

**DIGITALISERINGS
KATALOGET**

KOM GODT I GANG

TILSLUT BRUGERVENDT SYSTEM

En trin for trin guide til dig, der skal
tilslutte et brugervendt system for første gang

August 2021

KOMBIT

Kommunernes it-fællesskab

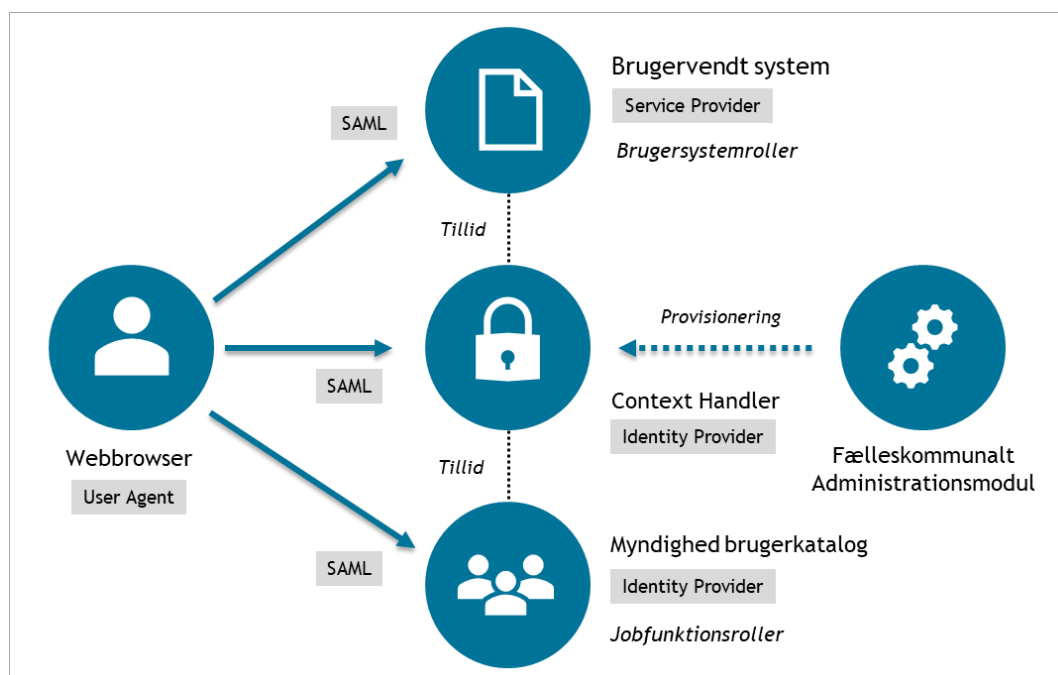
1 Introduktion

Denne guide henvender sig til dig, der skal integrere et fagsystem til *Adgangsstyring for brugere* (ADGBRUGER) for første gang. Guiden er et praktisk eksempel på de opgaver der skal udføres, for at en bruger kan logge ind i et fagsystem med en Brugersystemrolle efter autentificering hos en tilsluttet Identity Provider (IdP).

Det forudsættes, at du inden har læst vejledningen [Adgangsstyring for brugere](#), hvor tekniske detaljer og forudsætninger er beskrevet. Du skal udføre opgaver i:

- Det Brugervendte system
 - Betegnelsen for et fagsystem tilsluttet Adgangsstyring for brugere i den fælleskommunale infrastruktur
 - Betegnet *Service Provider* i SAML-terminologi
- Det fælleskommunale administrationsmodul
- Den tilsluttede Identity Provider (IdP)

Nedenstående tegning illustrerer de centrale komponenter og samspillet mellem disse.



Figur 1. Adgangsstyring for brugere oversigt.

Guiden tager udgangspunkt i .NET eksempelkoden fra Digitaliseringsstyrelsen (OIOSAML) og bruger dens site WebsiteDemo til at illustrere, hvordan man sætter et fagsystem op til at integrere med Adgangsstyring for brugere. WebsiteDemo er således vores fagsystem i denne guide.



Der findes adskillige SAML-rammeværk, og samme opgaver skal udføres, uanset hvilket rammeværk du vælger at anvende til dit fagsystem. Du behøver ikke hente OIOSAML-koden og anvende dennes WebsiteDemo til at gennemføre guiden, du kan også vælge at tilslutte dit eget fagsystem med det samme. Vær blot opmærksom på, at konfiguration af dit fagsystem er specifik for det valgte rammeværk.

2 Baggrundsdokumentation

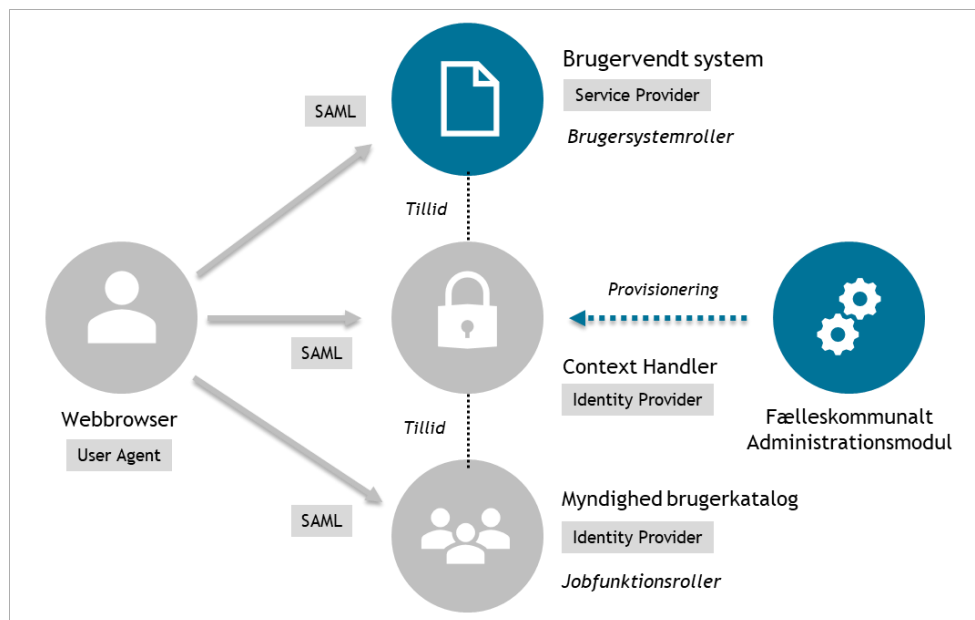
Læs [\[INTRO\]](#) og [\[VEJL\]](#) så du har en grundlæggende forståelse af funktion og roller af de centrale komponenter. Se [\[KGIG-VEJL\]](#) - *certifikater* for hvordan du bestiller et funktionscertifikat. Se [\[ADMININTRO\]](#) for hvordan du bliver oprettet som leverandør, så du kan registrere dit fagsystem som Brugervendt system i den fælleskommunale infrastruktur.

