2025-02-18

SWAMID Identity Management Practice Statement for Handelshögskolan i Stockholm

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 4
   5.1 Credential Operating Environment 4
   5.2 Credential Issuing 5
   5.3 Credential Renewal and Re-issuing 8
   5.4 Credential Revocation 8
   5.5 Credential Status Management 9
   5.6 Credential Validation/Authentication 9

Version	Datum	Författare	Förändring
1.0	2021-11-20	Richard Westermark Joachim Ekebom	Första IMPS, AL1
2.0	2024-09-26	Joachim Ekebom	Utkast för AL2
2.1	2025-01-10	Joachim Ekebom	Kompletterad med nya krav från 2024
2.2	2025-01-27	Joachim Ekebom	Revidering efter ITS möte 2025-01-17
2.3	2025-02-18	Joachim Ekebom	Revidering efter påpekanden från Swamid operations 2025-02-04
2.4	2025-03-06	Joachim Ekebom	Revidering efter påpekanden från Swamid operations 2025-02-27

2025-02-18

1. Inledning

Handelshögskolan i Stockholm (härefter kallad HHS) är en av Europas ledande handelshögskolor med ett unikt nätverk för näringslivet. Vår forskning är internationellt erkänd och många av våra forskare är bland de ledande personerna inom sina respektive områden, HHS är beroende av att på ett säkert och enkelt sätt kunna ge sina anställda och studenter tillgång till nationella och internationella IT-resurser och är därmed medlem av den nationella identitetsfederationen SWAMID. HHS ser därför ett fortsatt medlemskap som en förutsättning för sin verksamhet.

Detta dokument beskriver hur HHS uppfyller SWAMID AL1 och AL2.

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, 4.1.2

Handelshögskolan i Stockholm, organisationsnummer 802006-2074 är en enskild utbildningsanordnare och regleras inom lagen (1993:792) om tillstånd att utfärda vissa examina. Handelshögskolan i Stockholm följer Sveriges lagar och förordningar. samt värnar om medarbetarnas och studenternas digitala suveränitet.

Lärosätets identitets- och behörighetssystem ADintegrate, Staff och TAS innehåller uppgifter om personens koppling till organisationen, unikt identifierande personuppgifter samt organisationsbaserade personuppgifter för alla som är verksamma vid lärosätet. Med avseende på detta måstesärskild hänsyn till behandling av personuppgifter tas enligt aktuell personuppgiftslagstiftning.

Lärosätet arbetar för att uppfylla aktuella föreskrifter om statliga myndigheters informationssäkerhet från Myndigheten för samhällsskydd och beredskap.

4.1.3

HHS följer gängse informations-säkerhetsstandarder och rutiner för säker hantering av lagringsmedia som är krypterat och även destrueras vid byte av lagringsmedia på servrar.

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
HHS har instruktioner för användning av användarkonton i SSE Portal, Personalhandboken samt på https://ex.hhs.se/UsageAgreement .

4.2.2
En användare accepterar ”Usage Agreement” i samband med kontoutlämning.

4.2.3
När användaravtalet ändras meddelas alla användare via e-post.

4.2.4
Alla användare godkänner ”Usage Agreement” när de får sitt konto. Datum för godkännande lagras i Active Directory.

4.2.5
HHS tjänstedefinition för SAML2 WebSSO finns beskriven på:
https://ex.hhs.se/SWAMID/doc/ServiceDefinitionSV.htm
I denna finns även policy för hur personuppgifter för tjänsten hanteras.

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, 4.3.2

HHS använder Microsofts Active Directory för att lagra tekniska konton.

IdP:n skyddas av ACL:er på samtliga filer som innehåller lösenord för signering, Encryption/Decryption-certifkaten och för IdP:ns inloggningssidas TLS-certifikat. Endast ett fåtal administratörer inom IT Services på HHS har access.

4.3.3

All kommunikation mellan ändpunkter inom datahallen och till/från datahallen skyddas av minst TLS 1.2 eller högre.

4.3.4

Samtliga SAML-nycklar är krypterade med minst 2048-bit RSA nyckel.

4.4 Security-relevant Event (Audit) Records

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

4.4.1

IdP, Identitets och behörighetssystem loggar samtliga händelser. Behörig IT-personal kan verifiera och spåra händelser i efterhand.

4.5 Incident Management

HHS följer SWAMIDs incidenthanteringsprocess i händelse av säkerhetsincident relaterad till HHS IdP eller användare med påverkan på federerade inloggningar.

