

IDENTITY AND MANAGEMENT PRACTICE STATEMENT

Högskolan i Borås



HÖGSKOLAN
I BORÅS

Innehållsförteckning

1. Inledning.....	3
4. Organisational Requirement.....	3
4.1 Enterprise and Service Maturity.....	3
4.2 Notices and User Information	4
4.3 Secure Communications.....	5
4.4 Security-relevant Event (Audit) Records	5
5. Operational Requirements.....	6
5.1 Credential Operating Environment	6
5.2 Credential Issuing.....	7
5.3 Credential Renewal and Re-issuing	12
5.4 Credential Revocation	13
5.5 Credential Status Management.....	14
5.6 Credential Validation/Authentication	14

1. Inledning

Högskolan i Borås är medlem i identitetsfederationen SWAMID som omfattar de flesta lärosäten, forskningsinstitut och andra myndigheter som är relaterade till svensk forsknings- och utbildningssektor. Medlemskapet ger förutsättning för samarbete inom digitalt identitetsutbyte. Högskolan använder profilerna SWAMID Assurance Level 1, 2 och 3 inom kontohanteringsprocessen.

4. Organisational Requirement

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

4.1 Enterprise and Service Maturity

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

Högskolan i Borås, organisationsnummer 202100-3138, är en statlig utbildningsmyndighet vilket gör att lärosätets verksamhet regleras i lagar, förordningar och regleringsbrev.

De viktigaste lagarna och förordningarna som styr 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 högskolans 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.

Studenters personuppgifter hämtas ur lärosätets studiedokumentationssystem Ladok och därför gäller även förordning (SFS 1993:1153) om redovisning av studier m.m. vid universitet och högskolor för hanteringen av studenters personuppgifter i kontohanteringssystemet.

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

De lagringsmedia som innehåller eller kan innehålla känsliga data som till exempel lösenord eller personuppgifter tas om hand i säkert förvar för att vid behov destrueras enligt gängse normer.

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.

Användarvillkor finns publicerad på vår webb

- Anställd:
<https://www.hb.se/anstalld/stod-och-service/it/natverk-och-datorer/nyttjande-av-hogskolans-natverk/>
- Student:
<https://www.hb.se/student/mina-studier/studiemiljo--sakerhet/rattigheter-och-skyldigheter-som-student/nyttjande-av-hogskolans-datanatverk/>

Användarna godkänner att följa föreskrivna regler och hålla sig uppdaterade om gällande regler vid kontoskapandet. Vid förändringar av föreskrivna regler meddelas användarna via e-post.

Tjänstebeskrivning och hantering av personuppgifter vid federerad autentisering

- Högskolan i Borås använder SWAMIDs best practice policys och aktuell tjänstebeskrivning samt personuppgiftshantering publiceras på högskolans publika webb med länkar på den gemensamma inloggningstjänsten (idp.hb.se).
<https://www.hb.se/anstalld/stod-och-service/it/natverk-och-datorer/gemensam-inloggningstjanst>

4.3 Secure Communications

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

IT-personal med teknisk åtkomst

- Personer med behov av administratörsrättigheter har ytterligare ett personalkonto som äger extra behörighet, ett så kallat administratörskonto. Administratörskontot tilldelas endast de personer som har ett behov av detta. När en person får andra arbetsuppgifter eller lämnar sin anställning raderas administratörskontot. För anställda som går på tjänsteledighet inaktiveras administratörskontot men personalkontot är fortsatt aktivt.

TLS-nycklar för webbtjänster skyddas av operativsystemets behörighetssystem där endast administratörer har tillgång. Nycklar utfärdas genom extern CA och är minst 2048 bitar. Giltighetstiden för nycklarna är som längst ett år.

IdP:ns krypterings- och signeringsnycklar är självsignerade certifikat som lagras i tjänstens metadata och har längre giltighetstid, dock max tio år, med en nyckelstorlek på minst 2048 bitar. De privata nycklarna skyddas av operativsystemets behörighetssystem där endast administratörer har tillgång.

Ett webbaserat lokalt tillgängligt system med flerfaktorinloggning och kryptering av data hanterar våra delade hemligheter i form av exempelvis lösenord. Vem som får tillgång till systemet hanteras på uppdrag av IT-chef genom beställning via ärendehanteringssystem. Kontohantering för systemet hanteras manuellt av systemansvarig och it-säkerhetsansvarig. Systemet loggar alla händelser.