Referencer:

[INTRO]	Adgangsstyring for brugere - Introduktionsside
[VEJL]	Vejledning til Adgangsstyring for brugere
[KGIG-VEJL]	Kom-godt-i-gang vejledninger
[RETL]	Retningslinjer for anvendelse af det eksterne testmiljø
[ADMININTRO]	Fælleskommunalt Administrationsmodul - Introduktionsside
[ADMGUI]	Fælleskommunalt Administrationsmodul - Brugerflade
[OIOSAML.Net]	OIOSAML.Net på Github
[SF1511]	SF1511 Sikkerhed - Hent Token fra Context Handler
[SF1515]	SF1515 Sikkerhed - SAMLSingleLogout
[META]	SAML Metadata dokumentation

3 Tilslut Brugervendt system

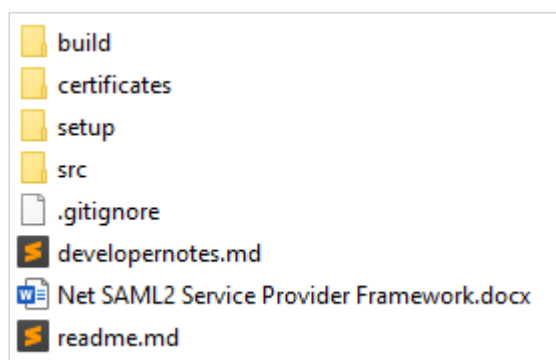
Konfiguration beskrevet i dette kapitel foregår i dit fagsystem og det fælleskommunale administrationsmodul.



Hvis du vælger at gennemføre guiden med dit eget fagsystem i stedet for OIOSAML WebsiteDemo, da bedes du se dokumentationen for dit valgte SAML-rammeverk.


3.1 Hent OIOSAML eksempelkode

Koden hentes fra <https://github.com/digst/OIOSAML.Net> og har følgende struktur:



Følg trin i readme.md for at få koden konfigureret og bygget, således at du har et fungerende brugervendt system "WebsiteDemo".

Vejledningen angiver, at du skal sætte Solution til at starte både IdentityProviderDemo og WebsiteDemo ved opstart. Du kan nøjes med at sætte WebsiteDemo som opstartsprojekt. Ved kørsel får du startsiden, og du er nu klar til konfiguration af din egen Service Provider, samt tilføjelse af Context Handler som trusted IdP:



[Go to My Page.](#)

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:\Users\xmag\source\repos\OIOSAML.Net-master\src\dk.nita.saml20\WebsiteDemo\idp-metadata`".

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

© OIOSAML.NET (www.oiosaml.info).

3.2 Anskaf et funktionscertifikat

Du skal anvende dedikerede funktionscertifikater (FOCES) for hvert af dine IT-systemer tilsluttet den fælleskommunale infrastruktur, også i testmiljøet. Anskaffelse af funktionscertifikat er beskrevet i [[KGIG-VEJL](#)] - *certifikater*.

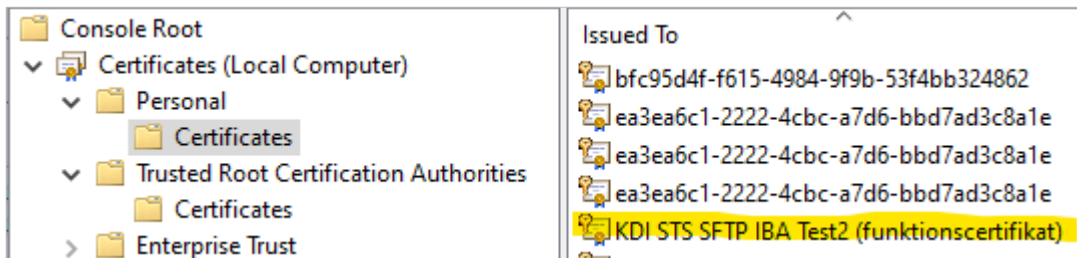
Du skal have et gyldigt funktionscertifikat samt adgangskoden til den private nøgle. Det er vigtigt, at du kender forskellen på den offentlige og private version af certifikatet og ved hvornår du skal anvende dem, hvilket også er beskrevet i certifikat-guiden.

I guiden har vi anvendt vores eget funktionscertifikat "KDI STS SFTP IBA Test2 (funktionscertifikat)".

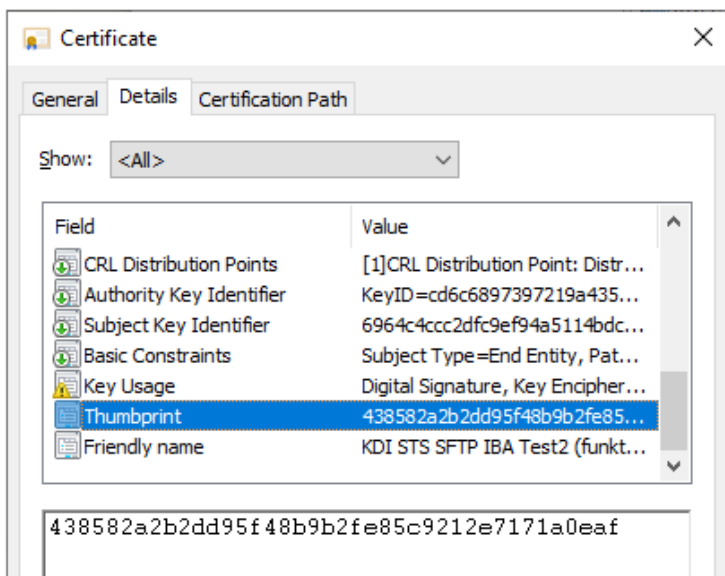
3.3 Konfigurer dit certifikat til anvendelse

Den private version af certifikatet skal konfigureres til anvendelse på den maskine dit fagsystem afvikles på, hvilket afhænger af OS/webserver/programmeringssprog der anvendes. I dette eksempel afvikles *WebsiteDemo* på Windows/.NET og IIS Express, og certifikatet skal derfor importeres i Windows Certificate Store.

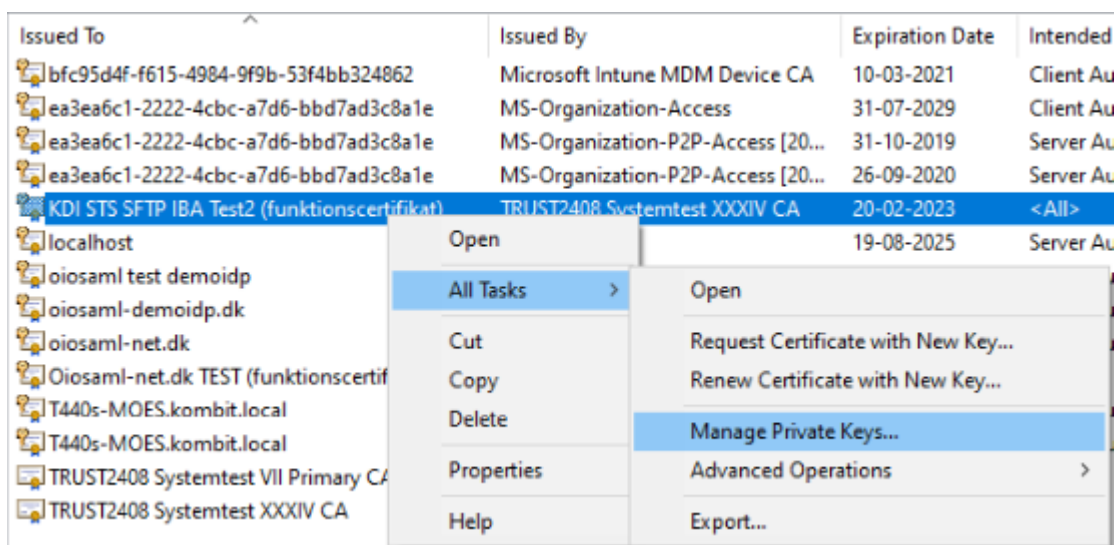
Det er beskrevet i certifikat-guiden hvorledes man importerer certifikater til Windows og Java Certificate Stores. OIOSAML eksempel-koden forventer, at den private version af dit funktionscertifikat er importeret under `\LocalMachine\My`:



Åben certifikatet for at se detaljer, og kopiér dernæst Thumbprint og gem i et arbejdsdokument:

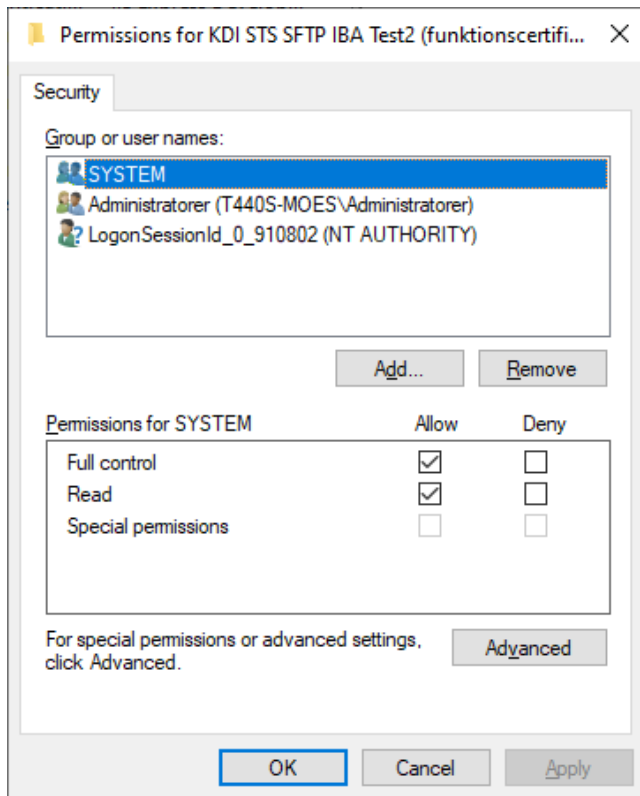


Dernæst skal vi sikre os, at den bruger-context som WebsiteDemo afvikles i har adgang til den private nøgle. Højre-klik på certifikatet og vælg "All tasks -> Manage Private Keys...":





Vi vil afvikle koden i Visual Studio i elevated mode (som administrator) og vi kan dermed se at de fornødne rettigheder er på plads. Hvis koden afvikles som en bruger der ikke har adgang til den private nøgle, da skal bruger tilføjes her:



Opdaterér thumbprint til signing certificate i Web.config, så det passer med dit eget certifikat:

```
<SigningCertificate findValue="438582a2b2dd95f48b9b2fe85c9212e7171a0eaf"  
storeLocation="LocalMachine" storeName="My" x509FindType="FindByThumbprint"/>
```

Følgende trin er kun nødvendigt, hvis du har behov for at generere din SAML metadata manuelt. Hvis fx din metadata fil genereret af rammeværket ikke er kompatibel med Context Handler og fejler ved registreringen i ADM.

Hvis du har behov for at generere din metadata fil manuelt, da skal du gemme den offentlige version af dit certifikat i PEM-format (se certifikat guiden), således at du har det som base64 encoded streng. Fjern start/end tags og line-breaks således at du kun har certifikatet i en enkelt lang streng:

```
MIIGITCCBQmgA ... S1tFsyINOBWQ== (forkortet eksempel)
```



3.4 Fastlæg SAML endpoints og EntityID

De tre centrale parametre i SAML konfigurationen af dit fagsystem (Service Provider) er den unike nøgle der identificerer dit system, samt adressen til endpoints der accepterer Authentication requests/responses. Her er værdierne anvendt i denne demo, hvor de to endpoints allerede er defineret af OIOSAML-koden:

SAML parameter	Værdi
entityID	https://saml.kdi-ctt-demo.dk (se note 1)
AssertionConsumerService	https://oiosaml-net.dk:20002/login.ashx (Se note 2,3)
SingleLogoutService	https://oiosaml-net.dk:20002/logout.ashx (Se note 2,3)

Note 1: Ifølge [META]: *The value of the entityID attribute SHOULD be the canonical URL of the entity's metadata document.* Vores eksempel køres kun lokalt og vores metadata er ikke udstillet, så derfor har vi til denne demonstration valgt et fiktivt domæne, da nøglen blot skal være unik. Men vær opmærksom på denne anbefaling, når dit brugervendte system er udstillet og du skal registrere det rigtige system.

Du skal fastlægge og anvende dit eget unike entityId, anvend ikke værdi fra guiden !!

Note 2: Der kan være en separat *Location* og *ResponseLocation* sti. OIOSAML koden anvender samme endpoint til håndtering af både Authentication Request og Response.

Note 3: *oiosaml-net.dk* er det host-navn som eksempel-koden opretter og anvender, som kun fungerer lokalt på maskine koden afvikles på. Script til konfiguration af OIOSAML koden opretter de lokale DNS entries i *C:\Windows\System32\drivers\etc\hosts*:

```
127.0.0.1 oiosaml-net.dk
127.0.0.1 oiosaml-demoidp.dk
```

3.5 Opdater din Service Provider konfiguration

I web.config under <ServiceProvider>, angiv dit eget unike Service Provider entityId:

```
<ServiceProvider id="https://saml.kdi-ctt-demo.dk" server="https://oiosaml-net.dk:20002">
...
</ServiceProvider>
```

Dernæst tilføj din Service Provider EntityID under *AllowedAudienceUris*:

```
<AllowedAudienceUris>
  <Audience>https://saml.oiosaml-net.dk</Audience>
  <Audience>https://saml.kdi-ctt-demo.dk</Audience>
</AllowedAudienceUris>
```




3.6 Generer din Service Provider SAML metadata

Alle SAML-rammeverk kan generere din metadata fil for dig, efter du har færdiggjort konfigurationen. Se dokumentationen for dit valgte SAML-rammeverk. Hvis du erfarer, at den genererede metadata ikke kan registreres på dit brugervendte system i [ADMGUI], da kan du generere metadata-filen manuelt, som beskrevet her.

