DIGITALISERINGS KATALOGET

VEJLEDNING TIL ADGANGSSTYRING FOR BRUGERE

Sådan implementerer du single-sign-on

KOMB:T

Kommunernes it-fællesskab

Versionshistorik

Version	Dato	Ændringer
1.0	2018-09-21	Publiceret
1.1	2018-10-29	Opdateret med præcisering af at User agent også kan anvendes til kommunkation -se (fodnote); Indsat sidetal. Opdatering af bilagsliste med nye links til [METADATA] Publiceret
1.1	2019-04-25	Afsnit 4. 1 er opdateret med en vejledning til, hvordan en leverandør kan: • opsætte egen IdP • anmode om og godkende en føderationsaftale teste IdP med jobfunktionsroller uden involvering af en kommune
2.0	2020-11-02	Helt ny version med opdateret indhold og layout samt ny struktur

Indholdsfortegnelse

1 Indledning

Adgangsstyring for brugere gør det muligt for myndigheden at konsolidere deres adgangsstyring i én løsning, som de selv har kontrol over. For leverandører af brugervendte systemer betyder det, at der ikke skal laves brugerstyring, men blot håndhæves definerede brugersystemroller i selve fagløsningen. Med Adgangsstyring for brugere er det muligt for myndighederne at implementere Single Sign On til alle deres løsninger.

Denne vejledning giver et overblik over de aktiviteter, der skal til for, at du som leverandør kan implementere Adgangsstyring for brugere succesfuldt. Overblikket kan du bruge til at opnå en bedre planlægning og forståelse af opgavens omfang og de nødvendige trin i implementeringen – både for dig som it-leverandør, men også set fra myndighedens vinkel, som bruger af dit it-system. Der henvises til andre vejledninger for den praktiske udførsel af opgaverne; se kapitel 6 - Bilagsliste for alle referencer.

Med denne vejledning gennemgår vi hvilke opgaver du som leverandør skal igennem for at tilslutte dit brugervendte system. Med Kom-godt-i-gang vejledninger *Certifikater* samt *Tilslut brugervendt system* eksemplificerer vi hvordan du løser opgaverne. Du skal læse følgende afsnit i [VILKÅR] og [SIKKERHEDSMODEL], før du går i gang med den tekniske implementering.

[VILKÅR]
Afsnit 1 og 5 samt appendiks

[SIKKERHEDSMODEL]
Afsnit 4 og 6.3.1

[KGIG-VEJL]
Certifikater samt *Tilslut brugervendt system*

Vejledningen introducerer blot de grundlæggende elementer i SAML, der er essentielle for implementeringen. Det forudsættes, at læseren allerede har kendskab til SAML rammeværk eller sætter sig ind i det, førend implementering af Adgangsstyring for brugere påbegyndes.

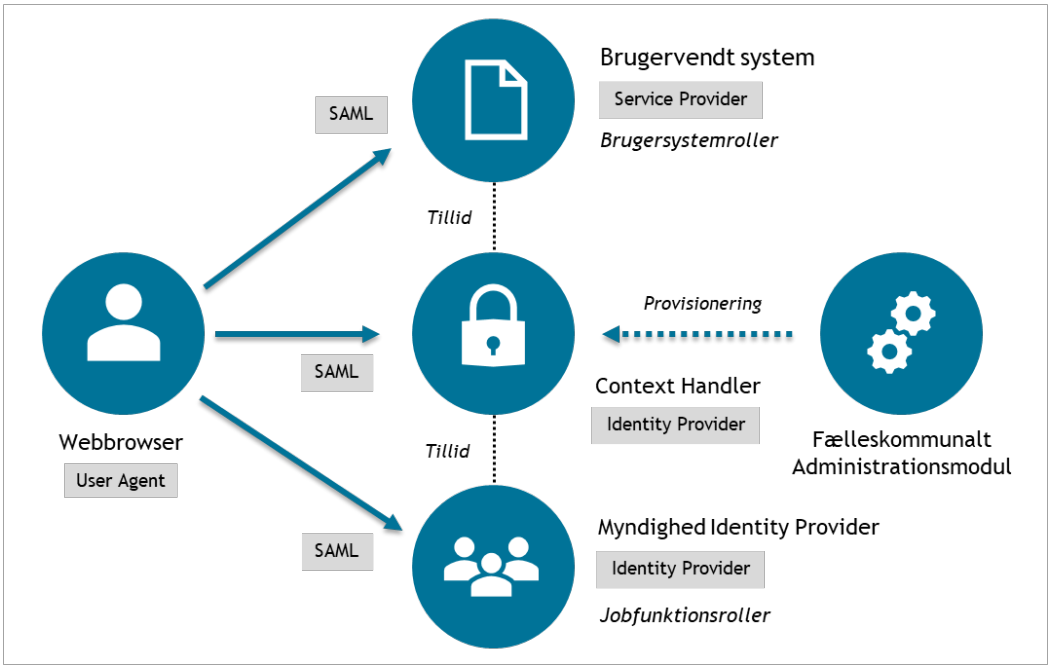
2 Sådan fungerer adgangsstyring for brugere

2.1 Oversigt

Komponenter og samspil

Adgangsstyring for brugere er en sikkerhedsmodel rettet mod it-systemer med en brugergrænseflade, kaldet *Brugervendte systemer* i den fælleskommunale infrastruktur. Sikkerhedsmodellen understøttes af støttesystemerne Context Handler og Fælleskommunalt Administrationsmodul (ADM). Integration til Adgangsstyring for brugere foregår først ved implementering af et SAML rammeværk, som er den standard sikkerhedsmodellen er baseret på, og dernæst etablering af tillid (trust) mellem parterne.

Komponenterne er illustreret på følgende tegning:



Figur 1. Adgangsstyring for brugere - komponenter og SAML betegnelser

Bemærk, at illustrationen blot viser en enkelt myndigheds Identity Provider (IdP), med henblik på at vise samspil mellem komponenterne. I praksis har hver myndighed deres egen IdP.

Brugervendt system

Betegnelsen for et fagsystem der er tilsluttet Adgangsstyring for brugere i den fælleskommunale infrastruktur. I SAML anvendes betegnelsen *Service Provider*. Fagsystemet tilsluttes ved at installere og konfigurere et SAML rammeværk, hvorefter fagsystemet registreres som IT-system af typen ”Brugervendt system” i det fælleskommunale administrationsmodul.

Myndighed Identity Provider

Komponent ansvarlig for autentificering af brugere fra en myndighed, hvilket typisk er implementeret som en SAML-overbygning til myndighedens eksisterende brugerkatalog. Administration af brugeres adgange til fagsystemer foretages ved tilknytning af jobfunktionsroller til brugerne. Myndigheden specificerer efterfølgende i Fælleskommunalt Administrationsmodul hvilke brugersystemroller, som er adgangsgivende, en specifik jobfunktionsrolle skal have.

Føderationsaftale

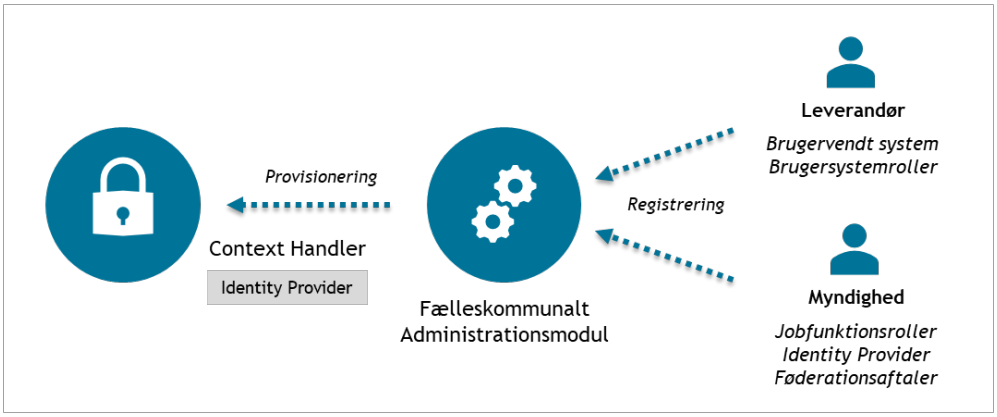
Når en IdP skal have tilladelse til at autentificere brugere fra en specifik myndighed, da skal der anmodes om en føderationsaftale mellem IdP og myndigheden. Myndigheden skal derefter godkende føderationsaftalen. En IdP kan således kun autentificere brugere for myndigheder hvortil der foreligger en godkendt føderationsaftale.

