IMPS Umeå universitet
Per Hörnblad
per.hornblad@umu.se

UMEÅ UNIVERSITET

Version: 2.5 FINAL

Umeå universitet Identity Management Practice Statement

Version	Datum	Författare	Förändring
0.1	2011-04-04	Torbjörn Wiberg	Initial beskrivning på IdM
0.2	2012-02-15	Torbjörn Wiberg	Lösenordsåterställning
1.0	2018-02-15	Mattias Wallmark	Initial IMPS, AL2 via legitimering i servicedesk, Antagning.se, fbf samt hushållsräkning
1.3	2021-12-02	Per Hörnblad	Externa konton, eduID, Freja eID+, ny AL-profil
2.1	2022-03-09	Per Hörnblad	IMPS-mallen, MFA, AL3 via e-leg tillitsnivå 3, AL2 via e-leg tillitsnivå 3 (även BankID), hushållsräkning, videosamtal AL2 för personal, videosamtal AL1
2.2	2022-06-08	Per Hörnblad	AL3 via SWAMID-IdP
2.3	2023-12-08	Per Hörnblad	AL2 eduID och eIDAS utan sv pnr, AL1 via Antagning.se och i-pnr
2.4	2024-11-25	Per Hörnblad	AL2 skyddade identitetsuppgifter via dig. repr. av resehandling i e-leg, MFA-reset via eIDAS
2.5	2025-03-30	Per Hörnblad	Anpassningar till tillitsprofiler 2024. AL2 via Freja eID, AL2 via Freja-UPI, AL2 via fbf, AL2 via eduGAIN (ESI resp. subject-id), utdelning av TOTP-dosa via fbf och hushållsräkning, AL3 via SWAMID-IdP utan sv pnr, AL3 via Freja-UPI, AL3 via eIDAS

1. Inledning

Umeå universitet är som svenskt lärosäte beroende av att på ett säkert och enkelt sätt kunna ge sina anställda och studenter tillgång till nationella och internationella IT-resurser. Detta ges genom medlemskap i SWAMID. Universitetet ser därför ett fortsatt medlemskap som en förutsättning för sin verksamhet.

Detta dokument beskriver hur Umeå universitet uppfyller kraven för tillitsnivåerna SWAMID AL1, SWAMID AL2 och SWAMID AL3.

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.

4.1.1 The Member Organisation MUST have a Swedish Company Registration Number

Umeå universitet har organisationsnummer 202100-2874.

4.1.2 The Member Organisation MUST adhere to applicable Swedish legislation.

Umeå universitet är en statlig utbildningsmyndighet vilket gör att lärosätets verksamhet regleras i lagar, förordningar och regleringsbrev. De viktigaste lagarna och förordningarna som styr universitetets/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 universitetets uppdrag under ett kalenderår. I övrigt följer lärosätet Sveriges övriga lagar och förordningar.

Lärosätets katalog- och behörighetssystem, Koncernkatalogen, 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.

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

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 Koncernkatalogen.

4.1.3 The Member Organisation MUST have documented procedures for data retention

Destruering av lagringsmedia, fysiska servrar/skrivare/etc samt lagringsmedia i SAN sker enligt universitetets (ITS) fastställda rutiner. För data i molntjänster finns rutiner för destruering/avveckling i respektive avtal.

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.

4.2.1 Each Member Organisation MUST publish the Acceptable Use Policy to all Subjects.

Umeå universitets användarvillkor finns publicerade på webben, länk https://www.umu.se/regelverk/lokaler-it-och-miljo/regel-for-anvandning-av-umea-universitets-it-resurser/.

4.2.2 All Subjects MUST indicate acceptance of the Acceptable Use Policy before use of the Identity Provider.

Användarvillkoren måste godkännas i samband med att användarkontot aktiveras eller återaktiveras.

4.2.3 All Subjects MUST indicate renewed acceptance of the Acceptable Use Policy if the Acceptable Use Policy is modified.

I händelse att användarregler ändras informeras samtliga användare om detta via e-post. Om det sker stora förändringar i reglerna finns möjligheten att återställa samtliga berörda användarkonton vilket medför att villkoren på nytt ska godkännas.

4.2.4 The Member Organisation MUST maintain a record of Subject Acceptable Use Policy Acceptance.

Eftersom godkännande krävs vid kontoskapande sker loggning av godkännandet genom loggning av kontoskapandet.

4.2.5 Each Member Organisation MUST publish the identity provider Service Definition.

Beskrivning av Service definition är publicerad på Umeå universitets webbplats, https://www.umu.se/it-stod-och-systemutveckling/federerad-inloggning/.

4.3 Secure Communications

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

4.3.1 Access to shared secrets MUST be subject to discretionary controls.

Åtkomst och administration av servrar kopplade till identitetshanteringssystemet kräver tvåfaktorautentisering med flertalet skalskydd. Administratörskonton på applikationsnivå är skilt från användarens vanliga konto samt tilldelas en begränsad mängd personer som arbetar med förvaltning av identitetshanteringssystemen.

4.3.2 Private keys and shared secrets MUST NOT be stored in plain text form unless given adequate physical or logical protection.

Inga lösenord, privata nycklar och liknande är åtkomliga för andra än utpekade administratörer.

4.3.3 All network communication between systems related to Identity or Credential management MUST be secure and encrypted or be physically secured by other means.

All kommunikation inom identitetshanteringssystemen sker krypterad med TLS-kryptering med minst 2048 bitar RSA eller motsvarande

4.3.4 Relying Party and Identity Provider credentials MUST NOT use shorter comparable key strength than a 2048-bit RSA key

SAML-nycklar har en nyckellängd på minst 2048 bitars RSA eller motsvarande.

4.4 Security-relevant Event (Audit) Records

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

4.4.1 The Member Organisation MUST maintain a log of all relevant security events concerning the operation of the Identity Provider and the underlying systems.

Loggning sker av alla händelser relaterade till identitetshanteringssystemen. Loggarna skrivs till en central loggserver som är skyddad för åtkomst där enbart IRT-gruppen har behörighet. Ett urval av händelser är åtkomligt via webbgränssnitt för servicedeskpersonal och motsvarande.

