2024-02-20

SÖDERTÖRN UNIVERSITY | STOCKHOLM
sh.se

Södertörn university Identity Management Practice Statement

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 tvåfaktorsautentisering för alla personalkonton och administrationskonton vid 1) inloggning om den swamidanslutna inloggningstjänsten kräver det eller om man frivilligt väljer tvåfaktorsautentisering framför enbart lösenord eller 2) om den swamidanslutna tjänsten kräver det för en enskild transaktion. I slutet av 2024 kommer även alla studentkonton att tillämpa tvåfaktorsautentisering på samma sätt. Alternativen för tvåfaktorsautentisering, utöver lösenord, som personal och studenter kan använda sig av är:

1. Microsofts Authenticator-app med pushnotifiering med inmatningskrav (som kräver att två siffror som visas på skärmen matas in i appen för godkännande)
2. Microsofts Authenticator-app med inmatning av kod (sexsiffrig kod som visas i appen skrivs in i inloggningsflödet på skärmen)
3. Token2 hårvarutoken, kallad ”SH-dosa” (sexsiffrig kod som visas i hårdvarutoken skrivs in i inloggningsflödet på skärmen). SH-dosan bokas i högskolans utlåningssystem och lämnas ut från kassaskåpet i Infocenter mot uppvisande av giltig legitimation, definition enligt 5.2.5.

De tre autentiseringsmetoderna ovan används enbart för tvåfaktorautentisering. För att ändra, hantera eller lägga till metoder för tvåfaktorautentisering krävs inloggning med tvåfaktorautentisering. För återställning av tvåfaktorautentisering måste SH-kontoinnehavaren hämta ut sitt SH-konto igen enligt 5.2.5.

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 legitimation. 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 där någon av följande uppgifter stämmer överens med källsystemet för studenter.
    - personnummer
    - ePPN / subject-id
    - födelsedata, för- och efternamn och epostadress
- 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 studenten bor i utlandet och därmed saknar folkbokföringsadress i Sverige.

Första gången en student, som saknar svenskt personnummer, validerar sig med ett SWAMID AL2 konto från eduID görs en riskbaserad bedömning. Den riskbaserade bedömningen godkänns endast om alla tre kontroller mellan personuppgifterna från eduID och källsystemet för studenterna uppfylls. Kontrollerna är 1) Födesledata måste vara samma, 2) För- och efternamn måste vara tillräckligt lika, 3) E-postadressen i eduID måste vara samma som registrerad adress i källsystemet för studenter. Vid godkänd riskbaserad bedömning sparas ePPN och subject-ID från eduID. Nästa gång studenten loggar in mot EduID sker kopplingen mellan eduID-kontot och SH-kontot på eduIDs ePPN eller subject-ID.

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 legitimation. 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 den anställda bor i utlandet och därmed saknar folkbokföringsadress i Sverige.

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
    - Vid manuell kontroll
        - Fiktivt personummervärde, födelsedata och namn. Studenter har ett fiktivt personnummervärde i Ladok (T-nummer) och personal har ett fiktivt personnummervärde i lönesystemet.
    - Kontroll mot eduID
        - födelsedata, för- och efternamn och epostadress
        - ePPN / subject-id
- 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
- Digitalt ID via BankID appen som verifieras via BankIDs API för verifiering

Verifiering av Digitalt ID via BankID för utlämning av SH-konto sker genom

1. Personen som vill hämta ut sitt SH-konto tar fram sitt Digitala ID i Mobilt BankID applikationen. För att göra det måste hen verifiera sig med sitt mobila BankID. Det digitala ID:t visar under en begränsad tidsperiod foto, ålder, namn och personnummer.
2. Kontohandläggaren kontrollerar att fotot på i det digitala ID:t stämmer överens med personen de har framför sig. Kontohandläggaren kontrollerar även säkerhetsdetaljerna enligt BankIDs instruktioner för visuell kontroll (https://www.bankid.com/foretag/digitalt-id-kort). Om kontrollerna av det digitala ID:t stämmer skannar kontohandläggaren qr-koden på mobilskärmen med en hårdvaruscanner.
3. QR-kodens värde skickas via kontoutlämningsapplikationen till BankIDs API för verifiering (https://www.bankid.com/utvecklare/guider/verifiering-av-digitalt-id-kort/introduktion).
4. Resultat
    a. Om BankIDs API godkänner QR-koden skickas användarens personnummer och namn tillbaka till kontoutlämningsapplikationen och utlämningen av SH-kontot kan göras med det verifierade personnumret.
    b. Om BankIDs API inte godkänner QR-koden returneras endast en felkod med beskrivning som visas i kontoutlämningsapplikationen. I och med att kontoutlämningsapplikationen inte fått något personnummer från BankIDs API kan inget SH-konto lämnas ut.

