



Södertörn university 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	3
5. Operational Requirements	4
5.1 Credential Operating Environment	4
5.2 Credential Issuing	4
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

Anvisningar

1. Inledning

Södertörns högskola är ett lärosäte i Stockholm som utbildar, forskar och samverkar för en hållbar samhällsutveckling. Campusområdet ligger i Flemingsberg, 19 minuter med pendeltåg från Stockholms central.

Södertörns högskola använder SWAMID bland annat för att logga in mot Ladok.

Södertörns högskola ansöker om att få tillämpa SWAMID AL1 och AL2 tillitsprofil.

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.

Södertörns högskola, organisationsnummer 202100-4896, är en statlig utbildningsmyndighet vilket gör att lärosätets verksamhet regleras i lagar, förordningar och regleringsbrev. 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 aktuell personuppgiftslagstiftning.

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

De lagringsmedia som innehåller, eller kan innehålla, känsliga data som till exempel lösenord eller personuppgifter destrueras vid utbyte eller kassering. Detta utförs av den leverantör som fått i uppdrag av Södertörns högskola att skrota eller utföra service på utrustningen.

4.2 Notices and User Information

The member organization provides an Acceptable Use Policy (AUP) and a Service Definition including a Privacy Policy (PP) for the organization Subjects. These policies are needed to fulfil the SWAMID Policy and the Swedish legislation including the Swedish Personal Data Act (sv. Personuppgiftslagen, SFS 1998:204).

Användarvillkoren får den anställde och studenten upp när hen ska aktivera sitt konto med texten att genom aktiveringen av kontot godkännes villkoren. Användarvillkoren och rutiner finns även dokumenterade på högskolans hemsida, som den anställde eller studenten alltid har tillträde till. Användarvillkoren och länken till dessa gäller både anställda och studenter.

<https://www.sh.se/student/hur-gor-jag/regler-och-villkor-for-it-system>

Om villkoren ändras skickas e-post ut till alla anställda och studenter om förändringen samt att informationen uppdateras på högskolans hemsida.

Som tjänstedefinition används SWAMIDs mall för tjänstedefinition:

<https://wiki.sunet.se/display/SWAMID/SWAMID+template+Service+Definition>

<https://www.sh.se/om-oss/det-har-ar-sodertorns-hogskola/swamid-tjanstedefinition>

<https://www.sh.se/english/sodertorn-university/meet-sodertorn-university/this-is-sodertorn-university/swamid-service-definition>

4.3 Secure Communications

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

Administratörsrättigheter tilldelas endast de personer på Södertörns högskola som har ett behov av detta. Om en person skulle få andra arbetsuppgifter tas administratörsrättigheterna bort.

Nycklar och lösenord som behöver lagras i klartext i systemet skyddas av operativsystemets behörighetssystem där endast systemadministratörer har tillgång.

Den tekniska lösning Södertörns högskola använder sig av är Microsoft Active Directory Federation Services (ADFS).

Datakommunikationen för att nå identitetshanterarens tjänster sker i krypterad form med TLS. Utöver detta skyddas även ADFS-servern av Södertörns högskolas brandvägg. Lösningen består av fyra servrar (Två internt, och två externt). De servrar som är exponerade mot internet är ADFS-proxys.

Certifikaten för Swamid-kommunikationens signering och kryptering är självgenererade som har en giltighetstid på 10 år.

För ADFS autentiseringen används certifikat utfärdade genom SUNETs certifieringstjänst. Giltighetstiden för nycklarna är som längst 2 år.

Alla nycklar är minst 2048 bitar.

Om servarna skulle bytas ut eller om en större uppgradering skulle behövas skapas nya nycklar för systemet

4.4 Security-relevant Event (Audit) Records

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

Loggning av säkerhetsrelaterade händelser görs i både Active Directory och ADFS. För att kunna fånga relevant information är auditing påslaget i både AD och ADFS. Data skickas till en loggserver där den lagras. De händelser som loggas är bland annat lösenordsförändringar, konton som läggs till eller tas bort, rollförändringar, förändringar av attribut, onormala inloggningsförsök och tiden händelsen inträffade. Av säkerhetsskäl har endast systemadministratörer hos Södertörns högskola tillgång till loggservern.

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.

Södertörns högskolas lösenordskrav är i enlighet med SWAMIDs rekommendationer.

