Elektroniska identiteter vid Högskolan i Borås

Revisionshistorik

Datum	**Revision**	Fastställt av
2009-06-15	Fastställande av dokument	IT-chef
2012-10-26	Reviderat med hänsyn till ändrad kontoprocess via HBKAT samt SWAMID 2.0	IT-chef
2012-11-14	Reviderat efter synpunkter från SWAMID operations	IT-chef

Elektroniska identiteter vid Högskolan i Borås

Dokumentet beskriver de olika typer av elektroniska identiteter som finns i katalogtjänsten vid Högskolan i Borås (HB). Dokumentets syfte är att

- kortfattat beskriva högskolans identitetstyper
- definiera identitetstypernas förtroendenivå enligt NIST[1] och OMB M-04-04[2]
- utgöra underlag för högskolans medlemskap i Swedish Academic Identity Federation – nedan kallad SWAMID[3]

1. Förtroendenivåer

I NIST och OMB M-04-04 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 och dels med vilken metod autentisering – även kallat inloggning – kan ske. I detta dokument är det bara säkerställandet att en viss identitet tillhör en viss person som bedöms. Inom ramen för denna begränsning uppfyller en identitet med en högre förtroendenivå även kraven för en lägre, d.v.s. en identitet som uppfyller LoA2 uppfyller även LoA1.

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

LoA2 innebär att det finns rimlig eller viss möjlighet att fastställa vem som innehar och använder en elektronisk identitet. Vem som innehar identiteten fastställs genom att identiteten styrks vid utlämnande av identitetsinformation eller att informationen skickas till en postadress – t ex. folkbokföringsadressen eller för personal arbetsplatsens adress – där det är stor sannolikhet att den person som identitetsinformationen tillhör även är den person som tar del av den informationen. Med identitetsinformation menas bland annat inloggningsuppgifter.

LoA3 innebär att det finns god möjlighet att fastställa vem som innehar och använder en elektronisk identitet. Vem som innehar identiteten säkerställs via kontroll av giltig identitetshandling vid utlämnandet av identitetsinformation. Med giltig identitetshandling menas nationellt identitetskort, pass, körkort, SIS-godkänt identitetskort och e-legitimation[4].

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

---

[1] NIST Special Publication 800-63-1, Electronic Authentication Guideline, december 2011, http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf

[2] Executive Office of the President, Office of Management and Budget Memorandum M-04-04, E-Authentication Guidance for Federal Agencies, 16 december 2003, http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

[3] SWAMID, http://www.swamid.se

[4] Nämnden för elektronisk förvaltning, 24-timmarsdelegationen, E-legitimation för säkra e-tjänster , februari 2005, http://www.verva.se/web/t/Publication____1346.aspx

2. Kontoadministration och verktyg vid högskolan

En ny metakatalog samt nytt kontoadministrationsverktyg HBKAT utvecklas etappvis vid högskolan och implementeras stegvis under tiden 2012 till 2013. I samband med att det nya systemet togs i drift genomfördes en översyn och utveckling av processer och rutiner för kontoadministration. För närvarande hanteras personalidentiteter, externidentiteter, gästidentiteter och besöksidentiteter i HBKAT. Dessa identiteter har migrerats in i det nya systemet, övriga hanteras som beskrivet under respektive identitetstyp i avsnitt 4.

3. SWAMIDs relation till förtroendenivåer

För att en identitet ska få delta i identitetsfederationen SWAMID krävs att det inte finns något som hindrar att identiteten kan uppfylla LoA2.

4. HBs relation till förtroendenivåer

Nedan följer en beskrivning av identitetstyper i katalogtjänsten vid HB inklusive förtroendenivåklassificering och definition av eventuellt deltagande i SWAMID. En sammanfattning redovisas i tabellen som följs av en längre beskrivning.

Identitetstyp	Förtroendenivå	SWAMID
Personalidentitet	LoA2	Ja
Studentidentitet	LoA2	Ja
Externidentitet	LoA2	Ja
Funktionsidentitet	LoA1	Nej
Gästidentitet	LoA1	Nej
Besöksidentitet	LoA1	Nej
Maskin/systemidentitet	LoA1	Nej

4.1. Personalidentitet

Denna identitetstyp omfattar följande kategorier:
- personal under den period de är anställda vid högskolan
- doktorander under den period de innehar doktorandtjänst vid högskolan
- personer som av avdelningschef eller motsvarande anses vara verksam vid högskolan utan att inneha en formell anställning – s.k. person med anställnings-liknande förhållande