Nederst på [Adgangsstyring for brugere - Introduktionsside](#) finder du *Eksempel: metadata for brugervendt system*. Gem denne fil lokalt. Du skal dernæst erstatte følgende attributter med dine egne værdier:

```
<md:EntityDescriptor
  xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
  ID="d3b3f5fa-1865-47ef-b595-166f6f02dlbe"
  entityID="https://bvs.domain.com">
  <md:SPSSODescriptor AuthnRequestsSigned="true" WantAssertionsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
  <md:KeyDescriptor use="signing">
  <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmlsig#">
  <ds:X509Data>
  <ds:X509Certificate>MIIGJjCCBQ6...</ds:X509Certificate>
  </ds:X509Data>
  </ds:KeyInfo>
  </md:KeyDescriptor>
  <md:KeyDescriptor use="encryption">
  <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmlsig#">
  <ds:X509Data>
  <ds:X509Certificate>MIIGJjCCBQ6...</ds:X509Certificate>
  </ds:X509Data>
  </ds:KeyInfo>
  </md:KeyDescriptor>
  <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://bvs.domain.com/saml/SingleLogout"/>
  <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://bvs.domain.com/saml/SingleLogout"/>
  <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName</md:NameIDFormat>
  <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://bvs.domain.com/saml/SSO" index="0" isDefault="true"/>
  </md:SPSSODescriptor>
</md:EntityDescriptor>
```

Generér et vilkårligt UUID til anvendelse i attributten "ID". Du har nu din SAML Service Provider metadata, som du skal bruge ved registrering af dit Brugervendte system i den fælleskommunale infrastruktur.

Hvis EntityDescriptor har en "validUntil" attribut, tjek at den stemmer overens med udløbsdato på certifikatet.

Metadata behøver ikke være signeret, hvilket gør det nemmere, hvis der er behov for at tilpasse filen manuelt.

3.7 Etablér tillid til Context Handler som IdP

Hent filen *Metadata Ekstern Test*, der er link til nederst på [\[INTRO\]](#). Giv metadata-filen et navn uden mellemrum, fx "Context_Handler_ExtTest.xml", og gem den i følgende folder:

```
\src\dk.nita.saml20\WebsiteDemo\idp-metadata\
```

Context Handler vil dernæst automatisk dukke op som Identity Provider, der kan vælges ved login, som illustreret senere i "Test login" afsnittet.

3.8 Registrér dit brugervendte system

Følg vejledningen i [\[ADMININTRO\]](#) for hvorledes du opretter dit IT-system. Til guiden har vi oprettet et IT-system "KDI CTT Brugervendt system TEST" og givet det typen "Brugervendt system":

KDI CTT Brugervendt system TEST

Stamdata	Dataafgrænsningstyper	Anvendersystem	Brugervendt system
UUID:	f051e500-5f56-4e38-9ffe-44f304e4628c		Oprettet:
Leverandør:	KOMBIT A/S		Ændret:
Navn: *	<input type="text" value="KDI CTT Brugervendt system TEST"/>		
E-mail: *	<input type="text" value="xmag@kombat.dk"/> ?		
Beskrivelse:	<input type="text" value="Til test af OIOSAML klient mod context handler"/>		
Type:	<input type="checkbox"/> Anvendersystem <input checked="" type="checkbox"/> Brugervendt system <input type="checkbox"/> Identity Provider <input type="checkbox"/> Serviceudbyder		

Vi har dernæst valgt faneblad "Brugervendt system" og her har vi uploadet vores Service Provider metadata med drag-and-drop, som vi genererede i forrige afsnit (*vær opmærksom på, at du kun kan uploade filen med drag-and-drop*):



KDI CTT Brugervendt system TEST

Stamdata Dataafgrænsningstyper Anvendersystem **Brugervendt system**

EntityId: **https://saml.kdi-ctt-demo.dk**

Krævet assurance level: * Niveau 3 - Høj tillid til påstået identitet ▼

SAML metadatafiler: *

Træk SAML metadata fil herind ?

Certifikat	Udløb ^
KDI STS SFTP IBA Test2 (funktions...	2023-02-20

Vigtigt: EntityId læses fra SAML-metadatafilen og tilknyttes det brugervendte system ved oprettelse i ADM. Du kan efterfølgende IKKE ændre EntityId. Hvis denne parameter ved fejl er forkert, da er man nød til at slette pågældende IT-System og oprette et nyt som brugervendt system med korrekte metadata-fil.

Vigtigt: Du skal angive og benytte HTTPS på alle dine endpoints. Ellers accepteres metadata ikke.



3.9 Opret Brugersystemrolle

På fanebladet "Brugervendt system" for dit IT-system opretter du Brugersystemroller (BSR). Som eksempel har vi oprettet en enkelt "Sagsbehandler" BSR:

Opret brugersystemrolle

UUID: 472567e7-86af-474b-e916-e12c7b86898e

Navn: *

Beskrivelse:

EntityId ⓘ

Domæne: *

Rollenavn: *

Version: *

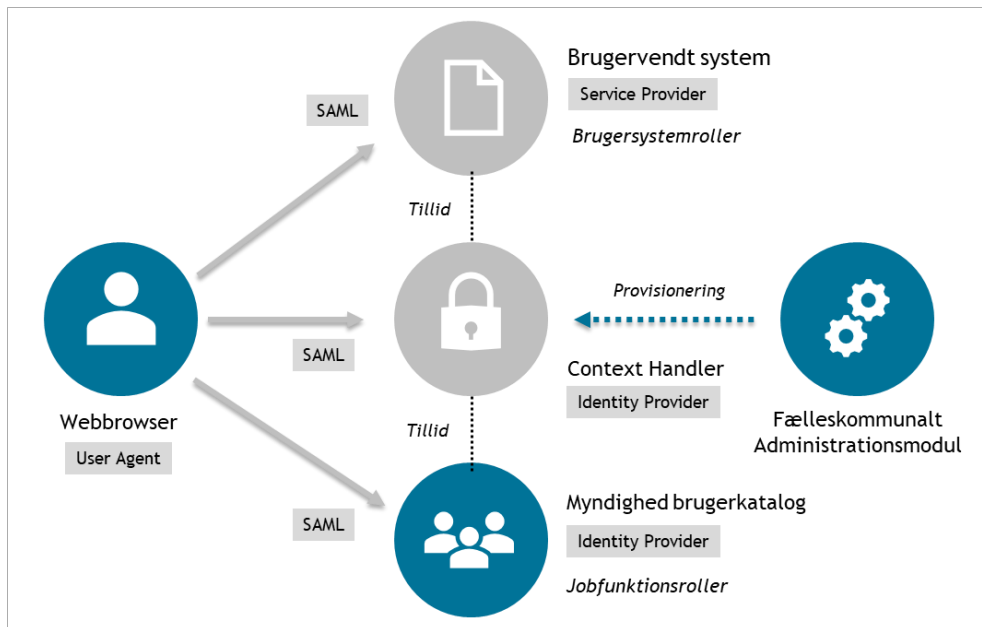
<http://kdi-ctt-demo.dk/roles/usersystemrole/sagsbehandler/1>

Og denne fremgår da af oversigten:

Brugersystemroller		
UUID	Navn ^	Dataafgrænsningstyper
<input type="text"/>	<input type="text"/>	<input type="text"/>
10661f...	Sagsbehandler	

4 Anvend brugervendt system

Konfiguration beskrevet i dette kapitel foregår i det fælleskommunale administrationsmodul og den valgte Identity Provider. Test udføres fra en browser.



