Document KTH Identity Management Practice Statement
Version V2.0
Last modified 2024-03-01
Pages 18
Status FINAL

KTH Royal Institute of Technology

Identity Management Practice Statement

1. Inledning

KTH är Sveriges största universitet för teknisk forskning och utbildning. På KTH finns sedan 2001 ett gemensamt identitetshanteringssystem, KTH:s centrala användardatabas UG, Users and Groups som hanterar konto- och användaruppgifter. KTH är sedan 2008 medlem i SWAMID.

KTH har sedan dess godkänts för utfärdande av TCS personliga certifikat och Swamid 2.0.

Dokumentet är framtaget för att ansöka om/uppdatera medlemskap enligt tillitsnivå SWAMID AL1 och AL2.

4. Organisational Requirement

The purpose of this section is to define conditions and guidance regarding participating organizations responsibilities.

4.1 Enterprise and Service Maturity

KTH, organisationsnummer 202100-3054, 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), högskolelagen (SFS 1992:1434), högskoleförordningen (1993:100), förvaltningslagen (SFS 2017:900), tryckfrihetsförordning (SFS 1949:105), offentlighets- och sekretesslagen (SFS 2009:400), arkivlagen (SFS 1990:782) och myndighetsförordningen (SFS 2007:515). 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 UG 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. Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning, förordning (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning reglerar, utöver de regler som finns i GDPR, behandlingen av personuppgifter. I offentlighets- och sekretesslagen (SFS 2009:400) finns också bestämmelser om sekretess för olika kategorier av personuppgifter som kan tillämpas bland annat vid hantering av uppgifter avseende personer med behov av skyddade personuppgifter.

Studenters personuppgifter hämtas ur lärosätets studiedokumentationssystem Ladok och därför gäller även förordning (SFS 1993:1153) om redovisning av studier m.m. vid universitet och högskolor för hanteringen av studenters personuppgifter i UG.

Som statlig myndighet arbetar lärosätet även med ledningssystem för informationssäkerhet enligt Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6).

4.1.3 Rutiner för destruering av lagringsmedia (4.1.3)

Systemadministratörer på IT-avdelningen ansvarar alltid för att all data på lagringsmedia som tas ur drift raderas på ett tillbörligt sätt. Detta gäller naturligtvis även diskar från KTH:s IdP.

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.

Till denna ansökan inkluderas (i länkform):

1. Acceptable User Policy (AUP) - Ansvarsförbindelse KTH
2. Password policy - Lösenordsregler vid KTH
3. Privacy policy
4. Service definition

Acceptable User Policy (AUP) – Ansvarsförbindelse KTH finns tillgänglig på KTH:s webbplats på följande länk, https://intra.kth.se/administration/blanketter/it-tele.

KTH's Password policy - Lösenordsregler vid KTH finns tillgänglig på KTH:s intranät på följande länk: https://intra.kth.se/it/natverk/identitetshantering.

KTH:s Privacy Policy återfinns på KTH:s Intranät på följande länk: Information om behandling av personuppgifter vid användning av KTHs IT-stöd | KTH Intranät.

SWAMID Service definition kan hittas på KTH:s intranät på följande länk: https://intra.kth.se/it/natverk/identitetshantering.

Ansvarsförbindelsen undertecknas av användaren digitalt när kontot aktiveras och kontot lämnas ut. Sedan sommaren 2023 har KTH infört en ny digital kontoaktiveringslösning där användarna aktiverar sitt konto, signerar och godkänner ansvarsförbindelsen med hjälp av Svensk e-legitimation på tillitsnivå 3 eller högre. För personer som inte har möjlighet att legitimera sig med hjälp av Svensk e-legitimation på tillitsnivå 3 eller högre så använder vi aktiveringskoder som lämnas ut från våra service center efter genomförd legitimationskontroll.

Vid förändring av ansvarsförbindelsen kommer information om detta skickas ut till användarna via e-post.

Det är värt att notera att lösenordshanteringen på IdP-maskiner vida överstiger vad som generellt fastslås i KTH:s lösenordspolicy.

