

SSO - FAQ - Kendte problemer med op-sætninger

Indhold

Introduktion	3
ErrorCode: urn:oasis:names:tc:SAML:2.0:status:Responder. Message:	4
Fejlbesked/fejlkode	4
Validering af fejl	4
Kendte løsninger	4
Error details: MSIS7007: The requested relying party trust...	5
Fejlbesked/fejlkode	5
Validering af fejl	5
Kendte løsninger	5
Fejl detaljer: ID4037: The key needed to verify the signature could not be resolved	6
Fejlbesked/fejlkode	6
Validering af fejl	6
Kendte løsninger	6
Fejl detaljer: No value set for NameClaimType	7
Fejlbesked/fejlkode	7
Validering af fejl	7
Kendte løsninger	7
Fejl med hexadecimal referencenummer	8
Validering af fejl	8

Kendte løsninger	8
Dit login kan ikke behandles da den konto du bruger ikke opfylder nogle prædefinerede betingelser.condition"	9
Validering af fejl	9
Kendte løsninger	9
An error occurred during an attempt to read the federation metadata.....	10
Fejlbesked/fejlkode	10
Validering af fejl	10
Løsning	10
Transformationspipelinen blev stoppet.....	11
Fejlbesked/fejlkode	11
Validering af fejl	11
Løsning	11

Introduktion

Moderniseringsstyrelsen vil løbende vedligeholde dette dokument, der oplister kendte fejl med tilhørende løsninger. Moderniseringsstyrelsens kan dog ikke garantere at en løsning virker for alle IDP'er og SP'er, da opsætninger af IDP'er og SP'er kan variere, samt der kan være variationer fra den ene software til den anden i forhold til konfigurationsmuligheder.

Dette dokument skal derfor kun ses, som en vejledning til mulige løsninger – og ikke som en løsning til et konkret problem.

ErrorCode: urn:oasis:names:tc:SAML:2.0:status:Responder. Message:

Fejlbesked/fejlkode

Følgende fejl er set ved opsætning af en identitetsudbyder – og giver følgende besked:

ErrorCode: urn:oasis:names:tc:SAML:2.0:status:Responder. Message:

Validering af fejl

Det er muligt at spore fejlen til den konkrete identitetsudbyder ved at kigge i SAMLresponse:

```

<?xml version="1.0"?>
- <samlp:Response Version="2.0" IssueInstant="2018-12-21T11:21:57Z" InResponseTo="Id17a3811214124:3c8cd29b7166e5c543" ID="Id46JUodCqmEK8M7Dhv0zRw0B2U"
  Destination="https://
xmlns:saml="urn:oasis:names:tc:SAML:2.0:protocol" Consent="urn:oasis:names:tc:SAML:2.0:consent:obtained" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  <saml:Issuer>https:// </saml:Issuer>
- <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  - <ds:SignedInfo>
    <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" xmlns="http://www.w3.org/2000/09/xmldsig#" />
    <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
    - <ds:Reference URI="Id46JUodCqmEK8M7Dhv0zRw0B2U">
      - <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmenc#sha256" />
      <DigestValue xmlns="http://www.w3.org/2000/09/xmldsig#">/OF6v3f4s/tvIoKhYUDY5VHSDQZ5sbA3MkiKwxYU4=</DigestValue>
    </ds:Reference>
    <ds:SignatureValue xmlns="http://www.w3.org/2000/09/xmldsig#">Sz3uV0dEgO1nbUwaadFR6bi/9ID2ci5qaFKAhGv38snXe1uY3YDnILyozvF1agV1w/XE8bBUU
7ra0qCjWJjDm0CvK4mkQYRu+FXlg UFHBL0exPgs7kqQNZ9x+S2IERsgKsv10z26YYofx
r5Bxslp5U18F05Uj3Hkpaufw9Hh. g=</SignatureValue>
  - <ds:KeyInfo>
    <ds:X509Data>
    </ds:KeyInfo>
  </ds:KeyInfo>
  </ds:Signature>
- <samlp:Status>
  - <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Responder">
  <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:RequestDenied"/>
</samlp:Status>
</samlp:Response>

```

I ovenstående SAMLresponse er det muligt at se IDP udbyder i **<saml:Issuer>** *[IDP Navn]* **</saml:Issuer>**, som er markeret med en grøn firkant - oftest ligner navnet en URL.

