PM Konfidentiell

Diarienummer 21/618
2025-04-04

IT-avdelningen
Elisabeth Smedberg
IT-chef

Riktlinjer för hantering av elektroniska identiteter på KMH

Sammanfattning

Detta dokument beskriver rutiner för att hantera elektroniska identiteter på KMH och utgör grunden för KMH:s medlemskap i SWAMID Identity Assurance Level 1 Profile, respektive SWAMID Identity Assurance Level 2.

1. Inledning

Kungl. Musikhögskolan är som svensk högskola medlem av den nationella identitetsfederationen SWAMID. Högskolan har en identitets- och behörighetslösning som innehåller konton för anställda (ca 450 konton), aktiva studenter (ca 1 000 konton) samt övriga verksamma (ca 300 konton).

Högskolan uppfyller tillitsnivåerna SWAMID Assurance Level 1 resp SWAMID Assurance Level 2. Högskolan presenterar identiteter både enligt SWAMID Assurance Level 1 Profile och SWAMID Assurance Level 2 Profile samt beroende på hur säker identifiering har skett av individen.

4. Organizational requirements

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.

4.1.1-4.1.2

KMH, organisationsnummer 202100-1215, är en statlig myndighet vilket gör att lärosätet regleras i lagar, förordningar och regleringsbrev. De viktigaste lagarna och förordningarna som styr universitets/högskolans arbete är regeringsformen (SFS 1974:152), tryckfrihetsförordning (SFS 1949:105),

myndighetsförordningen (SFS 2007:515), högskolelagen (SFS 1992:1434) och högskoleförordningen (SFS 1993:100).

Regleringsbrevet utställs årligen av regeringen och styr högskolans uppdrag under ett kalenderår. I övrigt följer lärosätet Sveriges övriga lagar och förordningar.

Lärosätets IT-tjänst vilken identifierar roller och rättigheter i KMH:s IT-miljö innehåller uppgifter om lärosätets organisation samt personuppgifter om alla som är verksamma vid lärosätet (studenter, personal) och som får behörighet till KMH:s IT-tjänster. Med avseende på detta måste hänsyn tas till, Dataskyddsförordningen (EU) No. 679/2016 och offentlighets- och sekretesslagen (SFS 2009:400) reglerar behandlingen av personuppgifter samt hantering av personer med behov av skyddade personuppgifter och tillämpas av lärosätet tillsammans med övrig relevant personuppgiftslagstiftning.

Studenters personuppgifter hämtas ur lärosätets studiedokumentationssystem och därför gäller förordning (SFS 1993:1153) om redovisning av studier m.m. vid universitet och högskolor för hanteringen av studenters personuppgifter även för IT-tjänsten som identifiering av roller och rättigheter.

Som statlig myndighet arbetar lärosätet även med informationssäkerhet enligt Myndigheten för samhällsskydd och beredskaps (MSB:s) föreskrifter om statliga myndigheters informationssäkerhet, skyddsåtgärder för IT-system samt incidenthantering (MSBFS 2020:06, 2020:07, 2020:08).

4.1.3

Som en del i informationssäkerhetsarbetet finns det framtagna rutiner för hur utrustning som innehållit elektronisk information avvecklas. Tillämpandet av dessa rutiner innebär att hårddiskar som använts för servrar vid lärosätet raderas på ett sätt så att informationen ska vara svår att återskapa och att elektronikskrot lämnas in för destruering på ett säkert sätt.

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 General Data Protection Regulation (EU) No 679/2016.

4.2.1-4.2.2

KMH har instruktioner, för nyttjande av användarkonto vid KMH, i den s k ansvarsförbindelsen, som respektive användare genom aktiv handling måste intyga att den godkänner innan användarkontot aktiveras. Dessa finns även

tillgängliga på KMH:s webbplats. I ansvarsförbindelsen ingår även information om SUNET:s policy för användning av nätet.

4.2.3
Vid förändringar så upplyses alla med aktiva konton via mail.

4.2.4
Det initiala godkännandet sparas i en databas.

4.2.5
Via inloggningssidor för användare på autentiseringstjänsterna finns även länkar till både aktuella användarvillkor och riktlinjer för hantering av personuppgifter samt Service Definition för KMH:s Idp (se bilaga 2). Användarvillkor och riktlinjer för hantering av personuppgifter finns även länkade till i metadatan för IdP:n. Tydliga markeringar sker här i samband med revisioner av dessa dokument så att användarna uppmärksammas på detta. Även kontaktuppgifter till dataskyddsombud samt IT-säkerhetsansvarig finns här, dataskyddsombud@kmh.se.

