SWAMID Identity Management Practice Statement Template

1. Inledning

Luleå tekniska universitet (LTU) förnyar medlemskap i SWAMID och kommer att efterleva deras policyer. Förutom SWAMID Federation Policy finns ett antal tillitsprofiler: LTU 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 LTUs 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

LTU har en katalogtjänst/användardatabas via vilken användare till de gemensamma systemen autentiserar sig. Tjänsten utgörs av en Lightweight Directory Access Protocol (LDAP)- katalog på katalogtjänstmiljön 389 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.

3. Compliance and Audit

Revision av rutiner angivna i detta dokument, sker senast inom 12 månader från senaste revisionstidpunkt och ingår i tjänstekartan under förvaltningsplanen för objektet plattform inom gemensamma tekniska plattformar. Vid förändringar i hanteringsprocesser eller teknik granskas dokumentet av identitentshanteringsteamet och en uppdaterad IMPS skickas till SWAMID för godkännande.

4. Organisational Requirement

The purpose of this section is to define conditions and guidance regarding participating organizations responsibilities.

4.1 Enterprise and Service Maturity

4.1.1 Lärosätets/myndighetens/stiftelsens organisationsnummer

LTU har organisationsnummer 202100-2841och 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 efter aktuella föreskrifter för informationssäkerhet enligt Myndigheten för samhällsskydd och beredskap.

4.1.3 Rutiner för destruering av lagringsmedia

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

4.2 Notices and User Information

4.2.1 Användarvillkor

Användarvillkor finns på verktygen Mitt LTU för studenter och anställda hittar den i ITS-admin där användaren uppdaterar sitt konto och kontouppgifter.

4.2.2 Godkännande

Anställda godkänner användarvillkoren i samband med att de hämtar ut sitt konto. Studenter godkänner användarvillkoren elektroniskt i samband då de hämtar ut sin användare.

4.2.3 Ny ansvarsförbindelse

Vid förändring av användarvillkoren kommer vid nästa inloggning via CAS visas en uppdaterad användarvillkorssida där användaren kan välja att acceptera / neka användarvillkoren

Accepterad och godkänt användarvillkor sparas i användarens profil och kan läsas och ses av användaren själv i användarportalen (ITS-admin)

Ej godkänt användarvillkor gör att användaren inte kommer vidare och tillåts ej använda LTUs tjänster (inaktiverad).

4.2.4 Loggning av ansvarsförbindelsen

Ansvarsförbindelser loggas i kontoinnehavarens profil och kan kontrolleras och läsas av användaren i användarportalen. (ITS-admin)

4.2.5 Service definition

Service definition/tjänstebeskrivning finns publicerad på LTU webb.

Privacy policy finns publicerad på LTU webb privacy policy.

Länk till Policy för hantering av personuppgifter inom ramen för identitetsutgivaren (Identity Provider, IdP):

https://www.ltu.se/ltu/it-support/IT-support-personal/Anvandarnamn-och-losenord/Policy-for-hantering-av-personuppgifter-inom-ramen-for-identitetsutgivaren-Identity-Provider-IdP-1.218207

Länk till generell beskrivning av SAML2 WebSSO:

https://www.ltu.se/ltu/it-support/IT-support-personal/Anvandarnamn-och-losenord/Generell-beskrivning-av-SAML2-WebSSO-1.218206

4.3 Secure Communications

4.3.1 IT-personal med teknisk åtkomst

IT personal med utökade behörigheter, till exempel teknisk åtkomst till de servrar och datamedia där lösenord lagras ansöks och godkänns av chef.

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 minst 2048 bitar RSA.

4.4 Security-relevant Event (Audit) Records

4.4.1 Loggning av säkerhetsrelaterade händelser

Alla IT-relaterade händelser registreras och loggas i ett centralt loggsystem. Loggsystemet sköts av begränsat antal behöriga administratörer som arbetar med

IT-relaterade säkerhetsincidenter. Systemets loggar är säkrat för riktighet och skydd mot förvanskning.

5. Operational Requirements

5.1 Credential Operating Environment

5.1.1 Lösenord

Lösenordet får inte vara samma som ditt Eduroam-lösenord.

Lösenordet måste bestå av minst 12 tecken och innehålla minst en versal, minst en gemen och antingen minst ett specialtecken eller en siffra.

Följande tecken är godkända:

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

Följande tecken är godkända men bör undvikas:

* ? \ / och mellanslag.

5.1.2 Tekniska protokoll

All kommunikation mellan de olika delarna som används för hantering av användare och lösenord sker krypterat enligt SWAMID föreskrifter och rekommendationer.

Det gäller service providers och identity providers.

Replikeringen mellan domänkontrollanter i Active Directory sker enligt Microsofts standardiserade säkerhetsmetod för replikering.

5.1.3 Skydd mot missbruk

Rutin för skydd mot missbruk finns genom Regler för användning av Luleå tekniska universitets IT-resurser - Dnr LTU-644-2018.

I LTUs 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.

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 ltu.se används alltid vid attributrelease till det system där användare vill logga in. Detta oberoende om det är SAML2 eller Eduroam.

5.2.2 Identitetsutfärdarens globalt unika identifierare

Samtliga identitetsservrar vid LTU använder unika identifierare. ltu.se

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

När en användare har fler än ett användarkonto kan de välja vilket konto de använder vid inloggning. Vid LTU finns studentkonton och anställdkonton.