4.5 Incident Management

4.5.1 The Member Organisation MUST follow the SWAMID Incident Management Procedure in case of a suspected security incident if

Umeå universitet följer SWAMIDs incidenthanteringsprocess i händelse av säkerhetsincident relaterad till Umeå universitets IdP eller användare med påverkan på federerade inloggningar.

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.

5.1.1 The Identity Provider MUST authenticate Subjects at the request of the Relying Party.

Umeå universitet använder Microsofts Active Directory:s inbyggda lösenordskrav med minimum åtta (8) tecken varav minst en av vardera versal, gemen samt siffra.

Vid multifaktorautentisering så används någon av dessa:

1. Microsofts Authenticator-app med pushnotifiering och inmatningskrav kopplad till användaren i Azure AD som andra faktor i kombination med användarens lösenord (Single-Factor Cryptographic Software in combination with memorised secret)
2. TOTP i Authenticator-app kopplad till användaren i Azure AD som andra faktor i kombination med användarens lösenord (Single-Factor OTP Device in combination with memorised secret)
3. TOTP-dosa kopplat till användaren i Azure AD som andra faktor i kombination med användarens lösenord (Single-Factor OTP Device in combination with memorised secret)
4. TOTP-dosa kopplat till användaren i Azure AD som andra faktor i kombination med användarens lösenord (Single-Factor OTP Device in combination with memorised secret)
5. Svensk e-legitimation på minst tillitsnivå 3 i kombination med användarens lösenord, personnummer används för att knyta inloggning till identitet vid Umeå universitet

Användare som saknar en andra faktor kan själva registrera en sådan i Azure AD med enbart lösenordsinloggning. När väl en andra faktor registrerats i Azure AD för en användare är denna oberoende av användarens lösenord. Lösenordet går inte att använda för att påverka den andra faktorn eller tvärtom. Samma gäller för TOTP-dosor.

Microsoft anser att deras Authenticator-app med pushnotifiering uppfyller kraven för Single-Factor Cryptographic Software enligt NIST 800-63B. Detta beskrivs i Microsofts dokumentation för *Achieving NIST AALs*, https://docs.microsoft.com/en-us/azure/active-directory/standards/nist-authenticator-types - Microsoft Authenticator App (Notification). Umeå universitets bedömning är att detta stämmer och att Microsoft Authenticator-appen uppfyller kraven för Single-Factor Cryptographic

Software i NIST 800-63B när den används med pushnotifieringar och godkännande av inloggning i appen.

För att minimera risken för phishing och oavsiktliga inloggningar så kräver inloggning via pushnotifieringar i Microsoft Authenticator-appen inmatning av två siffror som visas i användarens webbläsare vid inloggning. Användaren anger siffrorna i Microsofts Authenticator-app och får också upp en karta som visar var webbläsaren som initierade inloggningen befinner sig (baserat på IP-adress). Om fel siffror anges avbryts inloggningen.

Vissa användare vill inte använda sina mobiltelefoner för MFA. Dessa får typiskt en TOTP-dosa istället.

5.1.2 All protocols used MUST be protected against message replay.

De protokoll som används är skyddade mot message replay. För alla system som är kopplade mot universitetets inloggningstjänst är trafiken krypterad med TLS.

5.1.3 Subjects MUST be actively discouraged from sharing credentials with other subjects

Enligt lösenordspolicyn får inga lösenord, pinkoder eller enheter som används för inloggning delas med andra. Lösenordspolicyn i sin helhet finns på https://www.aurora.umu.se/globalassets/dokument/universitetsforvaltningen/enheten-for-it-stod-och-systemutveckling-its/regler/skyddade/68770_losenord.pdf.

5.1.4 The organisation MUST take into account applicable system threats

Säkerhetsövervakning sker löpnade genom loggning, genomgång/analys av loggar, övervakning, etc. Vid införande av nya system eller större förändringar i befintliga lösningar, sker säkerhetsgranskning genom universitetets IRT verksamhet. Alla kodförändringar granskas av utvecklare/testare innan de driftsätts.

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 Each Subject assertion MUST include a unique representation of one or more administrative domain(s)

Universitets DNS-domän för identitetshantering är umu.se. Denna används som Scope i SAML WebSSO och eduroam. Umeå universitet äger domänen umu.se.

5.2.2 Each Identity Provider instance MUST have a globally unique identifier

Umeå universitets SAML-IdP har ett unikt entityID, RADIUS-servern för eduroam har ett unikt DNS-namn.

5.2.3 Each Subject MUST be represented by one or more globally unique identifiers.

Varje användare är unikt identifierad med ett användarnamn.

Alla användarnamn sparas och återanvänds inte till andra personer.

5.2.4 If the Subject have more than one unique identifier within the Identity Provider the Subject MUST be able to choose which one to be used at login.

Vid inloggning anger användaren sitt användarnamn. Om den har flera kan den själv välja vilket den anger.

5.2.5 Identity proofing MUST be done in order to issue credentials. Credential issuing or renewed identity proofing MUST be done using one of the defined methods.

Legitimationskontroll

Vid all kontroll av legitimation sker matchning mellan identitetshandling och de uppgifter som finns kopplat till kontot i Koncernkatalogen. Giltiga legitimationshandlingar vid Umeå universitet är de legitimationshandlingar som är godkända av polisen för utfärdande av svenskt pass, internationella pass som uppfyller IAO Doc 9303 samt nationella id-kort inom EU/EES som uppfyller EU-förordningen 2019/1157.

Vid legitimationskontroll via skanning av digital representation av resehandling i e-legitimation (se nedan för när det används) finns dokumentation som personal följer.

Sammanfattning utlämningsmetoder

Nedan följer en sammanställning av utlämningsmetoder. Metoderna i första kolumnen refererar till motsvarande metod i punktlistan under 5.2.5 i respektive tillitsprofil.

