Service Provider error handling during federated login

- Utökad hantering av errorURL
- Aktivera stöd för errorURL i en tjänst (SP)
  - Läsa ut errorURL via Shibboleth Service Provider
  - Länka till identitetsutfärdarens errorURL vid fel
- SWAMID-specifik användning av ERRORURL_CTX
- Exempel på felsidor vid vanliga inloggningsproblem i en tjänst
  - Inloggning i en tjänst som kräver SWAMID AL2 (bekräftad identitet) men där det inte uppfylls
  - Inloggning i en tjänst som kräver personnummer för identifiering av användare men som inte får det
- Interna felmeddelanden via Shibboleth Service Provider
  - Misslyckad autentisering
  - AttributeChecker

Vid federerad inloggning med SAML finns en funktion för att möjliggöra för tjänster att hänvisa användare som har hindrande inloggningsproblem tillbaka till hjälpsidor hos användarens organisation. Samtliga identitetsutfärdare (IdP) i SWAMID har en "errorURL" i metadatan med information om hur användare ska lösa hindrande inloggningsrelaterade problem. Tidigare har bara en generell webbadress kunnat konfigureras som "errorURL" för en identitetsutfärdare som då behöver täcka alla olika typer av fel. Under 2020 kompletterades detta med en utökning som gör att tjänster kan hänvisa användare till mer specifika informationssidor hos användarens organisation vid olika typer av fel för att bättre kunna hjälpa användaren att lösa hindrande inloggningsproblem.

> **errorURL i SWAMID**
>
> Sedan mars 2021 har samtliga identitetsutfärdare i SWAMID en registrerad errorURL. En del identitetsutfärdare använder traditionellt enkel errorURL men de flesta använder idag nedanstående beskrivna utökade hantering.

Utökad hantering av errorURL

Se SAML V2.0 Metadata Deployment Profile for errorURL Version 1.0 för definitionen av den utökade hanteringen av errorURL.

Felen som omfattas av errorURL-hanteringen är endast de fel som användaren förväntas kunna lösa själv eller med hjälp av sin identitetsutfärdare. Det finns fyra olika felkatagorier:

- IDENTIFICATION_FAILURE - Attribut som behövs för att identifiera användaren eller för att kunna personanpassa tjänsten saknas, exempelvis unika identifierare, namn eller e-post
- AUTHENTICATION_FAILURE - Kvalitén på autentiseringen uppfyller inte kraven som tjänsten har, exempelvis krav på tvåfaktorsautentisering
- AUTHORIZATION_FAILURE - Användaren saknar behörigheter i tjänsten, och användaren förväntas kunna åtgärda detta själv eller genom kommunikation med sin identitetsutfärdare, exempelvis för låg tillitsnivå (Assurance Level), saknad association till identitetsutfärdaren (affiliation) eller saknade entitlements (roller i tjänsten som överförs från identitetsutfärdaren vid inloggning)
- OTHER_ERROR - Annat fel som användaren förväntas kunna åtgärda själv eller med hjälp av sin identitetsutfärdare

Vid användning av tillägget till errorURL konstrueras URL:en med ett antal specifika strängar som tjänster kan byta ut till olika värden beroende på fel som uppstår vid inloggning. Den viktigaste av dessa är strängen "ERRORURL_CODE" som byts ut mot "IDENTIFICATION_FAILURE", "AUTHENTICATION_FAILURE" eller någon av de andra felkategorierna.

En errorURL för en identitetsutfärdare skulle exempelvis kunna vara

```
https://saml-error.example.com/ERRORURL_CODE.html
```

Vid fel i kategorin IDENTIFICATION_FAILURE skulle då länken som tjänsten ger till användaren bli

```
https://saml-error.example.com/IDENTIFICATION_FAILURE.html
```

På denna adress kan identitetsutfärdaren beskriva hur användare som får ett fel av denna kategori bör agera för att lösa just den typen av problem.

