



VEJLEDNING TIL OPSÆTNING AF IDENTITY PROVIDER

Februar 2024

Indhold

- [Om jobfunktionsroller og brugersystemroller](#)
- [Oprettelse af jobfunktionsroller](#)
- [Tilslutning af lokal Identity Provider:](#)
 - 1. [Registrering af Context Handler som Service Provider/Relying Party](#)
 - [Safewhere Identify](#)
 - [AD FS 3.0](#)
 - [OpenAM](#)
 - [OS2faktor](#)
 - 2. [Metadata udtrækkes og registreres hos KOMBIT](#)
 - [Udtræk metadata fra Identity Provider](#)
 - [Registrering i Fælleskommunal Administrationsmodul](#)
 - 3. [Identity Provider tilpasses KOMBITs Attributprofil](#)
 - 4. [Test af Identity Provider](#)
 - [Test af login-flow - Context Handler 1](#)
 - [Test af login-flow - Context Handler 2](#)

OM JOBFUNKTIONSROLLER OG BRUGERSYSTEMROLLER

Hvad er en brugersystemrolle?

- En brugersystemrolle er et sæt af rettigheder i et bestemt it-system (fx Valg)
- Brugersystemroller er defineret af it-systemet, og er ens for alle myndigheder

Hvad er en jobfunktionsrolle?

- En jobfunktionsrolle er en samling af brugersystemroller, der tilsammen gør det muligt for en medarbejder at udføre en funktion
- En jobfunktionsrolle kunne være *‘Valgkortsadministrator’*, *‘Stemmetæller’* eller *‘Politiker’*
- Jobfunktionsroller er roller, som er oprettet og vedligeholdt af de enkelte myndigheder

OPRETTELSE AF JOBFUNCTIONSROLLER

Oprettelse af jobfunktionsroller

- Foregår i Fælleskommunalt Administrationsmodul, der er brugergrænsefladen til Fælleskommunal Adgangsstyring
- Opbygges efter den arbejdsgang, der er vist på de følgende sider

1. Liste over eksisterende roller

Opgaveoversigt

Organisationer

It-systemer

Serviceaftaler

Føderationsaftaler

Jobfunktionsroller

Rapporter

Brugerprofiler

KOMBIT Administration

Aftalebetingelser

Adviseringer

Dataafgrænsningstyper

Servicekoblinger

Visningsgrupper

Servicegrupper

Provisionering

Jobfunktionsroller

På vegne af

KOMBIT A/S

+ Opret jobfunktionsrolle

Navn ^	System	Beskrivelse	Delegeret
A SAPA Administrator	SAPA Overblik BvS	Denne rolle indeholder alle brugersystemroller til en SAPA administrator	
BBR Adgangskontrol - TEST	BBR Demo Fagsystem	Test jobfunktionsrolle til pilotkommunernet test	
BBR adresseopretter	BBR		
BBR standardbruger	BBR		
Klassifikation Læs Aabenraa	Klassifikation	Denne jobfunktionrolle oprettes med formålet at give Aabenraa kommunes brugere adgang til at læse de fælles-kommunale klassifikationer i STS Klassifikation GUI. Uden denne jobfunktionrolle vil en bruger ikke kunne se, eksempelvis KLE i GUI.	Til: Aabenraa kommune (Cvr. 2...

Helpdesk: 70 11 15 39 - helpdesk@serviceplatformen.dk - KOMBIT A/S, Halfdansgade 8, 2300 København S - CVR-nr.: 19435075 - EAN-nr. 5790001969370

2. Udfyld stamdata

Opgaveoversigt

Organisationer

It-systemer

Serviceaftaler

Føderationsaftaler

Jobfunktionsroller

Rapporter

Brugerprofiler

KOMBIT Administration

Aftalebetingelser

Adviseringer

Dataafgrænsningstyper

Servicekoblinger

Visningsgrupper

Servicegrupper

Provisionering

Opret jobfunktionsrolle

(På vegne af KOMBIT A/S)

Navn:

EntityId

Rollenavn:

<http://kombit.dk/roles/jobrole/valgrolle1/1>

Beskrivelse:

Dette er en Jobfunktionsrolle til Valg systemet

Delegeret til: [Klik her for at uddelegere jobfunktionsrollen](#)

+ Tilknyt brugersystemrolle

Helpdesk: 70 11 15 39 - helpdesk@serviceplatformen.dk - KOMBIT A/S, Halldansgade 8, 2300 København S - CVR-nr.: 19435075 - EAN-nr. 5790001969370

3. Vælg "Valg" som it-system

Opgaveoversigt

Organisationer

It-systemer

Serviceaftaler

Føderationsaftaler

Jobfunktionsroller

Rapporter

Brugerprofiler

KOMBIT Administration

Aftalebetingelser

Adviseringer

Dataafgrænsningstyper

Servicekoblinger

Visningsgrupper

Servicegrupper

Provisionering

Tilknyt brugersystemrolle (På vegne af KOMBIT A/S)

System	Rolle	Dataafgrænsning
Navn: Min 1. rolle til valg		
EntityId: http://kombit.dk/roles/jobrole/valgrolle1/1		
System		
Valg		
Navn ^		
valg		
Valg		

Annuler

Næste

Vælg et brugervendt system fra listen, eller fremsøg det ved at begynde at skrive i feltet Navn.

Helpdesk: 70 11 15 39 - helpdesk@serviceplatformen.dk - KOMBIT A/S, Halldansgade 8, 2300 København S - CVR-nr.: 19435075 - EAN-nr. 5790001969370

4. Vælg én brugersystemrolle fra Valg

Opgaveoversigt

Organisationer

It-systemer

Serviceaftaler

Føderationsaftaler

Jobfunktionsroller

Rapporter

Brugerprofiler

KOMBIT Administration

Aftalebetingelser

Adviseringer

Dataafgrænsningstyper

Servicekoblinger

Visningsgrupper

Servicegrupper

Provisionering

Tilknyt brugersystemrolle (På vegne af KOMBIT A/S)

System	Rolle	Dataafgrænsning
Navn:	Min 1. rolle til valg	
EntityId:	http://kombit.dk/roles/jobrole/valgrolle1/1	
System:	Valg	
Rolle	Testrolle	
Navn ^ Testrolle		

Vælg en rolle fra listen, eller fremsøg det ved at begynde at skrive i feltet Navn.

Helpdesk: 70 11 15 39 - helpdesk@serviceplatformen.dk - KOMBIT A/S, Halldansgade 8, 2300 København S - CVR-nr.: 19435075 - EAN-nr. 5790001969370

5. Gentag til færdig (og tryk Gem)

Opgaveoversigt

Organisationer

It-systemer

Serviceaftaler

Føderationsaftaler

Jobfunktionsroller

Rapporter

Brugerprofiler

KOMBIT Administration

Aftalebetingelser

Adviseringer

Dataafgrænsningstyper

Servicekoblinger

Visningsgrupper

Servicegrupper

Provisionering

EntityId

Rollenavn: valgrolle1
http://kombit.dk/roles/jobrole/valgrolle1/1

Beskrivelse: Dette er en Jobfunktionsrolle til Valg systemet

Delegeret til: [Klik her for at uddelegere jobfunktionsrollen](#)

Brugersystemroller

System ^	Rolle	Dataafgrænsning
Valg	Testrolle	

Gem

Annuller

+ Tilknyt brugersystemrolle

Helpdesk: 70 11 15 39 - helpdesk@serviceplatformen.dk - KOMBIT A/S, Halfdansgade 8, 2300 København S - CVR-nr.: 19435075 - EAN-nr. 5790001969370

TILSLUTNING AF LOKAL IDENTITY PROVIDER

Overblik over trin i tilslutning af Identity Provider

1. Fælleskommunal Adgangsstyring for brugere (Context Handler) registreres i den lokale Identity Provider som en *Service Provider/Relying Party (SP/RP)*
2. SAML-metadata:
 1. Context Handler 1 (den gamle version):
 - Udtrækkes fra den lokale Identity Provider, og registreres i Fælleskommunalt Administrationsmodul
 2. Context Handler 2 (den nye version):
 - *Enten* udtrækkes fra den lokale Identity Provider, og registreres i Fælleskommunalt Administrationsmodul
 - *Eller* der registreres en metadata-URL i Fælleskommunalt Administrationsmodul
3. Identity Provideren tilpasses/konfigureres til at overholde KOMBITs Attributprofil
4. For at teste, at integrationen er korrekt udført, gennemføres et login mod et demo-system opsat af KOMBIT

1. REGISTRERING AF CONTEXT HANDLER SOM SP/RP

Registrering af metadata i Identity Provider

Metadata (en XML-fil) for Fælleskommunal Adgangsstyring for brugere kan downloades direkte fra Støttesystemerne. Typisk er registrering af metadata en del af oprettelsesprocessen, når man opretter en ny Service Provider i sit Identity Provider-produkt.

Metadata til Context Handler 1

Eksternt testmiljø: <https://adgangsstyring.ekstern-test-stoettesystemerne.dk/runtime/saml2auth/metadata.idp>

Produktionsmiljø: <https://adgangsstyring.stoettesystemerne.dk/runtime/saml2auth/metadata.idp>

Metadata til Context Handler 2 (ny version)

Eksternt testmiljø: <https://n2adgangsstyring.ekstern-test-stoettesystemerne.dk/runtime/saml2auth/metadata.idp>

Produktionsmiljø: <https://n2adgangsstyring.stoettesystemerne.dk/runtime/saml2auth/metadata.idp>

SAFEWHERE IDENTIFY

Registrering af metadata i Identity Provider: Safewhere Identify (side 1 af 2)

Identify Web Administration
Safewhere Identify*Admin build 4.2.0.2079 Copyright © Safewhere 2014

Language: [English](#) | [Danish](#) You are logged in as: admin | [Sign off](#)

[My Profile](#) [Groups](#) [Users](#) [Claims](#) [System Setup](#) [Transformations](#) [Connections](#) [Help](#)

[Home](#) > [Organization: Root](#) > Add Connection: SAML 2.0

Add Connection: SAML 2.0

Name

Please give an appropriate name for the protocol connection. All characters are allowed, but the name should be at least be between 3 and 255 characters.

