eduID Identity Management Practice Statement

1. Inledning

Tjänsten eduID är en identitetsutfärdare (Identity Provider) som används primärt för studenter, personal och övriga verksamma individer vid Sveriges universitet och högskolor. För studenter går eduID att använda både innan, under och efter studierna. eduID är alltså inte en identitetsutfärdare för en enskild organisation utan för all forskning och utbildning i Sverige.

eduID uppfyller kraven i tillitsprofilerna SWAMID AL1, SWAMID AL2 och SWAMID AL3.

I dokumentet betyder obekräftad användare en användare som uppfyller SWAMID AL1, bekräftad användare en användare som uppfyller SWAMID AL2 och verifierad användare en användare som uppfyller SWAMID AL3.

1.1 Uppdateringshistorik

Uppdaterad	Ansvarig	Kommentarer
2019-02-05	Pål Axelsson	Första versionen
2022-03-23	Pål Axelsson	SWAMID AL3, passwordless, eIDAS och Svipe iD
2022-11-15	Zacharias Törnblom	Brev via digital brevlåda
2024-03-12	Zacharias Törnblom	Verifiering med resehandling, Svensk e-legitimation tillitsnivå 2 för personer utan svenskt identitetsbegrepp

4. Organisational Requirement

4.1 Enterprise and Service Maturity

4.1.1 eduID drivs och utvecklas inom Sunet. Sunet är organisatoriskt en enhet inom myndigheten Vetenskapsrådet, organisationsnummer 202100-5208.

4.1.2 Vetenskapsrådets arbete definieras av flera lagar, bl.a. Lagen om Vetenskapsrådet (SFS 2000:662). Tjänsten eduID innehåller personuppgifter och det tas särskild hänsyn till EU:s dataskyddsförordning (“GDPR” (EU) 2016/679), Lag (SFS 2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning samt tillämpbara registerförordningar.

Informationssäkerhetsarbetet för eduID baseras övergripande på Vetenskapsrådets informationssäkerhetspolicy.

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

4.1.3 Rutin för hantering av lagringsmedia som tas ur drift finns och innebär att diskar och liknande som har innehållit personuppgifter för eduID låses in i ett säkerhetsskåp. Diskarna återanvänds inte och kommer när de tas ur säkerhetsskåpet destrueras på ett säkert sätt.

4.2 Notices and User Information

4.2.1 Användarvillkor för eduID presenteras för användaren när eduID-kontot skapas. Användarvillkoren finns även tillgängliga för användarna i eduID.

4.2.2 En ny användare måste godkänna användarvillkoren innan eduID-kontot skapas.

4.2.3 Då villkoren ändras måste användaren godkänna de nya villkoren i identitetsutfärdaren för eduID vid första inloggning efter ändringen.

4.2.4 Användarens acceptans av användarvillkoren lagras i eduID.

4.2.5 Tjänstedefinition och integritetsinformation för eduID finns publicerad på eduID.se under länken Hjälp i sidfoten (https://eduid.se/faq.html).

4.3 Secure Communications

4.3.1 Behörighetskontroll används för all tillgång till privata nycklar och delade hemligheter (shared secrets) som lagras på fil. Endast utsedd personal har tillgång.

4.3.2 Privata nycklar lagras åtkomstskyddat i Sunets Hardware security modules (HSM), Yubikey eller annan säker hårdvarumodul. Hemligheter som lagras på fil skyddas med strikt behörighetskontroll enligt 4.3.1.

4.3.3 Kommunikation mellan distribuerade delar av systemet sker via VPN-tunnlar med stark kryptering. Kommunikation mellan eduID, användare och tjänster skyddas med HTTPS och stark kryptering. Administrativ access till systemet görs via SSH

eller Puppet med nycklar lagrade i krypteringshårdvara (Yubikey). Alla nycklar har en styrka som motsvarar RSA 2048 bitar eller högre.

4.3.4 eduID använder minst 2048 bitar RSA för de federationsspecifika krypteringsnycklarna.

