EHS Identity Management Practice Statement

1. Inledning

Enskilda Högskolan Stockholm AB (lärosätet) är en medlemsorganisation i SWAMID som lagrar inloggnings- och personuppgifter för lärosätets anställda i Active Directory för autentisering mot lärosätessystem som är kopplade till SWAMID. Systemet Shibboleth används för federerad inloggning. Lärosätet tillhandahåller personliga konton åt sina anställda och tillitsnivåerna AL1/AL2 definieras när kravet är uppfyllt. Lärosätet förser inga konton till sina studenter.

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 Organisationsnummer: 556947-8968

4.1.2 Tillämpningsbara lagrum

Enskilda Högskolan Stockholm är en enskild utbildningsanordnare med statliga anslag för att genomföra utbildning enligt avtal med svenska staten och vad som i övrigt framgår av årliga regleringsbrev om anslag 2:63 och 2:65 inom utgiftsområde 16 Utbildning och universitetsforskning.

Lärosätet använder Active Directory och Shibboleth som identitets- och behörighetssystem som 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 i enlighet med Dataskyddsförordningen, a.k.a. General Data Protection Regulation (GDPR 2016/679), som reglerar behandlingen av personuppgifter samt hantering av personer med behov av skyddade personuppgifter.

Studenters personuppgifter hämtas ur lärosätets studiedokumentationssystem Ladok. Därför tillämpas även förordning (SFS 1993:1153) om redovisning av studier med mera vid universitet och högskolor för hanteringen av studenters personuppgifter i kontohanteringssystemet.

4.1.3 Rutiner för destruering av lagringsmedia

Lagringsmedia som har förbrukats demonteras, destrueras och lämnas till återvinningscentral.

4.2 Notices and User Information

The Member Organisation provides an Acceptable Use Policy (AUP) and a Service Definition including a Privacy Policy (PP) for the organisation 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 Användarvillkor

Användarvillkoren presenteras vid första inloggning i sidan ’terms of use’.

4.2.2 Godkännande

Användarvillkoren presenteras efter lyckad inloggning och måste godkännas av användaren för åtkomst till tjänsten.

4.2.3 Uppdatering av användarvillkor

När användarvillkoren uppdateras så publiceras informationen på IdP:ns inloggningssida samt ansvarsförbindelsen nollställs för samtliga användare för nytt godkännande.

4.2.4 Loggning av ansvarsförbindelsen

Ansvarsförbindelsen loggas i en MySQL-databas på IdP:ns server och lagras i 365 dagar.

4.2.5 Tjänstedefinition

Kan läsas på Tjänstebeskrivning för federerad inloggning – SAML2 WebSSO - Enskilda Högskolan Stockholm som syns i PrivacyStatementURL
i metadatan för idp;n.

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 IT-personal med teknisk åtkomst

Lärosätets IT-leverantör lagrar autentiseringsuppgifter om administratörskonton för åtkomst till IT-miljön samt nycklar som berör identitetshanteraren i ett dokumentationssystem som kräver tvåfaktorsautentisering.

Samma system används för lagring av delade hemligheter.

4.3.2 Hantering av privata nycklar, RADIUS-hemligheter etc

Informationen sparas krypterat hos IT-leverantören i skyddad serverhall. Särskild dörrkod krävs för fysisk åtkomst till lärosätets servermiljö där server för identitetsutfärden finns.

4.3.3 Kryptering

All nätverkskommunikation mellan idP och Active Directory sker via LDAPS. RSA-nyckel med 4096 bitar.

4.3.4 Entity keys

Encryption och signing cert använder 4096-bitars RSA.

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 säkerhetsrelaterade händelser

Händelser som lyckade och misslyckade inloggningar loggas i Shibboleth samt förändring av attribut på användarkonton loggas i Active Directorys händelselogg.

4.5 Incident Management

4.5.1

Vid en säkerhetsincident som innefattar, eller riskerar att innefatta, inloggning via SWAMID, följer EHS SWAMID Incident Management Procedure.