För att möjliggöra ännu tydligare information till användaren finns förutom ERRORURL_CODE även dessa strängar som tjänsten kan ge lämpliga värden:

- ERRORURL_TS - tid då felet inträffade (unix time eller sekunder sedan 1970-01-01)
- ERRORURL_RP - entityID för tjänsten
- ERRORURL_TID - en transaktionsidentifierare i tjänsten (för användning i kommunikation i tjänsten om det uppkomna felet, för den specifika användaren)
- ERRORURL_CTX - mer specificerad kontext för felet (t.ex. vilka attribut som saknas, vilken behörighet som saknas eller något annat som underlättar felsökandet för eventuell support hos identitetsutgivutfärdaren)

Dessa ytterligare attribut kan användas i en dynamisk implementation av errorURL för att ytterligare förbättra informationen till användare som får problem vid inloggning i tjänster. En mer dynamisk errorURL för en identitetsutfärdare skulle kunna vara

```
https://saml-error.example.com/?
errorurl_code=ERRORURL_CODE&errorurl_ts=ERRORURL_TS&errorurl_rp=ERRORURL_RP&errorurl_tid=ERRORURL_TID&errorurl_ctx
=ERRORURL_CTX
```

Om exempelvis en tjänst som kräver att användare uppfyller tillitsnivån SWAMID AL2 får en inloggning på tillitsnivå SWAMID AL1 kan tjänsten hänvisa användaren till

```
https://saml-error.example.com/?
errorurl_code=AUTHORIZATION_FAILURE&errorurl_ts=1607969220&errorurl_rp=https://www.student.ladok.se/student-
sp&errorurl_tid=error-5fd7a9c448086&errorurl_ctx=http%3A%2F%2Fwww.swamid.se%2Fpolicy%2Fassurance%2Fal2
```

Där kan då identitetsutfärdaren beskriva för användaren hur denne löser det uppkomna problemet, t.ex. bekräfta sin identitet för att uppnå tillräcklig nivå inkl. detaljerad information om hur användare gör det.

Aktivera stöd för errorURL i en tjänst (SP)

För att tjänster ska kunna utnyttja errorURL:en för användares identitetsutfärdare behöver detta läsas ut ur identitetsutfärdarens metadata. Detta hanteras olika i olika SAML Service Providers.

Läsa ut errorURL via Shibboleth Service Provider

För att läsa ut errorURL för en användares identitetsutfärdare i Shibboleth Service Provider behöver tillägget **Metadata Attribute Extraction** aktiveras i konfigurationen. Instruktioner finns under rubriken **Activate Metadata Attribute Extraction for Identity Provider metadata** på 3.3 Configure Shibboleth SP - Check for Identity Assurance or REFEDS SIRTFI.

När detta är gjort finns errorURL:en (i förekommande fall) tillgänglig i HTTP-headern/miljövariabeln **Meta-errorURL**.

Länka till identitetsutfärdarens errorURL vid fel

Läs noga igenom profilen SAML V2.0 Metadata Deployment Profile for errorURL Version 1.0, där beskrivs i vilka fall som errorURL:en kan användas och hur. Se även beskrivningen under **Utökad hantering av errorURL** ovan.

Försök beskriva felet så utförligt som möjligt ur tjänstens synvinkel för att hjälpa användaren att åtgärda det.

SWAMID-specifik användning av ERRORURL_CTX

För att ytterligare förbättra möjligheten till relevant information till användare vid olika fel används en konvension kring ERRORURL_CTX i SWAMID. Tjänster rekommenderas att lägga till dessa strängar till eventuell annan ERRORURL_CTX vid respektive fel, och identitetsutfärdare rekommenderas att hantera dessa speciellt:

Felkategori och specifikt fel	ERRORURL_CTX	Rekommenderad instruktion till användaren på errorURL:en
AUTHORIZATION_FAILURE Krav på SWAMID AL1 uppfylls ej	http://www.swamid.se/policy/assurance/al1	Uppmana användaren att kontakta identitetsutfärdarens support och upplysa om att SWAMID AL1 inte skickas till tjänsten
AUTHORIZATION_FAILURE Krav på SWAMID AL2 uppfylls ej	http://www.swamid.se/policy/assurance/al2	Beskriv hur användaren kan bekräfta sin identitet hos identitetsutfärdaren
AUTHORIZATION_FAILURE Krav på SWAMID AL3 uppfylls ej	http://www.swamid.se/policy/assurance/al3	Beskriv hur användaren kan verifiera sin identitet hos identitetsutfärdaren och i samband med detta även få tillgång till tvåfaktorsautentisering

Dessa komplement är implementerade i exempelimplementationen och i den federationsgemensamma errorURL:en i SWAMID.

Exempel på felsidor vid vanliga inloggningsproblem i en tjänst

Inloggning i en tjänst som kräver SWAMID AL2 (bekräftad identitet) men där det inte uppfylls

Alla identitetsutfärdare i SWAMID är inte godkända för tillitsprofilen SWAMID Assurance Level 2 Profile. Vilka som är godkända framgår på SWAMID Members. Oavsett om användarens identitetsutfärdare är godkänd eller inte så behöver användaren informeras om att det krävs en bekräftad identitet för inloggning i tjänsten.

