Karlstads universitet
Identity Management Practice Statement

IT-avdelningen

2023-10-10

KAU.SE

Karlstads universitet
651 88 Karlstad

054-700 10 00
information@kau.se

Innehåll

1. Inledning

Detta dokument är Karlstads universitets Identity Management Practice Statement (IMPS), för den svenska akademiska identitetsfederationen SWAMID.

Detta dokument beskriver Karlstads universitets rutiner för att hantera digitala identiteter. Dokumentet är avsett för universitetets medlemskap i SWAMID och uppfyllande av SWAMID tillitsprofiler 1, 2 och 3.

4. Organisation Requirement

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

4.1 Enterprise and Service Maturity

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

Karlstads universitet, organisationsnummer 202100-3120, är en statlig 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 identitets- och behörighetssystem 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 enligt aktuell personuppgiftslagstiftning.

Som statlig myndighet arbetar lärosätet även med ledningssystem för informationssäkerhet enligt Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet.

Gamla eller trasiga lagringsmedia plockas ur och samlas i låst och larmat utrymme innan de förstörs fysiskt av universitetets upphandlade avfalls- och återvinningsföretag.

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.

Karlstads universitet har användarvillkor som måste godkännas vid första inloggning (eller vid ändring av villkor) i universitetets identitetsutgivare. Godkännandet av dessa villkor lagras i en databas.

En användaranpassad tjänstebeskrivning och integritetspolicy finns publicerad på adressen https://weblogin.kau.se

Användarreglerna finns publicerade på webben.

Allmänna regler för informationssäkerhet

För samtliga verksamma vid universitetet. Finns på intranät och externa webben:

https://www.kau.se/student/ar-student/it-stod/hjalp/it-sakerhet

Policy och regler

Policy och regler för digitala identiteter. Vissa finns på universitetets intranät och är bakom inloggning.

Policy för digitala identiteter (direktlänk):
https://intra.kau.se/dokument/upload/82F319910773220B80OIO202EE64/policy-digitala-identiteter.pdf
Regler för digitala identiteter (direktlänk):
https://intra.kau.se/dokument/upload/82F3194F0a61a19DC5MU9E698F8A/Regler%20-%20Digitala%20identiteter.pdf
En särskild policy finns för KauID för studenter på externa webben:
https://www.kau.se/student/ar-student/it-stod/hjalp/it-sakerhet

4.3 Secure Communications

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

De tjänster som ingår i identitetshanteringens infrastruktur driftas på virtuella servrar i datorhallar och åtkomst är begränsad till de personer som ska hantera systemen. Privata nycklar lagras på dessa servrar och åtkomst är begränsad via filsystemsrättigheter. Lösenord som delas mellan systemadministratörer lagras i ett centralt lösenordshanteringssystem. Åtkomst är begränsad till personer som har ansvar för identitetshanteringssystemen.

All nätverkskommunikation mellan de olika system som ingår i identitetshantering är krypterad med TLS. Relying party och identitetsutgivare nycklar är minst 2048 bitar RSA.

4.4 Security-relevant Event (Audit) Records

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

Samtliga system som ingår i identitetshantering lagrar alla händelser med tillhörande tidsstämpel lokalt och på en central loggserver i minst sex månader. Ändringar av samtliga uppgifter och attribut i LDAP systemet loggas i LDAP.

5. Operational Requirements

The purpose of this section is to ensure safe and secure operations of the service.

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.

Karlstads universitets identitetsutgivare har stöd för autentisering på samtliga AL nivåer.

Vid multifaktorautentisering används någon av dessa:

1. Svensk e-legitimation på tillitsnivå 3 i kombination med användarens lösenord.
2. En TOTP-app som en andra faktor i kombination med användarens lösenord (Single-Factor Cryptographic Software in combination with memorised secret).

Dessa kombinerad multifaktor är oberoende av varandra.

Lösenorden uppfyller SWAMIDs rekommendationer och ger en entropi på minst 24 bitar enligt NIST SP 800-63-2.

