JÖNKÖPING UNIVERSITY

Identity Management Practice Statement

Högskolan i Jönköping

AUTHOR: *Joakim Danielsson*
JÖNKÖPING *2023-05-09*
Version: 1.5

Contents

1 Inledning

Högskolan i Jönköping är en stiftelsehögskola med fyra fackhögskolor: Hälsohögskolan, Högskolan för lärande och kommunikation, Jönköping International Business School och Tekniska Högskolan. Högskolan är medlem i identitetsfederationen SWAMID som omfattar de flesta lärosäten, forskningsinstitut och andra myndigheter som är relaterade till svensk forsknings- och utbildningssektor. Medlemskapet ger förutsättningar för samarbete inom digitalt identitetsutbyte. Högskolan använder profilerna SWAMID Assurance Level 1 och 2 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.

Stiftelsen Högskolan i Jönköping, med organisationsnummer 826001–7333 nedan kallat Jönköping University eller JU är en s.k. stiftelsehögskola. Detta innebär att JU, till skillnad från statliga lärosäten, inte är en integrerad del av svenska staten. JU är i stället ett privaträttsligt subjekt med egen rättskapacitet, vilket bland annat innebär möjlighet att förvärva rättigheter och ikläda sig skyldigheter. Den närmare relationen mellan JU och svenska staten är reglerad genom avtal.

JU är organiserad som en koncern. I koncernen ingår Stiftelsen Högskolan i Jönköping (”Stiftelsen”) och dess sex helägda dotterföretag. Dotterföretagen är organiserade som aktiebolag. Dessa är:

- Tekniska Högskolan i Jönköping AB (”JTH”),
    - Org.nr: 556487-2751
- Internationella Handelshögskolan i Jönköping AB (”JIBS”),
    - Org.nr: 556487-2728
- Högskolan för lärande och kommunikation i Jönköping AB (”HLK”),
    - Org.nr: 556487-2769
- Hälsohögskolan i Jönköping AB (”HHJ”),
    - Org.nr: 556619-6399
- Jönköping University Enterprise AB (”JUE”),

    - Org.nr: 559028-3056
- Högskoleservice i Jönköping AB (”HS”).
    - Org.nr: 556487-2744

Samt dessa som delägare:

- Högskolefastigheter i Jönköping AB (”HÖFAB”)
    - Org.nr: 556284-1089
- Campus Gränna AB (CGAB)
    - Org.nr: 559175-5599

JTH, JIBS, HLK och HHJ är fackhögskolor som bedriver utbildning, forskning och uppdragsverksamhet JUE tillhandahåller s.k. Pathway-kurser, i första hand till internationella studenter. HS är koncernens gemensamma serviceorgan med ansvar för väsentligen all stödverksamhet inom koncernen. Högskolefastigheter i Jönköping AB ägs av Jönköpings Rådhus (85,7%) samt Stiftelsen Högskolan i Jönköping (14,3%). Bolaget har även ett dotterbolag, Campus Gränna AB som ansvarar för campus i Gränna.

JU:s organisation och verksamhet grundar sig på Stiftelsens stadgar och ett långsiktigt ramavtal om utbildning och forskning som ingåtts mellan Stiftelsen och svenska staten. Det långsiktiga ramavtalet kompletteras med årliga avtal om utbildnings- och forskningsuppdrag. I dessa finns mer detaljerade bestämmelser om högskolans uppdrag, ersättningar samt därmed sammanhängande verksamhetskrav. I stiftelselagen (1994:1220) och aktiebolagslagen (2005:551) finns grundläggande lagreglering beträffande JU:s organisation och verksamhet.

Som stiftelsehögskola är JU en s.k. enskild utbildningsanordnare. JU har rätt att utfärda statligt reglerade examina under de förutsättningar som anges i lag (1993:792) om tillstånd att utfärda vissa examina. Av denna lag följer bl.a. att utbildningen ska vila på vetenskaplig eller konstnärlig grund och på beprövad erfarenhet samt att den ska bedrivas så att den i övrigt uppfyller de krav som uppställs på utbildning i 1 kap högskolelagen (1992:1434). Vidare gäller att utbildningen, för varje examen som tillståndet avser, ska svara mot de särskilda krav som gäller för denna examen enligt examensordningen (bilaga 2 till högskoleförordningen (1993:100).

Objektivitets- och likhetsprincipen i 1 kap 9 § regeringsformen är tillämplig på den verksamhet hos JU som har samband med examenstillståndet.