I **<samlp:StatusCode Value="[værdi]">** markeret med rød firkant, er det muligt at læse status for SAMLresponse. Heri inkluderet hvem fejlen opstod hos (i eksemplet **Responder**), samt hvad status på request (i eksemplet **Denied**).

OBS på, at der er flere **<samlp:StatusCode Value="[værdi]">**.

Kendte løsninger

På IDP-siden skal MODST SSO stå som en **Transient name identifier** som default.

Error details: MSIS7007: The requested relying party trust...

Fejlbesked/fejlkode

Denne fejl kan vise sig, når en bruger ønsker at anvende et fagsystem, eksempelvis Modst SSO SamlClaimApp.

Error details

- Activity ID: 02e50268-9bfc-4ffa-2269-0080000000a3
- Error details: MSIS7007: The requested relying party trust 'https://testssso.modst.dk/runtime/' is unspecified or unsupported. If a relying party trust was specified, it is possible that you do not have permission to access the trust relying party. Contact your administrator for details.
- Node name: b9a8e34c-8a91-446f-b25d-d858a6fb7984
- Error time: Tue, 09 Apr 2019 12:56:09 GMT
- Cookie: enabled
- User agent string: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:66.0) Gecko/20100101 Firefox/66.0

Validering af fejl

Fejlen skyldes manglende opsætning. Fejlbeskrivelsen specificere også, at det er en ”unspecified or unsupported” trust til Modst SSO. Om det er en fagsystem eller identitetsudbyder kan kontrolleres ved at vælge Modst SSO SamlClaimApp – og efterfølgende vælge relevant identitetsudbyder. Kan brugeren se sine claims er det ikke identitetsudbyderen, der er udfordringen.

For at anvende SamlClaimApp fra Modst SSO produktionsmiljø anvendes:

<https://sso.modst.dk/samlclaimapp/>

For at anvende SamlClaimApp fra Modst SSO testmiljø anvendes:

<https://testssso.modst.dk/samlclaimapp/>

Kendte løsninger

Lad IdP'en eller systemet blive opsat før SSO tages i brug.

Fejl detaljer: No value set for NameClaimType...

Fejlbesked/fejlkode

Denne type fejl indikerer at der mangler en værdi for det nævnte claim. I dette tilfælde handler det om claimet ”*http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name*”

Fejl detaljer: No value set for NameClaimType:
'http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name'

Validering af fejl

Denne fejl kan valideres ved, at vælge relevant identitetsudbyder på Modst SSO SamlClaimApp. Denne fejl ses typisk i forbindelse med opsætning af en identitetsudbyder.

For at anvende SamlClaimApp fra Modst SSO produktionsmiljø anvendes:

<https://sso.modst.dk/samlclaimapp/>

For at anvende SamlClaimApp fra Modst SSO testmiljø anvendes:

<https://testssso.modst.dk/samlclaimapp/>

For at se standard claims i MS ADFS kan man gå til: <https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/technical-reference/the-role-of-claims>

Kendte løsninger

Der skal opsættes en claim-værdi hos IdP. Hvilken værdi, der forventes fra specifikke claims er specificeret i IdP'ernes opsætningsvejledning, der er tilgængelig på <https://modst.dk>

Fejl med hexadecimal referencenummer

Fejl, der giver et referencenummer angivet i hexadecimaler, kan betyde mange forskellige ting. Oftest vil MODST ikke have mulighed for at bistå med problemløsning for denne type fejl, da den egentlige fejlkode ikke kendes.

I forbindelse med fejlen vil identitetsudbyderes domæne også figurere, hvilket tyder på, at referencenummeret og med dertilhørende årsagsforklaring og fejlkode kan findes hos identitetsudbyderen.

Der opstod et problem under forsøget på at få adgang til siden. Prøv at gå til siden igen.
Hvis problemet fortsætter, skal du kontakte administratoren for siden og angive referencenummeret for at identificere problemet.
Referencenummer: 20c5de32-41e7-4a92-a764-691da358d011

OBS! Layout af denne fejl kan findes i flere varianter.

Validering af fejl

Der kan gøres forsøg med forskellige indstillinger på SSO-siden, for at se om fejlen kan fremprovokeres flere steder eller om det er et specifikt sted i login-flowet.