4.3 Secure Communications

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

De tjänster som ingår i KTH:s identitets- och behörighetssystem driftas på servrar som endast ett fåtal definierade driftpersoner har åtkomst till. Åtkomsten till privata nycklar och delade hemligheter är begränsat till endast systemets administrativa användare och respektive applikation. Detta gäller även i de fall då privata nycklar i klartext och delade hemligheter förekommer.

All nätverkskommunikation mellan de olika komponenterna som ingår i lärosätets identitets- och behörighetssystem är krypterad med moderna versioner av TLS (version 1.2) och vi använder oss primärt av moderna TLS chiffersvit för denna kommunikation. Alla privata nycklarna är minst 2048 bitar.

Vi har även stängt av osäkra cipher suites på systemen som ingår i vårt identitets- och behörighetssystem.

4.4 Security-relevant Event (Audit) Records

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

Alla förändringar som genomförs i UG (KTH:s interna IAM system) på en användare eller grupp loggas och sparas i en transaktionslogg. Följande data loggas i transaktionsloggen:

- Objekt som ändras
- Vad som ändrades
- Vem som gjorde ändringen
- Från vilket systemförändringen gjordes
- Unikt versionsnummer för ändringen
- Datum och tid när ändringen genomfördes

Transaktionsloggen över händelser samt databasen replikeras till annan server så att alla förändringar kan återspelas vid behov. All relevant logginformation (inloggning/säkerhetsloggar) för systemen som ingår i IdP-miljön skickas vidare till den centrala loggservermiljön som hanteras av den centrala IT-avdelningen på KTH. Loggar hanteras enligt KTH:s dokumenthanteringsplan, https://intra.kth.se/administration/dokument/informationshanteringsplan, och är endast tillgängliga för behörig personal.

Samtliga händelser i universitetets identitets- och behörighetssystem loggas och behörig IT-personal kan verifiera loggar i efterhand

- Loggning av säkerhetsrelaterade händelser, exempelvis inloggningar i identitetstjänsten, lösenordsbyten lagras i den centrala logglösningen.

5. Operational Requirements

The purpose of this section is to ensure safe and secure operations of the service.

5.1 Credential Operating Environment

KTH övervakar kontinuerligt den tekniska infrastrukturen via en dedicerad IT-säkerhetsfunktion. Denna har befogenheten att inaktivera samtliga konton som misstänks ha kommit i orätta händer eller som använts på ett sätt som strider mot antagna regler.

5.1.1 Lösenord i UG

Basen för lösenordkomplexitet på KTH är "Microsofts password complexity requirement" eftersom lösenorden lagras i den gemensamma Active Directory miljön på KTH.

Användarnas lösenord måste uppfylla följande krav:

- Lösenordet måste bestå av minst 12 tecken
- Det måste innehålla minst en gemen: a-z
- Det måste innehålla minst en versal: A-Z
- Det måste innehålla minst en siffra: 0-9
- Det får inte innehålla tre eller fler sammanhängande tecken från ditt användarnamn, förnamn, efternamn, födelsedatum eller personnummer
- Det får inte innehålla mellanslag

5.1.2 Vilka tekniska protokoll som används

Följande protokoll används i KTH:s mijö för inloggning

Mot SWAMID

- SAML2 – Används för inloggning mot SWAMID och webbtjänster som inte stöder OpenID Connect

Mot interna system

- Kerberos används för autentisering av användare från våra managerade klient- och servermiljöer
- NTLMv2 – Används av vissa av våra legacy tjänster som tex printlösning
- LDAPS (TLS) – Används för autentisering av användare för applikationer som inte stödjer OIDC eller SAML2
- OpenID Connect – Vårt primära protokoll för inloggning i våra egenutvecklade applikationer och införskaffade tjänster
- SAML2 – Används för inloggning mot SWAMID och webbtjänster som inte stöder OpenID Connect

5.1.3 Rutiner för information till användarna rörande missbruk

Ansvarsförbindelsen informerar användaren om tillåten användning och påföljder vid avsteg från detta. Ansvarsförbindelsen speglar den skrivelse SUNET/SWAMID själva har publicerat.

