Stockholms universitet

BESLUT
2018-06-08 Dnr SU

IT-avdelningen
Infrastruktursektionen

SU Identity Management Practice Statement

1. Inledning

Stockholms universitet (SU) förnyar medlemskap i SWAMID och kommer att efterleva deras policyer. Förutom SWAMID Federation Policy finns ett antal tillitsprofiler:

Stockholms universitet ämnar uppfylla kraven för Identity Assurance Level 1 och Identity Assurance Level 2 beroende på användarkategori. Detta inkluderar att universitet följer de rekommendationer som SWAMID har satt upp gällande interaktion mellan de lokala systemen och externa system i federationen.

Detta dokument är Stockholms universitets Identity Management Practice Statement (IMPS).

Som en del av medlemskapet i SWAMID krävs att universitetet årligen bekräftar till SWAMID att dokumentet fortfarande är giltigt. Om denna handläggningsordning uppdateras skall SWAMID ta del av denna och godkänna medlemskapet på nytt.

2. Identitetstyper

SUKAT är den katalogtjänst/användardatabas vid SU via vilken användare till de gemensamma systemen autentiserar sig. Tjänsten utgörs av en Lightweight Directory Access Protocol (LDAP)-katalog på katalogtjänstmiljön Open LDAP. Till denna katalogtjänst finns även ett Active Directory (AD) som ett gränssnitt för de system som inte autentiserar via LDAP. Samtliga konton och delar av kontoinformationen replikeras från LDAP till AD. Autentisering mot katalogtjänsten sker krypterat. Detta beskrivs i detalj av dokument: Identitetshantering vid Stockholms universitet, 2010-07-12 version 1.2

3. Compliance and Audit

Revision av rutiner angivna i detta dokument, sker senast inom 12 månader från senaste revisionstidpunkt och ingår i tjänsteplan för IdM under objekt Teknisk plattform. Vid förändringar i hanteringsprocesser eller teknik granskas dokumentet av Informationssäkerhetsfunktionen och en uppdaterad IMPS skickas till SWAMID för godkännande.

4. Organisational Requirement

4.1 Enterprise and Service Maturity

4.1.1 Lärosätets/myndighetens/stiftelsens organisationsnummer

Stockholms universitet har organisationsnummer 202100-3062 och är en statlig utbildningsmyndighet vilket gör att lärosätets verksamhet regleras i lagar, förordningar och regleringsbrev.

4.1.2 Tillämpbara lagrum

De viktigaste lagarna och förordningarna som styr universitetets 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 högskolans uppdrag under ett kalenderår. I övrigt följer lärosätet Sveriges övriga lagar och förordningar.

Universitetets katalog- och behörighetssystem LDAP 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. Dataskyddsförordningen a.k.a. General Data Protection Regulation (GDPR 2016/679) och offentlighets- och sekretesslagen (SFS 2009:400) reglerar behandlingen av personuppgifter samt hantering av personer med behov av skyddade personuppgifter.

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

Som statlig myndighet arbetar lärosätet även med ledningssystem för informationssäkerhet enligt Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2009:10).

4.1.3 Rutiner för destruering av lagringsmedia

Rutin beslutad av IT-avdelningen under SU Universitetsförvaltning.

ITAM-SU Processhandbok, LCM - Life Cycle Management för hårdvara och programvara

(Bilaga 1)

4.2 Notices and User Information

4.2.1 Användarvillkor

Användarvillkor finns på IdP i enligt SWAMID’s föreskrift. (bilaga 2)

4.2.2 Godkännande

Användarna godkänner användarvillkoren i samband med att de hämtar ut sitt konto och loggar in på IdP.

4.2.3 Ny ansvarsförbindelse

När universitetet beslutar om att ge ut en ny version av ansvarsförbindelsen, hanteras det genom att ny ansvarsförbindelse publiceras på IdP-inloggningssida. Vid nästa IdP inloggning kommer kontoinnehavaren att avkrävas nytt godkännande.

4.2.4 Loggning av ansvarsförbindelsen

Ett godkännande av ansvarsförbindelsen loggas i kontoinnehavarens profil/attribut i SUKAT.

4.2.5 Service definition

Service definition/tjänstebeskrivning (bilaga 2) finns publicerad på SU webb.

