KONSTFACK
University of Arts, Crafts and Design

Konstfack - SWAMID Identity Management Practice Statement

Datum: 2024-11-27
Version: 2.0

1. Inledning

Konstfack är en konstnärlig högskola och är en registrerad medlem av Swedish Academic Identity (SWAMID) Federation.

Konstfack IDP: Konstfack avser att använda egen identitetsutfärdare tillsammans med högskolekonton för SWAMID AL1 och SWAMID AL2.

EduID connect: Konstfack avser att använda Sunet tjänsten eduID connect som identitetsutfärdare tillsammans med eduID-konton för SWAMID AL1, SWAMID AL2 och SWAMID AL3. Användarens personliga personuppgifter hanteras i eduID. Uppgifter kopplade till organisationen hanteras i eduID Connect. Med avseende på detta hanteras användarens tillitsnivå och personuppgifter i eduID. eduID Connect hanterar uppgifter om användarens koppling till organisationen.

4. Organisational Requirement

4.1 Enterprise and Service Maturity

4.1.1 Konstfack, organisationsnummer 2021001199, 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.

4.1.2 Lärosätets katalog- och behörighetssystem innehåller uppgifter om lärosätets organisation samt personuppgifter om alla som är verksamma vid lärosätet. Med avseende på detta måste särskild hänsyn till behandling av personuppgifter tas enligt aktuell personuppgiftslagstiftning.

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

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

4.1.3

Konstfack IDP: Konstfack använder en extern leverantör för att sälja eller hantera gammal utrustning. I samband med detta så säkerhetsraderas alla hårddiskar (minimum 3 överskrivningar). För media som innehåller känslig information kan Konstfack välja antingen att 7 överskrivningar görs eller 3 överskrivning och fysisk destruktion av hårddisk. Allt som skrotas destrueras i en press med ca 20 tons tryck.

EduID connect: Konstfack använder sig av eduID som IdP och då denna är godkänd på SWAMID AL3 så hanteras destruktion enligt process som beskrivs i eduID:s Identity Management Practice Statement.

4.2 Notices and User Information

4.2.1

Konstfack IDP: Vid användning av Konstfacks IDP gäller Konstfacks användarregler som finns publicerad på Konstfacks webbsida.

EduID connect: EduID connect har inga egna användarregler. Vid användning av eduID connect gäller följande användarregler.

- Konstfacks användarregler som finns publicerad på Konstfacks webbsida.
- Användarregler för EduID som finns publicerade på eduID:s hemsida.

4.2.2

Konstfacks användarregler: Användaren måste ha tillgång till ett högskolekonto för att kunna använda någon av Konstfacks IDP tjänster. För att få tillgång till ett högskolekonto måste användaren först acceptera Konstfacks användarregler. Användaren har tillgång till användarreglerna innan godkännande, antingen som utskriven kopia eller som bifogad fil i ett e-postmeddelande. Vid kontoutdelning på plats, sker godkännandet genom att användaren skriver under ett formulär innan de erhåller sina kontouppgifter. Vid kontoutdelning på distans sker godkännandet när användaren aktiverar sitt högskolekonto.

EduID:s användarregler: Användaren måste acceptera användarreglerna för eduID i samband med att de skapar sitt EduID konto.

4.2.3

Konstfacks användarregler: Vid uppdatering av användarreglerna meddelas samtliga användare via e-post.

EduID:s användarregler: Om och när användarreglerna i eduID uppdateras måste användarna godkänna dem vid nästa inloggning. Det går inte att logga in med eduID innan uppdateringen är godkänd.

4.2.4

Konstfacks användarregler: För högskolekonton bevaras underskrivna godkännanden och godkännande som görs på distans loggas och sparas.

EduID:s användarregler: För EduID konton förs inget register över godkännande då användarna måste godkänna dem om de ska använda kontot och att användarna informeras i det fall reglerna ändras. Användarens acceptans av eduID:s användarvillkoren lagras i eduID.

4.2.5 Konstfack har publicerat sin service definition och privacy policy för Identitetsutgivaren för webbaserad inloggning på Konsfacks webbsida, https://www.konstfack.se/sv/Om-Konstfack/Forvaltning/IT-enheten/.