All kommunikation inom hantering av identitet och kontouppgifter är krypterad med TLS med inbyggda skydd mot message replay via SAML protokollet.

I våra policydokument nämns tydligt att KauID, lösenord samt andra faktorer är personliga och får inte tilldelas eller överlämnas till en annan person.

Säkerheten i våra system upprätthålls genom regelbunden patchning, övervakning, begränsad åtkomlighet, krypterad kommunikation och till vissa system krävs även multifaktorautentisering för driftspersonal.

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.

Subject assertions för samtliga användare inkluderar en unik identifierare (scope) av kau.se. Karlstads universitets identitetsutgivare har globalt unik identifierare (entity id).

Ett användarnamn på Karlstads universitet kallas för KauID och är unikt för varje individ på universitetet. En person kan ha flera KauID om de är både personal och student. Ett KauID för student består av bokstäver och siffror. Alla andra typer av KauID består vanligtvis av enbart bokstäver. En person som är personal och student kan välja vilket KauID de vill använda vid inloggning.

Ett KauID kan inte återanvändas av en annan person. Detta säkras genom att förbrukade KauID sparas.

Vid granskning av legitimation för både anställda och studenter, accepteras följande typer:

- Godkänd svensk ID-handling (SIS-märkt ID-kort, körkort, Identitetskort för folkbokförda i Sverige)
- Svenskt nationellt ID-kort eller pass
- Utländskt pass som uppfyller ICAO Doc 9303
- EU/EES nationellt ID-kort som uppfyller European Commission Regulation 562/2006

Det finns intern dokumentation som medarbetare som granskar legitimation har tillgång till. Den beskriver processen för att verifiera en ID-handling, vilka ID-handlingar som accepteras och länkar till externa sajter för hjälp med verifiering (t.ex. PRADO).

Användare uppfyller olika tillitsnivåer, inloggningstjänsten kan via attributrelease signalera till aktuell tjänst vilken tillitsnivå som användaren har.

Ändringar av tillitsnivån på ett KauID loggas i LDAP-katalogen samt i den applikation som utfört ändringen. I loggen sparas vilken typ av legitimation som använts.

Alla som har ett KauID vid Karlstads universitet har möjlighet att uppdatera sina egenuppgivna uppgifter. För studenter sker detta via Ladok. För personal och samarbetspartner sker det via olika gränssnitt, via IT-avdelningen eller sin HR-specialist.

All personal vid Karlstads universitet som har rätt att administrera KauID använder själv ett KauID på minst samma tillitsnivå som KauID:t som ska administreras. Detta säkerställs av de administrativa verktyg som används för kontohantering.

Personal

En anställd kan skapa sitt KauID med hjälp av en aktiveringskod. Aktiveringskoden är en tidsbegränsad engångskod. En administratör beställer en kod för aktivering i universitetets identitetshanteringssystem. Vilken AL-nivå som sätts för ett nytt KauID beror på metoden som används:

1. Via videomöte. Användaren visar en godkänd legitimationshandling och administratören visar upp aktiveringskoden på ett utskrivet papper. För de som har svenskt personnummer är detta identifieraren. För de som inte har svenskt personnummer används en kombination av passnummer, namn, nationalitet och födelsedata som identifierare. Denna metod ger AL1.
2. Legitimering i helpdesk. Användaren visar en godkänd legitimationshandling och får en aktiveringskod på ett utskrivet papper. För de som har svensk id-handling är personnummer identifieraren. För de som inte har svensk id-handling används en kombination av passnummer, namn, nationalitet och födelsedata som identifierare. Denna metod ger AL2.

Användaren aktiverar sedan sitt KauID i kontoaktiveringsportalen. Portalen är skyddad med en reCaptcha. Inloggning sker med personnummer, samordningsnummer eller födelsedatum (ej skrivet på pappret) tillsammans med aktiveringskoden. KauID:t är oanvändbart tills det är aktiverat.