Privacy policy finns publicerad på SU webb privacy_policy (bilaga 2)

4.3 Secure Communications

4.3.1 IT-personal med teknisk åtkomst

IT personal med teknisk åtkomst till de servrar och datamedia där lösenord lagras undertecknar även särskild ansvarsförbindelse (Bilaga 3). Ansvarsförbindelse för medarbetare med dessa priviligierade behörigheter finns i SU diarium.

4.3.2 Privata nycklar mm

Privata nycklar och hemligheter skyddas med behörighetskontroll i filsystem och serveraccess.

4.3.3 Kryptering

All nätverkskommunikation skyddas med användning av TLS eller motsvarande kryptering.

4.3.4 Entity keys

Alla entity keys är 2048 bitar RSA .

4.4 Security-relevant Event (Audit) Records

4.4.1 Loggning av säkerhetsrelaterade händelser

Alla förändringar på ett datorkonto loggas.

5. Operational Requirements

5.1 Credential Operating Environment

5.1.1 Lösenord

Lösenord måste vara minst 10 tecken långa och innehålla minst en gemen (liten) bokstav och en versal (stor bokstav) och minst en siffra eller specialtecken. Lösenorden kan ej återanvändas vid lösenordsbyte.

Vara sammansatt av följande tecken:

- A – Z
- a – z
- 0 – 9
- mellanslag
- följande specialtecken: ~,!, @, #, $, %, ^, &, (,), _, +, -, *, /, =, {, }, [,], |, \, :, ;, ’ (enkelt citationstecken), ” (dubbelt citationstecken), <, >, , (kommatecken), . (punkt), och ?.

Användaren uppmanas att inte sätta samma lösenord som de använder i antingen andra interna eller externa IT-tjänster.

Lösenordet får INTE vara eller baseras på:

- namn, hemort, kurs, telefonnummer eller annan personlig, lättillgänglig information
- ett uppslagsord på något språk
- gamla, redan använda lösenord
- innehålla å, ä, ö

Kompletta riktlinjer finns i SU portal. (Bilaga 4)

5.1.2 Tekniska protokoll

All kommunikation mellan de olika delarna som används för hantering av användare och lösenord sker krypterat såsom beskrivet under rubriken SWAMID AL1 4.3.3 – 4.3.4. TLSv1 har inbyggda skydd mot återspelningsattacker (eng. message replay). Replikeringen mellan domänkontrollanter i Active Directory sker enligt Microsofts standardiserade säkerhetsmetod för replikering. SU synkroniserar inte lösenord med externa leverantörer, t.ex. molntjänster.

5.1.3 Skydd mot missbruk

Rutin för skydd mot missbruk finns genom användarpolicyn. Se 4.2.1 ovan.

5.1.4 Personligt ansvar

I SU ansvarsförbindelse framgår att kontoinnehavare är personligt ansvariga för användningen av användarkontot och att det inte får göras tillgängligt för andra. Användarna godkänner detta regelverk innan de använder kontot första gången samt när de gör en lösenordsåterställning.

5.1.5 Konfiguration

Alla servrar som används för kontohantering, webbinloggning och Eduroam är uppsatta och konfigurerade så att de endast är tillgängliga på avsedda tjänsteprotokoll såsom Kerberos, LDAPS, HTTPS, Radius med flera för reglerade IP-adresser med hjälp av brandvägg. Vid IT-avdelningen finns ansvar för att hålla servrar och annan hårdvara uppdaterade med avseende på säkerhetsproblem.

5.2 Credential Issuing

5.2.1 Identitetshanterarens DNS-domän

Den administrativa DNS-domänen su.se används alltid vid attributrelease till det system där användare vill logga in. Detta oberoende om det är SAML2 eller Eduroam.

5.2.2 Hanteringen av användarnamn/konton

Samtliga identitetsservrar vid SU använder unika identifierare. su.se (Stockholms universitet).

5.2.3 Unik användaridentitet

En användaridentitet används bara för en enda person och återanvändas inte för någon annan person.

5.2.4 Flera användaridentiteter

Inom SU har en användare endast ett användarkonto, dvs. både som student och anställd.

5.2.5 Identifieringsmetoder

Legitimationer som accepteras för utlämnande av engångslösen/aktiveringskod:

Europeiska medborgare: Giltig legitimationshandling definieras i Skatteverkets 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 kraven i Rådets förordning (EG nr 2252/2004). På PRADO (Public Register of Authentic Identity and TravelDocuments Online) finns giltiga legitimationshandlingar för de olika länderna i EU.