4.4 Security-relevant Event (Audit) Records

4.4.1 Alla säkerhetsrelevanta händelser loggas, både lyckade och misslyckade försök. Det innefattar bland annat:

- Skapande av konton
- Identitetsverifiering
- Inloggningsförsök (både för tjänstens användare och av administrativ tillgång till eduID)
- Ändringar av säkerhetsinställningar
- Sessioner och uppkopplingar mot brandväggar
- Säkerhetsrelaterade händelser i operativsystemet

NTP används för att synkronisera tid för alla komponenter för att säkerställa att alla logghändelser är synkroniserade.

5. Operational Requirements

5.1 Credential Operating Environment

5.1.1 Användare i eduID tillgång till flera olika inloggningstekniker. De kan använda en eller flera av dem parallellt. Multifaktorinloggning uppfyller även kraven för 1-faktorsinloggning.

Tabell över inloggningsmetoder i eduID:

Inloggningsmetod	1-faktorsinloggning	Multifaktorsinloggning
Lösenord	✓	
Lösenordsfri inloggning via 1-faktors WebAuthn Credential	✓	
2-faktors WebAuthn Credential	✓	✓
1-faktors WebAuthn Credential tillsammans med lösenord	✓	✓
Svensk e-legitimation och eIDAS	✓	✓
Logga in med annan enhet	✓	Endast om inloggning sker med multifaktor

Lösenord

När en användare sätter ett lösenord i eduID erbjuds automatgenererade lösenord som har minst en “score” 4 enligt metoden zxcvbn. Användaren kan också välja ett eget lösenord och då har detta minst en “score” 3 enligt samma metod.

Lösenordsfri inloggning via 1-faktors WebAuthn Credential

I eduID används WebAuthn med bakomliggande FIDO2 Authenticator för lösenordsfri inloggning. Vid registrering av en FIDO2 Authenticator kontrolleras att den är certifierad av Fido Alliance, alternativt i vissa undantagsfall särskilt verifierad av eduID. Certifieringen, eller i förekommande fall den särskilda verifieringen, säkerställer att aktuell FIDO2 Authenticator uppfyller kraven för Single-Factor Cryptographic Software eller kraven för Single-Factor Cryptographic Device i NIST 800-63-3B. Specifikationen för FIDO User Authentication Specifications finns publicerade på adressen https://fidoalliance.org/specifications/.

En 1-faktors WebAuthn Credential i eduID kan vara av två typer; antingen en FIDO2 Platform Authenticator (enhetsbaserad säkerhetsnyckel) eller en FIDO2 Cross-Platform Authenticator (fristående säkerhetsnyckel, även kallat Roaming Authenticator). Det som skiljer dessa bägge åt är att en Platform Authenticator genereras, sparas, skyddas och används i enhetens krypteringssystem, t.ex. i datorns TPM-chip eller i en säker digital nyckelring, medan en Cross-Platform Authenticator genereras, sparas, skyddas och används i en extern krypteringshårdvara, t.ex. en Yubikey.

2-faktors WebAuthn Credential

En 2-faktors WebAuthn Credential är en 1-faktors WebAuthn Credential med tillägget att den även skyddas med memorized secret och/eller biometri direkt i FIDO2 Authenticator. Detta betyder att det inte går att använda en 2-faktors WebAuthn Credential utan att samtidigt ange memorized secret eller använda biometri för att låsa upp den. Memorized secret kan vara en pinkod på minst 6 siffror eller ett lösenord enligt kraven för aktuell FIDO2 Authenticator. Exempel på var en 2-faktors FIDO2 Authenticator kan registreras och lagras är i iOS Secure Enclave, Android Keystore eller Yubikey.

För att en FIDO2 Authenticator ska kunna vara en 2-faktors WebAuthn Credential måste registrering av memorized secret eller biometri ske i den aktuella FIDO2 Authenticator när den skapas. Vid inloggning efter registrering måste alltid en FIDO2 Authenticator låsas upp med registrerad memorized secret eller registrerad biometri. Detta tillsammans med kraven för 1-faktors WebAuthn Credential uppfyller, beroende på typ av FIDO2 Authenticator, kraven för Multi-Factor Cryptographic Software eller kraven för Multi-Factor Cryptographic Device i NIST 800-63-3B.