Förslag på text, tillsammans med en länk till identitetsutfärdarens errorURL (i förekommande fall) med dessa förutsättningar:

- Namn på tjänst (gärna DisplayName från MDUI-metadata för tjänsten): **Ladok för studenter**
- entityID för tjänsten: **https://www.student.ladok.se/student-sp**
- errorURL för användarens identitetsutfärdare: **https://administrationsverktyg.umu.se/ErrorUrl/?errorurl_code=ERRORURL_CODE&errorurl_ts=ERRORURL_TS&errorurl_rp=ERRORURL_RP&errorurl_tid=ERRORURL_TID&errorurl_ctx=ERRORURL_CTX**

- Då det i det här fallet är behörighet som saknas så är det felkategori **AUTHORIZATION_FAILURE** som passar

> ***Säkerhetskrav uppfylls ej***
>
> *Ni har loggat in i Ladok för studenter med en användare som inte uppfyller aktuella säkerhetskrav. För att använda Ladok för studenter behöver ni bekräfta er användaridentitet. Kontakta helpdesk, service desk, IT-support eller motsvarande för er inloggningstjänst för hjälp.*
>
> *Er inloggningstjänst tillhandahåller en informationssida som ni uppmanas använda för att lösa detta problem: **https://administrationsverktyg.umu.se/ErrorURL/***
>
> *Aktuella säkerhetskrav: SWAMID Identity Assurance Level 2 Profile*

Länken ska konstrueras enligt följande:

1. Hämta identitetsutfärdarens errorURL från dess metadata
2. Ersätt **ERRORURL_CODE** med **AUHORIZATION_FAILURE**
3. Ersätt **ERRORURL_TS** med aktuell tid, på formen unix time, exempelvis **1616057384**
4. Ersätt **ERRORURL_RP** med tjänstens entityID, exempelvis **https://www.student.ladok.se/student-sp**
5. Ersätt **ERRORURL_TID** med en intern transaktionsidentifierare, om det skulle underlätta eventuell felsökning i kommunikation med tjänstens support
6. Ersätt **ERRORURL_CTX** med **http://www.swamid.se/policy/assurance/al2**
7. Visa länken för användaren med eventuella parametrar bortklippta

Resulterande länk skulle exempelvis kunna bli denna:

```
https://administrationsverktyg.umu.se/ErrorUrl/?
errorurl_code=AUTHORIZATION_FAILURE&errorurl_ts=1607969220&errorurl_rp=https://www.student.ladok.se/student-
sp&errorurl_tid=ERRORURL_TID&errorurl_ctx=http%3A%2F%2Fwww.swamid.se%2Fpolicy%2Fassurance%2Fal2
```

Inloggning i en tjänst som kräver personnummer för identifiering av användare men som inte får det

Personnummer används som identifierande attribut i många tjänster i SWAMID, bland annat kontoaktiveringsportaler, Ladok och Antagning.se. Inom de flesta studieadministrativa systemen används attributet **norEduPersonNIN** för överföring av personnummer. Andra tjänster använder normalt **personalIdentityNumber**.

> **norEduPersonNIN för att signalera bekräftad identitet**
>
> Det finns ett specialfall inom SWAMID där just **norEduPersonNIN** har använts för att indikera att identitetsutfärdaren med stor tillförlitlighet vet vilken personen bakom ett användarkonto är. Detta har då använts för att signalera att identiteten är "bekräftad". I och med tillitsprofilen SWAMID Identity Assurance Level 2 Profile så planeras detta fasas ut.

I de fall personnummer saknas så är det lämpligt att tjänsten meddelar detta, och också ger stöd till användaren i kommunikationen med sin identitetsutfärdare (IdP).

Förslag på text, tillsammans med en länk till identitetsutfärdarens errorURL (i förekommande fall) med dessa förutsättningar:

- Attribut som saknas: **norEduPersonNIN**
- Namn på tjänst (gärna DisplayName från MDUI-metadata för tjänsten): **Ladok för studenter**
- entityID för tjänsten: **https://www.student.ladok.se/student-sp**
- errorURL för användarens identitetsutfärdare: **https://administrationsverktyg.umu.se/ErrorUrl/?errorurl_code=ERRORURL_CODE&errorurl_ts=ERRORURL_TS&errorurl_rp=ERRORURL_RP&errorurl_tid=ERRORURL_TID&errorurl_ctx=ERRORURL_CTX**
- Tjänsten använder entitetskategorin **GÉANT Dataprotection Code of Conduct** för överföring av attribut
- Då det i det här fallet är identifierande attribut som saknas så är det felkategori **IDENTIFICATION_FAILURE** som passar

