Sveriges lantbruksuniversitet
Swedish University of Agricultural Sciences

IT-avdelningen

SLU IMPS

SLU ID: SLU.ua.2022.1.1.1-4039

V1.8 2023-06-16

Sveriges lantbruksuniversitet
Identity Management Practice Statement

1. Inledning 2

4. Organisational Requirement 2
4.1 Enterprise and Service Maturity 2
4.2 Notices and User Information 3
4.3 Secure Communications 3
4.4 Security-relevant Event (Audit) Records 4

5. Operational Requirements 5
5.1 Credential Operating Environment 5
5.2 Credential Issuing 5
5.3 Credential Renewal and Re-issuing 8
5.4 Credential Revocation 9
5.5 Credential Status Management 10
5.6 Credential Validation/Authentication 10

1. Inledning

Sveriges Lantbruksuniversitet (SLU) är en mångårig medlem i SWAMID och nyttjar ett flertal tjänster via SUNET. Detta dokument specificerar hur SLU uppfyller kraven för tillitsnivå AL1 och AL2.

4. Organisational Requirement

4.1 Enterprise and Service Maturity

4.1.1

Sveriges Lantbruksuniversitet, organisationsnummer 202100-2817, är en statlig utbildningsmyndighet vilket gör att lärosätets verksamhet regleras i lagar, förordningar och regleringsbrev.

4.1.2

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

Lärosätets katalog- och behörighetssystem Idis 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. Dataskyddslagen (SFS 2018:218), förordning med kompletterande bestämmelser till EU:s dataskyddsförordning (SFS 2018:219) samt offentlighets- och sekretesslagen (SFS 2009:400) reglerar behandlingen av personuppgifter samt hantering av personer med behov av skyddade personuppgifter.

Studenters personuppgifter hämtas ur lärosätets studiedokumentations-system 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 Idis.

Som statlig myndighet arbetar lärosätet även med ledningssystem för informationssäkerhet enligt Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet.

4.1.3

Backuprutiner och rutiner för hantering av media som innehållit känslig information finns i IT-avdelningens kvalitetshandbok:

- DRI DI RL 001 Informationssäkringsrutiner för datalagring
- DRI DI M 006 Hantering av media som hållit känslig data

4.2 Notices and User Information

4.2.1

Aktuellt användarkontrakt finns publicerat på https://internt.slu.se/stod-service/admin-stod/it/IT-support/mera-support/anvandarkontrakt/

4.2.2

Alla användare måste acceptera användarvillkoren vid uthämtning av konto eller nytt lösenord.

4.2.3

Notifieringar om förändringar i användarvillkor meddelas via epostmeddelande. Användaren anses godkänna förändringarna om ingen vidare åtgärd tas.

4.2.4

Användarens acceptans av användarvillkoren finns lagrat i digital eller fysisk form.

4.2.5

Tjänstebeskrivning finns publicerat på adressen https://internt.slu.se/stod-service/admin-stod/it/IT-support/datornatverk/externa-natverk/

4.3 Secure Communications

4.3.1

Alla administrativa konton hanteras enligt samma livscykelhantering som övriga konton. Delade konton och säkerheter lagras i en dedikerad lösenordsserver.

SLU Identity Providers har egna servrar med begränsad tillgång där endast adminkonton eller servicekonton som specifikt ska arbeta med servern har tillgång.

4.3.2

Delade konton och säkerheter lagras i en dedikerad lösenordsserver.

SLU Shibboleth IdPs interna certifikat och känsliga uppgifter ligger i en mapp som är begränsad till systemet och idp-administratörer.

Aktiveringskoder för användarkonton sparas i en databas och är saltade och hashade. Salt sparas separat i konfigurationsfiler på applikationsservern och är skyddade av operativsystemet.

4.3.3

Nätverkskommunikation är signerad, säker och krypterad.

4.3.4

De interna saml-certifikaten, signing och encryption, är 3072-bit RSA och nästa gång de förnyas planeras de att vara 4096-bit.