För personer som kommer från tredje land, d.v.s. länder utanför EU och Schengen, gäller pass som legitimationshandling. Vid tveksamhet kring giltigheten av utländskt pass äger kontrollören rätt att istället kräva svensk giltig legitimationshandling.

Personal
När en anställd börjar arbeta vid SU beställer administrativt ansvarig vid respektive organisation ett användarkonto via ärendehanteringssystemet och ett formulär på vårt ärendehanteringssystem. När handläggare vid katalogadministrationen tar emot begäran skapas ett användarkonto för den nyanställde. Kontouppgifterna (användaridentitet och temporärt lösenord) delas ut av administrativt ansvarig vid respektive organisatorisk enhet. Användare uppmanas att omedelbart byta lösenordet till ett eget som uppfyller kraven i 5.1.1

Vid uthämtandet krävs godkännande av ansvarsförbindelsen och uppvisande av giltig legitimation.

Studenter
Antagna studenter går till en webbsida där de identifierar sig via antagning.se eller EduID. Om ett personnummer returneras anses det som ett bekräftat konto (SWAMID AL2), i annat fall uppmanas studenten att bekräfta sitt konto hos antagning.se eller EduID och återkomma. De får då aktivera ett universitetskonto skapat med användarnamn och automatgenererat lösenord på webben. Lösenordet byts i rutinen Byt lösenord på universitetskonto. För studenter som inte kan identifiera sig via ovan angivna metoder används en tidsbegränsad aktiveringskod. Studenten kan efter legitimationskontroll hämta ut en aktiveringskod, som är en engångskod, på papper hos studerandeexpeditionen. Genom att använda aktiveringskoden tillsammans med sitt personnummer (eller motsvarande) i kontohanteringsportalen får studenten ett fullvärdigt konto och tillgång till alla studentresurser.

Distansstudenter som inte personligen infinner sig är vidimerade genom rutiner hos University Admissions, alternativt via motsvarande rutin på en institution. Rutinen kräver att den sökande skickar en inskannad färgbild direkt från den sida i personens pass som visar persondata och bild. Antagna studenter går till en webbsida där de identifierar sig via engångskod, antagning.se eller EduID. De får då ett konto skapat med användarnamn och automatgenererat lösenord på webben direkt. Lösenordet byts i rutinen Byt lösenord på universitetskonto.

Utländska distansstudenter som inte kan använda antagning.se eller eduID för kontoaktivering eftersom de ett, inte kan logga in och två, inte har ett personnummer kopplat till kontot (obekräftade användare). Rutinen på institutioner kräver att den sökande skickar en inskannad färgbild direkt från den sida i personens pass som visar persondata och bild. Institutionen skickar via e-post en engångskod för aktivering av kontot. Dessa konton åsätts tillitsnivå SWAMID AL1.

Utländsk distansstudent som börjar studera på lärosätet kan efter legitimationskontroll hämta ut en aktiveringskod, som är en engångskod, på papper hos studerandeexpeditionen. Genom att använda aktiveringskoden tillsammans med sitt personnummer (eller motsvarande) i kontohanteringsportalen får studenten ett SWAMID AL2 konto.

I det fall en student med SWAMID AL2 går till att vara utländsk distansstudent utan möjlighet att legitimera sig på lärosätet kommer kontot att återgå till AL1 efter en lösenordsåterställning.

5.2.6 Förändring av AL nivåer

Alla användare uppfyller SWAMID tillitsnivå AL2 förutom utländska distansstudenter som får tillitsnivå AL1. IdP med stödsystem åsätter och hanterar signalering av korrekt tillitsnivå beroende på användarkategori genom attribut eduPersonAssurance i enlighet med SWAMID's regelverk.

5.2.7 Ändring av självuppgiven information

All självuppgiven information kan ändras av kontoinnehavaren.

5.2.8 Krav på identitetsgranskningen

Vid SU är all personal som hanterar användaridentiteter verifierade med AL2-nivå.

5.3 Credential Renewal and Re-issuing

5.3.1 Möjlighet till lösenordsbyte

Alla användare kan byta sitt lösenord genom en webbsida som kräver inloggning.

(Bilaga 5)

5.3.2 Lösenordsbyte

När användaren gör lösenordsbyte på detta sätt anges först det gamla lösenordet innan man anger det nya två gånger. Det nya lösenordet måste uppfylla kraven i enligt 5.1.1 ovan.