Av Stiftelsens stadgar och dotterbolagens bolagsordningar följer att studenterna vid JU har rättsligt stöd för att hävda rätten till inflytande över

utbildningen. Möjligheterna att ta ut avgifter för utbildning vid JU är begränsad och noga reglerad i det långsiktiga ramavtalet.

JU:s katalog- 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. Genom 2 kap 4 § offentlighets- och sekretesslagen (2009:400) och bilagan till offentlighets- och sekretesslagen är offentlighetsprincipen och reglerna om allmänna handlingars offentlighet, vilka återfinns i 2 kap tryckfrihetsförordningen, tillämpliga på JU. Härav följer även att JU ska jämställas med myndigheter vid tillämpningen av offentlighets- och sekretesslagen och att JU ska följa arkivlagen (1990:782). Personuppgiftslagen (1998:204) och Dataskyddsförordningen (2016/679/EU) är tillämplig beträffande behandling av personuppgifter vid JU.

I övrigt följer JU Sveriges övriga lagar och förordningar.

De lagringsmedia som innehåller eller kan innehålla känsliga data som till exempel lösenord eller personuppgifter destrueras vid utbyte eller kassering. Detta utförs av den leverantör som fått i uppdrag av högskolan att skrota eller utföra service på utrustningen. Rutinen finns bland annat publicerad i IT-services ärendehanteringssystem FAQ.

4.2 Notices and User Information

The member organization provides an Acceptable Use Policy (AUP) and a Service Definition including a Privacy Policy (PP) for the organization Subjects. These policies are needed to fulfil the SWAMID Policy and the Swedish legislation including the Swedish Personal Data Act (sv. Personuppgiftslagen, SFS 1998:204).

Ansvarsförbindelse

Ansvarsförbindelsen visas och godkänns innan ett konto aktiveras. Utan godkännande aktiveras inte nämnda konto. Vid godkännande sparar vilken version och tidpunkt för godkännande i separat databas. Ett välkomstmeddelande skickas med e-post som innehåller länk till aktuell ansvarsförbindelse. Ansvarsförbindelsen är även publicerad på högskolans publika webbplats[1] och i ansvarsförbindelsen framgår det vilken version som är aktuell.

[1] http://ju.se/it-helpdesk/faq---manualer/mitt-anvandarkonto/ansvarsforbindelse.html

När högskolan beslutar om ny version av ansvarsförbindelse hanteras det genom att den skickas ut på e-post till samtliga användare samt annonseras på intranät och publika webben.

IT personal med teknisk åtkomst till de servrar och datamedia där lösenord lagras undertecknar även särskild ansvarsförbindelse för administratörskonto. Ansvarsförbindelse för medarbetare med dessa priviligierade behörigheter finns vid IT-service och hanteras av IT-chef.

Tjänstebeskrivning och hantering av personuppgifter vid federerad autentisering SAML2

Högskolan i Jönköping använder SWAMID best practice policys och aktuell tjänstebeskrivning och personuppgiftshantering publiceras på högskolans publika webb[2] samt med länkar på den federerade inloggningstjänsten och kan konsumeras innan inloggning sker.

4.3 Secure Communications

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

Personer med behov av administratörsrättigheter har ytterligare ett personalkonto som äger extra behörighet, ett så kallat administratörskonto. Administratörskonto tilldelas endast de personer som har ett behov av detta. Om en person skulle få andra arbetsuppgifter eller lämna sin anställning raderas administratörskontot. För anställda som går på tjänstledighet inaktiveras administratörskontot men personalkontot är försatt aktivt.

Nycklar som eventuellt behöver lagras i klartext, skyddas av operativsystemets behörighetssystem där endast administratörer har tillgång. Nycklar som används till biljettsignering och dekryptering gäller 10 år och är egensignerade i ADFS. Nycklar som är utfärdade genom den tjänst som SUNET tillhandahåller gäller som längst 1 år. Alla nycklar är minst 2048 bitar.

Ett webbaserat lokalt tillgängligt system med 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, både radering och kontoskapande ingår. Kontohantering för systemet hanteras manuellt av högskolans IT-säkerhetsansvariga efter beställning via ärendehanteringssystemet.