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

HHS förlitar sig på Microsofts implementation av komplex lösenordspolicy och uppnår därigenom kravet på 24 bitars lösenordsentropi. Lösenord måste innehålla minst 10 tecken och får ej återanvändas inom 4 gånger. Både studenter och anställda måste byta lösenord en gång per år.

HHS arbetar kontinuerligt med att förbättra säkerheten i samband med användning av IT-tjänster med till exempel Multi-factor authentication och Conditional Access Policys. MFA signaleras inte mot SWAMID.

5.1.2

HHS följer SWAMIDs teknologiprofiler.

Som autentiseringstjänster används SAML2 (via Active Directory Federation Services).

IT-tjänster som kräver åter-autentisering är konfigurerade att genomföra detta och inte förlita sig på tidigare inloggningssessioner.

5.1.3

I användaravtalet uppmanas användaren att aldrig lämna ut eller dela lösenord med någon annan. Se https://ex.hhs.se/UsageAgreement/ .

5.1.4

IT-tekniker övervakar kontinuerligt den tekniska infrastrukturen och de har befogenhet att inaktivera samtliga konton som misstänks att på något sätt användas av annan än innehavaren eller om misstänkt olovlig användning av konto och tjänster har skett. Det tillämpas även viss automatik/AI för att övervaka och inaktivera konton vid onormala beteenden ”compromised account”. Både IdP och övriga identitetssystem övervakas 24x7 och uppdateras löpande med säkerhetsuppdateringar av vår driftspartner.

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

HHS administrativa domän i SWAMID (”Scope”) är: hhs.se

5.2.2

HHS identitetsutfärdare har globalt unika identifierare.

5.2.3

Alla användare vid HHS får ett unikt användarnamn som aldrig återanvänds för en annan individ på HHS.

HHS har dokumenterade rutiner för att säkerställa att HHS unika identifierare (f.n. Enterprise ID) som signeraleras i SWAMID (typiskt ePPN och subject-id) aldrig

återanvänds för andra individer. I dagsläget sparas denna i IAMdb och tas aldrig bort.

5.2.4

Om användaren har flera användarkonton har alla konton ett unikt användarnamn som aldrig återanvänds för en annan individ på HHS.

Vid inloggning kan användaren välja vilket användarkonto som skall användas.

5.2.5

Vid legitimationskontroll krävs legitimationshandling som uppfyller polisens krav för utfärdande av svenskt pass, pass som uppfyller ICAO Doc 9303 eller ett nationellt id-kort inom EU/EES som uppfyller Regulation 2019/1157.

Alternativt kan legitimationskontroll ske via kontroll av digital representation av resehandling i e-legitimation enligt av SWAMID Board of Trustees godkända modell, https://wiki.sunet.se/pages/viewpage.action?pageId=204341308 där QR-kod avläses antingen med en BankID-app eller en QR-läsare kopplad till dator och där slagning görs mot BankID:s API.

Utlämning av konto kan ske med följande metoder:

Personlig utlämning i servicedesk eller vid antagningsenheten

Ett temporärt lösenord erhålles efter legitimationskontroll där personnummer eller namn och födelsedata jämförs med HHS katalogtjänster. Detta används som förregistrerad identifierare. Användare får SWAMID AL2.

Online via svensk e-legitimation

Efter inloggning med svensk e-legitimation på minst tillitsnivå 3 där personnummer jämförs med HHS katalogtjänster får användaren sätta ett lösenord. Personnummer används som förregistrerad identifierare. Användaren får SWAMID AL2.

Online via eduID för användare med svenskt personnummer

Efter inloggning via eduID på minst SWAMID AL2-nivå (där tillitsnivå och för eduID godkänd tillitsnivå kontrolleras) där personnummer jämförs med HHS katalogtjänster får användaren sätta ett lösenord. Personnummer används som förregistrerad identifierare. Användaren får SWAMID AL2.

Online via eduID för användare utan svenskt personnummer

Efter inloggning via eduID på minst SWAMID AL2-nivå (där tillitsnivå och för eduID godkänd tillitsnivå kontrolleras) görs en riskbaserad bedömning att namn och födelsedata tillräckligt väl stämmer med uppgifter i HHS katalogtjänster och användaren får sätta ett lösenord. Vid automatisk riskbedömnig skall förutom namn och födelsedata även e-postadress i eduID stämma överens mot förregistrerad e-postadress i HHS katalogtjänster och användaren får sätta ett lösenord. Även eppn/subject-id från eduID sparas och används som förregistrerad identifierare för senare lösenordsåterställning. Användaren får SWAMID AL2.