En anställd kan höja AL-nivå på befintligt KauID till AL2 med en av följande metoder:

1. Legitimering i helpdesk. Användaren måste visa en godkänd legitimationshandling som jämförs med tidigare kontroll. För de som har svensk id-handling är personnummer identifieraren. För de som inte har svensk id-handling används en kombination av passnummer, namn, nationalitet och födelsedata som identifierare.
2. Online på AL2-nivå mot eduID eller antagning.se. Matchning sker med personnummer som identifierare. Identitetsutgivaren måste vara godkänd för AL2 vilket kontrolleras.

En anställd kan lägga till en multifaktor på befintligt KauID med en av följande metoder:

1. Online med en svensk e-legitimation på minst tillitsnivå 3. Användaren loggar in i en onboarding-portal med sitt KauID på AL1 eller AL2 nivå. Därefter loggar användaren in med sin e-legitimation. Systemet kontrollerar personnumret från den lokala identitetsutgivaren mot personnumret eller det styrkta samordningsnumret från e-legitimationens inloggning. Under förutsättning att dessa matchar, tillåts användaren skapa ett organisations eID (som är användarens eduPersonPrincipalName). Detta lagras hos leverantören. Identifieraren är personnumret/samordningsnumret. Denna metod ger AL3.
2. Online och helpdesk. För anställda som saknar personnummer/samordningsnummer eller av annan godkänd anledning inte kan skaffa e-legitimation finns möjlighet att skaffa multifaktor med en TOTP-app. Användaren loggar in i en onboarding-portal med sitt KauID på AL1 eller AL2 nivå och skapar en TOTP-kod. Efter verifiering av en testkod är multifaktorn inaktiv tills användaren besöker helpdesk. Vid helpdesk sker legitimering med

godkänd legitimationshandling samt en verifieringskod från TOTP-appen. Då aktiveras multifaktorn för användaren. För de som har svensk id-handling är personnummer identifieraren. För de som inte har svensk id-handling används en kombination av passnummer, namn, nationalitet och födelsedata som identifierare. Om användaren loggar in i onboarding-portalen när det redan finns en aktiv multifaktor, krävs multifaktor för att logga in. Denna metod ger AL2.

Student

En antagen student kan skapa sitt KauID på flera olika sätt. De olika metoderna är:

1. Online med svensk e-legitimation på minst tillitsnivå 3. Denna metod ger AL2.
2. Online via antagning.se eller eduID. Personnummer är identifierare. AL-nivån sätts utifrån assurance-värdet från identitetsutgivaren. Identitetsutgivaren måste vara godkänd för den aktuella tillitsnivån, vilket kontrolleras.
3. Via en aktiveringskod. En student kan beställa en kod för aktivering som behandlas av en administratör. Aktiveringskoden är en tidsbegränsad engångskod. För denna metod är identifieraren personnummer, samordningsnummer eller interimspersonnummer. AL-nivån för ett nytt KauID beror på hur aktiveringskoden delas ut till studenten:
   a) Via post till folkbokföringsadressen som finns i Ladok. Denna metod ger AL2.
   b) Via post till annan postadress som finns i Ladok. Denna metod ger AL1.
   c) Via e-post till e-postadressen som finns i Ladok. Denna metod ger AL1.
   d) Personligt besök i helpdesk. Studenten måste visa en godkänd legitimationshandling. För de som har svenskt personnummer är detta identifieraren. För de som inte har svenskt personnummer används en kombination av passnummer, namn, nationalitet och födelsedata som identifierare. Denna metod ger AL2.

   Användaren aktiverar sedan sitt KauID i kontoaktiveringsportalen. Portalen är skyddad med en reCaptcha. Inloggning sker med personnummer, samordningsnummer eller interimspersonnummer (ej skrivet på pappret) tillsammans med aktiveringskoden. KauID:t är oanvändbart tills det är aktiverat.

En student kan som högst få AL2. En student kan höja sin AL-nivå genom att göra om processen med en metod som är godkänd för AL2.

