Senast ändrad: 2025-03-03

Hantering av elektroniska identiteter vid Blekinge Tekniska Högskola

SWAMID Identity Management Practice Statement

IT-avdelningen
Blekinge Tekniska Högskola, Postadress: 371 79 Karlskrona, Telefon: 0455-38 50 00

1. Inledning

Detta dokument är Blekinge Tekniska Högskolas Identity Management Practice Statement, nedan förkortat IMPS, för den svenska akademiska identitetsfederationen SWAMID. Dokumentet beskriver hur BTH uppfyller kraven för SWAMID AL1 och AL2.

4. Organisational Requirement

4.1 Enterprise and Service Maturity

Blekinge Tekniska Högskola, organisationsnummer 202100-4011, är en statlig myndighet vilket gör att lärosätets verksamhet regleras i lagar, förordningar och regleringsbrev. De viktigaste lagarna och förordningarna som styr 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 högskolans uppdrag under ett kalenderår. I övrigt följer lärosätet Sveriges övriga lagar och förordningar.

BTH:s katalog- och behörighetssystem innehåller uppgifter om lärosätets organisation samt personuppgifter om alla som är verksamma vid lärosätet. Dataskyddsförordningen (GDPR) och offentlighets- och sekretesslagen (SFS 2009:400) reglerar behandlingen av personuppgifter samt hantering av personer med behov av skyddade personuppgifter.

Studenters personuppgifter hämtas ur lärosätets studiedokumentationssystem Ladok eller NyA, och därför gäller även förordning (SFS 1993:1153) om redovisning av studier m.m. vid universitet och högskolor för hanteringen av studenters personuppgifter i katalog-/behörighetssystemet.

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

BTH har definierade och dokumenterade avvecklings- och utrangeringsprocesser och rutiner för servrar, hårddiskar och annan lagring. Dessa rutiner innefattar säkerställande av rensning och destruering av känslig och privat information.

4.2 Notices and User Information

“Regler för användning av BTH:s IT-resurser" bifogas ansökan. Vid varje utfärdande av ett konto godkänns regelverket av kontoinnehavaren via en webbapplikation. Varje gång en användare godkänner regelverket loggas detta. Om en uppdatering av regelverket görs så informeras samtliga användare om detta via epost. Om det sker stora förändringar i reglerna finns möjligheten att återställa samtliga berörda användarkonton vilket medför att villkoren på nytt ska godkännas.

Tjänstedefinition och integritetspolicy (SAML Policy) finns publicerade på https://www.bth.se/om-bth/myndigheten-bth/behandling-av-personuppgifter/swamid-tjanstedefinition

4.3 Secure Communications

De tjänster som ingår i ekosystemet för användare och inloggningar relaterat till SWAMID, f.n. Active Directory (AD) och Active Directory Federation Services (ADFS), driftas på dedikerade servrar som endast serverdriftpersonalen vid högskolan har åtkomst till. Åtkomsten till privata nycklar och delade hemligheter är begränsad till enbart systemets administrativa användare och respektive applikation.

All nätverkskommunikation mellan de olika systemen som ingår i ekosystemet för användare och inloggningar är skyddad och krypterad. I de allra flesta fall används TLS-protokollet för kommunikation. Alla privata nycklar för SAML och SSL/TLS är minst 2048 bitar. Replikeringen mellan domänkontrollanter sker enligt Microsofts standardiserade säkerhetsmetod för replikering.

4.4 Security-relevant Event (Audit) Records

BTH loggar samtliga händelser kopplade till ett konto, såsom skapande, aktivering, inaktivering, lösenordsbyte, lösenordsåterställning, ändring av kontots tillitsnivå samt gallring av kontoinformation. Loggar relaterade till konton skickas till BTHs egen tjänst för loggning.

