Identity Management Practice Statement

HÖGSKOLAN DALARNA

1 Innehåll

2 Inledning

Detta dokument utgör Högskolan Dalarnas **Identity Management Practice Statement** (IMPS) för den svenska akademiska identitetsfederationen SWAMID och beskriver lärosätets rutiner för att hantera elektroniska identiteter.

Dokumentet är avsett för högskolans medlemskap i SWAMID och uppfyllande av SWAMID tillitsprofiler 1 och 2.

Rubriknumrering från och med 4 och framåt motsvarar en rubrik i SWAMID Identity Assurance Level 2 Profile.

2.1 Dokumenthistorik

Datum	Rev.	Författare	Kommentar
2017-03-03	1	Dennis Sjögren	Dokumentet upprättat
2024-10-10	2	Dennis Sjögren	Uppdaterat för BankID
2024-11-07	3	Dennis Sjögren	Revidering efter granskning av SWAMID
2024-11-29	4	Dennis Sjögren	Uppdaterat för AL1 och Antagningen

2.2 Kontaktuppgifter

Dennis Sjögren, Utvecklare/Arkitekt
Avdelningen för IT och digital infrastruktur, Högskolan Dalarna
E-post: dempa@du.se
Telefon: 023-778891

Magnus Höglund, IT-chef
Avdelningen för IT och digital infrastruktur, Högskolan Dalarna
E-post: mho@du.se
Telefon: 023-778120

4 Organisational Requirement

4.1 Enterprise and Service Maturity

4.1.1 Svenskt organisationsnummer

Högskolan Dalarna har organisationsnummer 202100-2908.

4.1.2 Tillämpbara lagrum

Högskolan Dalarna, organisationsnummer 202100-2908, är en statlig utbildningsmyndighet vilket gör att högskolans 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.

4.1.3 Rutiner för destruering av lagringsmedia

Lagringsmedia (hårddiskar etc.) i serversystem som innehåller information om elektroniska identiteter (lösenordsuppgifter etc.) får ej säljas eller överlåtas. När hårdvaran tas ur drift skrivs lagringsmediet över samt destrueras.

4.2 Notices and User Information

4.2.1 Publicering av ansvarsförbindelse

På webbadressen https://www.du.se/aup finns Högskolan Dalarnas ansvarsförbindelse.

4.2.2 Godkännande av ansvarsförbindelse

Innan en elektronisk identitet lämnas ut måste ansvarsförbindelsen godkännas.

4.2.3 Godkännande av ändrad ansvarsförbindelse

Om ansvarsförbindelsen ändras meddelas samtliga innehavare av elektroniska identiteter. De har då en viss tid på sig att via portalen för identitetshantering godkänna den nya ansvarsförbindelsen. Om detta inte görs återkallas identiteten.

4.2.4 Lagring av godkännandet av ansvarsförbindelsen

Tidpunkt och andra data om godkännandet lagras i identitetshanteringssystemet.

4.2.5 Publicering av tjänstebeskrivning

På webbadressen https://www.du.se/saml2websso finns en tjänstedefinition (*service definition*) för federerad inloggning och attribututbyte med organisationer inom identitetsfederationen. På denna webbsida finns även information om högskolans integritetspolicy gällande elektroniska identiteter (*privacy policy*).

4.3 Secure Communications

4.3.1 Skydda hemligheter

All information rörande elektroniska identiteter lagras i högskolans identitetshanteringssystem.

All nätverkskommunikation till och från systemet är krypterad.

Endast de som har behov av tillgång till systemet i sin anställning har behörighet.

4.3.2 Skydda privata krypteringsnycklar

Alla krypteringsnycklar lagras på ett säkert sätt. Endast ett fåtal personer har tillgång till dessa.

4.3.3 Säker nätverkskommunikation

All kommunikation till och från identitetshanteringssystemet är krypterad med TLS.