4.1 Tilknyt brugersystemrolle til jobfunktionsrolle

Denne opgave skal udføres af en Rolleadministrator i den fælleskommunale infrastruktur, der er tilknyttet samme myndighed som testbrugeren. Se *Nemlog-in rettigheder* under *Forudsætninger* i [VEJL]. Hvis testbruger er tilknyttet Myndighed A, da skal en Rolleadministrator fra Myndighed A udføre opgaven.

I guiden har vi anvendt en testbruger i vores test-IdP som er tilknyttet myndighed ”Korsbaek Kommune”. Vi er logget ind i ADM som Rolleadministrator for Korsbaek Kommune. Vi har genanvendt en eksisterende Jobfunktionsrolle:

<http://korsbaek.dk/roles/jobrole/kombitrolle1/1>

Dette er eksklusivt for guiden! Du skal selv aftale med ansvarlige for den test-IdP du anvender, hvilken Jobfunktionsrolle de har registreret, som du kan anvende til testen. Samt hvilken myndighed din testbruger er tilknyttet.

Vi skal da tilknytte vores brugersystemrolle til jobfunktionsrollen for myndigheden. Vælg ”Jobfunktionsroller” i venstre menu og dernæst jobfunktionsrollen:



Jobfunktionsroller		
Navn ^	System	Beskrivelse
kombi		
kombitrolle1		Benyttes til general test

Herfra vælges "Rediger":

kombitrolle1

Navn: kombitrolle1

EntityId: http://korsbaek.dk/roles/jobrole/kombitrolle1/1

Beskrivelse: Benyttes til general test

Delegeret til:

Brugersystemroller

System ^	Rolle
----------	-------

[Rediger](#) [Tilbage](#) [Kopier](#)

Og brugersystemrollen kan tilknyttes jobfunktionsrollen:

[+ Tilknyt brugersystemrolle](#)



Tilknyt brugersystemrolle

System	Rolle	Dataafgrænsning
Navn:	kombitrolle1	
EntityId:	http://korsbaek.dk/roles/jobrole/kom bitrolle1/1	
System		
KDI CTT Brugervendt system TEST		Vælg et brugervendt system fra listen, eller fremsøg det ved at begynde at skrive i feltet Navn.
Navn ^		
kdi ctt		
KDI CTT Brugervendt system TEST		
KDI CTT Test System #2		

Annuller **Næste**

Det brugervendte system (dit eget) vælges, hvor brugersystemrollen er defineret. Klik derefter "Næste".



Tilknyt brugersystemrolle

System	Rolle	Dataafgrænsning
Navn:	kombitrolle1	
Entityid:	http://korsbaek.dk/roles/jobrole/kombitr olle1/1	
System:	KDI CTT Brugervendt system TEST	
Rolle	Sagsbehandler	Vælg en rolle fra listen, eller fremsøg det ved at begynde at skrive i feltet Navn.
Navn ^	<input type="text"/>	
	Sagsbehandler 	

Forrige **Annuler** **Næste**

Når man har valgt System, vises automatisk tilgængelige brugersystemroller. Her vælger vi "sagsbehandler", som vi har oprettet til testen. Vælg dernæst "Tilknyt":

Tilknyt

Bemærk, at der kan gå et par minutter før dette er provisioneret til Context Handler!

Vi har nu fået oprettet en mapping mellem jobfunktionsrollen "kombitrolle1" til brugersystemrollen "sagsbehandler" i vores eget brugervendte system, for brugere tilknyttet myndighed "Korsbaek Kommune":

Jobfunktionsroller

Navn ^	System	Beskrivelse
kombi	<input type="text"/>	<input type="text"/>
kombitrolle1	KDI CTT Brugervendt system TE...	Benyttes til general test


4.2 Opret testbruger i Identity Provider

Oprettelse af testbruger og tillknytning af jobfunktionsrolle er helt individuelt for hver lokale Identity Provider. Der findes adskillige produkter, og man har valgt forskellige måder at tildele jobfunktionsroller til brugere på. Der er derfor ikke vejledning i guiden for hvordan dette gøres; det må du aftale med de ansvarlige for den IdP du har fået lov til at bruge til testen.

Til vores test har vi en bruger som er tilknyttet myndighed "Korsbaek kommune" og denne har fået tildelt jobfunktionsrollen "http://korsbaek.dk/roles/jobrole/kombitrolle1/1".

4.3 Test login

Vi er nu klar til at teste. Start projektet:



OIOSAML.NET

[Go to My Page.](#)

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:\Users\xmag\source\repos\OIOSAML.Net-master\src\dk.nita.saml20\WebsiteDemo\idp-metadata".

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

© OIOSAML.NET (www.oiosaml.info).

Vælg "Go to My Page". Da du ingen session har, da bedes du vælge IdP du ønsker at autentificere dig mod (læg mærke til at Context Handler er dukket op som IdP der kan vælges):

Choose Identity Provider

Please choose the identity provider of your choice from the list below:

<https://saml.test-nemlog-in.dk/>
<https://oiosaml-demoidp.dk:20001/>
<https://saml.adgangsstyring.eksterntest-stoettesystemerne.dk>



Det er specifikt for OIOSAML-koden, at vi her kan vælge IdP vi ønsker at autentificere mod. I praksis vil dit fagsystem kun være integreret med Context Handler som IdP, og bruger vil automatisk blive videresendt til denne med det samme.

Vælg det sidste punkt (Context Handler = <https://saml.adgangsstyring...dk>). Du sendes da til startside hos Context Handler, hvor du skal vælge hvilken lokale IdP du ønsker at autentificere dig mod. Til denne test har vi valgt "KOMBIT Test Kommune" (som faktisk er "KOMBIT Test IdP"), da det er her vores testbruger er oprettet. Du skal selvfølgelig vælge den IdP som din testbruger er oprettet i:

Login Page

Please select an authentication method

KOMBIT Test Kommune

Remember this authentication connection

OK

Dernæst vises login-side hos den IdP du har valgt, hvor din testbruger er oprettet:

Please enter your login information

Please notice that both Name and password are case sensitive.

<brugernavn>

.....

OK

[Forgot password? Click here!](#)

Dette er skærmbillede fra vores test-IdP, det vil se anderledes ud for den IdP du anvender til testen. Indtast brugernavn og adgangskode for din testbruger.