Samarbetspartner och associerade personer

En samarbetspartner följer samma regelverk som anställda men har inte samma behörigheter. De får enbart tillgång till de specifika system som de behöver.

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.

Alla användare kan byta sitt lösenord via två olika lösenordsportaler. För anställda är detta en tredjepartsprodukt[1]. För studenter är detta kontoaktiveringsportalen.

När användaren gör lösenordsbyte anges först det gamla lösenordet innan man anger det nya två gånger. Det nya lösenordet måste uppfylla kraven i avsnitt 5.1.

Personal, samarbetspartner och associerade personer

Om KauID-lösenordet till en anställd har löpt ut, kan det gamla lösenordet användas för att logga in i lösenordsportalen för att sedan bytas till nytt.

Om en anställd har glömt sitt lösenord använder man en av följande metoder för att få tillgång till sitt KauID:

1. Via videomöte som beskrivs i avsnitt 5.2 med kontroll av personnummer eller kombination av passnummer, namn, nationalitet och födelsedata för att säkerställa att det är samma individ. Denna metod ger AL1.
2. Legitimering i helpdesk som beskrivs i avsnitt 5.2 med kontroll av personnummer eller kombination av passnummer, namn, nationalitet och födelsedata för att säkerställa att det är samma individ. Denna metod ger AL2.
3. Via en för-registrerad e-postadress. Användaren kontaktar helpdesk och uppger sitt personnummer, samordningsnummer eller födelsedatum. Därefter kan de få en aktiveringskod skickad till sin för-registrerade e-postadress. Aktiveringskoden är en tidsbegränsad engångskod. Denna process används endast i de fall användaren har ett aktivt KauID och har glömt sitt lösenord. Ingen legitimering sker. Denna metod ger AL1.

Om AL-nivån har sänks vid återställning, måste man genomför en process för att höja det till AL2 eller AL3 som beskrivs i avsnitt 5.2.

För att tvinga ett lösenordsbyte, kan vi manuellt justera kontoinställningar i AD och LDAP-katalogen, till exempel för att kräva lösenordsbyte vid nästa AD inloggning.

Om ett KauID ska återaktiveras efter att har varit inaktiverat sker det på samma sätt som beskrivs i avsnitt 5.2.

Om en anställd som innehar ett Organisations eID och ligger på AL3 förlorar access till sin e-legitimation (t.ex. genom att tappa bort eller byta mobiltelefon), så kan AL3 återfås genom att logga in i onboarding-portalen och göra om processen som beskrivs i avsnitt 5.2.

[1] Denna portal används för närvarande enbart för lösenordsbyte för personal, samarbetspartner och associerade personer. Den är inte samma portal som kontoaktiveringsportal som beskrivs under 5.2

Om en anställd som använder en TOTP-app förlorar access till sin multifaktor (t.ex. genom att tappa bort eller byta mobiltelefon), måste multifaktorn tas bort ur identitetshanteringssystemet av en administratör och processen som beskrivs i avsnitt 5.2 göras om.

Student

Processen för återställning är identisk med processen för credential issuing som beskrivs i avsnitt 5.2.

För att tvinga ett lösenordsbyte, byter vi lösenordet till ett okänt värde och därmed tvinga studenterna att gå igenom återställningsprocessen.

För studenter som återupptar sina studier efter uppehåll kan KauID:t återaktiveras på samma sätt som beskrivs i avsnitt 5.2. För detta krävs en aktiv antagning i Ladok och en matchning av personnummer/samordningsnummer/interimspersonnummer och/eller Ladok student uuid med ett avaktiverat KauID. Finns det ingen matchning, så skapas ett nytt KauID.

5.4 Credential Revocation

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

Karlstads universitet kan spärra och avaktivera alla egenutfärdade konton på begäran av organisationen eller användaren. Ett KauID spärras i samband med en säkerhetsincident eller missbruk. Ett KauID avaktiveras efter avslutad anställning eller avslutade studier, eller när en student tillfälligt stängs av.