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
KMH använder Microsofts Active Directory för att lagra tekniska konton. Kommunikation av lösenord i Active Directory är krypterad. All kommunikation till och från servrar som ingår i identitets- och behörighetssystemet är krypterad enligt standardprotokoll. Endast relevanta systemadministratörer har tillgång till känsliga uppgifter i identitetshanteringssystemet.

KMH har en identitetslösning som bygger på att persondata hämtas från olika källsystem till KMH:s system för identifiering av roller och rättigheter vilken har implementerat processtöd för person- och organisationsinformation samt behörighetsstyrning för högskolans IT-tjänster.

4.3.2
Privata nycklar till certifikat och motsvarande skyddas av rättigheter i servrarna.

4.3.3
All kommunikation till och från servrar som ingår i identitets- och behörighetssystemet är krypterad enligt standardprotokoll.

4.3.4
Shibboleth-nycklarna använder minst 2048-bit RSA eller motsvarande.

4.4 Security-relevant Event (audit) records

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

4.4.1
Samtliga händelser i lärosätets persondatabaser för hantering av identiteter, roller och rättigheter loggas och behörig IT-personal kan verifiera audit-loggar i efterhand.

Loggar över lyckade och misslyckade inloggningsförsök skapas i AD och i Shibboleth IdP:n och sparas automatiskt. Även inloggning via svensk e-legitimation med tillitsnivå 2 eller högre loggas. Samtliga loggar har tidsstämpel.

4.5 Incident Management
Om vi har en incident som påverkar våra användare på något sätt så följer KMH Swamids incidentshanteringsprocess.

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
KMH har en lösenordspolicy vilken följer SWAMIDs lösenordspolicy. Se bilaga 1. KMH har krav på minst 8 teckens lösenord och förlitar sig på Microsofts implementation av komplex lösenordspolicy och uppnår därigenom kravet på *24 bitars lösenordsentropi*.

5.1.2
Som autentiseringstjänster stödjer lärosätet SAML2 (via Shibboleth), federering via Azure Active directory samt Radius (primärt för eduroam). De protokoll som KMH stödjer skyddar mot message replay.

5.1.3
KMH uppmanar sina användare att inte dela lösenord med varandra eller på annat sätt minimera risken för otillåten användning av konton.

5.1.4
Lärosätet övervakar kontinuerligt den tekniska infrastrukturen via en dedikerad funktion. Denna funktion har befogenhet att inaktivera samtliga konton som misstänks på något sätt användas av annan än korrekt innehavare och/eller för annat än tillåten användning enligt lärosätets instruktioner.

För IT-tjänster som kräver återautentisering är identitetshanteraren konfigurerad att genomföra detta och inte förlita sig på existerande inloggningssessioner.

KMH håller samtliga IT-system och nätverk uppdaterade så snart nya säkerhetsuppdateringar levereras och uppgraderar till nya versioner när support för tidigare upphör.

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.

Fokus för lärosätets hantering av elektroniska identiteter är att i möjligaste mån automatisera hanteringen för att uppnå kostnadseffektivitet och hög informationskvalitet. Som en del i detta används två huvudsakliga källsystem för att sammanställa informationen.

Ifrån lärosätets personalsystem hämtas information om de som är personal vid lärosätet samt den formellt beslutade kostnadsställeshierarkin. I KMH:s system för identitetshantering sammanställs detta med en verksamhetsfokuserad hierarki.

Information om aktiva studenter hämtas ifrån det studieadministrativa systemet (Ladok) vid lärosätet.

5.2.1
I federationsperspektiv innebär detta att KMH:s system för identitetshantering är auktoritär källa för all person- och organisationsinformation för domänen kmh.se. KMH har ett scope för SAML respektive Eduroam (kmh.se) som KMH har registrerat och äger.

5.2.2
IdP:n för SAML respektive Eduroam har unika identifierare.

5.2.3
Varje användare får en unik användaridentitet.

Den tekniska lösningen återanvänder aldrig tidigare utfärdade konton utan ett konto är alltid unikt knuten till en individ oavsett om kontot är aktivt eller inte.

Användardatabasen har en räknare i sig som ökas för varje ny användare vilket säkerställer att ett id aldrig återanvänds för en annan individ nu eller i framtiden.

5.2.4

Användare använder sitt användarnamn vid inloggning och kan därmed välja användare.

5.2.5

Som förregistrerade identifierare används personnummer, samordningsnummer, interimspersonnummer från NyA/Ladok eller namn och födelsedata. E-postadressen som används vid utskick av engångskod är en förregistrerad identifierare för att knyta aktiveringen till rätt person.