Om användaren har verifierat och använder en 2-faktors WebAuthn Credential i enlighet med hur en WebAuthn Credential blir registrerad och verifierad för SWAMID AL3 såsom beskrivet i avsnitt 5.2.5 uppfylls kraven för en multifaktorinloggning på nivån SWAMID AL3.

1-faktors WebAuthn Credential tillsammans med lösenord

Om en användare använder en 1-faktors WebAuthn Credential tillsammans med lösenord kan dessa i kombination användas vid multifaktorinloggning eftersom de är oberoende från varandra, se nedan.

Om en användare verifierat och använder en 1-faktors WebAuthn Credential i enlighet med hur en WebAuthn Credential blir registrerad och dessutom både har ett lösenord i eduID och är verifierad för SWAMID AL3 såsom beskrivet i avsnitt 5.2.5 uppfylls kraven för en multifaktorinloggning på nivån SWAMID AL3.

Svensk e-legitimation och eIDAS

Om en användare har använt en svensk e-legitimation på minst nivå LoA3 för att bli verifierad användare i eduID kan de även använda e-legitimationen som multifaktor i eduID. För svensk e-legitimation används personnummer för att identifiera vem det är som loggar in. Om användaren använder e-legitimation på minst nivån LoA3 vid inloggning är det en multifaktorinloggning på SWAMID AL3-nivå.

På samma sätt kan en användare som använt eIDAS-inloggning som är på nivån Substantial eller High använda denna för multifaktorinloggning. För eIDAS används identifieraren för e-legitimationen för att identifiera vem som loggat in. Om användaren använder eIDAS-inloggning på minst nivå Substantial är det en multifaktorinloggning på SWAMID AL3-nivå.

Logga in med annan enhet

Det är möjligt att använda en eduID-inloggning på annan enhet, t.ex. en mobiltelefon, för att genomföra en eduID-inloggning på den enhet som användare försöker logga in i en tjänst med. En sådan inloggning går till på så sätt att identitetsutfärdaren för eduID presenterar via en QR-kod på första enheten en kryptografisk säker URL som inkluderar en kortlivad delad engångskod med minst 128 bitars entropi. Användaren använder kameran på den andra enheten för att läsa av QR-koden för att öppna upp eduID:s identitetsutfärdare för att fortsätta inloggningen. Användaren använder nu någon av eduID:s inloggningsmetoder, t.ex. en WebAuthn Credential, för att logga in. När inloggningen är klar informeras användarens första inloggningssession via back-channel vilken användare som har loggat in och vilken inloggningsmetod som användes, den delade engångskoden kopplar ihop de bägge sessionerna. Därmed är inloggningen är genomförd och kopplad till rätt inloggningssession.

Inloggningsfaktorers oberoende

När en användare skapar sitt eduID-konto väljer användaren antingen lösenordsbaserad eller lösenordsfri inloggning. Användaren kan när inloggad i eduID:s självservicegränssnitt lägga till en 1-faktors WebAuthn Credential om lösenord användes vid aktivering och vice versa. När bägge finns är det inte möjligt att byta lösenord med hjälp av endast en WebAuthn Credential och inte heller möjligt att lägga till en WebAuthn Credential med enbart hjälp av lösenordet. Det är inte heller möjligt att byta eller ta bort en 2-faktors WebAuthn Credential med enbart lösenord eller en 1-faktors WebAuthn Credential.

5.1.2 eduID använder SWAMIDs WebSSO-teknologiprofiler för autentisering. Detta skyddar mot attacker såsom återspelning (replay) och avlyssning (capture).

5.1.3 Användaren måste vid registrering bekräfta att eduID-kontot, lösenord, koder och säkerhetsnycklar är personliga och endast får användas av användaren själv.

5.1.4 eduID är en tjänst vid Sunet och följer de riktlinjer för IT-säkerhet som finns vid Vetenskapsrådet. För eduID genomförs förutom det reaktiva säkerhetsarbetet regelbundet en riskanalys för att säkerställa att eduID hanterar risker som gäller bl.a. intrång från skadlig kod, insiders, out-of-band attacker, spoofing samt felaktigt eller bedrägligt beteende från användare.

