POLICYDOKUMENT

BESLUTAD AV REKTOR 2025-11-12

SWAMID Identity Management Practice Statement för eduID Connect

* Numreringen i detta policydokument utformas så att den stämmer överens med policydokument för SWAMID Identity Assurance Level 1/2/3 Profile, enligt önskemål från SUNET. Se vidare wiki.sunet.se/display/SWAMID/SWAMID+Policy

1. Inledning

Stiftelsen Stockholms Musikpedagogiska Institut (SMI) är en enskild högskola och använder SWAMID för att ge verksamma vid organisationen möjlighet att logga in webbaserade tjänster som är anslutna till identitetsfederationen SWAMID.

SMI uppfyller kraven för SWAMID:s tillitsprofiler SWAMID AL1, SWAMID AL2 och SWAMID AL3. SMI 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 organisationen.

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 Stiftelsen Stockholms Musikpedagogiska Institut (SMI), organisationsnummer 802002-3670, är en enskild utbildningsanordnare och regleras inom Stiftelselag (1994:1220) och Lagen (1993:792) om tillstånd att utfärda vissa examina. SMI följer Sveriges lagar och förordningar.

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

4.1.3 SMI använder sig av eduID som Identitetsutfärdare 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

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 SMI använder användarkonton på eduID för inloggning i organisationens identitetsutfärdare och därför gäller eduID:s användarregler inkl. rutiner om uppdatering. eduID:s användarregler finns publicerade på eduID.se.

4.2.2 En användare accepterar användarreglerna för eduID i samband med att de skapar kontot.

4.2.3 Om och när användarreglerna i eduID uppdateras måste användarna godkänna dem vid nästa inloggning. Det går inte att logga in med eduID innan uppdateringen är godkänd.

4.2.4 Användarens acceptans av eduID:s användarvillkoren lagras i eduID.

4.2.5 Service definition och privacy policy finns publicerad på smi.se/sunet/swamid/.

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 Endast personal vid Sunet NOC, samt särskilt godkända personer, har teknisk och administrativ åtkomst till eduID:s Identitetstjänster. 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 Identitetstjänsterna. 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 eduIDs identitetstjänster uppfyller kraven för respektive teknologiprofil, dvs. minst motsvarande 2048 bitar RSA/DSA.

4.4 Security-relevant Event (Audit) Records

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

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.

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

5.1.2 eduID:s Identitetstjänster 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 eduID:s Identitetstjänster uppdateras och övervakas kontinuerligt i syfte att motverka missbruk av användarkonton. Identitetstjänsterna 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

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 SMI använder domänen smi.se för att koppla unika användare till organisationen.

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

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

5.2.4 Alla användare har endast ett användarkonto.

5.2.5 SMI 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 SMI genomförs av kontoadministratör i inloggningstjänsten genom att kontoadministratören registrerar organisationsuppgifter, en gemensam identifierare samt en självuppgiven e-postadress för inbjudan. Identifieraren är personnummer för personer med svenskt personnummer. För personer utan svenskt personnummer används födelsedata och namn som kombinerad identifierare för riskbaserad

bedömning. Inbjudan skickas därefter ut med e-post till personen. E-postmeddelandet innehåller länk till aktiveringstjänsten samt en tidsbegränsad engångskod.

Genom att gå till länken och använda inbjudningskoden i inbjudan kopplar användaren sin organisationstillhörighet i inbjudan till ett specifikt eduID genom att logga in på ett befintligt eduID. Vid aktiveringen används förregistrerade identifierare för att säkerställa att det är rätt person som genomför aktiveringen. Om personnummer överensstämmer eller namn, födelsedata och e-postadress överensstämmer för personer utan svenskt personnummer genomförs aktiveringen automatiskt, annars genomförs manuell riskbedömning bedömning av organisationens kontoadministratörer. En ytterligare förutsättning för att koppling ska kunna ske är att användarkontot är minst SWAMID AL2 i eduID, vilket automatiskt 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 organisationens Identitetstjänst 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 SMI inloggningstjänst är godkända för SWAMID AL3 som aktivt kontrolleras 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.

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

5.4 Credential Revocation

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

5.4.1 SMI 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

organisationens 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 SMI följs organisationens definierade rutiner. Om en person själv vill stänga sitt användarkonto vid SMI måste denne vända sig till SMI:s expedition för att få det genomfört.

5.4.2 Vid återaktivering av en avstängd organisationsidentitet aktiverar organisationshandläggaren identiteten igen. Organisationsidentiteten är bunden till samma eduID-konto som tidigare.

Vid en säkerhetsincident stängs kontot av enligt 5.4.1. Efter att användaren informerats om säkerhetsincidenten får användaren tillbaka kontot genom att handläggaren aktiverar organisationsidentiteten enligt ovan.

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

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 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 SMI har samma tillgänglighetskrav på Identitetstjänsterna som för övriga interna tjänster inom organisationen beroende på att denna används för att logga in i flera av tjänsterna.

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 SMI följer genom eduID Connect SWAMIDs regler och best practice för konfiguration av sina Identitetstjänster.

5.6.2 Det går endast att logga in i SMI Identitetsutfärdare med aktiva användarkonton i eduID som har en organisationskoppling till SMI 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 SMI webbaserade Identitetstjänst genom eduID Connect har inte eget stöd WebSSO utan varje inloggning valideras mot eduID och följer eduID:s regelverk för WebSSO.