4.3.4 Entitetsnycklar

Alla krypteringsnycklar som används i systemet är minst 2048 bitar. Detta inkluderar identitetsutgivaren (IdP).

4.4 Security-relevant Event (Audit) Records

4.4.1 Loggning av säkerhetsrelaterade händelser

Uppgifter om alla elektroniska identiteter som lämnas ut lagras i en logg, bland annat för att säkerställa att inget identitetsnamn återanvänds men även för spårbarhet. På samma sätt sparas

tidpunkt och händelsebeskrivning när attribut tillhörande en identitet förändras, inklusive lösenordsbyten.

Dessa och övriga händelser som är av relevans för upprätthållandet av identitetshanteringssystemet loggas på ett säkert sätt. Tillgång till dessa loggar är begränsade till ett fåtal personer med behörighet.

5 Operational Requirements

5.1 Credential Operating Environment

5.1.1 Autentisering

Inloggning sker med enfaktorinloggning eller multifaktorinloggning.

Lösenordet till den elektroniska identiteten måste uppfylla dessa krav:

- Minst 8 tecken långt
- Får ej innehålla mellanslag
- Måste innehålla tecken från minst tre av dessa grupper:
    - Gemener: a-z, ej ääö
    - Versaler: A-Z, ej ÅÄÖ
    - Siffror: 0–9
    - Specialtecken: - _ . ! % : = #

Vid identitetens skapande samt vid lösenordsbyte kontrolleras även att det inte kan återfinnas som ett ord eller del av ord i svenska och engelska ordlistor.

Internt inom högskolan används multifaktorinloggning med autentiseringsapp på mobiltelefon alternativt Yubikey (U2F). Alla student- och personalkonton har tvingande registrering av en multifaktor. Den huvudsakliga metoden som används är ”pushnotifiering med inmatningskrav”. I undantagsfall kan SMS användas. För viss inloggning krävs endast en faktor (användarnamn/lösenord) om inte inloggningsmekanismen signalerar ”misstänkt inloggning” vilket då aktiverar kravet på en andra faktor. För vissa typer av tjänster krävs alltid multifaktorinloggning. Exempel på sådana tjänster är VPN, logghantering, administrationsportaler etc.

5.1.2 Skydd av protokoll

Alla protokoll som används, exempelvis SAML, är skyddade mot s.k. *message replay*.

5.1.3 Skydd mot missbruk av inloggningsuppgifter

Innehavare av en elektronisk identitet förbinder sig (via ansvarsförbindelsen, se 4.2.2) att hålla lösenordet hemligt och att ej dela detta med någon annan. Andra typer av missbruk, exempelvis sabotage och försök till intrång i skyddade system, regleras också i ansvarsförbindelsen.

5.1.4 Hantering av säkerhetshot

I högskolans säkerhetsarbete ingår att hålla alla system uppdaterade med de senaste uppdateringarna från leverantör. Samtliga system skyddas av brandvägg. Förutom detta övervakas alla system inom identitetshantering av personal med särskild behörighet. För åtkomst till dessa övervakningssystem krävs multifaktorinloggning.

5.2 Credential Issuing

5.2.1 Identitetsutgivarens (IdP) DNS-domän

Högskolan Dalarnas DNS-domän är ”du.se”.

5.2.2 Unik identifierare för identitetsutgivare (IdP)
Högskolans identitetsutgivare (IdP) har en globalt unik identifierare (*entityID*).

5.2.3 Unik identifierare för elektronisk identitet
Alla elektroniska identiteter har en unik identifierare (användarnamn) som ej återanvänds (förutom om samma person återkommer till organisationen).

5.2.4 Val av identitet vid inloggning
Personer som har multipla elektroniska identiteter kan vid inloggning välja vilken som används.

5.2.5 Säkerställande av identitet vid utlämnande av inloggningsuppgifter
Högskolan Dalarna definierar ett antal olika identitetstyper. Rutinerna för utlämning av dessa varierar baserat på typ. Inte alla identitetstyper exponeras i SWAMID för federerad inloggning.