IdM-systemet vid Högskolan i Borås använder idag Microfocus eDirectory och Microsoft Active Directory för att lagra elektroniska identiteter. Produktsviten NetIQ Identity Manager används för processtöd, behörighetsstyrning och kontohantering. Utöver detta finns det egenutvecklad programvara i .NET samt bakomliggande databaser för att stödja identitetshanteringen, bland annat kontoprovisionering- och självserviceportal. Samtliga ingående delar i IdM-systemet är implementerade enligt respektive leverantörs best practice för att säkerställa säker kommunikation. Krypterat standardprotokoll används mellan de olika tjänsterna inom IdM-systemet.

4.4 Security-relevant Event (Audit) Records

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

Alla statusförändringar för elektroniska identiteter loggas till extern SQL-databas och kan visas vid behov. Denna loggning sker från alla relevanta delar i IdM-system, portaler samt kringliggande stödsystem.

Auditing- och systemloggar för alla ingående delar i IdM-systemet och IdP skickas till en extern ELK-stack. Detta innefattar säkerhetshändelser, lyckade och misslyckade inloggningsförsök och sparas så länge det behövs för att kunna utreda säkerhetsincidenter.

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.

De protokoll som används är i enlighet med SWAMIDs tekniska profiler. Det protokoll som framför allt används för kommunikation är TLS/SSL. Som autentiseringstjänster stöds SWAMID WebSSO och Eduroam.

För användarkonton krävs att lösenord skall uppfylla Microsoft AD Complex password policy. Minsta längd på lösenordet är åtta tecken. Lösenorden kan ej återanvändas vid lösenordsbyte.

Lösningen tillåter idag tre typer av multifaktorer:

- Enfaktor kryptografisk programvara (TOTP-app) i kombination med användarens lösenord. Dessa två faktorer är oberoende av varandra på så vis att tillgång till endast den ena faktorn inte möjliggör återställning av den andra faktorn. Användningen av denna typ av multifaktor kommer att upphöra senast 2027-12-31.
- Enfaktor kryptografisk hårdvara (Yubikey eller motsvarande) i kombination med användarens lösenord. Dessa två faktorer är oberoende av varandra på så vis att tillgång till endast den ena faktorn inte möjliggör återställning av den andra faktorn.
- Svensk e-legitimation tillitsnivå 3 eller 4. Denna kräver signering med kod för att vara multifaktorinloggning.

Vår lösning för multifaktorinloggning följer SWAMIDs rekommendationer med avseende på tekniska lösningar för multifaktor.

För att vid inloggning uppnå SWAMID AL3 krävs alltid multifaktor.

Kontouppgifterna för Eduroam lagras i ett eget Active Directory skilt från primär användarkatalog.

Användaren uppmanas att hålla kontouppgifter hemliga genom användarvillkor och lösenordspolicy.

Systemet för kontoadministration använder egna systemkonton mot katalogtjänsten.

För skydd mot hot finns brandvägg aktiverat på alla system och loggning sker till ELK-stack med larm. Rutiner finns för att hålla systemen uppdaterade och för att begränsa skada vid säkerhetsrelaterade incidenter.

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.

5.2.1 Högskolan i Borås använder domänen hb.se för att koppla unika användare till organisationen.

5.2.2 Identitetsutgivarna för de olika federativa teknikerna som används av Högskolan i Borås använder unika identifierare via antingen URL eller DNS-namn där alla DNS-delar avslutas med hb.se.

5.2.3 Användning av unikt användarnamn för olika identiteter över tid

En identitet kan återanvändas för kontotyp personal och extern om det är samma identitet, d.v.s. samma personnummer. Användarnamn kan aldrig återanvändas för en annan identitet då vi sparar information om tidigare användarnamn.

