Riktlinjer

2021-11-25 Diarienummer 21/618

IT-avdelningen
Elisabeth Smedberg
IT-chef

Ange mottagare
Ange adress
Ange postadress

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.

KMH, organisationsnummer 20 21 00 – 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).

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.

KMH har instruktioner, för nyttjande av användarkonto vid KMH, i den s k ansvarsförbindelsen, som respektive användare genom aktiv handling måste intyga att den läst igenom innan användarkontot aktiveras. Dessa finns även tillgängliga på KMH:s webbplats. I ansvarsförbindelsen ingår även information om SUNET:s policy för användning av nätet. I likhet med motsvarande

dokument är det individens skyldighet att hålla sig ajour med förändringarna och vid större förändringar så upplyses alla med aktiva konton via mail.

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 och 3). 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.

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

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

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

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 omplex lösenordspolicy och uppnår därigenom kravet på *24 bitars lösenordsentropi*.

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

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

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.

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 studieadministrationssystemet vid lärosätet.

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.

IdP:n för SAML respektive eduroam har unika identifierare

För respektive individ skapas en elektronisk identitet i systemet för identitetshantering och generellt ett användarkonto.

Personuppgifter i studieadministrativa systemet baseras på de uppgifter som kommer från antagningssystemet (NyA). Personuppgifter i personalsystemen baseras på de personuppgifter som en anställd lämnat. Samtliga användare måste uppvisa ID-legitimation vid ankomst till KMH för att kunna erhålla passerkort och för att kunna höjas från SWAMID Identity Assurance Level 2.

För att aktivera ett användarkonto behöver individen få tillgång till ett engångs-lösenord som distribueras av katalogadministratör via en särskild IT-tjänst till användarens privata e-postkonto vilket innebär SWAMID Assurance Level 1. Den privata e-postkontoadressen erhålles via NyA i samband med att sökande ansöker om utbildning. Anställda anger privat e-postadress i rekryteringssystemet när de ansöker till en tjänst eller i uppdragsavtalet när uppdragstagare anlitas. Användaren har genom detta uppnått SWAMID Identity Assurance Level 1. För att användaren ska kunna erhålla SWAMID Identity Assurance Level 2 behöver användaren när den är på plats på KMH uppvisa sitt ID-kort i internservice där personnummer används som identifierare samtidigt som lösenordet ersätts med ett nytt.

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.

Slutanvändare kan själv ändra personlig information. Studenterna kan göra detta i studentportalen i studieadministrativa systemet. Ändringar kan även göras genom anmälan till studieadministrativa avdelningen.

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

Slutanvändare erhåller behörighet till ett antal grundläggande IT-tjänster vilka styrs utifrån identifiering av roll och rättighet via KMH:s system för identitetshantering. Slutanvändare kan även ansöka om behörigheter för övriga IT-tjänster enligt gällande rutiner för respektive IT-system/-tjänst.

En katalogadministratör kan genomföra en identitetskontroll av en användare antingen som en del i utlämnande av en engångskod för aktivering av användarens konto eller som separat händelse. Personnummer används som

identifierare. Användaren presenterar en identitetshandling som uppfyller regelverket för giltiga identitetshandlingar enligt definition i punkt 2 resp 3 under 5.2.5 i SWAMID Assurance Level 2 Profile. Personnummer angivet på ID-kortet ska då stämma överens med namn och personnummer angivet i systemet för identitetshantering. Användarens konto kan om alla uppgifter överensstämmer höjas till tillitsnivån SWAMID Assurance Level 2.

Som grund för identitetskontroll används även utdelande av lärosätets campus-täckande passerkort för anställda, studenter och övriga verksamma. I internservice kan identitetskontrollen genomföras med stöd av personnummer som identifierare och passerkortet i kombination med att logga in på sitt konto. Internservice identifierar användaren och verifierar via internservicesystemet. Informationen exporteras till kontohanteringssystemet och anses vara en fullgod identitetskontroll för att medföra höjning till SWAMID Identity Assurance Level 2.

