetare kontakta sin institutions administratör för att hämta ut ett nytt lösenord. Administratören utför legitimationskontroll samt använder tjänsten Återställ lösenord i Identitets- och behörighetssystemet IDAC genom att uppge användarens KIID. Lösenordet presenteras på skärm för administratören och lämnas sedan ut till användaren i en sekvens. Användaren behöver sedan ändra sitt erhållna lösenord. Rutinbeskrivning för administratören (IDAC-administratör) finns på internwebben Medarbetarportalen https://medarbetare.ki.se/rutinbeskrivningar-idac
- Om en användare är en student och att det inte går att nollställa sitt lösenord, så behöver denne antingen beställa en ny aktiveringskod för att sätta om sitt lösenord. Aktiveringskoden som endast kan användas en gång skickas hem till studentens folkbokföringsadress. Studenten kan också hämta ut ett nytt lösenord hos studentsupporten Student IT på Universitetsbiblioteket mot uppvisande av legitimation. Student IT administratör använder tjänsten Återställ Lösenord student i Identitets- och behörighetssystemet IDAC genom att uppge användarens Student KIID. Lösenordet presenteras på skärm till administratören och lämnats sedan ut till studenten i en sekvens. Därefter behöver studenten sedan ändra sitt erhållna lösenord.

Om ett lösenord misstänks ha kompromettерats kan KI suspendera kontot till dess en lösenordsaktivering skett på samma sätt som beskrivits ovan med personligt besök.

Ändring av kontots tillitsnivå till obekräftad (SWAMID AL1) sker vid återställning av lösenord via Identitets- och behörighetssystemet IDAC.

Användaren kan byta/återställa sin Microsoft Authenticator-app genom att kontakta sin institutions administratör för att erhålla ett tillfälligt tidsbegränsat åtkomstpass. Koden är 8-siffrig och kan endast användas en gång. Användaren följer därefter fastställd rutin för återställningen.

5.4 Credential Revocation

The purpose of this subsection is to ensure that credentials can be revoked.

När användaren lämnar organisationen blir kontot inaktiverat då kontots slutdatum har inträffat. För att kontot ska öppnas på nytt behöver ny information flöda in till Identitets- och behörighetssystemet IDAC från källsystemen. Under tiden så finns det ingen möjlighet att använda kontot. På KI är Identitets- och behörighetssystemet IDAC det styrande systemet vad gäller status på kontot gentemot Active Directory (AD) och IdP:n (IKAT).

När misstanke finns om att ett konto blivit komprometterat eller att kontot ska spärras av en annan anledning så finns fastställda rutiner för hantering av detta. Det sker antingen tvinga till ett lösenordsbyte för användaren för det specifika tillfället eller låsa/spärra kontot helt.

En användare kan på egen begäran få sitt konto spärrat genom att kontakt tas med IT Helpdesk. Samma förfarande utförs som nedan att använda sig av tjänsten Nödutelåsning i Identitets- och behörighetssystemet IDAC

Om inte kontot behöver spärras utan endast en återställning av lösenord önskas, så kontaktar användaren sin Institutions administratör för IDAC alternativ Student IT.

Kontot spärras av IT genom att använda sig av tjänsten Nödutelåsning i identitets- och behörighetssystemet IDAC. I tjänsten anges identifieraren KIID tillsammans med orsaken till att kontot ska spärras. Efter genomförd utelåsning, så innebär det att användaren inte längre kan använda några av de centrala tjänsterna knutna till inloggningen. Studenten kan inte heller ändra, nollställa sitt lösenord eller erhålla ett nytt.

Hantering av att informera och öppna upp kontot sker enligt fastställd rutin. Kontakt tas med administratören på institutionen som

användaren är knuten till alternativt studentsupporten Student IT. Kontakten med användaren sker sedan via administratören eller Student IT. Information om orsak till att kontot har spärrats ges och vilka steg som behöver vidtas innan kontot kan öppnas upp och användas igen. Användaren får ett nytt lösenord via sin administratör på institutionen alternativt studentsupporten Student IT (hanteringen beskrivs i avsnitt 5.2).

Kontot öppnas upp igenom genom att återställa nödutelåsningen för det aktuella kontot (KIID är den fördefinierade identifieraren) med orsak. I samband med nödutelåsningen så sker en ändring av kontots tillitsnivå till obekräftad (SWAMID AL1).

Användaren behöver också konfigurera om multifaktorautentiseringen enligt guide (hanteringen beskrivs under 5.3)

Användaren uppmanas också att gå igenom avsnitt om Informationssäkerhet på interwebben Medarbetarportalen.

I de fall som kontot ska spärras av en annan anledning, så tar närmaste chef kontakt med IT. Det är samma förfarande som ovan men skillnaden är att det är närmaste chefen som tar kontakt med IT för åtgärd. Ska kontot ska öppnas på nytt så är det också närmaste chef som tar kontakten med IT i övrigt samma förfarande som ovan.

Allvarligare fall av missbruk eller andra liknande regelbrott anmäls till säkerhetschefen för vidare handläggning. Misstankar om brottslig verksamhet polisanmäls. Utförligare beskrivning beskrivet i dokument Handledning i informationssäkerhet vi Karolinska Institutet" https://medarbetare.ki.se/media/691/download

Rutinen för att hantera säkerhetsincidenter så att dessa inte återupprepas finns beskriven i KI:s ledningssystem under kapitel D Informationssäkerhet för säkerhetsfunktioner.
https://medarbetare.ki.se/media/4475/download

5.5 Credential Status Management

The purpose of this subsection is to ensure that credentials are stored accordingly and that Identity Management systems have a high degree of availability.

Identitetshanteraren hanterar och sparar historiken över alla aktiva och inaktiva konton. UIDn återanvänds aldrig.

Karolinska Institutet garanterar en tillgänglighet till tjänsten som stämmer överens med Karolinska Institutets krav och förväntningar. Det finns erfarenhetsmässigt bevis på att KI uppfyller kravet att tillgänglighet till tjänsten överstiger 95%.

5.6 Credential Validation/Authentication

The purpose of this subsection is to ensure that the implemented Validation/Authentication processes meet proper technical standards.

KI autentiserar endast aktiva konton, dvs inaktiva (inkl återkallade) konton autentiseras inte.

Användaren får inte bli inloggad på IdP:n utan att uppge användarnamn och lösenord.

Single-Sign-On till andra tjänster är inte implementerat på KI med andra ord kan man inte bli automatiskt inloggad utan att det krävs en aktiv handling av användaren. Giltig sessionstid i IdP:n är satt till 1 timma.

KI använder SAML, Shibboleth och RADIUS för Eduroam, vilket innebär att SWAMIDs krav uppfylls.