5.1.4 Rutiner för tekniskt skydd mot missbruk

KTH övervakar kontinuerligt den tekniska infrastrukturen via en dedicerad IT-säkerhetsfunktion. Denna har befogenheten att inaktivera samtliga konton som misstänks ha kommit i orätta händer eller som använts på ett sätt som strider mot antagna regler. Vi spärrar konton efter 15 antal felaktiga inloggningar och spärrningen av kontot gäller i 15 minuter.

Samtliga komponenter den tekniska infrastrukturen omfattas av kontinuerlig och skyndsam hantering av systemuppdateringar. KTH arbetar systematiskt med att hålla samtliga komponenter i miljön aktuella och säkerhetsuppdaterade.

Interna applikationer som inte underhålls tillgängligörs inte via SWAMID.

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.

Konton i UG lämnas ut efter genomförd identitetskontroll eller legitimering med Svensk e-legitimation på tillitsnivå 3 eller högre (vidare Svensk e-legitimation på tillitsnivå 3 eller högre).

Användare som har möjlighet att använda sig av Svensk e-legitimation på tillitsnivå 3 eller högre aktiverar sitt KTH konto och godkänner KTH:s ansvarsförbindelse digitalt.

Användare som inte har möjlighet att legitimera sig med Svensk e-legitimation på tillitsnivå 3 eller högre måste besöka något av KTH:s IT-supportcenter eller servicenter och genomföra en identitetskontroll. Efter kontrollen är genomförd så får användaren en unik aktiveringskod som gäller i 24 timmar. Användaren använder denna aktiveringskod och sitt födelsedatum för att aktivera sitt konto och godkänna KTH:s ansvarsförbindelse digitalt.

Datum för godkännande av ansvarsförbindelsen och AL-nivån lagras i UG som värden på användaren.

Vi bedömer att KTH:s rutiner säkerställer minst tillitsprofil AL2 för samtliga användare.

Tillitsprofilen för ett konto kan höjas genom att man legitimerar sig på plats genom att besöka något av KTH:s IT supportcenter eller servicenter eller genom att använda sig av vår selfservice applikation och legitimera sig med Svensk e-legitimation på tillitsnivå 3 eller högre.

Från och med den 28:e juni så måste alla användare antingen användas sig av Svensk e-legitimation på tillitsnivå 3 eller högre för att hämta ut ett konto eller besöka något av våra service center med vissa undantag.

Undantagen begränsade till enstaka kurser för icke nationella studenter så fått dispans. Dessa studenter får tillitsprofil AL1 på sina konton.

5.2.1 Identitetsutfärdarens administrativa domän i SWAMID (”Scope”) som används för att unikt knyta användare till organisation

Vi använder oss av kth.se som scope i SWAMID.

5.2.2 Identitetsutfärdarens globalt unika identifierare

KTH har globalt unika identifierare för våra två IdP:er. Detsamma gäller för de RADIUS-servrar som används inom eduroam.

5.2.3 Varje användare ska ha ett eller flera unika användarnamn som inte får återanvändas för andra användare

Varje användare har ett unikt användarnamn i UG.

5.2.4 Om användare har fler än ett användarkonto ska de kunna välja vilken de använder vid inloggning, exempelvis ett studentkonto och ett anställdkonto

Varje användare har ett unikt konto i vår miljö.

5.2.5 Rutiner för utdelande av kontouppgifter (5.2.5)

Mer information om hur vi lämnar ut konton finns på följande länk, https://intra.kth.se/it/kth-se-konto/kth-konto-1.471319 och mer information om giltiga id-handlingar som är godkända för legitimering på KTH finns på följande länk, https://www.kth.se/student/it/kth-account/acceptable-forms-of-identification-at-kth-1.738834.

Inga konton lämnas ut utan att det genomförts en legitimationskontroll.