- § Name
Your name must be between 3 and 255 characters long.

Name:*

Description

A description of the connection for administrative purposes.

Description:

[Edit localized text](#)

Enabled

If a protocol connection is disabled it will not allow the relying party to request authentication.

☒ Enabled

Use Persistent Pseudonym

Federation with persistent name IDs establishes a permanent relationship between a user on an identity provider and a user on a service provider or users on an affiliation of service providers. The persistent name ID is used by an identity provider and a service provider as a common name for a single user. If this name ID for a user is the same for multiple service providers, the service providers are said to be affiliated or belong to an affiliation group. Use this kind of federation to link accounts out-of-band, but without using identifiers that can be traced back to a specific user. This increases the security of your systems by preventing eavesdroppers from determining identities on the basis of name ID formats that pass logon IDs or e-mail addresses.

☐ Use persistent pseudonym

Owner Organization

This connection is owned by the following organization

Owner Organization:

Connection Dependency

Please choose the protocol connections for the replying parties that should be offered this authentication method when requesting federated access for their users.

Connection Dependency:

☒ Username & password

Registrering af metadata i kommunal Identity Provider: Safewhere Identify

Identify Web Administration
Safewhere Identify*Admin build 4.2.0.2079 Copyright © Safewhere 2014

Language: [English](#) | [Danish](#) You are logged in as: admin | [Sign off](#)

My Profile Groups Users Claims System Setup Transformations **Connections** Help

Connections

Home > Organization: Root > All connections

All connections

New Metadata Tools

Name
https://idp.projekt-stoettesystemerne.dk/admin/
KOMBIT
SAML2 for Kmodel change
SAML2 for MAIN
SAML2 for Preprod
Username & password

Upload metadata for 'KOMBIT' Protocol Connection

☒ Upload from url

<https://kombit.safewhere.local/runtime/saml2auth/metadata>

☐ Upload from file

Browse

Metadata options

☐ Accept untrusted certificates

☐ Skip signature validation

☐ Import certificate to store

Store location

Store name

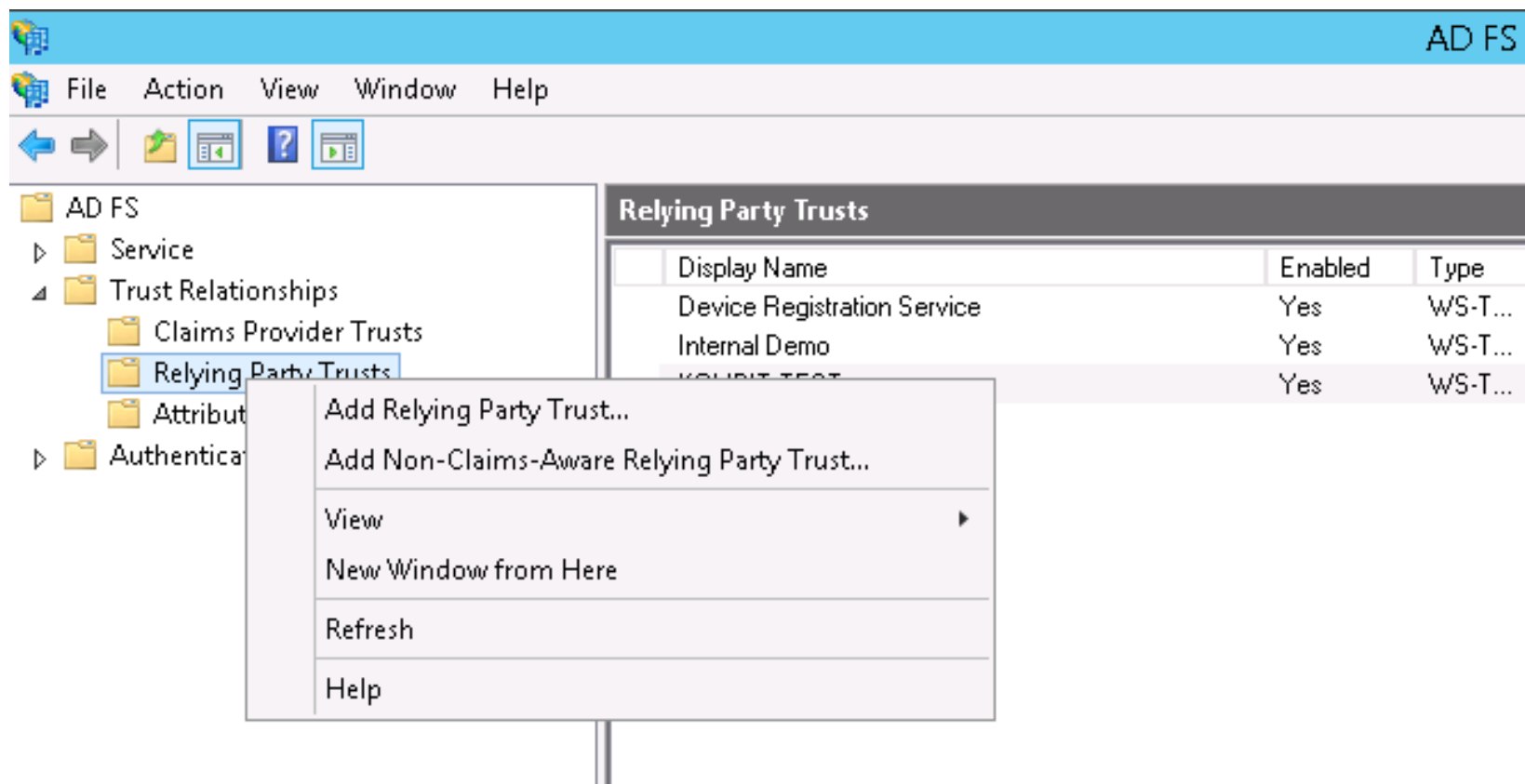
Upload Cancel

Organization	Type	Sub Type
Root	Protocol	WSFederation protocol plug-in
Root	Protocol	SAML 2.0
Root	Protocol	SAML 2.0
Root	Protocol	SAML 2.0
Root	Protocol	SAML 2.0
Root	Authentication	Username & password Login plug-in

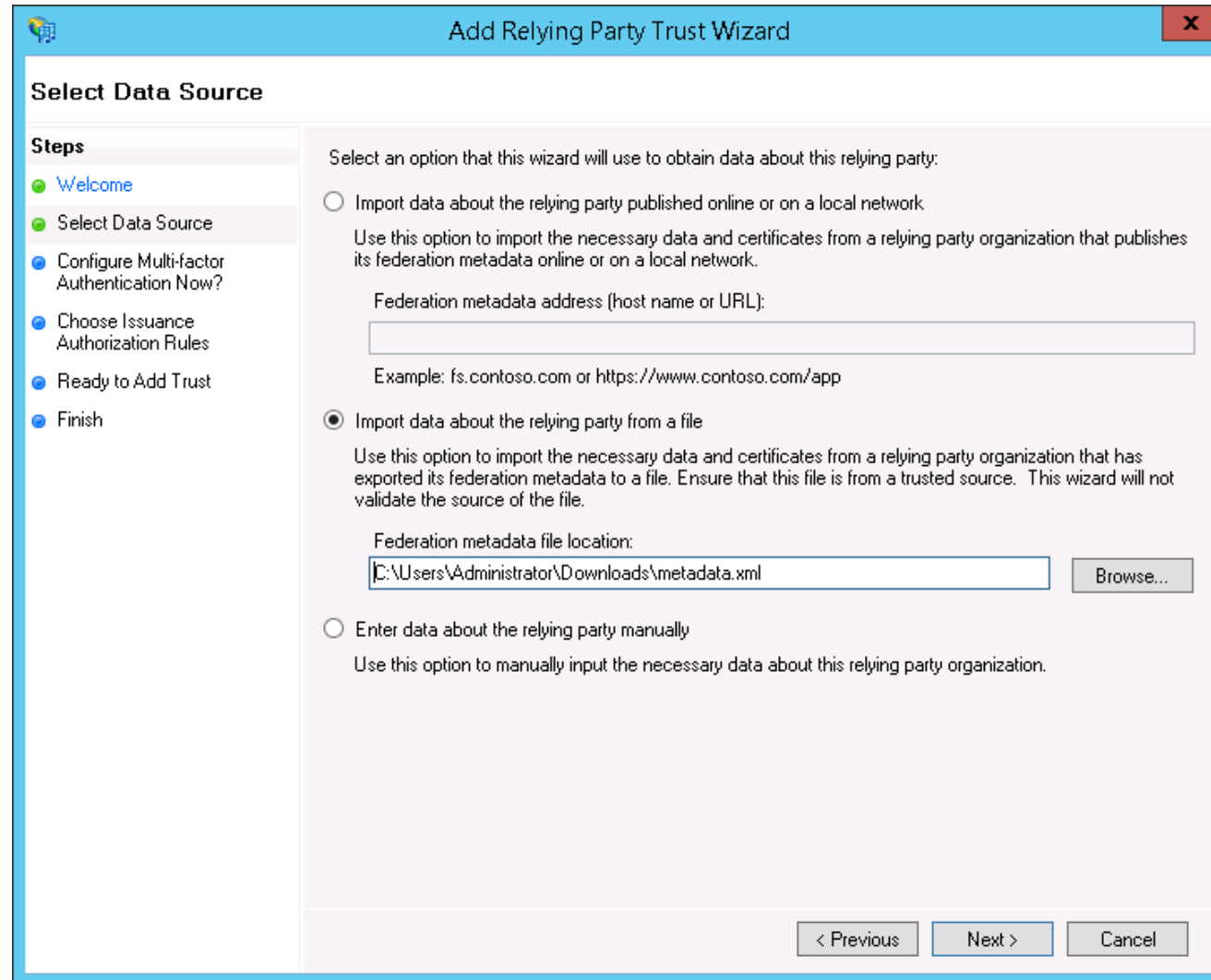
Page 1 Records/Page 20

AD FS 3.0

Registrering af metadata i Identity Provider: AD FS 3.0 (side 1 af 2)