5.2 Credential Issuing

5.2.1 eduID använder domänen eduid.se vid federativ inloggning. Domänen ägs och administreras av Vetenskapsrådet/Sunet.

5.2.2 Alla identitetsutfärdare för eduID använder tjänsteunika identifierare inom domänen eduid.se.

5.2.3 Alla användare i eduID har en unik eduID-identifierare som tillsammans med domännamnet eduid.se är globalt unik. Den unika eduID-identifieraren återanvänds aldrig.

5.2.4 Vid inloggning identifieras användaren antingen med validerad e-postadress, validerat mobilnummer, personnummer eller eduID-identifierare. Det är även möjligt att använda svensk e-legitimation och eIDAS-inloggning och då sker kopplingen implicit.

En specifik e-postadress eller mobilnummer kan endast ha en status av "validerad" på en användare i eduID vid ett givet tillfälle. En användare kan dock ha flera e-postadresser och mobilnummer registrerade till sitt eduID-konto.

5.2.5 Ett eduID-konto kan ha tre olika tillitsnivåer: Obekräftad (SWAMID AL1), bekräftad (SWAMID AL2) och verifierad (SWAMID AL3). Nedan beskrivs de identifieringsmetoder som används i eduID och till vilken tillitsnivå dessa kopplas. En person kan ha flera obekräftade eduID-konton men endast ett som är bekräftat och eventuellt verifierat.

Tabell över identifieringsmetoder i eduID:

Identifieringsmetod	**SWAMID AL1**	**SWAMID AL2**	**SWAMID AL3**
Validerad e-postadress eller validerat mobilnummer	✓		
Validerat mobiltelefonabonnemang		✓	
Digital identifiering via pass eller nationellt identitetskort		✓	
Brev med engångskod till folkbokföringsadress		✓	
Brev med engångskod till digital brevlåda		✓	
Svensk e-legitimation på tillitsnivå 2		✓	
Svensk e-legitimation på minst tillitsnivå 3			✓
eIDAS på nivå Substantial eller High			✓

Validerad e-postadress eller validerat mobilnummer (SWAMID AL1)

När ett eduID-konto skapas görs två kontroller av att den som skapar kontot uppfyller kraven för SWAMID AL1. Först registrerar användaren en e-postadress eller ett mobilnummer, därefter skickas ett e-postmeddelande eller ett sms med en tidsbegränsad engångslänk (giltig i 24 timmar) till den registrerade e-postadressen eller det mobilnumret. När användaren har visat att denne har tillgång till e-postadressen eller mobilnumret genom att använda engångslänken får användaren genomföra en sannolikhetskontroll (turingtest) att det är en människa som skapar kontot genom ett s.k. robotfilter (captcha). E-postadressen eller mobilnumret blir validerat efter att kontoaktiveringen är genomförd.

Sista steget i kontoaktiveringen är att användaren väljer mellan lösenordsfri och lösenordsbaserad inloggning. Om valet faller på lösenordsfri inloggning får användaren skapa en 1-faktors WebAuthn Credential. Om lösenordsbaserad inloggning väljs får användaren ett automatgenererat lösenord visat i webbläsarfönstret, alternativt anger användaren ett eget lösenord. Därefter är eduID-kontot klart att använda som obekräftat eduID-konto.

Efter att det obekräftade kontot är klart initieras automatiskt uppgradering till att bekräfta användaren. Det är möjligt för användaren att avbryta uppgraderingen och stanna som obekräftad användare.

Validerat mobiltelefonabonnemang (SWAMID AL2)

En användare kan bekräfta sig med hjälp av ett SMS till en mobiltelefon om användaren har ett personligt registrerat abonnemang hos en svensk telefonoperatör. Valideringen sker i två steg:

1. Användaren registrerar och validerar att de har kontroll över mobiltelefonnumret genom en tidsbegränsad engångskod (giltig i två timmar) som skickas med SMS. Engångskoden används i eduID:s självservicegränssnitt för att slutföra valideringen av mobiltelefonnumret.
2. Användaren anger sitt personnummer och begär att bekräfta sig med mobiltelefonabonnemanget. eduID hämtar abonnemangsinformation, inkl. personnummer, ur teleregistret och jämför detta sedan med information från folkbokföringsregistret. Vid överensstämmelse blir användaren bekräftad i eduID.