Kendte løsninger

Identitetsudbydere skal finde den rigtige fejlkode i egen log – og kan efterfølgende indsende den til MODST. Identitetsudbyderen kan også selv afhjælpe fejlen uden MODST's indblanding.

Dit login kan ikke behandles da den konto du bruger ikke opfylder nogle prædefinerede betingelser.condition"

Denne fejl vises, hvis brugeren ikke opfylder de definitioner, som Moderniseringsstyrelsen skal have oplyst for at identificere en valid adgang til en identitetsudbyder.

Safewhere Identify*Runtime build 5.2.0.5009 Copyright © Safewhere 2014



Validering af fejl

Luk din browser og prøv igen. Forsætter fejlen kontakt MODST Support via serviceportalen.

OBS! SSO-fejl indmeldes i kategorien Øvrige → Single sign-on

Kendte løsninger

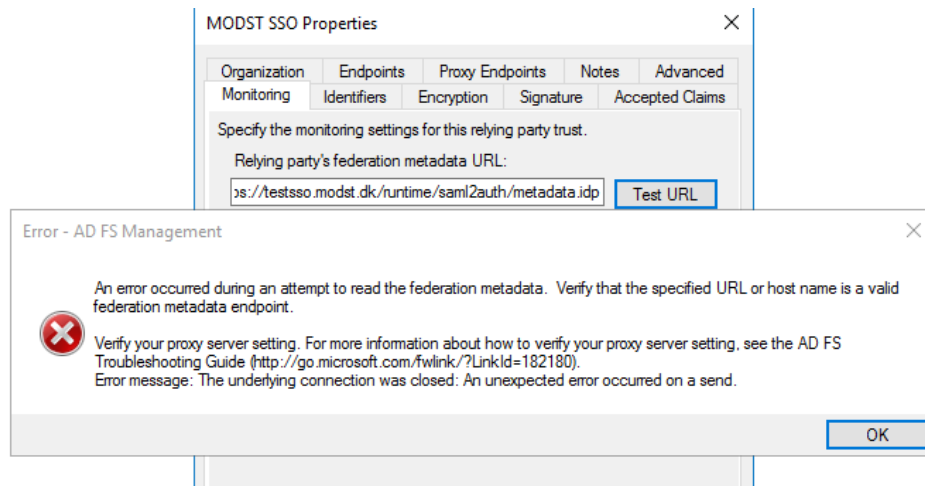
Brugeren kontakter MODST Support med skærmbillede af fejl, samt skærmbillede af brugerens claims. Brugeren kan få vist sine claims på:

<https://sso.modst.dk/samlclaimapp/>

An error occurred during an attempt to read the federation metadata...

Fejlbesked/fejlkode

Fejl ved indlæsning af metadata URL i ADFS.



Validering af fejl

Dette er en fejl hos den opsættende part, hvis MODST metadata kan tilgås og udtrækkes via en browser. Kunden kan forsøge, at åbne en browser på sin server, for at se om filen er tilgængelig fra serveren. Kan metadata ikke hentes, så har serveren ikke adgang til internettet. Kan metadata hentes, er der udført konfiguration i ADFS, der bevirker at URL'en ikke kan testes.

Løsning

Kunden skal tage kontakt til egen teknikker, der har erfaring med opsætning af ADFS. Dette er ikke et MODST problem, så længe metadata kan hentes via metadata-URL.

Transformationspipelinen blev stoppet

Fejlbesked/fejlkode

Denne fejl kan ses i forbindelse med Identitetsudbydere og Serviceudbydere. Fejlen er observeret i forbindelse med opsætning af ny IdP'er og SP'er.



Validering af fejl

Når en bruger anvender SSO-URL til et fagsystem, der er i opsætningsfasen for enten systemet eller institutionen, vil denne fejl blive præsenteret efter, at brugeren er logget ind på domænet. Dette kan verificeres ved at anvende Firefox, som afbryder SSO-login, da Firefox ikke kan anvende Kerberos-token udstedt af Windows. Brugeren skal derfor logge ind igen med egen institutionsbrugerprofil og password i Firefox. Hvis fejlen eksisterer stadig, vil den blive præsenteret herefter i login'et.

Løsning

Brugeren kontakter MODST Support med skærmbillede af fejl, samt skærmbillede af brugerens claims. Brugeren kan få vist sine claims på:

<https://sso.modst.dk/samlclaimapp/>