Sunet Identity Management Practice Statement

Datum: 2023-05-30
Version: 2.0

1. Inledning

Sunets unika datanät och säkra och stabila it-tjänster gör det möjligt för lärosäten och andra organisationer knutna till forskning eller högre utbildning att samverka nationellt och globalt. Sunet är en grundbult i Sveriges akademiska värld sedan 1984. Sunet använder SWAMID för att ge verksamma vid Sunet åtkomst tjänster inom Sunet och tjänster registrerade i SWAMID eller tjänster tillgängliggjorda via eduGAIN.

Sunet uppfyller kraven för SWAMID:s tillitsprofiler SWAMID AL1, SWAMID AL2 och SWAMID AL3. Sunet använder tjänsten eduID Connect som identitetsutfärdare och eduID för inloggning. Användarens personliga personuppgifter hanteras i eduID. Uppgifter kopplade till organisationen hanteras i eduID Connect. Med avseende på detta hanteras användarens tillitsnivå och personuppgifter i eduID. eduID Connect hanterar uppgifter om användarens koppling till Sunet.

1.1 Uppdateringshistorik

Uppdaterad	Ansvarig	Kommentarer
2021-12-01	Pål Axelsson	Version 1.0, beskrev AL1 via Google Workspace
2023-05-30	Zacharias Törnblom	Sunet börjar använda eduID Connect

4. Organisational Requirement

4.1 Enterprise and Service Maturity

4.1.1 Sunet är en avdelning på Vetenskapsrådet, 202100-5208. Sunet använder egna IdP-tjänster beroende på att alla verksamma vid Sunet inte är anställda vid Vetenskapsrådet utan är ofta inhyrda från lärosäten och andra organisationer.

4.1.2 Den viktigaste författningen som styr Vetenskapsrådets arbete utöver regeringsformen (SFS 1974:152), tryckfrihetsförordning (SFS 1949:105), myndighetsförordningen (SFS 2007:515), förvaltningslagen (2017:900), offentlighets och sekretesslagen (2009:400) m.fl. är förordningen (2009:975) med instruktion för Vetenskapsrådet.

Regleringsbrevet utställs årligen av regeringen och styr myndighetens uppdrag under ett kalenderår. I övrigt följer myndigheten Sveriges övriga lagar och förordningar.

Sunet identitets- och behörighetssystem innehåller personuppgifter för alla som är verksamma vid Sunet. Med avseende på detta måste särskild hänsyn till behandling av personuppgifter tas enligt aktuell personuppgiftslagstiftning.

Sunet följer även samtliga föreskrifter från Myndigheten för samhällsskydd och beredskaps gällande området informationssäkerhet.

4.1.3 Sunet använder sig av eduID som IdP och då denna är godkänd på SWAMID AL3 så hanteras destruktion enligt process som beskrivs i eduID:s Identity Management Practice Statement.

4.2 Notices and User Information

4.2.1 Sunets användarregler är en del av dokumentet Information Technology Security Policy. Denna policy finns publicerad på Sunets interna wikisidor på wiki.sunet.se. Sunet använder användarkonton med eduID för inloggning i Sunets identitetsutfärdare och därför gäller även eduID:s användarregler inkl. rutiner om uppdatering.

4.2.2 Det finns två uppsättningar regler. Dels användarreglerna för eduID, som alltid gäller när eduID används. Utöver detta finns det användningsregler för att använda eduID Connect instans hos Sunet. En användare accepterar användarreglerna för eduID i samband med att de skapar kontot. Användaren måste ta del av och godkänna Sunets användarregler innan man blir tillagd i Sunets IdP.

4.2.3 Vid uppdatering av användarreglerna meddelas samtliga användare via e-post.

4.2.4 Sunet för inget register över att användarna har godkänt användarreglerna beroende på att användarna måste godkänna dem om de ska använda kontot och att användarna informeras i det fall reglerna ändras.

4.2.5 Sunet har publicerat sin kombinerade service definition och privacy policy för Identitetsutgivaren för webbaserad inloggning på adressen https://wiki.sunet.se/display/info/Sunet+Identity+Provider+Service+Definition+and+Privacy+Policy.

4.3 Secure Communications

4.3.1 Endast personal vid Sunet NOC, samt särskilt godkända personer, har teknisk och administrativ åtkomst till Sunets IdP-tjänster. Säkerhetsskyddsåtgärder runt åtkomst till servrar, och innehållet på dessa, hanteras på samma sätt som Sunets övriga infrastruktur.