4.1.1. Kontoprocess

4.1.1.1 Fast anställning registrerad via personalsystemet

När personaladministratör registrerar en anställning i personalsystemet fångar identitetshanteringssystemet upp detta och lägger upp motsvarande information i metakatalogen. Nytt datakonto, hemkatalog och e-post skapas. Grundrättigheter tilldelas automatiskt beroende på organisationstillhörighet.
Information om kontot skickas via e-post till sponsor[5] för den nyanställdes organisation som via ett webbgränssnitt genererar temporärt lösenord. Inloggningsuppgifterna lämnas ut på papper efter id-kontroll och signatur på ansvarsförbindelse. Vid inloggning med temporärt lösenord tvingar systemet användaren att byta lösenordet. Aktivering och inaktivering av konto baseras på anställningsstatus i personalsystemet. När anställningen upphör skickas information om att kontot kan komma att stängas till sponsorn och den anställde.
30 dagar efter anställningens utgång stängs användarens konto och associerade e-postadress. Om fast anställning övergår till aktiv timanställning registrerad i HBKAT öppnas/förblir kontot öppet till och med registrerat slutdatum + 30 dagar.
160 dagar efter stängningen raderas kontot och brevlåda.
Kontonamn är kopplat till person-/idnummer och kan bara återanvändas av samma person om denne återkommer till organisationen.

Lösenordsåterställning görs via ett personligt besök hos IT-avdelningen som, efter legitimationskontroll, genererar ett temporärt lösenord som måste bytas vid nästa inloggning.

4.1.1.2 Manuell anställningsregistrering via HBKAT

Sponsor[5] registrerar anställning för timanställd med startdatum och slutdatum för tjänsten i HBKAT. I övrigt enligt 4.1.1.1. Om timanställning övergår till fast anställning som registreras i personalsystemet så associerar HBKAT detta automatiskt.

4.1.2. LoA-nivå

LoA2 uppnås vid kontoskapandet genom att identitet styrks vid det personliga mötet mellan sponsor[5] och nyanställd. Innehavaren kan identifieras över tiden genom att innehavarens personnummer, land/pass-nummer eller officiellt accepterad id-handling registreras och lagras.

[5] Sponsor är en av enhetschef eller motsvarande utsedd person att hantera anställningsinformationen i HBKAT

4.2. Studentidentitet

Denna identitetstyp omfattar följande kategorier:

- Studenter som är aktivt studerande vid högskolan.
  Med aktivt studerande menas att den studerande är registrerad på kurs, utbytesstudier eller har resultatregistrering på en kurs innevarande termin. Som aktiv student räknas också studenter utan registrering som har delmoment kvar eller betraktas vara färdig med sin utbildning under en övergångstid på högst 4 månader efter terminsslut.
- studenter som inte är aktivt studerande vid högskolan kan behålla sin identitet
  a) då de innehar ett arvoderat förtroendeuppdrag i studentkår eller annan studentorganisation underställd studentkåren
  b) vid tidsbegränsat studieuppehåll för återhämtningsstudier samt vid tidsbegränsat studieuppehåll av annan anledning efter individuell prövning

4.2.1. Kontoprocess

Studenter som antagits via Antagning.se får anvisningar hemskickade för att registrera sig och skapa sitt konto med hjälp av sin inloggning på Antagning.se (NyA IdP). Övriga studenter får en folder med en aktiveringskod i ett personligt möte med studieadministrativ personal eller om möjligt skickade till sin svenska folkbokföringsadress.
Vid aktivering i webbgränssnittet sker en kontroll mot Ladok att studenten är registrerad innan kontot kan aktiveras. Efter aktivering och godkännande av ansvarsförbindelse skapas automatiskt konto, hemkatalog och e-post samtidigt som aktuella behörigheter tilldelas kontot. Kontots behörigheter sätts utifrån de kurser eller program som finns registrerade i Ladok.

Förändringar hanteras genom att studentens behörigheter kontinuerligt jämförs med Ladok och vid ändrade kurser eller program i Ladok ändras kontots behörighet med automatik. Borttagning av studentkonto sker automatiserat. Då studenten enligt Ladok inte har någon registrering låses kontot efter en övergångstid från terminsslut på högst 4 månader, sedan tas kontot bort efter ytterligare 6 månader. Studentkontonamn återanvänds inte, om samma student återkommer efter raderingen provisioneras ett nytt konto.

Lösenordsåterställning görs via webbgränssnitt med hjälp av NyA IdP eller genom ett personligt besök hos IT-avdelningen som, efter legitimationskontroll, genererar ett temporärt lösenord som måste bytas vid nästa inloggning.

4.2.2. LoA-nivå

LoA2 uppnås vid kontoskapandet genom aktivering av konto via NyA IdP eller genom att identitet styrks vid upprop eller vid personligt möte mellan student och studieadministrativ personal. Innehavaren kan identifieras över tiden genom att innehavarens personnummer, land/pass-nummer eller officiellt accepterad id-handling registreras och lagras.