Webbrowser

Komponent som en bruger typisk anvender til at tilgå fagsystemet - i SAML betegnet en *User Agent*. Kan også være en mobil enhed, eller hvilken som helst anden type klient der understøtter SAML.

Fælleskommunalt administrationsmodul

Brugervendte systemer, brugersystemroller, Jobfunktionsroller, Identity Providers og Føderationsaftaler registreres alle i det fælleskommunale administrationsmodul (ADM). Hvorefter de provisioneres til Context Handler, som illustreret på følgende figur:



Figur 2. Registrering og provisionering

Provisioneringen foregår umiddelbart efter registrering og træder i kraft med det samme. Hvis du foretager ændringer i din SAML-konfiguration der afstedkommer ændringer i SAML metadata, da skal du opdatere SAML-metadata på dit registrerede Brugervendte system eller Identity Provider i ADM.

Context handler

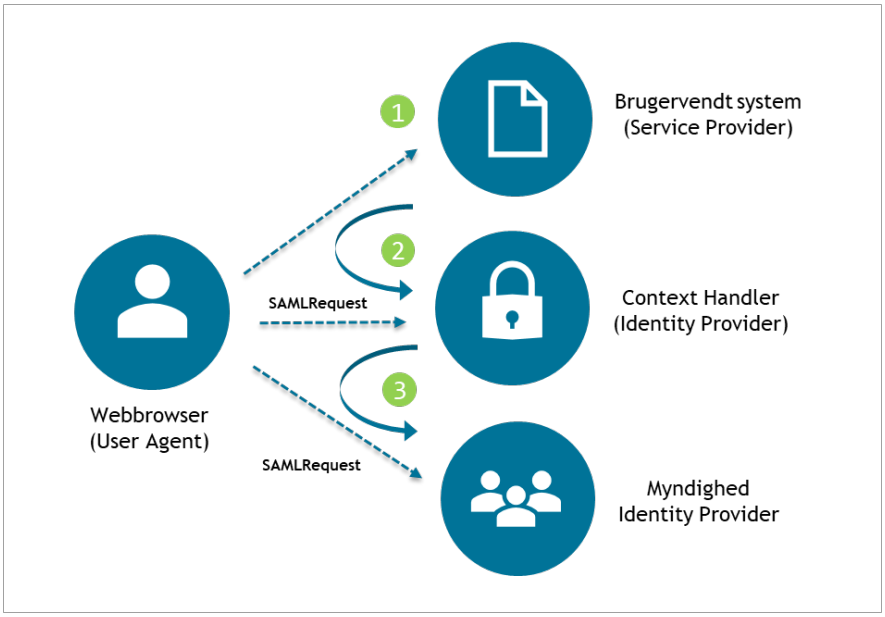
Context Handleren agerer proxy for kommunernes Identity Providers og oversætter en brugers jobfunktionsroller på arbejdspladsen til brugersystemroller i fagsystemet. En myndigheds Identity Provider kender kun jobfunktionsroller (JFR), og et brugervendt system kender kun brugersystemroller (BSR). Det defineres i ADM hvorledes JFR skal oversættes til BSR når en bruger autentificeres og sendes tilbage til fagsystemet. Se beskrivelsen af brugerroller i det efterfølgende afsnit.

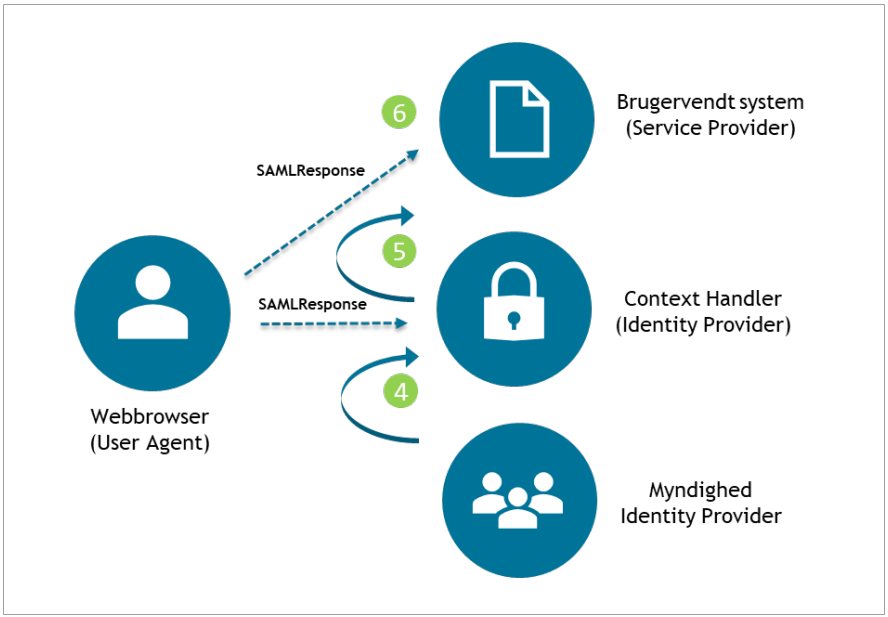
SAML tillid (Trust)

Tilliden etableres ved at det Brugervendte system eller Identity Provider registreres i ADM med deres SAML-metadata, hvor systemets certifikat er indlejret. Efter registrering provisioneres informationen til Context Handler, som er den centrale komponent i føderationen. Ligeledes skal det brugervendte system og Identity Provider etablere tillid til Context Handler ved at registrere dennes SAML-metadata.

Login-sekvens

SAML-sessionen foregår alene ved client-redirects og der er ingen fysisk forbindelse mellem fagsystem, Context Handler og den kommunale IdP. Login-sekvensen foregår i korte træk på følgende vis:





1. Bruger tilgår fagsystemet og har ingen session. Fagsystem laver redirect af bruger til Context Handler (CH).

2. Bruger tilgår CH med et SAMLRequest genereret af fagsystemet. Bruger bliver bedt om at vælge IdP vedkommende er tilknyttet. CH sender bruger videre til valgte IdP.

3. Bruger tilgår myndighedens IdP med SAMLRequest genereret af CH. Bruger autentificeres i den kommunale IdP og brugers jobfunktionsroller aflæses.

4. Myndighedens IdP sender bruger tilbage til CH.

5. Bruger tilgår CH med et SAMLResponse genereret af kommunale IdP. Jobfunktionsroller oversættes til brugersystemroller og CH sender bruger videre til fagsystem.

6. Bruger tilgår fagsystem med et SAMLResponse genereret af CH. Brugersystemroller aflæses og bruger gives session og rettigheder i fagsystemet i henhold til disse.

Brugerroller er indlejret i SAMLResponse som hvert sit *Privilege*. En eventuel dataafgrænsning på en rolle er defineret som en *Constraint* på et *Privilege*. For tekniske detaljer se afsnit *7.2 Roller og afgrænsninger i SAML*. Logout-sekvens er beskrevet i appendiks.

