

4.4 Implementera krav på tillitsnivå samt ev. multifaktor vid inloggning

Vid inloggning till en tjänst som kräver en viss tillitsnivå eller kräver multifaktorsinloggning behöver ett antal kontroller göras. Om någon kontroll misslyckas ska användaren informeras om hur den bäst löser problemet.

- [Tillitsnivåer och autentiseringskrav](#)
 - [SWAMIDs tillitsnivåer](#)
 - [Internationella tillitsnivåer - REFEDS Assurance Framework \(RAF\)](#)
 - [Särskilda autentiseringskrav i inloggningsbegäran](#)
 - [Tekniska kontroller efter svar på inloggningsbegäran](#)
- [Teknisk implementation baserat på krav om SWAMID AL2](#)
- [Teknisk implementation baserat på krav om multifaktorinloggning och åsidosättande av single sign-on](#)

Tillitsnivåer och autentiseringskrav

SWAMIDs tillitsnivåer

I SWAMID finns tre tillitsnivåer beslutade och samtliga identitetutfärdare (IdP) är godkända för en eller fler av dessa.

Tillitsnivå	Identifierare	Grundkrav på användare	Autentiseringskrav
SWAMID AL1	http://www.swamid.se/policy/assurance/al1	Det är en person som innehar och använder kontot	1-faktors- eller multifaktorinloggning ¹
SWAMID AL2	http://www.swamid.se/policy/assurance/al2	Det är en identifierad person som innehar och använder kontot	1-faktors- eller multifaktorinloggning ¹
SWAMID AL3	http://www.swamid.se/policy/assurance/al3	Det är en identifierad och legitimerad person som innehar och använder kontot	Enbart multifaktorinloggning

¹ Med 1-faktorsinloggning menas inloggning med lösenord eller lösenordsfri inloggning med hjälp av t.ex. WebAuthn Credential. Vid multifaktorsinloggning är det kraven i SWAMIDs tillitsprofiler som reglerar vad som är en godkänd multifaktorinloggning.

För att kontrollera om en identitetsutgivare är godkänd för en viss tillitsnivå i SWAMID behöver tjänsten titta i metadataattributet **Meta-Assurance-Certification**. Attributet är multivärt och innehåller samtliga tillitsnivåer som tjänsten är godkänd för, t.ex. både <http://www.swamid.se/policy/assurance/al2> och <http://www.swamid.se/policy/assurance/al1> om identitetutfärdare är godkänd för SWAMID AL2.

Vilken tillitsnivå en specifik användare har finns angivet i attributet **eduPersonAssurance**.

Internationella tillitsnivåer - REFEDS Assurance Framework (RAF)

Inom eduGAIN används inte SWAMID tillitsnivåer utan [REFEDS Assurance Framework \(RAF\)](#). Dessa är inte lika omfattande som SWAMIDs tillitsnivåer men det går ur perspektivet identifierade användare att definiera motsvarande nivå.

Tillitsnivå	Identifierare ²	Motsvarar grundkrav för användare	Autentiseringskrav
RAF IAP Low	https://refeds.org/assurance/IAP/low	SWAMID AL1	1-faktors- eller multifaktorinloggning ³
RAF IAP Medium	https://refeds.org/assurance/IAP/medium https://refeds.org/assurance/profile/cappuccino	SWAMID AL2	1-faktors- eller multifaktorinloggning ³
RAF IAP High	https://refeds.org/assurance/IAP/high https://refeds.org/assurance/profile/espresso	SWAMID AL3	1-faktors- eller multifaktorinloggning ³

² När mer än en identifierare visas kan en IdP använda någon av dem, eller båda.

³ Med 1-faktorsinloggning menas inloggning med lösenord eller lösenordsfri inloggning med hjälp av t.ex. WebAuthn Credential. Vid multifaktorsinloggning är det kraven i REFEDS MFA som reglerar vad som är en godkänd multifaktorinloggning.

I REFEDS Assurance Framework finns inget krav på att en identitetsutgivare granskas innan de får använda tillitssignalering och därför går det inte att i metadata se vad en identitetsutgivare är godkänd för men användarens uppgivna tillitsnivå finns i attributet **eduPersonAssurance**.

Särskilda autentiseringskrav i inloggningsbegäran

1. **Om multifaktorinloggning krävs:** Inom SWAMID används signalering enligt REFEDS Multi-Factor Authentication Profile (REFEDS MFA). Begär att multifaktorinloggning används genom att i attributet **RequestedAuthnContext** ange värdet **<https://refeds.org/profile/mfa>** i Authentication Request.
2. **Om Single Sign-On inte får användas:** Begär att ny inloggning används genom att i attributet **ForceAuthn** ange värdet **true** i Authentication Request.

