DNR UFV 2022/2617

Hur Uppsala universitet uppfyller SWAMID Identity Assurance Level 2 Profile

Identity Management Practice Statement

Version 2023.0
Fastställd av Per-Olof Andersson

Innehållsförteckning

1 Terminologi 3

2 Purpose, Scope and Summary 3

3 Compliance and Audit 3

4 Organisational Requirement 3

4.1 Enterprise and Service Maturity 3

4.2 Notices and User Information 4

4.3 Secure Communications 4

4.4 Security-relevant Event (Audit) Records 5

5 Operational Requirements 5

5.1 Credential Operating Environment 5

5.2 Credential Issuing 6

5.3 Credential Renewal and Re-issuing 7

5.4 Credential Revocation 8

5.5 Credential Status Management 8

5.6 Credential Validation/Authentication 9

1 Terminologi

Placeholder för att matcha SWAMIDs form för AL2.

2 Purpose, Scope and Summary

Uppsala universitet är medlem i identitetsfederationen SWAMID[1] och som medlem måste universitetet uppfylla SWAMIDs regelverk för att användarna på Uppsala universitet ska kunna använda tjänster som är anslutna till federationen. Exempel på tjänster som är anslutna till identitetsfederationen är SUNETs e-mötestjänst Sunet ZOOM, antagningssystemet Antagning.se och dess administrativa gränssnitt, forskningsansöknings- och ärendehanteringssystemet Prisma, Ladok och det trådlösa nätverket eduroam.

Detta dokument beskriver hur Uppsala universitet genom katalog- och behörighetssystemet AKKA med närliggande system uppfyller SWAMID AL1 och AL2. Denna typ av beskrivning heter på engelska Identity Management Practice Statement (IMPS).

3 Compliance and Audit

I SWAMID AL2 granskar SWAMID Operations, eller av SWAMID Board of Trusteees utsedd tredje part, att Uppsala universitet uppfyller kraven. Universitetet skickar in denna IMPS tillsammans med de dokument som refereras till för granskning. När Uppsala universitet har blivit godkända för SWAMID AL2 ska universitetet årligen verifiera till SWAMID Operations att innehållet i denna IMPS fortfarande beskriver universitetets rutiner. Ändrar universitetet rutinerna och säkerhetsarrangemangen runt kontohanteringen uppdateras IMPS och underliggande dokument inför ny granskning av SWAMID.

4 Organisational Requirement

4.1 Enterprise and Service Maturity

Uppsala universitet, organisationsnummer 202100-2932, är en statlig utbildningsmyndighet vilket gör att universitetets verksamhet regleras i lagar, förordningar och regleringsbrev. 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 universitetets uppdrag under ett kalenderår. I övrigt följer universitetet Sveriges övriga lagar och förordningar.

Uppsala universitetets katalog- och behörighetssystem AKKA innehåller uppgifter om universitetets organisation samt personuppgifter om alla som är verksamma vid universitetet. Med avseende på detta måste särskild hänsyn till behandling av personuppgifter tas. Gällande personuppgiftslagstiftning och offentlighets- och sekretesslagen (SFS 2009:400) reglerar behandlingen av personuppgifter samt hantering av personer med behov av skyddade

[1] http://www.swamid.se

personuppgifter. AKKA följer Skatteverkets vägledning för hantering av sekretessmarkerade personuppgifter i offentlig förvaltning[2].

Studenters personuppgifter hämtas ur universitetets studiedokumentationssystem Ladok.

Som statlig myndighet arbetar universitetet även löpande med ledningssystem för informationssäkerhet enligt aktuella föreskrifter från MSB.

SWAMID 4.1.3

Personuppgifter och andra känsliga uppgifter finns lagrade på hårddiskar och backupband. Vid avveckling av servrar och backupband följs Riktlinjer för informationssäkerhet - hantering av utrangerad IT-utrustning (UFV 2014/1279)[3].

4.2 Notices and User Information

SWAMID 4.2.1

Uppsala universitet har användarregler för samtliga användare vid universitetet beskrivna i dokumentet Allmänna regler för användning av användarkonton och datornät (UFV 2013/1502)[4].