4.3 Secure Communications

4.3.1

Konstfack IDP: Endast särskilt godkända personer på Konstfack tilldelas administratörsrättigheter. För denna utökade behörighet skapas specifika konton. Dessa konton är personliga. Om en anställd slutar, är tjänstledig eller byter arbetsuppgifter inaktiveras dessa konton. Externa leverantörer tilldelas tillfälliga tidsbegränsade konton som inaktiveras när uppdraget är slutfört.

EduID connect: Endast särskilt godkända personer på Konstfack samt särskilt utsedda personer vid Sunet NOC, har teknisk och administrativ åtkomst till EduID:s identitetstjänster. Säkerhetsskyddsåtgärder runt åtkomst till servrar, och innehållet på dessa, hanteras på samma sätt som Sunets övriga infrastruktur.

4.3.2

Konstfack IDP: Nycklar och lösenord som behöver lagras i klartext i systemet skyddas av operativsystemets behörighetssystem där endast systemadministratörer har tillgång. De lösenord som av någon anledning behöver lagras som klartext på annan plats lagras i en programvara för lösenordshantering med en krypterad databas. Databasen skyddas av filserverns behörighetssystem där databasfilen är lagrad, samt av ett lösenord och en nyckelfil.

EduID connect: Alla krypterings- och signeringsnycklar samt delade lösenord är lagrade under åtkomstkontroll på servrarna för IdP-tjänsterna. I Sunets konfigurationshanterare är dessa krypterings- och signeringsnycklar samt delade lösenord krypterade för att förhindra oavsiktlig åtkomst.

4.3.3

Konstfack IDP: Konstfack använder Microsofts Active Directory för att lagra konton. Identitetslösning för kommunikation med SWAMID är Microsofts Active Directory Federation Services (ADFS). Powershell modulen ADFS toolkit används för att läsa in metadata från SWAMID. ADFS kommunikation sker krypterat mellan ADFS tjänsten och AD. All kommunikation mellan SWAMID, proxy och interna nätverk sker enbart via krypterade anslutningar och unika konton mellan tillåtna punkter, samt allt genomsöks efter hot, förändringar eller påverkan.

EduID connect: All åtkomst till ingående servrar och tjänster sker krypterat enligt gängse protokoll och best practice. Då SSL/TLS används sker detta endast med TLS protokoll som ännu inte har blivit “deprecated” och där nyckellängden uppfyller kraven på att vara säkra enligt NIST SP 800-57.

4.3.4

Konstfack IDP: Konstfack använder kommersiella RSA SSL/TLS certifikat enligt SHA-256 (SHA-2) standard med 2048-bitars kryptering unika för tjänsten med max. giltighetstid 27 månader samt egenutfärdade certifikat enligt SHA-256 (SHA-2) standard med 4096-bitars kryptering unika för tjänsten med max. giltighetstid 10 år.

EduID connect: Teknologispecifika krypterings- och signeringsnycklar för EduID:s IdP-tjänster uppfyller kraven för respektive teknologiprofil, dvs. minst motsvarande 2048 bitar RSA/DSA.

4.4 Security-relevant Event (Audit) Records

4.4.1

Konstfack IDP: Loggning av säkerhetsrelevanta händelser påslaget i Active Directory och ADFS. Loggarna kopieras och sparas i ett separat system där behörig IT-personal kan kontrollera loggarna i efterhand.

EduID Connect: Alla organisationella förändringar på organisationsinformationen kopplade eduIDs användarkonton loggas. EduID loggar i enlighet med SWAMID AL3 alla förändringar på användarkontot i eduID enligt process som beskrivs i eduID:s Identity Management Practice Statement. EduID loggar alla lyckade och misslyckade inloggningsförsök och eduID Connect loggar alla påbörjade och genomförda inloggningsförsök och dessa går att korsreferera vid behov. EduID Connect har ingen kunskap om misslyckade inloggningar.

5. Operational Requirements

5.1 Credential Operating Environment

5.1.1

Konstfack IDP: Konstfacks högskolekonton används för webbaserad inloggning. Nedan följer fullständiga lösenordskrav för Konstfacks högskolekonton.

Konstfacks lösenordskrav
Första gången du loggar in så måste du sätta ett eget lösenord.

