Mittuniversitetet
MID SWEDEN UNIVERSITY

Mittuniversitetets Identity Management Practice Statement

1. Inledning

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

Mittuniversitetet uppfyller 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 Mittuniversitetets 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.

4. Organisational Requirement

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

4.1 Enterprise and Service Maturity

This subsection defines the organization and the procedures that govern the operations of the identity provider.

4.1.1 Lärosätets/myndighetens/stiftelsens organisationsnummer

Mittuniversitetet har organisationsnummer 202100-4524 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/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 identitets- och behörighetssystem 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 enligt gällande lagstiftning angående personuppgifter.

Studenters personuppgifter hämtas ur lärosätets studiedokumentationssystem Ladok och därför gäller även registerförordning 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.

4.1.3 Rutiner för destruering av lagringsmedia

Mittuniversitet har rutiner för säker destruering av lagringsmedia avseende servrar, flyttbara lagringsmedia och övriga arbetsredskap.

4.2 Notices and User Information

The Member Organisation provides an Acceptable Use Policy (AUP) and a Service Definition including a Privacy Policy (PP) for the organisation Subjects. These policies are needed to fulfil the SWAMID Policy and the Swedish legislation including the General Data Protection Regulation (EU) No 679/2016.

4.2.1 Användarvillkor

Användarvillkoren finns publicerade på Miuns webb Användarregler

4.2.2 Godkännande

Personal godkänner användarvillkoren i samband med att de hämtar ut sitt konto.
Studenter godkänner användarvillkoren digitalt i samband med att de skapar sitt studentkonto.

4.2.3 Ny ansvarsförbindelse

När universitetet beslutar om en ny ansvarsförbindelse informerar vi alla användare via e-post.

4.2.4 Loggning av ansvarsförbindelse

Det loggas när kontot aktiveras första gången för studenter och medarbetare när de hämtar ut sina kontouppgifter.
Utskick om ny ansvarsförbindelse loggas i ärendehanteringssystemet i och med att det är en change.

4.2.5 Service definition

Tjänstebeskrivningen finns publicerad på Miuns web **Användarregler**
Privacy policy för IDP finns publicerad på Miuns web **Policy för hantering av personuppgifter**

4.3 Secure Communications

This subsection defines how clear text passwords, private keys and shared secrets must be protected to obtain operational security.

4.3.1 Filsäkerhet

Lösenordsdokumentation lagras i lösenordsvalv där lösenord är krypterade och åtkomst kräver tvåfaktors verifiering.
Säkerheten är inbyggd i servrar där endast utpekade användare kan logga in.

4.3.2 Privata nycklar

Privata nycklar hanteras privat i respektive system.
Dokumentation av privata nycklar sker på säkert sätt i lösenordsvalv.

4.3.3 Kryptering

All nätverkskommunikation skyddas med användning av TLS eller motsvarande kryptering.

4.3.4 Entity nycklar

Alla krypteringsnycklar är 2048 bitar RSA eller högre enligt Swamids teknologi profiler.

4.4 Security-relevant Event (Audit) Records

This section defines the need to keep an audit trail of relevant systems.

4.4.1 Loggning av säkerhetsrelaterade händelser

Alla förändringar på ett användarkonto med avseende på kontosäkerhet loggas i Active Directorys loggfunktioner. Lyckade, misslyckade inloggningar och förändringar på kontot loggas. Loggarna behålls i 6 månader.

5. Operational Requirements

The purpose of this section is to ensure safe and secure operations of the service.

5.1 Credential Operating Environment

The purpose of this subsection is to ensure adequate strength of Subject credentials, such as passwords, and protection against common attack vectors.

5.1.1 Lösenord

Mittuniversitet uppfyller kravet på komplexa lösenord i AD't. Minsta längd på lösenorden är 8 tecken.

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, använder endast aktuella TLS versioner, har inbyggda skydd mot återspelningsattacker (eng. message replay). Replikeringen mellan domänkontrollanter i Active Directory sker enligt Microsofts standardiserade säkerhetsmetod för replikering. Mittuniversitetet synkroniserar inte lösenord med externa leverantörer, t.ex. molntjänster.

