HÖGSKOLAN DALARNA

HANDLÄGGNINGSORDNING

Gäller från och med
2016-11-21

Beslutat av
Rektor

Diarienummer
C 2022/729

Handläggningsordning för hantering av elektroniska identiteter

Inledning

Elektroniska identiteter används dagligen vid Högskolan Dalarna för en rad olika tjänster. De primära användningsområdena är:

- **Autentisering och auktorisation**
  T ex inloggning på dator eller mot en tjänst (autentisering). Vad personen har rätt att göra på datorn/tjänsten bestäms också utifrån identiteten (auktorisation).
- **Identifikation/signatur**
  T ex markeras (signeras) en inlämningsuppgift i den webbaserade lärplattformen med studentens identitet för att läraren skall veta vem som har lämnat in arbetet.

Vilka elektroniska tjänster en person har tillgång till baseras ofta på *identitetstyp*, t ex ”personal”, ”student” osv. Dock begränsas även tjänsteutbudet av hur stort förtroende högskolan har för en individuell identitet. Det är därför nödvändigt att klassificera identiteter i s.k. *förtroendenivåer*.

Förtroendenivåer

Förtroendenivåer på Högskolan Dalarna beskriver hur väl en identitet kan säkerställas tillhöra en viss person med fokus på hur överlämnandet har gått till.

Tidigare användes begreppet LoA (Level of Assurance) för att beskriva förtroendenivåer. Dessa nivåer (LoA 1 till 3) ersätts med begreppen **obekräftad** (LoA 1) och **bekräftad** (LoA 2-3) identitet.

Identitetstyper

På Högskolan Dalarna finns ett antal identitetstyper definierade. Nedan följer en beskrivning av dessa, hur de relaterar till förtroendenivåer och hur utgivningen går till. Samtliga identitetstyper gäller för DNS-domänen **du.se**.

Personalidentitet

Högskolans personal har i allmänhet alltid en elektronisk identitet tilldelad. För att denna skall utfärdas krävs en skriftlig rekvisition signerad av prefekt/avdelningschef eller motsvarande. Vid utlämnandet kontrolleras giltig ID-handling, t ex körkort, vilket uppfyller villkoren för **bekräftad** identitet. När anställningen upphör meddelar personalavdelningen Högskolans helpdesk som då avslutar den elektroniska identiteten.

Externidentitet

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** identitet. Identiteten avslutas på ett av beställaren (kursansvarig) förutbestämt datum.

Studentidentitet

Studenter vid högskolan har rätt till en elektronisk identitet under sin studietid. Beroende på studerandeform hanteras tilldelningen på olika sätt.12 månader efter sista undervisningsdag blir identiteten kandidat för automatisk radering. Studenten meddelas via ett antal kanaler och fyra veckor senare tas identiteten automatiskt bort, förutsatt att ingen ny antagning/registrering gjorts.

Det primära sättet för studenter att kvittera ut en elektronisk identitet är via en webbaserad portal. Där går det även att skaffa ett nytt lösenord till sin identitet samt i vissa fall höja förtroendenivån från obekräftad till bekräftad.

Beroende på vilken *identifikationsmetod* som används på portalen blir identiteten antingen **obekräftad** eller **bekräftad**.

Identifikationsmetoder i portalen

- **Extern identifikation** via federerad (SWAMID) inloggning, exempelvis via **antagning.se** eller **eduID.se**. Förtroendenivån på kontot som används vid den externa identitetsutgivaren måste vara bekräftat.
- **ID-nyckel**, dvs. en genererad kod, som tillsammans med studentens personnummer kan användas som identifikation. Om ID-nyckeln har skickats via brev till folkbokföringsadressen anses sessionen vara bekräftad (och resulterar t.ex. i en bekräftad elektronisk identitet). Om ID-nyckeln har skickats via e-post anses sessionen vara obekräftad (och resulterar t.ex. i en obekräftad elektronisk identitet). Vid användning av ID-nyckel måste ett s.k. CAPTCHA-test utföras.

Andra identifikationsmetoder

- Utlämning av en elektronisk identitet, lösenordsbyte samt höjning av förtroendenivån kan göras i helpdesk efter kontroll av giltig ID-handling.

Serviceidentitet

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

Gästidentitet

Högskolans gäster, som på behöver komma åt en nätverkstjänst, trådlöst nät etc., kan tilldelas en gästidentitet. 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**, avslutas på ett av beställaren förutbestämt datum. Lösenordsbyte är ej möjlig för denna identitetstyp.

Sammanfattning av identitetstyper

Nedan följer en sammanfattning av hur varje identitetstyp relaterar till förtroendenivå samt om identitetstypen publiceras i SWAMID[1] eller inte. Huruvida en ansvarsförbindelse har signerats anges i kolumnen ”ansv.förb.”.

Identitetstyp	**Förtroendenivå**	**SWAMID**	**Ansv.förb.**
Personalidentitet	Bekräftad	Ja	Ja
Externidentitet	Obekräftad	Nej	Nej
Studentidentitet	Varierande	Ja (för bekräftade identiteter)	Ja
Serviceidentitet	Obekräftad	Nej	Nej
Gästidentitet	Obekräftad	Nej	Nej

Låsning och tvingande lösenordsbyte

Om en elektronisk identitet har kompromitterats (t.ex. om lösenordet finns att tillgå i någon form av lösenordsdatabas på webben) låses identiteten omedelbart. För att låsa upp identiteten igen måste ett nytt lösenord erhållas antingen via webbportalen eller via besök i helpdesk.