> ***Din identitetsutfärdare skickade ingen identitet***
>
> *Ingen identitet skickades med när du loggade in i Ladok för studenter. Kontakta helpdesk, service desk, IT-support eller motsvarande för er inloggningstjänst för hjälp.*
>
> *Er inloggningstjänst tillhandahåller en informationssida som ni uppmanas använda för att lösa detta problem: **https://administrationsverktyg.umu.se/ErrorURL/***
>
> *Teknisk information: norEduPersonNIN (personnummer) saknas*

Länken ska konstrueras enligt följande:

1. Hämta identitetsutfärdarens errorURL från dess metadata
2. Ersätt **ERRORURL_CODE** med **IDENTIFICATION_FAILURE**
3. Ersätt **ERRORURL_TS** med aktuell tid, på formen unix time, exempelvis **1616057384**
4. Ersätt **ERRORURL_RP** med tjänstens entityID, exempelvis **https://www.student.ladok.se/student-sp**

5. Ersätt **ERRORURL_TID** med en intern transaktionsidentifierare, om det skulle underlätta eventuell felsökning i kommunikation med tjänstens support
6. Ersätt **ERRORURL_CTX** med "**norEduPersonNIN http://www.geant.net/uri/dataprotection-code-of-conduct/v1"**
7. Visa länken för användaren med eventuella parametrar bortklippta

Resulterande länk skulle exempelvis kunna bli denna:

```
https://administrationsverktyg.umu.se/ErrorUrl/?
errorurl_code=IDENTIFICATION_FAILURE&errorurl_ts=1607969220&errorurl_rp=https://www.student.ladok.se/student-
sp&errorurl_tid=ERRORURL_TID&errorurl_ctx=norEduPersonNIN
```

Interna felmeddelanden via Shibboleth Service Provider

Shibboleth Service Provider kan hantera vissa hindrande inloggningsrelaterade problem internt. I fallet problem med autentisering/authnContextClass så måste felmeddelandet hanteras inne i Shibboleth. För hantering av saknade attribut är den inbyggda "AttributeChecker Handler" ett alternativ till hantering av detta i tjänsten. Mer information om detta finns på https://wiki.shibboleth.net/confluence/display/SP3/Errors.

Misslyckad autentisering

Vid misslyckad autentisering hos identitetsutfärdaren på grund av exempel felaktigt lösenord så stannar användaren normalt hos identitetsutfärdaren och denne får hantera eventuella felmeddelanden och rekommentationer till användaren. I de fall tjänsten begär en autentisering med en specifik authnContextClass (exempelvis https://refeds.org/profile/mfa) som inte identitetsutfärdaren kan uppfylla så skickas dock normalt användaren tillbaka till tjänsten med ett SAML-fel. Detta hanteras internt i Shibboleth Service Provider som ett sessionsfel, dock så följer information från inloggningsbegäran inte med till hanteringssidan för sessionsfel. En bättre lösning för hantering av detta är Redirection-metoden (se länken till Shibboleth SP:s dokumentation ovan) och låta den landa i applikationen som sedan dels i användarens webbsession kan veta att en MFA-inloggning påbörjats och sedan kunna tolka felet den får som parametrar av Redirection i Shibboleth Service Provider. Nedan följer ett exempel på en enklare metod för detta som hanteras helt av Shibboleth.

Sessionsfel hanteras av den template som definieras i shibboleth.xml:

shibboleth2.xml

```
<Errors supportContact="root@localhost"
        helpLocation="/about.html"
        styleSheet="/shibboleth-sp/main.css"
        session="sessionError.html" />
```

Shibboleth tillåter ett par macron i templates. Den är dock ganska begränsad och kan kompletteras med javascript. Exempel som hänvisar användaren till identitetsutfärdarens errorURL när autentisering misslyckas, sannolikt på grund av misslyckad MFA-autentisering. Denna gissning bygger på att **eventType** är **Login** och att **SAML-felkoden** är något av **AuthnFailed**, **NoPassive**, **NoAuthnContext** eller **RequestDenied**.

sessionError.html

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/>
  <link rel="stylesheet" type="text/css" href="<shibmlp styleSheet/>" />
  <title>Session Error</title>
</head>
<body>