4.3.2 Alla krypterings- och signeringsnycklar samt delade lösenord är lagrade under åtkomstkontroll på servrarna för IdP-tjänsterna. I Sunets konfigurationshanterare är dessa krypterings- och signeringsnycklar samt delade lösenord krypterade för att förhindra oavsiktlig åtkomst.

4.3.3 All åtkomst till ingående servrar och tjänster sker krypterat enligt gängse protokoll och best practice. Då SSL/TLS används sker detta endast med TLS protokoll som ännu inte har

blivit “deprecated” och där nyckellängden uppfyller kraven på att vara säkra enligt NIST SP 800-57.

4.3.4 Teknologispecifika krypterings- och signeringsnycklar för Sunets IdP-tjänster uppfyller kraven för respektive teknologiprofil, dvs. minst motsvarande 2048 bitar RSA/DSA

4.4 Security-relevant Event (Audit) Records

4.4.1 eduID Connect loggar alla organisationella förändringar på organisationsinformationen kopplade eduIDs användarkonton. eduID loggar i enlighet med SWAMID AL3 alla förändringar på användarkontot i eduID enligt process som beskrivs i eduID:s Identity Management Practice Statement.

eduID loggar alla lyckade och misslyckade inloggningsförsök och eduID Connect loggar alla påbörjade och genomförda inloggningsförsök och dessa går att korsreferera vid behov. eduID Connect har ingen kunskap om misslyckade inloggningar.

Alla inloggningsförsök i eduroam loggas.

5. Operational Requirements

5.1 Credential Operating Environment

5.1.1 Sunet använder användarkonton i eduID för webbaserad inloggning. Detta innebär att de metoder som är tillgängliga i eduID även är tillgängliga för Sunets identitetsutfärdare. eduID Connect har stöd för alla metoder som används i eduID.

För eduroam används antingen slumpade lösenord på minst 10 tecken där teckenrymden är a-z, A.Z, 0-9 samt specialtecken eller inloggningscertifikat via geteduroam.

5.1.2 Sunets IdP-tjänster är konfigurerade enligt aktuella rekommendationer från SWAMID och är därmed skyddade från s.k. ”message replay”.

5.1.3 eduID är godkänt för SWAMID AL3 och därmed gäller eduID:s regler kring inloggningsfaktorer.

5.1.4 Sunets IdP-tjänster uppdateras och övervakas kontinuerligt i syfte att motverka missbruk av användarkonton vid Sunet. Sunets IdP-tjänster är även placerade bakom brandväggar för att minska risken för oavsiktlig åtkomst. Övervakning i eduID beskrivs i eduID:s Identity Management Practice Statement.

5.2 Credential Issuing

5.2.1 Sunet använder domänen sunet.se för att koppla unika användare till Sunet.

5.2.2 Identitetsutgivarna för de olika federativa teknikerna som används av Sunet använder unika identifierare via antingen URL eller DNS-namn där alla DNS-delar avslutas med sunet.se eller för eduID Connect unik delegerad namnrymd under connect.eduid.se.

5.2.3 Alla användare har unika användaridentifierare som aldrig återanvänds för användaren själv eller andra individer.

5.2.4 Alla användare har endast ett användarkonto.

5.2.5 Sunet använder eduID för all inloggning i eduID Connect. Verifiering av användare sker enligt aktuella metoder i eduID. eduID ansvarar för att signalera korrekt tillitsprofil till eduID Connect som sedan signalerar samma till tjänsten som användaren loggar in i.

Aktivering av nya personers användarkonton vid Sunet genomförs av kontoadministratör i inloggningstjänsten genom att kontoadministratören registrerar organisationsuppgifter och en gemensam identifierare. Identifieraren är personnummer för personer med svenskt personnummer, och e-postadress för övriga personer. Inbjudan skickas därefter ut som en länk till en användare. Länken är tidsbegränsad.