SWAMID 4.2.2, 4.2.3 och 4.2.4

I avsnitt 3.1 och 3.5 i Användarkonton i AKKA vid Uppsala universitet (version 3.5)[5] beskrivs hur användarna godkänner regler vid kontoaktivering, vid förändrade regler och med ett 24-månadersintervall. Alla godkännanden registreras och sparas i AKKA för framtida referens.

SWAMID 4.2.5

En användaranpassad tjänstebeskrivning finns publicerad på adressen https://weblogin.uu.se.

4.3 Secure Communications

SWAMID 4.3.1 och 4.3.2

De tjänster som ingår i AKKA, Gemensam webbinloggning (Shibboleth IdP) och eduroam driftas på dedikerade servrar som endast ett fåtal definierade i driftpersonalen har åtkomst till. Åtkomsten till privata nycklar och delade hemligheter är begränsat till endast systemets administrativa användare och resp. applikation. Detta gäller även i de fall då privata nycklar i klartext och delade hemligheter förekommer.

SWAMID 4.3.3 och 4.3.4

All nätverkskommunikation mellan de olika systemen som ingår i AKKA, Gemensam webbinloggning (Shibboleth IdP), Active Directory och eduroam är skyddad och krypterad. TLSv1.2 eller högre används för kommunikation. Ett undantag är den skyddade LDAP-tjänsten som även tillåter SSLv3, beroende på att visa tjänster inte kan använda TLSv1.2, men där de tillåtna krypteringsalgoritmerna har begränsats och åtkomsten till tjänsten är begränsad till reglerade IP-adresser på icke publika nät. Alla privata nycklarna är minst 2048 bitar. För Gemensam

[2] https://www.skatteverket.se/foretagochorganisationer/myndigheter/informationsutbytemellanmyndigheter/folkbokforingsekretessmarkeradepersonuppgifter.4.18e1b10334ebe8bc80002541.html

[3] https://regler.uu.se/dokument/?contentId=752674

[4] https://regler.uu.se/dokument/?contentId=283312

[5] Bifogas till detta dokument.

webbinloggning (Shibboleth IdP) används 4096-bitarsnycklar. Synkroniseringen av kontouppgifter till Active Directory sker genom TLS-baserad LDAP och replikeringen mellan domänkontrollanter sker enligt Microsofts standardiserade säkerhetsmetod för replikering. Uppsala universitet synkroniserar inte lösenord med externa leverantörer, t.ex. molntjänster.

4.4 Security-relevant Event (Audit) Records

Alla förändringar som genomförs i AKKA på en användare loggas och sparas. Det som loggas är vem som ändrades, vad som ändrades, vem som gjorde ändringen och när ändringen genomfördes. Denna logg över händelser i AKKA är skyddad mot förändringar samt rensas inte utan händelserna sparas under lång tid. Loggen säkerhetskopieras tillsammans med övrig data från AKKA.

Inloggningar och andra relevanta säkerhetshändelser i AKKAs LDAP-miljö, Gemensam webbinloggning (Shibboleth IdP och CAS), Active Directory och radius sparas och säkerhetskopieras i respektive system samt skickas till gemensam logguppsamling vid universitetet. I loggarna sparas logghändelse, vem som utförde händelsen, varifrån händelsen utfördes och när händelsen utfördes.

5 Operational Requirements

5.1 Credential Operating Environment

SWAMID AL2 5.1.1

Universitetets kontohantering följer Riktlinjer för informationssäkerhet vid Uppsala universitet – Lösenordshantering (UFV 2013/1490)[6] när det gäller hur lösenord ska se ut, användas och bytas. Dessa riktlinjer kräver att lösenordet är minst 10 tecken och består av små och stora bokstäver ur det engelska alfabetet samt siffror eller specialtecken. Detta ger en entropi på minst 27 bitar enligt NIST SP 800-63-2 bilaga A. Eduroam använder inte samma lösenord som övriga inloggningar vid universitet.