Vid kontroll av fysisk ID-handling godkänner högskolan följande:

- Identitetshandling godkänd av Polisen för utlämning av svenskt pass.
- Nationellt ID-kort inom EU.
- Utländskt pass.

Kontroll av ID-handling innefattar:

- ID-handlingens giltighet (äkta, godkänd och ej utgången).
- Namn
- Personnummer/födelsedatum
- Fotografi

Gemensamt för alla identitetstyper

Bekräftade (AL2) identiteter exponeras mot SWAMID. Obekräftade (AL1) identiteter exponeras ej mot SWAMID (se undantag gällande Ladok Student och Antagning under avsnittet ”Studentidentitet”).

Högskolan Dalarna arbetar kontinuerligt med att minska antalet obekräftade (AL1) identiteter.

Personalidentitet

Högskolans personal har i allmänhet alltid en elektronisk identitet tilldelad. För att denna skall utfärdas krävs en skriftlig rekvisition signerad av behörig person. Vid utlämnandet kontrolleras giltig ID-handling vilket uppfyller villkoren för utlämnande av en bekräftad (AL2) identitet. När anställningen upphör meddelar HR-avdelningen helpdesk som då avslutar den elektroniska identiteten. Förregistrerade identifierare är:

- Svenskt personnummer, interimspersonnummer eller samordningsnummer från HR-system.
- Namn och födelsedatum från HR-system om svenskt personnummer saknas.

Generellt sett är majoriteten av alla personalidentiteter bekräftade (AL2). Eventuella obekräftade (AL1) personalidentiteter exponeras ej mot SWAMID.

Studentidentitet

Studenter vid högskolan har rätt till en elektronisk identitet under sin studietid. Beroende på studerandeform hanteras tilldelningen på olika sätt. Gemensamt för alla är att identiteten automatiskt avslutas 12 månader efter sista undervisningsdatum (enligt Ladok), om ingen ny kursregistrering görs.

Det primära sättet för studenter att kvittera ut en elektronisk identitet är via en webbaserad portal. Beroende på vilken *identifikationsmetod* som används i portalen blir identiteten antingen obekräftad (AL1) eller bekräftad (AL2). Utlämnande kan även ske fysiskt via helpdesk.

- [Online] Extern identifikation via svensk e-legitimation på tillitsnivå 3 eller högre. Förregistrerad identifierare är svenskt personnummer. Utlämnad elektronisk identitet är alltid bekräftad (AL2).
- [Online] Extern identifikation via federerad (SWAMID) inloggning, exempelvis via antagning.se eller eduID.se. Tillitsnivån på kontot som används vid den externa identitetsutgivaren måste vara bekräftad (AL2). Identitetsutgivaren måste vara godkänd för SWAMID AL2. Kan endast användas av person med svenskt personnummer. Förregistrerad identifierare är svenskt personnummer. Utlämnad elektronisk identitet är alltid bekräftad (AL2).
- [Online] ID-nyckel, en genererad kod, som tillsammans med studentens svenska personnummer eller interimspersonnummer kan användas som identifikation. Om ID-nyckeln har skickats via brev till folkbokföringsadressen resulterar detta i en bekräftad (AL2) elektronisk identitet. Om ID-nyckeln har skickats via e-post resulterar detta i en obekräftad (AL1) elektronisk identitet. Vid användning av ID-nyckel måste ett s.k. CAPTCHA-test utföras. ID-nyckeln är tidsbegränsad och kan endast användas en gång. Förregistrerade identifierare är:
    - Svenskt personnummer eller interimspersonnummer från Ladok.
    - Namn och födelsedatum från Ladok om svenskt personnummer saknas.
    - Vid utskick via e-post, e-postadress i NyA eller Ladok.
- [Offline] Kontroll av giltig ID-handling i helpdesk. Utlämnad elektronisk identitet är alltid bekräftad (AL2). Förregistrerade identifierare är:
    - Svenskt personnummer eller interimspersonnummer från Ladok.
    - Namn och födelsedatum från Ladok om svenskt personnummer saknas.