Ditt lösenord:

- *måste vara minst tio (10) tecken långt*
- *måste innehålla både stora och små bokstäver samt siffror*
- *får inte innehålla ditt namn*
- *får inte innehålla ÅÄÖääö*
- *får innehålla följande specialtecken: ~!@#$%^&*_-+=` |\(){}[]:;"'<>,.?/*

Undvik lösenord med en personlig koppling som kan vara lätt för andra att gissa. Förvara inte lösenordet skriftligt eller i ett sammanhang där andra kan ta del av det.

Var åttonde månad slutar ditt lösenord att gälla och du kommer uppmanas att byta det. Du får en påminnelse via e-post en månad innan det går ut. Det går inte att återanvända något av dina fem senast använda lösenord.

Det är inte tillåtet att låta någon annan använda dina inloggningsuppgifter. Du får inte heller avslöja eller tillgängliggöra dina inloggningsuppgifter för någon annan. Om detta ändå skulle hända ska du anmäla detta omgående till Helpdesk. Du som ägare av inloggningsuppgifterna är alltid ansvarig för vilken aktivitet som pågår när du är inloggad. Det innebär att det är du som hålls ansvarig för eventuella brott eller andra överträdelser som kan kopplas till inloggningen.

EduID connect: Användarkonton i eduID används för webbaserad inloggning. Samtliga EduID:s metoder är tillgängliga för EduID connect.

5.1.2 Konstfacks Idp-tjänster är konfigurerade enligt aktuella rekommendationer från SWAMID och är därmed skyddade från s.k. ”message replay”.

5.1.3

Konstfack IDP: För Konstfacks högskolekonton gäller att användare uppmanas att inte dela med sig av sina lösenord, samt att inte förvara lösenordet där utomstående kan ta del av det. Detta står beskrivet i Konstfacks användarregler som finns att läsa på Konstfacks webbsida, https://www.konstfack.se/sv/Om-Konstfack/Forvaltning/IT-enheten/

EduID connect: EduID är godkänt för SWAMID AL3 och därmed gäller eduID:s regler kring inloggningsfaktorer.

5.1.4

Konstfack IDP: Tjänsten skyddas av NGFW med antivirus och annan malware skanning, URL och innehållsfiltrering samt IDS och IPS på all kommunikation. Alla servrar har även lokala brandväggar och antivirus. Klienter ägda av Konstfack är utrustade med olika klientskydd beroende på plattform. Alla system uppdateras automatiskt eller enligt löpande rutiner.

EduID connect: EduID:s Idp-tjänster uppdateras och övervakas kontinuerligt i syfte att motverka missbruk av användarkonton vid Konstfack. EduID:s IdP-tjänster är även placerade bakom brandväggar för att minska risken för oavsiktlig åtkomst. Övervakning i eduID beskrivs I eduID:s Identity Management Practice Statement.

5.2 Credential Issuing

5.2.1 Konstfack använder domänen konstfack.se för att koppla unika användare till Konstfack.

5.2.2 Identitetsutgivarna för de olika federativa teknikerna som används av Konstfack använder unika identifierare via antingen URL eller DNS-namn där alla DNS-delar avslutas med konstfack.se eller för eduID Connect unik delegerad namnrymd under connect.eduid.se.

5.2.3

Alla användare har unika användaridentifierare som aldrig återanvänds.

För högskolekonton används kontonamn tillsammans med Konstfacks domännamn som unik användaridentifierare i SWAMID. Det är inte möjligt att skapa flera konton med samma kontonamn, och den namnstandard som används förhindrar att kontonamn återanvänds.

Konstfack IDP: Den unika användaridentifieraren för högskolekontot används.

EduID connect: Ett krav för att få tillgång till EduID connect på Konstfack är att användaren redan har ett högskolekonto, den unika användaridentifieraren för högskolekontot används som eduPersonPrincipalName i EduID connect.

5.2.4

Konstfack IDP: Användare med flera konton till exempel anställda som även studerar på skolan kan välja vilket konto som skall användas genom vilket användarnamn som uppges vid inloggningen.

EduID connect: Alla användare har endast ett användarkonto.

5.2.5

Konstfack IDP:
För Konstfacks egna identitetsutfärdare används högskolekonton för all autentisering.