Multifaktorautentisering av användare sker alltid genom att inloggningen med användarnamn och lösenord kompletteras med något av dessa alternativ:

- En kryptografisk enhet med enkelfaktor (NIST 800-63B avsnitt 5.1.7). Enheten är en U2F-kompatibel nyckel från Yubikey.
- En engångslösenordsenhet med enkelfaktor (NIST 800-63B avsnitt 5.1.4). För detta används algoritmen Time Based One Time Password (TOTP), RFC 6238 och en enhet som är kompatibel med detta, t ex app i mobiltelefon eller särskild säkerhetsdosa.

Den kompletterande enkelfaktorn är oberoende av lösenordet. En användare som har en kompletterande faktor registrerad måste autentisera sig med multifaktor (dvs både lösenord och kompletterande faktor) för att kunna ändra lösenord eller byta kompletterande faktor. Alternativt autentisera sig på annat sätt som uppfyller motsvarande krav, dvs med svensk e-legitimation på tillitsnivå 3 eller med engångskod som användaren fått vid en reception efter att genomfört en fullständig identitetskontroll enligt avsnitt 3.1 i Användarkonton i AKKA vid Uppsala universitet (version 3.5).

SWAMID AL2 5.1.2

[6] https://regler.uu.se/dokument/?contentId=732302

All kommunikation mellan de olika delarna som används för hantering av användare och lösenord sker krypterat såsom beskrivet under rubriken SWAMID AL2 4.3.3 & 4.3.4. TLS och SSLv3 har inbyggda skydd mot återspelningsattacker (en. message replay).

SWAMID AL2 5.1.3

I användarreglerna som nämns under 4.2 finns det en tydlig regel om att användarkonton, lösenord och koder är personliga och endast får användas av innehavaren. Eftersom användarna måste godkänna reglerna när de aktiverar sitt konto samt därefter godkänna dem när de ändras, anses det att universitetet aktivt avråder användarna från att dela med sig av sina lösenord.

Användarreglerna är under uppdatering. Satsen “att användarkonton, lösenord och koder är personliga och får endast användas av innehavaren” ändras till “att användarkonton, lösenord, koder och inloggningsenheter är personliga och får endast användas av innehavaren”.

När användare får en andra faktor kopplad till sitt konto upplyses användaren om att inte dela faktorn med någon annan person. Se avsnitt 3.8 och 3.9 i Användarkonton i AKKA vid Uppsala universitet (version 3.5).

SWAMID AL2 5.1.4

Alla servrar som används för AKKA, Gemensam webbinloggning och eduroam är uppsatta och konfigurerade så att de endast är tillgängliga på avsedda tjänsteprotokoll såsom LDAPS, HTTPS osv. för reglerade IP-adresser. Vid avdelningen för universitetsgemensam IT finns förutom de enskilda driftteamens ansvar för att hålla servrar uppdaterade med avseende på säkerhetsproblem även en särskild krisorganisation som aktiveras då större säkerhetsproblem uppträder.

5.2 Credential Issuing

SWAMID AL2 5.2.1

Vid attributrelease till det system där användare vill logga in används alltid den administrativa domänen user.uu.se. Detta oberoende om det är SAML2 eller eduroam.

SWAMID AL2 5.2.2

SAML2-baserad inloggning för Uppsala universitet använder alltid den unika identifieraren https://weblogin.uu.se/idp/shibboleth. Denna identifierare används endast för den klustrade inloggningstjänsten och ingen annan tjänst.

Eduroambaserad inloggning använder alltid radiusservern radiusauth.uu.se för inloggning mot Uppsala universitet.

SWAMID AL2 5.2.3

Användaridentiteter används bara för en enda person och kan inte återanvändas för någon annan person. Detta beskrivs i avsnitt 3.7 Användarkonton i AKKA vid Uppsala universitet (version 3.5).

SWAMID AL2 5.2.4

Om en användare har mer än ett användarkonto, dvs. är både student och anställd eftersom det är två olika användarkonton enligt avsnitt 2 enligt Användarkonton i AKKA vid Uppsala universitet (version 3.3), väljer användaren vid inloggning vilket användarkonto denna ska använda vid det aktuella tillfället.

SWAMID AL2 5.2.5

I avsnitt 3.1 och 3.2 i Användarkonton i AKKA vid Uppsala universitet (version 3.5) beskrivs hur en användare aktiverar sitt användarkonto och de begränsningar som gäller. I avsnitt 2 i samma

dokument beskrivs vilka konton som ska uppnå bekräftad användare dvs. SWAMID AL2, respektive obekräftad användare dvs. SWAMID AL1.