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 Organisationens val av autentiseringsmekanismer

Lärosätet skapar ett personligt användarkonto åt användaren och genererar ett

lösenord som följer Microsofts Active Directory inställning för komplexa lösenord, med ett krav på minst 10 tecken.

5.1.2 Vilka tekniska protokoll som används

Vi följer SWAMIDs rekommendationer kring konfigurering av tekniska protokoll för IdP.

5.1.3 Rutiner för information till användarna rörande missbruk

Användarvillkor och regler för användning visas på användarnas första inloggningssida.
Användaren informeras även vid utdelning av inloggningsuppgifter.

5.1.4 Rutiner för tekniskt skydd mot missbruk

Inloggning blockeras efter 10 misslyckade försök och kontot låses i 30 minuter.
Loggar kontrolleras kontinuerligt. Vid misstänkt missbruk kontaktas användaren.

Nätverkets brandvägg tillåter endast nödvändig trafik, och automatiskt installerar firmware uppdateringar när de finns tillgängliga.
Säkerhetsuppdateringar för dess operativsystem körs även automatiskt varje vecka. (om de finns tillgängliga).
Systemen övervakas av IT-leverantör som får larm så fort övervakningsmjukvaran eller antivirusprogrammet rapporterar potentiellt missbruk.

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 Identitetsutfärdarens administrativa domän i SWAMID

Som administrativ domän i SWAMID används ehs.se samt ths.se.

5.2.2 Identitetsutfärdarens globalt unika identifierare

idp.ths.se

5.2.3 Varje användare ska ha ett eller flera unika användarnamn som inte får återanvändas för andra användare

Varje användaridentitet kan bara användas för en användare, och en tilldelad identitet kan inte därefter tilldelas om till en annan användare.

Vid nyskapande av konto jämförs och anpassas kontots användaridentifierare mot befintliga, så att det aldrig sker en dubblett.
Detta uppnås genom att gamla konton inte rensas bort från Active Directory. Dock vid avslut så flyttas användarna till OU i Active Directory som Shibboleth inte kan läsa från, så att det inte kan användas för inloggning inom SWAMID.

Användarens eduPersonPrincipalName är knutet till användarobjektets userprincipalname, som följer standarden fornamn.efternamn@ehs.se.
Detta attribut är statisk och inte förknippad med e-postadress.

SubjectID skapas enligt följande standard. Två första bokstäverna i förnamn samt sista bokstav i förnamnet, följt av de två första bosktäverna i efternamn samt den sista bokstaven följt av 01 (som adderas om inlägget redan finns).

5.2.4 Om användare har fler än ett användarkonto ska de kunna välja vilken de använder vid inloggning, exempelvis ett studentkonto och ett anställdkonto

Användare får endast ett personligt användarkonto.

5.2.5 Rutiner för utdelande av kontouppgifter

Studierektor, prefekt eller administrativ chef på lärosätet tar person- och kontaktuppgifter av användaren och uppgifter som förnamn, efternamn, personnummer, mobilnummer samt tillitsnivå noteras på användarens konto i Active Directory. En person som inte har legitimerats tilldelas tillitsnivå AL1. Vid behov av tillitsnivå AL2 så utförs legitimationskontroll och datum och tid för kontroll samt vem som har utfört kontrollen noteras på användarens konto.

Användarkontot skapas med ett slumpmässigt genererat lösenord som ingen känner till. Användaren meddelas sedan per e-post att kontot är skapat och uppmanas att gå

in på självbetjäningsportalen för lösenordsåterställning, denna återställning beskrivs i §5.3.3.

E-postadress och telefonnummer används som förregistrerade identifierare för att säkerställa att det är samma individ vid lösenordsåterställning.
eduPersonPrincipalName anges för att påbörja återställningsprocessen.

Innan kontot kan delas ut behöver användaren verifiera sitt telefonnummer, som ska användas som förregistrerad identifierare.
Detta görs genom att IT-administratören skickar en 6-siffrig kod till telefonnumret via SMS som användaren får skicka tillbaka till IT-administratören inom 15 minuter.
Denna rutin genomförs ej för mejladressen då det alltid är deras tjänstemejladress.