5.2.5 Identifieringsmetoder

Alla användare uppfyller minst SWAMID tillitsnivå AL1. Nivån sätts utifrån aktiveringsmetod och kontotyp. Det är enbart personalkonton som kan ges SWAMID AL2 vid utfärdande, studentkonton ger oavsett identifieringsmetod SWAMID AL1.

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

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.

För legitimationer som saknar personnummer kontrolleras namn och födelsedata mot data som finns i Ladok och/eller LTUs katalog då personnummer inte finns att tillgå. Samt även nationalitet och passets utfärdandeland.

Student

Antagna studenter går till en webbsida där de identifierar sig via eduID, antagning.se.

Metod	Ger Tillitsnivå	Förregistrerad identifierare
Antagning.se	SWAMID AL1	Personnummer/Samordningsnummer (ev. LADOKUUID)
EduID	SWAMID AL1	Personnummer/Samordningsnummer

Utbytesstudenter

Studieadministratörer hanterar utbytesstudenter för respektive institution via MoveOn där studenten gör sin ansökan. Studieadministratörerna hanterar antagna utbytesstudenter genom kontakt till servicepoint som skapar användaridentiteter och de vidareförmedlas sedan till respektive utbytesstudent personligen av studieadministratören. Därefter går studenterna till webbsidan för ny student och aktiverar kontot enligt tidigare beskrivning.

Metod	Ger Tillitsnivå	Förregistrerad identifierare
Servicepoint	SWAMID AL1	Namn, födelsedata, utfärdat pass / nationellt identitetskort

Personal

När en anställd börjar arbeta vid LTU beställer chef vid respektive organisation ett användarkonto via ett formulär till LTUs ärendehanteringssystem. När handläggare vid katalogadministrationen tar emot begäran skapas ett användarkonto för den nyanställde. Användaren går till ServicePoint och identifierar sig med legitimation, godkänner ansvarsförbindelsen och kvitterar ut sina användaruppgifter.

Metod	Ger Tillitsnivå	Förregistrerad identifierare
Servicepoint	SWAMID AL2/AL1	Personnummer (Legitimation krävs)

5.2.6 Förändring av AL nivåer

LTU loggar alla händelser rörande AL-nivåer till Greylog. Loggarna är sökbara i 6 månader.

5.2.7 Ändring av självuppgiven information

All självuppgiven information kan ändras av kontoinnehavaren.

5.2.8 Krav på identitetsgranskningen

Vid LTU 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.

Länk personal https://itsadmin.ltu.se/

Länk student https://www.ltu.se/mittltu

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 liknande sätt som utdelning vid kontoaktivering (5.2.5). Identifiering görs med hjälp av förregistrerade identifierare som finns beskrivna i 5.2.5.

Student

Metod	Ger Tillitsnivå	Förregistrerad identifierare
Antagning.se	SWAMID AL1	Personnummer/Samordningsnummer (ev. LADOKUUID)
EduID	SWAMID AL1	Personnummer/Samordningsnummer
Servicepoint	SWAMID AL1	Personnummer (Legitimation krävs)

Anställd

Metod	Ger Tillitsnivå	Förregistrerad identifierare
Engångskod	SWAMID AL1	Användarkonto med förregistrerat telefonnummer
Servicepoint	SWAMID AL2	Personnummer (Legitimation krävs)

5.4 Credential Revocation

5.4.1 Inaktivering av användarkonton

Samtliga konton kan deaktiveras av IT-administratör. När en anställd avslutar sin anställning vid LTU beställer chef avstängning av kontot. Studenter får vid deaktivering ny affiliation som Alumn och kontot behålls.

Användare kan begära deaktivering av sitt konto, detta görs i kontakt med servicepoint.

5.4.2 Återaktivering av användarkonton

Anställda som återanställs innan kontot gallrats blir aktiverade på nytt. Om två år har passerat sedan senaste lösenordbyte krävs nytt lösenord enligt 5.2.5.

Vid spärrat konto på grund av säkerhetsincident eller att lösenordet röjts förblir kontot låst tills åtgärd vidtages. Vid spärrande av konto kontaktas alltid användaren om orsaken och vad som krävs för att återaktivera kontot. Därefter kan användaren skapa nytt lösenord enligt 5.2.5.

Studenter som återupptar studier innan kontot gallrats får kontot återaktiverat.

Om det avser disciplinärenden: Kontot är låst så länge disciplinärendet pågår.

5.4.3 Process för säkerhetsincidenter

LTU 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 LTU i framtiden förebygger motsvarande typer av incidenter.

5.5 Credential Status Management

5.5.1 Historik över utfärdade identiteter

LTU loggar alla händelser rörande lösenordsförändringar till Greylog, dock inte själva lösenordet. Loggarna är indexerade (sökbara) i 30 dagar. Datum för senaste lösenordsbyte lagras i användarens profil.

LTU har en separat databas där samtliga historiska användarnamn lagras i syfte att jämföra med nyskapade av konton för att hindra återanvändande av tidigare använt användarnamn.

5.5.2 Tillgängligheten för identitetstjänsten

Inloggningsservern för SAML2 och inloggningsservern för Eduroam har en tillgänglighet lika med eller högre än de krav som satts på inloggningservrar för LTUs interna system.

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

Inaktiva användare är deaktiverade i autentiseringstjänsterna och kan därmed ej nyttjas för inloggning. Undantaget är alumnsida för inaktiva studenter.

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 LTU 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 LTU kraven med att den maximala längden för SSOsessionen är nio timmar. Den maximala giltighetstiden från att användaren gör inloggningen, eller använder SSO-sessionen, tills att tjänsten släpper in användaren i tjänsten är fem minuter.