Vid kontroll av giltig **utländsk** ID-handling i helpdesk sparas även namn, födelsedatum, utfärdandeland samt ID-handlingens nummer i identitetshanteringssystemet. Detta för att säkerställa identifiering enligt 5.3.3 och 5.4.2.

Obekräftade (AL1) studentidentiteter exponeras ej ut mot SWAMID förutom vid inloggning mot Ladok Student och Antagningen via högskolans identitetsutgivare (IdP).

Extern identitet

I den webbaserade lärplattformen finns det ibland ett behov av att involvera externa, dvs. ej anställda, personer som lärare. Dessa kan då tilldelas en externidentitet. Denna skapas av IT-avdelningen eller Helpdesk på begäran av kursansvarig. Kursansvarig ansvarar även för utlämnandet av identitetsuppgifterna, på godtyckligt sätt, vilket endast uppfyller kraven för obekräftad (AL1) identitet. Identiteten avslutas på ett av beställaren (kursansvarig) förutbestämt datum. Förregistrerade identifierare är:

- Svenskt personnummer om tillgängligt.
- E-postadress.

Externa identiteter exponeras ej mot SWAMID.

Serviceidentitet

Det finns i enstaka fall behov av att tilldela en identitet till en service eller funktion. Dessa identiteter markeras som obekräftade (AL1). En serviceidentitet tas bort manuellt när servicen/funktionen avvecklas. Lösenordsbyte är ej möjlig för denna identitetstyp.

Serviceidentiteter exponeras ej mot SWAMID.

Gästidentitet

Högskolans gäster, som på behöver komma åt en nätverkstjänst, trådlöst nät etc., kan tilldelas en gästidentitet under en kortare tidsperiod. Helpdesk, receptionerna, biblioteket etc. utfärdar dessa på begäran av beställaren (anställd vid högskolan som är värd för gästen). Beställaren ansvarar för utlämningen av uppgifterna. Identiteten, som markerats som obekräftad (AL1), avslutas på ett av beställaren förutbestämt datum. Lösenordsbyte är ej möjlig för denna identitetstyp.

Gästidentiteter exponeras ej mot SWAMID.

5.2.6 Ändring av tillitsnivå

Alla händelser som rör tillitsnivå för en elektronisk identitet loggas.

5.2.7 Ändring av angiven information

Information som innehavaren av en elektronisk identitet har angivit själv kan ändras antingen via källdatasystemets gränssnitt eller med hjälp av källdatasystemets systemansvarige.

5.2.8 Behörighet till identitetshanteringssystemet

Behörighet till identitetshanteringssystem tilldelas endast till personal som behöver detta i sin tjänst. Denna personal utbildas i dessa system innan behörigheten tilldelas. Samtliga innehar bekräftade (AL2) identiteter.

5.3 Credential Renewal and Re-issuing

5.3.1 Tillåt lösenordsbyte

Innehavaren av en elektronisk identitet kan närsomhelst byta det associerade lösenordet. Undantaget detta är om identiteten är inaktiverad (låst) eller återkallad (raderad).

5.3.2 Krav på kännedom om aktuellt lösenord vid byte

Vid lösenordsbyte måste innehavaren av en elektronisk identitet uppge det aktuella (gamla) lösenordet.

5.3.3 Utlämnande av uppgifter vid glömt lösenord

Om innehavaren av en elektronisk identitet har glömt lösenordet kan ett nytt erhållas via den webbaserade portalen för identitetshantering. För att identifiera sig behöver innehavaren använda någon av de metoder som angivits i 5.2.5.

De förregistrerade identifierare som angivits i 5.2.5 kontrolleras.