Registrering af metadata i Identity Provider: AD FS 3.0 (side 2 af 2)



The screenshot shows the 'Add Relying Party Trust Wizard' window. The title bar is blue with a close button. The main area is white. On the left, there is a 'Steps' pane with a list of steps: 'Welcome' (selected), 'Select Data Source' (current step), 'Configure Multi-factor Authentication Now?', 'Choose Issuance Authorization Rules', 'Ready to Add Trust', and 'Finish'. The main content area has a heading 'Select Data Source' and a sub-heading 'Select an option that this wizard will use to obtain data about this relying party:'. There are three radio button options: 1. 'Import data about the relying party published online or on a local network' (unselected). Description: 'Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.' Input field: 'Federation metadata address (host name or URL):' with a text box and an example: 'fs.contoso.com or https://www.contoso.com/app'. 2. 'Import data about the relying party from a file' (selected). Description: 'Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.' Input field: 'Federation metadata file location:' with a text box containing 'C:\Users\Administrator\Downloads\metadata.xml' and a 'Browse...' button. 3. 'Enter data about the relying party manually' (unselected). Description: 'Use this option to manually input the necessary data about this relying party organization.' At the bottom right, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

Add Relying Party Trust Wizard

Select Data Source

Steps

- Welcome
- Select Data Source
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

Select an option that this wizard will use to obtain data about this relying party:

☐ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

☒ Import data about the relying party from a file

Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

Federation metadata file location:

C:\Users\Administrator\Downloads\metadata.xml

Browse...

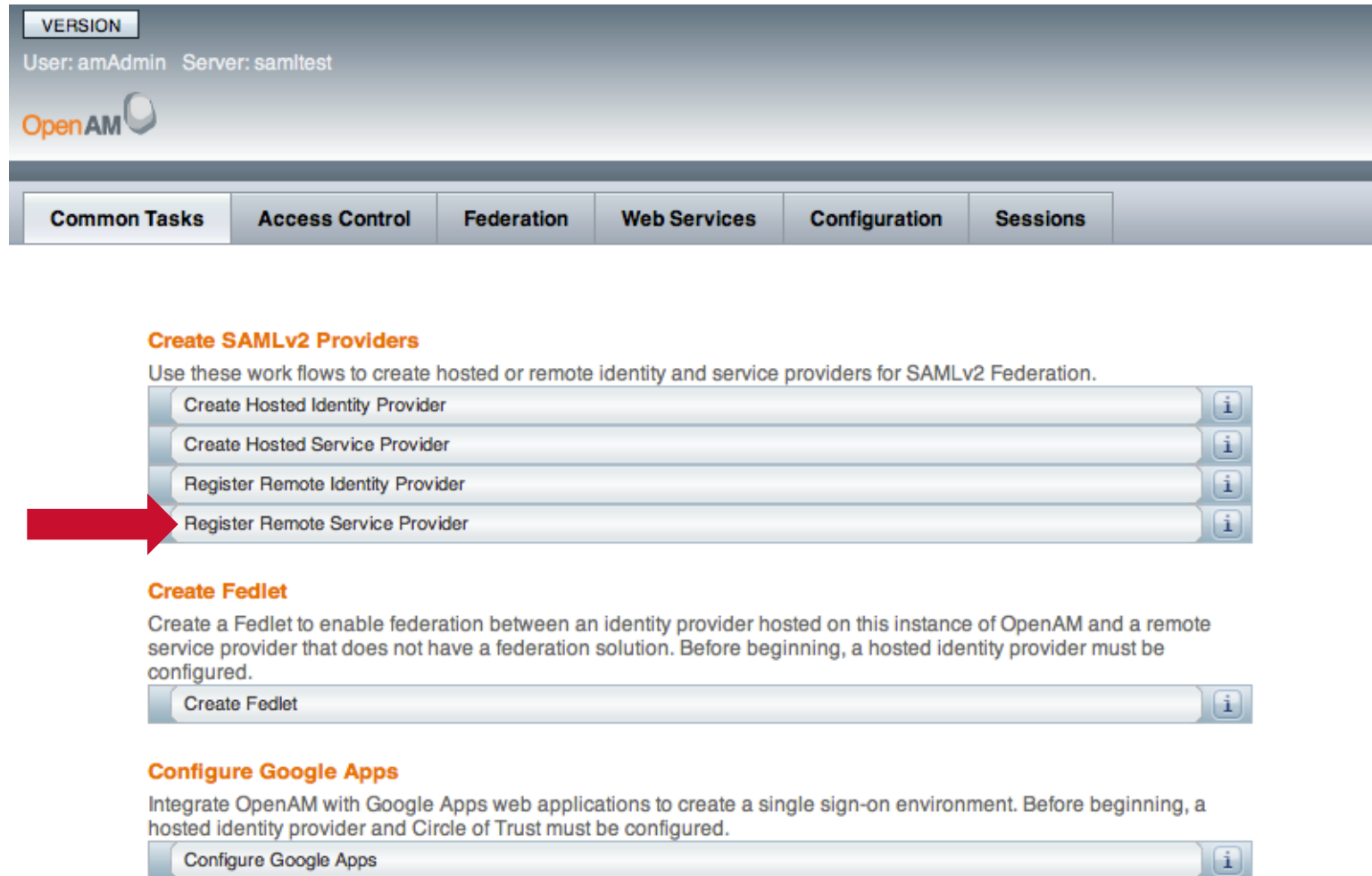
☐ Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

< Previous Next > Cancel

OpenAM

Registrering af metadata i Identity Provider: OpenAM (side 1 af 2)



VERSION

User: amAdmin Server: samtest

OpenAM

Common Tasks Access Control Federation Web Services Configuration Sessions

Create SAMLv2 Providers

Use these work flows to create hosted or remote identity and service providers for SAMLv2 Federation.

- Create Hosted Identity Provider
- Create Hosted Service Provider
- Register Remote Identity Provider
- Register Remote Service Provider**

Create Fedlet

Create a Fedlet to enable federation between an identity provider hosted on this instance of OpenAM and a remote service provider that does not have a federation solution. Before beginning, a hosted identity provider must be configured.

- Create Fedlet

Configure Google Apps

Integrate OpenAM with Google Apps web applications to create a single sign-on environment. Before beginning, a hosted identity provider and Circle of Trust must be configured.

- Configure Google Apps

Registrering af metadata i Identity Provider: OpenAM (side 2 af 2)



Create a SAMLv2 Remote Service Provider

This page allows you to register a remote Service Provider (SP). You need two things: Circle of Trust (IDPs) and SPs that trust each other and in effect represents the confines within which all federation necessary to execute federation protocols (eg SAMLv2) as well as the mechanism to communicate.

Where does the metadata file reside?: ☐ URL ☒ File 

* URL where metadata is located: 

OS2FAKTOR

Registrering af metadata i Identity Provider: OS2faktor (side 1 af 2)

OS2faktor har en indbygget integration til Context Handler, og en egentlig opsætning er ikke nødvendig.

 Se tjenesteudbydere

Nedenfor listes alle de tjenesteudbydere som er opsat i løsningen. De tjenesteudbydere som er opsat via direkte integrationer inde i løsningen, kan ikke redigeres her, men blot ses. Alle andre tjenesteudbydere kan redigeres ved at klikke på blyants-ikonet ud for disse.

Anvend menupunktet "Opret ny tjenesteudbyder" i højre-menuen for at oprette en ny tjenesteudbyder.