Identitetstyp	Unikt användarnamn	Exponeras till SWAMID	Återanvändning av unikt användarnamn
Personal	JA	JA	NEJ (Ja, om samma identitet)
Extern	JA	JA	NEJ (Ja, om samma identitet)
Student	JA	JA	NEJ
Gäst användare för lokal nätaccess	JA	NEJ	NEJ
Gäst användare	JA	NEJ	NEJ
Walkin	JA	NEJ	NEJ
Funktion	NEJ	NEJ	JA

5.2.4 Om en användare (identitet) har både student- och anställdkonto, kan användaren välja att logga in som student eller anställd genom att autentisera sig med respektive konto. I de fall autentisering sker med en metod som bara ger identiteten måste användaren välja vilken kontotyp som avses.

5.2.5 Kontoutdelning

Studenter initierar kontoskapningsprocessen genom att från systemet konto.hb.se begära ut ett konto, välja lösenord och kontrollera sina uppgifter. Informationen till detta konto samlas från Ladok och skickas som ett uppdrag till IdM-systemet. IdM-systemet skapar sedan identiteten samt kontot och meddelar sedan kontoskaparsystemet att kontot är färdigt för användning.

Ny personalidentitet läses in från lärosätets personalsystem men kan också läggas upp som en så kallad manuell timanställning efter beställning via formulär i IdM-systemets användargränssnitt.

Legitimering

För vad som räknas som giltig legitimation används identitetshandlingar enligt polisens regler för utlämning av pass. Vi godkänner även nationellt ID-kort utfärdat av land inom EU/ESS samt pass. De medarbetare som granskar legitimation följer internt framtagna dokumentation som beskriver processen för att verifiera en ID-handling, vilka ID-handlingar som accepteras och länkar till externa sidor för hjälp med verifiering. All personal som ska utföra legitimering utbildas i hur denna utförs och dokumenteras.

Identifieringsmetoder

För användare med svenskt personnummer används detta. För användare utan svenskt personnummer används födelsedata, namn och utfärdandeland av pass kombinerat med en riskbaserad bedömning eller etablerat interimspersonnummer i Ladok.

De fördefinierade identifierare som vi tillåter vid federerad inloggning är personnummer (svenskt/interim) från SWAMID-godkänd IdP eller svensk e-legitimation tillitsnivå 3 eller 4. Dessa fördefinierade identifierare används även för att säkerställa att det är samma person vid senare identifiering av innehavaren av användarkontot.

Vid identifiering loggas metod och identitetsinformation

Utfärdande av multifaktor

Vid utfärdande av multifaktor krävs en ny legitimering enligt ovan nämnda identifieringsmetoder. Multifaktor ges endast till användare vars konto är minst AL2.

Kontoutdelningsprocesser

Personal/extern

Kontotyp personal och extern kan skapas antingen automatiskt via HR-system eller manuellt av servicedesk.

Anställd personal via HR-system:

- Etablering av identitet i HR-system vid anställning
- Identitet synkas över till katalogsystem och konto skapas
- Användaren kvitterar ut kontouppgifter och sätter ett personligt lösenord efter uppvisande av giltig legitimation vid personligt besök till servicedesk eller genom att göra en lösenordsåterställning
- Alla personalkonton som skapas via HR-system skapas som AL2

Övrig personal och externa:

- Etablering av identitet sker i IdM-system av servicedesk
- Konto skapas
- Användaren kvitterar ut kontouppgifter och sätter ett personligt lösenord efter uppvisande av giltig legitimation vid personligt besök till servicedesk eller genom att göra en lösenordsåterställning
- Kontot skapas initialt som AL1 och kan sedan uppgraderas till AL2, som beskrivet i 5.2.6, om så behövs

Studenter

All kontoutdelning för studenter sker på motsvarande AL-nivå som uppnåtts vid autentisering, dock ej högre än AL2.

Kontotyp student ges möjlighet att välja en av följande aktiveringsmetoder:

- OTP-kod till e-postadress och/eller mobilnummer som finns registrerat i Ladok
- OTP-kod via personligt möte
- Inloggning via federerad inloggning
- Svensk e-legitimation tillitsnivå 3 eller 4

Vid aktivering med OTP-kod via e-post och/eller svenskt mobilnummer:

- Beställning av OTP-kod initieras av att användaren anger sitt personnummer varpå e-postadress och/eller mobilnummer läses in från Ladok. Kod med begränsad giltighetstid genereras och skickas till dessa.
- Om koden har slutat att gälla kan en ny kod beställas genom att börja om aktiveringsprocessen.
- Metod loggas och identiteten får via denna metod AL1-nivå vilket noteras på identiteten.
- Vid inloggning med OTP-kod krävs CAPTCHA

