

Peter Falck  
IT-sektionen

+46 21 101499 (mobile extension)  
peter.falck@mdh.se

## Elektroniska identiteter vid Mälardalens högskola

**Detta dokument beskriver vilka elektroniska identiteter som används vid Mälardalens högskola samt definierar identiteternas förtroendenivåer.**

Förtroendenivåerna som används i detta dokument bygger på NIST Electronic Authentication Guideline Version 1.0.2<sup>1</sup>.

### Definition av förtroendenivåer

I NIST Electronic Authentication Guideline definieras fyra förtroendenivåer - eng. Level of Assurance, nedan förkortat LoA. I bedömningen av förtroendenivå ingår dels hur väl en identitet kan säkerställas tillhöra en viss person vid utlämnandet av identiteten och dels med vilken metod som autentisering - även kallat inloggning - kan ske.

I detta PM bedöms bara förtroendenivåer med utgångspunkt i med vilken säkerhet utlämnaren av en elektronisk identitet kan verifiera mottagarens identitet. Vid överlämnandet av identiteten överlämnas även ansvaret för att endast avsedd användare brukar identiteten. Användaren bär sedan ansvaret för att rapportera in förlust av kontouppgifter och andra händelser som kan medföra att användaren inte längre kan garantera suveränitet över kontouppgifterna.

En identitet med högre förtroendenivå uppfyller även kraven för en lägre, det vill säga en identitet som uppfyller LoA2 uppfyller även LoA1.

#### LoA1 - obekräftad användare

LoA1 innebär att det finns liten eller ingen möjlighet att fastställa vem som tar emot en elektronisk identitet.

#### LoA2 - bekräftad användare

LoA2 innebär att det finns rimlig eller viss möjlighet att fastställa vem som tar emot en elektronisk identitet. Vem som tar emot identiteten fastställs genom att identiteten styrks vid utlämnande av identitetsinformation eller att identitetsinformationen skickas till en postadress – till exempel folkbokföringsadressen eller arbetsplatsens adress – där det är stor

<sup>1</sup> NIST Special Publication 800-63 Version 1.0.2, Electronic Authentication guideline, april 2006, [http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1\\_0\\_2.pdf](http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf)

Peter Falck  
IT-sektionen

+46 21 101499 (mobile extension)  
peter.falck@mdh.se

sannolikhet att den person som identitetsinformationen tillhör även är den person som tar del av den informationen.

### LoA3 - kontrollerad användare

LoA3 innebär att det finns god möjlighet att fastställa vem som tar emot en elektronisk identitet. Detta säkerställs via kontroll av giltig identitetshandling vid utlämnade av identitetsinformation. Med giltig identitetshandling menas nationellt identitetskort, pass, körkort, SIS-godkänt identitetskort och e-legitimation.

### LoA4 - verifierad användare

LoA4 innebär att det finns mycket god möjlighet att fastställa vem som tar emot en elektronisk identitet. Med avseende på att detta PM är begränsat till identitetshantering är det ingen skillnad mellan LoA3 och LoA4.

## Förtroendenivåer för högskolans identitetstyper

Följande tabell innehåller de identitetstyper som används vid Mälardalens högskola, vilken förtroendenivå som kan garanteras för identitetstypen samt vilka användningsområden med särskilda krav som identitetstypen kan komma att användas inom.

Identitetstyp	Förtroendenivå	SWAMID
Personalkonto	LoA2	Ja
Personalkonto med personligt certifikat	LoA3	Ja
Studentkonto	LoA3	Ja
Uppdragskonto	LoA2	Ja
Företagskonto	LoA1	Nej
Bibliotekskonto	LoA2	Nej

## Identitetstyper

Detta avsnitt beskriver närmare de olika elektroniska identiteter som skapas, delas ut och används vid Mälardalens högskola.

### Personalkonto

Personal vid Mälardalens högskola har möjlighet att ha en elektronisk identitet i form av ett användarkonto under sin anställning vid högskolan. Som personal räknas i det här fallet de typer av formella anställningar av olika slag där personen finns aktiv i högskolans personaldatabas.

Peter Falck  
IT-sektionen

+46 21 101499 (mobile extension)  
peter.falck@mdh.se

Kontot kan lämnas ut till den anställda på flera sätt. Antingen genom att ett förseglat kuvert skickas med internpost till mottagarens postadress vid högskolan eller genom att personal anställd vid mottagarens akademi som fått kontohanteringsfunktionen delegerad till sig lämnar ut kontouppgifterna personligen till den anställda.

Personalkontot inaktiveras automatiskt i samband med att personens anställning upphör enligt vad som finns angivet i personaldatabasen.

### **Personalkonto med personligt certifikat**

Möjlighet finns för personal att hämta ut ett personligt certifikat. För att detta skall vara möjligt måste manuell kontroll av identitetshandling genomföras. Den manuella kontrollen sker av helpdesk och efter kontrollen sätts ett attribut i katalogtjänsten som talar om att kontrollen är genomförd.