Utlämning av kontouppgifter för personal

Personuppgifter i personalsystemen baseras på de personuppgifter som en anställd lämnat.

Vid kontoskapande erhåller användaren alltid ett e-postmeddelande till en självuppgiven e-postadress med ett tidsbegränsat engångslösenord för att sätta ett lösenord på sitt konto. Den självuppgivna e-postadressen hämtas från personalsystem. I samband med detta används en CAPTCHA för att säkerställa att det är en person som gör detta. Användaren blir här SWAMID AL1.

Utlämning av kontouppgifter för studenter

Personuppgifter för studenter i studieadministrativa systemet baseras på de uppgifter som kommer från antagningssystemet (NyA) och Ladok.

Vid kontoskapande erhåller studenten alltid ett e-postmeddelande till den adress studenten har i NyA eller Ladok med ett tidsbegränsat engångslösenord för att sätta ett lösenord på sitt konto. I samband med detta används en CAPTCHA för att säkerställa att det är en person som gör detta. Studenten blir här SWAMID AL1.

5.2.6

Följande ID-handlingar kan användas vid identitetskontroll, tillsammans med säkerställande att bild på ID-handling matchar identifierad person:

- Svenskt vanligt pass (provisoriskt pass är inte giltigt som legitimation)
- Svenskt nationellt id-kort
- Svenskt körkort
- Svenskt SIS-märkt id-kort
- Identitetskort för folkbokförda i Sverige

- Internationellt pass som uppfyller ICAO Doc 9303
- Nationellt id-kort inom EU/EES som uppfyller Regulation (EU) 2019/1157

Användare kan höja sin tillitsnivå till SWAMID AL2 via följande metoder:

- Legitimering i internservice eller vid IT-avdelningen med ID-handlingar enligt ovan där personnummer eller samordningsnummer från ID-handling matchar uppgifter i persondatabasen (PDB). (metod 4 under 5.2.5 i AL2-profilen)
- Legitimering i internservice eller vid IT-avdelningen med ID-handlingar enligt ovan där namn och födelsedata från ID-handling matchar uppgifter i persondatabasen. En riskbaserad bedömning görs för att säkerställa att det är rätt individ som identifieras. (metod 5 under 5.2.5 i AL2-profilen)
- Inloggning i kontohanteringsportal (för närvarande ett egenutvecklat system, Preflite) i kombination med legitimering via svenskt e-legitimation på minst tillitsnivå 2 eller högre. Personnummer från e-legitimationen jämförs med personnummer för kontot i persondatabasen. (metod 2 under 5.2.5 i AL2-profilen)

Förändringar av tillitsnivåer loggas i kontohanteringssystemen och lagras enligt KMH:s rutiner.

5.2.7

Identifierande uppgifter för användare hämtas från ID-handling vid identifiering eller från NyA/Ladok. Användare kan begära att få sina uppgifter uppdaterade. KMH kan också besluta att uppgifter ska uppdateras. Kontaktuppgifter är antingen självuppgivna, ägs av KMH eller hämtas från andra system (exempelvis Ladok).

Studenterna kan göra detta i studentportalen i studieadministrativa systemet Ladok. Ändringar kan även göras genom anmälan till studieadministrativa avdelningen.

Anställda kan via självbetjäningsportalen i personalsystemet ändra personlig information eller genom kontakt med personalavdelningen.

KMH har kontaktvägar till alla användare. Antingen självuppgivna kontaktuppgifter, kontaktuppgifter som hämtats från andra system (exempelvis Ladok) eller via folkbokföringen.

Tillhörighet för användare hämtas från andra system (exempelvis personalsystemet och Ladok). Vid ändring av tillhörighet ändras detta i persondatabasen inom 31 dagar från beslutet.

Personal kan uppdatera sin privata e-postadress och sitt privata telefonnummer genom inloggning i ”KMH Kontakter”. Vid ändring av dessa sker ingen verifiering att de hör till användaren. Verifiering av detta har inte prioriterats än. Planering pågår för att implementera detta.

5.2.8

Samtlig personal som hanterar användarkonton vid till exempel utdelande och ID-kontroll uppfyller SWAMID AL2 vid inloggning i kontoadministrativa system.

5.3 Credential Renewal and Re-issuing

The purpose of this subsection is to ensure that credentials are stored accordingly and that Identity Management systems have a high degree of availability.

5.3.1

Användare kan byta sitt lösenord.