Mittuniversitetet uppfyller Swamids teknologiprofiler.

5.1.3 Personligt ansvar

I Mittuniversitetets ansvarsförbindelse framgår att kontoinnehavaren är personligt ansvarig för användningen av användarkontot och att det inte får överlåtas eller på annat sätt göras tillgänglig för annan person. Användaren godkänner detta regelverk innan de aktiverar användarkontot.

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. Svartlistning används i central brandvägg och vissa specifika system (t. ex. e-post). Vid INFRA finns ansvar för att hålla servrar och annan hårdvara uppdaterade med avseende på säkerhetsproblem.

5.2 Credential Issuing

The purpose of this subsection is to ensure that the Identity Provider has control over the issuing process including issuing of credentials and binding of other information to the Subject. Furthermore, the Identity Provider and its Subjects must be uniquely identified.

5.2.1 Identitetshanterarens DNS-domän

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

5.2.2 Hantering av användarnamn/konton

Samtliga identitetsservrar vid MIUN har unika identifierare under domänen miun.se (Mittuniversitetet).

5.2.3 Unik användaridentitet

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

5.2.4 Flera användaridentiteter

Inom Miun kan en användare ha två användarkonton, ett som anställd och ett som student. Valet sker vid inloggning till dator eller tjänst.

5.2.5 Identifieringsmetoder

Legitimationer som accepteras för att knyta en person till ett universitetskonto vid utlämnande av t ex temporära inloggningsuppgifter.

Person med svenskt personnummer
Legitimationshandling som är godkänd av Polisen för att ansöka om ett pass. Godkänd svensk e-legitimation kan även användas för identifiering. Personnumret är den unika kopplingen mellan identifieringen och användarkontot.

Medborgare inom EU och EES
Pass eller resehandling av typen nationellt identifikationskort utfärdat inom EU/EES. Legitimationshandling i kombination fullständigt namn, födelsedatum och passutfärdande land. Vid tveksamhet kring giltigheten av utländskt pass äger kontrollören rätt att i stället kräva svensk giltig legitimationshandling.

Person från tredje land
För personer som kommer från tredje land, d.v.s. länder utanför EU och Schengen, gäller pass som legitimationshandling i kombination fullständigt namn, födelsedatum och passutfärdande land. Vid tveksamhet kring giltigheten av utländskt pass äger kontrollören rätt att i stället kräva svensk giltig legitimationshandling.

Lista med onlinetjänster för identifiering av person
Dessa tjänster används för identifiering av användare för tillitsnivå AL2
* Antagning.se (enbart studenter)
* EduID
* svensk e-legitimation med minsta tillitnivå LoA3
* Av Swamid godkända inloggningstjänster för tillitsnivå AL2 eller högre.

Temporära inloggningsuppgifter
Med temporära inloggningsuppgifter menar vi ett slumpat användarnamn och slumpat lösenord som är aktiv under en begränsad tidsperiod. Den temporära inloggningsuppgiften är knuten till en identitet och innehåller information om legitimationskontroll har utförts. De temporära inloggningsuppgifterna kan bara skapas på en förregistrerad person i ett personal-/studentadministrativt system.

Vi kan även lagra information om att en legitimationskontroll har gjorts

eller inte.

Medarbetare SWAMID AL2
När en medarbetare börjar arbeta vid Mittuniversitetet beställer ansvarig chef vid respektive avdelning/institution ett användarkonto via ett formulär som startar en process som skapar användarkontot.

Medarbetaren kan hämta ut sitt universitetskonto på tre olika sätt.

- Medarbetaren kan via Svensk e-legitimation med minst tillitsnivå LoA3 eller av Swamid godkända inloggningstjänster för tillitsnivå AL2 eller högre hämta sina inloggningsuppgifter. Lyckad inloggning ger oss ett personnummer vilket används för att starta en process där det används till att koppla personen till ett universitetskonto med unikt användarnamn, ett eget satt lösenord samt avtalgodkännande. När denna process är slutförd har användaren hämtat ut sitt universitetskonto.
Kontrollen görs både på att identifierad användare har tillitsnivå AL2 och vald inloggningstjänst uppfyller kraven för tillitsnivå AL2.