Avsnit 3.1 i dokumentet beskrivs de proofing- och aktiveringsmetoder som används för att uppnå bekräftad användare. De är:

- Inloggning med en giltig Svensk E-legitimation med tillitsnivå 3 eller högre.
- Inloggning med Antagning.se eller eduID.se konto och denna inloggning har SWAMID tillitsnivå 2 eller högre.
- Engångskod som användaren fått vid en reception efter att genomfört en fullständig identitetskontroll
- Engångskod som användaren fått skickat till sin folkbokföringsadress.

Med övriga proofing- och aktiveringsmetoder, som samtliga inbegriper engångskodsutlämning, uppnås obekräftad användare. Närmare beskrivning av de alternativ som finns för detta finns i avsnitt 3.2 i dokumentet.

Engångskoder är tidsbegränsade. Vid utlämning i reception gäller de i fyra timmar och vid utlämning till folkbokföringsadress gäller de i fyra veckor.

För AL2-konton används som förregistrerad identifierare används personnummer när det finns. Saknas personnummer används istället identitetshandlingens idnummer i kombination med utfärdandeland eller kombinationen födelsedatum, förnamn, efternamn och identitetshandlingens utfärdandeland. Se avsnitt 3.2 i dokumentet.

För AL1-konton används personnummer, förnamn och efternamn som förregistrerade identifierare. Om personnummer saknas används istället födelsedatum. Se avsnitt 3.2 i dokumentet.

SWAMID AL2 5.2.6

Ett användarkonto i AKKA kan bara ha en tillitsnivå. Tillitsnivå kan höjas men aldrig sänkas. Om tillitsnivån inte kan upprätthållas blir kontot otillgängligt för användaren tills nivån är upprättad igen. Samtliga förändringar av tillitsnivå sparas i logg.

SWAMID AL2 5.2.7

Alla som har användarkonton kan själva uppdatera de uppgifter de själva angav i samband med användarkontot aktiverades i AKKA via självservicegränssnitt. Övriga uppgifter hanteras av de lokala katalogadministratörerna för anställda och övriga verksamma, självservice och personaladministratör i Primula för anställda och självservice och studiedokumentationsadministratörer i Ladok för studenter.

SWAMID AL2 5.2.8

All personal vid universitetet som arbetar med katalog- och kontohantering i AKKA och övriga system som bär kontoinformation är validerade på tillitsnivå SWAMID AL2 eller högre. Vidare är de externa system som används för att genomföra kontoaktivering och lösenordsåterställning motsvarande tillitsnivå SWAMID AL2, dvs. eduID och Antagning.se. AKKA och övriga system som används för kontaktivering är uppsatta så att endast behöriga användare kan administrera systemen.

5.3 Credential Renewal and Re-issuing

SWAMID AL2 5.3.1 och 5.3.2

Alla användare kan byta sina två olika lösenord via AKKAs olika självservicegränssnitt. För att byta lösenord måste först användaren ange sitt nuvarande lösenord och sedan två gånger sitt nya. Vid

bytet av lösenord följs Riktlinjer för informationssäkerhet vid Uppsala universitet – Lösenordshantering (UFV 2013/1490).

I avsnitt 3.6 i Användarkonton i AKKA vid Uppsala universitet (version 3.5) beskrivs hur en användare hanterar sitt lösenord B.

I avsnitt 3.8 i Användarkonton i AKKA vid Uppsala universitet (version 3.5) beskrivs hur användaren byter personverifierad andra faktor.

I avsnitt 3.9 i Användarkonton i AKKA vid Uppsala universitet (version 3.5) beskrivs hur användaren byter egenverifierad andra faktor.

SWAMID AL2 5.3.3

I avsnitt 3.3 i Användarkonton i AKKA vid Uppsala universitet (version 3.5) beskrivs hur en användare ska gå tillväga om de har glömt sitt lösenord, dvs. de gör på samma sätt som när de aktiverar sitt användarkonto.