2.2 Brugerroller og dataafgrænsning

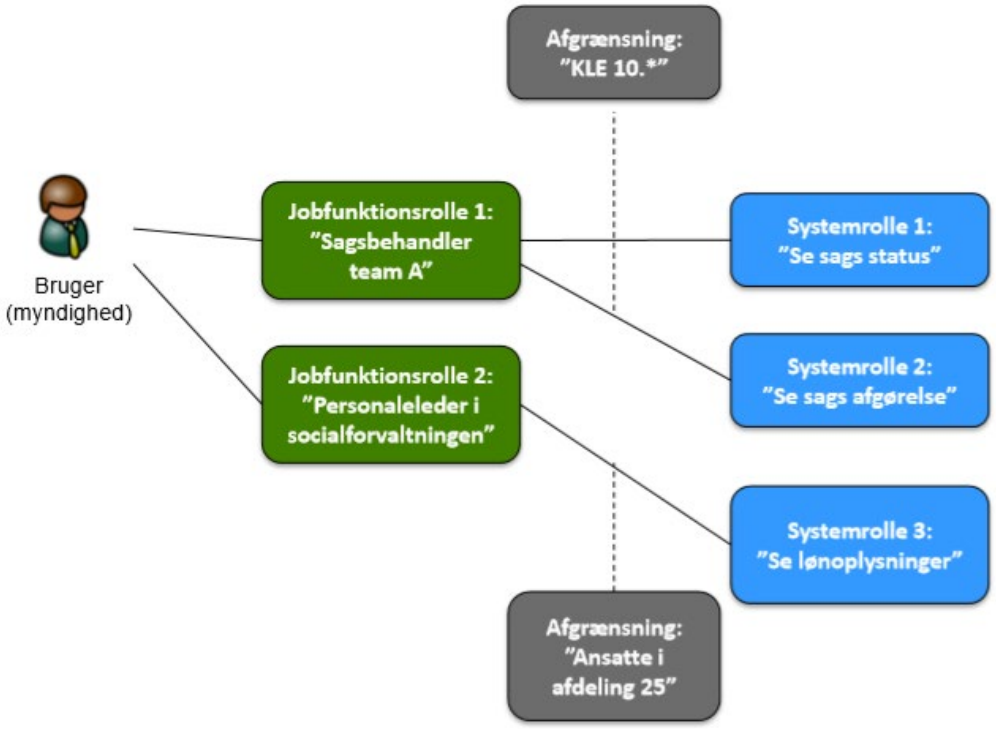
En brugers rettigheder i sikkerhedsmodellen udtrykkes ved kombinationer af roller og afgrænsninger. Fx kan man udtrykke en rettighed som ”du må læse dokumenter, men kun de dokumenter der omhandler dagpenge” eller ”som medarbejder må du se lønoplysninger, men kun i din egen afdeling”.

For detaljeret beskrivelse se [SIKKERHEDSMODEL] - afsnit *4.1 Rollemodel* samt det første afsnit i [IDP]. Begreberne introduceres kort her:

Brugersystemrolle	*Systemroller er tekniske roller, som giver adgang til at udføre bestemte handlinger i de underliggende it-systemer. Systemrollerne er specifikke for det enkelte it-system (defineres af dette)*
Dataafgrænsningstype	*De enkelte it-systemer kan håndtere forskellige typer dataafgrænsninger i deres rettighedsmodel. Eksempler på dataafgræsninger kan være KLE numre, følsomhed (ud fra en klassifikation), organisatorisk tilhørsforhold mv.*
Jobfunktionsrolle	*Jobfunktionsroller er forretningsmæssige roller, som defineres individuelt af hver myndighed og tildeles brugere via det lokale brugerkatalog*

Når du har modelleret og registreret dit systems brugersystemroller, skal myndigheden efterfølgende kombinere brugersystemroller (og eventuelle dataafgrænsninger) i myndighedens samleroller – også kaldet jobfunktionsroller. Denne efter-modellering af rettigheder er kommunens opgave, og den udføres lokalt i henholdsvis det fælleskommunale administrationsmodul og kommunens lokale rettighedsstyringssystem.

Følgende eksempel er gengivelse fra [SIKKERHEDSMODEL] afsnit 4.1 *Rollemodel*:



2.3 Teknisk fundament

Sikkerhedsmodellen baserer sig på [SAML] (Security Assertion Markup Language) version 2.0. SAML specificerer både en række kommunikationsprotokoller (kaldet Bindings) og et beskedformat til at udveksle informationer og forespørgsler, der er relateret til autentifikation og autorisation af brugere.

SAML specifikationer er profileret i en dansk udgave, som kaldes [OIOSAML]. Den beskriver hvilke protokoller det er lovlige at anvende, og hvilke data som må/skal medsendes i beskederne, der sendes via protokollerne. KOMBIT har sub-profileret OIOSAML profilen ved at tilføje ekstra krævede felter til de beskeder, der sendes over SAML protokollerne. Når du skal implementere SAML i dit brugervendte system, anvender du typisk et kode-rammeværk, der understøtter SAML protokollerne, og som kan generere de beskedformater, der sendes over protokollen.

Læs mere i [VILKÅR] appendix D.

2.4 Forudsætninger

Bestilling af FOCES certifikat

Certifikater anvendes i SAML til signering og kryptering af beskeder, og der skal etableres tillid (Trust) mellem parterne før en besked kan accepteres af modtageren. Du skal således have et dedikeret funktionscertifikat for at kunne fuldføre SAML-konfigurationen i dit fagsystem eller din Identity Provider. Bestilling af funktionscertifikat er beskrevet i [KGIG-VEJL] - *certifikater*. Tillid etableres efterfølgende ved at begge parter registrerer modpartens SAML metadata, hvor certifikatet er indlejret.

Registrering som leverandør

Hvis du ikke allerede er oprettet som leverandør og har registreret dit IT-system, følg da vejledninger der henvises til i [ADMINTRO] - *Brugervejledning til Administrationsmodulerne for leverandører*. Her beskrives hvordan du oprettes som organisation (leverandør) og hvordan du opretter dit IT-system. For IT-systemer der integrerer med Adgangsstyring for brugere benyttes betegnelsen *Brugervendt system*.

Nemlog-in rettigheder

For at kunne anvende det fælleskommunale administrationsmodul som leverandør eller myndighed skal din medarbejdersignatur have tildelt rettigheder. Se [ADMINTRO] - *Vejledning i tildeling af rettigheder i NemLog-in til Fælleskommunalt Administrationsmodul*.

Valg af Identity Provider til testformål

Hvis du skal tilslutte dit fagsystem til Adgangsstyring for brugere, som Brugervendt system i den fælleskommunale infrastruktur, har du brug for at kunne teste integrationen via en

Identity Provider som også er tilsluttet føderationen. Du skal have adgang til testbrugere der har dine brugersystemroller tilknyttet deres jobfunktionsroller. Du har følgende muligheder:

(1) Brug en myndigheds Identity Provider, ved at bede dem om at oprette brugere til dig. Du kan vælge, at anvende en af dine kommunale kunders IdP, da alle kommuner har etableret en IdP i det eksterne testmiljø. Det skal du afklare direkte med den enkelte kommune, uden om KOMBIT.

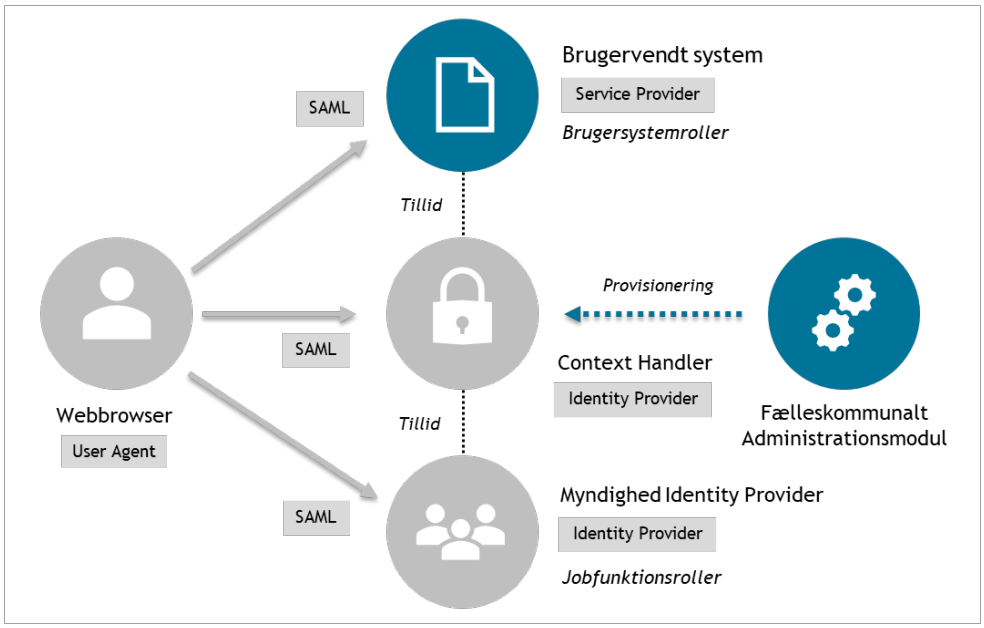
(2) Opsætning af egen Identity Provider. Tilslutning af IdP er beskrevet i kapitel 5 - *Tilslut Identity Provider*. Bemærk at det kræver, at du er oprettet som Leverandørmyndighed, hvilket også er beskrevet i kapitel 5. Du etablerer da en føderationsaftale for din egen myndighed og opretter selv dine brugere.