Minimum 10 tecken, AD-komplexitet, inga iterationer av gamla lösenord, och inget återanvändande av de 5 senaste lösenorden, byte av lösenord senast inom 24 månader, 5 felaktiga lösenordsförsök, 60 minuters autoupplåsning, och nollställning av räknare efter 60 minuter.

De tekniska profiler som används är i enlighet med SWAMIDs tekniska profiler eduroam och SAML WebSSO. Det protokoll som framför allt används för kommunikation är TLS vilket ger skydd emot s.k. message replay. Alla SAML attribut namn representeras med urn:oid.

Södertörns högskola tillämpar inte tvåfaktorsautentisering för alla, men för vissa administrationskonton.

Brandväggar är aktiverade på alla system och klienter.

Underhålls och uppdateringsrutiner finns för både system och klienter.

Användarna informeras om att konton är personliga, och inte får delas med andra samt att brott mot detta resulterar i avstängning.

5.2 Credential Issuing

The purpose of this subsection is to ensure that the Identity Provider has control over the issuing process. All relying parties have a need to uniquely identify the Identity Provider and the Identities provided by that Identity Provider.

5.2.1 Vi använder suni.se som unik domänidentifierare.

5.2.2 Vår IDP har en global unik identifierare.(idp-v2.suni.se)

5.2.3 Alla användarnamn är unika och återanvänds aldrig. Om en användare skulle återkomma efter en längre frånvaro, kommer denne att få ut ett nytt unikt användarnamn

5.2.4 I de fall en användare har mer än en affiliation, kommer denne att ha två olika användarnamn beroende på om den är student eller personal och får välja vilket konto som skall användas i samband med inloggningen.

5.2.5 Södertörns högskolas studenter kan hämta ut konto enligt kraven för tillitsnivån SWAMID AL2 med ett tidsbegränsat engångslösenord via något av följande alternativ:

- Över disk mot uppvisande av giltig. Se definition av giltig legitimation i sista stycket 5.2.5.
- Via verifiering med giltig Svensk E-legitimation på tillitsnivå 3 eller 4.

- Via verifierat konto med minst tillitsnivå AL2 från EduID eller Antagning.se
- Få det skickat till folkbokföringsadress
- Få det skickat till adress som studenten verifierar med legitimation och hushållsräkning och som kontrolleras av behörig personal. Detta kan användas om personen saknar svenskt personnummer och därmed folkbokföringsadress oavsett om personen bor i Sverige eller i utlandet.

Södertörns högskolas studenter har även möjlighet att hämta ut konto enligt kraven för tillitsnivån SWAMID AL1 med ett tidsbegränsat engångslösenord via följande alternativ:

- Mata in personnummer, e-postadress, captcha samt godkänna att den angivna e-postadressen sparas under hela IT-kontots livstid och få en engångs pinkod skickad till e-postadressen som sedan måste anges för att komma vidare till uthämtningen av engångslösenord för IT-kontot.

Konton som hämtas ut enligt kraven för tillitsnivån SWAMID AL1 klassificeras som AL1 och konton som hämtas ut enligt kraven för tillitsnivån SWAMID AL2 klassificeras som AL2. AL-klassificeringen återspeglas i SWAMIDS eduPersonAssurance.

Anställda kan bara hämta ut konto enligt kraven för tillitsnivån SWAMID AL2 och kontot klassificeras som AL2. Kontot hämtas ut med tidsbegränsat engångslösenord via något av följande alternativ:

- Över disk mot uppvisande av giltig. Se definition av giltig legitimation i sista stycket 5.2.5.
- Via verifiering med giltig Svensk E- legitimation på tillitsnivå 3 eller 4.
- Få det skickat till folkbokföringsadress
- Få det skickat till adress som den anställda verifierar med legitimation och hushållsräkning och som kontrolleras av behörig personal. Detta kan användas om personen saknar svenskt personnummer och därmed folkbokföringsadress oavsett om personen bor i Sverige eller i utlandet.

De anställdas kontons AL-klassificering återspeglas i SWAMIDS eduPersonAssurance.

De förregistrerade identifierare som används vid uthämtning av konto med ett tidsbegränsat engångslösenord är följande:

- För personer med svenskt personnummer på AL2 nivå är det svenskt personnummer.