Genom att klicka på länken i inbjudan kopplar användaren sin organisationstillhörighet i inbjudan till ett specifikt eduID genom att logga in på ett befintligt eduID, förutsatt att den gemensamma identifieraren är den samma mellan kontot i eduID som används och inbjudningstjänsten för Sunets IdP. Om e-postadress har använts som identifierare kontrolleras av handläggare att det är rätt person som har använts sitt eduID-konto. Till sin hjälp har handläggaren de unika identifierarna som finns i punktlistan nedan. Med personnummer sker matchningen automatiskt.. En ytterligare förutsättning för att koppling ska kunna ske är att användarkontot är minst SWAMID AL2 i eduID, vilket aktivt kontrolleras när kopplingen genomförs.

Det sker ingen koppling i eduID till organisationen, utan kopplingen sker genom att användarens eduPersonPrincipalName i eduID kopplas till användarens organisationsinformation i eduID Connect.

Förregistrerad identifierare som används för att unikt identifiera användaren framöver är användarens unika identifierare i eduID samt

- ett svenskt personnummer
- eller födelsedata (ÅÅMMDD) samt förnamn och efternamn från pass eller eIDAS

Om förregistrerade identifierare (ett svenskt personnummer, eller födelsedata samt förnamn och efternamn) förändras i eduID måste användaren logga in i Sunets IdP-tjänst med sitt eduID-konto. Uppgifterna jämförs med användarens unika identifierare i eduID, därefter uppdateras uppgifterna automatiskt.

5.2.6 All hantering av tillitsnivå sker i eduID i eduID:s register över nuvarande och historiska tillitsnivåer.

5.2.7 All hantering av självuppgivna personuppgifter hanteras i eduID, det finns inga ytterligare självuppgivna personuppgifter i eduID Connect.

5.2.8 Alla system- och kontoadministratörer i Sunets inloggningstjänst är godkända för SWAMID AL3 som aktivt kontrolleras vid inloggning.

5.3 Credential Renewal and Re-issuing

5.3.1–5.3.3 All hantering av inloggningsuppgifter hanteras i eduID vilket gör att byte och återställning av inloggningsuppgifter återställs enligt eduID:s rutiner.

5.4 Credential Revocation

5.4.1 Sunet kan för sin instans av eduID Connect vid behov stänga av en organisationsidentitet för ett eduID-konto. Antingen genom att tills vidare förhindra att kontot används inom Sunets instans (exempelvis vid tillfällig avstängning), eller genom att ta bort användarens eduID-konto från instansen (exempelvis vid anställningens avslut). När en person inte längre är verksam vid Sunet följs Sunets definierade rutiner. Om en person själv vill stänga sitt användarkonto vid Sunet måste denne vända sig till Sunet NOC för att få det genomfört.

5.4.2 Om eduID-kontot som är kopplat till organisationsidentiteten inte längre kan användas, så kan användaren skapa ett nytt eduID-konto och istället få detta kopplat till Sunet. Den identifierande informationen i det nya kontot behöver överensstämma med informationen i organisationsidentiteten med hjälp av de förregistrerade identifierarna under 5.2.5. För detta används inbjudningstjänsten beskriven under avsnitt 5.2.5.

Vid en säkerhetsincident tas kopplingen mellan eduID-kontot och organisationsidentiteten bort. Efter att användaren informeras om varför kopplingen tagits bort så genomförs samma process som i föregående stycke.

5.4.3 Om ett användarkonto stängts av beroende på en säkerhetsincident genomförs en analys om hur incidenten uppkom och hur Sunet kan minska risken för att motsvarande incident återuppträder.

5.5 Credential Status Management

5.5.1 I eduID Connect finns alla aktuella och nyligen avstängda användaridentifierare. Unika identifierare för raderade konton sparas i ett särskilt register för att säkerställa att dessa inte återanvänds.

5.5.2 Sunet har samma tillgänglighetskrav på IdP-tjänsterna som för övriga interna tjänster inom Sunet beroende på att denna används för att logga in i tjänsterna eller i det trådlösa nätverket.

5.6 Credential Validation/Authentication

5.6.1 Sunet följer SWAMIDs regler och best practice för konfiguration av sina IdP-tjänster.

5.6.2 Det går endast att logga in i Sunets IdP med aktiva användarkonton i eduID som har en organisationskoppling till Sunet i eduID Connect.

5.6.3 För att logga in måste användaren logga in via eduID enligt det regelverk som finns där.

5.6.4 Sunets webbaserade IdP-tjänst genom eduID Connect har inte eget stöd WebSSO utan varje inloggning valideras mot eduID och följer eduID:s regelverk för WebSSO.