Ett exempel kan vara en medarbetare som identifierar sig via EduID. Om användaren har tillitsnivå AL2 hos EduID får de samma tillitsnivå hos Mittuniversitetet. Om medarbetaren identifierar sig med svensk e-legitimation görs motsvarande kontroll att tillitsnivån är minst LoA3.

-Medarbetaren kan personligen hämta ut kontouppgifterna (användaridentitet och temporärt lösenord) i receptionen på Servicecentret. Användaren uppmanas att omedelbart byta lösenordet till ett eget som uppfyller kraven i 5.1.1
Vid uthämtandet krävs godkännande av ansvarsförbindelsen. Kontroll görs att universitetskontot är för samma individ som hämtar ut det genom uppvisande av giltig legitimation. Kontroll görs att de förregistrerade uppgifterna för universitetskontot stämmer överens med giltig legitimation.

Alternativt kan temporära inloggningsuppgifter hämtas personligen ut av den nya medarbetaren i receptionen på Servicecentret (se tidigare text).

Detta används för att fortsätta processen online.
Kontroll görs att de förregistrerade uppgifterna för universitetskontot stämmer överens med giltig legitimation. Bland annat kontrolleras fullständigt namn, personnummer eller födelsedatum där personnummer saknas.

-Om medarbetaren inte kan hämta ut sitt universitetskonto enlig de två sätten ovan så skickas temporära inloggningsuppgifter med ett tidsbegränsat engångslösenord till medarbetarnas folkbokföringsadress. Personnumret används för att hitta folkbokföringsadressen.

Medarbetare SWAMID AL1.
Medarbetare som saknar folkbokföringsadress får sina temporära inloggningsuppgifter skickade med e-post. De temporära inloggningsuppgifterna innehåller information om att ingen legitimationskontroll har gjorts av individen. En förregistrerad e-postadress hämtas från personaladministrativa system.
Medarbetaren byter engångslösenordet via resetpassword, som använder sig av CAPTCHA, eller använder de temporära inloggningsuppgifterna för att fortsätta processen online.

Studenter SWAMID AL2
- Antagna studenter går till en webbsida där de identifierar sig via vald onlinetjänst (se lista tidigare i avsnittet) för identifiering. Lyckad inloggning ger oss ett personnummer vilket används för att starta en process för att skapa ett universitetskonto med användarnamn, ett eget satt lösenord samt godkänna avtal. När denna process är slutförd har användaren hämtat ut sitt universitetskonto.

Kontrollen görs både på att identifierad användare har tillitsnivå AL2 och vald inloggningstjänst uppfyller kraven för tillitsnivå AL2.

Ett exempel kan vara en student som identifierar sig via EduID. Om användaren har tillitsnivå AL2 hos EduID får de samma tillitsnivå hos Mittuniversitetet. Om studenten identifierar sig med svensk e-legitimation görs motsvarande kontroll att tillitsnivån är minst LoA3.

- Studenter som inte kan verifieras via onlinetjänst hanteras manuellt i receptionen på Servicecentret. Temporära inloggningsuppgifter hämtas personligen ut av den nya studenten i receptionen på Servicecentret. Med temporära inloggningsuppgifter menar vi ett slumpat användarnamn och slumpat lösenord som är aktiv under en begränsad tidsperiod. De temporära inloggningsuppgifterna innehåller information om att kontroll har gjorts av individen och används för att fortsätta processen online.

De temporära inloggningsuppgifterna används för att fortsätta processen online. Kontroll görs att universitetskontot är för samma individ som hämtar ut det genom uppvisande av giltig legitimation. Bland annat kontrolleras fullständigt namn, personnummer eller födelsedatum där personnummer saknas.

- Distansstudenter som inte kan identifiera sig online hanteras genom att temporära inloggningsuppgifter eller användaridentitet med ett tidsbegränsat engångslösenord skapas och skickas till folkbokföringsadressen.