Tjenesteudbydere

Navn	EntityId	Protokol	Status	Handler
Søg	Søg	Søg	Søg	
KOMBIT Context Handler	https://saml.adgangsstyring.stoettesystemerne.dk	SAML20	Aktiv	
OS2faktor selvbetjening	https://demo-selvbetjening.os2faktor.dk	SAML20	Aktiv	



Registrering af metadata i Identity Provider: OS2faktor (side 1 af 2)

Tilpas evt. hvorvidt der skal anvendes 2-faktor login til de enkelte tilsluttede brugervendte systemer, ved at tilgå detaljesiden for Context Handler i OS2faktor, og sæt flueben ud for de Brugervendte Systemer, som kræver 2-faktor login:

Kombit Brugervendte Systemer		
Navn	EntityId	Kræv altid 2-faktor
 SAPA Overblik	https://saml.sapaoverblik.dk	☒
 BBR	https://bbr.dk/	☐
 Danmarks Adresseregister	https://dar.dk	☐
 DUBU	https://saml.dubu.kombit.dk	☒

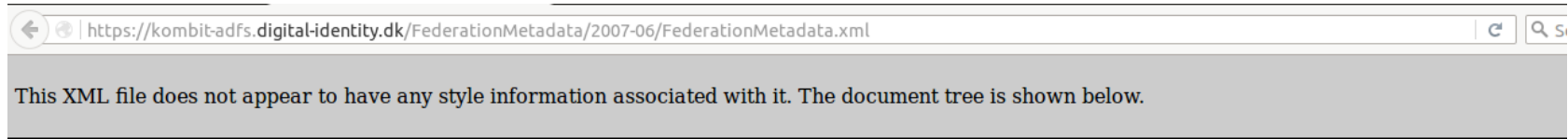
2. METADATA UDTRÆKKES OG REGISTRERES HOS KOMBIT

Udtræk metadata fra Identity Provider

Metadata fra kommunens egen IdP kan downloades fra den server, hvor IdP'en er installeret:

- Safewhere Identify: <https://<server>/runtime/saml2/metadata.idp>
- AD FS: <https://<server>/FederationMetadata/2007-06/FederationMetadata.xml>
- OpenAM: <https://<server>/openam/saml2/jsp/exportmetadata.jsp?entityid=<??>>
- OS2faktor: <https://<server>/sso/saml/metadata>

Udtræk metadata fra Identity Provider



```
-<EntityDescriptor ID="_440531c3-ab96-42b9-a2ae-4dc03e22de4b" entityID="http://kombit-adfs.digital-identity.dk/adfs/services/trust">
  -<ds:Signature>
    -<ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
      <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
      -<ds:Reference URI="#_440531c3-ab96-42b9-a2ae-4dc03e22de4b">
        -<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/xmldsig-more#sha256"/>
        <ds:DigestValue>rBZ99OgUkUlR0GhrxqAfeRhmRtH85jwf/m5xItTnaDg=</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
    -<ds:SignatureValue>
      Lmp0dFUeKwxokTQFN87oIZmawUXrpxWonIKiSoBJ+iPTDCN1aMVouKwmzZLO/AKL249yzGh4eS2SQm7Ecej5MzV8kK1UoNzYrBtHSCkEVBVvKON5{
    </ds:SignatureValue>
  -<KeyInfo>
    -<X509Data>
      -<X509Certificate>
        MIIGIzCCBQugAwIBAgIEUw/NqTANBgkqhkiG9w0BAQsFADBBHMQswCQYDVQQGEwJESzESMBAGA1UECgwJVfJVU1QyNDA4MSQwIgYDVQQD
        /KKneBo6ojLQf8ZgaXa6eFK15lyI4nGM3xZ/OgC8/vjsW2XWQE08vL09W8SKiujEt6xs967Z/Y4rNl1S8hZa5TVmBTlOEwEbmlzGB8tckVj14KnZ6kcZC
        /9yrr8hj7590vu3X0EkeI5dQAFPG41sUqzjDMZhZol5zhHCqkxXf0C+H+1gYYvNvEYGc1WXfaK0j3i66RcKAWJvozgfgjDQfwHsV7qswndxbvIhoZ6W7
        /ikfpws86/jLnoKvA5q3IGYJliwZssj85kcXmbhOpi1x9SjCRqgXldDVqiSEBVcuU8WKqvDVhloFJzpsDbWvjeGnlgtU0mK55tjYvm9i0leaoaAEKesRd2M
        /ZbC8tiok6eBwu4FvGqyrpm11xjQs
      </X509Certificate>
    </X509Data>
  </KeyInfo>
```

Krav om anvendelse af OCES-certifikat

Registrering af IdP i Fælleskommunalt Administrationsmodul

Forudsætning

For at kunne registrere jeres egen IdP og efterfølgende teste log-in med jobfunktionsroller, skal I først tilføjes som "myndighed" i KOMBITs testmiljø. Se afsnit 7 i [Brugervejledning til Administrationsmodulerne for leverandører](#).

I skal registrere jeres IdP i Fælleskommunalt Administrationsmodul. For at kunne gøre dette, skal du være logget ind med rollen "*Leverandøradministrator*". Hvis du ikke er tildelt denne rolle, skal du sørge for, at jeres NemLog-in administrator tildeler dig denne rolle i NemLog-in.

Guide til oprettelse og tildeling af roller i Nem-Login finder I [her](#).

1. Gå til listen af eksisterende it-systemer

It-systemer

[+ Tilslut it-system](#)

UUID	<u>Navn</u> ^	<u>Organisation</u>	Typer
f7e838...	KOMBIT Test Kommune	KOMBIT A/S	Identity Provider

Helpdesk: 70 11 15 39 - helpdesk@serviceplatformen.dk - KOMBIT A/S, Halldansgade 8, 2300 København S - CVR-nr.:

2. Indtast stamdata

Opgaveoversigt

Organisationer

It-systemer

Serviceaftaler

Føderationsaftaler

Jobfunktionsroller

Rapporter

Brugerprofiler

KOMBIT Administration

Aftalebetingelser

Adviseringer

Dataafgrænsningstyper

Servicekoblinger

Visningsgrupper

Servicegrupper

Provisionering

Tilslut it-system

Stamdata	Dataafgrænsningstyper	Anvendersystem	Brugervendt system	Identity Provider	Serviceudbyder
UUID:	Normalt ikke udfyldt ?				
Leverandør:	KOMBIT A/S ▼				
Navn:	KOMBITs Identity Provider				
E-mail:	support@kombit.dk ?				
Beskrivelse:	Det it-syste vi bruger til at logge vores brugere på fagsystemer i infrastrukturen				

Helpdesk: 70 11 15 39 - helpdesk@serviceplatformen.dk - KOMBIT A/S, Halldansgade 8, 2300 København S - CVR-nr.: 19435075 - EAN-nr. 5790001969370

3. Angiv type af it-system

The screenshot shows the 'It-systemer' section of the KOMBIT administration interface. On the left is a dark sidebar with a menu containing: Opgaveoversigt, Organisationer, It-systemer (highlighted in blue), Serviceaftaler, Føderationsaftaler, Jobfunktionsroller, Rapporter, Brugerprofiler, KOMBIT Administration, Aftalebetingelser, Adviseringer, Dataafgrænsningstyper, Servicekoblinger, Visningsgrupper, Servicegrupper, and Provisionering. The main content area has a 'Beskrivelse:' field with the text 'Det it-syste vi bruger til at logge vores brugere på fagsystemer i infrastrukturen'. Below this is a 'Type:' section with four radio buttons: 'Anvendersystem', 'Brugervendt system', 'Identity Provider' (which is selected), and 'Serviceudbyder'. A note below the radio buttons states: 'Vær opmærksom på at du ikke kan vælge systemtyper fra, når først du har gemt.' At the bottom of the main area is a grey bar labeled 'Afgrænsning af myndighed' with a right-pointing arrow. Below this bar is a blue link 'Accepter vilkår og betingelser'. At the very bottom are two buttons: 'Gem' (blue) and 'Annuller' (grey). A footer at the bottom of the page contains contact information: 'Helpdesk: 70 11 15 39 - helpdesk@serviceplatformen.dk - KOMBIT A/S, Halldansgade 8, 2300 København S - CVR-nr.: 19435075 - EAN-nr. 5790001969370'.

Opgaveoversigt

Organisationer

It-systemer

Serviceaftaler

Føderationsaftaler

Jobfunktionsroller

Rapporter

Brugerprofiler

KOMBIT Administration

Aftalebetingelser

Adviseringer

Dataafgrænsningstyper

Servicekoblinger

Visningsgrupper

Servicegrupper

Provisionering

Beskrivelse:

Det it-syste vi bruger til at logge vores brugere på fagsystemer i infrastrukturen

Type:

☐ Anvendersystem

☐ Brugervendt system

☒ Identity Provider

☐ Serviceudbyder

Vær opmærksom på at du ikke kan vælge systemtyper fra, når først du har gemt.

Afgrænsning af myndighed

[Accepter vilkår og betingelser](#)

Gem Annuller

Helpdesk: 70 11 15 39 - helpdesk@serviceplatformen.dk - KOMBIT A/S, Halldansgade 8, 2300 København S - CVR-nr.: 19435075 - EAN-nr. 5790001969370

4a. For Context Handler 1 (gammel version):

Upload metadatafil

Understøtter Context Handler: ☒

SAML metadatafiler: *



Træk SAML metadata fil herind



Understøtter Context Handler NSIS: ☒

OIOSAML Profil: *

OIOSAML2





Udbudt NSIS assurance level:





NSIS SAML metadatafil: *



Træk SAML metadata fil herind



4b. For Context Handler 2 (ny version):

Enten upload metadatafil

Understøtter Context Handler NSIS: ☒

OIOSAML Profil: * ?

Udbudt NSIS assurance level: ?

NSIS SAML metadatafil: * ?

NSIS SAML metadata URL: * ?
NSIS SAML Metadata URL skal udfyldes når understøttelse er valgt og NSIS SAML metadatafil ikke er uploadet.

ADFS Produkttype: ☐

[Accepter vilkår og betingelser](#)

Eller registrér metadata-URL

Understøtter Context Handler NSIS: ☒

OIOSAML Profil: * ?

Udbudt NSIS assurance level: ?

NSIS SAML metadatafil: * ?

NSIS SAML metadata URL: * ?
NSIS SAML Metadata URL skal udfyldes når understøttelse er valgt og NSIS SAML metadatafil ikke er uploadet.

ADFS Produkttype: ☐

[Accepter vilkår og betingelser](#)

5. Specifikt for ADFS-IdP'er - *kun* for Context Handler 2

ADFS IdP-produkter kan som udgangspunkt ikke håndtere krævede sikringsniveauer (hverken NIST eller NSIS).