[2] http://ju.se/it-helpdesk/faq---manualer/mitt-anvandarkonto/ovrigt/gemensam-inloggningstjanst.html

IdM systemet på Högskolan i Jönköping använder i dag Microsofts katalogtjänst Active Directory för att lagra elektroniska identiteter. Det ingår även en identitetslösning baserad på Microsoft Identity Manager för processtöd samt behörighetsstyrning. Till denna finns en egenutvecklad frontend för slutanvändare via webbgränssnitt i form av ex aktiverings- och självserviceportal och backend i form av SQL. Samtliga delar är implementerade enligt varje leverantörs best practice för att säkerställa säker kommunikation. Det gäller alla ingående delar i IdM systemet inklusive SQL backend. Kommunikation mellan de olika tjänsterna internt inom IDM systemet sker via krypterat standardprotokoll.

4.4 Security-relevant Event (Audit) Records

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

IdM systemet som helhet skickar loggar till central loggtjänst där den behandlas löpande och sammanställs/analyseras vid behov. Exempel på händelser som loggas är Active Directory security events, inloggningar via federationstjänster och förändringar på identiteter. Vilka som har tillgång till loggtjänsten, vad som loggas och hanteras fastställs av tjänstens förvaltningsorganisation.

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 SAML WebSSO och eduroam. Det protokoll som framför allt används för kommunikation är TLS/SSL. Som autentiseringstjänster stöds SAML2 via Active Directory Federation Services, samt Radius (för eduroam).

I lösenordspolicyn[3] framgår det förenklat att för normala kontotyper krävs ett komplext lösenord enligt definitionen i Active Directory på minst 10 tecken vilket uppfyller kravet på en entropi på minst 24 bitar.

För användare som innehar ett eduroamkonto ska lösenordet för eduroamtjänsten vara exakt 7 tecken för att säkerställa att inte samma lösenord används. Kontouppgifterna för eduroam sparas i ett eget Active Directory som är avskilt från användarens huvudsakliga elektroniska identitet.

IdM systemets portaler för lösenordsåterställning skyddas av Captcha samt ratelimiting som är påslaget i Active Directory samt ExtranetLockout i ADFS Användare uppmanas att hålla kontouppgifter hemliga i användarvillkoren samt i lösenordspolicyn.

Kontoadministrationssystemet använder egna systemkonton mot katalogtjänsten för att hantera kontoadministration.

För att skydda sig för hot mot systemet finns brandvägg med IPS och antivirus på alla system, många system har även en EDR-lösning. Det finns i övrigt rutiner för att hålla systemen uppdaterade och rutiner för att begränsa skada vid eventuella säkerhetsrelaterade incidenter.

5.2 Credential Issuing

The purpose of this subsection is to ensure that the Identity Provider has control over the issuing process. All relying parties have a need to uniquely identify the Identity Provider and the Identities provided by that Identity Provider.

5.2.1 Unik domän

Högskolan i Jönköpings identitetshanterare ingår i DNS-domänen ju.se och har DNS-namnet adfs.ju.se. Denna IdP hanterar den administrativa domänen **hj.se** som är globalt unikt inom federationen.

5.2.2 Unik IdP identifierare

IdPn har en global unik identifierare (entityid) som baseras på DNS domäner som ägs av Högskolan.

5.2.3 Användning av unikt användarnamn för olika identiteter över tid.

[3] https://ju.se/it-helpdesk/faq---manualer/mitt-anvandarkonto/byta-losenord.html

En identitet återanvändas för konton med anställningslikt förhållande om det är samma identitet, d.v.s. personnummer.

Kontotyp	Unikt användarnamn	Exponeras till SWAMID	Återanvändning av unikt användarnamn
Personal	JA	JA	NEJ (JA, om samma identitet)
Personal - Extern	JA	JA	NEJ (JA, om samma identitet)
Lätt användare	JA	JA	NEJ (JA, om samma identitet)
Student	JA	JA	NEJ (NEJ, om samma identitet)
Begränsad användare	JA	JA	NEJ (JA, om samma identitet)
Förstudent	JA	JA	NEJ (NEJ, om samma identitet)
Besök	NEJ	NEJ	JA
Funktion	NEJ	NEJ	JA

5.2.4 Flera användarnamn för samma identiteter.

Om en användare äger flera elektroniska identiteter, exempelvis är både student och anställd kan användaren välja att logga in som student eller anställd genom att autentisera sig med respektive identitet.

5.2.5 Kontoutdelning

Vad används som identifierare

AL2
För personer med svenskt personnummer eller samordningsnummer används dessa som identifierare. Kontroll sker mot Ladok eller SPAR löpande. För övriga används id-handlingens typ (PASS/Id-kort, etc), referensnummer samt utfärdande land. Ex PASS, G1888368, DK

AL1
Samma som för AL2 men vi tillåter även privat e-postadress som identifierare för kontotypen *Förstudent* och *Begränsad användare*.