Du sendes derefter tilbage til Context Handler (usynligt for bruger), som oversætter din jobfunktionsrolle til brugersystemrolle, og som dernæst sender dig tilbage til dit fagsystem (i dette eksempel WebsiteDemo):



Welcome, C=DK,O=11111111,CN=[REDACTED],Serial=fd2ed2a9-09fc-4b4f-98a6-6d7bf206d088

Attribute name	Attribute value
dk:gov:saml:attribute:CvrNumberIdentifier	11111111
dk:gov:saml:attribute:KombitSpecVer	1.0
dk:gov:saml:attribute:SpecVer	DK-SAML-2.0
dk:gov:saml:attribute:AssuranceLevel	3
dk:gov:saml:attribute:Privileges_intermediate	<pre><?xml version="1.0" encoding="UTF-8"?><bpp:PrivilegeList xmlns:bpp="http://itst.dk/oiosaml/basic_privilege_profile" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"> <PrivilegeGroup Scope="urn:dk:gov:saml:cvrNumberIdentifier:11111111"> <Privilege>http://kdi-ctt- demo.dk/roles/usersystemrole/sagsbehandler/1<Privilege> </PrivilegeGroup></bpp:PrivilegeList></pre>

Logoff

Relogin with IdP:

Du har nu integreret dit fagsystem med Context Handler og har gennemført et login, hvor din testbruger kommer tilbage med en tildelt brugersystemrolle

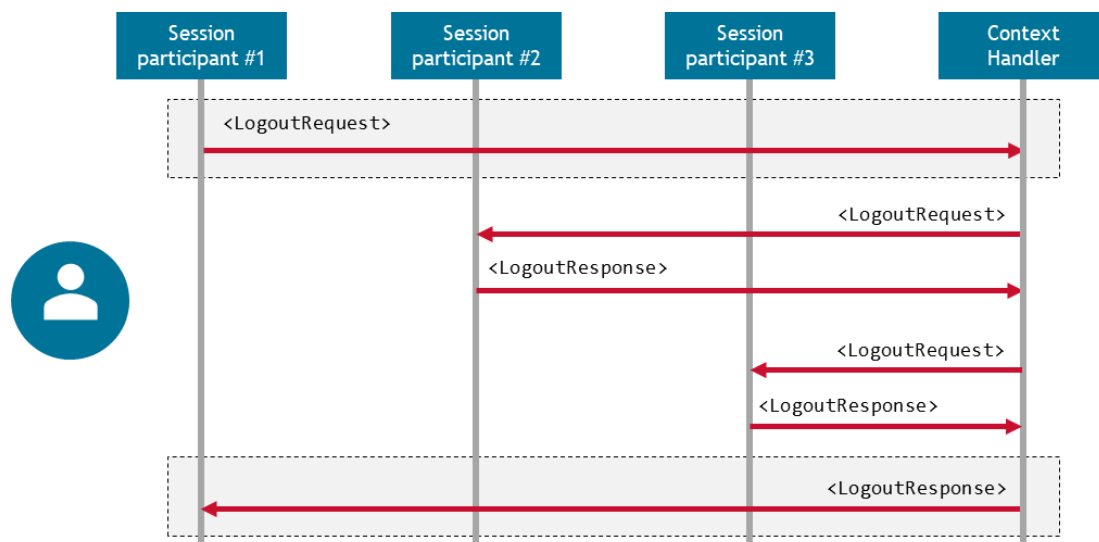
Læg mærke til en lille tilføjelse til OIOSAML-koden. På brugersiden har vi valgt at udpakke og vise *Privileges_Intermediate* hvori brugersystemroller er gemt. Se i appendiks hvordan dette er gjort.

5 Implementer SingleLogout

5.1 Implementer SingleLogoutService ResponseLocation

Dette endpoint anvendes, når Logout-sekvens initieres fra dit system:

- Bruger vælger "Log ud" i dit system og du fjerner brugers lokale session.
- Du sender bruger til CH med et SAMLRequest indeholdende et LogoutRequest.
- CH sender bruger videre til de andre systemer, hvor bruger også har en aktiv SAML-session udstedt af CH, med et LogoutRequest. Hvert system fjerner brugers lokale session, og sender bruger tilbage til CH. (*)
- Bruger ender ved dit system med et LogoutResponse, og du kan her afslutte sekvensen, ved fx at vise en "Du er nu logget ud" side.



Figur 2 - Logout-sekvens initieret fra dit system

(*) Dette gælder også Identity Provider, hvor bruger blev autentificeret. Den vil også modtage et LogoutRequest, og svare med et LogoutResponse.

Du angiver i din metadata med *ResponseLocation*, hvor CH skal sende bruger tilbage med LogoutResponse:

Service Provider SAML metadata

```

<SingleLogoutService
  Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
  Location="https://mit-fagsystem.dk/saml/logout.php"
  ResponseLocation="https://mit-fagsystem.dk/saml/logged-out.php"/>
    
```

Du skal således implementere:

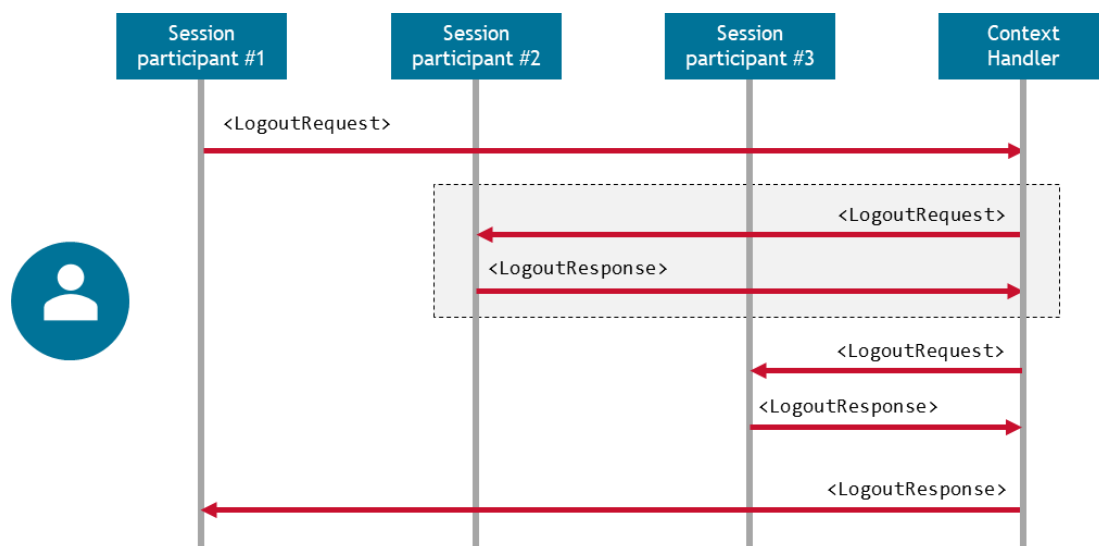
1. At brugers lokale session fjernes ved logout.
2. At bruger sendes til CH med et LogoutRequest.
3. At sekvensen afsluttes på fornuftig vis; fx med en "Du er nu logget ud" side.

Se dokumentationen for dit valgte SAML-rammeverk, for hvorledes du implementerer dette.

5.2 Implementer SingleLogoutService Location

Dette endpoint anvendes, når Logout-sekvens initieres fra et andet system:

- Bruger sendes til dit system med et SAMLRequest indeholdende et LogoutRequest.
- Du fjerner brugers lokale session, og sender bruger tilbage til CH med et LogoutResponse.



