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

UMEÅ UNIVERSITET

Version: 2.3 FINAL

UmU Identity Management Practice Statement

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.

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. MFA i Azura AD via Microsofts Authenticator-app med pushnotifiering och inmatningskrav i kombination med användarens lösenord (Single-Factor Cryptographic Software in combination with memorised secret)
2. MFA i Azure AD via TOTP i Authenticator-app i kombination med användarens lösenord (Single-Factor OTP Device in combination with memorised secret)
3. TOTP-dosa kopplat till användaren via Azure AD i kombination med användarens lösenord (Single-Factor OTP Device in combination with memorised secret)
4. TOTP-dosa kopplat till användaren via Azure AD i kombination med användarens lösenord (Single-Factor OTP Device in combination with memorised secret)
5. Svensk e-legitimation på LoA3-nivå i kombination med användarens lösenord

När väl en multifaktor registrerats i Azure AD för en användare så är denna oberoende av användarens lösenord. Lösenordet går inte att använda för att påverka multifaktorn 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.

Användarnamn 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.

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**
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 utan personnummer AL2	eduID/Antagning.se personnummer, eduID utan personnummer AL2
AL2 metod 2	Svensk e-legitimation	Svensk e-legitimation
AL2 metod 3	eIDAS	eIDAS
AL2 metod 4	Svensk legitimationshandling	Svensk legitimationshandling
AL2 metod 5	Utländsk legitimationshandling	Utländsk legitimationshandling
AL2 metod 7	Inskannad legitimationshandling och hushållsräkning	Inskannad legitimationshandling och hushållsräkning
AL2 metod 8	Treparts videosamtal	

Personal/extern person

Samtliga AL2-metoder nedan kan även användas för att AL2-bekräfta ett AL1-konto.

AL1 metod 4, post/e-post/sms

Tidsbegränsad engångskod distribueras till ansvarig chef/katalogansvarig 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/katalogansvarig 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 födelsedatum och namn 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 LoA3-nivå. Användarens personnummer från personalkatalogen används som identifierare.

AL2 metod 3 eIDAS, utan svenskt personnummer

Aktivering i kontoaktiveringsportal via inloggning på minst tillitsnivå substantial via eIDAS. Matchning görs på de fördefinierade identifierarna födelsedatum och namn 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. Födelsedatum och namn används som identifierare. Passnummer och utfärdandeland sparas för att möjliggöra senare lösenordsåterställning utan riskbaserad bedömning.

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 födelsedatum och namn 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 födelsedatum och namn används som identifierare. Passnummer och utfärdandeland sparas som identifierare för att möjliggöra senare lösenordsåterställning utan riskbaserad bedömning.

Studenter

Samtliga AL2-metoder nedan kan även användas för att AL2-bekräfta ett AL1-konto.

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. Födelsedatum och namn 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 födelsedatum och namn 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 LoA3-nivå. Användarens personnummer från Ladok används som identifierare.

AL2 metod 3 eIDAS, utan svenskt personnummer

Aktivering i kontoaktiveringsportal via inloggning på minst tillitsnivå substantial via eIDAS. Matchning görs på de fördefinierade identifierarna födelsedatum och namn 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. Födelsedatum och namn används som identifierare. Passnummer och utfärdandeland sparas för att möjliggöra senare lösenordsåterställning utan riskbaserad bedömning.

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 födelsedatum och namn används som identifierare. Passnummer och utfärdandeland sparas som identifierare för att möjliggöra senare lösenordsåterställning utan riskbaserad bedömning.

MFA på SWAMID AL1- och AL2-nivå

Användare med tillitsnivå AL1 och AL2 som inte har en multifaktor kopplad till sin identitet kan koppla en multifaktor till sin identitet och använda den för att utföra

inloggning enligt profilen REFEDS MFA i SWAMID och eduGAIN. Vid koppling loggar användaren in i Microsoft 365 med sitt användarnamn och lösenord och registrerar en authenticator-app.

Personal kan efter legitimering i ServiceDesk få en TOTP-dosa kopplad till sitt konto.

Verifierade identiteter (SWAMID AL3-nivå)

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

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

- Via inloggning mot SWAMID AL3-IdP i SWAMID

Inloggning sker med användarens multifaktor 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.

- Via svensk e-legitimation

Inloggning sker med användarens multifaktor i kombination med användarnamn och lösenord varpå användaren autentiserar sig med svensk e-legitimation på LoA3-nivå. Mappning mellan lokalt konto och svensk e-legitimation görs med personnummer.

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.

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

Användare kan få självuppgivna uppgifter uppdaterade.

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 multifaktor så kan en till multifaktor 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 multifaktor så behöver befintlig multifaktor presenteras tillsammans med lösenord.

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

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 5.2.5.

- 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 som beskriver att ett videosamtal har hållits med användaren där en ny kontoaktiveringskod har förmedlats. Meddelandet är endast informativt 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 5.2.5.

Återställning av multifaktor

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

Om användare har tappat sin multifaktor 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. Koden kan sedan användas i Microsoft 365 för att registrera en ny multifaktor kopplad till användarens konto. Kontot behåller befintlig AL-nivå.

- Via svensk e-legitimation (bibehållen AL-nivå)

Om användare har tappat sin multifaktor så kan den ersättas med en ny med hjälp av inloggning med svensk e-legitimation på LoA3-nivå. 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 multifaktor kopplad till användarens konto. Kontot behåller befintlig AL-nivå.

- 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, födelsedatum och namn 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 multifaktor kopplad till användarens konto.

Efter detta kan kontot, om det sänkts till AL2, höjas till AL3 enligt 5.2.5.

- 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 multifaktor

Efter detta kan kontot höjas till AL2/AL3 enligt 5.2.5.

- 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 multifaktor 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 multifaktor

Efter detta kan kontot höjas till AL2/AL3 enligt 5.2.5.

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. 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 multifaktorer loggas. Tillitsnivå för konton sparas i koncernkatalogen.

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 MFA-faktorer 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.