Hvis din IdP er en ADFS-produkttype, er det derfor vigtigt, at du sætter hak ved *"ADFS Produkttype"* i registreringen af IdP'en i Fælleskommunalt Administrationsmodul:

The screenshot shows the 'It-systemer' section of the Fælleskommunalt Administrationsmodul. The 'ADFS Produkttype' checkbox is checked and highlighted with a red box. Other fields include 'Understøtter Context Handler' (checked), 'NSIS' (empty), 'OIOSAML Profil' (set to 'OIOSAML2'), 'Udbudt NSIS assurance level' (empty), 'NSIS SAML metadatafil' (empty), and 'NSIS SAML metadata URL' (empty).

Certifikat	Udløb
Kombit_Test_ADFS	2026-08-20



OBS

Når der er sat hak ved *"ADFS Produkttype"* sker der følgende, når et brugervendt system kræver et givent sikringsniveau:

- Hvis der kræves NIST-sikringsniveau 3 eller NSIS-sikringsniveau *"Betydelig"*:
Sendes et ADFS-specifikt multipleauthn med
- Hvis der kræves NIST-sikringsniveau 1-2 eller NSIS-sikringsniveau *"Lav"*:
Sendes der ikke noget sikringsniveau med

Hvis der derimod *ikke* er sat hak ved *"ADFS Produkttype"*, sendes det sikringsniveau, et brugervendt system kræver, med til IdP'en. Det kan en ADFS-IdP som udgangspunkt ikke håndtere.

6. Gå til liste over føderationsaftaler

Føderationsaftaler

[+ Anmod om føderationsaftale](#)

UUID	Navn ^	Identity_provider	Myndighed	Status
260d79...	KOMBIT Test Kommune - KOMBIT A/S	KOMBIT Test Kommune	KOMBIT A/S	Godkendt

Helpdesk: 70 11 15 39 - helpdesk@serviceplatformen.dk - KOMBIT A/S, Halfdansgade 8, 2300 København S - CVR-nr.: 19435075 - EAN-nr. 5790001969370

7. Udfyldt anmodning

Opgaveoversigt

Organisationer

It-systemer

Serviceaftaler

Føderationsaftaler

Jobfunktionsroller

Rapporter

Brugerprofiler

KOMBIT Administration

Aftalebetingelser

Adviseringer

Dataafgrænsningstyper

Servicekoblinger

Visningsgrupper

Servicegrupper

Provisionering

Anmod om føderationsaftale

Stamdata	Identity provider	Myndighed	Godkend
Navn:	Aftale om login		
Begrundelse:	Denne aftale indgås for at vores Identity Provider kan logge brugere på for netop vores myndighed ?		
Gyldig fra:	2019-02-28		
Gyldig til:			

Udfyld navn, gyldighedsperiode samt en begrundelse.

Heldesk: 70 11 15 39 - heldesk@serviceplatformen.dk - KOMBIT A/S. Halldansgade 8. 2300 København S - CVR-nr.: 19435075 - EAN-nr. 5790001969370

8. Vælg ny-oprettet Identity Provider

Opgaveoversigt

Organisationer

It-systemer

Serviceaftaler

Føderationsaftaler

Jobfunktionsroller

Rapporter

Brugerprofiler

KOMBIT Administration

Aftalebetingelser

Adviseringer

Dataafgrænsningstyper

Servicekoblinger

Visningsgrupper

Servicegrupper

Provisionering

Anmod om føderationsaftale

Stamdata

Identity provider

Myndighed

Godkend

UUID

Navn ^

Leverandør

kombit

kombit

f7e838...

KOMBIT Test Kommune

KOMBIT A/S

i

Forrige

Næste

Vælg et anvendelsesystem fra listen.
Anvendelsesystemet kan fremsøges ved at begynde at skrive i et af felterne: UUID, Navn eller Leverandør.

Helpdesk: 70 11 15 39 - helpdesk@serviceplatformen.dk - KOMBIT A/S, Halldansgade 8, 2300 København S - CVR-nr.: 19435075 - EAN-nr. 5790001969370

9. Vælg egen myndighed

Opgaveoversigt

Organisationer

It-systemer

Serviceaftaler

Føderationsaftaler

Jobfunktionsroller

Rapporter

Brugerprofiler

KOMBIT Administration

Aftalebetingelser

Adviseringer

Dataafgrænsningstyper

Servicekoblinger

Visningsgrupper

Servicegrupper

Provisionering

Anmod om føderationsaftale

Stamdata

Identity provider

Myndighed

Godkend

Vælg en eller flere myndigheder fra listen. Myndigheder kan fremsøges ved at begynde at skrive navnet i et af felterne.

Myndighed ^

kombit

KOMBIT A/S

Forrige

Næste

Helpdesk: 70 11 15 39 - helpdesk@serviceplatformen.dk - KOMBIT A/S, Halfdansgade 8, 2300 København S - CVR-nr.: 19435075 - EAN-nr. 5790001969370

10. Se liste over afventende aftaler

Opgaveoversigt

Organisationer

It-systemer

Serviceaftaler

Føderationsaftaler

Jobfunktionsroller

Rapporter

Brugerprofiler

KOMBIT Administration

Aftalebetingelser

Adviseringer

Dataafgrænsningstyper

Servicekoblinger

Visningsgrupper

Servicegrupper

Provisionering

Føderationsaftaler

+ Anmod om føderationsaftale

UUID	Navn ^	Identity_provider	Myndighed	Status
			kombit	afventer
1e9d50...	Aftale om login	KOMBIT Test Kommune	KOMBIT A/S	Afventer

Helpdesk: 70 11 15 39 - helpdesk@serviceplatformen.dk - KOMBIT A/S, Halfdansgade 8, 2300 København S - CVR-nr.: 19435075 - EAN-nr. 5790001969370

11. Godkend aftale

Opgaveoversigt

Organisationer

It-systemer

Serviceaftaler

Føderationsaftaler

Jobfunktionsroller

Rapporter

Brugerprofiler

KOMBIT Administration

Aftalebetingelser

Adviseringer

Dataafgrænsningstyper

Servicekoblinger

Visningsgrupper

Servicegrupper

Provisionering

Aftale om login

Status:	Afventer	UUID:	1e9d5012-a939-4208-b96a-a8139cbc2fd7
System:	KOMBIT Test Kommune	Oprettet:	2019-02-28 05:53:39 af Brian Storm Graversen, KOMBIT A/S
Begrundelse:	Denne aftale indgås for at vores Identity Provider kan logge brugere på for netop vores myndighed		
Betingelser:	Vis vilkår og betingelser ved anmodning	Ændret:	2019-02-28 05:53:39 af Brian Storm Graversen, KOMBIT A/S
Myndighed:	KOMBIT A/S		
Gyldig fra:	2019-02-28		
Gyldig til:	?		

Godkend

Afvis

Tilbage

Slet

Helpdesk: 70 11 15 39 - helpdesk@serviceplatformen.dk - KOMBIT A/S, Halldansgade 8, 2300 København S - CVR-nr.: 19435075 - EAN-nr. 5790001969370

Når aftalen er godkendt

Login Page

Please select an authentication method

Hvidovre Kommune ▼

- Albertslund Kommune
- Digital Identity Kommune
- Dragør Kommune
- Favrskov Kommune
- Faaborg-Midtfyn Kommune
- Hvidovre Kommune
- Syddjurs Kommune**
- Vallensbæk Kommune
- Aarhus Kommune

connection

3. IDENTITY PROVIDER TILPASSES KOMBITS ATTRIBUTPROFIL

KOMBITs Attributprofil

```
<Assertion>
  <Issuer>https://vallensbaek.dk/</Issuer>
  <Signature> ... </signature>
  <Subject>
    <NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
      C=DK,O=19583910,CN=Gitte Jensen,Serial=e8a0f8a6-2393-4c46-b96c-214afebaa616
    </NameID>
    <SubjectConfirmation> ... </SubjectConfirmation>
  </Subject>
  <Conditions> ... </Conditions>
  <AttributeStatement>
    <Attribute Name="dk:gov:saml:attribute:CvrNumberIdentifier">
      <AttributeValue>19583910</AttributeValue>
    </Attribute>
    <Attribute Name="dk:gov:saml:attribute:AssuranceLevel">
      <AttributeValue>3</AttributeValue>
    </Attribute>
    <Attribute Name="dk:gov:saml:attribute:SpecVer">
      <AttributeValue>DK-SAML-2.0</AttributeValue>
    </Attribute>
    <Attribute Name="dk:gov:saml:attribute:KombitSpecVer">
      <AttributeValue>1.0</AttributeValue>
    </Attribute>
    <Attribute Name="dk:gov:saml:attribute:Privileges_intermediate">
      <AttributeValue>PD94bWwgdmVyc2lvdj0iMS4wIiBlbmNvZGluZz0...</AttributeValue>
    </Attribute>
  </AttributeStatement>
</Assertion>
```

Standard formatering, Serial skal være unik!

Krævede attributter

Privilegier, der er
Base 64 encoded

Statiske attributter: Safewhere Identify

1

Identify Web Administration
Safewhere Identify*Admin build 4.2.0.155 Copyright © Safewhere 2014

Transformations

Home > Organization: Root > All transformations

All transformations

New Filter View All

Create Organization

Create a new organization under the current organization

"Claim Value" Transformation

Create "Claim Value" Transformation

"Claim Mapping" Transformation

Create "Claim Mapping" Transformation

"Exclude Passthrough Claims" Transformation

Create "Exclude Passthrough Claims" Transformation

"Exclude Identify Claims" Transformation

Create "Exclude Identify Claims" Transformation

"Claim Filter" Transformation

Create "Claim Filter" Transformation

SQL Transformation

SQL Transformation

External Transformation

Create "External Transformation"

Create LDAP Attribute Transformation

Create a new LDAP attribute transformation

Create User Account Update transformation

Create a new user account update transformation

Create "NameId Format" Transformation

Create a NameId format transformation

Create "Scripting" Transformation

Create a "Scripting" transformation

2

Identify Web Administration
Safewhere Identify*Admin build 4.2.0.155 Copyright © Safewhere 2014

Language: English | Danish You are logged in as: masadmin | Sign off

My Profile Groups Users Claims System Setup Transformations Connections

Home > Organization: Root > Add Claim Transformation: "Scripting" Transformation

Add Claim Transformation: "Scripting" Transformation

Transformation Name
Give the Transformation a unique name that will make it easy to remember when setting up a Claim Pipeline.