4.3. Externidentitet

Denna identitetstyp omfattar följande kategori:

- individuellt konto för externer, som inte uppfyller villkoren för en personal- eller studentidentitet, där behov av konto föreligger för verksamhet vid högskolan under en längre tid eller med annan behörighet än vad som tillhandahålls med gästkonto. Exempel på innehavare kan vara externa projektdeltagare, konsulter etc.
- personal vid Studentkåren eller annan studentorganisation underställd Studentkåren

.

4.3.1. Kontoprocess

Enhetschef eller motsvarande anmäler behov av identitet via ett formulär till IT-avdelningen.
IT-avdelningen registrerar användarinformation, start- samt sluttid i HBKAT som provisionerar nytt datakonto, hemkatalog och e-post. Grundrättigheter tilldelas automatiskt beroende på organisationstillhörighet.
Information om kontot skickas via e-post till sponsor[5] som via ett webbgränssnitt genererar temporärt lösenord. Inloggningsuppgifterna lämnas ut på papper efter id-kontroll och signatur på ansvarsförbindelse. Vid inloggning med temporärt lösenord tvingar systemet användaren att byta lösenord.
30 dagar innan kontots sluttid skickas information om att kontot kan komma att stängas till sponsor och kontoinnehavare.
Användarens konto och associerade e-postadress raderas 160 dagar efter stängningen.
Kontonamn är kopplat till person-/idnummer och kan bara återanvändas av samma person om denne återkommer till organisationen.

4.3.2. LoA-nivå

LoA2 uppnås vid kontoskapandet genom att identitet styrks vid det personliga mötet mellan sponsor och användare. Innehavaren kan identifieras över tiden genom att innehavarens personnummer, land/pass-nummer eller officiellt accepterad id-handling registreras och lagras.

Lösenordsåterställning görs genom ett personligt besök hos IT-avdelningen som efter legitimationskontroll genererar ett temporärt lösenord som måste bytas vid nästa inloggning.

4.4. Funktionsidentitet

Denna identitetstyp omfattar följande kategorier:

- avdelningar och funktioner vid högskolan med behov av konto/e-post där flera personer delar på eller har tillgång till samma konto/e-post
- funktioner vid högskolan där funktionens varaktighet är längre än den enskilda individens engagemang i funktionen vilket innebär att innehavaren av konto/ e-post växlar över tiden
- avdelningar och funktioner vid studentkår, studentorganisation underställd studentkåren och annan av högskolan godkänd studentorganisation med behov av konto/e-post där flera personer delar på eller har tillgång till samma konto/e-post
- funktioner inom studentkår, studentorganisation underställd studentkåren och annan av högskolan godkänd studentorganisation där funktionens varaktighet är längre än den enskilda individens engagemang i funktionen vilket innebär att innehavaren av konto/e-post växlar över tiden

4.4.1. Kontoprocess

Behov av funktionskonto samt ansvarig person för kontot anmäls till IT-avdelningen. Till varje funktionskonto finns en utsedd ansvarig person.
IT-avdelningen lämnar ut kontouppgifter och tillfälligt lösenord till ansvarig efter id-kontroll och signatur på ansvarsförbindelse.
Förändringar för funktionskonton hanteras genom att konton där innehavaren växlar över tiden förses med tidsbegränsning och därmed omprövas regelbundet.
Byte av ansvarig person initierats normalt av den ansvarige kontoinnehavaren. I händelse av att ansvarig person avslutat sin anställning, initieras byte av närmaste chef eller kontoadministratör.
Förändringar för funktionskonton där flera personer har tillgång till konto hanteras genom att ansvarig person för kontot begär förändring eller genom att IT-avdelningen hanterar förändring av funktionskontot i händelse av att ansvarig person slutar sin anställning.
Vid begäran om att kontot ska tas bort, eller om ovanstående hantering i samband med förändringar visar på att kontot kan tas bort, avvecklar IT-avdelningen kontot.

4.4.2. LoA-nivå

Funktionsidentiteter uppnår endast LoA1 beroende på att ett konto kan ha flera användare samt att kontots innehavare kan växla över tiden. Ansvarig innehavare kan identifieras över tiden genom att innehavarens personnummer, land/pass-nummer eller officiellt accepterad id-handling registreras och lagras.

4.5. Gästidentitet

Denna identitetstyp omfattar följande kategorier:

- individuella konton för personal från andra lärosäten på tillfälligt besök vid högskolan för en till högskolan relaterad verksamhet
- individuella konton för studenter från andra lärosäten på tillfälligt besök vid högskolan för en till högskolan relaterad verksamhet
- individuella konton för övriga besökare på tillfälligt besök vid högskolan för en till högskolan relaterad verksamhet. Exempel på innehavare kan vara gästföreläsare, externa projektdeltagare, konsulter, utställare, servicepersonal m fl.