Ovanstående loggar lagras under kontots fulla livstid. Övriga loggar, som exempelvis lyckade/misslyckade autentiseringar, systemloggar mm gallras efter sex månader enligt "Bevarande och gallring för handlingar av liten och kortvarig betydelse vid Blekinge Tekniska Högskola”

4.5 Incident Management

BTH följer SWAMID Incident Management Procedure vid misstänkta säkerhetsincidenter som involverar identitetsleverantör eller användare med federerade inloggningar. Vi säkerställer att alla misstänkta federerade säkerhetsincidenter hanteras enligt riktlinjerna, och vid internationella incidenter använder vi REFEDS Security Incident Response Trust Framework for Federated Identity (Sirtfi) för att hantera säkerhetsincidenter.

5. Operational Requirements

5.1 Credential Operating Environment

Lösenord vid Blekinge Tekniska Högskola måste vara minst tio tecken samt uppfylla kraven för komplexa lösenord enligt Microsofts standard i Active Directory. Detta ger en entropi om minst 24 bitar.

All kommunikation mellan de olika delarna som används för hantering av användare och lösenord sker krypterat såsom beskrivet under rubriken SWAMID AL1 4.3.3 – 4.3.4. TLS har inbyggda skydd mot återspelningsattacker (en. message replay). Replikeringen mellan domänkontrollanter i Active Directory sker enligt Microsofts standardiserade säkerhetsmetod för replikering.

I ”*Regler för användning av BTH:s IT-resurser*” (bifogat) finns tydligt angivet att kontoinnehavaren är personligt ansvarig för användningen av användarkontot och att det inte får göras tillgängligt för andra. Kontoinnehavaren godkänner alltid regelverket innan kontot används första gången.

Alla servrar som används för kontohantering och webbinloggning är uppsatta och konfigurerade så att de endast är tillgängliga på avsedda tjänsteprotokoll såsom Kerberos, LDAPS och HTTPS för reglerade IP-adresser med hjälp av brandvägg. Avdelningen för IT- och service ansvarar för att hålla servrar och annan hårdvara uppdaterade med avseende på säkerhetsproblem.

5.2 Credential Issuing

Den administrativa DNS-domänen bth.se används alltid vid attributrelease till det system där användare vill logga in. BTH använder unika entityID och eduroam-realms för SAML-IdP och eduroam-IdP.

På BTH har alla studenter som antas via Ladok möjlighet att skapa ett användarkonto. Användarkonton för anställd personal, arvodister och i vissa fall externa personer med anknytning till BTH (till exempel gästprofessorer och praktikanter) skapas av utsedda kontoadministratörer. Alla skapade användarkonton är inaktiva tills de aktivt hämtas ut i en webbapplikation av kontoinnehavaren.

Varje användarkonto på BTH har en unik användaridentitet som är kopplad till personens identitet. Användarnamnet för kontot slumpas fram i samband med att kontot skapas.

Normalt används svenskt personnummer som unik identifierare. För personer som saknar svenskt personnummer sparas personens namn och födelsedata.

Användaridentiteter för uthämtade personalkonton gallras inte med anledning av att identiteten för ett uthämtat konto inte ska kunna återanvändas för någon annan person.

Användaridentiteter för studenter gallras, men användarnamn återanvänds inte till andra personer.

För användare som har mer än ett användarkonto, till exempel både student och anställd, väljer användaren vid inloggning vilket användarkonto denna ska använda vid det aktuella tillfället.

I samband med kontoutlämning eller lösenordsåterställning kan kontoinnehavare identifiera sig på följande sätt:

1. Via inloggning mot en svensk e-legitimation med minst tillitsnivå 2 eller eduID. Matchning sker mot personnummer. Tillitsnivån från identitetsleverantören återanvänds och sätts på kontot. För att kunna nå AL2 behöver identitetsleverantören vara godkänd för AL2. För eduID gäller förutsättningarna att kontoinnehavaren har personnummer i norEduPersonNIN och AL2 i eduPersonAssurance. EPPN från identitetsleverantören sparas.
2. Med en tidsbegränsad engångskod som lämnas ut efter uppvisande av godkänd identitetshandling i BTHs reception, IT Helpdesk eller motsvarande funktion. Engångskoden används för att verifiera personens identitet i en webbapplikation. Detta ger tillitsnivå SWAMID AL2 på kontot. Identitetshandlingens nummer samt utfärdandeland sparas för icke-svenska identitetshandlingar.
3. Med en tidsbegränsad engångskod som skickas till kontoinnehavarens privata e-postadress eller mobiltelefonnummer. Detta ger tillitsnivå SWAMID AL1 på kontot. Den kanal som används sätts som verifierad för att senare kunna användas för lösenordsåterställning.
4. Med en tidsbegränsad engångskod som skickas till kontoinnehavarens folkbokföringsadress. Detta ger tillitsnivå SWAMID AL2 på kontot.
5. Med en tidsbegränsad engångskod som skickas till en av kontoinnehavaren självuppgiven adress. Detta ger tillitsnivå SWAMID AL1 på kontot.

Vid punkt 2 - 5 används CAPTCHA vid verifiering.

Med godkänd identitetshandling i punkt 2 menar vi något av följande:

- är godkänt av svenska polisen för uthämtande av pass.
- ett nationellt id-kort från ett EU/EES land som uppfyller Europaparlamentets och rådets förordning (EU) 2016/399.

- ett internationellt pass som uppfyller ICAO Doc 9303.

En höjning av tillitsnivån på kontot görs i en webbapplikation av kontoinnehavaren själv. Identifiering vid höjning av tillitsnivå görs antingen via metoden som beskrivs i punkt 1 ovan, eller via en engångskod som lämnas till kontoinnehavaren efter uppvisande av godkänd identitetshandling hos en kontoadministratör. Görs identifieringen hos en kontoadministratör kontrollerar denne att person, identitetshandling och konto stämmer överens.

Tillitsnivån på ett konto sänks från AL2 till AL1 vid lösenordsåterställning då kontoinnehavare endast använder en återställningskanal eller en engångskod som endast är utfärdad för AL1, det vill säga då identiteten inte är återverifierad. Alla förändringar i tillitsnivå på konton loggas enligt 4.4.

Identitetsuppgifter för studenter hämtas från Ladok. Identitetsuppgifter för personal kontrolleras av kontoadministratör vid skapande av konton.

Alla kontoinnehavare kan kontaktas via antingen självuppgiven e-postadress eller kontots BTH-epostadress.

Alla självuppgivna kontaktuppgifter kan uppdateras av kontoinnehavaren, antingen via en webbapplikation, via kontoadministratör eller via Ladok.

All kontoadministration görs av kontoadministratörer som loggar in med konton med tillitsnivå SWAMID AL2.

Ett kontos organisatoriska tillhörighet (affiliation) ändras ej. Alla som studerar på BTH får ett studentkonto (affiliation Student och Member). All personal på BTH får ett personalkonto (Affiliation Employee och Member). Om en person både studerar och arbetar på BTH så får denne både ett studentkonto och ett personalkonto. Om tillhörigheten inte längre är aktuell så avslutas kontot.

5.3 Credential Renewal and Re-issuing

Samtliga användare kan genomföra ett lösenordsbyte genom att ange sitt befintliga lösenord innan man anger det nya lösenordet två gånger. Det nya lösenordet måste uppfylla kraven i avsnitt 5.1.

Lösenordsåterställning kan endast ske via en webbapplikation där kontoinnehavaren först identifierar sig enligt punkt 1 - 4 i avsnitt 5.2 och därefter anger ett nytt lösenord. Detta förutsätter att återställningskanalen/-erna som används är verifierad/-e.

CAPTCHA används vid verifiering enligt punkt 2 - 4 i avsnitt 5.2.

Vid lösenordsåterställning krävs att samma identifierare som beskrivits under 5.2 används.