Online via obekräftat eduID-konto

Efter inloggning via eduID på minst SWAMID AL1-nivå (där tillitsnivå och för eduID godkänd tillitsnivå kontrolleras) där e-postadress från eduID jämförs med uppgifter i HHS katalogtjänster och användaren får sätta ett lösenord. E-postadress används som förregistrerad identifierare. Även eppn/subject-id från eduID sparas och används som förregistrerad identifierare för senare lösenordsåterställning. Användaren får SWAMID AL1.

Det är endast konton som representeras av en fysisk person vid HHS som exponeras mot SWAMID. Opersonliga konton som systemkonton etcetera exponeras inte mot SWAMID.

5.2.6

Användare som är på SWAMID AL1-nivå kan använda AL2-metoder från 5.2.5 för att bli bekräftad på SWAMID AL2-nivå. Förregistrerade identifierare enligt beskrivning används för att säkerställa att rätt individ bekräftas.

HHS kontohanteringssystem loggar tidpunkt, metod och förändring för alla ändringar av tillitsnivå. Dessa sparas för att senare kunna utreda säkerhetsincidenter.

Lösenordsåterställning efter avaktiverat konto blivit återaktiverat sker via någon av metoderna beskrivna under 5.2.5. AL-nivån kan ej sänkas i den processen.

5.2.7

Personuppgifter som personnummer, födelsedata och namn samt ev. mailadress för användare på AL2-nivå hämtas från HHS katalogtjänster, från legitimationshandlingar eller andra betrodda system.

Användare kan uppdatera lagrad självhävdad personlig information på SSE Portal.

HHS har kontaktvägar till alla användare.

Tillhörighet (affiliation) för användare hämtas från HHS katalogtjänster. Denna uppdateras senast 31 dagar efter beslut om ändring av tillhörighet för användare.

5.2.8

Alla vid HHS som utför kontoadministration uppfyller tillitsnivån SWAMID AL2. Kontoadministrationsverktyget kontrollerar att kontoadministratören är SWAMID AL2 vid inloggning.

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, 5.3.2

Alla användare kan byta sitt lösenord på SSE Portal. För att byta sitt lösenord måste användaren ange sitt nuvarande lösenord i direkt samband med att det nya anges.

5.3.3

Återställning av lösenord sker via någon av metoderna beskrivna under 5.2.5. med de förregistrerade identifierarna för respektive metod. AL-nivån kan ej sänkas i den processen.

Lösenord kan också återställas genom att en tidsbegränsad engångskod skickas till av användaren verifierat mobilnummer (alternativt mobilabonnemang hanterat av HHS) i kombination med tidsbegränsad engångslänk som skickas till av användaren verifierad e-postadress. Användaren får då ange ett nytt lösenord och bibehåller AL-nivå.

5.4 Credential Revocation

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

5.4.1

Konto kan avaktiveras för användning både efter begäran av användaren och efter beslut av HHS. Efter avaktivering kan inte kontot användas förrän det låsts upp av HHS.

Ett konto avaktiveras 2–3 veckor efter personals anställning har upphört.

Studenter som avregistreras utan examen får sina konton avaktiverade automatiskt på avregistreringsdagen. Studenter som avregistreras med examen får behålla sina konton under en period på ca tre månader, men dess behörighet begränsas. Detta med tanke för att underlätta överföring av data från skolans Office 365 till studenters egna lagringsutrymmen.

5.4.2

Vid eventuella missbruk så finns automatiserade processer som spärrar konto, vilket endast kan återställas av Servicedesk efter att analys utförts av orsak till spärr.

Användare kontaktas personligen vid säkerhetsincident för att informeras om vad som skett och hur användaren skall agera för att konto skall återaktiveras.

Lösenordsåterställning efter avaktiverat konto blivit återaktiverat sker via någon av metoderna beskrivna under 5.2.5. AL-nivån kan ej sänkas i den processen.

5.4.3

HHS arbetar kontinuerligt för att förbättra IT-säkerhet och för att skydda användarnas identiteter och information. Vid spärrande av konto pga säkerhetsincident följs orsaken upp för att undvika att motsvande sker igen.

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

Identitets- och behörighetssystemet innehåller historik över utfärdade identiteter, och där till kopplade IT-konton. Dessa sparas för att kunna utreda säkerhetsincidenter.

5.5.2

Som Identity Provider har HHS en hög tillgänglighet eftersom det används även för interna system.

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

HHS använder tekniska protokoll enligt SWAMID rekommenderade best practices.

5.6.2

HHS tillåter inte autentisering av stängda eller avaktiverade konton.

5.6.3
HHS kräver lösenord vid inloggning.

5.6.4
En Single Sign-on session har en livstid på max 12 timmar.