Vid aktivering med OTP-kod från servicedesk via personligt möte eller telefon:

- Beställning av OTP-kod inkommer via servicedesk.
- Vid personligt möte uppvisar användaren giltig legitimation och mottager utskrift av tidsbegränsad OTP-kod. Vid telefonsamtal skickas OTP-kod som SMS till det nummer som finns lagrat i Ladok för personen med det uppgivna personnumret.
- Metod loggas och kontot får via denna metod AL1-nivå vilket noteras på identiteten.
- Vid inloggning med OTP-kod krävs CAPTCHA

Vid val av inloggning via federerad inloggning (t.ex. antagning.se eller eduld.se):

- Användaren väljer sin önskade inloggningskälla.
- Användaren genomför en inloggning mot vald källa vilket levererar de attribut som behövs för att processen ska kunna fortsätta.

- Kraven för detta, förutom ett konto vid källan, är även att identitetsutgivaren skickar med personnummer (svenskt/interim). Om ett komplett personnummer ej kan erhållas från identitetsutgivaren så skapas inte heller något konto.
- I dagsläget har kontot som skapas samma AL-nivå som uppnåddes vid inloggningen, dock högst AL2.
- För att säkerställa att rätt AL-nivå uppnåtts vid federerad inloggning kontrolleras att assurance-attributet innehåller önskad AL-nivå. Detta kontrolleras även mot IdP'ns certifieringsnivå i metadata.

Vid val av inloggning via svensk e-legitimation tillitsnivå 3 eller 4:

- Användaren väljer sin önskade e-legitimation.
- Användaren genomför en inloggning mot vald e-legitimation vilket levererar de attribut som behövs för att processen ska kunna fortsätta.
- I dagsläget har kontot som skapas AL2-nivå.
- Matchning görs mellan personnummer från inloggning och fördefinierat personnummer på konto.

Gemensamt för studenternas aktiveringsmetoder:

- Systemet kontrollerar att identiteten finns öppen för aktivering.
- Aktivering av kontot och sättande av lösenord sker automatiskt efter att kontot skapats av IdM-systemet.
- Kontot får högst samma tillitsnivå som uppfylls av autentiserat konto (AL1/AL2).
- Kontots behörigheter sätts utifrån de uppgifter vi har i IdM-systemet, som t.ex kurser och program.
- För att kontoskapande ska kunna genomföras måste det finnas möjlighet att uppnå minst en registrering. Detta innebär minst en antagning till kurstillfälle som är öppet för registrering och ej har hinder för registrering, eller minst en registrering på ett kurstillfälle för pågående termin.

5.2.6 Förändring av tillitsnivå

Höjning av tillitsnivå

Användaren kan själv höja sitt konto till max AL2-nivå via självhjälpsportal om användaren kan logga in via annan IdP som uppfyller SWAMID AL2 och där användaren redan är AL2, eller svensk e-legitimation tillitsnivå 3 eller 4. Denna identifikationsnivå loggas även i samband med höjningen.

Personal som ska höjas till AL3 kan endast göra det genom personligt besök till servicedesk.

Höjning av tillitsnivån görs via kontoadministratör med hjälp av IdM-systemets användargränssnitt och kräver då att kontoadministratören gör en godkänd identifiering av individen enligt tidigare beskrivna regler (5.2.5). Denna identifikationsnivå loggas även i samband med höjningen. Är höjningen till AL3 så skapas även en andra faktor som beskrivet ovan (5.2.5).

Sänkning av tillitsnivå

Tillitsnivån kan endast sänkas manuellt av en kontoadministratör. Denna åtgärd kan beställas via servicedesk och innebär att kontots AL-nivå sänks. För att åter höja AL-nivån kan användaren genomföra aktiviteterna enligt ovan. Alla förändringar loggas.

5.2.7 Självuppgiven information

För personal måste all information ändras via personalsystem vilket sköts av HR-administratör. Denna information distribueras sedan ut till alla kringliggande system.

