SKH SWAMID Identity Management Practice Statement

Versionshistorik

Version	Datum	Författare	Beskrivning
1.0	2021-11-29	Zacharias Böhm	Första version godkänd för AL2
1.1	2024-05-16	Bat-Erdene Ganbat	Kontobekräftelse via eduID

1. Inledning

Stockholms konstnärliga högskola (SKH) utbildar och forskar inom cirkus, dans, film, media, opera och scenkonst. Vi vill med vår unika sammansättning av utbildningar och konstnärlig forskning ge nya möjligheter för framtidens kunskaps- och samhällsutveckling.

SKH är i dag medlem av 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.

Stockholms Konstnärliga Högskolor (SKH), organisationsnummer 202100-6560, 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 SKH:s olika enheter och transporteras till ett centralt förråd. Förrådet är beläget på ett låst våningsplan 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.

4.2 Notices and User Information

4.2.1-4.2.2 Alla anställda och studenter hos SKH skriver under en ansvarsförbindelse [Ansvarsförbindelse för användning av IT 2015-01-08.pdf, bifogad] innan konton lämnas ut och tillgång till nätverk ges.

Varje medarbetare måste ha en IT-introduktion där reglerna gås igenom, legitimation kontrolleras samt ansvarsförbindelsen skrivs under.

I samband med att studenter hämtar ut sitt konto godkänner de Allmänna regler för IT-användning inom Stockholms konstnärliga högskola.

Den underskriva ansvarsförbindelsen ger att personen har läst och förbinder sig att följa SKH:s allmänna regler för användning av IT-resurser vid Stockholms konstnärliga högskola [Allmänna regler för IT-användning inom Stockholms konstnärliga högskola 2015-01-09.pdf, bifogad], de allmänna reglerna innehåller även SKH:s tjänstedefinition för IT-resurser.

4.2.3 Vid förändringar av olika policys kommuniceras detta ut på SKH:s intranät samt via e-post. Länk till IT-policyn finns även på idp:s inloggningssida.

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 SKH:s intranät samt externa websidor.

Länk till svenska sidan: https://www.uniarts.se/om-skh/service-definition/

Länk till engelska sidan: https://www.uniarts.se/english/about-skh/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 Inloggning till administrativa system är till administratörer som använder sina administrativa konton.

4.3.2 Okrypterad information (exvis 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 som har med AD:t att göra

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

4.3.3 Alla nycklar för SSL/TLS är minst 2048 bitar. Replikeringen mellan domänkontrollanter sker enligt Microsofts standardiserade säkerhetsmetod för replikering, i denna ingår Azure AD password synchronization.

4.3.4 Krypterings och signeringsnycklar för SAML är minst 2048 bitar RSA.

4.4 Security-relevant Event (Audit) Records

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

SKH 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.

I övrigt så används synkroniserade tidsservar och loggarna ingår i SKH: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 SKH tillämpar följande lösenordsregler:

När det gäller ”credentials” är lösenordskomplexiteten är Microsoft Active directorys inbyggda. Minst 8 tecken, stora bokstäver, små bokstäver och specialtecken eller siffra.

5.1.2 Protokoll som förhidrar ”message replay” används.

5.1.3 Användare uppmanas i användarpolicyn om att inte dela sina lösenord med andra.

5.1.4 SKH har brandväggar ut mot internet, klientdatorerna uppdateras regelbundet, detta gäller även virusskyddet. Serverparken uppdateras en gång per månad under ett servicefönster.

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 SKH äger uniarts.se.

SKH använder uniarts.se som scope i eduroam och SAML.

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

5.2.3 Varje användare har ett unikt användarnamn.

Användarnamn återanvänds aldrig. Gamla konton ligger i en black-list som kontrolleras vid skapande av nya användare.

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

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 i servicedesk/IT-intro 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 servicedesk 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 i servicedesk 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.

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. 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 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 SKH. En black-list med gamla kontouppgifter finns.

5.5.2 Gällande tillgängligheten har SKH övervakning på hela IT-miljön samt tillhörande infrastruktur under kontorstid, stora delar av miljön samt infrastrukturen är redundant. Detta gäller även SKH: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 SKH 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 SKH:s idp till SSO-tjänster behöver användaren logga in med sina användaruppgifter för att få en aktiv session.

5.6.4 Sessionstiden i ADFS är 8 timmar.