Kontoutdelning SWAMID AL2

SWAMID AL2 konton skapas i förväg och de har engångslösenord som användaren måste byta första gången de loggar in. För SWAMID AL2 konton förregistreras namn + personnummer/passuppgifter (passnummer och utfärdandeland) för att kunna användas vid identifiering. Följande kontoutdelningsmetoder används för SWAMID AL2 konton.

- *På plats*
  Inloggningsuppgifterna för kontot skrivs ut på papper och placeras i ett kuvert märkt med de förregistrerade uppgifterna för kontot som används vid identifiering. Identitetskontroll utförs i samband med utlämnande av kuvertet. Användaren måste vara på plats och uppvisa godkänd ID-handling. Uppgifterna på ID-handlingen jämförs med uppgifterna på kuvertet.
  För personer med svenskt personnummer följer Konstfack polisens föreskrifter för giltiga ID-handlingar (https://polisen.se/tjanster-tillstand/pass-och-nationellt-id-kort/besok-passexpedition/giltiga-id-handlingar/).
  Utöver detta godtas även internationellt pass enligt PRADO, (https://www.consilium.europa.eu/prado/SV/prado-start-page.html).
- *E-legitimation*
  Inget lösenord skickas till användaren, i stället uppmanas användaren att återställa lösenordet med hjälp av e-legitimation. Vid återställningen görs identitetskontroll med Svensk e-legitimation på tillitsnivå 3 eller högre där personnumret jämförs med det förregistrerade personnumret för kontot. Övriga kontouppgifter skickas separat via e-post. Studenters e-postadress hämtas från antagning.se och för personal hämtas motsvarande från blivande chef.
- *Rekommenderat brev*
  Ett engångslösenord för kontot skickas till användarens folkbokföringsadress med rekommenderat brev och tilläggstjänsten personlig utlämning. Övriga kontouppgifter skickas separat via e-post eller sms. Studenters kontaktinformation hämtas från antagning.se och för personal hämtas motsvarande uppgifter från blivande chef. Efter en förutbestämd tid görs en uppföljning för att se om användaren har aktiverat kontot och bytt lösenord. Om kontots lösenord inte har bytts sätts ett nytt engångslösenord. Denna hantering är inte automatiserad då denna metod används väldigt sällan. För att inte missa att kontrollera att lösenordet har bytts skickas automatiska påminnelser till ansvariga på IT-enheten efter att den förutbestämda tiden har löpt ut.

Kontoutdelning SWAMID AL1

Utdelning av SWAMID AL1 konton sker enbart i undantagsfall när det inte finns möjlighet att utföra en identitetskontroll som uppfyller SWAMID AL2. SWAMID AL1 konton skapas i förväg och de har engångslösenord som användaren måste byta första gången de loggar in. För SWAMID AL1 förregistreras samma uppgifter som för SWAMID AL2 när det är möjligt, annars förregistreras alltid minst namn + födelsedatum för att kunna användas vid identifiering. Utöver kontoutdelningsmetoderna som används för SWAMID AL2 kan följande metoder användas för SWAMID AL1 konton.

- *Videolänk*
  IT-enheten styrker användarens identitet över videolänk (person och giltig ID-handling måste vara synlig samtidigt). IT-enheten förmedlar sedan engångslösenordet till användaren och kontrollerar att användaren byter lösenord. Övriga kontouppgifter skickas separat via e-post. Studenters e-postadress hämtas från antagning.se och för personal hämtas motsvarande från blivande chef.
- *E-postadress*
  Ett engångslösenord för kontot skickas till den e-postadress som studenten har registrerat i antagning.se. Övriga kontouppgifter skickas i ett separat e-postmeddelande till samma e-postadress. I samband med att engångslösenordet byts görs en CAPTCHA kontroll. Efter en förutbestämd tid görs en uppföljning för att se om användaren har aktiverat kontot och bytt lösenord. Om kontots lösenord inte har bytts sätts ett nytt engångslösenord. Denna hantering är inte automatiserad då denna metod används väldigt sällan. För att inte missa att kontrollera att lösenordet har bytts skickas automatiska påminnelser till ansvariga på IT-enheten efter att den förutbestämda tiden har löpt ut.