Allmänt

Lag

Högskolan Dalarna är en statlig utbildningsmyndighet vilket gör att högskolans verksamhet regleras i lagar, förordningar och regleringsbrev. De viktigaste lagarna och förordningarna som styr högskolans arbete är regeringsformen (1974:152), myndighetsförordningen (2007:515), högskolelagen (1992:1434) och högskoleförordningen (1993:100). Regleringsbrevet utställs årligen av regeringen och styr högskolans uppdrag under ett kalenderår. I övrigt följer högskolan Sveriges övriga lagar och förordningar.

Högskolan Dalarnas katalog- och behörighetssystem innehåller uppgifter om högskolans organisation samt personuppgifter om alla som är verksamma vid högskolan. Med avseende på detta måste särskild hänsyn till behandlingen av personuppgifter tas. Personuppgiftslagen (1998:204) och offentlighets- och sekretesslagen (2009:400) reglerar behandlingen av personuppgifter samt hantering av personer med behov av skyddade personuppgifter. Högskolan Dalarna följer Skatteverkets vägledning för hantering av sekretessmarkerade personuppgifter i offentlig förvaltning[2].

Studenters personuppgifter hämtas ur högskolans studiedokumentationssystem Ladok och därför gäller även förordning (1993:1153) om redovisning av studier m.m. vid universitet och högskolor vid hantering av studenters personuppgifter i katalog- och behörighetssystemet.

Som statlig myndighet arbetar Högskolan Dalarna även med ledningssystem för informationssäkerhet enligt Myndigheten för samhällsskydd och beredskapsföreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2009:10).

---

[1] Swedish Academic Identity. Identitetsfederation för universitet och högskolor i Sverige.

[2] https://www.skatteverket.se/offentligaaktorer/informationsutbyte/folkbokforingsekretessmarkeradepersonuppgifter.4.18e1b10334ebe8bc80002541.html

Säkerhet

Behörighet till identitetshanteringssystem

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 identiteter.

Krypterad kommunikation

Alla krypteringsnycklar lagras på ett säkert sätt. Endast ett fåtal personer med behörighet har tillgång till dessa nycklar. Alla nycklar är av typen 2048 bitar eller högre.

All kommunikation mellan de system som hanterar elektroniska identiteter görs över krypterade förbindelser, antingen genom inbyggt stöd i protokollet eller med hjälp av IPsec.

Lösenordshantering

Vid utlämnandet av en elektronisk identitet skapas ett slumpgenererat lösenord som uppfyller de krav som ställs (minst 8 tecken, komplext lösenord). Detta lösenord kan bytas på högskolans webbplats. Vid bytet kontrolleras att innehavaren av den elektroniska identiteten känner till sitt nuvarande lösenord. Det sker även en kontroll att gällande lösenordsregler efterföljs (i den mån det går att maskinellt kontrollera detta).

Innehavare av studentidentiteter kan återställa sitt lösenord (dvs. erhålla ett slumpgenererat lösenord) via webbportalen. Personal som önskar återställa sitt lösenord måste besöka helpdesk.

Loggning

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.

Utrangering av hårdvara och lagringsmedia

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

Ansvarsförbindelse

Innehavare av vissa identitetstyper (bland annat de som publiceras i identitetsfederationen SWAMID) har samtliga signerat en ansvarsförbindelse vid överlämnandet. Denna finns alltid att tillgå på webbadressen https://www.du.se/aup. Tidpunkt och andra data om signeringen lagras i identitetshanteringssystemet.

Om ansvarsförbindelsen förändras meddelas detta via e-post till samtliga innehavare av elektroniska identiteter. De meddelas även via student- och personalportalerna.

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*).

Medlemskap i SWAMID

För medlemskap i SWAMID krävs att deras policys efterföljs. Förutom SWAMID Federation Policy finns ett antal *tillitsprofiler*:

- SWAMID Identity Assurance Level 1 Profile
  https://wiki.sunet.se/display/SWAMID/Identity+Assurance+Level+1+Profile
- SWAMID Identity Assurance Level 2 Profile
  https://wiki.sunet.se/display/SWAMID/Identity+Assurance+Level+2+Profile
- SWAMID Identity Assurance Level 3 Profile
  https://wiki.sunet.se/display/SWAMID/Identity+Assurance+Level+3+Profile

Högskolan Dalarna uppfyller kraven för Identity Assurance Level 2. Detta inkluderar att högskolan följer de rekommendationer som SWAMID har satt upp gällande interaktion mellan de lokala systemen och externa system i federationen.

Högskolan Dalarna ämnar på sikt att uppfylla Identity Assurance Level 3.

Identity Management Practice Statement (IMPS)

Detta dokument skall användas som Högskolan Dalarnas IMPS. Som en del av medlemskapet i SWAMID krävs att högskolan årligen bekräftar till SWAMID att dokumentet fortfarande är giltigt. Om denna handläggningsordning uppdateras skall SWAMID ta del av denna och godkänna medlemskapet på nytt.