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.

5.3.1, 5.3.2 Credential renewal.

Användare kan när som helst själva byta lösenord. Detta görs då genom att ändra lösenordet för Active Directory eller EntraID (tidigare benämnd 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.

Så länge en användare har en giltig tvåfaktorautentiseringsmetod kan hen logga in på https://mysignins.microsoft.com/security-info med lösenord och den giltiga tvåfaktorautentiseringsmetoden och lägga till, ta bort eller uppdatera sina tvåfaktorautentiseringsmetoder.

5.3.3 Credential Re-issuing

Om ett lösenord behöver återställas kan användaren hämta ut ett nytt tidsbegränsat engångslösenord enligt 5.2.
De förregistrerade identifierarna som används är de som specificeras enligt 5.2.

Om användaren inte längre har tillgång till en giltig tvåfaktorautentiseringsmetod kan tvåfaktorautentiseringsmetoderna återställas. Processerna för återställningen skiljer sig åt för Microsoft Authenticator (tvåfaktorautentiseringsmetod 1 och 2 enligt 5.1) och återställning av Token2 hårdvarutoken ”SH-dosa” (tvåfaktorautentiseringsmetod 3 enligt 5.1).

För att återställa tvåfaktorautentiseringsmetoderna för Microsoft Authenticator måste användaren hämta ut ett nytt tidsbegränsat engångslösenord enligt 5.2. När uthämtning av ett nytt tidsbegränsat engångslösenord görs enligt 5.2 nollställs alla tvåfaktorautentiseringsmetoder förutom Token2 hårdvarutoken ”SH-dosa” och användaren måste sätta upp Microsoft Authenticator som tvåfaktorautentiseringsmetod igen.

Radering av koppling mellan utlånad Token2 hårvarutoken ”SH-dosa” och användarens SH-konto sker vid återlämning av SH-dosa till Infocenter, när utlåningstiden har gått ut eller vid rapporterad förlust. Om användaren rapporterar förlust av Token2 hårvarutoken ”SH-dosa” till Infocenter raderas den från EntraID (tidigare benämnd Azure Activive Directory) och användarens sessioner raderas och användarens lösenord återställs. Användaren måste då hämta ut ett nytt tidsbegränsat engångslösenord enligt

5.2 och låna en ny Token2 hårdarutoken ”SH-dosa” eller sätta upp Microsoft Authenticator för tvåfaktorautentiseringsmetod.

Lösenord är giltiga i 21 månader. Byte 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 engångslösenord 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 engångslösenord enligt punkt 5.2.
De förregistrerade identifierarna som används är de som specificeras enligt 5.2.

Vid behov kan tvåfaktorautentiseringsmetoder och befintliga tvåfaktorautentiseringssessioner inaktiveras. I de fall denna åtgärd görs återställs även lösenordet om och användaren måste hämta ut ett nytt tidsbegränsat engångslösenord enligt 5.2.

I alla fall där användaren hämtar ut ett nytt tidsbegränsat engångslösenord enligt punkt 5.2 så nollställs även Microsoft Authenticator tvåfaktorautentiseringsmetoder (metod 1 och 2 enligt 5.1) och användaren uppmanas sätta upp Microsoft Authenticator för tvåfaktorautentiseringsmetod igen.

Om Token2 hårvarutoken ”SH-dosa” inaktiverats måste användaren låna en ny Token2 hårdarutoken ”SH-dosa” via Infocenter eller sätta upp Microsoft Authenticator för tvåfaktorautentiseringsmetod.

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.