Metod	**Personal**	**Student**
Utdelning av konto		
AL1 metod 1		Antagning.se.interimspersonnummer
AL1 metod 4	Post/e-post/sms	e-post Ladok intersimspersonnummer, e-post och inskannat pass
AL1 metod 5	Via chef/katalogansvarig	
AL2 metod 1	eduID/Antagning.se personnummer	eduID/Antagning.se personnummer

AL2 metod 1	eduID utan personnummer AL2	eduID utan personnummer AL2
AL2 metod 2	Svensk e-legitimation personnummer	Svensk e-legitimation personnummer
AL2 metod 2	Svensk e-legitimation utan personnummer via Freja eID	Svensk e-legitimation utan personnummer via Freja eID
AL2 metod 2		Svensk e-legitimation Freja-UPI
AL2 metod 3	eIDAS	eIDAS
AL2 metod 4	Svensk legitimationshandling	Svensk legitimationshandling
AL2 metod 5	Utländsk legitimationshandling	Utländsk legitimationshandling
AL2 metod 6	Folkbokföringsadress	Folkbokföringsadress
AL2 metod 7	Inskannad legitimationshandling och hushållsräkning	Inskannad legitimationshandling och hushållsräkning
AL2 metod 8	Treparts videosamtal	Fysiskt möte eller videosamtal student med skyddade identitetsuppgifter digital representation av e-legitimation
AL2 metod 8		eduGAIN-IdP RAF-medium ESI
AL2 metod 8		eduGAIN-IdP RAF-medium subject-id
Registrering av andra faktor		
AL1/AL2 metod 1	Authenticator-app mot Azure via inloggning via egen IdP	Authenticator-app mot Azure via inloggning via egen IdP
AL1/AL2 metod 4	TOTP-dosa svensk legitimationshandling	TOTP-dosa svensk legitimationshandling
AL1/AL2 metod 5	TOTP-dosa utländsk legitimationshandling	TOTP-dosa utländsk legitimationshandling
AL1/AL2 metod 6	TOTP-dosa folkbokföringsadress	TOTP-dosa folkbokföringsadress
AL1/AL2 metod 7	TOTP-dosa hushållsräkning	TOTP-dosa hushållsräkning
Höjning av tillitsnivå		
AL3 metod 1	SWAMID-IdP med personnummer	SWAMID-IdP med personnummer
AL3 metod 1	SWAMID-IdP utan personnummer (eppn/subject-id)	SWAMID-IdP utan personnummer (eppn/subject-id)
AL3 metod 2	Svensk e-legitimation personnummer	Svensk e-legitimation personnummer
AL3 metod 2	Svensk e-legitimation Freja-UPI	Svensk e-legitimation Freja-UPI
AL3 metod 3	eIDAS	eIDAS

Personal/extern person

AL1 metod 4, post/e-post/sms

Tidsbegränsad engångskod distribueras till ansvarig chef/kataloganvarig som överlämnar koden oförändrad till användaren via post, e-post eller sms. För säkerställande av att användaren är en person används en CAPTCHA i samband med aktivering. Användarens personnummer från personalkatalogen används som identifierare.

AL1 metod 5, personlig utlämning

Tidsbegränsad engångskod distribueras till ansvarig chef/kataloganvarig som överlämnar koden oförändrad till användaren mot uppvisande av legitimation. Användarens personnummer från personalkatalogen används som identifierare.

AL2 metod 1 eduID/Antagning.se, med svenskt personnummer

Aktivering i kontoaktiveringsportal via inloggning på minst SWAMID AL2-nivå mot eduID eller Antagning.se. Personnummer matchas mot personalkatalogen.

AL2 metod 1 eduID, utan svenskt personnummer

Aktivering i kontoaktiveringsportal via inloggning på minst SWAMID AL2-nivå mot eduID. Matchning görs på de fördefinierade identifierarna namn och födelsedata mot personalkatalogen/kontot. Hela efternamnet och minst ett förnamn måste stämma. Viss variation tillåts (totalt två tecken fel enligt levenshteinavståndet). Vid misslyckad matchning kan ärende läggas för manuell riskbaserad bedömning. Eppn/subject-id från eduID sparas som identifierare för att möjliggöra senare lösenordsåterställning utan riskbaserad bedömning.

AL2 metod 2 svensk e-legitimation, med svenskt personnummer

Aktivering i kontoaktiveringsportal via inloggning med svensk e-legitimation på minst tillitsnivå 3. Användarens personnummer från personalkatalogen används som identifierare.

AL2 metod 2 svensk e-legitimation, Freja eID utan svenskt personnummer

Aktivering i kontoaktiveringsportal via inloggning med svensk e-legitimation från Freja eID på minst tillitsnivå 3. Matchning görs på de fördefinierade identifierarna namn och födelsedata mot personalkatalogen/kontot. Hela efternamnet och minst ett förnamn måste stämma. Viss variation tillåts (totalt två tecken fel enligt levenshteinavståndet). Vid misslyckad matchning kan ärende läggas för manuell riskbaserad bedömning.

Freja eID har en intern identifierare för alla användare, Unique Personal Identifier (Freja-UPI), som har samma värde för alla tjänster. Denna bibehålls för en person även vid utfärdande av ny e-legitimation så länge som Freja kan säkerställa att det rör sig om samma individ.

Freja-UPI från Freja sparas som identifierare för att möjliggöra senare lösenordsåterställning utan riskbaserad bedömning.

AL2 metod 3 eIDAS, utan svenskt personnummer

Aktivering i kontoaktiveringsportal via inloggning på minst tillitsnivå substantial via eIDAS. Matchning görs på de fördefinierade identifierarna namn och födelsedata mot personalkatalogen/kontot. Hela efternamnet och minst ett förnamn måste stämma. Viss variation tillåts (totalt två tecken fel enligt levenshteinavståndet). Vid misslyckad matchning kan ärende läggas för manuell riskbaserad bedömning. Prid från eIDAS sparas som identifierare för att möjliggöra senare lösenordsåterställning utan riskbaserad bedömning.

AL2 metod 4, med svenskt personnummer

Legitimering i ServiceDesk där tidsbegränsad engångskod lämnas ut. Personnummer används som identifierare.

AL2 metod 5, utan svenskt personnummer

Legitimering i ServiceDesk där tidsbegränsad engångskod lämnas ut. Namn och födelsedata används som identifierare. Passnummer och utfärdandeland sparas för att möjliggöra senare lösenordsåterställning utan riskbaserad bedömning.

AL2 metod 6, med svenskt personnummer

En tidsbegränsad engångskod skickas till användarens folkbokföringsadress. Personnummer används som identifierare.