Tilslutning i Produktion

Du skal læse [VILKÅR] - Vilkår for adgangsstyring for et brugervendt system inden tilslutning påbegyndes i produktionsmiljøet. Se også afsnit *2.1.3 Specifikke forsætninger for tilslutning af denne integrationspart* i [SF1511].

3 Tilslut brugervendt system

Beskrivelse af opgaver der skal udføres, når du som leverandør skal tilslutte dit fagsystem som brugervendt system i den fælleskommunale Adgangsstyring for brugere.



Brugervendt system

- 3.1 Fastlæg brugersystemroller
- 3.2 Vælg SAML rammeværk
- 3.3 Udfør SAML konfiguration
- 3.4 Etabler tillid til Context Handler

Fælleskommunalt administrationsmodul

- 3.5 Registrer Brugervendt system

Se [KGIG-VEJL] - *Tilslut brugervendt system* for praktisk eksempel på udførsel af opgaverne.

3.1 Fastlæg brugersystemroller

Design og modellér de brugersystemroller din løsning skal understøtte. Deriblandt om dataafgrænsning er relevant for de enkelte roller. Du kan hente inspiration i [ROLLEDESIGN].

Selve opgaven omkring design og modellering af brugersystemroller skal du gennemføre, før du påbegynder den tekniske implementering. Du kan løbende tilpasse sættet af brugersystemroller og dataafgrænsningstyper, så du kan starte med et initielt design og gennemføre hele integrationen med dette, for derefter at tilrette til det endelige design på et senere tidspunkt. Det vil dog være nødvendigt at genteste efter tilretning.

3.2 Vælg SAML-rammeværk

Vælg et SAML framework og indarbejd det i din løsning, så du kan danne SAML metadata. Rammeværket kan typisk danne den nødvendige XML-fil. Hvis du ikke allerede har valgt rammeværk, kan det være relevant at kigge på de rammeværk, som Digitaliseringsstyrelsen stiller til rådighed på digitaliser.dk (se [OIOSAML]) til hhv. Java og .NET platformen).

3.3 Udfør SAML konfiguration

Se dokumentationen for dit valgte SAML rammeværk, for hvorledes du konfigurerer din Service Provider. Et praktisk eksempel er at finde i [KGIG-VEJL] - *Tilslut brugervendt system*. Konfigurationen skal være komplet, før du kan generere din SAML metadata, som du skal bruge ved registreringen af dit brugervendte system.

Som reference finder du nederst på siden Adgangsstyring for brugere - *Eksempel: metadata for brugervendt system*.

Bemærk at du skal anvende et FOCES certifikat fra Nets/DanID til dette formål, som beskrevet i afsnit *2.4 Forudsætninger*.

3.4 Etabler tillid til Context Handler

Du skal registrere Context Handler som Identity provider for dit fagsystem. Se dokumentationen for dit valgte SAML rammeværk, for hvorledes du gør dette. Du finder SAML-metadata for Context Handler nederst på siden Adgangsstyring for brugere - *Link til metadata*:

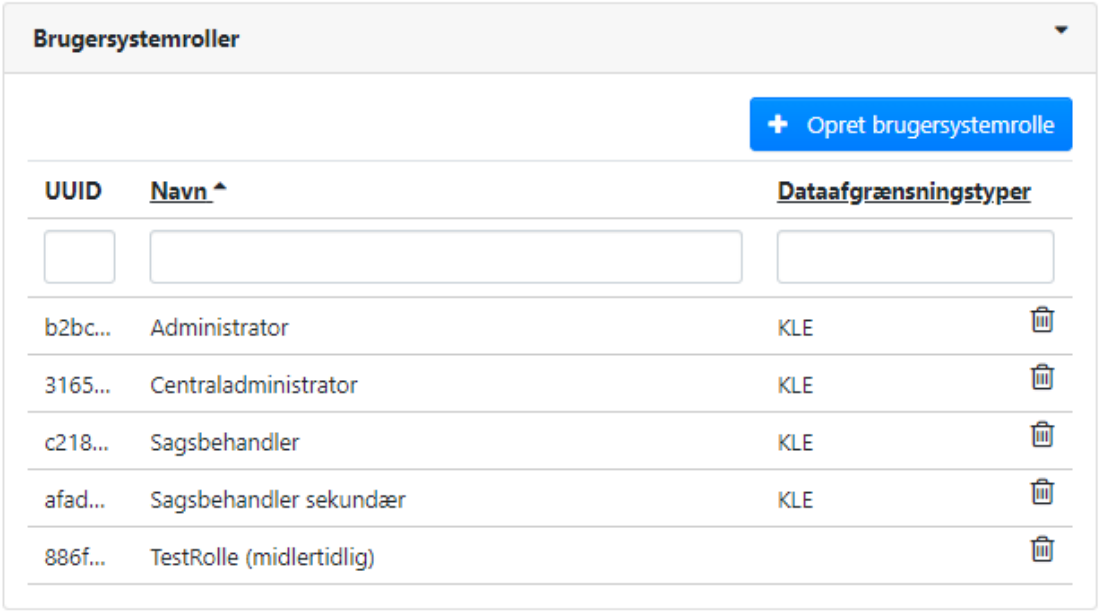
- Metadata Ekstern Test
- Metadata Produktion

3.5 Registrer brugervendt system

Du kan nu melde dit fagsystem ind i SAML føderationen og integrere med Adgangsstyring for brugere. De følgende trin er beskrevet i detaljer i [KGIG-VEJL] - *Tilslut brugervendt system*:

- Opret dit IT-system som type "Brugervendt system"
- Upload SAML metadatafilen for dit brugervendte system i Fælleskommunal Administration.
- Indtast brugersystemroller og eventuelle dataafgrænsningsværdier, som dit brugervendte system understøtter.

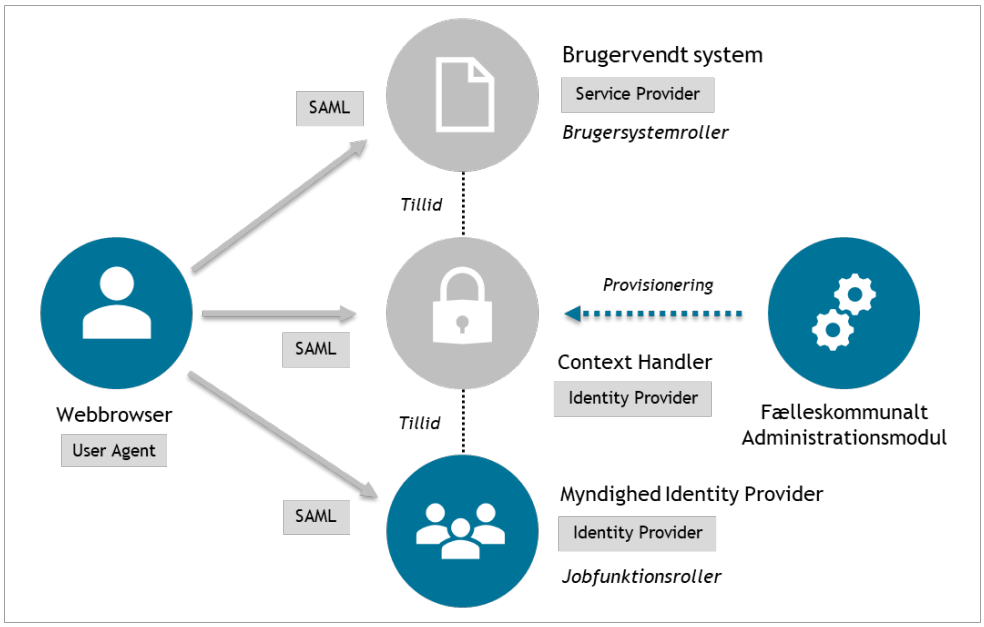
Når du har gennemført ovenstående trin, er der etableret teknisk forbindelse mellem dit brugervendte system og Context Handler (via udvekslingen af SAML metadata). Det er nu muligt at autentificere brugere fra myndigheder, der har registreret jobfunktionsroller og mapping til brugersystemroller knyttet til dit fagsystem, som beskrevet i det efterfølgende kapitel. Følgende er et eksempel på et registreret brugervendt system i den fælleskommunale administration:



Dit fagsystem er nu integreret til Adgangsstyring for brugere. For at kunne udføre integrationstest skal opgaverne beskrevet i kapitel 4 - "Anvend brugervendt system" gennemføres, for myndigheder hvis brugere skal kunne logge ind i fagsystemet.