- För att åsidosättande av Single Sign-On ska fungera korrekt måste alla godkända inloggningsmetoder vara definierade i attributet **RequestedAuthnContext**, t.ex. <https://refeds.org/profile/mfa>, <https://refeds.org/profile/sfa> och **urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport** för både multifaktor- och singelfaktorinloggning. Vissa identitetsutgivarprogramvaror kan luta sig tillbaka på operativsysteminloggningen om det inte explicit pekas ut vilka inloggningsmetoder som är godkända.

Tekniska kontroller efter svar på inloggningsbegäran

1. **Om multifaktorinloggning krävs:**
 - Kontrollera att attributet **AuthnContext** i Authentication Response från IdP är <https://refeds.org/profile/mfa>.
2. **Om Single Sign-On inte får användas:**
 - Kontrollera att attributet **AuthnInstant** i Authentication Response från IdP är färsk, dvs. inte äldre några minuter (t.ex. 5 minuter).
3. **Om aktuell IdP är registrerad i SWAMID (registrationAuthority är <http://www.swamid.se/>) och tillitsnivå krävs:**
 - Kontrollera att IdP:n uppfyller vald tillitsnivå via metadata attributet **assurance-certification**.
4. Kontroll att identifierande attribut följer med (t.ex. något av attributen **eduPersonPrincipalName/eppn** eller **subject-id**).
5. **Om tillitsnivå krävs:**
 - Kontrollera att användaren uppfyller vald tillitsnivå genom att titta på värdena i attributet **eduPersonAssurance**.

Om användaren inte uppfyller ett eller flera av angivna krav rekommenderas att användaren får en bra felinformationssida och hänvisas till sin identitetsutfärdare för mer hjälp. Inom SWAMID krävs att alla identitetsutfärdare använder metoden **errorURL** i metadata för att en tjänst ska peka användaren till rätt hjälp, se [Service Provider error handling during federated login](#) för mer information.

Teknisk implementation baserat på krav om SWAMID AL2

Instruktionerna nedan är skrivna för Shibboleth Service Provider. Motsvarande behöver göras för annan SP-programvara.

Referenssidor:

- [3.2 Configure Shibboleth SP - attribute-map.xml](#)
- [3.3 Configure Shibboleth SP - Check for Identity Assurance or REFEDS SIRTfi](#)
- [Kravställning vid inloggning](#)
- [Service Provider error handling during federated login](#)

1. Kontroll om att IdP:n uppfyller SWAMID AL2

Se [3.3 Configure Shibboleth SP - Check for Identity Assurance or REFEDS SIRTfi#3](#).

[3ConfigureShibbolethSPCheckforIdentityAssuranceorREFEDSSIRTfi-GetassuranceprofilesfrommetadataintheShibbolethServiceProvider](#) för att säkerställa att **Meta-Assurance-Certification** följer med som ett attribut till applikationen.

Metadataattributet **Meta-Assurance-Certification** är en lista med certifieringar som IdP:n har i metadatan. Listan är typiskt en semikolonseparerad sträng, exempel:

```
http://www.swamid.se/policy/assurance/al1;http://www.swamid.se/policy/assurance/al2;https://refeds.org/sirtfi
```

Kontrollera att exakt <http://www.swamid.se/policy/assurance/al2> finns i listan. Om så inte är fallet så är det lämpligt att meddela användaren att IdP:n inte är godkänd för **SWAMID AL2**, uppmana användaren att uppmana sin IdP att ordna med detta samt eventuellt att hänvisa till eduID där alla med svenskt personnummer kan uppnå **SWAMID AL2**. En **errorURL** bör även presenteras för användaren med kod **AUTHORIZATION_FAILURE** och URL:en till **SWAMID AL2** som kontext:



Din inloggningstjänst uppfyller inte tillitsnivån SWAMID AL2.

För tillgång till tjänsten så behöver både ditt lärosäte och ditt användarkonto uppfylla [SWAMID Identity Assurance Level 2 Profile](#).

Vilka lärosäten och inloggningstjänster som gör detta framgår i [SWAMID:s medlemslista](#).

Kontakta IT-support eller motsvarande för ditt lärosäte och uppmana dem att implementera tillitsnivån **SWAMID AL2** så att tjänster i SWAMID säkert kan identifiera dig.

Din inloggningstjänst tillhandahåller denna informationssida som kan hjälpa dig att lösa detta problem: <https://idp.example.se/ErrorMessage>

I väntan på att ditt eget lärosäte implementerar SWAMID AL2 så kan du skapa ett eduID-konto på eduID.se och där bekräfta din identitet. I och med det så lyfter du då upp ditt eduID-konto till SWAMID AL2 och kan få tillgång till tjänsten via ditt konto på eduID.

Ditt användarnamn: abcdef01@example.se.