AL2 metod 7, med eller utan svenskt personnummer

Personer som bor utomlands kan skicka in kopia av identitetshandling (enligt Legitimationskontroll ovan) och hushållsräkning (elräkning eller motsvarande) där namn matchar. En tidsbegränsad engångskod skickas till postadressen på hushållsräkningen som ej får vara en svensk postadress. Personnummer eller namn och födelsedata används som identifierare. Passnummer och utfärdandeland sparas som identifierare för att möjliggöra senare lösenordsåterställning utan riskbaserad bedömning.

AL2 metod 8, treparts videosamtal, med eller utan svenskt personnummer

Identifiering via videosamtal enligt av SWAMID Board of Trustees godkänd rutin (https://wiki.sunet.se/display/SWAMID/SWAMID+BoT+2021-03-11) mellan kontoadministratör (ServiceDesk-personal), betrodd part (kollega eller blivande kollega som känner kontoinnehavare) samt kontoinnehavare. Personnummer eller namn och födelsedata används som identifierare. Passnummer och utfärdandeland sparas som identifierare för att möjliggöra senare lösenordsåterställning utan riskbaserad bedömning.

Studenter

AL1 metod 1 Antagning.se, med interimspersonnummer

Aktivering i kontoaktiveringsportal via inloggning på minst SWAMID AL1-nivå mot Antagning.se. Interimspersonnummer matchas mot Ladok.

AL1 metod 4, e-postadress i Ladok, med interimspersonnummer

Tidsbegränsad engångskod skickas till antagen students e-postadress i Ladok. Aktivering görs i kontoaktiveringsportal. För säkerställande av att användaren är en person används en CAPTCHA i samband med aktivering. Användarens interimspersonnummer från Ladok används som identifierare.

AL1 metod 4, e-post och skannad identitetshandling, utan svenskt personnummer

Uppladdning av skannad bild av identitetshandling (enligt Legitimationskontroll ovan). ServiceDesk granskar bilden och utfärdar en tidsbegränsad engångskod som skickas till uppgiven e-postadress. För säkerställande av att användaren är en person används en CAPTCHA i samband med aktivering. Namn och födelsedata används som identifierare. Passnummer och utfärdandeland sparas för att möjliggöra senare lösenordsåterställning utan riskbaserad bedömning.

AL2 metod 1 eduID/Antagning.se, med svenskt personnummer

Aktivering i kontoaktiveringsportal via inloggning på minst SWAMID AL2-nivå mot eduID eller Antagning.se. Personnummer matchas mot Ladok.

AL2 metod 1 eduID, utan svenskt personnummer

Aktivering i kontoaktiveringsportal via inloggning på minst SWAMID AL2-nivå mot eduID. Matchning görs på de fördefinierade identifierarna namn och födelsedata mot Ladok/kontot. Hela efternamnet och minst ett förnamn måste stämma. Viss variation tillåts (totalt två tecken fel enligt levenshteinavståndet). Vid misslyckad matchning kan ärende läggas för manuell riskbaserad bedömning. Eppn/subject-id från eduID sparas som identifierare för att möjliggöra senare lösenordsåterställning utan riskbaserad bedömning.

AL2 metod 2 svensk e-legitimation, med svenskt personnummer

Aktivering i kontoaktiveringsportal via inloggning med svensk e-legitimation på minst tillitsnivå 3. Användarens personnummer från Ladok används som identifierare.

AL2 metod 2 svensk e-legitimation, Freja eID utan svenskt personnummer

Aktivering i kontoaktiveringsportal via inloggning med svensk e-legitimation från Freja eID på minst tillitsnivå 3. Matchning görs på de fördefinierade identifierarna namn och födelsedata mot Ladok/kontot. Hela efternamnet och minst ett förnamn måste stämma. Viss variation tillåts (totalt två tecken fel enligt levenshteinavståndet). Vid misslyckad matchning kan ärende läggas för manuell riskbaserad bedömning.

Freja eID har en intern identifierare för alla användare, Unique Personal Identifier (Freja-UPI), som har samma värde för alla tjänster. Denna bibehålls för en person även vid utfärdande av ny e-legitimation så länge som Freja kan säkerställa att det rör sig om samma individ.

Freja-UPI från Freja sparas som identifierare för att möjliggöra senare lösenordsåterställning utan riskbaserad bedömning.

AL2 metod 2 svensk e-legitimation, med Freja-UPI

Aktivering i kontoaktiveringsportal via inloggning med svensk e-legitimation från Freja eID på minst tillitsnivå 3 där Freja-UPI förmedlas. Freja-UPI från inloggning matchas mot Freja-UPI-värde på student i Ladok.

Freja eID har en intern identifierare för alla användare, Unique Personal Identifier (Freja-UPI), som har samma värde för alla tjänster. Denna bibehålls för en person även vid utfärdande av ny e-legitimation så länge som Freja kan säkerställa att det rör sig om samma individ.

Ladok kan ha flera Freja-UPI-värden kopplade till en student som bland annat kan komma från:

- Initial ansökan där Freja-UPI använts som identifierare vid inloggning mot Antagning.se som förmedlar Freja-UPI till Ladok i samband med antagning
- Via en kontokoppling där studenten varit inloggad i Ladok och därefter autentiserat sig via en inloggning med svensk e-legitimation på minst tillitsnivå 3 som förmedlar Freja-UPI

Ladok säkerställer att kopplingen mellan Freja-UPI och student är korrekt.

AL2 metod 3 eIDAS, utan svenskt personnummer

Aktivering i kontoaktiveringsportal via inloggning på minst tillitsnivå substantial via eIDAS. Matchning görs på de fördefinierade identifierarna namn och födelsedata mot Ladok/kontot. Hela efternamnet och minst ett förnamn måste stämma. Viss variation tillåts (totalt två tecken fel enligt levenshteinavståndet). Vid misslyckad matchning kan ärende läggas för manuell riskbaserad bedömning. Prid från eIDAS sparas som identifierare för att möjliggöra senare lösenordsåterställning utan riskbaserad bedömning.

AL2 metod 4, med svenskt personnummer

Legitimering i ServiceDesk där tidsbegränsad engångskod lämnas ut. Personnummer används som identifierare.

AL2 metod 5, utan svenskt personnummer

Legitimering i ServiceDesk där tidsbegränsad engångskod lämnas ut. Namn och födelsedata används som identifierare. Passnummer och utfärdandeland sparas för att möjliggöra senare lösenordsåterställning utan riskbaserad bedömning.