5.2.5.1 Vilka identifieringsmetoder som används vid vilka tillfällen

Vid KTH finns tre sätt att dela ut ett konto

a) med hjälp av Svensk e-legitimation på tillitsnivå 3 eller högre

b) med hjälp av aktiveringskod som erhålls efter på-plats identitetskontroll och legitimering, där identitetskontroll och legitimation görs med samtliga legitimationshandlingar som är godkända på KTH, dessa finns dokumenterade på följande länk, https://www.kth.se/student/it/kth-account/acceptable-forms-of-identification-at-kth-1.738834 (samt bifogat med ansökan)

c) med aktiveringskod på distans där användaren inte varit på plats när identitetskontroll gjorts.

Samtliga metoder för utlämning av konto innefattar antingen programmatiska kontroller av fördefinierade identifierare eller manuell kontroll.

Vid aktivering av konto görs kontroll av de identifierare som kommer med inloggningen via den tidigare nämnda godkända legitimationslösningen mot de värden som finns i KTH:s IAM-system där informationen kommer från lärosätets studiedokumentationssystem och/eller lärosätets masterdata-system för personalinformation.

För metod a så kontrollerar vi det tolvsiffriga personnumret.
För metod b och c så kontrollerar vi det tiosiffriga personnumret för personer med giltiga svenska legitimationshandlingar. För personer utan svenska

legitimationshandlingar så använder vi oss av födelsedata som identifierare tillsammans med deras förnamn och efternamn.

En användare MÅSTE legitimera sig för att kunna aktivera sitt konto enligt metod b och c. Om man inte kan legitimera sig så kan man inte aktiveringskod lämnas ut.

KTH gör skillnad på konton som lämnas ut på distans där ingen fysisk verifikation av legitimationshandling görs jämfört med om fysisk verifikation görs (metod c jmf metod b), såsom beskrivs ovan. Ett konto som delas ut enligt metod c ovan tilldelas tillitsprofil AL1.

5.2.5.2 Resulterande tillitsnivåer beroende på identifieringsmetod

- Legitimering med Svensk e-legitimation på tillitsnivå 3 eller högre - AL2
- Aktiveringskod med på-plats identitetskontroll och legitimering - AL2
- Aktiveringskod där användaren inte varit på plats när man gjort identitetskontrollen och legitimeringen – AL1

5.2.5.3 Eventuella skillnader mellan anställda och studenter

Vi har inga skillnader i hanteringen av anställda och studenter i våra processer. Vi importerar t.ex. ingen privat e-postadress eller telefonnummer från Ladok till KTH:s IAM-system då datakvalitén på denna information ej går att säkerställa.

5.2.5.4 Vilka typer av användarkonton som exponeras mot SWAMID, om det inte gäller alla användarkonton

Vi exponerar primärt alla verifierade användarkonton mot SWAMID. I vissa undantag så exponerar vi även personliga systemkonton för tjänster som inte vill ha personliga konton med administrativa rättigheter, tex administrationskontot för Box tjänsten. Dessa personliga konton ägs av en person på KTH. Detta för att en användares personliga konto inte har administrativa rättigheter i tjänster som konsumeras av KTH enligt Least Priviliged-modellen.

5.2.5.5 Vilka föreregistrerade identifierare som förekommer och hur de kontrolleras vid identifiering

Personnummer – Maskinellt med Svensk e-legitimation på tillitsnivå 3 eller högre och manuellt vid aktiveringskod.

Födelsedata, förnamn och efternamn i kombination - Riskbaserad manuell bedömning vid legitimering där personnummer saknas.

5.2.5.6 Hur eventuell legitimationskontroll utförs och hur den dokumenteras kopplat till tillitsnivå

Legitimationskontroll gör antingen manuellt av specifik KTH personal, eller via Svensk e-legitimation på tillitsnivå 3 eller högre. Vi lagrar för tillfället inte metoden för verifiering men vi har det i vår backlog att ta lagra denna information i vår transaktionslog i framtiden.

5.2.6 Hur eventuellt byte av tillitsnivåer för användare hanteras

Tillitsnivåer kan bara ändras genom att användaren besöker något av KTH's IT-supportcenter eller service center och genomföra en identitetskontroll eller genom att använda sig av vår self service applikation och legitimera sig med Svensk e-legitimation på tillitsnivå 3 eller högre.