ErrorURL:en ovan ska då peka på https://idp.example.se/ErrorMessage/?errorurl_code=AUTHORIZATION_FAILURE&errorurl_ts=...&errorurl_rp=...&errorurl_tid=...&errorurl_ctx=http://www.swamid.se/policy/assurance/al2. Se [Service Provider error handling during federated login](#) för mer information om **errorURL**.

2. Kontroll om att identifierande attribut följer med

Kontrollera att de attribut som krävs av tjänsten har ett värde. Detta kan typiskt röra sig om **eduPersonPrincipalName** som ofta används som användarnamn i tjänster, eller kanske **norEduPersonNIN** eller **personalIdentityNumber**. Om attribut saknas så är det lämpligt att meddela användaren att IdP:n inte skickar attributen som krävs för att identifiera dig, hänvisa användaren till sin support via IdP:ns **errorURL**, med kod **IDENTIFICATION_FAILURE** och entitetskategori (samt eventuellt specifikt attribut) som kontext:



Din inloggningstjänst skickade ingen identitet

Ingen identitet skickades med vid inloggning. Kontakta IT-support eller motsvarande för ditt lärosäte eller din inloggningstjänst för hjälp.

Din inloggningstjänst tillhandahåller denna informationssida som kan hjälpa dig att lösa detta problem: <https://idp.example.se/ErrorUrl>

Teknisk information: **eduPersonPrincipalName (epn)** saknas

ErrorURL:en ovan ska då peka på https://idp.example.se/ErrorUrl/?errorurl_code=IDENTIFICATION_FAILURE&errorurl_ts=...&errorurl_rp=...&errorurl_tid=...&errorurl_ctx=http://refeds.org/category/research-and-scholarship,%20eduPersonPrincipalName.

3. Kontroll om att assurance-attributet följer med från IdP:n

Förutom de direkt identifierande attributen så behöver även kontroll göras att **assurance**-attributet följer med. IdP:er kan vara konfigurerade att släppa användarnamn och personnummer men specifikt inte **assurance**. Alla användare i SWAMID måste uppfylla minst **SWAMID AL1** så frånvaro av attributet beror sannolikt på att IdP:n inte alls släpper attributet. Om attribut saknas så är det lämpligt att meddela användaren att IdP:n inte skickar tillitsnivå, hänvisa användaren till sin support via IdP:ns **errorURL**, med kod **IDENTIFICATION_FAILURE** och entitetskategori (samt eventuellt **eduPersonAssurance**) som kontext:



Din inloggningstjänst skickade ingen tillitsnivå

Ingen tillitsnivå skickades med vid inloggning. Kontakta IT-support eller motsvarande för ditt lärosäte eller din inloggningstjänst för hjälp.

Din inloggningstjänst tillhandahåller denna informationssida som kan hjälpa dig att lösa detta problem: <https://idp.example.se/ErrorUrl>

Teknisk information: **eduPersonAssurance** saknas

ErrorURL:en ovan ska då peka på https://idp.example.se/ErrorUrl/?errorurl_code=IDENTIFICATION_FAILURE&errorurl_ts=...&errorurl_rp=...&errorurl_tid=...&errorurl_ctx=http://refeds.org/category/research-and-scholarship,%20eduPersonAssurance.

4. Kontroll om att användaren uppfyller SWAMID AL2

Kontrollera slutligen att SWAMID AL2 uppfylls för användaren. Attributet **assurance** är en lista med tillitsnivåer som användaren uppfyller. Listan är typiskt en semikolonseparerad sträng, exempel:

<http://www.swamid.se/policy/assurance/al1>;<http://www.swamid.se/policy/assurance/al2>

Kontrollera att exakt <http://www.swamid.se/policy/assurance/al2> finns i listan. Om så inte är fallet så är det lämpligt att meddela användaren att kontot behöver bekräftas hos användarens lärosäte/inloggningstjänst. En errorURL bör även presenteras för användaren med kod **AUTHORIZATION_FAILURE** och URL:en till **SWAMID AL2** som kontext:



Bekräftad användare krävs

Ditt användarkonto vid ditt lärosäte eller din inloggningstjänst är inte bekräftat. Kontakta IT-support eller motsvarande för ditt lärosäte för hjälp. Använder du eduID för att logga in måste du logga in i **eduID** och där bekräfta din identitet.

Din inloggningstjänst tillhandahåller denna informationssida som kan hjälpa dig att lösa detta problem: <https://idp.example.se/ErrorUrl>

Ditt användarnamn: **abcdef01@example.se**.

ErrorURL:en ovan ska då peka på https://idp.example.se/ErrorUrl/?errorurl_code=AUTHORIZATION_FAILURE&errorurl_ts=...&errorurl_rp=...&errorurl_tid=...&errorurl_ctx=http://www.swamid.se/policy/assurance/al2.