4 Anvend brugervendt system

Beskrivelse af opgaver der skal udføres, når du som myndighed, eller leverandørmyndighed i testøjemed, skal give brugere adgang til et brugervendt system



Identity Provider

- 4.1 Opret jobfunktionsroller
- 4.2 Tildel brugere jobfunktionsroller

Fælleskommunalt administrationsmodul

- 4.3 Tilknyt brugersystemroller til jobfunktionsroller

User (webbrowser)

- 4.4 Udfør Integrationstest

4.1 Opret jobfunktionsroller

Når du som myndighed har besluttet dig for din ønskede model for styring af adgange til det nye fagsystem, kan der være behov for at introducere nye jobfunktionsroller til formålet. Det kan også tænkes, at dine eksisterende jobfunktionsroller er fyldestgørende og kan genanvendes, hvorefter denne opgave bortfalder.

En forudsætning for at kunne udføre opgaven er, at leverandøren har udleveret en oversigt af brugersystemroller implementeret i fagsystemet, der for hver af disse inkluderer en beskrivelse af hvilke rettigheder der tildeles i fagsystemet.

Da tildeling af jobfunktionsroller til en bruger udmønter sig i brugersystemroller i pågældende fagsystem, som igen udmønter sig i brugers rettigheder til at se/opdatere information i fagsystemet, anbefales det, at du dokumenterer dit design for tildeling af rettigheder via jobfunktionsroller, inden disse implementeres. Til inspiration kan du se eksempler i [ROLLEDESIGN].

Hvis der er behov for at introducere nye jobfunktionsroller, skal denne funktionalitet tilføjes din IdP-løsning, så det er muligt at tildele dem brugere i din brugeradministration.

Bemærk navnestandard for Jobfunktionsrolle EntityId, inden du opretter dem! For en sikkerheds skyld kan du oprette dem i ADM først, som beskrevet i afsnit 4.3. Her fremgår EntityId.

Hvis du i testøjemed har etableret og tilsluttet egen IdP som leverandørmyndighed, er det frit for dig at definere passende jobfunktionsroller, der gør det muligt for dig at teste alle varianter af brugersystemroller.

Bemærk, at det er muligt at oprette delegerede jobfunktionsroller, således at en bruger fra myndighed A kan tilgå et brugervendt system med brugersystemroller på vegne af myndighed B. Dette er ikke nærmere beskrevet i denne vejledning.

4.2 Tildel brugere jobfunktionsroller

Hvis du har genanvendt eksisterende jobfunktionsroller, vil dine brugere automatisk få adgang til det nye fagsystem, så snart du har tilføjet de nye brugersystemroller i ADM, og denne opgaver bortfalder.

Hvis du har introduceret nye jobfunktionsroller, skal disse selvfølgelig tildeles relevante brugere, før at de vil kunne tilgå det nye fagsystem. Der vil således foreligge en opgave på dette, der skal planlægges og udføres, i forbindelse med ibrugtagning i produktionsmiljøet.

4.3 Tilknyt brugersystemroller til jobfunktionsroller

I ADM definerer du som myndighed, hvorledes dine jobfunktionsroller skal oversættes til brugersystemroller, der giver rettigheder i fagsystemet.

Du logger ind i den fælleskommunale administration og vælger ”Jobfunktionsroller” i hovedmenuen. Se [IDP] afsnit *HVORDAN OPRETTES JOBFUNKTIONSROLLER?*.

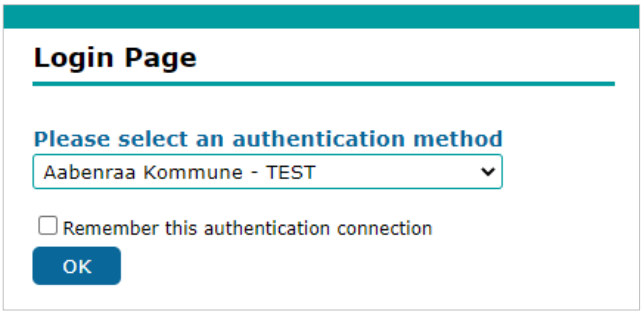
Her et eksempel på en jobfunktionsrolle ”bbrregisterfoerer” som oversættes til brugersystemrollen ”Registerfoerer” i systemet BBR, når bruger er autentificeret i en IdP der har føderationsaftale for myndighed ”Aalborg kommune”:

Hvis du genanvender eksisterende jobfunktionsroller, skal de nye brugersystemroller tilføjes disse som specificeret i din model for styring af adgange og rettigheder.

Hvis du har introduceret nye jobfunktionsroller til formålet, skal disse oprettes, hvorefter de respektive brugersystemroller kan tilknyttes.

4.4 Udfør integrationstest

Med Context Handler registreret som Identity Provider for fagsystemet, sendes brugere videre til Context Handler med et SAML Authentication Request når de prøver at tilgå fagsystemet uden en session, som beskrevet i afsnit 2.1 Oversigt *Login-sekvens*. Her vises startsiden for Context Handler, hvor bruger skal vælge Identity Provider de vil autentificeres mod:



Bruger vælger Identity Provider fra den myndighed de tilhører, hvorefter de sendes videre til denne for autentificering.

I testmiljøet

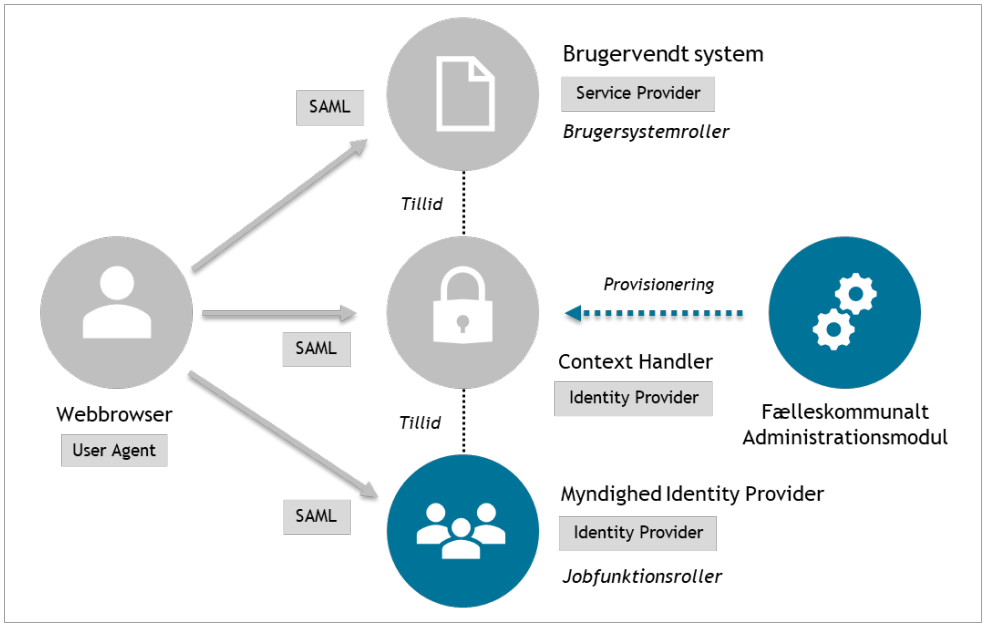
Her vælges Identity Provider der blev bestemt i testøjemed, som beskrevet i 2.4 *Forudsætninger*.

