KONSTFACK
University of Arts, Crafts and Design

Konstfack - SWAMID Identity Management Practice Statement – revision 2022-11-15

1. Inledning

Konstfack är en konstnärlig högskola och är en registrerad medlem av Swedish Academic Identity (SWAMID) Federation. Konstfack avser att använda sig av SWAMID AL2 samt SWAMID AL1.

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

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 (Active Directory) 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 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.

4.2 Notices and User Information

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

4.2.1
Användarregler finns att läsa på Konstfacks webbsida [https://www.konstfack.se/PageFiles/1518/Konstfacks_regler_f%c3%b6r_anv%c3%a4ndning_av_inloggningsuppgifter_och_n%c3%a4tverk.pdf] samt i IT-handboken på Konstfacks intranät.

4.2.2
Alla användare behöver godkänna att de lovar att ta del av och följa IT-handboken innan de får tillgång till ett användarkonto på skolan. Alla användare har tillgång till IT-handboken innan godkännande, antingen som utskriven kopia på plats eller som bifogat dokument i mail. I de fall då kontoutdelningen sker på plats sker godkännande genom att skriva under en blankett. I de fall då kontoutdelningen sker på distans sker godkännandet i samband med att användaren aktiverar sitt konto.

4.2.3
Uppdateringar av användarregler skickas ut via e-post.

4.2.4
Underskrivna blanketter sparas och godkännande på distans loggas och sparas.

4.2.5
Som tjänstedefinition använder Konstfack SWAMID:s best practice policy. Denna finns publicerad på Konstfacks externa webb [https://www.konstfack.se/PageFiles/1518/SWAMID_Service_Definition_SV.pdf] samt på Konstfacks intranät. På dessa ställen ligger även SWAMID Privacy Policy [https://www.konstfack.se/PageFiles/1518/SWAMID_Privacy_Policy_SV.pdf]

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
Administratörsrättigheter tilldelas enbart ett fåtal personer på IT-enheten med behov av detta. 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.

4.3.2
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.

4.3.3
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.

4.3.4
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.

4.4 Security-relevant Event (Audit) Records

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

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

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
Se Konstfacks fullständiga lösenordskrav i bilaga A.

5.1.2
Konstfack använder de protokoll SWAMID stödjer enligt tekniska profiler för SAML WebSSO samt EduRoam och är skyddade från s.k. ”message replay”. Endast tillåtna protokoll godkänns i våra brandväggar.

5.1.3
Konstfacks användare uppmanas att inte dela med sig av sina lösenord, samt att inte förvara lösenordet där utomstående kan ta del av det.

5.1.4
Konstfacks NGFW har antivirus och annan malware skanning, URL och innehållsfiltrering samt IDS och IPS på all kommunikation och uppdateras var 15’e minut automatiskt med de senaste upptäckta hoten globalt. 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.

5.2 Credential Issuing

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

5.2.1-5.2.2
Konstfacks identitetshanterare har en unik identifikation bekräftad med certifikat, verifierade via DNS och knuten till vår unika identifierare för organisationen, konstfack.se.

5.2.3
Alla användarnamn är unika och återanvänds inte. Konstfack använder MS Active Directory som identitetstjänst och attributet sAMAccountName används som användarnamn tillsammans med Konstfacks domännamn. Det är inte möjligt att

skapa flera konton med samma sAMAccountName, och den namnstandard som används förhindrar att användarnamnet återanvänds.

5.2.4
Användare med flera konton t.ex. anställda som även studerar på skolan kan välja vilket konto som skall användas genom vilket användarnamn som uppges vid inloggningen.

5.2.5

Rutin för utdelande av kontouppgifter för 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.

Kontoutdelning med identitetskontroll på plats (ID-handling)
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/giltiga-id-handlingar/). Utöver detta godtas även internationellt pass enligt PRADO (https://www.consilium.europa.eu/prado/SV/prado-start-page.html).

Kontoutdelning med identitetskontroll via rekommenderat brev
Ett engångslösenord för kontot skickas till användaren med rekommenderat brev med 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 med identitetskontroll online (Bank-ID)
Inget lösenord skickas till användaren, i stället uppmanas användaren att återställa lösenordet online. Vid återställningen görs identitetskontroll med Bank-ID 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.

Rutin för utdelande av kontouppgifter för 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.

Kontoutdelning med identitetskontroll över videolänk (ID-handling)
IT-enheten styrker användarens identitet över videolänk (person och giltig ID-handling måste vara synlig samtidigt). IT-enheten förmedlar sedan engångslösenordet till användaren. Övriga kontouppgifter skickas separat via e-post. Studenters e-postadress hämtas från antagning.se och för personal hämtas motsvarande från blivande chef.