Om användarna i tjänsten förväntas ha en hög teknisk kompetens kan det ofta också vara lämpligt att hänvisa till <https://release-check.swamid.se/> där användaren kan se sina egna attribut och annan information kopplat till sin inloggningstjänst.

Teknisk implementation baserat på krav om multifaktorinloggning och åsidosättande av single sign-on

Instruktionerna nedan är skrivna för Shibboleth Service Provider och webbservern Apache. Motsvarande behöver göras för annan SP- och webbserverprogramvara.

1. Begär multifaktorinloggning och åsidosättande av single sign-on

I konfigurationen för Apache finns det flera sätt att aktivera inloggning med Shibboleth och det beskrivs inte här, se [1.2 Configuring Apache Web Server to use Shibboleth](#) för ett exempel. Autentiseringsinställningar i via location-objektet beskrivs nedan.

För att aktivera krav på multifaktorinloggning via signaleringen för REFEDS MFA:

- ShibRequestSetting authnContextClassRef <https://refeds.org/profile/mfa>

För att aktivera åsidosättande av single sign-on:

- ShibRequestSetting forceAuthn true

Exempel från hur man lägger till krav på REFEDS MFA och krav på åsidosättande av single sign-on i en location-konfiguration i Apache

```
<Location /mfa-protected-directory>
  AuthType shibboleth
  ShibRequireSession On
  ShibRequestSetting authnContextClassRef https://refeds.org/profile/mfa
  ShibRequestSetting forceAuthn true
  require valid-user
</Location>
```

2. Kontroll om att multifaktorinloggning är genomförd

Shibboleth släpper normalt sätt inte in användaren användaren in till webbtjänsten om inte multifaktorinloggning har skett men man bör ändå kontrollera att multifaktorinloggning har genomförts.

Använd inloggningsmetod finns i servervariablen Shib-AuthnContext-Class.

Det är möjligt att anpassa den generella felsidan för Shibboleth SP så att den visar ett bra felmeddelande istället för det generella som är inbyggt i Shibboleth SP, se [Errors - Shibboleth Service Provider 3](#). Det är även möjligt att använda ett passiv, eller lazy, modell för inloggning men då krävs att applikationen både hanterar autentiseringsbegäran och autentiseringskontrollen i applikationen istället för att låta standardmekanismerna göra det men det beskrivs inte på denna wikisida.

Om authentication context class är felaktigt så är det lämpligt att meddela användaren att IdP:n inte skickar tillitsnivå, hänvisa användaren till sin support via IdP:ns **errorURL**, med kod **AUTHENTICATION_FAILURE** och <https://refeds.org/profile/mfa> som kontext:



Inloggning har inte skett via multifaktor eller din inloggningstjänst signalerade inte att det gjorts.

Fel inloggningsmetod skickades med vid inloggning. Kontakta IT-support eller motsvarande för ditt lärosäte eller din inloggningstjänst för hjälp.

Din inloggningstjänst tillhandahåller denna informationssida som kan hjälpa dig att lösa detta problem: <https://idp.example.se/ErrorMessage>

Teknisk information: **Authentication context class är felaktig (REFEDS MFA)**

ErrorURL:en ovan ska då peka på https://idp.example.se/ErrorMessage?errorurl_code=AUTHENTICATION_FAILURE&errorurl_ts=...&errorurl_rp=...&errorurl_tid=...&errorurl_ctx=https://refeds.org/profile/mfa.

3. Kontroll om att är genomförd "nyss"

Om inte single sign-on tillåts vid inloggningen ska man i applikationen kontrollera att inloggningen har skett i närtid, t.ex. inom fem minuter från aktuell tid. När inloggningen skedde finns i servervariabeln Shib-Authentication-Instant.

Om inloggningstiden är felaktig så är det lämpligt att meddela användaren att IdP:n inte skickar tillitsnivå, hänvisa användaren till sin support via IdP:ns **errorURL**, med kod **AUTHENTICATION_FAILURE** och forceAuthn som kontext:



Inloggningen är inte gjord tillräckligen nyligen.

Inloggningen i din identitetutgivare är inte tillräckligt aktuell. Kontakta IT-support eller motsvarande för ditt lärosäte eller din inloggningstjänst för hjälp.

Din inloggningstjänst tillhandahåller denna informationssida som kan hjälpa dig att lösa detta problem: <https://idp.example.se/ErrorUrl>

Teknisk information: **Tidsstämpel för inloggning är inte tillräckligt aktuell (forceAuthn)**

ErrorURL:en ovan ska då peka på https://idp.example.se/ErrorUrl/?errorurl_code=AUTHENTICATION_FAILURE&errorurl_ts=...&errorurl_rp=...&errorurl_tid=...&errorurl_ctx=forceAuthn.