Figur 3 - Logout-sekvens initieret fra et andet system

Du angiver i din metadata med *Location*, hvor CH skal sende bruger til med LogoutRequest:

Service Provider SAML metadata

```

<SingleLogoutService
  Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
  Location="https://mit-fagsystem.dk/saml/logout.php"
  ResponseLocation="https://mit-fagsystem.dk/saml/logged-out.php"/>
  
```

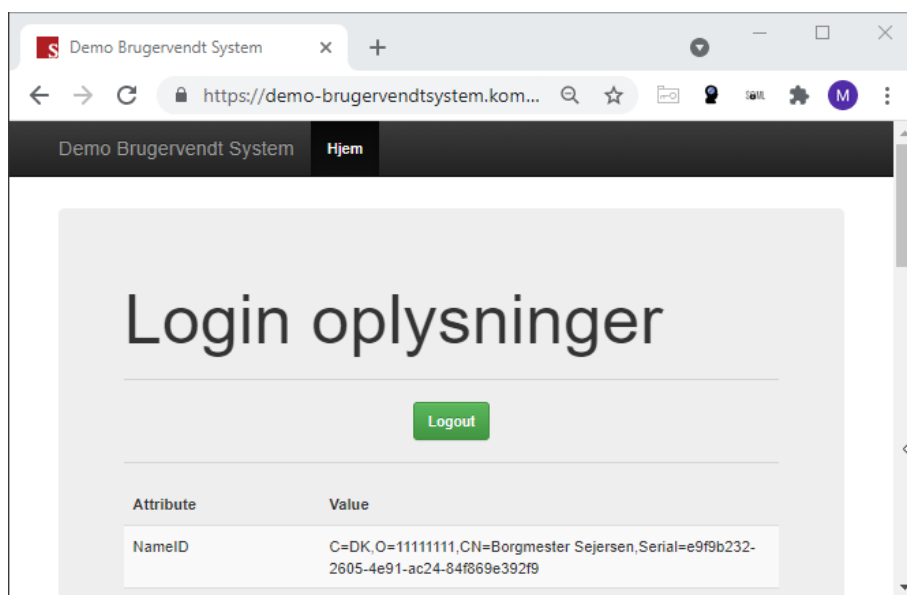
Du skal således implementere:

1. At brugers lokale session fjernes, ved modtagelse af et LogoutRequest.
2. At bruger sendes tilbage CH med et LogoutResponse.

Se dokumentationen for dit valgte SAML-rammeverk, for hvorledes du implementerer dette.

5.3 Eksempel

Her et praktisk eksempel. Vi er logget ind i KOMBIT [Demo Brugervendt System](#):



Bemærk, at alle brugere fra samtlige Identity Providers med føderationsaftale til CH i ExtTest-miljøet kan logge på Demo Brugervendt System. Så den er god at teste integrationen med.

Vi klikker "Logout" som peger på:

<https://demo-brugervendtsystem.kombit.dk/test/saml/logout>

Demo-systemet fjerner vores lokale session og sender os til CH med redirect:

<https://adgangsstyring.eksternetest-stoettesystemerne.dk/runtime/saml2/issue.idp?SAMLRequest=nVJNb9wgFLz...>



SAMLRequest indeholder LogoutRequest:

```
<saml2p:LogoutRequest
  Destination="https://adgangsstyring.eksterntest-
stoettesystemerne.dk/runtime/saml2/issue.idp"
  ID="a594a3ef361608404089f82929d9e24" IssueInstant="2021-08-17T09:38:06.752Z"
  Version="2.0"
  xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol">
  <saml2:Issuer
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">https://saml.demo-
brugervendtsystem.kombit.dk/test</saml2:Issuer>
  <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName"
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">C=DK,O=11111111,CN=Borgmester
Sejersen,Serial=e9f9b232-2605-4e91-ac24-84f869e392f9</saml2:NameID>
  <saml2p:SessionIndex>1516271577</saml2p:SessionIndex>
</saml2p:LogoutRequest>
```

CH sender os videre til IdP vi blev autentificeret mod, hvor vi også har en session:

<https://test-idp.kombit.dk/adfs/ls/?SAMLRequest=jZJRi50w...>

SAMLRequest indeholder LogoutRequest:

```
<LogoutRequest Destination="https://test-idp.kombit.dk/adfs/ls/"
  ID="id1d35b112f533446b9be1b61fa328c171" IssueInstant="2021-08-
17T09:38:06.7891806Z" Version="2.0"
  xmlns="urn:oasis:names:tc:SAML:2.0:protocol">
  <Issuer
xmlns="urn:oasis:names:tc:SAML:2.0:assertion">https://saml.adgangsstyring.eksterntest
-stoettesystemerne.dk</Issuer>
  <NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName"
  xmlns="urn:oasis:names:tc:SAML:2.0:assertion">C=DK,O=11111111,CN=Borgmester
Sejersen,Serial=e9f9b232-2605-4e91-ac24-84f869e392f9</NameID>
  <SessionIndex>_4382e44b-eef8-43f1-a5a4-254a84b6c4f8</SessionIndex>
</LogoutRequest>
```

Vi er nu logget ud af IdP. Denne sender os tilbage til CH:

<https://adgangsstyring.eksterntest-stoettesystemerne.dk:443/runtime/saml2auth/signoffresponse.idp?SAMLResponse=fZJNj5swEI...>

SAMLResponse indeholder LogoutResponse:

```
<samlp:LogoutResponse ID="_031294f0-a1a1-4af0-b9c8-79b9757eb9ca" Version="2.0"
  IssueInstant="2021-08-17T09:38:06.012Z"
  Destination="https://adgangsstyring.eksterntest-
stoettesystemerne.dk/runtime/saml2auth/signoffresponse.idp"
  Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified"
  InResponseTo="id1d35b112f533446b9be1b61fa328c171"
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
  <Issuer xmlns="urn:oasis:names:tc:SAML:2.0:assertion">http://test-
idp.kombit.dk/adfs/services/trust</Issuer>
  <samlp:Status>
  <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
  </samlp:Status>
</samlp:LogoutResponse>
```



Og til sidst sendes vi tilbage fra CH til Demo Brugervendt System:

<https://demo-brugervendtsystem.kombit.dk/test/saml/SingleLogout?SAMLResponse=jZI%2fb8M>

SAMLResponse indeholder LogoutResponse:

```
<LogoutResponse ID="id8381810327cf467c9d9fb2f300ecded0" Version="2.0"
IssueInstant="2021-08-17T09:38:06.898575Z" Destination="https://demo-
brugervendtsystem.kombit.dk/test/saml/SingleLogout"
Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified"
InResponseTo="a594a3ef361608404089f82929d9e24"
xmlns="urn:oasis:names:tc:SAML:2.0:protocol">
  <Issuer
xmlns="urn:oasis:names:tc:SAML:2.0:assertion">https://saml.adgangsstyring.eksterntest
-stoettesystemerne.dk</Issuer>
  <Status>
    <StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
  </Status>
</LogoutResponse>
```

SingleLogout-sekvensen er hermed afsluttet. Vi er logget ud af IdP og fagsystem vi kom fra, og vores SAML-session er afsluttet på Context Handler.