- § Transformation Name
All characters are allowed, but the name should be between 1 and 60 characters long.

Transformation Name:*

3

Script claim
This section helps specify what the script should be.

Script:

```
if (!Match("dk:gov:saml:attribute:SpecVer", "DK-SAML-2.0"))
{
  Issue("dk:gov:saml:attribute:SpecVer","DK-SAML-2.0");
}

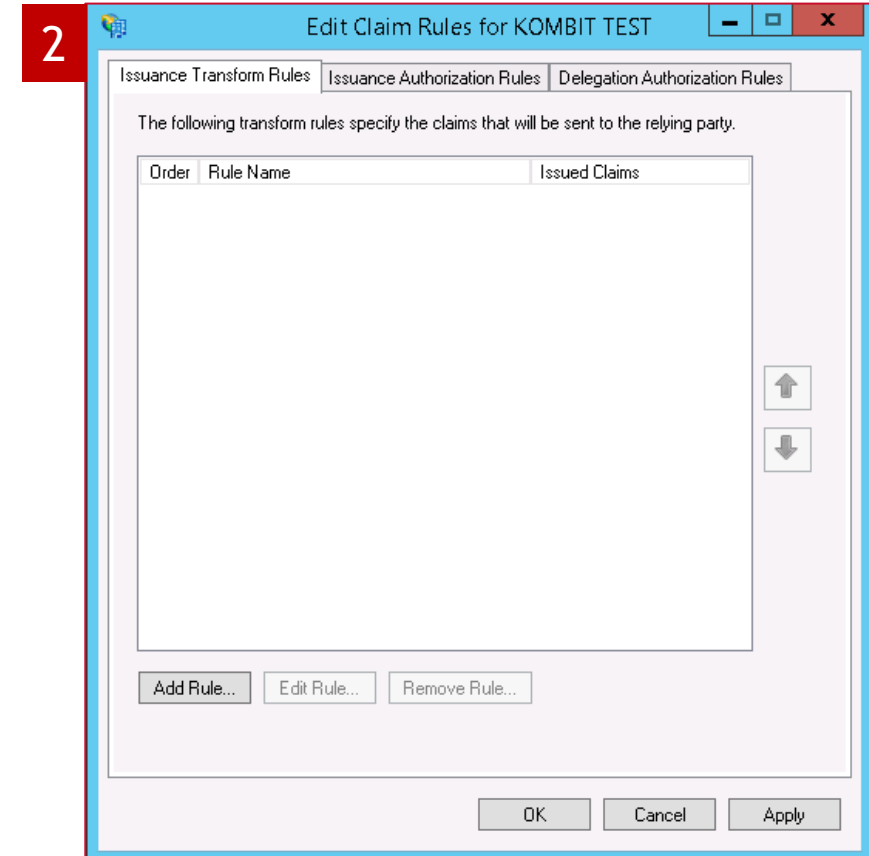
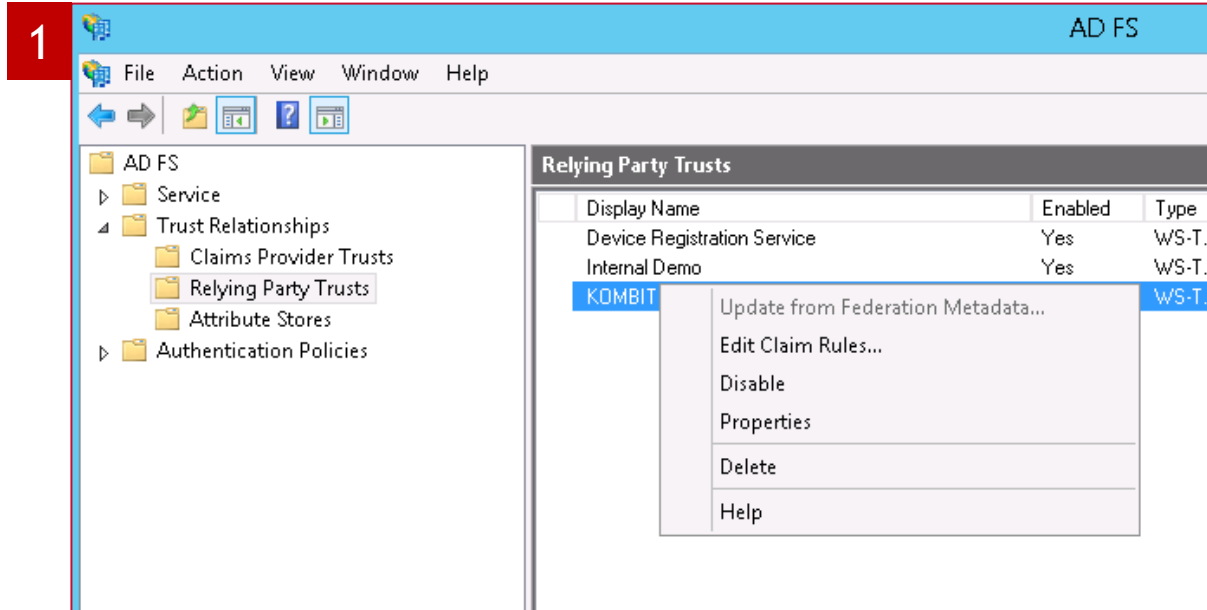
if (!Exist("dk:gov:saml:attribute:AssuranceLevel"))
{
  Issue("dk:gov:saml:attribute:AssuranceLevel","3");
}

if (!Match("dk:gov:saml:attribute:KombitSpecVer", "1.0"))
{
  Issue("dk:gov:saml:attribute:KombitSpecVer","1.0");
}
```

[Open expanded editor](#)

Save Save & Close Cancel

Statische attributter: AD FS 3.0 (side 1 af 2)



Statische attributter: AD FS 3.0 (side 2 af 2)

3

Add Transform Claim Rule Wizard

Select Rule Template

Steps

- Choose Rule Type
- Configure Claim Rule**

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template:

Send Claims Using a Custom Rule

Claim rule template description:

Using a custom rule, you can create rules that can't be created with a rule template. Custom rules are written in the AD FS claim rule language. Capabilities that require custom rules include:

- Sending claims from a SQL attribute store
- Sending claims from an LDAP attribute store using a custom LDAP filter
- Sending claims from a custom attribute store
- Sending claims only when 2 or more incoming claims are present
- Sending claims only when an incoming claim value matches a complex pattern
- Sending claims with complex changes to an incoming claim value
- Creating claims for use only in later rules

< Previous Next > Cancel

4

Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type**
- Configure Claim Rule

You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS claim rule language.

Claim rule name:

KombitSpecVer

Rule template: Send Claims Using a Custom Rule

Custom rule:

```
=> issue(Type = "dk:gov:saml:attribute:KombitSpecVer",  
        Value = "1.0",  
        Properties  
        ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/attrib  
ute:username"] = "urn:oasis:names:tc:SAML:2.0:attrname-format:basic");
```

< Previous Finish Cancel

Statiske attributter: OpenAM

OpenAM anvender en AttributeMapper til at udvælge hvilke attributter på brugerens konto (fx AD-konto), der mappes til hvilke attributter i det udgående token. Fx på følgende måde:

```
dk:gov:saml:attribute:AssuranceLevel=assuranceLevel
```

Hvis man ønsker at anvende statiske værdier, understøttes det fra OpenAM 11 på følgende måde:

```
dk:gov:saml:attribute:AssuranceLevel="3"
```

Statiske attributter: **OS2faktor**

OS2faktor understøtter alle de statiske attributter, som er krævet af Context Handler, og ingen yderligere opsætning er nødvendig.

**JOBFUNKTIONSROLLER
ANGIVES SOM OIO-BPP**

Jobfunktionsroller i Attributprofilen

```
<Assertion>
  <Issuer>
  <Signature>
  <Subject>
    <Name>
      <bpp:PrivilegeList xmlns:bpp="http://itst.dk/oiosaml/basic_privilege_profile">
        <PrivilegeGroup Scope="urn:dk:gov:saml:cvrNumberIdentifier:19583910">
          <Privilege>http://vallensbaek.dk/roles/jobrole/sagsbehandler/1</Privilege>
        </PrivilegeGroup>
        <PrivilegeGroup Scope="urn:dk:gov:saml:cvrNumberIdentifier:19583910">
          <Privilege>http://vallensbaek.dk/roles/jobrole/leder/1</Privilege>
        </PrivilegeGroup>
      </bpp:PrivilegeList>
    </Name>
    <Attribute Name="dk:gov:saml:attribute:AssuranceLevel">
      <AttributeValue>3</AttributeValue>
    </Attribute>
    <Attribute Name="dk:gov:saml:attribute:SpecVer">
      <AttributeValue>DK-SAML-2.0</AttributeValue>
    </Attribute>
    <Attribute Name="dk:gov:saml:attribute:KombitSpecVer">
      <AttributeValue>1.0</AttributeValue>
    </Attribute>
    <Attribute Name="dk:gov:saml:attribute:Privileges_intermediate">
      <AttributeValue>PD94bWwgdmVyc2lvdj0iMS4wIiBlbmNvZGluZz0...</AttributeValue>
    </Attribute>
  </AttributeStatement>
</Assertion>
```

Base64 enkodet OIO-BPP struktur

Hvordan enkodes én jobfunktionsrolle

1 PrivilegeGroup = 1 jobfunktionsrolle

CVR-nr. for den kommune, der ejer rollen (typisk egen kommune)

```
<bpp:PrivilegeList xmlns:bpp="http://itst.dk/oiosaml/basic_privilege_profile">  
  <PrivilegeGroup Scope="urn:dk:gov:saml:cvrNumberIdentifier:19583910">  
    <Privilege>http://vallensbaek.dk/roles/jobrole/sagsbehandler/1</Privilege>  
  </PrivilegeGroup>  
  <PrivilegeGroup Scope="urn:dk:gov:saml:cvrNumberIdentifier:19583910">  
    <Privilege>http://vallensbaek.dk/roles/jobrole/leder/1</Privilege>  
  </PrivilegeGroup>  
</bpp:PrivilegeList>
```

ID på jobfunktionsrollen
(matcher ID registreret hos KOMBIT)

OIO-BPP er bare en enkelt attribut/claim

- Identity Provideren skal tilpasses, så den kan danne en OIO-BPP-struktur, der indeholder de ID'er på jobfunktionsroller, som medarbejderen er tildelt.
- OIO-BPP-strukturen base64 enkodes, og udstedes som en SAML-attribut på lige fod med de statiske attributter.