<h1>Ett fel uppstod i sessionen</h1>

<script>
    var eventtype = '<shibmlp eventType/>';

    var statuscode2 = '<shibmlp statusCode2/>';
    // Replace & #58; with : (shibmlp variables are html-encoded)
    statuscode2 = statuscode2.replace(/&#58;/g,":");

    var errorurl = "<shibmlp errorURL/>";

    var now = "<shibmlp now/>";
    // Replace & #58; with : (shibmlp variables are html-encoded)
    now = now.replace(/&#58;/g, ":");

    var ts = Date.parse(now)/1000;

    if (errorurl !== null && errorurl !== ''){
        if (eventtype === "Login"  && (
                statuscode2 === "urn:oasis:names:tc:SAML:2.0:status:AuthnFailed" ||
                statuscode2 === "urn:oasis:names:tc:SAML:2.0:status:NoPassive" ||
                statuscode2 === "urn:oasis:names:tc:SAML:2.0:status:NoAuthnContext" ||
                statuscode2 === "urn:oasis:names:tc:SAML:2.0:status:RequestDenied")) {
            errorurl = errorurl.replace(/ERRORURL_CODE/, "AUTHENTICATION_FAILURE");
            errorurl = errorurl.replace(/ERRORURL_TS/, ts);
            errorurl = errorurl.replace(/ERRORURL_RP/, "ERRORURL_RP");
            errorurl = errorurl.replace(/ERRORURL_CTX/, "https://refeds.org/profile/mfa");

            var errorurl_short = errorurl.replace(/\?.*/, "");
            document.write('<p>Er inloggningstjänst tillhandahåller en informationssida som ni uppmanas använda
för att lösa detta problem: <a href="' + errorurl + '">' + errorurl_short + '</a>.');
        }
    } else {
        document.write('<p>Kontakta din inloggningstjänst för felsökning.');
    }
</script>

<p>
Teknisk information:
<p><font size="-1"><pre>
<shibmlp errorType/> at (<shibmlp requestURL/>)
<shibmlp errorText/>
<shibmlpif statusCode>
Error from identity provider:
Status: <shibmlp statusCode/>
<shibmlpif statusCode2>
Sub-Status: <shibmlp statusCode2/>
</shibmlpif>
<shibmlpif statusMessage>
Message: <shibmlp statusMessage/>
</shibmlpif>
</shibmlpif>
</pre>
</body>
</html>
```

AttributeChecker

AttributeChecker aktiveras i shibboleth.xml. Exempel med krav på attributet **norEduPersonNIN**:

shibboleth2.xml

```
<Handler type="AttributeChecker" Location="/AttrChecker" template="attrChecker.html"
         attributes="norEduPersonNIN" flushSession="true"/>
```

Shibboleth tillåter ett par macron i templates. Den är dock ganska begränsad och kan kompletteras med javascript. Exempel som hänvisar användaren till identitetsutfärdarens errorURL när attributet **norEduPersonNIN** saknas:

attrChecker.html

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/>
  <link rel="stylesheet" type="text/css" href="<shibmlp styleSheet/>" />
  <title>Din identitetsutfärdare skickade ingen identitet</title>
</head>
<body>

<shibmlpif entityID>
<h1>Din identitetsutfärdare skickade ingen identitet</h1>

Ingen identitet skickades med när du loggade in i Ladok för studenter. Kontakta helpdesk, service desk, IT-
support eller motsvarande för er inloggningstjänst för hjälp.

<script>
    var missing_attributes = "<shibmlpifnot norEduPersonNIN>norEduPersonNIN </shibmlpifnot>";
</script>

<shibmlpif errorURL>
<p>
Er inloggningstjänst tillhandahåller en informationssida som ni uppmanas använda för att lösa detta problem:
<script>
    var errorurl = "<shibmlp errorURL />";
    var now = "<shibmlp now />";
    now = now.replace(/&#58;/g, ":");
    var ts = Date.parse(now)/1000;

    if (errorurl)
    {
        errorurl = errorurl.replace(/ERRORURL_CODE/, "IDENTIFICATION_FAILURE");
        errorurl = errorurl.replace(/ERRORURL_TS/, ts);
        errorurl = errorurl.replace(/ERRORURL_RP/, "<shibmlp target />");
        errorurl = errorurl.replace(/ERRORURL_CTX/, missing_attributes + "http://www.geant.net/uri
/dataprotection-code-of-conduct/v1");

        var errorurl_short = errorurl.replace(/\?.*/, "");

        document.write('<a href="' + errorurl + '">' + errorurl_short + '</a>.');
    }
</script>
</shibmlpif>

<p>
Teknisk information: <script>document.write(missing_attributes);</script> saknas
</shibmlpif>

<shibmlpifnot entityID>
<h1>Session invalidated</h1>
<p>Your session was already invalidated before your information could
 be examined for completeness.</p>
</shibmlpifnot>

</body>
</html>
```