- För personer utan svenskt personnummer på AL2 är det födelsedata och namn.
- För övriga användare som är på AL1 nivå räcker det med en kontaktadress. (Endast studenter kan hämta ut konto på AL1 nivå)

Kontohandläggare och systemansvariga som används vid kontohantering är verifierade för tillitsnivån SWAMID AL2. Alla kontohändelser som skapas av kontohandläggarnas användande av systemet eller som skapas automatiskt i system som används vid kontohantering loggas enligt kraven för tillitsnivån SWAMID AL2.

Användare, både studenter och anställda, som är inloggade kan ändra självuppgiven information. Om de inte kan logga in måste de hämta ut nytt tidsbegränsat engångslösenord enligt ovan.

Med giltig legitimation menas

- ID-handlingar godkända enligt polisen för uthämtning av pass och nationellt ID (<https://polisen.se/tjanster-tillstand/pass-och-nationellt-id-kort/besok-passexpedition/giltiga-id-handlingar/>)
- Nationella identitetskort utfärdade inom EU/EES
- Pass som uppfyller kraven för gränskontroll

5.2.6 Alla ändringar gällande Assurance Level loggas på högskolans SQL-cluster.

5.3 Credential Renewal and Re-issuing

Renewal of credentials occur when the Subject changes its credential using normal password reset. Re-issuing occurs when credentials have been invalidated.

Användare kan när som helst själva byta lösenord. Detta görs då genom att ändra lösenordet för Active Directory eller Azure Active Directory vars lösenord synkroniseras. För att kunna göra detta måste användaren uppge sitt nuvarande lösenord. Det nya lösenordet måste uppfylla kraven för Södertörns högskolas lösenordspolicy.

Om ett lösenord behöver återställas kan användaren hämta ut ett nytt tidsbegränsat lösenord enligt 5.2.

De förregistrerade identifierarna som används är de som specificeras enligt 5.2.

Om de tidigare har angivit självuppgivet mobilnummer och e-postadress i inloggat läge, enligt kraven för tillitsnivån SWAMID AL2, kan de återställa lösenord via Azure Self Service Password Reset med tvåkanalsverifiering där både den självuppgivna e-postadressen och mobilnumret används.

Dessa valideras vid angivandet, med engångskoder, för att säkerställa innehavet och korrekt inmatning.

Lösenord byts var 21:a månad. Bytet framtvingas automatiskt av Windows Active Directory.

5.4 Credential Revocation

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

Vid behov kan användarkonton inaktiveras.

Användare kan själva begära att deras användarkonton ska inaktiveras.

Detta kan göras omedelbart om ärendet är brådskande. Ett exempel på detta skulle kunna vara vid misstanke om brott eller som straff i disciplinnämndsärenden. Inaktivering av användarkonton sker också vid tjänstledighet samt vid avslutad anställning eller avslutade studier i väntan på att användarkontot raderas i kontorevision.

Om ett användarkonto blivit inaktiverat på grund av missbruk mot användarvillkoren förs alltid en dialog med användaren innan eventuell återaktivering av kontot. Om kontot återaktiveras får användaren tillgång till kontot igen genom att hämta ut ett tidsbegränsat lösenord enligt punkt 5.2. De förregistrerade identifierarna som används är de som specificeras enligt 5.2.

Återaktivering sker när anställd åter är i tjänst eller student återupptar sina studier. Om misstanke finns att användaren blivit av med sitt lösenord via phishing måste hen hämta ut ett nytt tidsbegränsat lösenord enligt punkt 5.2.

De förregistrerade identifierarna som används är de som specificeras enligt 5.2.

Om ett användarkonto inaktiveras på grund av en säkerhetsrelaterad incident vidtas åtgärder, enligt Södertörns högskolas rutiner för incidenthantering, för att förhindra att incidenten ska hända 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.

Alla användaridentiteter utfärdade av Södertörns högskola och deras status är dokumenterade. Förändringar för utfärdade användaridentiteter loggas.

Södertörns högskolas identitetstjänst har samma tillgänglighet som interna system som använder identitetstjänsten. Ett exempel på interna system är LADOK.

5.6 Credential Validation/Authentication

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

I detta avsnitt följer Södertörns högskola SWAMIDs rekommendationer.

Södertörns högskolas identitetstjänst autentiserar inte inloggningsuppgifter som har inaktiverats.

Södertörns högskolas identitetstjänst kräver autentiseringsuppgifter vid inloggning.

Södertörns högskolas identitetstjänst kräver att användaren autentiserar sig minst en gång var 12:e timme. Det innebär att Single Sign-On sessioner inte är giltiga i mer än 12 timmar.