`dk:gov:saml:attribute:Privileges_intermediate`

4. TEST AF IDENTITY PROVIDER

TEST AF LOGIN-FLOW - CONTEXT HANDLER 1 (GAMMEL VERSION)

Test mod demo-system - Context Handler 1

I test-miljøet stiller KOMBIT et demosystem til rådighed, hvor man kan foretage et login: <https://demo-brugervendtsystem.kombit.dk/test>

- Systemet har ingen anden funktionalitet end login
- Efter succesfuld login, vises et skærm billede, der viser det token, som demo-systemet har modtaget

Test mod demo-system - Context Handler 1

[Demo Brugervendt System](#) [Hjem](#)

Demo Brugervendt System

Dette demo system anvendes alene til at teste login funktionalitet i Adgangsstyring for Brugere. Ved at klikke på linket nedenfor, vil man blive sendt videre til Adgangsstyring for Brugere (Context Handleren), hvor man kan gennemføre et login med den Identity Provider man har tilsluttet det eksterne testmiljø.

[Login](#)

Brugersystemroller

For at understøtte en test af Jobfunktionsroller og Brugersystemroller, er der oprettet 3 Brugersystemroller til dette Demo Brugervendte System.

Brugersystemrolle	Dataafgrænsninger
http://demo-brugervendtsystem.kombit.dk/roles/usersystemrole/adgang/1	<i>ingen</i>
http://demo-brugervendtsystem.kombit.dk/roles/usersystemrole/se_sag/1	http://sts.kombit.dk/constraint/KLE/1
http://demo-brugervendtsystem.kombit.dk/roles/usersystemrole/opdater_sag/1	http://sts.kombit.dk/constraint/KLE/1 http://sts.kombit.dk/constraint/orgenhed/1

Typiske udfordringer

- Spærrecheck af certifikat fejler (kun test-miljø)
- En af de fire krævede attributter mangler
- NameID ikke på x509 format
- Anvender sha-1 algoritmen (sha-256 krævet)

Test mod demo-system - Context Handler 1

Demo Brugervendt System

Hjem

Login oplysninger

Logout

Attribute	Value
NameID	C=DK,O=36074051,CN=user1,Serial=407417b2-7c7e-405a-aeda-69900b8b2b49
SpecVer	DK-SAML-2.0
KombitSpecVer	1.0
AssuranceLevel	3
Cvridentifier	36074051
Privileges_intermediate	<pre><bpp:PrivilegeList xmlns:bpp="http://itst.dk/oiosaml/basic_privilege_profile" xmlns:xsi="http://www.w3.org/2001/XMLSchema" > <PrivilegeGroup Scope="urn:dk:gov:saml:cvrNumberIdentifier:36074051"> <Privilege>http://demo-brugervendtsystem.kombit.dk/roles/usersystemrole/adgang/1</Privilege> </PrivilegeGroup> </bpp:PrivilegeList></pre>

TEST AF LOGIN-FLOW - CONTEXT HANDLER 2 (NY VERSION)

Test af login-flow - Context Handler 2

Den nye version af Context Handler (Context Handler 2) understøtter:

- IdP'er, der anvender NIST-baserede sikringsniveauer (AssuranceLevel 1-4) samt
- IdP'er, der anvender NSIS-baserede sikringsniveauer (Lav, Betydelig og Høj)

Det er muligt at teste, at en IdP er korrekt tilkoblet Context Handler 2, og at den kan gennemføre et login med korrekt sikringstype (NIST eller NSIS). Der er testværktøjer til både Eksternt testmiljø og Produktionsmiljøet. Flows er præcis de samme, derfor er skærmbilleder på de følgende sider kun fra Eksternt testmiljø.

Testværktøjer Eksternt testmiljø:

- NIST-sikringsniveauer: <https://spwithoutnsis.eksterntest-stoettesystemerne.dk/>
- NSIS-sikringsniveauer: <https://spwithnsis.eksterntest-stoettesystemerne.dk/>

Testværktøjer Produktionsmiljø:

- NIST-sikringsniveauer: <https://spwithoutnsis.stoettesystemerne.dk/>
- NSIS-sikringsniveauer: <https://spwithnsis.stoettesystemerne.dk/>

1. Test af login-flow med NIST-sikringsniveauer

1 .Vælg mellem

Eksternt testmiljø: <https://spwithoutnsis.ekstern-test-stoettesystemerne.dk>

eller Produktionsmiljø: <https://spwithoutnsis.stoettesystemerne.dk/>



Ekstern Test - brugervendt demo med NIST

- [Go to My Page \(required assurance level not specified\)](#)
- [Go to My Page \(require assurance level 2\)](#)
- [Go to My Page \(require assurance level 3\)](#)
- [Go to My Page \(require assurance level 4\)](#)

Metadata

The identity provider and the service provider must exchange metadata in order to establish SAML connections. The Identity provider's metadata should be put in the directory "C:\inetpub\wwwroot\ServiceProviderWebApp_Non-NSIS\idp-metadata".

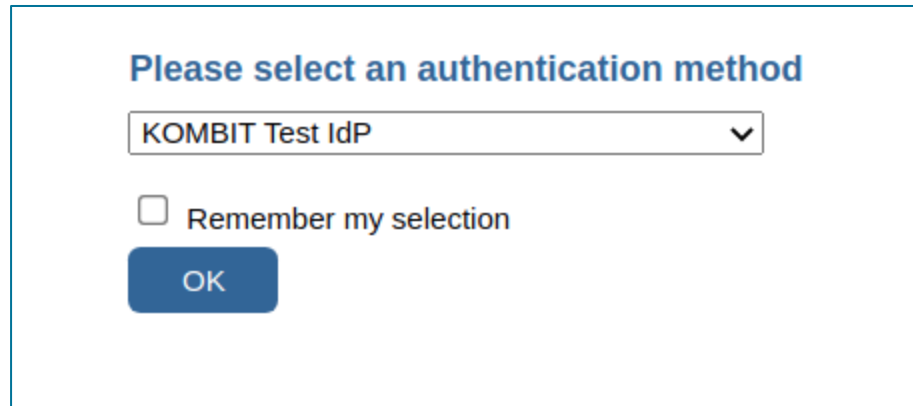
The metadata of the service provider can be downloaded [here](#).

© OIOSAML.NET (www.oiosaml.info).

2. Vælg krævet assurance level ved at klikke på 'Go to My Page' for at starte login-flow

2. Test af login-flow med NIST-sikringsniveauer

Browseren vil gå til Context Handler 2, hvor du i dropdown skal vælge den IdP, du ønsker at teste:



Please select an authentication method

KOMBIT Test IdP ▼

☐ Remember my selection

OK

Når du har klikket 'OK', sendes du til den tilsluttede IdP, hvor et login gennemføres som normalt.

3a. Test af login-flow med NIST-sikringsniveauer

Hvis IdP er opsat korrekt, vil browseren ende på en statusside for testtjenesten, hvor du kan se de attributter, der er knyttet til den bruger, der har gennemført login (bemærk, at der anvendes de attributter, som findes i OIOSAML 2.0 og KOMBITs Attributprofil 1.0):



OIOSAML.NET

Welcome, C=DK,O= xxxxxxxx ,CN= yyyyyy ,Serial= zzzzzz-zzz-zzz-zzzzzzzzzzz

SAML attributes

Attribute name	Attribute value
dk:gov:saml:attribute:AssuranceLevel	3
dk:gov:saml:attribute:SpecVer	DK-SAML-2.0
dk:gov:saml:attribute:KombitSpecVer	1.0
dk:gov:saml:attribute:CvrNumberIdentifier	xxxxxxxx

Hvis du får et lignende resultat, er IdP korrekt tilsluttet Context Handler 2, og kan gennemføre login til tjenester, der kræver NIST-sikringsniveau.