Process
Förväntade studenter läses in och sparas i IdM systemet och markeras som öppna för aktivering. Källsystem för studenter är Ladok eller Bliss/ISA. Bliss/ISA är internt utvecklade system som hanterar inresande utbytesstudenter. Förväntad personal läses in från personalsystem eller

skapas manuellt efter beställning via ärendehanteringssystem. För de identiteter som av olika anledningar inte kommer från dessa system kan en kontoadministratör manuellt ange nödvändiga data för att förbereda en kontoaktiveringsprocess. Alla kontotyper som kräver aktivering utförs via ett webbgränssnitt av användaren.

Följande kontoutdelningsmetoder tillåts per kontotyp:

- Personal: AL2 metoder.
- Personal - extern: AL1 och AL2 metoder.
- Student: AL1 och AL2 metoder.
- Delad brevlåda och funktionskonto: OTP (engångslösenord) till förregistrerad e-postadress. (Exponeras inte mot SWAMID)
- Besök: Saknar aktiveringsbehov. (Exponeras inte mot SWAMID)
- Lätt användare (Online konto O365): AL1 och AL2 metoder.
- Begränsad användare och förstudent: AL1 metoder.

Kontotyper

- **Personal**
  - Individuellt konto för personal under den period de är anställda vid högskolan och som uppbär lön från högskolan.
  - Källa är personalsystem.
  - Kontotypen stöder AL2.
  - Gäller tills vidare, längst pensionsålder.
- **Personal - extern**
  - Individuellt konto för personal med anställningslikt förhållande som inte uppbär lön från högskolan.
  - Källa är ärendehanteringssystem.
  - Gäller som längst 1 år i taget, kan dock förlängas årligen
  - Kontotypen stöder AL1 och AL2.
  - I övrigt samma rättigheter/befogenhet som personal.
  - Exempel på innehavare kan vara gästprofessorer, gästforskare, gästföreläsare, externa projektdeltagare, konsulter m fl.
- **Lätt användare (Online konto Office 365)**
  - Individuellt konto för externa, som inte uppfyller villkoren för en personal-, extern- eller studentidentitet, där behov av konto föreligger för verksamhet vid högskolan under en längre tid eller med annan behörighet än vad som tillhandahålls med besökskonto.
  - Källa är ärendehanteringssystem.
  - Gäller som längst 1 år, kan dock förlängas.
  - Kontotypen stöder AL1 och AL2.
  - Exempel på innehavare kan vara gästprofessorer, gästforskare, gästföreläsare, externa projektdeltagare, konsulter m fl.
- **Begränsad användare**
  - Individuellt konto för användare där behov av konto föreligger i enskilda informationssystem.
  - Ger endast access till enskilda resurser/informationssystem.

  - Källa är enskilda informationssystem eller ärendehanteringssystem.
  - Gäller som längst 1 år, kan dock förlängas.
  - Kontotypen stöder AL1.
  - Exempel på innehavare kan vara VFU-handledare, konsulter.
- **Förstudent**
  - Individuellt konto för användare där behov av konto föreligger i enskilda informationssystem.
  - Ger endast access till enskilda resurser/informationssystem.
  - Källa är enskilda informationssystem.
  - Gäller som längst 1 år, kan dock förlängas.
  - Kontotypen stöder AL1.
  - Exempel på innehavare kan vara kommande internationella studenter.
- **Student**
  - Studenter som är aktivt studerande vid högskolan.
  - Med aktivt studerande menas att den studerande är registrerad på kurs 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 18 månader.
  - Kontotypen stöder AL1 och AL2.
- **Funktion och delad brevlåda**
  - 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 skiftar 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.
- **Besök**
  - Individuella konto för besökare på tillfälligt besök vid högskolan för en till högskolan relaterad verksamhet. Exempel på innehavare kan vara gästföreläsare, externa projektdeltagare, konsulter, utställare, servicepersonal med flera.
  - Individuella konto för besökare vid uthyrning av högskolans lokaler till extern part.
  - Individuella konto för besökare till högskolebiblioteket.