Kontoutdelning med identitetskontroll via 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.

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.

Rutin för att höja tillitsnivån 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.

Höjning av tillitsnivå med identitetskontroll på plats (ID-handling)
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/giltiga-id-handlingar/). Utöver detta godtas även internationellt pass enligt PRADO (https://www.consilium.europa.eu/prado/SV/prado-start-page.html).

Höjning av tillitsnivå med identitetskontroll online (Bank-ID)
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 Bank-ID där personnumret jämförs med det förregistrerade personnumret för kontot. IT-enheten verifierar att användaren har återställt lösenordet och att identitetskontrollen vid tillfället gjordes med Bank-ID och höjer sedan tillitsnivån för kontot till AL2.

5.2.6
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.

5.2.7
I dagsläget sparas ingen självuppgiven information i identitetssystemet.

5.2.8
Kontohanteringen sköts av ett fåtal administratörer på IT avdelningen. Personliga administratörskonton som uppfyller SWAMID AL2 används för detta. I dagsläget används inte två-faktorautentisering.

5.3 Credential Renewal and Re-issuing

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

5.3.1
Användare kan när som helst själva byta lösenord. Detta görs genom att ändra lösenordet för kontot i Active Directory.

5.3.2
Användaren måste uppge sitt nuvarande lösenord för att kunna byta till ett nytt. Det nya lösenordet måste uppfylla kraven för Konstfacks lösenordspolicy.

5.3.3

Rutin för lösenordsåterställning för SWAMID AL2
Följande metoder används för lösenordsåterställning för SWAMID AL2 konton.

Lösenordsåterställning med identitetskontroll online (Bank-ID)
Användaren kan själv återställa sitt lösenord online. Vid återställningen görs identitetskontroll med Bank-ID där personnumret jämförs med det förregistrerade personnumret för kontot.

Lösenordsåterställning med identitetskontroll på plats (ID-handling)
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.

Lösenordsåterställning med identitetskontroll via rekommenderat brev
IT-enheten återställer lösenordet för kontot och skickar det nya engångslösenord till användaren med rekommenderat brev med 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.

Lösenordsåterställning med identitetskontroll via 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.

Rutin för lösenordsåterställning för SWAMID AL1
Utöver återställningsmetoderna som används för SWAMID AL2 kan följande metod användas för SWAMID AL1 konton.

Lösenordsåterställning med identitetskontroll över videolänk (ID-handling)
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.

5.4 Credential Revocation

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

5.4.1
Konton kan spärras på användarens begäran eller efter ett beslut inom organisationen.

Att ett konto spärras innebär att Active Directory kontot inaktiveras så att det inte längre går att använda. Enbart behörig administratör på IT-enheten kan ta bort spärren.

När en anställning/studiekurs upphör spärras kontot automatiskt.

Vid en misstänkt säkerhetsincident spärrar IT-enheten det berörda kontot. Utöver det så sätts ett okänt lösenord för kontot och registrerade återställningsmetoder för lösenordet tas bort.

5.4.2
Spärrade konton återaktiveras av behörig administratör på IT-enheten efter beslut från organisationen. Spärren tas bort genom att Active Directory kontot aktiveras.

Om kontot har spärrats pga. en säkerhetsincident måste användare för att få tillgång till kontot sätta ett nytt lösenord enligt rutinen för lösenordsåterställning (se 5.3.3).

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 spärrat. Grovt missnyttjande tas upp som disciplinärende.

5.4.3
Om en säkerhetsincident beror på brister i befintliga rutiner eller i befintlig teknik planeras åtgärder för att förhindra att det inträffade upprepas.

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
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.

5.5.2
Konstfacks identitetstjänster inklusive SWAMID är resilienta och har en tillgänglighet på över 95% vilket bedöms vara tillräckligt för att uppfylla högskolans krav.

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
Konstfacks identitetstjänst är konfigurerad enligt de protokoll och valideringsautentiseringskrav SWAMID rekommenderar.

5.6.2
Identitetstjänsten autentiserar inte inaktiverade/spärrade konton.

5.6.3
Identitetstjänsten kräver att användaren anger sina inloggningsuppgifter vid autentisering om det inte finns en giltig SSO biljett.

5.6.4
Identitetstjänsten SSO biljett är endast giltiga i 8 timmar. Efter det måste användaren autentisera på nytt.