Digital identifiering via pass eller nationellt identitetskort (SWAMID AL2)

Med hjälp av maskinläsbara resehandlingar enligt ICAO Doc 9303, dvs. pass och europeiska nationella identitetskort (European Commission Regulation (EU) 2019/1157) kan en användare digitalt legitimera sig för att bekräfta sitt eduID-konto.

eduID använder externa tjänster för att genomföra den digitala identifieringen. Den externa tjänsten är en mobilapp eller en webbtjänst som kontrollerar den avlästa informationen med en bakomliggande servertjänst för att validera det digitala innehållet i en resehandling. När resehandlingen är inläst kontrolleras först dess autenticitet genom att kryptografiskt validera att handlingen är utfärdad av rätt utfärdare. Därefter kontrolleras att bilden i resehandlingen stämmer överens med den person som finns framför enheten. Detta görs med hjälp av användarens kamera för att säkerställa att rätt person genomför registreringen. Detta kontrollerar både “proof of possession” och “proof of user presence”. Den externa tjänsten använder

standarden ICAO9303 för att uppnå tillräcklig kontroll av "proof of possesssion" samt videobaserad biometrisk kontroll mot innehållet i resehandlingen för "proof of user presence".

Den digitala legitimeringen går till enligt följande:

1. När användaren är inloggad i eduID:s självservicegränssnitt begär användaren att verifiera sig med en resehandling
2. eduID informerar användaren om tillvägagångsättet
3. användaren läser in resehandlingen och bekräftar "proof of possession" och "proof of user presence" i den externa tjänsten samt tar del av vilka uppgifter ur resehandlingen som eduID behöver ta del av och godkänner överföringen
4. eduID tar emot och sparar relevant information ur resehandlingen och information om transaktionen med den externa tjänsten i syfte att underlätta återverifiering och säkerställer möjlighet att vid behov spåra verifieringen
    a. relevant information för de med svenskt personnummer: Personnummer, namn och information om transaktionen med den externa tjänsten
    b. relevant information för de utan svenskt personnummer: Födelsedata, namn och nationalitet samt information om transaktionen med den externa tjänsten.
    c. eduID markerar att användaren har en bekräftad identitet

Brev med engångskod till folkbokföringsadress (SWAMID AL2)

Användaren begär att bekräfta sig via brev till svensk folkbokföringsadress och anger sitt personnummer. Användaren får därefter ett brev med en tidsbegränsad engångskod (giltig i fjorton dagar) skickad till sin folkbokföringsadress. Engångskoden används i eduID:s självservicegränssnitt för att slutföra bekräftandet av användarens identitet.

Brev med engångskod till digital brevlåda (SWAMID AL2)

Användaren begär att bekräfta sig via brev till sin digitala brevlåda och anger sitt personnummer. Brevet skickas ut via Mina meddelanden till den digitala brevlåda som är kopplad till personnumret. Användaren får därefter ett brev med en tidsbegränsad engångskod (giltig i fjorton dagar) skickad till sin digitala brevlåda. Engångskoden används i eduID:s självservicegränssnitt för att slutföra bekräftandet av användarens identitet.

Svensk e-legitimation på tillitsnivå 2 (SWAMID AL2)

Användaren identifierar sig med hjälp av en svensk e-legitimation på tillitsnivå 2 när denne är inloggad i eduID:s självservicegränssnitt. Efter identifieringen blir användaren verifierad med det identitetsbegrepp samt födelsedata och namn som är registrerat i e-legitimationen. eduID använder endast svenska e-legitimationer som tillåter identitetsväxling.

Svensk e-legitimation på minst tillitsnivå 3 LoA3 (SWAMID AL3)

Användaren identifierar sig med hjälp av en svensk e-legitimation på minst nivå LoA3 när denne är inloggad i eduID:s självservicegränssnitt. Efter identifieringen blir användaren verifierad med det personnummer eller annat identitetsbegrepp som är registrerat i e-legitimationen. eduID använder endast svenska e-legitimationer som tillåter identitetsväxling.

eIDAS på nivå Substantial eller High (SWAMID AL3)

Användaren identifierar sig med hjälp av en eIDAS-inloggning (utländsk e-legitimation) på nivån Substantial eller High när denne är inloggad i eduID:s självservicegränssnitt. Efter identifieringen blir användaren verifierad med födelsedata, namn och land samt eIDAS-inloggningens utfärdare och unika identifierare.

