Error Handling URL in SWAMID

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. Organisationer kan lägga in en särskild uppgift om "errorURL" i metadatan för sin identitetsutfärdare (IdP) med en länk till organisationens hjälpsidor. 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.

Från och med 16 mars 2021 måste alla identitetsutfärdare (IdP) registrerade i SWAMID ha en errorURL registrerad i sin IdPs metadata. Det finns två alternativ till errorURL:

- Organisationen som står bakom identitetsutfärdaren skapar en egen errorURL-sida lokalt, SWAMID rekommenderar en dynamisk webbsida motsvarande referensimplementationen enligt beskrivning under Sätta upp eget stöd för errorURL.
- SWAMID lägger in den federationsgemensamma errorURL:en i identitetsutfärdarens metadata, se Använda SWAMIDs federationsgemensamma stöd för errorURL.

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 identitetsutfärdare (IdP)

Sätta upp eget stöd för errorURL

SWAMID har byggt en referensimplementation av den utökade hanteringen av errorURL. Denna finns utvecklad i PHP, JSP, .NET Core samt statiska HTML-sidor. Implementationen är fri att använda och modifiera efter identitetsutfärdares egna behov.

Exempelimplementatonen återfinns på https://github.com/SUNET/swamid-errorurl.

En dynamisk sida

En dynamisk sida har möjlighet att avgöra vilken tjänst som efterfrågades och vilken kontext som skickades med. Det möjliggör också att ytterligare information som kan underlätta vid felsökning hos identitetsutfärdaren finns med i en eventuell supportförfrågan till identitetsutfärdaren från användaren.

Exempel:

```
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
```

Fem statiska sidor

Då det finns fyra felkategorier räcker det med fem statiska webbsidor för att tillhandahålla information för de fyra felkategorierna. Den femte sidan är då en omodifierad errorURL där tjänsten inte bytt ut strängen ERRORURL_CODE mot någon felkategori, och bör innehålla information om alla kategorier av fel eller länkar till respektive felsida.

Exempel:

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

En statisk sida

Vid utelämnande av strängen ERRORURL_CODE i en errorURL finns ingen sträng att ersätta för tjänster. På så vis hänvisas användare vid alla kategorier av fel till samma sida.

Exempel:

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

Detta kan vara det enda alternativet för tjänsteleverantörer som inte kan välja namn på webbsidor.

Använda SWAMIDs federationsgemensamma stöd för errorURL

Arbete pågår inom SWAMID att se till att samtliga identitetsutfärdare har en definierad errorURL i sin metadata. För att underlätta övergången finns en federationsgemensam errorURL som identitetsutfärdare som inte har någon egen errorURL kan använda.

I den gemensamma errorURL:en finns generell information om olika inloggningsproblem och tänkbara lösningar, samt hänvisning till den e-postadress som finns registrerat som identitetsutfärdarens supportfunktion i dess metadata.

SWAMIDs gemensamma errorURL går att testa på https://error.swamid.se/test/. Där finns även en länk till aktuell errorURL för respektive IdP i SWAMID. IdP:er som inte har någon egen errorURL har där en länk till den gemensamma errorURL:en, anpassad för den specifika identitetstutfärdaren.

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.