KKH SWAMID Identity Management Practice Statement

Innehållsförteckning

Versionshistorik

Version	Datum	Författare	Beskrivning
1.0	2023-05-29	Fredrik Reuterswärd	Första version godkänd för AL2
1.1	2024-08-20	Hedvig Engelmark	Helt digital kontoutrullning med EduID

1. Inledning

Kungliga Konsthögskolan (KKH) är en konstnärlig högskola och är en registrerad medlem av Swedish Academic Identity (SWAMID) där vi använder tjänster som SAML WebSSO och Eduroam. Syftet med detta dokument är att beskriva hur vi uppfyller tillitsprofilerna AL1 samt AL2.

4. Organisational Requirement

4.1 Enterprise and Service Maturity

This subsection defines the organization and the procedures that govern the operations of the identity provider.

Kungliga Konsthögskolan (KKH), organisationsnummer 202100-2957, är en statlig utbildningsmyndighet vilket gör att lärosätets verksamhet regleras i lagar, förordningar och regleringsbrev. De viktigaste lagarna och förordningarna som styr 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 identitets- och behörighetssystem Microsoft 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.

Som statlig myndighet arbetar lärosätet även med ledningssystem för informationssäkerhet enligt Myndigheten för Samhällsskydd och Beredskaps föreskrifter om statliga myndigheters informations-säkerhet.

Lagringsmedia av traditionell eller hybridtyp samlas ihop från KKH:s olika enheter och transporteras till ett centralt förråd. Förrådet är beläget på ett låst våningsplan, är larmat och kräver höjd behörighet för inträde.

Lagringsmedierna placeras i ett låst skåp under uppsamlingstiden, därefter destrueras de genom ”degaussing” samt mekanisk påverkan av den fysiska disken.

Studenternas privata e-postadress hämtas från KKH:s ansökningsportal där studenterna skickat in sina arbetsprover när de söker till våra utbildningar.

4.2 Notices and User Information

4.2.1-4.2.2 Alla anställda och studenter hos KKH signerar en ansvarsförbindelse (Ansvarsförbindelsen för användning av KKH:s dator-, nät- och Systemresurser) innan konton lämnas ut, och tillgång till nätverk ges.

Varje medarbetare måste ha en IT-introduktion där reglerna gås igenom, legitimation kontrolleras och ansvarsförbindelsen signeras.

I samband med att studenter hämtar ut sitt konto kontrolleras legitimation och ansvarsförbindelsen signeras.

Den signerade ansvarsförbindelsen intygar att personen har läst och förbinder sig att följa KKH:s allmänna regler för användning av IT-resurser vid Kungliga Konsthögskolan (Ansvarsförbindelse för användning av KKH:s dator-, nät- och Systemresurser) de allmänna reglerna innehåller även KKH:s tjänstedefinition för IT-resurser.

Ansvarsförbindelsen finns publicerad i uppdaterad form på KKH:s intranät och vid kontoaktivering.

4.2.3 Vid förändringar av olika policys kommuniceras detta ut på KKH:s intranät samt via e-post.

4.2.4 Förändringar i policys dokumenteras, vid inloggning i idp:n accepteras policyn.

4.2.5 ”Service Definition” finns dokumenterad i olika dokument samt policys på KKH:s intranät samt externa websidor.

Länk till svenska sidan: https://kkh.se/sv/swamid-service-definition/

Länk till engelska sidan: https://kkh.se/en/swamid-service-definition/

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 Okrypterad information (exempelvis interna SAML-certifikat i IdP:n) har rättigheter som gör att inte obehöriga kan läsa den, gäller även SSL-certifikat för IdP:n, detta gäller också andra system samverkar med AD:t.

Utåt är kommunikationen krypterad med https (TLS 4) samt certifikat.
Mellan identitetsutgivaren och Ms AD är den inbyggda krypteringen påslagen.

4.3.3
Kungl. Konsthögskolan använder Microsofts Active Directory för att lagra konton. Identitetslösning för kommunikation med SWAMID är Shibboleth. All kommunikation mellan Shibboleth och AD sker krypterat. All kommunikation mellan SWAMID, Shibboleth och interna nätverk sker enbart via krypterade anslutningar och unika konton mellan tillåtna punkter.