Eftersom en långsiktig unik identifierare typ personnummer inte kan används måste användaren efter byte av eIDAS-inloggning knyta den nya eIDAS-inloggningen till sitt eduID-konto. Detta görs genom att användaren gör ett nytt verifieringsflöde men vid detta tillfälle kontrolleras även att födelsedata, namn och land mot redan registrerad information i eduID-kontot överensstämmer.

Verifiera WebAuthn Credential för SWAMID AL3

En användare kan i eduID registrera och använda en WebAuthn Credential som uppfyller de tekniska säkerhetskraven för multifaktorinloggning via SWAMID. Vid registreringen uppfyller WebAuthn Credential kraven för SWAMID AL1 och/eller SWAMID AL2 beroende på om användaren är obekräftad eller bekräftad. En WebAuthn Credential kan sedan höjas till SWAMID AL3 genom att begära verifiering. Vid verifiering av WebAuthn Credential måste användaren både återautentisera med multifaktorinloggning där den aktuella WebAuthn Credential används och göra en inloggning med en med svensk e-legitimation på nivå LoA3 eller LoA4, eller en eIDAS-inloggning på nivå Substantial eller High. Om användaren inte redan är verifierad för SWAMID AL3 sker detta automatiskt i samband med att WebAuthn Credential höjs till SWAMID AL3, se ovan.

Rutin för identitetskontroll

I eduID används inte uppvisande av legitimationshandling för att bli verifierad användare och därför finns ingen definierad process för att kontrollera identitetshandling enligt de krav som definieras i SWAMID AL3. Svensk e-legitimation eller eIDAS-inloggning används för att användaren ska bli verifierad.

Unika förregistrerade identifierare

För SWAMID AL1 används validerad e-postadress och/eller mobilnummer som förregistrerad identifierare.

För SWAMID AL2 och SWAMID AL3 används personnummer för personer med svenskt personnummer.

För SWAMID AL2 och SWAMID AL3 utan svenskt personnummer används en validerad e-postadress, födelsedata, namn och land som en kombinerad unik förregistrerad identifierare. Om eIDAS-inloggning skett sparas även den unika eIDAS-identifieraren för användarens e-legitimation.

5.2.6 Alla ändringar av information relaterat till ett eduID-konto, inklusive ändring av tillitsnivå registreras som logghändelse i en eduID:s databas.

5.2.7 eduID innehåller för obekräftade användare namn, validerade e-postadresser, validerade mobilnummer, i eduID unik identifierare. Alla uppgifter förutom unik identifierare i eduID är självuppgivna och kan ändras av användaren via självservicegränssnittet.

För personer med svenskt personnummer innehåller eduID för bekräftade och verifierade användare namn, personnummer, i eduID unik identifierare, validerade e-postadresser och validerade mobilnummer. E-postadresser och mobiltelefonnummer är självuppgivna och kan ändras av användaren via självservicegränssnittet. Övriga uppgifter uppdateras från folkbokföringsregistret.

För personer utan svenskt personnummer innehåller eduID för bekräftade och verifierade användare namn, födelsedata, land, i eduID unik identifierare, validerade e-postadresser och validerade mobilnummer. E-postadresser och mobiltelefonnummer är självuppgivna och kan ändras av användaren via självservicegränssnittet. Övriga uppgifter uppdateras genom att samma rutin med samma resehandling eller samma eIDAS-inloggning används som när användaren blev bekräftad eller verifierad.

Alla registrerade e-postadresser och mobiltelefonnummer valideras och binds till användaren genom att en tidsbegränsad engångskod (24-timmar) skickas till användaren vid inläggning. Innan registrering är slutförd måste användaren ange den skickade engångskoden i eduID:s självservicegränssnitt för att den ska sparas.