Vid höjning av tillitsnivå så utförs samma kontroll som beskrivs tidigare i denna paragraf, alltså AL2 kontrollen, samt en lösenordåterställning enligt samma rutin som är beskrivs i §5.3.3.

Vid höjning av tillitsnivå, så binder vi legitimationskontrollen till användarkontot med hjälp av namn, eduPersonPrincipalName samt personnummer/samordningsnummer.
Studenter berörs inte av detta då de autentiserar med sitt eduID.
För att binda de som saknar svenskt personnummer till rätt individ görs en riskbedömning med hjälp av kombination av namn, födelsedatum, utfärdande land samt eventuell ytterligare kunskap.

Rutin för legitimering av:

Svensk medborgare:
För giltig ID-handling följer legitimationskontrollen Polisens riktlinjer för svenska medborgare enligt: https://polisen.se/tjanster-tillstand/pass-och-nationellt-id-kort/giltiga-id-handlingar/

EU-medborgare:
Giltig legitimationshandling definieras i Skatteverks föreskrifter om identitetskort (SKVFS 2009:14). I föreskriften nämns EU-pass som giltig legitimationshandling. Med EU-pass menas pass eller nationellt identitetskort utfärdade enligt kraven i Rådets förordning (EG nr 2252/2004). På PRADO (Public Register of Autenthic Identity and TravelDocuments Online) finns giltiga legitimationshandlingar för de olika länderna i EU.

Tredjelandsmedborgare:
För personer från länder utanför EU och Schengen gäller pass som legitimationshandling. Vid tveksamhet kring giltigheten av utländskt pass äger kontrollören rätt att i stället kräva svensk giltig legitimationshandling.

5.2.6 Hur eventuellt byte av tillitsnivåer för användare hanteras

Vid höjning av tillitsnivå till AL2 måste användaren legitimera sig till studierektor, prefekt eller administrativ chef på lärosätet som sedan meddelar IT-avdelningen att förändring av AL-nivå ska ske för användaren. Datum och tid för kontroll, tillitsnivå samt vem som har utfört kontrollen noteras på användarens konto i Active Directory.

För att säkerställa att det är samma individ som identifieras som tidigare fått kontot

utdelat till sig så kräver vi att lösenordsåterställningsprocessen genomförs, som beskrivs i §5.3.3.
Detta åstadkoms genom att IT-administratören i samband med höjningen inaktiverar det aktuella lösenordet till ett okänt lösenord.

Efter ovannämnda legitimationskontroll jämförs namnet,eduPersonPrincipalName samt personnummer/samordningsnummer som skickas in till IT-administratören med uppgifterna i Active Directory som behöver vara överens innan tillitsnivån kan utdelas.
För att binda de som saknar svenskt personnummer till rätt individ görs en riskbedömning med hjälp av kombination av namn, födelsedatum, utfärdande land samt eventuell ytterligare kunskap

5.2.7 Ändring av eventuell självuppgiven information, exempelvis privat epostadress

Vi använder informationen under identitetskontrollen, som beskrivs i §5.2.5, som underlag för personlig information.

Lärosätet har möjlighet att uppdatera personlig information i registret om det efterfrågas av användare eller lärosätet i sig.

Lärosätet i sig matar in användarens kontaktinformation och användaren har möjligheten att uppdatera sin personliga information med hjälp av lärosätets administratörer.

Lärosätet har möjlighet att använda användarens registrerade kontaktuppgifter om så behövs.

Information om tillhörighet inom organisationen kommer från lärosätet i sig och uppdateras inom 31 kalenderdagar efter ändringen.

5.2.8 Krav på tillitsnivå vid all kontoadministration

För all personal med behörighet att utföra kontoadministration krävs tillitsnivå AL2.
Det är endast IT-administratörer som får administrera konton, som samtliga uppnår AL2.
Samtliga som genomför legitimationskontroll uppnår tillitsnivå AL2.