AL2 metod 6, med svenskt personnummer

En tidsbegränsad engångskod skickas till användarens folkbokföringsadress. Personnummer används som identifierare.

AL2 metod 7, med eller utan svenskt personnummer

Studenter som bor utomlands kan skicka in kopia av identitetshandling (enligt Legitimationskontroll ovan) och hushållsräkning (elräkning eller motsvarande) där namn matchar. En tidsbegränsad engångskod skickas till postadressen på hushållsräkningen som ej får vara en svensk postadress. Personnummer eller namn och födelsedata används som identifierare. Passnummer och utfärdandeland sparas

som identifierare för att möjliggöra senare lösenordsåterställning utan riskbaserad bedömning.

AL2 metod 8, fysiskt möte/videosamtal, för studenter med skyddade identitetsuppgifter

Studenter med skyddade identitetsuppgifter har sitt riktiga personnummer i NyA/Ladok bakom skydd som endast ett fåtal utvalda handläggare vid lärosätet har tillgång till. Där finns koppling till studentens interimspersonnummer som används i lärosätets system. Studentens riktiga personnummer ska exponeras så lite som möjligt, det är därför olämpligt att använda inloggning via svensk e-legitimation i lärosätets system för dessa studenter.

Handläggare med tillgång till skyddade identitetsuppgifter i NyA/Ladok identifierar studenten under fysiskt möte med kontroll av legitimation eller under videosamtal med hjälp av skanning av digital representation av resehandling i e-legitimation i BankID-app eller genom styrkt kontroll med skanner, se Identitetskontroll via digital representation av resehandling i e-legitimation (SWAMID AL2). Handläggaren plockar fram studentens interimspersonnummer ur NyA/Ladok utifrån identifierat svenskt personnummer och söker fram studentens lärosäteskonto baserat på interimspersonnumret. Handläggaren förmedlar en tidsbegränsad engångskod till studenten under mötet som ger tillgång till kontot. Handläggaren kan också ta hjälp av en kontoadministratör från ServiceDesk för hantering av lärosäteskonto/engångskod vid behov.

AL2 metod 8 eduGAIN-IdP, med European Student Identifier

Aktivering i kontoaktiveringsportal via inloggning på minst REFEDS Assurance Framework (RAF) medium-nivå mot IdP inom eduGAIN. European Student Identifier (ESI) från inloggning matchas mot ESI-värde på student i Ladok.

Ladok kan ha flera ESI-värden kopplade till en student som bland annat kan vara:

- Utländskt lärosätes ESI för studenten som följer med vid initial ansökan på Antagning.se där ESI använts som identifierare vid inloggning som sedan förmedlas till Ladok i samband med antagning
- Utländskt lärosätes ESI för studenten som är inmatat/inhämtat från ett Learning Agreement (LA) inom Erasmus Without Paper (EWP)
- Utländskt lärosätes ESI som studenten kopplat till sin identitet i Ladok via en kontokoppling där studenten varit inloggad i Ladok och därefter autentiserat sig via en inloggning från en annan IdP i eduGAIN som förmedlat ESI för studenten
- Internt Ladok-ESI för en student som delas mellan Ladok/Antanging.se, baserat på ExterntStudentUID/STUDENT_UID

Ladok säkerställer att kopplingen mellan ESI och student är korrekt.

Subject-id sparas för att möjliggöra senare lösenordsåterställning utan ESI eller riskbaserad bedömning.

AL2 metod 8 eduGAIN-IdP, med subject-id

Aktivering i kontoaktiveringsportal via inloggning på minst REFEDS Assurance Framework (RAF) medium-nivå mot IdP inom eduGAIN. Subject-id från inloggning matchas motsubject-id-värde på student i Ladok.

Ladok kan ha flera subject-id-värden kopplade till en student som bland annat kan komma från:

- Initial ansökan där subject-id använts som identifierare vid inloggning mot Antagning.se som förmedlar subject-id till Ladok i samband med antagning
- Via en kontokoppling där studenten varit inloggad i Ladok och därefter autentiserat sig via en inloggning från en annan IdP i eduGAIN som förmedlar subject-id

Ladok säkerställer att kopplingen mellan subject-id och student är korrekt.

MFA på SWAMID AL1- och AL2-nivå

Användare med tillitsnivå AL1 och AL2 som inte har en andra faktor kopplad till sin identitet kan koppla en andra faktor till sin identitet och använda den för att utföra inloggning enligt profilen REFEDS MFA i SWAMID och eduGAIN.När väl en andra faktor kopplats till en användare är denna oberoende av användarens lösenord. Lösenordet går inte att använda för att påverka den andra faktorn eller tvärtom. Se även 5.1.1 ovan.

AL1/AL2 metod 1 registrering av authenticator-app mot Azure via inloggning mot egen IdP

Användaren loggar in i Microsoft 365 med sitt användarnamn och lösenord och kan där registrera en authenticator-app. AL-nivå bibehålls.

AL1/AL2 metod 4, utdelning av TOTP-dosa, med svenskt personnummer

Legitimering i ServiceDesk där en TOTP-dosa lämnas ut. ServiceDesk-personal kopplar TOTP-dosan som en andra faktor till användaren. Personnummer används som identifierare. AL-nivå bibehålls.

AL1/AL2 metod 5, utdelning av TOTP-dosa, utan svenskt personnummer

Legitimering i ServiceDesk där en TOTP-dosa lämnas ut. ServiceDesk-personal kopplar TOTP-dosan som en andra faktor till användaren. Namn och födelsedata används som identifierare. AL-nivå bibehålls.

AL1/AL2 metod 6, utdelning av TOTP-dosa, med svenskt personnummer

En TOTP-dosa skickas till användarens folkbokföringsadress. ServiceDesk-personal kopplar TOTP-dosan som en andra faktor till användaren. Personnummer används som identifierare. AL-nivå bibehålls.

AL1/AL2 metod 7, utdelning av TOTP-dosa, med eller utan svenskt personnummer

Personer som bor utomlands kan skicka in kopia av identitetshandling (enligt Legitimationskontroll ovan) och hushållsräkning (elräkning eller motsvarande) där namn matchar. En TOTP-dosa skickas till postadressen på hushållsräkningen som ej får vara en svensk postadress. ServiceDesk-personal kopplar TOTP-dosan som en andra faktor till användaren. Personnummer eller namn och födelsedata används som identifierare. AL-nivå bibehålls.