5.2.8 Vid administration och utveckling av tjänsten används tvåfaktorautentisering med minst 2048-bitars GPG- och SSH-nycklar placerade i personlig Yubikey som fysisk faktor.

De personer som arbetar i eduID support använder ett webbgränssnitt för att titta på eduID-konton. Inloggning i detta webbgränssnitt sker med hjälp av inloggning på nivån SWAMID AL3.

5.3 Credential Renewal and Re-issuing

5.3.1 Användarna kan byta både lösenord och WebAuthn Authenticator via eduID:s självservicegränssnitt.

5.3.2 Vid byte av lösenord krävs att det gamla lösenordet anges samtidigt som ett nytt sätts. Användaren kan antingen själv ange ett nytt lösenord eller få ett nytt automatgenererat lösenord. Samma kvalitetskontroll utförs vid byte av lösenord som vid skapande av nytt lösenord.

En användare kan byta en 1-faktors WebAuthn Credential genom att först lägga till en ny och därefter ta bort den gamla. För att genomföra bytet krävs att användaren har loggat in med en 1-faktors WebAuthn Credential eller med en multifaktorinloggning.

En användare kan byta en 2-faktors WebAuthn Credential genom att först lägga till en ny och därefter ta bort den gamla. För att genomföra bytet krävs att användaren har loggat in med multifaktorinloggning.

5.3.3 eduID skiljer på metod för återställning av inloggningsuppgifter baserat på om användaren har enbart en faktortyp eller multipla faktortyper.

Återställning då en faktortyp används

Om en användare utför lösenordsåterställning enbart med validerad e-postadress eller validerat mobilnummer sänks tillitsnivån automatiskt till obekräftad användare. Användaren blir då tvungen att genomföra en ny identitetsverifiering enligt avsnitt 5.2.5 för att bli bekräftad och eventuellt verifierad igen.

Om en bekräftad eller verifierad användare har både en validerad e-postadress och ett validerat mobilnummer kan lösenordsåterställning göras via en kombination av validerad e-postadress och validerat mobilnummer. I detta fall skickas ett SMS med en tidsbegränsad engångskod till mobilnumret och en tidsbegränsad engångslänk till den primära e-postadressen (bägge giltiga i två timmar). Användaren öppnar länken i e-postbrevet och anger pinkoden som kom via SMS för att skapa ett nytt lösenord som uppfyller kraven i 5.1.1. Med denna metod förblir användaren bekräftad efter lösenordsåterställningen.

För en bekräftad eller verifierad användare i eduID kan svensk e-legitimation eller eIDAS-inloggning användas för lösenordsåterställning, förregistrerade identifierare definierade i 5.2.5 används.

Om användaren använder lösenordsfri inloggning istället för lösenordsbaserad återställs 1-faktors WebAuthn Credentials på motsvarande sätt som för lösenord.

Återställning då multipla faktortyper används

Det är inte av säkerhetsskäl möjligt att göra återställning av 1-faktors (plus lösenord) eller 2-faktors WebAuthn Credential som används för multifaktorinloggning. Användaren måste logga in med en annan multifaktor i självservicegränssnittet, dvs. med 1-faktors WebAuthn Credential plus lösenord, 2-faktors WebAuthn Credential, svensk e-legitimation eller eIDAS-inloggning och genomföra ett byte enligt 5.3.2. För svensk e-legitimation och eIDAS-inloggning används förregistrerade identifierare definierade i 5.2.5. Som riskminimering vid eIDAS-inloggning används även ett återställningsbrev till validerad e-postadress eller validerat mobilnummer.

5.4 Credential Revocation

5.4.1 I eduID är det möjligt att stänga av användarkonton men också möjligt ta bort enskilda inloggningsuppgifter från användarkontot. eduID har även funktionalitet för att vid behov kunna manuellt inaktivera eduID-konton och framtvinga återaktivering.

Avstängning och radering av användarkonto

En person kan stänga av sitt eget eduID-konto. Under 7-dagar efter egen avstängning kan användaren återaktivera det igen för att minimera risken för egen felaktig avstängning. Efter de 7 dagarna raderas eduID-kontot inkl. tillhörande personuppgifter. Vissa uppgifter sparas längre i säkerhetsloggarna för att kunna följa upp säkerhetsincidenter.