Samtliga kontohändelser relaterade till tillitsnivåer loggas i ett separat loggsystem frikopplat från kontoaktiveringsapplikationen. Förändringar av tillitsnivån loggas även i UG (KTH:s interna IAM system).

Användare som använder metod c kommer att få sin tillitsnivå satt på nivå 1, oavsett vilken nivå de hade tidigare.

5.2.7 Ändring av eventuell självuppgiven information, exempelvis privat e-postadress

Användare kan inte ändra sin information själv utan hänvisas till ändring i källsystemen.

5.2.8 Krav på tillitsnivå vid all kontoadministration

Alla användare som skall administrera konton måste ha AL2 nivå på sitt konto för att kunna skapa/byta lösenord/höja AL-nivå på ett konto.

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 Användares frivilliga byte av lösenord och andra inloggningsfaktorer

Samtliga användaren kan själv byta lösenord med hjälp av Svensk e-legitimation på tillitsnivå 3 eller högre via vår self-service applikation. Vi tillåter inte användaren att byta lösenord även om det tidigare lösenordet är känt. I de fall användaren behöver byta sitt lösenord betraktar vi det som en lösenordsåterställning och kräver fullständig validering av identifikationen enligt tidigare beskrivna rutiner.

Användare som aktiverat sitt konto med metod b från 5.2.5.1 och som inte har möjlighet att legitimera sig med Svensk e-legitimation på tillitsnivå 3 eller högre måste besöka antingen KTH:s IT-Support eller något av våra servicecenter för att legitimera sig och få en aktiveringskod för att kunna byta sitt lösenord. Aktiveringskoden kan sedan användas för att byta lösenord på kontot via self-service applikationen.

Användare som aktiverat sitt konto med metod c från 5.2.5.1 som inte har möjlighet att legitimera på plats med Svensk e-legitimation på tillitsnivå 3 eller högre måste kontakta KTH:s IT-Support eller något av våra servicecenter för att legitimera sig och få en aktiveringskod för att kunna byta sitt lösenord. Aktiveringskoden kan sedan användas för att byta lösenord på kontot via self-service applikationen.

5.3.2 Användare MÅSTE aktivt visa att de innehar aktuella behörigheter i processen för förnyelse av aktuellt lösenord och andra inloggningsfaktorer

Användaren kan inte återställa sitt lösenord eller andra inloggningsfaktorer själv med hjälp av befintliga lösenord eller andra lösenord faktorer då återställning av lösenord behandlas likt en kontoaktivering. I KTH:s avseende så kommer samtliga och samma fördefinierade identifierare som användes vid kontoaktiveringen att användas vid återställning.

5.3.3 Återställning av användares lösenord och andra inloggningsfaktorer

Vi har möjlighet att återställa användarens lösenord vid behov.

Då återställning av lösenord behandlas likt en kontoaktivering i KTH:s avseende så kommer samtliga och samma fördefinierade identifierare som användes vid kontoaktiveringen att användas vid återställning.

5.4 Credential Revocation

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

Användare kan även begära deaktivering av sitt konto när de själva önskar oavsett status på KTH. Användaren kan begära deaktivering genom att besöka IT-supporten.

5.4.1 Hur ett användarkonto spärras när användaren lämnar organisationen eller om ett användarkonto missbrukas

Om ett konto missbrukas kan det genom olika processer i IT-avdelningens säkerhets- och kontohantering spärras för inloggning. Denna spärr omöjliggör dessutom användaren att återaktivera sitt konto på egen begäran.

Med användare så menar vi studenter, anställda eller affilierade personer som har ett konto på KTH.