3b. Test af login-flow med NIST-sikringsniveauer

Hvis der testes med en bruger, der er tildelt brugersystemrollen "*Test rolle 1*" fra systemet "*STS Serviceprovider without NSIS*", vil statussiden ved succesfuldt login også vise den medsendte rolle (privilegie):



OIOSAML.NET

Welcome, C=DK,O= xxxxxxxx ,CN= yyyyyyy ,Serial= zzzzzz-zzzz-zzzz-zzzzzzzzz

SAML attributes

Attribute name	Attribute value
dk:gov:saml:attribute:AssuranceLevel	3
dk:gov:saml:attribute:SpecVer	DK-SAML-2.0
dk:gov:saml:attribute:KombitSpecVer	1.0
dk:gov:saml:attribute:CvrNumberIdentifier	xxxxxxxx
dk:gov:saml:attribute:Privileges_intermediate	PD94bWwgdMvYc2lvbj0iMS4wLjIiB4bWwuc2p4c2k9Imh0dHA6Ly93d3cudzMub3JnLjZwMDEvWE1MU2NoZW1hLWluc3RhbmNlIj48UHJpdmlsZWdlR3JvdXAgU2NvcGU9InVybjpkazpnb3Y6c2FtbDpjdnJ0dW1iZXJJZGVudGhmaWVyojExMTExMTExIj48UHJpdmlsZWdlPmh0dHA6Ly9la3N0ZXJudGVzdC1zdG9ldHRlc3lzdGVtZXJuZS5kay9yb2xley91c2Vyc3lzdGVtc m9sZS90ZXN0cm9sbGUxLzE8L1ByaXZpbGVnZT48L1ByaXZpbGVnZUdyb3VwPjwvYnBwOlByaXZpbGVnZUxpc3Q+

Basic Privilege Profile of the dk:gov:saml:attribute:Privileges_intermediate

Scope	Privilege	Constraints
urn:dk:gov:saml:cvrNumberIdentifier:11111111	http://eksterntest-stoettesystemerne.dk/roles/usersystemrole/testrolle1/1	

Hvis du får et lignende resultat, er IdP korrekt tilsluttet Context Handler 2, og kan både gennemføre login til tjenester, der kræver NIST-sikringsniveau samt medsende privilegier.

1. Test af login-flow med NSIS-sikringsniveauer

1 .Vælg mellem

Eksternt testmiljø: <https://spwithnsis.ekstern-test-stoettesystemerne.dk/>

eller Produktionsmiljø: <https://spwithnsis.stoettesystemerne.dk/>



Ekstern Test - brugervendt demo med NSIS

- [Go to My Page \(required assurance level not specified\)](#)
- [Go to My Page \(require low assurance level\)](#)
- [Go to My Page \(require substantial assurance level\)](#)
- [Go to My Page \(require high assurance level\)](#)
- [Go to My Page \(request a Professional attribute profile\)](#)

Metadata

The identity provider and the service provider must exchange metadata in order to establish SAML connections. The Identity provider's metadata should be put in the directory "C:\inetpub\wwwroot\ServiceProviderWebApp_NSIS\idp-metadata".

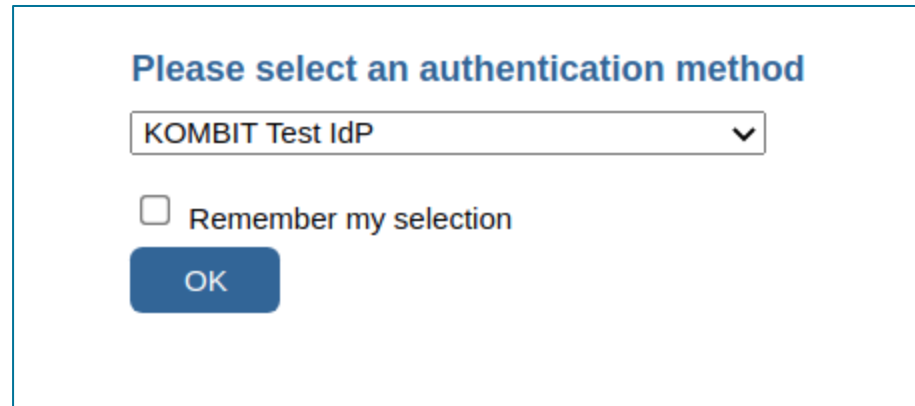
The metadata of the service provider can be downloaded [here](#).

© OIOSAML.NET (www.oiosaml.info).

2. Vælg krævet assurance level ved at klikke på 'Go to My Page' for at starte login-flow

2. Test af login-flow med NSIS-sikringsniveauer

Browseren vil gå til Context Handler 2, hvor du i dropdown skal vælge den IdP, du ønsker at teste:



Please select an authentication method

KOMBIT Test IdP ▼

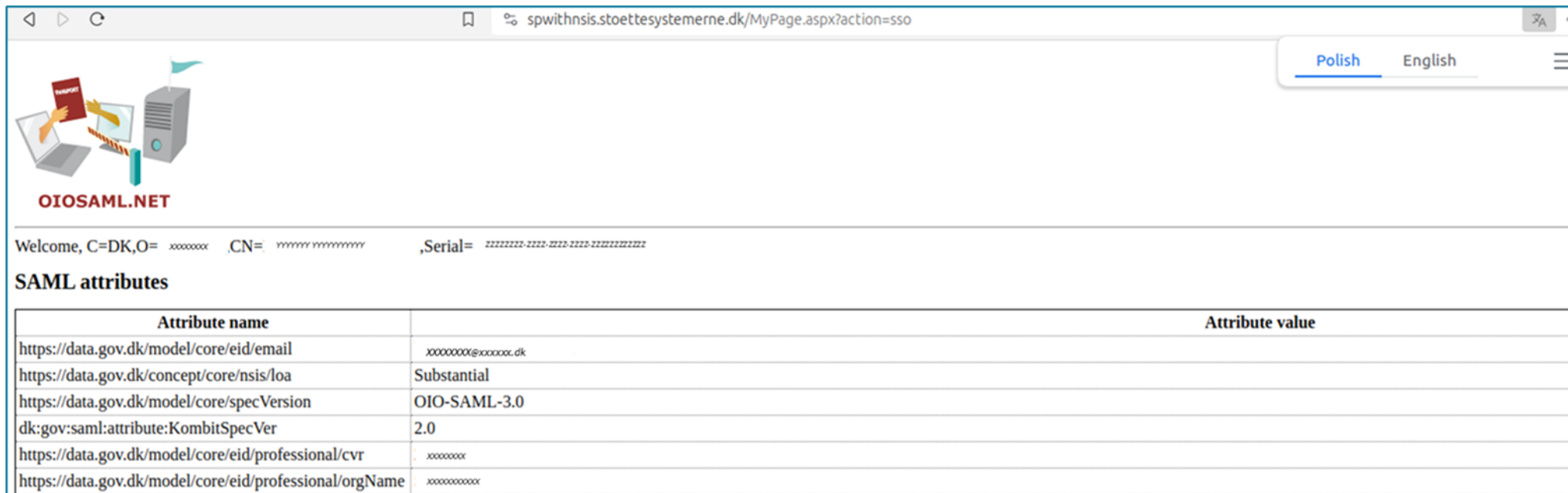
☐ Remember my selection

OK

Når du har klikket 'OK', sendes du til den tilsluttede IdP, hvor et login gennemføres som normalt.

3a. Test af login-flow med NSIS-sikringsniveauer

Hvis IdP er opsat korrekt, vil browseren ende på en statusside for testtjenesten, hvor du kan se de attributter, der er knyttet til den bruger, der har gennemført login (bemærk, at der anvendes de attributter, som findes i OIOSAML 3.0 og KOMBITs Attributprofil 2.0):



Hvis du får et lignende resultat, er IdP korrekt tilsluttet Context Handler 2, og kan gennemføre login til tjenester, der kræver NSIS-sikringsniveau.

3b. Test af login-flow med NSIS-sikringsniveauer

Hvis der testes med en bruger, der er tildelt brugersystemrollen "*Test rolle 1*" fra systemet "*STS Serviceprovider with NSIS*", vil statussiden ved succesfuldt login også vise den medsendte rolle (privilegie):



Welcome, C=DK,O= xxxxxxxx ,CN= yyyyyy yyyyyyyy ,Serial= zzzzzzzz-zzzz-zzzz-zzzzzzzzzzz

SAML attributes

Attribute name	Attribute value
https://data.gov.dk/model/core/eid/email	xxxxxxxx@xxxxxx.dk
https://data.gov.dk/concept/core/nsis/loa	Substantial
https://data.gov.dk/model/core/specVersion	OIO-SAML-3.0
dk:gov:saml:attribute:KombitSpecVer	2.0
https://data.gov.dk/model/core/eid/professional/cvr	xxxxxxxx
https://data.gov.dk/model/core/eid/professional/orgName	xxxxxxxxxxx
https://data.gov.dk/model/core/eid/privilegesIntermediate	PD94bWwgdMvYc2lvdj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz48YnBwOlByaXZpbGVnZUxpc3QgeG1sbmM6YnBwPSJodHRwOi8vZGlnYmFtZWVudC9yZy8yMDAxL1hNTFNjaGVrYS1pbmN0YW5jZSI+PFByaXZpbGVnZUdyb3VwiFNjb3BlPSJ1cm46ZGs6Z292OnNhbw6Y3ZyTnVtYmVySWRlbnRpZnRLbWVybmluZGsvcm9ScXNMdXNlcjN5c3RlbXJvbGUvdGVzdHJvbkxMS8xPC9Qcmll2aWxlZ2U+PC9Qcmll2aWxlZ2VHcm91cD48L2JwcDpQcmll2aWxlZ2VMaX

Basic Privilege Profile of the https://data.gov.dk/model/core/eid/privilegesIntermediate

Scope	Privilege	Constraints
urn:dk:gov:saml:cvrNumberIdentifier: xxxxxxxx	http://stoettesystemerne.dk/roles/usersystemrole/testrolle1/1	

Hvis du får et lignende resultat, er IdP korrekt tilsluttet Context Handler 2, og kan både gennemføre login til tjenester samt medsende privilegier.