	Staff (Agresso)	Staff-External	Light user	Visitor
Giltighetstid	Anställningstid	1 år	1 år	1/10/25 dagar
E-post	**Ja**	**Ja** (valbart)	**Ja** (valbart)	Nej
Office 365 licens	A5 faculty	A5 faculty	A1 faculty	Nej
Office 365 licens kostnad	**Ja**	**Ja**	Nej	Nej
Eduroam	**Ja**	**Ja**	**Ja**	Nej (JU-visitor)
Logga in på JU dator	**Ja**	**Ja**	Nej	**Ja**
MFA på ej JU dator (2-faktors inloggning)	**Ja**	**Ja**	**Ja**	Nej
Använda JU mobil	**Ja**	**Ja**	Nej	Nej
Office Pro Plus	**Ja**	**Ja**	Nej	Nej
Office Online	**Ja**	**Ja**	**Ja**	Nej
Lokal JU lagring	**Ja**	**Ja**	Nej	Nej
JU Print	**Ja**	**Ja**	**Ja**	**Ja**
Åtkomst till Intranät	**Ja**	**Ja**	**Ja**	Nej
VPN	**Ja**	**Ja**	**Ja**	Nej
Zoom	**Ja**	**Ja**	**Ja**	Nej
Canvas	**Ja**	**Ja**	**Ja**	Nej
Beställa Visitorkonto	**Ja**	**Ja** (om bekräftad användare)	Nej	Nej

Figur 1 Jämförelse av några kontotyper och dess funktioner.

Utdelning av identifierare (NYA/ladok genererat T-nummer eller användarnamn) för studenter som saknar svenskt personnummer.

NYA-studenter

I de fall där användaren besöker campus delas identifierare ut till användaren genom en fysisk kontroll av identitetshandling. Om användaren inte kan besöka campus hanteras det genom att studenten kan aktivera sitt JU-konto genom ett bekräftat konto hos universityadmissions.se, vilket innebär att identifierare inte delas ut. Alternativt hanteras det enligt avsnittet ”*Lokalt antagna (ISA) – Övriga”*

Lokalt antagna (Bliss) - Utbytesstudenter

I de fall där användaren besöker campus delas identifierare ut till användaren genom en fysisk kontroll av identitetshandling. Om användaren inte kan besöka campus hanteras det genom att identifierare skickas till e-postadress tillhandahållen av partneruniversitet.

Lokalt antagna (ISA) - Övriga

I de fall där användaren besöker campus delas identifierare ut till användaren genom en fysisk kontroll av identitetshandling. Om användaren inte kan besöka campus hanteras det genom följande process:

E-postadressen har samlats in i anslutna system, ex bostads-, antagnings- eller betalningssystem och lagras i en central metadatakatalog för studenter ”BLISS”. Systemet hanterar olika e-postadresser, ex student och agentadress

samt övrig information såsom kopia på giltig identitetshandling. Handläggare genomför en riskbedömning baserat på tillgänglig information. Riskbedömning innebär bland annat att angiven e-postadress för studenten tillhör studenten och inte en annan person, ex agent eller målsman. Vid misstanke gällande felaktig e-postadress undersöks möjligheten att rätta uppgiften enligt GDPRs principer. Efter riskbedömning och eventuell rättning skickas identifierare till angiven e-postadress.

Kontoutdelningsprocesser

Användaren ges möjlighet att välja aktiveringsmetod. Nedan beskrivs de olika metoderna.

- OTP (engångslösenord) via självuppgiven e-postadress.
  - Kontot får via denna metod AL1-nivå vilket noteras på kontot.
  - Metod fungerar för kontotyperna personal-externa, studenter, förstudent, lätt och begränsad användare.
- OTP (engångslösenord) från servicedesk via folkbokföringsadress.
  - Kontot får via denna metod AL2-nivå vilket noteras på kontot.
  - Metod fungerar för kontotyperna personal, personal-externa, studenter och lätt användare.
- OTP (engångslösenord) från servicedesk vid personligt besök.
  - Kontot får via denna metod AL2-nivå vilket noteras på kontot.
  - Metod fungerar för kontotyperna personal, personal-externa, studenter och lätt användare.
- Inloggning via federerad SAML2 för bekräftade konton.
  - Kontot får via denna metod AL2-nivå vilket noteras på kontot.
  - Metod fungerar för kontotyperna personal, externa, studenter och lätt användare.
  - Inloggning med obekräftat konto kan inte använda metoden.
  - Inloggning med minst AL2 konto krävs.
- Inloggning via nationell godkänd e-legitimation.
  - Kontot får via denna metod AL2-nivå vilket noteras på kontot.
  - Metod fungerar för kontotyperna personal, personal-externa, studenter och lätt användare.

Vid aktivering med OTP

Gemensamt för OTP är att användaren anger sitt personnummer, passnummer eller motsvarande och löser ett robotfilter en s.k. ”CAPTCHA”.