I produktion

Alle myndigheder, der har gennemført opgaverne beskrevet i dette kapitel, kan nu logge ind i fagsystemet.

5 Tilslut Identity Provider

Beskrivelse af opgaver der skal udføres, når en Identity Provider skal tilsluttes den fælleskommunale Adgangsstyring for brugere



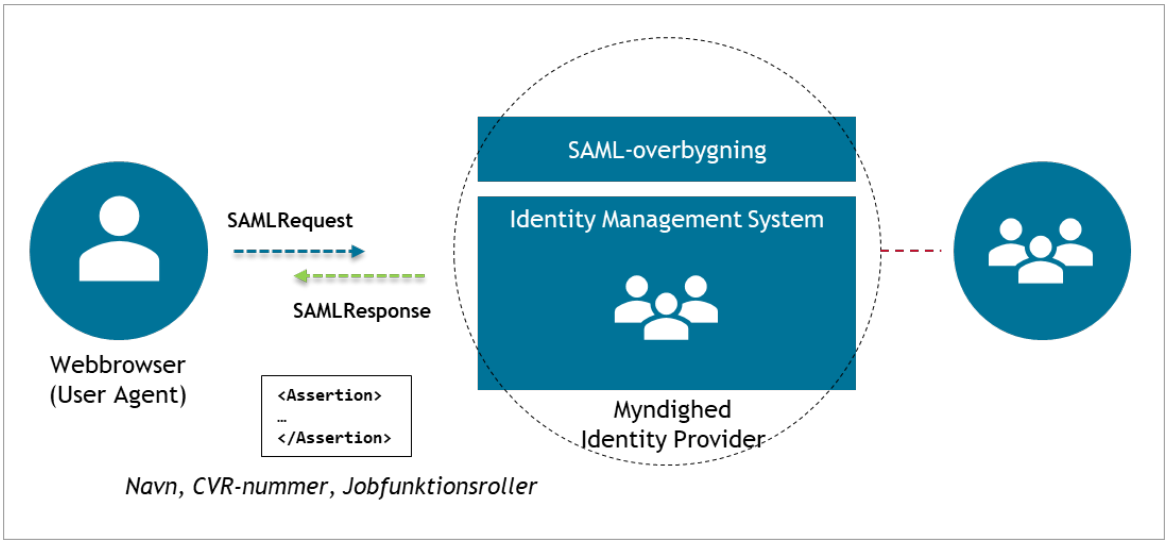
Identity Provider

- 5.1 Tilføj KOMBIT attributprofil
- 5.2 Tilføj jobfunktionsrolle-funktionalitet
- 5.3 Etabler tillid til Context Handler

Fælleskommunalt administrationsmodul

- 5.4 Registrer Identity Provider
- 5.5 Opret føderationsaftale

En IdP består typisk af et Identity Management System med et brugerkatalog (fx Active Directory) med en SAML-overbygning (fx AD FS), der udstiller login/logout endpoints samt metadata. Der skal udføres opgaver i begge komponenter, således at en autentificeret bruger sendes tilbage til Context Handler med korrekt formateret Assertion indeholdende information om brugeren samt jobfunktionsroller.



Det er individuelt for hver lokale løsning, hvilke attributter man har defineret på brugere, samt hvorledes man har valgt at strukturere brugere i grupper mm.

Der findes også selvstændige IdP-løsninger, der har SAML indbygget fra starten, hvor hele konfigurationen således foregår i samme komponent. Disse anvendes typisk i testøjemed.

Grundet de mange produkter og lokale løsningsvarianter er det således ikke muligt, at komme med specifikke retningslinjer for udførsel af opgaverne. Her er blot krav til opsætningen angivet, og du bedes se dokumentationen for de produkter du anvender.

Opgaverne er nærmere beskrevet i [IDP] - *HVORDAN TILSLUTTES IDENTITY PROVIDEREN?*, dette er blot en kort gennemgang med formål at give overblik.

Note: En Identity Provider kan autentificere brugere fra flere myndigheder, hvis disse er registreret i dens brugerkatalog og der foreligger føderationsaftaler, men i praksis og i produktion har hver kommune typisk sin egen dedikerede IdP. Derfor er mange IdP navngivet ”xxx kommune” i det fælleskommunale administrationsmodul. Hvis brugere fra myndighed A skal tilgå et fagsystem på vegne af myndighed B, da anvendes delegerede jobfunktionsroller.

5.1 Tilføj KOMBIT attributprofil

Du skal sikre dig, at tokens (Assertions) udstedt af din IdP i et SAML Response har den korrekte struktur, format og indhold. Dette er nærmere beskrevet i [VILKÅR] *Appendiks D: KOMBIT Attributprofil for SAML tokens*.

Forneden er vist et forkortet eksempel med essentielle parametre markeret med gult:

```
<Assertion>
    ...
    <Subject>
        <NameID>C=DK,O=19435075,CN=Test Testesen,Serial=fd2ed2a9-09fc-4b4f-98a6-6d7bf206d088</NameID>
    </Subject>
    <Conditions>
        <AudienceRestriction>
            <Audience>https://saml.adgangsstyring.eksterntest-stoettesystemerne.dk</Audience>
        </AudienceRestriction>
    </Conditions>
    <AttributeStatement>
        <Attribute Name="dk:gov:saml:attribute:CvrNumberIdentifier">
            <AttributeValue>19435075</AttributeValue>
        </Attribute>
        <Attribute Name="dk:gov:saml:attribute:KombitSpecVer">
            <AttributeValue>1.0</AttributeValue>
        </Attribute>
        <Attribute Name="dk:gov:saml:attribute:SpecVer">
            <AttributeValue>DK-SAML-2.0</AttributeValue>
        </Attribute>
        <Attribute Name="dk:gov:saml:attribute:AssuranceLevel">
            <AttributeValue>3</AttributeValue>
        </Attribute>
        <Attribute Name="dk:gov:saml:attribute:Privileges_intermediate">
            <AttributeValue>PD94bW...aXN0Pg==</AttributeValue>
        </Attribute>
    </AttributeStatement>
</Assertion>
```

Se dokumentationen for din SAML-udvidelse, for hvorledes du konfigurerer denne til at følge KOMBITs attributprofil.

Elementet *Privileges_Intermediate* skal indeholde brugers jobfunktionsroller som base64-indkodet streng, hvilket er beskrevet i det efterfølgende afsnit.

5.2 Tilføj jobfunktionsrolle-funktionalitet

Ved autentificering af bruger skal vedkommendes jobfunktionsroller aflæses og angives i *Assertion - Privileges_Intermediate*. Format er specificeret i:

- [IDP] *JOBFUNKTIONSROLLER ANGIVES SOM OIOBPP*
- [VILKÅR] *6.4 Brugertokens med jobfunktionsroller*

Her et forkortet eksempel:

```
<bpp:PrivilegeList xmlns:bpp="http://itst.dk/oiosaml/basic_privilege_profile">
    <PrivilegeGroup Scope="urn:dk:gov:saml:cvrNumberIdentifier:22222222">
        <Privilege>http://kommuneB.dk/roles/jobrole/klassifikationsadministrator/1</Privilege>
        <Privilege>http://kommuneB.dk/roles/jobrole/OrganisationAdministrator/1</Privilege>
    </PrivilegeGroup>
</bpp:PrivilegeList>
```

Det er individuelt for hver lokale løsning, hvorledes en brugers jobfunktionsroller aflæses og tilføjes SAML Response. Se dokumentationen for dit valgte produkt.

5.3 Etabler tillid til Context Handler

Der skal etableres tillid til Context Handler (CH), før at SAML Authentication requests bliver accepteret af din IdP. Dette gøres ved at registrere CH SAML metadata. Du finder CH SAML metadata til både test og produktion nederst på siden Adgangsstyring for brugere.