Incident Response Team (IRT) hos IT-avdelningen ansvarar för kontakt med kontoinnehavaren efter att ett KauID spärras. IRT tar kontakt med personen med hjälp av kontaktuppgifterna i våra system. Vid behov kontaktar man ansvarig chef, HR-avdelningen, Ladok eller fakulteten för att bekräfta kontaktuppgifter. Vi kan också kontrollera uppgifter i folkbokföring. Genom att kontrollera flera system och personer kan IRT säkerställa att de tar kontakt med rätt individ.

För att få tillbaka access till KauID måste kontoinnehavaren följa processen som beskrivs i avsnitt 5.3.

IRT samtalar med den drabbade personen efter att en incident har skett i syfte att minimera risken för att problemet återupprepas. Gällande personal kan de också ta kontakt med ansvarig chef och HR-avdelningen.

IT-chef och IRT ansvarar tillsammans för att utredning görs, och eventuella åtgärder vidtas, efter incidenter. Det gäller såväl om en incident har påverkat flera konton, som om en isolerad incident visar sig bero på brister i system eller processer.

Personal, samarbetspartner och associerade personer

Ett KauID är aktivt en månad efter avslutad tjänst. Sedan avaktiveras kontot i LDAP och AD. Efter sex månader rensas AD kontot helt. En chef kan dock besluta om förlängd tillgång vid behov.

Om en anställd som har slutat innehar ett Organisations eID eller en multifaktor i TOTP-appen tas detta bort automatiskt samtidigt som KauID avaktiveras.

Om en anställd som innehar ett Organisations eID och ligger på AL3 förlorar access till sin e-legitimation (t.ex. genom att tappa bort eller byte av mobiltelefon), ska Organisations eID tas bort[2] och AL3 sänks till AL2. Om en anställd har en TOTP-kod, ska multifaktorn tas bort ur identitetshanteringssystemet.

Vid missbruk kan ett KauID spärras enligt samma rutin som ovan fast utan fördröjning. Det kan också göras genom att supportpersonal tillfälligt sätter om lösenordet och/eller lägger till ett attribut i LDAP som blockerar inloggning. Kontot sänks till AL1. Organisations eID eller TOTP-kod, om dessa finns, tas bort.

Student

Ett KauID för student är aktivt i 18 månader efter senaste avslutat kurstillfälle och efter det avaktiveras kontot i LDAP och AD-kontot raderas.

KauID avaktiveras tillfälligt om en student blir avstängd. När avstängningen löper ut blir KauID automatiskt återaktiverat.

Vid missbruk kan en systemadministratör spärra KauID:t samt sätta ett attribut som förhindrar återaktivering. I och med detta är det inte möjligt för en student att återaktivera sitt KauID.

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.

Alla system som används för kontohantering loggar aktivitet och ändringar som sker till konton och dessa skickas till en central syslog server. LDAP katalogen har ett attribut som sparar händelse- och historisk information.

LDAP katalogen är ett register av samtliga utfärdade identiteter hos Karlstads universitet.

Karlstads universitet har en databas av samtliga utfärdade identiteter för att säkerställa att ett KauID inte kan återanvändas.

[2] Om den anställde spärrar, eller skaffar en ny e-legitimation tas också Organisations eID bort automatiskt av leverantören.

Karlstads universitets har en tillgänglighet på sin identitetsutgivare och underliggande system som bedöms tillräcklig för att uppfylla universitetets krav och bevakas under och utanför arbetstid.

5.6 Credential Validation/Authentication

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

Karlstads universitet följer SWAMIDs teknologiprofiler samt rekommendationer.

Det är inte möjligt att autentisera ett konto som är avaktiverat eller spärrat.

Identitetshanteringssystemen på Karlstads universitet kräver att användaren matar in sina kontouppgifter under autentisering. En SSO funktion finns för webbtjänsterna.

För SAML2-baserad webbinloggning uppfyller universitetet kraven med att den maximala längden för SSO-sessionen är tolv timmar.