Vid aktivering med OTP till privat e-postadress

Beställning av OTP initieras av användaren själv som anger en privat e-postadress. En unik OTP med begränsad giltighet skickas till e-postadressen vilket anges innan aktivering kan fortsätta. Om koden har slutat att gälla kan en ny kod beställas genom att börja om aktiveringsprocessen.

Metod loggas och kontot får via denna metod AL1-nivå vilket noteras på kontot.

Vid aktivering med OTP från servicedesk till folkbokföringsadress

Beställning av OTP har inkommit via ärendehanteringssystem eller via IdM systemet. Detta resulterar i en utskrift av ett brev som innehåller folkbokföringsadress, information om kontoaktivering samt en unik OTP som har begränsad giltighet och som skickas till användaren.

Metod loggas och kontot får via denna metod AL2-nivå vilket noteras på kontot.

Vid aktivering med OTP från servicedesk via personligt möte

Beställning av OTP har inkommit via ärendehanteringssystem eller via IdM systemet. Detta resulterar i en utskrift som innehåller folkbokföringsadress, information om kontoaktivering samt en unik OTP som har begränsad giltighet. Användaren besöker servicedesk och uppvisar giltig legitimation och mottager utskriften.

Giltig legitimationshandling
För AL1 och AL2 används Skatteverkets[4] definition för giltig legitimationshandling med undantag för att vi i alla lägen godkänner PASS som giltig legitimation. (För AL3 kommer vi använda Polisens[5] definition för giltig legitimation.)

Kontrollprocess
Vid personligt möte används metodiken från de sju stegen. De sju stegen produceras och distribueras av Kronan Säkerhet på uppdrag av Svenska Bankföreningen.

Om utländsk legitimationshandling används genomförs en riskbedömning gällande korrekt koppling mellan digital identitet och den fysiska identiteten.

Metod loggas och kontot får via denna metod AL2-nivå vilket noteras på kontot.

Vid val av Inloggning via federerad SAML

Användaren väljer sin önskade inloggningskälla. Idag är det antagning.se samt eduID.se som är godkända att användas av JU. (Hösten 2023 kommer antagning.se att avvecklas.) Användaren genomför en inloggning på vald källa vilket levererar de attribut som behövs för att processen ska kunna

---

4 https://www.skatteverket.se/privat/folkbokforing/idkort/villkorforattfaansokaomidkort/godkandaidhandlingar

5 https://polisen.se/tjanster-tillstand/pass-och-nationellt-id-kort/giltiga-id-handlingar/

fortsätta. Kraven för detta förutom ett konto vid källan krävs även en AL2 notering på kontot.

Metod loggas och kontot får via denna metod AL2-nivå vilket noteras på kontot.

Vid val av inloggning via nationell e-legitimation.

Användaren genomför en inloggning via vald e-legitimation vilket levererar de attribut som behövs för att processen ska kunna fortsätta. Resultatet av inloggning via e-legitimation ska leverera tillitsnivå 3 eller 4 för att godkännas.

Metod loggas och kontot får via denna metod AL2-nivå vilket noteras på kontot.

Gemensamt för alla aktiveringsmetoder

Systemet kontrollerar att identiteten finns öppen för aktivering. I aktiveringsflödet ska även användarreglerna godkännas innan kontot kan aktiveras. Användaren ges möjlighet att ange privata kontaktuppgifter som kan verifieras i direkt anslutning till uppgifterna. Efter aktivering och godkännande av ansvarsförbindelse aktiveras konto samtidigt som aktuella behörigheter tilldelas kontot. Vilken version samt att användaren har godkänt ansvarsförbindelsen loggas i databas. Kontots behörigheter sätts utifrån de uppgifter vi har i IdM-systemet, exempelvis kurser, program eller avdelningstillhörighet.

Förstudent kan omvandlas till student

En identitet med kontotypen förstudent kan omvandlas till student om denne registreras som student i våra källsystem. När detta sker krävs en helt ny kontoaktivering enligt de krav som gäller för studentkontotypen.

Höjning av tillitsnivå.

Höjning kan ske via självserviceportalen genom en lösenordsåterställning eller via en ”Bekräfta min identitet” funktion. Användaren höjer sin tillitsnivå genom att genomföra en kontoutdelningsprocess enligt metoder godkända för en högre AL-nivå. Metoderna som stöds är samma som vid kontoaktivering samt möjlighet att använda en kopia på hushållsräkning tillsammans med en ”Selfie” och en giltig legitimationshandling. Denna metod hanteras i övrigt som ”Brev till folkbokföringsadress”. Ett brev som innehåller hushållsräkningen adress, information om kontoaktivering samt en unik OTP som har begränsad giltighet och som skickas till användaren.

