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 aktuella föreskrifter om statliga myndigheters informationssäkerhet.

4.1.3 Rutiner för destruering av lagringsmedia

Avvecklingstjänsten säkerställer att uttjänt hårdvara avvecklas på ett säkert sätt, både ur ett informationssäkerhetsperspektiv och ett miljöperspektiv.

Avvecklingstjänsten

Återtag av servrar och servermedia

Mediedestruktion

(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. zxcvbn används för att bedöma styrkan på lösenordet och endast lösenord med 4 poäng godkänns. Lösenorden kan ej återanvändas vid lösenordsbyte.

Godkända tecken i ett lösenord:

- 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.

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.

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.

5.1.4 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

Metod	Ger Tillitsnivå	Förregistrerad identifierare
Engångskod	SWAMID AL1	Personnummer/Samordningsnummer, interimspersonnummer i kombination med namn, födelsedata i kombination med namn ellere-postadress
Antagning.se	SWAMID AL1, SWAMID AL2	Personnummer/Samordningsnummer /Interimspersonnummer
eduID	SWAMID AL2	Personnummer/Samordningsnummer
Svensk e-legitimation	SWAMID AL2	Personnummer/Samordningsnummer

Alla användare uppfyller minst SWAMID tillitsnivå AL1. Nivån sätts utifrån aktiveringsmetod. Oavsett metod får användaren bekräfta att denne är samma som utfärdaren avser i aktiveringsflödet. Oavsett metod så är personnummer/samordningsnummer/interimspersonnummer förregistrerade i SUs katalog eller LADOK.

Aktivering av konto via engångskod ger alltid tillitsnivå SWAMID AL1 och CAPTCHA krävs alltid.

Aktivering av konto via Antagning.se ger tillitsnivå SWAMID AL1 om användaren är AL1 på Antagning.se och ett interimspersonnummer följer med från Antagning.se och tillitsnivå SWAMID AL2 om inloggningen uppfyller kraven för AL2 (assurance och assuranceCertification).

Aktivering av konto via eduID ger tillitsnivå SWAMID AL2 om inloggningen uppfyller kraven för AL2 (assurance och assuranceCertification).

Aktivering av konto via Svenskt e-legitimation på minst tillitsnivå 3 ger tillitsnivå SWAMID AL2.

Personnummer/samordningsnummer/interimspersonnummer är förregistrerade på konton och jämförs i en legitimationskontroll vid uthämtande av Engångskod. För personer som inte har personnummer/samordningsnummer används en riskbaserad bedömning baserat på födelsedata och namn på giltig legitimation.

Legitimationer som accepteras för utlämnande av Engångskod:
Europeiska medborgare:

- ett pass eller identitetskort som uppfyller Polisen krav "Giltiga id-handlingar när du ansöker om pass eller nationellt id-kort",
- ett pass som uppfyller ICAO Doc 9303 eller
- ett nationellt identitetskort inkl. information om medborgarskap enligt EU-förordning 562/2006. 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.

För legitimationer som saknar personnummer kontrolleras namn och födelsedata mot data som finns i Ladok och/eller SUs katalog då personnummer inte finns att tillgå.

Aktiveringsflöde för olika kontotyper:
Personal
När en anställd börjar arbeta vid SU beställer administrativt ansvarig vid respektive organisation ett användarkonto via ett formulär till SUs ärendehanteringssystem. När handläggare vid katalogadministrationen tar emot begäran skapas ett användarkonto för den nyanställde. Användaren går till en webbsida där de identifierar sig via en svensk e-legitimation, eduID, antagning.se eller Engångskod (som i så fall delas ut av administrativt ansvarig vid respektive organisatorisk enhet eller Infocenter).

Studenter
Antagna studenter går till en webbsida där de identifierar sig via en svensk e-legitimation, eduID, antagning.se eller Engångskod (som i så fall delas ut av institution eller Infocenter).

Studenter utan svenskt personnummer kan också få en engångskod skickad till sin e-postadress. Dessa blir alltid AL1.

5.2.6 Förändring av AL nivåer

SU loggar allt händelser rörande AL-nivåer till Syslog. Loggarna är indexerade (sökbara) i 90 dagar och arkiverade arkiverade oindexerat i 13 månader.

Vidare sparas alla aktiveringar i en audit log där man kan se vilken AL-nivå som fås vid varje aktiveringstillfälle. Audit loggen sparas för alltid i databasen.

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 alternativt ber systemet om ett nytt säkert lösenord. 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 (5.2.5). Identifiering görs med hjälp av förregistrerade identifierare som finns beskrivna i 5.2.5.

(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.

Användaren själv, en IdM/SUKAT-administratör eller prefekt motsvarande kan begära ett konto låst. Kontot behöver begäras upplåst av samma personer samt att en lösenordsåterställning enligt 5.2.5 behöver göras.

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 tills problemet är åtgärdat därefter måste kontoinnehavaren göra lösenordsåterställning enligt 5.2.5. Identifiering görs med hjälp av förregistrerade identifierare som finns beskrivna i 5.2.5.

Om det avser disciplinärenden: Kontot är låst så länge disciplinärendet pågår därefter måste kontoinnehavaren göra lösenordsåterställning enligt 5.2.5. Identifiering görs med hjälp av förregistrerade identifierare som finns beskrivna i 5.2.5.

Om lösenord är på drift: Kontoinnehavaren måste göra lösenordsåterställning enligt 5.2.5. Identifiering görs med hjälp av förregistrerade identifierare som finns beskrivna i 5.2.5.

5.4.3 Process för säkerhetsincidenter

Stockholms universitet arbetar efter en etablerad process för säkerhetsincidenter, baserad på MSB/CERT-SE:s incidenthanteringsprocess (CIHSP). Denna process innehåller erfarenhetensåterföring, används vid allvarliga incidenter och säkerställer att SU i framtiden förebygger motsvarande typer av incidenter.

5.5 Credential Status Management

5.5.1 Historik över utfärdade identiteter

SU loggar alla händelser rörande lösenordsförändringar till Syslog, dock inte själva lösenordet. Loggarna är indexerade (sökbara) i 90 dagar och arkiverade oindexerat i 13 månader.

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.

Dokumentrevision

2024-08-07 Ny dokumentrevision 1.14 förtydligande kring studenter och tillitsnivåer

2024-06-26 Ny dokumentrevision 1.13 identifieringsmetod svensk e-legitimation tillagd

2021-05-24 Ny dokumentrevision 1.11 efter återkoppling från SWAMID

2021-05-24 Ny dokumentrevision 1.10 efter återkoppling från SWAMID

2021-05-21 Ny dokumentrevision 1.9 efter återkoppling från SWAMID

2021-05-18 Ny dokumentrevision 1.8 efter återkoppling från SWAMID

2021-04-xx Ny dokumentrevision 1.7 efter återkoppling från SWAMID

2021-04-16 Ny dokumentrevision 1.6 efter återkoppling från SWAMID

2020-09-16 Ny dokumentrevision 1.5

2020-09-16 Uppdatering kring lösenordspolicy 5.1.1

2020-09-16 Uppdatering kring tillitsnivåer 5.2.x

2019-12-17 Ny dokumentrevision 1.4

2019-12-17 Avsnitt 4.1.3 Rutiner för destruering av lagringsmedia, ny referens till instruktioner