För att konton med tillitsnivå SWAMID AL2 ska behålla sin tillitsnivå vid återställning av lösenord gäller att kontoinnehavaren identifierar sig antingen via

- Identifiering via någon av metoderna som ger AL2 enligt 5.2.
- Tidsbegränsade engångskoder genom två återställningskanaler (e-postadress + mobilnummer) som sedan tidigare har verifierats med ett konto på tillitsnivå AL2.

5.4 Credential Revocation

För studenter:

- Vid avstängning inaktiveras kontot när en avstängning dokumenteras i Ladok, och aktiveras automatiskt igen vid avstängningens upphörande.
- Konton för studenter får en tidsstämpel baserat på slutdatum för senaste registrering på kurs och inaktiveras därefter per automatik.
- IT Helpdesk har möjlighet att inaktivera/återaktivera studentkonton.

För personal:

- Konton för anställd personal, eller andra personer relaterade till BTH, får i samband med utfärdandet ett inaktiveringsdatum baserat på när anställningen eller relationen förväntas upphöra. Kontot inaktiveras direkt i samband med att anställningen eller relationen upphör.
- Det är även möjligt för IT Helpdesk och kontoadministratörer att inaktivera konton med omedelbar verkan.

Utöver ovanstående regler så kan användare även på egen begäran få sitt konto inaktiverat, genom att ta kontakt med IT Helpdesk.

Återaktivering av konton som har inaktiverats sker enligt samma förfarande som beskrivs i avsnitt 5.2. Kontoinnehavaren får en e-postnotifiering med instruktion om hur kontot återaktiveras när aktiveringsdatum inträffar.

Vid misstänkt missbruk av konto eller vid tillämpning av disciplinära åtgärder kan användares möjlighet till inloggning spärras genom att kontot inaktiveras.

Om ett studentkonto har spärrats så informeras studenten via privat e-postadress om anledningen, lämpliga åtgärder att vidta och vad som krävs för att kontot ska återaktiveras.

Om ett personalkonto har spärrats informeras kontoinnehavare via telefonsamtal till dennes BTH-mobilnummer eller via besök i IT Helpdesk om anledningen, lämpliga åtgärder att vidta och vad som krävs för att kontot ska återaktiveras. Efter att lämpliga åtgärder vidtagits eller efter avstängningsperiodens slut kan kontot återaktiveras enligt de rutiner som beskrivs i avsnitt. 5.2. För att förhindra att incidenter inträffar igen informeras användaren om hur kontot används på ett säkert sätt och vilka eventuella skyddsåtgärder som kan vidtas.

Om ett inaktiverat konto inte ska kunna återaktiveras av användaren, så är det inte heller möjligt för användaren att göra det.

Om ett konto behöver inaktiveras på grund av en incident så går detta via BTHs CSIRT. Teamet har etablerade arbetsrutiner för att kontinuerligt förbättra processer så att liknande incidenter inte behöver upprepas.

5.5 Credential Status Management

BTH loggar samtliga händelser kopplade till ett konto, såsom skapande, aktivering, inaktivering, lösenordsbyte, lösenordsåterställning, ändring av kontots tillitsnivå samt gallring av kontoinformation. Samtliga händelseloggar sparas enligt punkt 4.4.

Inloggningstjänsten för SAML2 har designats för en tillgänglighet på 99% för inloggning mot interna system.

5.6 Credential Validation/Authentication

Samtliga installationer av identitetshanterare och protokoll på BTH är konfigurerade enligt SWAMID:s rekommendationer och instruktioner för best practice. Detta innebär att BTH uppfyller samtliga krav för inloggning, autentisering och behörighetskontroll, samt giltighetstid för SSO-sessioner för SAML2-baserad webbinloggning. Giltighetstiden för SSO-sessioner är aldrig giltiga mer än 12 timmar. Användaren måste presentera sitt lösenord vid inloggning.

Vid lösenordsbyte ersätts det tidigare lösenordet och därmed kan det inte längre användas för inloggning.

När ett konto inaktiveras (stängs av, upphör eller spärras) är det inte längre möjligt att logga in eller få tillgång till system och tjänster enligt standardfunktionalitet i Active Directory.