Ett konto tillåts inte att sänka sin tillitsnivå, ex genom att användaren använder AL1 metoder vid lösenordsåterställning. (Det är inte möjligt att använda en återställningsmetod av lägre AL-nivå) Dock kan en kontoadministratör manuellt sänka tillitsnivån så att AL1 metoder kan användas vid lösenordsåterställning. Ändringen kan beställas via ärendehanteringssystemet. En sådan åtgärd innebär att kontots AL-nivå

sänks. För att åter höja AL-nivån kan användaren genomföra aktiviteterna enligt ovan.

5.2.6 loggning byte AL nivå.

Byte av AL nivå loggas inom IDM systemet samt skickas till SIEM.

5.2.7 Självserviceportal

Självserviceportal ger användare möjlighet byta lösenord, självuppgivna kontaktuppgifter, höjning av tillitsnivå samt sätta ett separat lösenord för tjänsten eduroam. Det finns även en funktion för lösenordsåterställning och hantering av I.C.E. uppgifter.

5.2.8 Identitetsidentifiering servicedesk

Sker med speciella systemadministrativa konton på högsta godkända AL nivån, idag AL2 med metodstöd från ”De sju stegen”. Inloggning till administrativa system för kontohantering kräver AL2 och MFA.

5.3 Credential Renewal and Re-issuing

Renewal of credentials occur when the Subject changes its credential using normal password reset. Re-issuing occurs when credentials have been invalidated.

Lösenordsbyte.
Lösenord kan bytas i självserviceportalen. Det sker genom att användaren loggar in med sina aktuella inloggningsuppgifter samt att användaren kan lösa ett robotfilter och sedan byter aktuellt lösenord mot ett nytt. Innan byte möjliggörs måste användaren på nytt bevisa att kännedom om lösenordet, detta sker genom att ange nuvarande lösenord i direkt samband med lösenordsbyte. SSO-funktionalitet saknas för tjänsten. Kontroll sker mot lösenordspolicyn i katalogtjänsten samt Azure Password Protection innan lösenordet kan bytas.

Lösenordsåterställning.
Ett konto tillåts inte att sänka sin tillitsnivå, ex genom att använda AL1 metoder vid lösenordsåterställning. Dock kan en kontoadministratör manuellt sänka tillitsnivån på kontot vilket gör att AL1 metoder kan användas vid lösenordsåterställning. En sådan åtgärd innebär att kontos AL-nivå sänks till samma nivå. Alla förändringar loggas. Kontroll sker mot lösenordspolicyn i katalogtjänsten samt Azure Password Protection innan lösenordet kan återställas.

Lösenordsåterställning kan göras via webtjänst med hjälp av samma metoder som vid kontoaktivering enligt avsnitt 5.2 med nedan undantag.

- AL1
    - Bekräftad privat kontaktuppgift
        - Engångskod via tidigare självuppgiven bekräftad e-postadress eller tidigare bekräftat SMS-nummer på minst AL1 nivå. Uppgifterna är bekräftade under tiden som kontot hade egenskapen AL1.
        - Koderna har begränsad giltighetstid.
- AL2
    - Bekräftade privata kontaktuppgifter
        - Engångskod via tidigare självuppgiven bekräftad e-postadress och tidigare bekräftat SMS-nummer på AL2 nivå. Uppgifterna är bekräftade under tiden som kontot hade egenskapen AL2.
        - Två olika koder skickas till de angivna uppgifterna. Båda koderna ska anges för att lösenordsåterställning ska ske.
        - Koderna har begränsad giltighetstid.

Lösenord gäller normalt tills vidare med undantag för personalkonton med administratörsrättigheter, där krävs byte av lösenord 1 gång per år.

5.4 Credential Revocation

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

5.4.1 Revokering av kontouppgifter.

Vid misstanke om missbruk eller säkerhetsincident har kontoadministratörer skyldighet att spärra en användares konto genom att inaktivera kontot. Vid säkerhetsincidenter det misstänks att lösenord inte längre är hemligt, sätts även ett nytt okänt lösenord. Det som föranledde spärren meddelas genom att information skickas till de privata kontaktuppgifterna genom ex e-postadress och SMS om dessa finns. Om dessa saknas måste innehavaren själv kontakta servicedesk.