5.3.2

Office365:s inloggningsfunktion används av studenter och personal utan tjänstedator för att utföra lösenordsbyte. Anställda med tjänstedator utför lösenordsbyte via sin tjänstedator via inställningar efter inloggning på datorn. För att byta lösenord behöver användare visa att man besitter kunskap om det nuvarande lösenordet knutet till kontot.

5.3.3

Användare kan återställa sitt lösenord via följande metoder:

- Legitimering vid IT-avdelningen med ID-handlingar enligt ovan där personnummer eller samordningsnummer från ID-handling matchar uppgifter i persondatabasen (PDB). (metod 4 under 5.2.5 i AL2-profilen). Användaren får därefter sätta ett nytt lösenord. Tillitsnivån blir AL2.
- Legitimering vid IT-avdelningen med ID-handlingar enligt ovan där namn och födelsedata från ID-handling matchar uppgifter i persondatabasen. En riskbaserad bedömning görs för att säkerställa att det är rätt individ som identifieras. (metod 5 under 5.2.5 i AL2-profilen). Användaren får därefter sätta ett nytt lösenord. Tillitsnivån blir AL2.
- Inloggning i kontohanteringsportal (för närvarande ett egenutvecklat system, Preflite) via svenskt e-legitimation på minst tillitsnivå 2 eller högre. Personnummer från e-legitimationen jämförs med personnummer för kontot i persondatabasen. (metod 2 under 5.2.5 i

AL2-profilen). Användaren får därefter sätta ett nytt lösenord. Tillitsnivå blir AL2.

Microsoft Self-Service Password Reset (SSPR) kan också användas för återställning av lösenord. För detta måste användaren först ha verifierat en självuppgiven e-postadress och ett självuppgivet mobilnummer med hjälp av en tidsbegränsad engångskod/engångslänk som verifieras i samband med en inloggning med sitt konto. Vid lösenordsåterställningen skickas en tidsbegränsad engångslänk till e-postadressen och en tidsbegränsad engångskod via SMS som matas in på länken. Användaren får därefter sätta ett nytt lösenord. Tillitsnivå bibehålls. Eventuell höjning av tillitsnivå loggas enligt 5.2.6.

5.4 Credential Revocation

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

5.4.1

Användaren kan själv begära att kontot inaktiveras och kontaktar då IT-avdelningen som ombesörjer detta.

Vid misstanke om missbruk av konto, antingen av användaren själv eller att tredje part fått tillgång till användarens konto, finns funktionalitet för att spärra för användandet av utpekat konto. Separat rutin för detta beskriver vem som har befogenhet att ta beslut för stängning resp hävande av stängning. Tekniskt utförs detta av katalogadministratör. Under tiden spärren är aktiv tillåts ingen inloggning och kontot kan inte användas för autentisering i IT-tjänster eller återaktiveras av användaren själv.

Konton för personal följer angivna tider för befattningen enligt lärosätets personalsystem. Personalens användarkonton inaktiveras per automatik när tiden för befattningen och aktuell karenstid upphör. Undervisande personals konton är aktiva 6-18 månader (beroende på om personen har månadslön eller är timavlönad) och inaktiveras efter detta. Källsystemet för studenter är systemet för studieadministration. Studentkonton är normalt aktiva maximalt 6 månader efter kursens sista dag och inaktiveras efter detta om studenten inte är antagen till utbildning nästkommande termin.

5.4.2

Återaktivering av konton sker enligt samma rutiner som i 5.3.3.

Innan ett konto som blivit inaktiverat på grund av en säkerhetsincident återaktiveras kontaktas användaren och orsaken till att kontot blivit inaktiverat beskrivs. Återaktivering av konton sker enligt samma rutiner som i 5.3.3 efter att *spärr har hävts*.”

5.4.3
Vid säkerhetsincidenter har KMH rutiner för att åtgärda dessa och säkerställa att de inte återupprepas.

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
KMH:s system för identitetshantering innehåller en komplett historik över utfärdade identiteter och via ett sökgränssnitt kan katalogadministratörer söka fram information knuten till individer med både aktiva och inaktiva konton. Historiken sparas så länge den behövs för att utreda säkerhetsincidenter.

5.5.2
Den tekniska lösningen är installerad med full redundans där det är bedömt relevant. Komponenterna är en del av den infrastruktur som omfattas av beredskapen för kritiska Bas-IT-tjänster och har därför aktiva insatser av IT-personal utanför normal arbetstid.

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
KMH har implementerat samtliga tekniska protokoll enligt SWAMIDs rekommenderade best practice och använder SWAMIDs rekommenderade installationsanvisningar för Shibboleth som utgångspunkt för lokal konfiguration.