4.4 Security-relevant Event (Audit) Records

Alla inblandade servrar loggar relevanta säkerhetshändelser till en central logserver som är skyddad från obehörig åtkomst. NTP servrar används för att få en tillförlitlig tid över hela universitetets IT-miljö.

4.4.1
Identity Providerns loggar packas ner och sparas lokalt på servern och i serverns backup. Endast åtkomligt för de adminkonton som har access till idpn.

5. Operational Requirements

5.1 Credential Operating Environment

5.1.1

SLU GPO som sätter gränserna för lösenord kräver i dagsläget minst 8 karaktärer. Dessutom används ADs kravkomplexa lösenord. Regler för användande och påföljder samt rekommendation för hur lösenord ska utformas finns i det användaravtal som varje ny användare godkänner, se https://internt.slu.se/stod-service/admin-stod/it/IT-support/mera-support/anvandarkontrakt/

5.1.2

Shibboleth IdP är installerad enligt rekommendationer och använder sig -av TLS som skydd mot message replay.

5.1.3

Avtalet förbjuder uttryckligen överlåtande av nyttjandet till annan part samt skyldigheten att rapportera inträffade eller misstänkta säkerhetsincidenter till IT-avdelningen. I det sistnämnda räknas förlust av inloggningsuppgifter in.

5.1.4
Endast specifika personer kommer åt servrarna med adminkonton som är till för identitetshantering och då med skilda adminkonton för produktion, test och utveckling. Admin-kontona kräver lösenordsbyten var 6:e månad. När ett adminkonto inte längre ska vara aktivt stängs det av enligt rutiner.

Servrarna som används för identitetshantering används inte för annat än det syftet. De skyddas bakom brandvägg, har endast nödvändiga portar öppna och om möjligt ligger de på privat nät. Servrarnas operativsystem patchas löpande.

5.2 Credential Issuing

5.2.1

SLUs identity provider använder SLUs ägda domän som scope (slu.se). Exempel på attribut med scope är eduPersonPrincipalName och eduPersonScopedAffiliation.

5.2.2

SLUs IDP:er har globalt unika identifierare då de använder sig av SLUs domän (slu.se) som del av entitetsid.
Eduroam radius server DNS name inkluderar SLUs domän.

5.2.3

Den globala unika identifieraren mot swamid är eppn. Eppn byggs upp av användarnamn och slu:s scope. När ett nytt konto skapas så kontrolleras användarnamnet mot SLU AD och mot identitetshanteringens historikdatabas att användarnamnet inte använts för tidigare konto. Därmed återanvänds aldrig ett eppn.

Ändringar av självuppgiven information görs via katalogansvarig (anställd, verksam) eller Ladok (student).

5.2.4

Användaren kan själv välja användarkonto för inloggningen.

5.2.5

Det finns tre typer av konton på SLU som får en AL-nivå

Anställda
Användarkonton skapas automatiskt för anställda genom integrationer med SLU:s personal- och lönesystem Primula som även är källan till personuppgifter. Telefonnummer, mobilnummer eller alternativ e-post kan uppdateras av katalogansvarig för den anställdes organisationsenhet.

Verksamma
Personer som är verksamma inom SLU utan att vara anställda (t.ex. inhyrd personal, konsulter eller ideell) erhåller konton genom att katalogansvariga lägger till konton på uppdrag av prefekt vid aktuell institution alternativt chef för organisatorisk enhet.

Studenter
För studenter skapas användarkonton genom integration med Ladok som är källan till all personinformation på studenter.

Förutom ovan nämnda konton finns det även andra typer av konton men dessa används inte vid inloggning via idp och får dessutom ingen AL-nivå.

För att få åtkomst till ett användarkonto av en typ som ger AL-nivå så måste användaren hämta ut sitt konto genom en godkänd metod för identifiering.

Videoutlämning

Ett konto kan lämnas ut över video där användaren visar upp en giltig legitimation där servicedesk kontrollerar att namn, ålder, land och foto stämmer med det förskapade kontot på SLU. Användaren får då ut en tidsbegränsad aktiveringsnyckel och kontot markeras som videoutlämning vilket ger AL1.