I avsnitt 3.8 i Användarkonton i AKKA vid Uppsala universitet (version 3.5) beskrivs hur en användare ska gå tillväga om de förlorat sin personverifierade andra faktor.

I avsnitt 3.9 i Användarkonton i AKKA vid Uppsala universitet (version 3.5) beskrivs hur en användare ska gå tillväga om de förlorat sin egenverifierade andra faktor.

5.4 Credential Revocation

SWAMID AL2 5.4.1 och 5.4.2

I AKKAs administrativa gränssnitt finns det möjlighet för kontoadministratörer att spärra en användares konto. Spärr kan vara tidsbegränsad eller gälla tills återaktivering beslutas. Innan användare kan logga in i ett återaktiverat konto måste användaren sätta ett nytt lösenord och eventuell andra faktor enligt rutinerna beskrivna i avsnittet SWAMID AL2 5.3.3. Endast rutiner som ger samma tillitsnivå som tidigare eller högre kan användas.

Spärrning kan också ske på kontoinnehavarens begäran.

Vid spärrning av ett konto kan orsak till spärrning anges. Finns orsak angiven så informeras användaren om denna innan kontot återaktiveras. Orsak anges alltid vid säkerhetsrelaterade incidenter. Återaktivering kan inte ske utan att beslut fattats om att häva spärren.

SWAMID AL2 5.4.3

Universitetets incidentprocess säkerställer att åtgärder vidtas efter en incident för att hindra att samma incident inträffar igen. Detta gäller både säkerhetsrelaterade incidenter och icke säkerhetsrelaterade incidenter.

5.5 Credential Status Management

SWAMID AL2 5.5.1

AKKA innehåller en historikfunktion som innehåller statusinformation runt förändringar i användarkonton. Statusinformationen innehåller bl.a. händelser om när användarkontot aktiverades, tidpunkter för lösenordsförändringar, stängdes av och eventuellt återaktiverades.

AKKA sparar alla användarnamn som någonsin använts och kan därför säkerställa att inga användarnamn återanvänds för någon annan individ än det ursprungligen användes för.

SWAMID AL2 5.5.2

Gemensam webbinloggningn(Shibboleth IdP) och bakomliggande LDAP-tjänst är installerade i feltoleranta och lastbalanserade systemuppsättningar med mer än en systemuppsättning per tjänst. Tjänsterna är tillgängliga även vid bortfall av enstaka systemuppsättningar och uppfyller universitetets tillgänglighetskrav för att användas för interna system.

5.6 Credential Validation/Authentication

SWAMID AL2 5.6.1

Både SAML- och radiusinstallationerna uppfyller dessa krav eftersom protokollen är konfigurerade enligt instruktioner från SWAMID och eduroam.org.

SWAMID AL2 5.6.2

När en användare byter lösenord eller får sitt lösenord spärrat tas det gamla lösenordet bort ur LDAP och därmed kan det gamla lösenordet inte användas för inloggning. Om lösenordet blir spärrat måste dessutom användaren göra en lösenordsåterställning innan användaren kan logga in igen. Då kontot upphör eller spärras tas all användarinformation i LDAP bort vilket medför att användaren inte längre kan använda sitt konto.

Revokerade andra faktorer tas bort från kontot och från de servrar (t ex LDAP) som hanterar dem. Därmed är de inte möjliga att använda vid inloggning.

SWAMID AL2 5.6.3

Både Gemensam webbinloggning och eduroam kräver att användaren matar in sitt användarnamn och lösenord för att användaren ska få tillgång till tjänsten. Gemensam webbinloggning har en SSO-funktionalitet som aktiveras efter användaren loggat in. Eduroam har ingen sådan men användaren kan oftast spara sin inloggningsuppgifter i den klientprogramvara som finns för eduroam och därför använder eduroam ett särskilt lösenord, lösenord B.

När multifaktorsautentisering begärts av service provider kräver gemensam webbinloggning förutom användarnamn och lösenord att användaren verifierar sin andra faktor. Användare som saknar andra faktor kan inte logga in i tjänster som kräver multifaktorautentisering.

SWAMID AL2 5.6.4

För SAML och Gemensam webbinloggning universitetet uppfyller 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.