- Svenskt personnummer vid användande av extern identifikation via svensk e-legitimation på tillitsnivå 3 eller högre. Gäller personal- och studentidentiteter med svenskt personnummer.
- Svenskt personnummer vid användande av extern identifikation via SWAMID. Gäller personal- och studentidentiteter med svenskt personnummer. (Observera att endast AL2-konton med svenskt personnummer vid den externa identitetsutgivaren kan användas)
- Svenskt personnummer eller interimspersonnummer, namn och födelsedatum från Ladok vid användande av ID-nyckel. Vid e-postutskick gäller den e-postadress som registrerades vid utlämnandet (källa: NyA eller Ladok). Gäller studentidentitet.
  Svenskt personnummer eller interimspersonnummer, namn och födelsedatum från Ladok (alternativt HR-system för personalidentitet) vid fysisk kontroll av ID-handling i helpdesk.

Sparade uppgifter från tidigare använd ID-handling (namn, födelsedatum, utfärdandeland samt ID-handlingsnummer) kontrolleras också. Om en ny ID-handling har utfärdats skall namn, födelsedatum och utfärdandeland överensstämma. Information om den nya ID-handlingen sparas i systemet. Gäller personal- och studentidentitet.

5.4 Credential Revocation

5.4.1 Återkallande av elektronisk identitet

Automatiserat återkallande, eller *radering*, av en elektronisk identitet sker olika beroende på identitetstyp. Se 5.2.5.

Administratörer i identitetshanteringssystemet kan närsomhelst återkalla en identitet.

Identiteten kan återkallas på begäran av innehavaren.

5.4.2 Utlämnande av uppgifter efter återkallning

En personal- eller studentidentitet kan återställas i identitetshanteringssystemet inom 30 dagar från det att den återkallades. Då återställs alla data inklusive lösenord (hash). Detta får endast göras om återkallningen gjordes automatiskt (avslutad anställning eller avslutade studier). Alla andra anledningar, exempelvis säkerhetsrelaterade, kräver manuell handläggning och återställning.

Vid återställning efter säkerhetsrelaterad incident, informeras innehavaren först om vad som har hänt och hur detta skall undvikas i framtiden, sedan kan återställning göras.

Vid manuell återställning krävs att ett nytt lösenord lämnas ut, identifiering enligt 5.3.3.

5.4.3 Återkallande av elektronisk identitet vid säkerhetsrelaterad incident

Personal som arbetar med IT-säkerhet vid högskolan beslutar om vidare utredning och eskalering behövs.

5.5 Credential Status Management

5.5.1 Register över elektroniska identiteter

Uppgifter om alla elektroniska identiteter som lämnas ut lagras i en logg, bland annat för att säkerställa att inget identitetsnamn återanvänds men även för spårbarhet. På samma sätt sparas tidpunkt och händelsebeskrivning när attribut tillhörande en identitet förändras, inklusive lösenordsbyten.

Dessa och övriga händelser som är av relevans för upprätthållandet av identitetshanteringssystemet loggas på ett säkert sätt. Tillgång till dessa loggar är begränsade till ett fåtal personer med behörighet.

5.5.2 Tillgänglighet för identitetsutgivare (IdP)

Tillgängligheten på högskolans identitetsutgivare (IdP) och underliggande system är tillräcklig för intern användning. Ingen formell SLA finns upprättad men dessa system bedöms vara verksamhetskritiska och hanteras således med högsta prioritet.

5.6 Credential Validation/Authentication

5.6.1 Validering av inloggningsuppgifter

Högskolan Dalarnas identitetsutgivare (IdP) följer SWAMID:s rekommendationer och *best practices*.

5.6.2 Tillåt ej inloggning med återkallad identitet

Inloggning är ej möjlig med återkallad elektronisk identitet.

5.6.3 Kräv inloggningsuppgifter vid inloggning

Följande krävs för att kunna logga in mot en tjänst:

- Giltig SSO-biljett
- Användarnamn och lösenord
- En andra faktor i tillämpbara fall

5.6.4 Aktiv session

En SSO-session är endast giltig i 12 timmar från det att sessionen skapades.