4.3.4 Kungl. Konsthögskolan använder kommersiella RSA SSL/TLS certifikat enligt SHA-256 (SHA-2) standard med 2048-bitars kryptering unika för tjänsten med max. giltighetstid 13 månader samt egenutfärdade certifikat enligt SHA-256 (SHA-2) standard med 4096-bitars kryptering unika för tjänsten med max. giltighetstid 10 år. IdP:ns interna SAML-certifikat är egenutfärdat och med minst 2048 bitars RSA-nyckel.

4.4 Security-relevant Event (Audit) Records

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

KKH använder sig av de inbyggda ”auditing” funktionerna i AD, dvs UAL (User Access Logging). All in/utloggning i servrar/nätverk loggas. Administratörerna använder sig av konton med eleverad men begränsad behörighet. Dvs grundregeln är att Administratörerna bara ska använda konton med eleverad behörighet när det är absolut nödvändigt. Lösenordsbyte på användarkonton loggas, loggarna sparas i ett år.

Utöver det används synkroniserade tidsservar där loggarna ingår i KKH:s backuplösning, säkerhetspatchning av samtliga servrar sker en gång per månad.

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 KKH tillämpar följande lösenordsregler:

Lösenorden måste enligt lösenordspolicyn vara minst 8 tecken långa samt innehålla minst en versal bokstav, minst en gemen bokstav samt minst en siffra eller specialtecken. Se Kungl. Konsthögskolans fullständiga lösenordskrav: *https://kkh.se/IT/Password_Policy_KKH_sv.pdf*

5.1.2
Kungl. Konsthögskolan 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
Kungl. Konsthögskolans lösenordspolicy uppmanar sina användare att inte dela med sig av sina lösenord, samt att inte förvara lösenordet där utomstående kan ta del av det.

5.1.4
Kungl. Konsthögskolans NGFW har antivirus och annan malware skanning, URL och innehållsfiltrering samt 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 Kungl. Konsthögskolan 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 including issuing of credentials and binding of other information to the Subject. Furthermore, the Identity Provider and its Subjects must be uniquely identified.

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

KKH använder kkh.se som scope i eduroam och SAML.

KKH:s IdP har ett entityID. För eduroam används radius-serverns dns-namn.

5.2.3
Alla användarnamn är unika och återanvänds inte. Kungl. Konsthögskolan använder MS Active Directory som identitetstjänst och attributet sAMAccountName används som användarnamn tillsammans med Kungl. Konsthögskolans domännamn.
Det är inte möjligt att skapa flera konton med samma sAMAccountName, och den namnstandard som används förhindrar att användarnamnet återanvänds

5.2.4
Vid inloggning så anger användare sitt användarnamn. Om de har fler kan de välja vilket användarnamn de loggar in med.

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
Vid legitimationskontroll godkänns samma identitetshandlingar som polisen godkänner för utfärdande av svenskt pass, samt utländska pass som uppfyller ICAO Doc 9303 och nationella ID-kort inom EU/EES som uppfyller EU-förordning 562/2006.

Anställda

Anställda kan hämta ut sitt konto eller höja sitt konto från AL1 till AL2 med följande metoder:

- Personligt besök hos IT-avdelningen med legitimationskontroll. Personnummer eller namn och födelsedata sparas som fördefinierade identifierare och jämförs med uppgifter i lönesystemet/kontosystemet. Ett engångslösenord erhålles som måste bytas vid första inloggning. Kontona blir AL2.

- Anställda **med** svenskt personnummer kan göra en inloggning mot kontoaktiveringsportalen via svensk e-legitimation på tillitsnivå 3 eller högre. Personnummer sparas som fördefinierade identifierare och jämförs med uppgifter i lönesystemet/kontosystemet. Kontona blir AL2.