5.3.3 Lösenordsåterställning

Lösenordsåterställning utförs på samma sätt som utdelning vid kontoaktivering. (Bilaga 6) Kontouppgifterna (användaridentitet och temporärt lösenord) delas ut av administrativt ansvarig vid respektive organisatorisk enhet. Användare uppmanas att omedelbart byta lösenordet till ett eget som uppfyller kraven i 5.1.1

5.3.4 Framtvingande av lösenordsbyte

Kontoansvariga/säkerhetsansvariga kan framtvinga lösenordsbyte genom att deaktivera kontot genom att skriva över lösenordet. SU helpdesk att kontaktar kontoinnehavare via kataloganSvarig eller via telefon/e-post/pappersbrev med information att kontot är låst och måste återaktiveras. Kontoinnehavaren måste göra genomföra en lösenordsåterställning enligt 5.2.5 på samma sätt som utdelning vid kontoaktivering (Bilaga 6).

5.4 Credential Revocation

5.4.1 Inaktivering av användarkonton

Samtliga konton kan deaktiveras för användning av IdM/SUKAT administratör genom att lösenordet skriv över. När en anställd avslutar sin tidsbegränsade anställning vid SU stängs kontot av direkt. Anställda med tillsvidare anställning som avslutar sin anställning meddelar via SUKAT administratör för organisatorisk enhet att kontot ska stängas som även medför att e-postkontot tas bort. Studenter får ny affiliation som Alumn och kontot behålls.

5.4.2 Återaktivering av användarkonton

Enligt IT-säkerhetsrutinen för spärrning av användarkonto kommer SU helpdesk att kontakta kontoinnehavare via kataloganSvarig eller via telefon/e-post/pappersbrev med information att kontot är låst. Kontot förblir låst intill problemet är åtgärdat.

Om det avser disciplinärenden: Lösenord ändras i befintligt verktyg så att studenten måste göra lösenordsåterställning enligt 5.2.5

Om lösenord är på drift: Kontoinnehavaren måste göra lösenordsåterställning enligt 5.2.5

5.5 Credential Status Management

5.5.1 Historik över utfärdade identiteter

SU loggar alla händelser rörande lösenordsförändringar till Syslog, dock inte själva lösenordet.

5.5.2 Tillgängligheten för identitetstjänsten

Inloggningsservern för SAML2 och inloggningsservern för Eduroam har en erfarenhetsmässigt högre tillgänglighet än 95%.

5.6 Credential Validation/Authentication

5.6.1 Validering av rättigheter

Både SAML2- och Radius-installationerna uppfyller dessa krav eftersom protokollen är konfigurerade enligt instruktioner från SWAMID och eduroam.org.

5.6.2 Autentisering av inaktiva konton

När en användare byter lösenord tas det gamla lösenordet bort ur Kerberos och ersätts med det nya. Därmed kan det gamla lösenordet inte användas för inloggning. Då kontot stängs av deaktiveras kontot i Kerberos så att autentisering inte kan göras.

5.6.3 Autentisering vid inloggning

SAML2-baserad webbinloggning och Eduroam kräver att användaren matar in sitt användarnamn och lösenord för att användaren ska få tillgång till tjänsten. Webbinloggning har en SSO-funktionalitet som aktiveras efter att användaren loggat in. Eduroam har ingen sådan men användaren kan oftast spara sina inloggningsuppgifter i den klientprogramvara som finns för Eduroam och SU använder därför separata lösenord.

5.6.4 Sessionstider

SAML2-baserad webbinloggning och Eduroam kräver att användaren matar in sitt användarnamn och lösenord för att användaren ska få tillgång till tjänsten. Webbinloggning har en SSO-funktionalitet som aktiveras efter att användaren loggat in. Eduroam har ingen sådan men användaren kan oftast spara sina inloggningsuppgifter i den klientprogramvara som finns för Eduroam.
För SAML2-baserad webbinloggning uppfyller SU kraven med att den maximala längden för SSO-sessionen är tolv timmar. Den maximala giltighetstiden från att användaren gör inloggningen, eller använder SSO-sessionen, tills att tjänsten släpper in användaren i tjänsten är fem minuter. För Eduroam finns ingen SSO-session för inloggning utan där finns en maxtid för hur lång tid en klient får på sig för att genomföra inloggningen. Denna maxgräns är mindre än en minut.