5.4 Test Logout-sekvenser

Nu du har implementeret fælleskommunal adgangsstyring for brugere, da skal du også teste begge SingleLogout-scenarier:

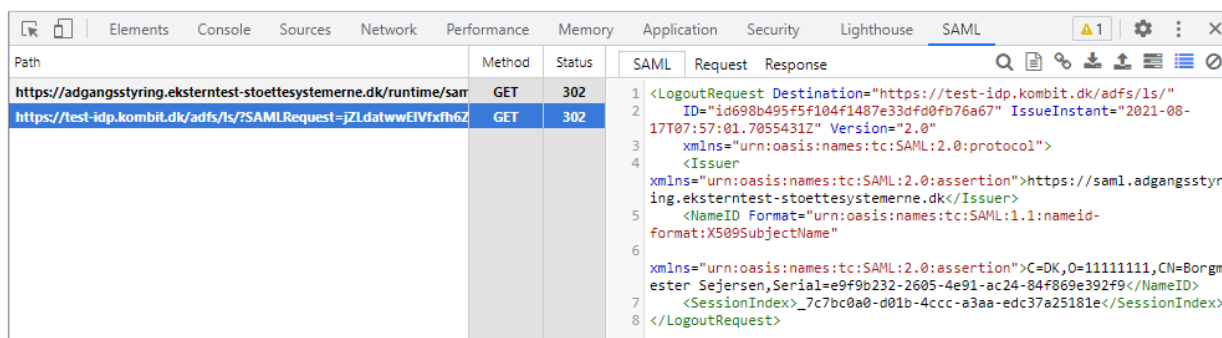
1. Når logout-forespørgsel kommer fra dit system
2. Når logout-forespørgsel kommer fra et andet system

Du kan med fordel benytte [Demo Brugervendt System](#) (DBS) til dette. Log ind i din egen applikation og tilgå dernæst DBS, hvor bruger automatisk vil blive logget ind af CH. Vælg dernæst "Logout" i DBS, og tjek, at brugers session i dit fagsystem efterfølgende også er fjernet.

6 Fejlsøgning

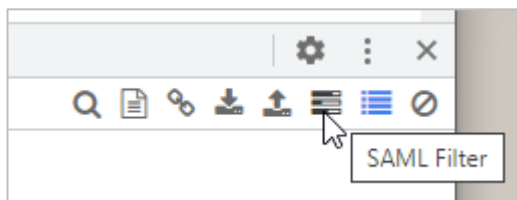
6.1 Inspektion af SAML kommunikationen

Hvis noget ikke fungerer, eller hvis man er nysgerrig, da kan man inspicere de beskeder der sendes frem og tilbage mellem bruger og henholdsvis Fagsystem, Context Handler og myndighedens Identity Provider. Der findes udvidelser til browsers der kan vise SAML-kommunikationen, såsom *SAML Chrome Panel* til Chrome og *SAML-tracer* til Firefox.



Figur 4. SAML Chrome Panel

Fjern hak ved "SAML Filter", da vi har erfaret, at den ved fejl også bort-filtrerer visse SAML-forespørgsler:



Dernæst kan anbefales <https://www.samltool.com/> som har adskillige værktøjer relateret til SAML-protokollen.

6.2 Authentication Request

Hvis din forespørgsel til Context Handler fejler, da skal du inspicere dit SAMLRequest og tjekke at de rigtige værdier sættes af dit rammeværk. I tilfælde af fejlkonfiguration vil du typisk se følgende svar i SAMLResponse:

```
<StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Responder" />
```



Tjek at dit rammeværk benytter SHA256 til signering af SAMLRequest:

```
GET https://adgangsstyring.eksternstest-stoettesystemerne.dk/runtime/saml2/issue.idp?
SAMLRequest=pVPBTsMwD...
&SigAlg=http%3A%2F%2Fwww.w3.org%2F2001%2F04%2Fxmldsig-more%23rsa-sha256
&Signature=hGh%2BX%2F... HTTP/1.1
```

Tjek også, at rammeværket sætter *AudienceRestriction*, som er påkrævet af Context Handler. Tilføj et *Audience* element med EntityID for din Service Provider (dit fagsystem).

Her et eksempel fra et fungerende Authentication Request:

```
<saml2p:AuthnRequest
  xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
  AssertionConsumerServiceURL="https://organisation.eksternstest-stoettesystemerne.dk/sts-rest-ork
  Destination="https://adgangsstyring.eksternstest-stoettesystemerne.dk/runtime/saml2/issue.idp"
  ForceAuthn="false"
  ID="kosdy-a7ea76dc-13a6-429b-bf58-a5a8c425d532"
  IsPassive="false"
  IssueInstant="2020-01-30T12:33:53.797Z"
  ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
  Version="2.0">
  <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">https://organisation.ekstern
  <saml2:Conditions xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
    <saml2:AudienceRestriction>
      <saml2:Audience>https://organisation.eksternstest-stoettesystemerne.dk</saml2:Audience>
    </saml2:AudienceRestriction>
  </saml2:Conditions>
</saml2p:AuthnRequest>
```

Dernæst, tjek også, om dit certifikat er udløbet. Hvis det er udløbet og du opdaterer din konfiguration med et nyt certifikat, glem ikke at opdatere SAML-metadata i ADM.

De tre nævnte emner (signatur-algoritme, AudienceRestriction, udløbet certifikat) er de hyppigste årsager til, at login-request ikke accepteres af Context Handler.

6.3 Service Provider SAML metadata

Hvis dit Authentication Request fejler, dobbelt-tjek indholdet i din metadata fil som du har registreret på dit brugervendte system, at værdierne er korrekte. Og prøv at uploade igen i den fælleskommunale administration på dit brugervendte system og gem ændringer. Så du er helt sikker på, at den korrekte metadata er registreret.

Det sker ofte, at man glemmer at opdatere SAML metadata på det brugervendte system i ADM, efter at man har lavet ændringer i den lokale konfiguration.



6.4 Vis Privileges_Intermediate

For at vise brugersystemroller returneret i brugers SAML-token, som illustreret på sidste skærbillede i afsnit "Test login", har vi ændret følgende i OIOSAML-koden MyPage.aspx:

```
<td>
  <% = att.AttributeValue.Length > 0 ? att.AttributeValue[0] : string.Empty %>
</td>
```

til:

```
<td>
  <%
    if (att.Name == "dk:gov:saml:attribute:Privileges_intermediate")
    {
      byte[] decodedBytes = Convert.FromBase64String(att.AttributeValue[0]);
      string decodedText = Encoding.UTF8.GetString(decodedBytes);
      Response.Write(System.Web.HttpUtility.HtmlEncode(decodedText));
    }
    else
    {
      Response.Write(att.AttributeValue.Length > 0 ? att.AttributeValue[0] :
string.Empty);
    }
  %>
</td>
```