5.2.6 The Member Organisation MUST maintain a record of all changes regarding Assurance Level of Subjects.

Loggning sker av samtliga förändringar av tillitsnivå kopplat till respektive individ. Dessa sparas så länge de behövs för att utreda säkerhetsincidenter.

Höjning av tillitsnivå

Samtliga AL2-metoder beskrivna under 5.2.5 ovan kan även användas för att AL2-bekräfta ett AL1-konto. De förregistrerade identifierarna används för att säkerställa att det är samma individ som identifieras.

Sänkning av tillitsnivå

I samband med återställning av lösenord och andra faktorer kan i vissa fall tillitsnivån sänkas. Se 5.3.3 för beskrivning av detta.

Verifierade identiteter (SWAMID AL3-nivå)

Efter att ha kopplat en andra faktor till sin identitet enligt AL1/AL2 ovan så kan användare knyta sin andra faktor till sin identitet på verifierad nivå genom en kontohanteringsportal.

Användarens andra faktor kan sedan, i kombination med användarens användarnamn och lösenord, användas för autentisering på SWAMID AL3-nivå.

AL3 metod 1, SWAMID-IdP med svenskt personnummer

Inloggning sker med användarens andra faktor i kombination med användarnamn och lösenord varpå användaren autentiserar sig med inloggning på SWAMID AL3-nivå mot en IdP i SWAMID. Mappning mellan lokalt konto och inloggning mot IdP i SWAMID görs med personnummer.

AL3 metod 1, SWAMID-IdP utan svenskt personnummer (eppn/subject-id)

Inloggning sker mot kontohanteringsportal med användarens andra faktor i kombination med användarnamn och lösenord. Användaren är därmed lokalt identifierad på AL1- eller AL2-nivå.

Ytterligare en autentisering sker mot SWAMID-IdP. Om inloggningen uppfyller SWAMID AL3 (assurance, AssuranceCertifikation respektive AuthnContext) görs ett försök att matcha inloggningen mot användarens lokala konto. Detta görs med tidigare registrerad eppn/subject-id som identifierare om det finns för lokalt konto.

Genom en MFA-inloggning med lokalt konto säkerställs att det är innehavaren av kontot som utför höjningen. Matchningen på eppn/subject-id mellan lokalt konto och SWAMID AL3-inloggning säkerställer att det är den verifierade individen som innehar det lokala kontot.

Denna metod kan inte användas om eppn/subject-id saknas för lokalt konto.***AL3 metod 2, svensk e-legitimation, med svenskt personnummer***

Inloggning sker med användarens andra faktor i kombination med användarnamn och lösenord varpå användaren autentiserar sig med svensk e-legitimation på minst tillitsnivå 3. Mappning mellan lokalt konto och svensk e-legitimation görs med personnummer.

AL3 metod 2 svensk e-legitimation, med Freja-UPI

Inloggning sker mot kontohanteringsportal med användarens andra faktor i kombination med användarnamn och lösenord. Användaren är därmed lokalt identifierad på AL1- eller AL2-nivå.

Ytterligare en autentisering sker med svensk e-legitimation från Freja eID. Om inloggningen uppfyller minst tillitsnivå 3 görs ett försök att matcha inloggningen mot användarens lokala konto. Detta görs med tidigare registrerad Freja-UPI som identifierare om det finns för lokalt konto.

Freja eID har en intern identifierare för alla användare, Unique Personal Identifier (Freja-UPI), som har samma värde för alla tjänster. Denna bibehålls för en person även vid utfärdande av ny e-legitimation så länge som Freja kan säkerställa att det rör sig om samma individ.

Genom en MFA-inloggning med lokalt konto säkerställs att det är innehavaren av kontot som utför höjningen. Matchningen på Freja-UPI mellan lokalt konto och inloggning med svensk e-legitimation från Freja eID säkerställer att det är den verifierade individen som innehar det lokala kontot.

Denna metod kan inte användas om Freja-UPI saknas för lokalt konto.

AL3 metod 3, eIDAS

Inloggning sker mot kontohanteringsportal med användarens andra faktor i kombination med användarnamn och lösenord. Användaren är därmed lokalt identifierad på AL1- eller AL2-nivå.

Ytterligare en autentisering sker mot eIDAS. Om inloggningen uppfyller minst nivå substantial görs ett försök att matcha inloggningen mot användarens lokala konto. Detta görs med tidigare registrerad prid som identifierare om det finns för lokalt konto.

Genom en MFA-inloggning med lokalt konto säkerställs att det är innehavaren av kontot som utför höjningen. Matchningen på prid mellan lokalt konto och eIDAS-inloggning säkerställer att det är den verifierade individen som innehar det lokala kontot.

Denna metod kan inte användas om prid saknas för lokalt konto.

5.2.7 The Subject MUST be able to update stored self-asserted personal information.

Identifierande information för användare på AL2- och AL3-nivå hämtas från Umeå universitets koncernkatalog, Ladok, från legitimationshandlingar eller från andra betrodda system.

Användare kan få självuppgivna uppgifter uppdaterade.

Umeå universitet har kontaktvägar till alla användare.

Tillhörighet (affiliation) för användare hämtas från koncernkatalogen för personal och från Ladok för studenter. Denna uppdateras senast 31 dagar efter beslut om ändring av tillhörighet för användare.

De enda självuppgivna kontaktuppgifterna som finns för användare är telefonnummer för anställda samt e-postadress och telefonnummer till externa personer. Dessa uppges till administratör som matar in dessa i koncernkatalogen. Det finns inget systemstöd för att bekräfta dessa men planer finns på en självservicefunktion för detta.

Självuppgiven kontaktinformation till användare bekräftas i möjligast mån.

5.2.8 To be authorised to perform identity proofing at this Identity Assurance Profile, the Registration Authority itself MUST be using credentials at this Identity Assurance Profile or higher.