SMS och e-postadresser för studenter hämtas initialt vid kontoskapandet från Ladok och administreras därefter av användaren själv via vår självhjälsportal. För att uppgifterna ska kunna användas vid lösenordsåterställning måste uppgifterna vara verifierade. Verifieringen görs genom att verifieringskoder skickas på angiven kanal via självhjälsportalen. Inga automatiska uppdateringar görs från externa källor efter kontoskapandet.

5.2.8 Krav för användarhantering

Vid tilldelning av rollen för kontoadministration i IdM-systemet kontrolleras manuellt att personen har minst AL2-nivå. En person med kontoadministrationsroll får inte sänkas till lägre nivå utan att rollen först tagits bort (detta kan enbart göras av ett fåtal personer på IT som har en rutin att följa).

En kontoadministratör kan ej hantera identiteter som har högre AL-nivå än kontoadministratören själv har.

All inloggning i IdM-systemet sker med MFA-inloggning.

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.

5.3.1 Lösenord kan bytas i självserviceportalen. Detta sker genom att användaren loggar in med sina aktuella inloggningsuppgifter och sedan byter aktuellt lösenord mot ett nytt.

För att byta MFA krävs personligt besök till servicedesk och identifiering sker då enligt procedur beskriven i 5.2.5.

5.3.2 Innan byte tillåts måste användaren ange sitt nuvarande lösenord i direkt samband med lösenordsbyte. Kontroll sker mot lösenordspolicyn i katalogtjänsten innan lösenordet kan bytas. Byte kan även ske i Windowsklienten genom "Ctrl+Alt+Del"-menyn och loggas av auditfunktion.

Användaren kan ej själv byta sin MFA utan behöver besöka servicedesk för detta.

5.3.3 Lösenordsåterställning

Vid lösenordsåterställning måste användaren uppnå samma tillitsnivå som kontots aktuella tillitsnivå. Om erforderlig tillitsnivå inte kan uppnås kan en kontoadministratör manuellt sänka tillitsnivån på kontot till AL1 vilket gör att AL1-metoder kan användas vid lösenordsåterställning. Alla förändringar loggas. Lösenordsåterställning kan göras med följande metoder:

- **Självhjälpsportal**

Kan göras på AL1-, AL2- eller AL3-nivå beroende på vilken nivå som uppnås vid inloggning. För att kunna återställa lösenord behöver man kunna uppnå minst den nivå som identiteten har. Engångskod kan endast användas på AL1- och AL2-nivå för studenter. För engångskod på AL2-nivå krävs att det kommuniceras till användaren på två separata kanaler (SMS och e-post). Vid beställning av engångskod(er) krävs alltid CAPTCHA och koden har begränsad giltighetstid. Alla kommunikationskanaler för lösenordsåterställning måste vara verifierade som beskrivs i 5.2.7.

- **Personligt möte med vår servicedesk**

Lösenordåterställning kan göras genom möte med vår servicedesk och då krävs alltid identifiering eller riskbaserad bedömning oavsett AL-nivå.

Lösenordsåterställning via federerad inloggning kräver, på samma sätt som för kontoutdelning i avsnitt ovan, att den federerade inloggningen uppnår samma eller högre AL-nivå som kontot i källan. De fördefinierade identifierare som vi tillåter vid federerad inloggning är personnummer (svenskt/interim) från SWAMID-godkänd IdP eller svensk e-legitimation tillitsnivå 3 eller 4. Vid federerad inloggning tillåter vi endast personnummer som förregistrerad identifierare och ej riskbaserad bedömning baserad på annan information.

Lösenordsåterställning kan även ske genom personligt möte med vår servicedesk. Vid manuell lösenordsåterställning används identifieringsprocess beskriven i 5.2.5.

Återställning av andra faktor sker genom personligt besök till servicedesk i enlighet med tidigare beskrivna rutiner för utlämning av andra faktor (se 5.2.5).

5.4 Credential Revocation

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

5.4.1 Kontoadministratörer har möjlighet att spärra en användares konto genom att inaktivera kontot samt sätta ett nytt okänt lösenord. Detta kan göras t.ex. vid misstanke om säkerhetsrelaterad incident eller på användarens begäran. Det som föranledde spärren meddelas genom att information skickas till de privata kontaktuppgifterna, om dessa saknas måste innehavaren själv kontakta servicedesk. Innehavaren av kontot kan sedan återfå kontrollen genom att kontakta servicedesk och genomföra en lösenordsåterställning.