Fysiskt besök på servicecenter

Anställda, verksamma och studenter kan hämta ut konto genom att besöka ett av SLU:s servicecenter. Användaren legitimerar sig och servicecenter verifierar att legitimationen är giltig och överensstämmer med de uppgifter som är registrerat på användarkontot. Servicecenter anger samtidigt att verifieringen av användarens legitimation är gjord vid ett fysiskt besök på ett av SLU:s servicecenter, vilket innebär att kontot markeras för AL2. Efter kontroll överlämnas ett dokument med en tidsbegränsad aktiveringsnyckel ut.

Användaren använder sedan aktiveringsnyckeln i kombination med personnummer för att logga in på SLU:s IdPortal för att aktivera, godkänna användarvillkor samt sätta ett lösenord för kontot.

Alla aktiveringsnycklar som lämnas ut är tidsbegränsade, och används i kombination med personnummer som ej finns med i samma dokumentation som den utlämnade aktiveringskoden.

Följande typer av legitimationer accepteras vid videutlämning eller fysiskt besök:

- Godkänd svensk ID-handling (SIS-märkt ID-kort, SIS-märkt tjänstekort, SIS-märkt företagskort, körkort)
- Svenskt nationellt ID-kort eller pass.
- Nationellt ID-kort eller pass utgivet av medlem i EU/EES
- Annat utländskt pass där ICAO doc 9303 är uppfyllt.

Personer utan svenskt personnummer använder sig av interimspersonnummer från Ladok eller samordningsnummer från Skatteverket. SLU har inga konton utan någon form av identifikationsnummer.

Uthämtning av konto genom digital identitetsväxling

Användarkonton kan också hämtas ut genom att genomföra en s.k. identitetsväxling i SLU:s IdPortal. Detta sker genom att användaren väljer att aktivera sitt konto genom en av flera identityproviders (se nedan).

- Antagning.se – Personnummer från antagning.se matchas med konto hos SLU. Beroende på ifall kontot hos antagning.se har AL2 status eller ej markeras kontot i vårat system med motsvarande nivå.
- Svensk e-legitimation – Efter autentisering matchas användaren genom personnummer med konto hos SLU. Identifiering med svensk e-legitimation gör att användarkontot markeras med AL2-nivå.
- Eduid – Efter autentisering matchas användaren mot ett konto hos SLU. Finns ett svenskt personnummer används det för matchningen. Om svenskt personnummer saknas görs en riskbaserad matching med förnamn, efternamn och födelsedatum mot motsvarande information på kontot hos SLU.
  Beroende på förtroendenivå hos användaren på eduid sätts korrekt AL-nivå på slu.

När användaren har identifierat sig hos identitetsprovidern presenteras användarvillkoren och denne måste godkänna dessa. Användaren sätter därefter ett nytt lösenord för sitt användarkonto.

Alla id-kontroller av användare loggas i databasen Iddb med information om tidpunkt och hur användaren har identifierat sig. Det i sin tur styr genom ett regelverk vilken AL-nivå en användare tilldelas i Idis.

Som fördefinierade identifierare för att säkerställa att det är samma person vid återställning av inloggningsuppgifter och återaktivering av användarkonto används personnummer, alternativt riskbedömning baserat på namn och födelsedata om svenskt personnummer saknas.

I alla varianter av kontouthämtning krävs det att det finns ett förskapat konto på SLU med någon form av aktiv status, annars nekas utlämningen.

5.2.6

Förändringar av AL-nivå loggas i en IDM-databas.

5.2.7

Användare har möjlighet att uppdatera sin personliga information genom att kontakta kataloganSvarig. Studenter som vill uppdatera sin självuppgivna information gör det via Ladok.

5.2.8

Samtliga kataloganSvariga, identitetsutlämnare och administratörer av kontohanteringen (AD, IdP, IDM) har AL2.

För att vara kataloganSvarig så krävs medlemskap i katalogrollen. Vid rolltilldelning nekas användaren att få rollen om den inte har nog hög nivå av identifiering. Vid händelse att nivån går under kravet så inaktiveras rollinnehavet av systemet.