All personal i ServiceDesk autentiserar sig på SWAMID AL3-nivå. Katalogansvariga loggar in i administrationsgränssnittet på minst SWAMID AL2-nivå. ServiceDesk-personal kan inte verifiera användare på SWAMID AL3-nivå, däremot kan de sänka användare från SWAMID AL3-nivå till SWAMID AL1/AL2-nivå.

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 All Subjects MUST be allowed to renew their credentials.

Användare kan själva byta sitt lösenord enligt gällande lösenordspolicy.

Efter autentisering med användarnamn, lösenord och en andra faktor så kan en till andra faktor registreras på samma tillitsnivå.

5.3.2 Subjects MUST actively demonstrate possession of current credentials in the process of credential renewal.

Vid byte av lösenord krävs att befintligt lösenord anges.

Vid byte av andra faktor så behöver befintlig andra faktor presenteras tillsammans med lösenord.

5.3.3 Credential Re-issuing MUST be done using one of the defined methods.

Sammanfattning återställningsmetoder

Nedan följer en sammanställning av återställningsmetoder. Metoderna i första kolumnen refererar till motsvarande metod i punktlistan under 5.2.5 i respektive tillitsprofil.

Metod	**Beskrivning**
Lösenordsåterställning	
Enligt 5.2.5	Enligt 5.2.5
AL1 metod 4 (endast studenter)	Verifierad e-postadress
AL1 metod 7 (endast studenter)	Videosamtal med ServiceDesk
Återställning av andra faktor	
AL1/2/3 metod 1	SWAMID-IdP med personnummer/eppn/subject-id
AL1/2/3 metod 2	Svensk e-legitimation med personnummer
AL1/2/3 metod 2	Svensk e-legitimation med Freja-UPI
AL1/2/3 metod 3	eIDAS
AL1 metod 5, AL2 metod 4/5	Legitimering i ServiceDesk
AL1 metod 4 (endast personal)	Kontakt med ServiceDesk (e-post)
AL1 metod 7	Videosamtal med ServiceDesk
AL1 metod 7, AL2 metod 8 (endast skyddade studenter)	Fysiskt möte eller videosamtal student med skyddade identitetsuppgifter digital representation av e-legitimation

Återställning av lösenord

- Enligt ordinarie utlämningsrutiner (AL-nivå enligt utlämningsrutin)

Återställning av lösenord kan göras enligt samma rutiner som under 5.2.5 med kontroll mot tidigare identifierare för kontot för att säkerställa att det rör sig om samma individ. AL-nivå erhålls enligt beskrivning under 5.2.5.

- Studenter: Engångslänk till verifierad e-postadress (AL-nivå sänks till AL1)

Studenter kan även återställa sitt lösenord via tidsbegränsad engångslänk till privat e-postadress som registrerats och verifierats vid etablering av identitet vid Umeå universitet eller senare. Detta ger tillitsnivå AL1.

Efter detta kan kontot höjas till AL2/AL3 enligt 5.2.6.

- Studenter: Via videosamtal med ServiceDesk (AL-nivå sänks till AL1)

Studenter utan verifierad e-postadress kan återställa sitt lösenord via ett videosamtal med ServiceDesk:

1. Användaren skickar in en fysisk eller elektronisk kopia av sin legitimationshandling till ServiceDesk
2. Användaren kopplar upp sig i ett videosamtal tillsammans med ServiceDesk-personal
3. Användaren visar upp den legitimationshandling som i förväg skickats in
4. Legitimationshandlingen kontrolleras av ServiceDesk-personal och jämförs med identitetsuppgifter för användarens konto
5. ServiceDesk-personal sänker kontot till AL1
6. ServiceDesk-personal skickar ut ett e-postmeddelande till användarens e-postadress och ett SMS (om mobilnummer finns registrerat) som beskriver att ett videosamtal har hållits med användaren där en ny kontoaktiveringskod har förmedlats. Meddelandena är endast informativa för att minska skadan vid eventuell identitetsstöld. Inga känsliga uppgifter skickas i meddelandet.
7. ServiceDesk-personal uppger en tidsbegränsad engångskod för användaren som kan användas för att sätta ett nytt lösenord på kontot

Efter detta kan kontot höjas till AL2/AL3 enligt 5.2.6.

Återställning av andra faktor

- Via inloggning mot SWAMID AL3-IdP i SWAMID (bibehållen AL-nivå)

Om användare har tappat sin andra faktor så kan den ersättas med en ny med hjälp av inloggning mot IdP i SWAMID på AL3-nivå. Användaren loggar in med användarnamn/lösenord, i kombination med inloggning mot IdP i SWAMID på AL3-nivå, i en kontohanteringsportal där en tidsbegränsad engångskod från Microsoft 365 genereras. Mappning mellan lokalt konto och inloggning mot IdP i SWAMID görs med personnummer eller eppn/subject-id. Koden kan sedan användas i Microsoft 365 för att registrera en ny andra faktor kopplad till användarens konto. Kontot behåller befintlig AL-nivå.

- Via svensk e-legitimation, med svenskt personnummer (bibehållen AL-nivå)

Om användare har tappat sin andra faktor så kan den ersättas med en ny med hjälp av inloggning med svensk e-legitimation på minst tillitsnivå 3. Användaren loggar in med användarnamn/lösenord i kombination med svensk e-legitimation i en kontohanteringsportal där en tidsbegränsad engångskod från Microsoft 365 genereras. Mappning mellan lokalt konto och e-legitimation görs med personnummer. Koden kan sedan användas i Microsoft 365 för att registrera en ny andra faktor kopplad till användarens konto. Kontot behåller befintlig AL-nivå.

- Via svensk e-legitimation, med Freja-UPI (bibehållen AL-nivå)

Om användare har tappat sin andra faktor så kan den ersättas med en ny med hjälp av inloggning med svensk e-legitimation från Freja eID på minst tillitsnivå 3.

Användaren loggar in med användarnamn/lösenord i kombination med svensk e-legitimation från Freja eID i en kontohanteringsportal där en tidsbegränsad engångskod från Microsoft 365 genereras. Mappning mellan lokalt konto och e-legitimation görs med Freja-UPI. Koden kan sedan användas i Microsoft 365 för att registrera en ny andra faktor kopplad till användarens konto. Kontot behåller befintlig AL-nivå.