Byte av tillitsnivå

Ett konto kan ändra tillitsnivå. För att ändra tillitsnivå från SWAMID AL1 till SWAMID AL2 måste alla krav för SWAMID AL2 vara uppfyllda. När man inte uppfyller SWAMID AL2, begränsas kontot till SWAMID AL1.

Höjning av tillitsnivå till SWAMID AL2

För att kunna höja tillitsnivån för ett befintligt konto till SWAMID AL2 måste namn + personnummer/passuppgifter (passnummer och utfärdandeland) finnas förregistrerat för kontot. Följande metoder används för att höja tillitsnivån till SWAMID AL2.

- *På plats*
  IT-enheten höjer tillitsnivån för kontot till AL2 efter identitetskontroll. Användaren måste vara på plats och uppvisa godkänd ID-handling. Uppgifterna på ID-handlingen jämförs med de förregistrerade identifieringsuppgifterna för kontot.

För personer med svenskt personnummer följer Konstfack polisens föreskrifter för giltiga ID-handlingar (https://polisen.se/tjanster-tillstand/pass-och-nationellt-id-kort/besok-passexpedition/giltiga-id-handlingar/).
Utöver detta godtas även internationellt pass enligt PRADO, (https://www.consilium.europa.eu/prado/SV/prado-start-page.html).

- *E-legitimation*
  IT-enheten ändrar kontots lösenord till ett för användaren helt okänt lösenord. Användaren uppmanas att återställa lösenordet online för att få tillgång till kontot. Vid lösenordsåterställningen görs identitetskontroll med Svensk e-legitimation på tillitsnivå 3 eller högre där personnumret jämförs med det förregistrerade personnumret för kontot. IT-enheten verifierar att användaren har återställt lösenordet och att identitetskontrollen vid tillfället gjordes med med Svensk e-legitimation på tillitsnivå 3 eller högre och höjer sedan tillitsnivån för kontot till AL2.

EduID connect:
Konstfack använder eduID för all inloggning i eduID Connect. Verifiering av användare sker enligt aktuella metoder i eduID. EduID ansvarar för att signalera korrekt tillitsprofil till EduID Connect som sedan signalerar samma till tjänsten som användaren loggar in i.

Aktivering av nya personers användarkonton vid Konstfack genomförs av kontoadministratör i inloggningstjänsten genom att kontoadministratören registrerar organisationsuppgifter, gemensam identifierare samt användarens e-postadress vid högskolan. Identifieraren är personnummer för personer med svenskt personnummer. För personer utan svenskt personnummer används födelsedata och namn som kombinerad identifierare för riskbaserad bedömning. Inbjudan skickas därefter ut med e-post. E-postmeddelandet innehåller länk till aktiveringstjänsten samt en tidsbegränsad engångskod.

Genom att gå till länken och använda inbjudningskoden i inbjudan kopplar användaren sin organisationstillhörighet i inbjudan till ett specifikt eduID genom att logga in på ett befintligt eduID. Vid aktiveringen används förregistrerade identifierare för att säkerställa att det är rätt person som genomför aktiveringen. Om personnummer överensstämmer eller namn, födelsedata och e-postadress överensstämmer för personer utan svenskt personnummer genomförs aktiveringen automatiskt, annars genomförs manuell riskbedömning bedömning av organisationens kontoadministratörer. En ytterligare förutsättning för att koppling ska kunna ske är att användarkontot är minst SWAMID AL2 i eduID, vilket automatiskt kontrolleras när kopplingen genomförs. Det sker ingen koppling i eduID till organisationen, utan kopplingen sker genom att användarens eduPersonPrincipalName i eduID kopplas till användarens organisationsinformation i eduID Connect.

Förregistrerad identifierare som används för att unikt identifiera användaren framöver är användarens unika identifierare i eduID samt

- ett svenskt personnummer
- eller födelsedata (ÅÅMMDD) samt förnamn och efternamn från pass eller eIDAS Om förregistrerade identifierare (ett svenskt personnummer, eller födelsedata samt förnamn och efternamn) förändras i eduID måste användaren logga in i EduID:s IdP-tjänst med sitt eduID-konto. Uppgifterna jämförs med användarens unika identifierare i eduID, därefter uppdateras uppgifterna automatiskt.

5.2.6

Konstfack IDP: Ändring av tillitsnivå samt vem som har utfört ändringen loggas och sparas i ett separat system så länge som det behövs för att kunna följas upp, se punkt 4.4.1.