Kontrollen ska innefatta:

- Legitimationshandlingen är äkta (ej förfalskad) och godkänd
- Legitimationshandlingen är giltig (kontrollera utgångsdatum)
- Legitimationshandlingen tillhör personen som visar upp den för kontroll

### **Studentkonto**

Samtliga studenter vid Mälardalens högskola har möjlighet att ha en elektronisk identitet i form av ett användarkonto så länge som de är aktivt studerande vid högskolan. Med aktivt studerande menas att studenten är registrerad i LADOK på minst en kurs under innevarande termin eller att studenten har varit registrerad på minst en kurs högst tre terminer tillbaka i tiden. Studenten har möjlighet att vara icke registrerad för till exempel utlandsstudier inom utbildningen i upp till tre terminer innan kontot inaktiveras.

Personal vid högskolans informationsdiskar lämnar ut studentkontot med förbindelsesida direkt till mottagaren för studenter som är anmälda till utbildningsprogram. Detta sker i samband med att studenten registrerar sig på programmet. Vid utlämnandet kontrolleras giltig identitetshandling.

Studenter registrerade på enskilda kurser hämtar ut studentkontot med förbindelsesida från sekreterare vid högskolans utbildningsakademier. Vid utlämnandet kontrolleras giltig identitetshandling.

Studentkonton inaktiveras med automatik vid terminsstart tre terminer efter det att studenten avslutat sitt senaste registrerade kurstillfälle i LADOK.

Peter Falck  
IT-sektionen

+46 21 101499 (mobile extension)  
peter.falck@mdh.se

### **Uppdragskonto**

Uppdragskonton tilldelas personer med informella eller tillfälliga uppdrag. Till personer som är berättigade till uppdragskonton räknas även personer som av akademichefer och motsvarande anses vara verksamma vid en akademi eller liknande och som därför kan anses ha anställningsliknande förhållanden. Dessa personer finns aktiva i personaldatabasen under anställningstiden.

Ansvar för att dela ut uppdragskonton till mottagare är delegerat av akademichef eller administrativ chef på akademi eller motsvarande till en vid högskolan anställd person, vanligen en akademisekreterare. Kontot kan delas ut personligen direkt till mottagaren, med eller utan krav på legitimering, eller genom att kontouppgifterna skickas i förseglat kuvert med intern postgång till mottagarens adress på högskolan.

Uppdragskontot inaktiveras automatiskt i samband med att personens uppdrag upphör enligt vad som finns angivet i personaldatabasen.

### **Företagskonto**

Företagskonton lämnas ut till besökare från företag, organisationer och motsvarande i samband med enskilda företagsmässor, utställningar och liknande händelser vid högskolan. Kontot ger begränsad åtkomst till internetanslutning via högskolans nätverk.

Kontot kan genereras i samband med utlämningstillfället och skapas i dessa fall av personal vid högskolans informationsdiskar vid förfrågan. Utlämnandet sker via direktöverlämning till mottagaren med eller utan krav på legitimering. Kontot har begränsad giltighetstid på mellan 1-14 dygn som sätts vid skapandet av kontot.

Kontot kan även genereras i förväg av personal vid högskolans IT-sektion. Därefter överlämnas kontouppgifterna i dessa fall till den person, vanligtvis personal eller student vid högskolan, som utsetts som ansvarig för kontohantering för mässan eller utställningen. Kontot har begränsad giltighetstid som bestäms vid skapandet av kontot.

Företagskontot inaktiveras automatiskt när giltighetstiden för kontot gått ut.

### **Bibliotekskonto**

Bibliotekskonton är användbara för inloggning på ett begränsat antal datorer i högskolans bibliotek och kan användas för åtkomst till biblioteksresurser. Kontot ger också begränsad åtkomst till internetanslutning via högskolans nätverk. Besökare till biblioteket kan begära ut dessa konton som är tidsbegränsade till 1-7 dygn.

Peter Falck  
IT-sektionen

+46 21 101499 (mobile extension)  
peter.falck@mdh.se

Kontot genereras på plats i samband med utlämningstillfället av bibliotekspersonalen och lämnas direkt till mottagaren. Vid utlämnandet kontrolleras giltig identitetshandling.

Kontot inaktiveras automatiskt när giltighetstiden gått ut.

### Externa användningsområden

Här följer beskrivningar av vilka särskilda krav som ställs på Mälardalens högskolas identitetstyper för att de ska vara godkända att användas inom nedan namngivna användningsområden.

Peter Falck  
IT-sektionen

+46 21 101499 (mobile extension)  
peter.falck@mdh.se

## **SWAMID<sup>2</sup>**

Ett konto som är markerat för SWAMID-användning i detta dokument kan komma att användas för att verifiera användaridentitet inom SWAMID-samarbetet. Identiteten kommer därför att kunna användas av högskolans användare hos övriga medlemmar i SWAMID via de teknologisamarbeten inom SWAMID som Mälardalens högskola deltar i.

Uppdateringar av detta dokument måste meddelas till SWAMID.

Följande krav ställs på identitetstyper för att de ska tillåtas vara aktiverade inom SWAMID-samarbetet:

- Identitetstypen måste uppfylla LoA2<sup>3</sup> eller högre.
- Användaren av identitetstypen måste tillhöra Mälardalens högskola, antingen i egenskap av personal, student eller annan person med grundläggande rättigheter inom högskolan (exempelvis e-postadress för domänen mdh.se eller sanktionerat användarkonto) och som associeras med någon typ av aktivt deltagande i högskolan som organisation.

---

<sup>2</sup> <http://www.swamid.se/>

<sup>3</sup> <http://www.swamid.se/content/1/c6/01/06/13/swamid-policy-1.0.pdf>