- Via eIDAS (bibehållen AL-nivå)

Om användare har tappat sin andra faktor så kan den ersättas med en ny med hjälp av inloggning med eIDAS på minst tillitsnivå substantial. Användaren loggar in med användarnamn/lösenord i kombination med eIDAS i en kontohanteringsportal där en tidsbegränsad engångskod från Microsoft 365 genereras. Mappning mellan lokalt konto och eIDAS görs med prid. Koden kan sedan användas i Microsoft 365 för att registrera en ny andra faktor kopplad till användarens konto. Kontot behåller befintlig AL-nivå. Notera att användaren inte kan använda denna återställningsmetod om användaren bytt europeisk e-legitimation och i samband med detta fått en ny prid.

- Via besök i ServiceDesk (AL3 sänks till AL2, annars bibehållen AL-nivå)

Alla användare kan också besöka ServiceDesk, legitimera sig och få en tidsbegränsad engångskod från Microsoft 365. Personnummer, namn och födelsedata för riskbaserad bedömning eller passnummer och utfärdandeland används som identifierare. Om kontot är på AL3-nivå så sänks det till AL2. Koden kan sedan användas i Microsoft 365 för att registrera en ny andra faktor kopplad till användarens konto.

Efter detta kan kontot, om det sänkts till AL2, höjas till AL3 enligt 5.2.6.

- Personal: Via kontakt med ServiceDesk (AL-nivå sänks till AL1)

Personal som varken kan använda svensk e-legitimation eller besöka ServiceDesk kan kontakta ServiceDesk som då:

1. Sänker kontot till AL1
2. Skickar ut ett e-postmeddelande till användarens tjänste-e-postadress och ett SMS (om mobilnummer finns registrerat) som beskriver att detta skett och varför
3. Skickar ut en tidsbegränsad engångskod från Microsoft 365 till användarens e-postadress som kan användas i Microsoft 365 för att registrera en ny andra faktor

Efter detta kan kontot höjas till AL2/AL3 enligt 5.2.6.

- Via videosamtal med ServiceDesk (AL-nivå sänks till AL1)

Användare som inte har tillgång till den e-postadress som är kopplad till användarens konto (exempelvis för att det krävs MFA för åtkomst till e-posten) kan byta ut sin andra faktor via ett videosamtal med ServiceDesk:

1. Användaren skickar in en fysisk eller elektronisk kopia av sin legitimationshandling till ServiceDesk

2. Användaren kopplar upp sig i ett videosamtal tillsammans med ServiceDesk-personal
3. Användare utför en inloggning där en kod som uppges av ServiceDesk-personalen anges
4. ServiceDesk-personal verifierar att förväntad användare loggat in och angivit koden
5. Användaren visar upp den legitimationshandling som i förväg skickats in
6. Legitimationshandlingen kontrolleras av ServiceDesk-personal och jämförs med identitetsuppgifter för användarens konto
7. ServiceDesk-personal sänker kontot till AL1
8. ServiceDesk-personal skickar ut ett e-postmeddelande till användarens e-postadress och ett SMS (om mobilnummer finns registrerat) som beskriver att detta skett och varför. Meddelandena är endast informativa för att minska skadan vid eventuell identitetsstöld. Inga känsliga uppgifter skickas i meddelandena.
9. ServiceDesk-personal uppger en tidsbegränsad engångskod från Microsoft 365 för användaren som kan användas i Microsoft 365 för att registrera en ny andra faktor

Efter detta kan kontot höjas till AL2/AL3 enligt 5.2.6.

- Via fysiskt möte/videosamtal, för studenter med skyddade identitetsuppgifter (AL3 sänks till AL2, annars bibehållen AL-nivå)

Enligt metod för studenter med skyddade identitetsuppgifter under 5.2.5, som också kan användas för lösenordsåterställning. I stället för en tidsbegränsad engångskod för tillgång till konto förmedlas en tidsbegränsad engångskod från Microsoft 365 som kan användas i Microsoft 365 för att registrera en ny andra faktor.

5.4 Credential Revocation

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

5.4.1 The Member Organisation MUST be able to revoke a Subject's credentials.

Umeå universitet kan revokera/inaktivera användarkonton på användarens egen eller organisationens begäran.

Inaktiverade konton kan inte aktiveras utan explicit beslut från organisationen.

Det finns rutiner för inaktivering av konton vid avslutade studier/avslutad anställning.

5.4.2 Credential Issuing after Credential Revocation MUST be done using one of the defined methods.

Återaktivering efter revokering/inaktivering sker enligt beskrivning i 5.3.3.

Om en användare har misskött sitt konto så kan IRT inaktivera och svartlista kontot. Användaren kontaktas och kontot kan sedan inte aktiveras förrän ServiceDesk-personal eller IRT plockat bort kontot från listan.

5.4.3 In the event of a Credential Revocation caused by a security related incident the Member Organisation MUST take precautions to prevent the incident from reoccurring.

Vid inaktivering av konto på grund av en säkerhetsrelaterad incident kopplas IRT in som har rutiner för att säkerställa att incidenten inte återupprepas.

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 The Member Organisation MUST maintain a record of all credentials issued.

Samtliga aktiva och historiska konton sparas i ett register. All hantering av byte och revokering av lösenord och andra faktorer loggas. Tillitsnivå för konton sparas i koncernkatalogen. Denna information sparas så länge den behövs för att utreda säkerhetsincidenter.

5.5.2 The Identity Provider MUST have an availability that allows the Member Organisation to use it for internal systems.

IT-systemen för identitetshanteringen har en tillgänglighetsnivå som uppfyller kraven för att använda dem för interna system.

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 The Identity Provider MUST provide validation of credentials to a Relying Party using a protocol with defined properties.

SWAMIDs rekommendationer följs kring vilka protokoll som används mot Relying Parties.

5.6.2 The Identity Provider MUST not authenticate credentials that have been revoked.

Endast aktuella lösenord och MFAfaktorer tillåts vid autentisering.

5.6.3 The Identity Provider MUST force the Subject to demonstrate possession of current credentials in the process of authentication.

Användaren måste presentera sitt lösenord eller MFA-faktorer vid inloggning.

5.6.4 The Identity Provider MUST force the Subject to authenticate at least once every 12 hours in order to maintain an active session.

Single Sign-On i identitetssystemet är giltig i åtta (8) timmar.