Giltighetstiden beräknas från källsystemen eller är manuellt inlagda. Då giltighetstiden har uppnåtts inaktiveras kontot samt flyttas till karantän. Tjänster, ex e-post, hemkatalog och onedrive som är kopplade till kontot tas sedan bort maskinellt efter ytterligare två månader. Konto ligger sedan kvar i Active Directorys papperskorg i 6 månader innan det raderas permanent.

Då studenten enligt Ladok är klar med sin utbildning inaktiveras kontot och flyttas till karantän efter en övergångstid på högst 18 månader. Studenter som har moment kvar i sin utbildning, men inte omregistrerar sig, hanteras efter 18

månader enligt samma princip som då en student enligt Ladok är klar med sin utbildning.

Studenter på utbildningar som inte hanteras i Ladok hanteras på ett motsvarande sätt. Vid kontoaktivering, behörighetstilldelning, förändringar och avveckling sker kontroll mot uppgifter som kontoadministratör lagt in i IdM systemet för aktuell student.

Om en användare begär radering av konto i förtid, hanteras det skyndsamt enligt manuell process och samma regler som ovan.

Om ny kontoaktivering sker och användaren identifieras som samma individ, återaktiveras konton i karantän förutsatt att kontot ännu inte har raderats.

Vid radering sparas kontonamn samt identifierare. IdM systemet återanvänder tidigare utfärdade kontonamn för användare med personalliknade anknytning om det är samma individ som kommer tillbaka. För studenter utfärdas alltid ett nytt konto om det tidigare är raderat.

5.4.2 Utdelning av kontouppgifter efter revokering.

Innehavaren av kontot kan återfå kontrollen genom att kontakta servicedesk och/eller genomföra en lösenordsåterställning enligt samma metoder som vid kontoaktivering. Om kontoinnehavaren saknar svenskt personnummer där utländsk legitimationshandling används genomförs en riskbedömning gällande riktigheten i handlingen och dess uppgifter kopplade till de uppgifter som redan finns i IdM systemet för att bedöma att det är samma person.

5.4.3 Lärdomar.

IT- och informationssäkerhets- samt personuppgiftsincident (nedan anges som säkerhetsincident) är en oönskad händelse, som orsakar, eller potentiellt kan orsaka negativa konsekvenser för Jönköping Universitys (JU) säkerhet och efterlevnad av rättsliga krav på området och hanteras enligt rutinen ”Övergripande rutiner vid säkerhetsincidenter”
”Efter att säkerhetsincidenten är avhjälpt/åtgärdad – genomför ett uppföljningsmöte för att dra lärdomar om händelsen och incidentprocessen. Uppföljningsmötet ska ske max en vecka efter att säkerhetsincidenten är åtgärdad. Föreslå eventuella förbättringar och presentera IT-ledningen och andra intressenter.”

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 5 år men användarnamn samt personnummer motsvarande sparas för evigt för kontotypen personal-, extern och lätt användare för att uppfylla **5.2.3**.

5.5.2

IdM systemet, innehållande katalogtjänst, kontoadministrationssystem och ADFS, samt medräknat underliggande infrastruktur så som nätverk mm ska enligt serviceavtal ha en tillgänglighet på minst 99,2% under tiden 08:00-17:00. Systemets ingående delar och tjänster övervakas för att säkerställa SLA under kontorstid. För ADFS IDP är tillgängligheten 100% de senaste 30 dagarna under kontorstid. Sett över hela dygnet under samma period är ADFS tillgänglig 100% av tiden. (2023-05-09)

Samma IDP används för många verksamhetskritiska system, ex mejl, LMS och digital tentamen.

5.6 Credential Validation/Authentication

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

Högskolan i Jönköping har implementerat samtliga tekniska protokoll enligt SWAMIDs rekommenderade best practice och använder SWAMIDs rekommenderade verktyg för ADFS som utgångspunkt för lokal konfiguration.

5.6.2
Endast aktiva konton vars giltighetstid inte gått ut kan autentisera sig enligt leverantörens best practice. Det går inte autentisera konton som har gått ut eller är inaktiverade. Vidare går det inte autentisera konton som är låsta av andra anledningar, exempelvis för många felaktiga försök, s.k. rate limit.

5.6.3
ADFS kräver att användaren identifierar sig i första hand med något man vet, ex användarnamn och lösenord. Om tjänsten stöder FIDO2 kan även SSO med stark autentisering med Windows Hello for Business användas genom något man har, ex TPM skyddat certifikat knutet till sin egen enhet tillsammans med något man vet eller är. Ex PINkod eller ansiktsigenkänning.

5.6.4
SSO lifetime är satt till 720 minuter eller 12 timmar.