Med termen "inaktiva konton" avses situationer där ett konto fortfarande är aktivt i KTH:s identitetssystem och tekniskt sett kan användas för att logga in, men i praktiken inte används av någon användare. KTH har fastställt interna riktlinjer för att avgöra när ett konto anses vara inaktivt. När en användare lämnar organisationen så finns ett antal scenarier som kan inträffa som beskrivs nedan men den generella riktlinjen är att inga konton gallras per automatik:

1. Man kan beställa deaktivering av ett specifikt konto vid avslut av anställning. Detta görs av ansvarig chef.
   Användare kan även begära deaktivering av sitt konto när de själva önskar.
2. Deaktivering av inaktiva konton görs 1 gång om året. Detta sker som rutin och utförs av dedikerade personer vid IT-avdelningen.
3. Manuellt om kontot misstänks vara komprometterat. Detta hanteras inom ramen för gängse rutiner för säkerhetsincidenter.
4. Manuellt om kontot spärras av andra säkerhetsskäl såsom överträdelse av regler. Detta hanteras inom ramen för gängse rutiner för säkerhetsincidenter.
5. Lösenordet ändras av systemadministrativa skäl.

När en användare lämnar organisationen så tas alla affilieringar bort från användarens konto och eduPersonScopedAffiliation skickas inte vidare till SWAMID federationen.

Radering av konton:

Värt att nämna är att KTH inte raderar några konton i enlighet med ett rektorsbeslut. Ett konto förblir aktivt även om en anställning upphör. Vi uppmuntrar dock å det starkaste att deaktivering görs. När ett konto deaktiveras kan användaren ej längre logga in i systemen.

I de fall ett konto faktiskt raderas kommer användarnamnet att spärras och hindras från att användas igen. Denna rutin säkerställs av regelverk i KTH:s IAM-system.

5.4.2 Hur ett användarkonto återaktiveras efter att tidigare ha varit spärrat och hur användare informeras vid säkerhetsincidenter

Konton återaktiveras antingen genom att det antingen kommer in en beställning för återaktivering eller att användaren börjat studera eller fått anställning.

Om kontot uppfyller kraven ovan så kan användaren besöka KTH:s IT-support eller Servicecenter och få en aktiveringskod eller så kan användaren aktivera sitt konto med en Svensk e-legitimation som uppfyller minst LoA3-nivå.

En användare vars konto har blivit spärrat behöver ta kontakt med användarstödet/Supporten för att få kontot återaktiverat. Vid kontakt blir användaren informerad om orsaken till att kontot blivit spärrat så att denne kan undvika att göra samma misstag igen.
De förregisterade identifierare som vi använder finns beskrivna under punkt 5.2.5.5.

5.4.3 Hur medlemsorganisationen minimerar risken för att säkerhetsincidenter återupprepas

Baserat på vilken typ av incident som inträffat så vidtar vi åtgärder för att mitigera och som minimerar risken för en framtida incident.

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 Att ett register upprätthålls över samtliga utfärdade identiteter

Alla identiteter som någonsin skapas lagras i UG.

5.5.2 Att medlemsorganisationen har en tillgänglighet på sin identitetsutfärdare som medger att den kan användas för inloggning till interna system

Ja, vår identitetsutfärdare används även för inloggning på interna system.

5.6 Credential Validation/Authentication

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

Beskriv nedan i löptext hur medlemsorganisationen uppfyller avsnittet. Tänk på att följande punkter skall beskrivas

5.6.1 The Identity Provider MUST provide validation of credentials to a Relying Party using a protocol that

Vi implementerar SAML2 protokollet enligt SWAMID:s best practises.

5.6.2 The Identity Provider MUST not authenticate credentials that have been revoked.

Användare kan endast autentisera sig med ett giltigt lösenord mot KTH:S IDP.

5.6.3 The Identity Provider MUST force the Subject to demonstrate possession of current credentials in the process of authentication.

Användare MÅSTE autentisera sig med ett giltigt lösenord mot IDP:n.

5.6.4 The Identity Provider MUST force the Subject to authenticate at least once every 12 hours in order to maintain an active session.

Användare som använder sig av KTH:s IDP måste autentisera sig var 12:e timme.

5.6.5 Konfigurationer och protokoll som ej täcks av SWAMIDs rekommenderade best practice

Se avsnitt 5.1.2 för detaljer.