Dette er helt individuelt for det specifikke produkt der anvendes. Praktiske eksempler kan ses i [IDP] - *1. REGISTRERING AF CONTEXT HANDLER SOM RP/SP*.

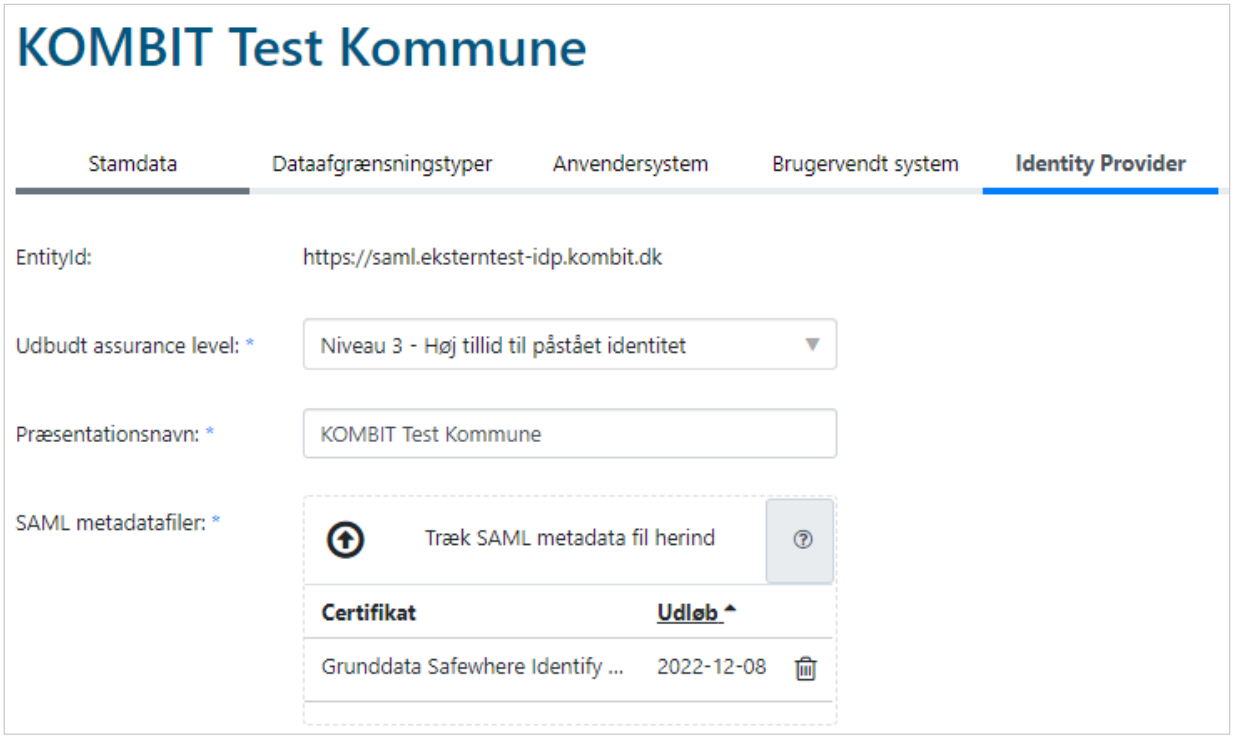
5.4 Registrer Identity Provider

Du skal være oprettet som Leverandør i den fælleskommunale administration, som beskrevet under 3.4 forudsætninger, for at kunne registrere et IT-system som Identity Provider. Du finder de specifkke instruktioner for registrering af Identity Provider i den fælleskommunale administration her:

- [IDP] 2. METADATA UDTRÆKKES OG REGISTRERES HOS KOMBIT
- [IDP] Registrering af IdP i Administrationsmodulet

Du skal inden have færdiggjort SAML-konfigurationen, for at sikre, at din SAML metadata er korrekt, Som reference kan du se Adgangsstyring for brugere - *Eksempel: metadata for Identity provider*.

Bemærk, at du efterfølgende ikke kan ændre entityId, der unikt identificerer din IdP! Hvis du har behov for at ændre entityId, da er du nød til at slette dit IT-system i administrationen og oprette det igen.



Figur 3. eksempel på en registreret Identity Provider

5.5 Opret føderationsaftale

En Identity Provider skal have mindst én tilknyttet føderationsaftale, før at denne kan anvendes til autentificering af brugere. En føderationsaftale giver en IdP lov til at autentificere brugere for en specifik myndighed. En føderationsaftale skal godkendes af den myndighed som aftalen omhandler.

Hvis du er oprettet som Leverandørmyndighed og skal teste med din egen IdP, da skal du oprette og godkende af føderationsaftale for egen myndighed gældende egen IdP.

Du kan se skærmbilleder fra føderationsaftale anmodning-godkendelse processen i [IDP] startende på slide 33 - *Liste over føderationsaftaler*.

Figur 4. Eksempel på en føderationsaftale

6 Bilagsliste

Nedenfor finder du links til de bilag, vejledningen refererer til. Links fører dig til listevisninger i vores dokumentbibliotek. Listerne kan indeholde flere dokumenter- vær derfor særlig opmærksom på dokumentets titel, så du får fat i det rigtige dokument.

[ADGBRUG]	Adgangsstyring for brugere (introside)
[VILKÅR]	Bilag 2 - Vilkår for anvendelse af sikkerhedsmodellen i Rammearkitekturen v.2.2
[SIKKERHEDSMODEL]	Bilag 2A - Beskrivelse af sikkerhedsmodellen i Rammearkitekturen v.2.2
[RETL]	Retningslinjer for anvendelse af det eksterne testmiljø
[ADMINTRO]	Fælleskommunalt Administrationsmodul - Introduktionsside
[ADMGUI]	Fælleskommunalt Administrationsmodul - Brugerflade
[NEMLOG-IN]	Vejledning til NemLogin
[METADATA]	Context Handler Metadata Ekstern Test Context Handler Metadata Produktion
[IDP]	Vejledning til opsætning af IdP
[SAML]	https://www.oasis-open.org/standards#samlv2.0
[OIOSAML]	https://www.digitaliser.dk/group/42063
[ROLLEDESIGN]	Jobfuntionsroller - principper
[KGIG-VEJL]	Kom-godt-i-gang vejledninger

[SF1511]	Sikkerhed - Hent Token fra Context Handler
[SF1515]	Sikkerhed - SAMLSingleLogout

7 Appendiks

7.1 Logout-sekvens

Ud over at kunne håndtere login, skal et brugervendt system også kunne håndtere logout, hvilket kan foregå på to forskellige måder, hvor det brugervendte system skal kunne håndtere begge disse. I SAML anvendes en single logout mekanisme, hvor en bruger der logger ud af ét brugervendt system vil blive logget ud af samtlige brugervendte systemer, brugeren er logget på. Dette single logout forløb håndteres af Context Handleren, men selve forløbet initieres fra ét af de brugervendte systemer. De to scenarier som et brugervendt system skal håndtere, er følgende:

Logout foretaget i det brugervendte system (trin 1+2+4+5 involverer det brugervendte system):

1 Brugeren vælger at logge ud af det brugervendte system (klikker på en knap, et link eller lignende).

2 Det brugervendte system danner et logout response (en SAML besked) og sender den til Context Handleren via en af de SAML Bindings, Context Handleren understøtter.

3 Der foretages nu single logout via Context Handleren – dette involverer ikke det brugervendte system.

4 Efter Context Handleren har foretaget single logout for brugeren, sendes et logout response tilbage til det brugervendte system via en af de SAML Bindings, som det brugervendte system understøtter.

5 Det brugervendte system har nu logget brugeren ud og kan give brugeren information om, at logout er gennemført.

Logout foretaget i et andet system end det brugervendte system (trin 3+4 involverer det brugervendte system):

1 Brugeren er logget ind både i det brugervendte system samt i mindst ét andet system, der er integreret med Context Handler.

2 Brugeren foretager logout i det andet system, og det andet system sender et logout request til Context Handleren.

3 Context Handleren sender nu et logout request til det brugervendte system via en af de SAML Bindings, som det brugervendte system understøtter.