Giltighetstiden beräknas från källsystemen eller är manuellt inlagda. Då giltighetstiden har passerats inaktiveras kontot, det flyttas till karantän, kontot stängs och behörigheter tas bort. Ett halvår efter karantäntiden raderas kopplade konton och tjänster. Identitetsobjektet ligger kvar med endast personnummer och användar-id för att garantera att kontonamnet är unikt över tid. Då studenten enligt Ladok inte längre har några registreringar flyttas kontot efter 12 månader till karantän. Om ny kontoaktivering sker och användaren identifieras som samma individ återaktiveras konton i karantän förutsatt att kontot ännu inte har raderats. IdM-systemet återanvänder tidigare utfärdade kontonamn för personal och extern om det är samma individ som kommer tillbaka. För studenter utfärdas alltid ett nytt konto om det tidigare är raderat.

5.4.2 Vid säkerhetsincident gällande student inaktiverar kontoadministratör aktuellt konto, byter lösenord och eventuella andra inloggningsfaktorer raderas. Studenten meddelas om vad som föranledde spärren genom verifierad privat e-postadress eller mobil om dessa finns, saknas dessa måste innehavaren själv kontakta servicedesk. Innehavaren av kontot kan sedan återfå kontrollen genom att kontakta servicedesk för återaktivering av konto, genomföra en lösenordsåterställning som beskrivet i 5.3.3 och begära ut ny andra faktor, som beskrivet i 5.2.5.

Vid säkerhetsincident gällande personal inaktiverar kontoadministratör aktuellt konto, byter lösenord och eventuella andra inloggningsfaktorer raderas. Användaren meddelas om vad som föranledde spärren via tjänstetelefon eller personligt besök. Kan personen ej nås måste innehavaren själv kontakta servicedesk. Innehavaren av kontot återfår kontrollen genom att kontakta servicedesk för återaktivering av konto, genomföra en lösenordsåterställning som beskrivet i 5.3.3 och begära ut ny andra faktor, som beskrivet i 5.2.5.

5.4.3 I händelse av att ett konto spärras eller nedgraderas till lägre tillitsnivå på grund av incident så upprättas alltid en incident-rapport där orsaken utreds och dokumenteras och vilka åtgärder som tas för att förhindra att händelsen kan uppstå igen.

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.

5.5.1 IdM-systemet innehåller en komplett historik över utfärdade identiteter och via ett sökgränssnitt kan kontoadministratörer söka fram information knuten till individer med både aktiva och inaktiva konton. Historiken rensas efter fem år men användarnamn samt personnummer eller motsvarande sparas för evigt för kontotyp personal och extern. Studenternas grundläggande identitetsuppgifter sparas men användarnamn tas bort och återanvänds aldrig.

För kontotyp personal och extern lagras tidigare använt användarnamn så denna ej kan användas på en annan identitet.

För kontotyp student lagras det senast använda användarnamnet och kan återanvändas så länge som kontot endast är arkiverat. När kontot sen slutligen tas bort skapas ett helt nytt användarnamn med prefix baserat på det innevarande året. På grund av längden på arkiveringen och giltighetstiden innebär detta att inget studentanvändarnamn kommer att återanvändas på en annan identitet.

5.5.2 IdM-systemet och dess katalogtjänst, kontoadministrationssystem, federerad inloggningstjänst samt medräknat underliggande infrastruktur som nätverk mm ska ha samma upptid som interna tjänster.

5.6 Credential Validation/Authentication

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

5.6.1 Högskolan i Borås har implementerat samtliga tekniska protokoll enligt SWAMIDs rekommenderade best practice och använder SWAMIDs rekommenderade installation för Shibboleth som utgångspunkt för lokal konfiguration.

5.6.2 För att inloggning ska kunna ske måste kontot vara aktivt och öppet för inloggning.

5.6.3 För att inloggning ska kunna ske måste användaren autentisera sig med godkänd metod.

5.6.4 Om det inte finns någon aktiv inloggningssession måste användaren logga in på nytt. Idag tillåter vi SSO-sessioner på maximalt 12 timmar.