För att uppfylla all funktionalitet kring tillitsnivåer stödjer KMH:s system för identitetshantering att tekniska konton kan ha antingen tillitsnivån SWAMID Assurance Level 1 alternativt SWAMID Assurance Level 2.

Studenter har dock endast uppnått SWAMID Assurance Level 2 baserat på de uppgifter studenter lämnat i samband med ansökan via NyA respektive anställda lämnat vid ansökan till tjänst och efter att de erhållit utskick på sin privata e-postadress mottagit information om inloggning med temporärt lösenord.

Efter att ett engångslösenord distribuerats till en användare har en användare endast uppnått SWAMID Assurance Level 1. När användaren loggar in första gången behöver den ange både privat e-postadress samt privat mobilnummer vid inloggningen samt ett nytt lösenord sättas.

För att användaren ska erhålla tillitsnivån SWAMID Assurance Level 2 krävs att användaren när den är på plats på KMH uppvisar giltig ID-legitimation. Detta görs samtidigt som användaren hämtar ut sitt passerkort.

Användaren besöker internservice vid KMH och visar upp sin giltiga ID-legitimation. Uppgifter och foto på ID-legitimationen kontrolleras av behörig personal i internservice att dessa överensstämmer med personen samt angivna uppgifter i systemet för identitetshantering. En e-postkod skickas till användarens privata e-postadress för att verifiera att det är rätt person som har tillgång till e-postkontot. När detta är verifierat registrerar behörig personal i systemet för identitetshantering att användaren har uppfyllt SWAMID Assurance Level 2. Passerkort tilldelas även användaren.

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

Samtlig personal som hanterar användarkonton vid till exempel utdelande och ID-kontroll uppfyller SWAMID Assurance Level 2 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.

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.

Skulle man sakna kunskap om nuvarande lösenord knutet till ett konto kan man kontakta internservice alternativt helpdesk för att få en engångskod som tillåter användaren att sätta ett nytt lösenord. En engångskod får inte lämnas ut till en person om inte uppvisar en giltig ID-handling där personnumret verifieras överensstämma med personnumret i systemet för identitetshantering.

Samtliga verksamma kan även återställa ett förlorat lösenord genom utskick av engångskod till i förväg verifierat mobilnummer i kombination med engångslänk utskickad till i förväg verifierad privat epost-adress och bibehåller då SWAMID Assurance Level 2.

Engångslösenord är endast giltigt 12 timmar.

5.4 Credential Revocation

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

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 6 månader efter kursens sista dag och inaktiveras efter detta om studenten inte är antagen till utbildning nästkommande termin.

Så länge användaren identifieras som samma individ så återaktiveras tidigare upplagda konton i de fall individen återvänder till lärosätet.

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.

För att åter få tillgång till kontot kontaktas användaren och orsaken till att kontot blivit spärrat beskrivs.

I övrigt gäller rutiner enligt 5.2 Credential Issuing och tillitsnivå för användare därefter sätts enligt vilken rutin som använts. KMH har rutiner för när en användare stängs av och om/när beslut fattas om att ta bort avstängningen.

KMH:s loggar visar när sådana händelser har inträffat och åtgärder företas för att minimera att samma typ av händelse 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.

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.

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. Lärosätet har däremot idag ej jour 24x7 på någon del av IT-infrastrukturen.

5.6 Credential validation/authentication

The purpose of this subsection is to ensure that the implemented Validation/Authentication processes meet proper technical standards.

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

KMH tillåter inte inloggning med spärrade konton.

KMH kräver lösenord vid inloggning.

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

BILAGA 1 (till riktlinjer för hantering av elektroniska identiteter på KMH)

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 – (till riktlinjer för hantering av elektroniska identiteter på KMH)

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 (till riktlinjer för hantering av elektroniska identiteter på KMH)

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 (bilaga 2) 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 framgår av detta huvuddokument. 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