5.6.2
KMH tillåter inte inloggning med spärrade konton.

5.6.3
KMH kräver att användaren anger sina inloggningsuppgifter vid inloggning.

5.6.4
Vid användning av SWAMID-tjänster krävs att lösenord matas in på nytt senast 12 timmar efter senaste inloggningen.

BILAGA 1

KMH:s lösenordspolicy för SWAMID.

Lösenordsregler

Detta dokument anger KMH:s policy för kvalitet på samt hantering av lösenord.

Som användare av KMH:s informationssystem ansvarar du själv för att

- dina lösenord uppfyller den kvalitet och hantering som anges i denna policy genom att
    - bestå av minst 8 tecken.
    - bestå av minst en versal, minst en gemen och antingen minst ett specialtecken eller en siffra.
- du håller dina lösenord hemliga genom att
    - aldrig uppge dina lösenord till någon som efterfrågar dem via e-post, i telefon eller på annat sätt.
    - aldrig använda samma lösenord i andra system.
- du ändrar ditt lösenord om du fått kännedom om att säkerheten runt ditt lösenord har äventyrats.

BILAGA 2

Policy för hantering av personuppgifter inom ramen för identitetsutgivaren (Identity Provider, IdP) som fastställts av KMH

Identitetsutgivaren genomför autentisiering på uppdrag av en tjänst som KMH har kännedom om, antingen genom att metadata om tjänsten levereras via SWAMID-federationen eller genom att tjänsten och KMH har en särskild överenskommelse. Beroende på vilken typ av tjänst det rör sig om, syftet med tjänsten och vilken relation tjänsten har till KMH:s IdP levereras en eller flera personuppgifter till tjänsten från KMH:s system för identitetshantering. Detta förfarande följer intentionerna i den svenska personuppgiftslagen.

Alla webbtjänster får tillgång till en unik identifierare som gör att det är möjligt för användaren göra inställningar vid en inloggning och få tillgång till samma inställningar vid nästa inloggning. Denna unika identifierare är unik för just denna tjänst och går inte samköra mellan olika webbtjänster.

Tjänster som kategoriseras i SWAMIDs metadata med entitetskategorier får attribut i enlighet med SWAMIDs rekommendationer, se nedan.

Tjänster vars primära syfte är att stödja forskning och utbildning får tillgång till ungefär samma personuppgifter som automatiskt skickas med varje e-postbrev, dvs. namn, e-postadress, användaridentitet, om användare är student eller verksam (anställd eller övrigt verksam) samt att användaren har ett konto hos KMH. Registrerade tjänster som via GÉANT Data Protection Code of Conduct följer den Europeiska unionens dataskyddsdirektiv, i Sverige personuppgiftslagen, får tillgång till samma information.

De tjänster vars syfte är att för studenter hantera antagning, kursregistrering, tentamensanmälan, examination, verksamhetsförlagd utbildning, stipendieansökan, självservice för användarkonton och självservice för KMH:s personalsystem får tillgång till användarens personnummer.

BILAGA 3

SWAMID Service Definition

Generell beskrivning av SAML2 WebSSO

Tjänsten innefattar autentisiering av användare som har en elektronisk identitet på KMH, samt attributöverföring gällande den autentiserade användaren. Tjänsteutgivaren/högskolan är medlem i SWAMID, den svenska identitetsfederationen för forskning och högre utbildning. Tjänsten är uppsatt i enlighet med SWAMIDs policy och övriga regler och riktlinjer som fastställts av SWAMID.

Policy för personlig integritet

Tjänsten följer den policy för hantering av personuppgifter (*länk till ”ovanstående”policy*) som fastställts av KMH, i enlighet med svensk lagstiftning.

Tjänsten och dess begränsningar

KMH garanterar en tillgänglighet till tjänsten som stämmer överens med KMH:s krav och förväntningar. Processen för utdelande, avslutande och underhåll av elektroniska identiteter vid KMH finns här (*länk till huvuddokumentet ”beskrivning av identitetshanteringsprocessen”*). KMH följer SWAMIDs rekommendationer för utlämning av attribut, baserad på entitetskategorier. KMH förbehåller sig att i kommunikation med en tjänsteutgivare förändra faktiskt utgivna attribut, oavsett vad som rekommenderas av SWAMID gällande den entitetskategori som tjänsteutgivaren har placerats i.

Servicedesk och supportfrågor

För frågor och felanmälan gällande KMH och dess SAML2 WebSSO-tjänst hänvisas till följande lokala supportkanaler

Tfn: 08-572 10 112

Epost: helpdesk@kmh.se

Webb: www.kmh.se