Verktyget identitetsutlämnare använder sig av blockerar utlämnaren från att lämna ut konton med högre identifikationsnivå än den själv.

5.3 Credential Renewal and Re-issuing

5.3.1

SLU GPO som sätter gränserna för lösenord kräver lösenordsbyte var sjätte månad. Användare har även möjligheten att själv initiera ett byte via sin klient, ID-portal eller webmail.

5.3.2

När lösenordet går ut krävs lösenordsbyte för att komma åt kontot eller det kopplat till kontot. För att byta lösenord krävs det gamla lösenordet.

Den lokala datorn har inte fungerande SSO om inte lösenordet bytes eller det nya lösenordet anges.

Shibboleth har en aktiv session på 8 timmar, men därefter kan man inte logga in på nytt innan man har ett giltigt lösenord.

5.3.3

Om en användare glömt sitt lösenord kan den hämta ut ett lösenord via samma metoder som kontoutlämningen i 5.2.5 med samma krav på identitetshandling.

I undantagsfall kan en tidsbegränsad aktiveringskod för att hämta ut nytt lösenord skickas ut med ett sms. Mobilnummer hämtas från SLU identitetshanteringssystemet där katalogansvarig sen tidigare registrerat användarens mobilnummer. Den här metoden för att få ut nytt lösenord gör att användarkontot markeras med AL1.

Om ett konto blivit automatiskt inaktiverat t.ex. pga. repeterade felaktiga lösenordsinmatningar låses kontot en predefinierad tidsperiod.

5.4 Credential Revocation

5.4.1

AD-förvaltning och servicedesk har möjlighet att omedelbart inaktivera ett användarkonto, antingen pga missbruk eller om direktiv har kommit om omedelbar inaktivering.

En användare kan kontakta servicedesk och begära att deras konto spärras. I samband med det döljs all information om användaren från webben.

En anställd får sitt konto inaktiverat en månad efter slutdatum. En verksam får sitt konto inaktiverat dagen efter slutdatum.
En student är aktiv i sju år efter senaste kursregistrering.

5.4.2

Återaktivering efter en incident sker efter personlig kontakt med användaren och efter åtgärd av incidenten. Inget konto återaktiveras utan att användaren har kontaktats och har genomgått kontoutlämning igen där de identifierat sig enligt reglerna. Användare som varit frånvarande under en tid behöver inte hämta ut kontot på nytt utan det räcker att sätta ett nytt lösenord. Vid glömt lösenord följs rutinerna för uthämtning av nytt lösenord i 5.3.3

5.4.3

I samband med säkerhetsincidenter tillsätts en incidentgrupp som hanterar processen runt incidenten. Beroende på typ av incident genomförs olika åtgärder. Förutom exv. IT-forensiska utredningar ger gruppen förslag på eventuella åtgärder som behöver genomföras för att händelsen inte skall uppstå igen. Det kan tex. vara

återkoppling till drabbad användare eller allmänna förändringar i rutiner eller processer.

SLU arbetar efter ramverket CIS18. Vi siktar på att uppfylla med MSBFS 2020:7.

5.5 Credential Status Management

5.5.1

Vid skapande av ny elektronisk identitet kontrolleras att denna inte har delats ut tidigare. Inaktiva identiteter raderas inte, utan ligger kvar inaktiva för framtida kontroll. Historik över händelser inklusive lösenordbyten finns i Idis databas och loggning från AD.

5.5.2

SLU Shibboleth IdP används för SWAMID men även för flera SLU-specifika system. SLU-IT har övervakning med beredskap och åtgärd på systemet mellan 08 – 22 dagligen.

5.6 Credential Validation/Authentication

5.6.1

SLUs Eduroam, IdP, samt SP för NyA, är installerade enligt instruktioner från SWAMID.

5.6.2

Då dessa arbetar direkt mot SLUs AD finns ingen risk att inaktiva konton felaktigt ska bli autentiserade. IdP och SP följer SAML2 enligt SWAMIDs rekommendationer.

5.6.3

Varje gång en användare loggar in behöver de uppge sina inloggningsuppgifter.

5.6.4

Användare behöver förnya sin autentisering var 8:e timme.