EduID connect: All hantering av tillitsnivå sker i eduID i eduID:s register över nuvarande och historiska tillitsnivåer.

5.2.7

Konstfack IDP: I dagsläget sparas ingen självuppgiven information i identitetssystemet.

EduID connect: All hantering av självuppgivna personuppgifter hanteras i eduID, det finns inga ytterligare självuppgivna personuppgifter i eduID Connect.

5.2.8

Konstfack IDP: Kontohanteringen sköts av ett fåtal administratörer på IT avdelningen. Personliga administratörskonton som uppfyller SWAMID AL2 används för detta. I dagsläget används inte två-faktorautentisering.

EduID connect: Alla system- och kontoadministratörer i EduID:s inloggningstjänst är godkända för SWAMID AL3 som aktivt kontrolleras vid inloggning.

5.3 Credential Renewal and Re-issuing

5.3.1-5.3.3

Konstfack IDP:
Användare kan när som helst själva byta lösenord. Detta görs genom att ändra lösenordet för kontot i Active Directory. Användaren måste uppge sitt nuvarande lösenord för att kunna byta till ett nytt. Det nya lösenordet måste uppfylla kraven för Konstfacks lösenordspolicy.

Lösenordsåterställning SWAMID AL2

Följande metoder används för lösenordsåterställning för SWAMID AL2 konton.

- *På plats*
  Användaren måste vara på plats och uppvisa godkänd ID-handling. Uppgifterna på ID-handlingen jämförs med de förregistrerade uppgifterna för kontot dvs. namn + personnummer/passuppgifter (passnummer och utfärdandeland). IT-enheten återställer sedan lösenordet för kontot och förmedlar det nya engångslösenordet till användaren.
- *E-legitimation*
  Användaren kan själv återställa sitt lösenord online. Vid återställningen görs identitetskontroll med Svensk e-legitimation på tillitsnivå 3 eller högre där personnumret jämförs med det förregistrerade personnumret för kontot.
- *Rekommenderat brev*
  IT-enheten återställer lösenordet för kontot och skickar det nya engångslösenord till användarens folkbokföringsadress med rekommenderat brev och tilläggstjänsten personlig utlämning. Efter en förutbestämd tid görs en uppföljning för att se om användaren har bytt lösenord. Om kontots lösenord inte har bytts sätts ett nytt engångslösenord. Denna hantering är inte automatiserad då denna metod används väldigt sällan. För att inte missa att kontrollera att lösenordet har bytts skickas automatiska påminnelser till ansvariga på IT-enheten efter att den förutbestämda tiden har löpt ut.
- *Återställningsinformation*
  Om användaren har aktiverat lösenordsåterställning för kontot kan användaren själv återställa sitt lösenord online. Aktivering av lösenordsåterställning görs genom att användaren registrerar en e-postadress och ett mobilnummer. Varje kontaktuppgift verifieras med en verifieringskod. Vid lösenordsåterställning verifieras användaren med hjälp av 2 stycken olika tidsbegränsade engångskoder där den ena skickas som e-post och den andra som SMS.

Lösenordsåterställning SWAMID AL1
Utöver återställningsmetoderna där SWAMID AL2 bibehålls/erhålls kan följande metod användas. Konton som är SWAMID AL2 vid lösenordsåterställningen sänks först till SWAMID AL1. Vid en eventuell höjning tillbaka till SWAMID AL2 används rutinerna som beskrivs i avsnittet 5.2.5.

- *Videolänk*
  IT-enheten styrker användarens identitet över videolänk (person och giltig ID-handling måste vara synlig samtidigt). IT-enheten återställer sedan lösenordet för kontot och förmedlar det nya engångslösenordet till användaren och kontrollerar att användaren byter lösenord.

EduID connect:
All hantering av inloggningsuppgifter hanteras i eduID vilket gör att byte och återställning av inloggningsuppgifter återställs enligt eduID:s rutiner.

5.4 Credential Revocation

5.4.1 Högskolekonto och organisationsidentiteten för ett eduID-konto kan stängas av på användarens begäran eller efter ett beslut inom organisationen. Om en person själv önskar att detta skall ske måste denne vända sig till Konstfacks IT-enhet för att få det genomfört.