Studenter

Studenter kan hämta ut sitt konto eller höja sitt konto från AL1 till AL2 med följande metoder:

- Personligt besök i på IT-enheten med legitimationskontroll. Personnummer eller namn och födelsedata sparas som fördefinierade identifierare och jämförs med uppgifter i Ladok/kontosystemet. Ett engångslösenord erhålles som måste bytas vid första inloggning. Kontona blir AL2.

- Studenter **med** svenskt personnummer kan göra en inloggning mot kontoaktiveringsportalen via svensk e-legitimation på tillitsnivå 3 eller högre. Personnummer sparas som fördefinierade identifierare och jämförs med uppgifter i Ladok/kontosystemet. Kontona blir AL2.

- Studenter **med** svenskt personnummer kan göra en inloggning mot kontoaktiveringsportalen via eduID. Kontroll görs att IdP och inloggning uppfyller AL2. Personnummer från eduID sparas som fördefinierade identifierare och jämförs med uppgifter i Ladok//kontosystemet. Kontona blir AL2.

- Studenter **utan** svenskt personnummer kan göra en inloggning mot kontoaktiveringsportalen via eduID. Kontroll görs att IdP och inloggning uppfyller AL2. En automatiserad, riskbaserad bedömning görs att namn och födelsedata från eduID tillräckligt väl matchar uppgifter i Ladok/kontosystemet. Dessa sparas också som fördefinierade identifierare. Kontroll sker även att e-postadress från eduID matchar e-postadress i Ladok/kontosystemet. Eppn/subject-id från eduID sparas för senare lösenordsåterställning utan riskbaserad bedömning. Kontona blir AL2.

5.2.6 All förändring av AL-nivå loggas.

5.2.7 Användare kan via ärendehantering eller besök på IT-enheten begära att självuppgivna uppgifter ändras.

5.2.8 All IT-personal som hanterar konton och engångskoder är inloggade med ett AL2-konto.

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 Alla anställda/studenter har möjligheten att själv byta sitt lösenord via lösenordsportal eller genom att ändra lösenordet för kontot i Active Directory.

5.3.2 Vid lösenordsbyte behöver nuvarande lösenord anges.

5.3.3 Metoderna under 5.2.5 kan användas för lösenordsåterställning.

De förregistrerade identifierarna som beskrivs under 5.2.5 används för att säkerställa att det handlar om samma person

Anställda som glömt sitt lösenord och inte kan identifiera sig via någon av metoderna i 5.2.5 kan få ett nytt lösenord via SMS till sin jobbmobil eller genom att visa ID-handling via videolänk. Via videolänk krävs det att person och giltig ID-handling måste vara synliga i bild samtidigt. Lösenordet måste bytas vid första inloggning. Kontona får AL1.

5.4 Credential Revocation

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

5.4.1 IT-enheten kan avaktivera konton på användares, chefs, prefekts eller IT-personals begäran. Studentkonton inaktiveras också efter viss definierad studieinaktivitet.

5.4.2 Återaktivering av konton sker enligt samma rutiner som under 5.3.3.

Vid avaktivering av konto på grund av misstänkt säkerhetsrelaterad incident kontaktas användaren innan återaktivering får göras.

5.4.3 Alla säkerhetsincidenter rapporteras till lärosätets säkerhetsfunktion som aktivt arbetar för att minimera risken att de återuppstår.

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 Vid skapande av ett konto finns det alltid ett underlag i form av en beställning, underlagen sparas.

Av underlagen går det på ett enkelt sätt se vilka användarnamn, kortnamn mm. en person har haft under sin aktiva tid hos KKH. En black-list med gamla kontouppgifter finns.

5.5.2 Gällande tillgängligheten har KKH övervakning på hela IT-miljön samt tillhörande infrastruktur under kontorstid, stora delar av miljön samt infrastrukturen är redundant. Detta gäller även KKH:s idp.

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 KKH följer SWAMIDS rekommendationer kring konfigurering av vår Identity Provider.

5.6.2 Bara aktiva konton tillåts inloggning. Användare behöver använda sitt lösenord vid inloggning.

5.6.3 För åtkomst via KKH:s idp till SSO-tjänster behöver användaren logga in med sina användaruppgifter för att få en aktiv session.

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