Kommunikation mellan administratör och IT-leverantör vid kontobeställning eller tillitsnivåförändring ska ske via säker kanal.

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.

5.3.1-5.3.2 Användares frivilliga byte av lösenord och andra inloggningsfaktorer

Användare kan återställa sitt lösenord genom att gå igenom lösenordsåterställningsprocessen via lärosätets SWAMID Self- Service Portal, som förklaras i §5.3.3.

Användarna kan ändra sitt lösenord genom att logga in på Self- Service portalen och byta lösenord. Det gamla lösenordet behöver anges för att kunna byta lösenord via detta verktyg. Det finns inte möjlighet för SSO vid denna process.

5.3.3 Återställning av användares lösenord

Användare kan återställa sitt lösenord på självbetjäningsportalen genom att först begära en engångslänk till sin verifierade e-postadress följt av engångskod till sitt verifierade mobiltelefonnummer. Engångslänkar och engångskoder har en livslängd på 5 minuter. Lösenordskomplexitet appliceras enligt § 5.1.1. eduPersonPrincipalName anges för att påbörja återställningsprocessen.

5.4 Credential Revocation

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

5.4.1 Hur ett användarkonto spärras när användaren lämnar organisationen eller om ett användarkonto missbrukas

När en användare avslutar sin anknytning till lärosätet spärras kontot och tas bort vid terminsslut.
Om missbruk upptäcks spärras användarkontot och användaren informeras.
Användaren kan själv begära att få sitt användarkonto spärrat.

5.4.2 Hur ett användarkonto återaktiveras efter att tidigare ha varit spärrat och hur användare informeras vid säkerhetsincidenter

Om användare åter knyts till lärosätet måste användaren genomgå rutin enligt § 5.2.5 och legitimationskontroll utförs för att säkerställa personens identitet. När kontot har aktiverats sätts ett slumpmässigt genererat lösenord och användaren får själv återställa sitt lösenord enligt §5.3.3. Om säkerhetsincident inträffats och/eller lösenord har äventyrats informeras användaren om situationen så att en incident kan motverkas, sedan återaktiveras kontot och användaren blir uppmanad att återställa sitt lösenord på självbetjäningsportalen enligt metod §5.3.3.

5.4.3 Hur medlemsorganisationen minimerar risken för att säkerhetsincidenter återupprepas

Lärosätet och IT-leverantören upplyser och utbildar användaren om

situationen/säkerhetsincidenten i förebyggande syfte.
IT-leverantören arbetar nära lärosätet med platsbesök där dialog kring säkerhet uppstår regelbundet.
IT-leverantören är ständigt uppdaterad vad gäller säkerhetsnyheter och tar regelbunda åtgärder för att anpassa lärosätets miljö.

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 Att ett register upprätthålls över samtliga utfärdade identiteter

Active Directory används som register och avslutade användarkonton återanvänds inte. Om en användare åter knyts till lärosätet tilldelas ett nytt konto och användaren genomgår rutin enligt § 5.2.5.

5.5.2 Att medlemsorganisationen har en tillgänglighet på sin identitetsutfärdare som medger att den kan användas för inloggning till interna system

Identitetsutfärdaren och tillhörande system har hög tillgänglighet och används för diverse interna system som Ladok. Den har möjlighet och tillgänglighet för att användas mot fler system.

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 Validering av rättigheter
Shibboleth och eduroam är konfigurerade enligt instruktioner från SUNET, SWAMID och eduroam.org.

5.6.2 Autentisering av inaktiverade konton
Inaktiverade konton kan ej autentiseras på IdP:n.

5.6.3 Autentisering vid inloggning
Användare måste mata in användarnamn och lösenord för autentisering på IdP:n och eduroam och autentiserar sig mot Active Directory med protokollet LDAPS.

5.6.4 Sessionstider
Sessionens livslängd för SAML2-baserad webbinloggning är inställd på 8 timmar. För eduroam är ingen tidsgräns satt.