Studenter SWAMID AL1

De som saknar folkbokföringsadress skickas ut av studieadministrativ personal via epost. De temporära inloggningsuppgifterna innehåller information om att ingen legitimationskontroll har gjorts av individen. En förregistrerad e-postadress hämtas från studieadministrativa system. Studenten byter engångslösenordet via resetpassword, som använder sig av CAPTCHA, eller använder den temporära inloggninsuppgiften för att fortsätta processen online.

Antagna studenter med interimspersonnummer går till en webbsida där de identifierar sig via en onlinetjänst som tillåter detta. Lyckad inloggning ger oss ett interimspersonnummer vilket används för att starta en process för att skapa ett universitetskonto med användarnamn, ett eget satt lösenord samt godkänna avtal. När denna process är slutförd har användaren hämtat ut sitt universitetskonto.

Förändring av Tillitsnivå
Medarbetare och studenter kan höja sin tillitsnivå på två olika sätt. En höjning av tillitsnivå kan leda till en lösenordsåterställning.

- Online genom att först logga in med sitt universitetskonto. Därefter höjer man sin tillitsnivå genom att identifiera sig antingen med svensk e-legitimation (tillitsnivå minst LoA3) eller med en annan kontouppgift med tillitsnivå AL2, eller bättre, inom SWAMID. Innan höjning kontrolleras att personnummer är samma för universitetskontot och den identifierade användaren.
Kontrollen görs både på att identifierad användare har tillitsnivå AL2 och vald inloggningstjänst uppfyller kraven för tillitsnivå AL2.

-Medarbetare och studenter som inte kan höja sin tillitsnivå online kan göra det genom att legitimera sig i servicecenter. Kontroll görs att det universitetskonto som ska höjas är för samma individ som legitimerar sig med giltig legitimation. Bland annat kontrolleras fullständigt namn, personnummer eller födelsedatum där personnummer saknas.

5.2.6 Förändring av AL nivåer

Förändring av AL-nivå loggas.

5.2.7 Ändring av självuppgiven information

Studenterna kan ändra i Ladok varifrån vi hämtar informationen.
Personalen kan ändra i HR systemet varifrån vi hämtar informationen.
Av användaren inlagda uppgifter i SSPR (resetpassword) kan ändras av användaren.
SSPR är en självbetjäningsportal för lösenordsåterställning. När användaren aktiverar SSPR så uppger de ett mobilnummer och / eller en alternativ e-postadress som de kan använda för lösenordsåterställningen. Det skickas en engångskod via SMS/e-post för att verifiera det som angetts som matas in för att slutföra registreringen.

5.2.8 Krav på identitetsgranskning

Vid Mittuniversitetet är all personal som hanterar användaridentiteter verifierade med minst AL2-nivå. Enligt rutin ska dessa personer inte använda resetpassword för lösenordsbyte. Tekniskt blockeras alla som hanterar användaridentiteter från lösenordsåterställning via resetpassword.

5.3 Credential Renewal and Re-issuing

The purpose of this subsection is to ensure that Subjects can change their credential and get new credentials when lost or expired.

5.3.1 Möjlighet till lösenordsbyte

Alla användare kan byta lösenord genom en websida som kräver inloggning.

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

Det finns olika sätt att göra lösenordåterställning för studenter och medarbetare. En lösenordsåterställning kan i vissa tillfällen sänka tillitsnivån men aldrig höja den.

Lösenordsåterställning via inloggningstjänst

Lösenordsåterställning kan ske via identifiering med Svensk e-legitimation minst tillitsnivå LoA3 eller av SWAMID godkända inloggningstjänster för tillitsnivå AL2 eller högre. I samband med lösenordåterställningen tar vi in information om vilket universitetskonto som ska återställas.
Kontrollen görs både på att identifierad användare har tillitsnivå AL2 och vald inloggningstjänst uppfyller kraven för tillitsnivå AL2.
Innan lösenordet återställs säkerställs att universitetskontot och identifierad användare har samma personnummer. Man behåller den tillitsnivå man har. Till exempel har man tillitsnivå AL2 så behåller man

den nivån.