Användarkonton som inte använts på tre år inaktiveras och raderas.

Den unika eduID-identifieraren läggs i karantänlista efter att användarkontot är raderat, se 5.5.1.

Borttag av inloggningsuppgifter

Om en användare har både lösenord och 1-faktors WebAuthn Credential kan användaren plocka bort lösenordet för att använda lösenordsfri inloggning eller plocka bort alla 1-faktors WebAuthn Credentials för att använda lösenordsbaserad inloggning. 2-faktors WebAuthn Credential kan finnas parallellt för att möjliggöra multifaktorinloggning vid behov.

En användare kan även plocka bort 2-faktors WebAuthn Credentials från sin användare.

5.4.2 eduID skiljer på metod för återaktivering baserat på om användaren har enbart en faktortyp eller multipla faktortyper.

Återaktivering då en faktortyp används

Återaktivering av ett eduID-konto med endast en faktortyp görs via återställning av inloggningsuppgifter enligt 5.3.3 med begränsningen att i eduID registrerade WebAuthn Credentials inte kan användas.

Återaktivering då multipla faktortyper används

Återaktivering vid multipla faktortyper görs med hjälpa av svensk e-legitimation eller eIDAS-inloggning för att säkerställa att det är rätt person genom att jämföra förregistrerade identifierare definierade i 5.2.5. Som riskminimering vid eIDAS-inloggning används även ett återställningsbrev till validerad e-postadress eller validerat mobilnummer.

Obekräftade användare med multifaktorinloggning, dvs. 1-faktors WebAuthn Credential med lösenord eller 2-faktors WebAuthn Credential, kan inte genomföra återställning av inloggningsuppgifter efter avstängning beroende på att för lite information om användaren finns.

Återaktivering beroende på säkerhetsincident

Vid avstängning av eduID-konto beroende på säkerhetsincident informeras användaren via de kontaktuppgifter som finns i eduID innan återaktivering enligt 5.2.5 kan ske. WebAuthn Credential kan normalt sett endast tas bort från kontot av användaren själv av säkerhetsskäl[1]. Enda undantaget till detta är om en WebAuthn Credential är orsaken till säkerhetsincidenten.

5.4.3 eduID har rutiner för att agera vid säkerhetsincidenter inkl. följa upp och förbättra eduID baserat på incidenterna.

5.5 Credential Status Management

5.5.1 All information om eduID-konton och alla ändringar av eduID-konton lagras i en databas och kan tas fram vid behov.

Alla användare har en unik eduID-identifierare och denna återanvänds aldrig utan läggs i karantän om användaren avvecklar sitt eduID-konto.

5.5.2 eduID har målsättningen 99,95% tillgänglighet för tjänsten. Driftsmiljön för eduID är redundant med flera olika driftställen för att minimera effekten av driftavbrott både gällande enskilda komponenter och ett helt driftställe. Det går inte att definiera att eduID har minst samma tillgänglighet som organisationens interna system eftersom eduID är tänkt att användas sektorsbrett, dvs. inom forskning och utbildning i Sverige.

5.6 Credential Validation/Authentication

5.6.1 eduID använder endast profilerna för webbaserad inloggning och följer SWAMID Best Practice för respektive profil.

[1] Att ta bort säkerhetsnyckeln innebär risk för att en person som kapat användarens e-postkonto kan få tillgång till användarens eduID-konto i samband med återaktivering. Säkerhetsnyckeln finns för ett utökat skydd.

5.6.2 När ett konto inaktiveras går det inte längre att använda det. När ett lösenord byts eller en WebAuthn Credential har tagits bort går de inte längre att använda för inloggning.

5.6.3 Användarens lösenord, WebAuthn Credential och ev. registrerade e-legitimation och eIDAS-inloggning används för att verifiera ”proof of possession” av kontot.

5.6.4 Single Sign-On session i eduID är 10 timmar.

Tjänster med extra höga krav på att det är rätt användare som loggar in i tjänsten kan begära åsidosättande av Single Sign-On genom att begära ny inloggning enligt standardmetod i aktuell WebSSO-teknologi (“proof of user presence”).