Konstfack IDP: Att stänga av ett högskolekonto innebär att Active Directory kontot inaktiveras så att det inte längre går att använda. Enbart behörig administratör på IT-enheten kan återaktivera kontot. När en anställning/studiekurs upphör inaktiveras kontot automatiskt. Vid en misstänkt säkerhetsincident inaktiverar IT-enheten det berörda kontot. Utöver det så sätts ett okänt lösenord för kontot och registrerade återställningsmetoder för lösenordet tas bort.

EduID connect: Konstfack kan för sin instans av eduID Connect vid behov stänga av en organisationsidentitet för ett eduID-konto. Antingen genom att tills vidare förhindra att kontot används inom Konstfacks instans (exempelvis vid tillfällig avstängning), eller genom att ta bort användarens eduID-konto från instansen (exempelvis vid anställningens avslut). När en person inte längre är verksam vid Konstfack följs Konstfacks definierade rutiner.

5.4.2 Högskolekonton och organisationsidentiteten för ett eduID-konton som har stängts av kan återaktiveras av behörig administratör på IT-enheten efter beslut från organisationen. Vid en säkerhetsincident förs en dialog med användaren för att belysa

vad som har hänt samt diskutera konsekvenserna för att säkra upp så att det inträffade inte sker igen. Skulle det ske att användaren inte accepterar ev. krav, att det skett avsiktligt eller att det sker igen, så kommer användarkontot fortsätta vara avstängt. Grovt missnyttjande tas upp som disciplinärende.

Konstfack IDP: Återaktiveringen av konton sker genom att Active Directory kontot aktiveras. Om kontot har inaktiverats pga. en säkerhetsincident måste användare för att få tillgång till kontot sätta ett nytt lösenord enligt rutinen för lösenordsåterställning som beskrivs i avsnittet ”5.3.1-5.3.3”.

EduID connect: Vid återaktivering av en avstängd organisationsidentitet aktiverar organisationshandläggaren identiteten igen. Organisationsidentiteten är bunden till samma eduID-konto som tidigare.
Vid en säkerhetsincident stängs kontot av enligt 5.4.1. Efter att användaren informerats om säkerhetsincidenten får användaren tillbaka kontot genom att handläggaren aktiverar organisationsidentiteten enligt ovan.

5.4.3 Om ett användarkonto stängts av beroende på en säkerhetsincident genomförs en analys om hur incidenten uppkom och hur Konstfack kan minska risken för att motsvarande incident återuppträder.

5.5 Credential Status Management

5.5.1

Konstfack IDP: Alla aktiva identiteter samt inaktiverade identiteter för anställda går att söka i identitetssystemet (AD). Inaktiverade identiteter för studenter går att söka i ett separat register. Förändringar av aktiva identiteter loggas. Loggarna kopieras och sparas i ett separat system.

EduID connect: I eduID connect finns alla aktuella och nyligen avstängda användaridentifierare. Unika identifierare för raderade konton sparas i ett särskilt register för att säkerställa att dessa inte återanvänds.

5.5.2 Konstfack har samma tillgänglighetskrav på IdP-tjänsterna som för övriga interna system som är beroende av dessa IdP-tjänster.

5.6 Credential Validation/Authentication

5.6.1 Konstfacks identitetstjänster följer SWAMIDs regler och best practice för konfiguration av sina IdP-tjänster.

5.6.2

Konstfack IDP: Identitetstjänsten autentiserar inte avstängda/inaktiverade konton.

EduID connect: Det går endast att logga in i EduID connect med aktiva användarkonton i eduID som har en organisationskoppling till Konstfack i eduID Connect.

5.6.3

Konstfack IDP: Identitetstjänsten kräver att användaren anger sina inloggningsuppgifter vid autentisering om det inte finns en giltig SSO biljett.

EduID connect: För att logga in måste användaren logga in via eduID enligt det regelverk som finns där.

5.6.4

Konstfack IDP: Identitetstjänstens SSO biljetter är endast giltiga i 8 timmar. Efter det måste användaren autentisera på nytt.

EduID connect: EduID Connect har inte eget stöd WebSSO utan varje inloggning valideras mot eduID och följer eduID:s regelverk för WebSSO.