Lösenordsåterställning via resetpassword
Studenter och medarbetare som glömt/tappat bort sitt lösenord hänvisas till https://resetpassword.miun.se/ som använder sig av CAPTCHA. Man anger e-postadressen till sitt universitetskonto. Resetpassword använder förregistrerad information, se 5.2.7. Detta ger SWAMID AL1.

Lösenordsåterställning via temporära inloggningsuppgifter
En tidsbegränsad temporär inloggningsuppgift kan skapas för en lösenordsåterställning. Processen fortsätter online där studenten eller medarbetaren kan återställa sitt lösenord. (se förklaring temporär inloggningsuppgift under 5.2.5)

Om den temporära inloggningsuppgiften ska skickas så görs det i första hand till folkbokföringsadressen. Man behåller den tillitsnivå man har. Till exempel har man tillitsnivå AL2 så behåller man den nivån.

Om inte folkbokföringsadress kan användas så används information som finns lagrad i personal-/studentadministrativa system. Om det skickas via epost, till telefonnummer eller med post till annan adress sätts tillitsnivån till SWAMID AL1.

IT Supporten har även möjlighet att skicka ett temporärt tidsbegränsat engångslösenord till en i förväg registrerat mobilnummer eller e-postadress lagrat i personal-/studentadministrativt system. Detta ger tillitsnivå AL1.

Lösenordsåterställning via fysiskt besök
Genom uppvisande av giltig legitimation kontrolleras namn och personnummer att de är korrekta och stämmer med universitetskonto enligt rutin på samma sätt som i 5.2.5.
Ett tillfälligt lösenord med tvingande lösenordsbyte ges till användaren. Det tillfälliga lösenordet byts direkt på plats. Detta ger tillitsnivå AL2.

5.4 Credential Revocation

The purpose of this subsection is to ensure that credentials can be revoked.

5.4.1 Inaktivering av användarkonton

När en anställd avslutar sin anställning vid Mittuniversitetet beställs stängning av användarkontot av ansvarig chef. Användarkontot hanteras enligt rutin för avslut av användarkonto. Ett studentkonto kan inaktiveras manuellt av IT Supporten eller automatiskt om vissa kriterier uppfylls, t.ex. upprepade felaktiga inloggningar, kontot inaktivt under för lång tid eller inte kopplad till en kurs inom en viss tid.
Användaren kan själv begära att kontot ska inaktiveras.
Användaren kan inte själv återaktivera kontot innan spärren är hävd.

5.4.2 Lösenordsåterställning och säkerhetsincidenter

Vid en avstängning av något skäl tex vid en säkerhetsincident kan IT Supporten deaktivera kontot. Användaren informeras av ansvarig handläggare om anledningen till deaktiveringen av kontot innan det aktiveras. Kontoinnehavaren måste efter aktivering genomföra en lösenordsåterställning på samma sätt som vid kontoaktiveringen enligt 5.3.3. Därigenom säkerställs att de förregistrerade uppgifterna för universitetskontot stämmer överens mellan kontot och identifieringen.

5.4.3 Skydd mot återupprepade incidenter

Mittuniversitetet har interna rutiner för att minimera risken att säkerhetsincidenter upprepas.

5.5 Credential Status Management

The purpose of this subsection is to ensure that credentials are stored accordingly and that Identity Management systems have a high degree of availability.

5.5.1 Historik över alla utfärdade identiteter

Historik finns över alla utfärdade användaridentiteter, en användaridentitet återanvänds inte.
Tidpunkten för lösenordsbyte och övriga kontohändelser loggas i Active Directorys loggfunktioner.

5.5.2 Tillgänglighet för identitetstjänsten

Inloggningsservern för SAML2 och inloggningsservern för Eduroam har samma tillgänglighetskrav som de interna systemen som använder de.

5.6 Credential Validation/Authentication

The purpose of this subsection is to ensure that the implemented Validation/Authentication processes meet proper technical standards.

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 spärrade konton

Konton som är spärrade kan inte användas.

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.

5.6.4 Sessionstider

För Swamid federerad inloggning uppfyller Mittuniversitet kraven med avseende på maximal längd för inloggad session.