4.5.1. Kontoprocess

En gästidentitet medför åtkomst till nätverk och Internet men saknar e-postkonto. Gästkonto är tidsbegränsade upp till maximalt 7 dagar.

Samtlig personal vid högskolan äger rätt att utfärda gästidentitet. Denna rättighet kan begränsas av högskolan. Utfärdaren loggar in via ett webbgränssnitt och anger besökarens namn samt personnummer, land/pass-nummer eller officiellt accepterad id-handling alternativt intygar att besökaren är känd och därmed kan identifieras vid ett senare tillfälle om behov föreligger. Efter att utfärdaren kompletterat med en tidsperiod skapas automatiskt kontot med en standardiserad behörighet. Regler för gästkontot och inloggningsuppgifter skrivs ut och lämnas till besökaren. Borttagning av gästkonto sker automatiskt då aktuell tidsperiod löpt ut.

4.5.2. LoA-nivå

Gästidentiteter uppnår endast LoA1 beroende på att kontots innehavare inte styrker sin identitet i enlighet med kraven för LoA2, samt att genom att innehavaren ofta endast har en lös och tillfällig koppling till högskolan. Innehavaren kan identifieras över tiden om innehavarens personnummer, land/pass-nummer eller officiellt accepterad id-handling registreras och lagras. Om utfärdaren angivit att besökaren är känd lagras uppgift om den användare som angivit detta.

4.6. Besöksidentitet

Denna identitetstyp omfattar följande kategorier:

- individuella konton för personal från andra lärosäten på tillfälligt besök vid högskolan för en till högskolan relaterad verksamhet
- individuella konton för studenter från andra lärosäten på tillfälligt besök vid högskolan för en till högskolan relaterad verksamhet
- individuella konton för övriga besökare på tillfälligt besök vid högskolan för en till högskolan relaterad verksamhet. Exempel på innehavare kan vara gästföreläsare, externa projektdeltagare, konsulter, utställare, servicepersonal m fl.

4.6.1. Kontoprocess

En besöksidentitet medför åtkomst till nätverk och Internet men saknar e-postkonto. Besökskonto tidsbegränsas till en arbetsdag.

Besöksidentitet utfärdas av Biblioteks och läranderesurser BLR. Utfärdaren loggar in via ett webbgränssnitt och anger besökarens namn samt personnummer, land/pass-nummer eller officiellt accepterad id-handling alternativt intygar att besökaren är känd och därmed kan identifieras vid ett senare tillfälle om behov föreligger. Kontot skapas därefter automatiskt med en standardiserad behörighet. Regler för besökskontot och inloggningsuppgifter skrivs ut och lämnas till besökare. Kontot stängs vid bibliotekets stängningstid och raderas automatiskt efter 7 dagar.

4.6.2. LoA-nivå

Besöksidentiteter uppnår endast LoA1 beroende på att kontots innehavare inte styrker sin identitet i enlighet med kraven för LoA2, samt att genom att innehavaren ofta endast har en lös och tillfällig koppling till högskolan. Innehavaren kan identifieras över tiden om innehavarens personnummer, land/pass-nummer eller officiellt accepterad id-handling registreras och lagras. Om utfärdaren angivit att besökaren är känd lagras uppgift om den användare som angivit detta.

4.7. Maskin- och systemidentitet

Denna identitetstyp omfattar följande kategorier:

- gemensamt konto för inbyggd användning i maskiner eller utrustning
- gemensamt konto för inbyggd användning i system eller applikationer
- individuella konton enbart nåbara från applikationer med behörighet enbart för autentisering till denna applikation

4.7.1. Kontoprocess

Behov av maskin- eller systemkonto samt ansvarig person för kontot anmäls av systemägare eller systemansvarig till IT-avdelningen.

IT-avdelningen skapar maskin- eller systemkonto i katalogtjänsten och skriver ut kontouppgifter som lämnas personligen till den som ansvarar för kontot.

Förändringar för maskin- och systemkonton hanteras genom att ansvarig person begär förändring samt genom att IT-avdelningen hanterar förändring av maskin- och systemkontot i händelse av att ansvarig person slutar sin anställning. Vid begäran om att kontot ska tas bort avvecklar IT-avdelningen kontot.

4.7.2. LoA-nivå

Maskin- och systemidentiteter uppnår endast LoA1 beroende på att kontot inte är ett individuellt konto utan används gemensamt av en maskin eller ett helt system. Ansvarig person kan identifieras över tiden genom att innehavarens personnummer, land/pass-nummer eller officiellt accepterad id-handling registreras och lagras.