4 Det brugervendte system skal på baggrund af dette request foretage et logout af brugeren og sende et logout response tilbage til Context Handleren via en af de SAML Bindings, som Context Handleren understøtter.

5 Context Handleren fortsætter single logout forløbet, og brugeren ender med at blive navigeret tilbage til det andet system, som initierede logoutforløbet.

Når du kan gennemføre et login, hvor det brugervendte system modtager brugersystemroller fra Context Handleren, har du succesfuldt etableret en integration til Adgangsstyring for brugere.

7.2 Roller og afgrænsninger i SAML

OIO-BPP formatet anvendes til at udtrykke de roller og afgrænsninger, en bruger er tildelt, hvilket er beskrevet i detaljer i [VILKÅR] appendiks D. Et eksempel på en tildelt rolle er vist nedenfor.

```
<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:19435075">
        <Privilege>http://sapa.kombit.dk/roles/usersystemrole/se_sager/1</Privilege>
        <Constraint Name="http://sts.kombit.dk/constraints/kle/1">
            27.24.00,27.24.27
        </Constraint>
        <Constraint Name="http://sts.kombit.dk/constraints/organisation/1">
            709545f1-c00f-43c1-818e-cb2cb066f56e
        </Constraint>
    </PrivilegeGroup>
</bpp:PrivilegeList>
```

Som brugervendt system vil du fra Context Handleren modtage en XML-struktur magen til ovenstående, når en bruger logger på. Der vil være et PrivligeGroup element per rolle, som brugeren er tildelt. Hver af disse roller kan være så afgrænset individuelt (hvis du har valgt at din løsning arbejder med et dataafgrænsningsbegreb).

I ovenstående eksempel er brugeren tildelt roller ”se sager”, identificeret ved rollens EntityId (http://sapa.kombit.dk/roles/usersystemrole/se_sager/1), og denne rolle er afgrænset til sager fra to udvalgte KLE emneområder (27.24.00 og 27.24.27) og samtidig afgrænset yderligere til kun at give adgang til sager, der er ejet af organisationen med det nævnte UUID.

Bemærk at der alene modtages brugersystemroller og dataafgrænsningsværdier, som du har specificeret for dit brugervendte system. Data som kommunen måtte sende med brugeren, og som ikke er relevant for løsningen, vil blive fjernet af Context Handler.

7.3 Praktiske værktøjer

Da al kommunikation mellem fagsystemet og Context Handleren foregår gennem slutbrugerens browser, er det typisk lidt besværligt at inspicere de beskeder, der sendes frem og tilbage.

I SAML 2.0 er der tale om en såkaldt SAML User Agent, som typisk er en webbrowser, men som også kan være en desktop applikation, smartphone app eller lignende. Det vil sige, at der du sagtens kan anvende fx en smartphone app som User Agent mod infrastrukturen i stedet for en webbrowser - de skal blot implementere SAML flowet i deres User Agent.

Der findes nogle udmærkede online værktøjer til at tage beskeder (fx ved at kopiere dem fra netværks-tabben i sin browser), og decode disse, så man kan se det faktiske indhold, fx https://www.samltool.com/decode.php.

Alternativt findes der plugins til browsere, der kan dekode beskeder on-the-fly og vise dem i browseren. Eksempler på disse er:

- SAML Chrome Panel (Chrome)
- SAML-Tracer (Firefox)

Mulighed for at inspicere en kørende integration

KOMBIT har etableret et demo-fagsystem, der er integreret til test-miljøet. Her kan du i din browser inspicere login-flowet, hvilket kan være en praktisk måde at få startet op på de initielle kald. Demo fagsystemet kan nås på dette endpoint:

https://demo-brugervendtsystem.kombit.dk/test/

Bemærk: Dette kan kun anvendes af myndigheder i test.

7.4 SAML beskeder og bindings

Der er ingen direkte kommunikation mellem Context Handler, det brugervendte system og myndigheders IdP – det er brugerens browser, der bærer beskeder frem og tilbage mellem parterne. Enten via URL parameter i et HTTP-GET request, eller som payload i et HTTP-POST request. Beskeder er XML-dokumenter i base64-indkodning. Eksempel:

```
GET https://adgangsstyring.eksterntest-
stoettesystemerne.dk/runtime/saml2/issue.idp?SAMLRequest=jZJBT%2B...
```

Indholdet i ovenstående SAMLRequest er et Authentication Request.

AuthnRequest

Authentication Request dannes af fagsystemet og bruger sendes til Context Handler med dette. CH lader bruger vælge IdP der skal autentificeres mod, og husker hvilket fagsystem bruger skal sendes tilbage til efter autentificering. CH sender derefter bruger videre til valgte IdP med tilsvarende login request. Her et eksempel på et Authentication Request:

```
<saml2p:AuthnRequest
    AssertionConsumerServiceURL="https://sapa.kombit.dk/saml/SSO"
    Destination="https://adgangsstyring.stoettesystemerne.dk/runtime/saml2/issue.idp"
    ForceAuthn="false" ID="a3e87841j3g5e499i376eeae3edb56" IsPassive="false"
    IssueInstant="2018-06-15T07:55:48.930Z"
    ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" 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.sapa.kombit.dk
    </saml2:Issuer>
</saml2p:AuthnRequest>
```

Forespørgslen indeholder en reference til fagsystemet (Issuer elementet), hvor man via dennes unikke ID (også kaldet EntityID), fortæller Context Handler, hvilket fagsystem login requestet kommer fra.

SAMLResponse

Et SAMLResponse indeholder svaret på et request, typisk et AuthnRequest. Et sådan svar vil enten indeholde en fejlbesked eller et SAML token som vist i nedenstående eksempel. Bemærk at SAMLResponse indeholder et krypteret SAML token – og ens SAML framework automatisk vil dekryptere dette. For god ordens skyld vises både SAMLResponse og det tilhørende dekryptede Assertion element.

```
<Response Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified"
    Destination="https://sapa.kombit.dk/saml/SSO"
    ID="idac97669bec99434a92736645762b5e93"
    InResponseTo="a13b8791058c47e138gf64ci3g81hag" Version="2.0"
    IssueInstant="2018-06-15T09:26:26.4228635Z"
    xmlns="urn:oasis:names:tc:SAML:2.0:protocol">
    <Issuer xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
        https://saml.adgangsstyring. stoettesystemerne.dk
    </Issuer>
    <Status><StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/></Status>
    <EncryptedAssertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
        <xenc:EncryptedData Type="http://www.w3.org/2001/04/xmlenc#Element"
            xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
        <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-
cbc"/>
            <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
                <e:EncryptedKey xmlns:e="http://www.w3.org/2001/04/xmlenc#">
                    <e:EncryptionMethod
            Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
                        <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                    </e:EncryptionMethod>
                    <KeyInfo>
                        <o:SecurityTokenReference
                            xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-secext-1.0.xsd">
                            <X509Data>
                                <X509IssuerSerial>
```

```
                                    <X509IssuerName>CN=TRUST2408 Systemtest XXII CA,
O=TRUST2408, C=DK</X509IssuerName>
                                    <X509SerialNumber>1494997565</X509SerialNumber>
                                </X509IssuerSerial>
                            </X509Data>
                        </o:SecurityTokenReference>
                    </KeyInfo>
                    <e:CipherData>
                        <e:CipherValue>f3Lyb…s3Wg==</e:CipherValue>
                    </e:CipherData>
                </e:EncryptedKey>
            </KeyInfo>
            <xenc:CipherData>
                <xenc:CipherValue>BKw+ak…zisNU=</xenc:CipherValue>
            </xenc:CipherData>
        </xenc:EncryptedData>
    </EncryptedAssertion>
</Response>
```

Assertion

Denne besked kaldes også et SAML token og er en XML struktur, der indeholder brugerens identitet, brugersystemroller og dataafgrænsningsværdier. Det SAML framework, man anvender i sit fagsystem, vil håndtere disse SAML beskeder, så nedenstående eksempler er blot for at illustrere indholdet af beskederne, og ikke fordi man aktivt skal forsøge at parse og behandle disse.

```
<Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
ID="id622063e2c04b49d898bfad1a8827e6fe"
           IssueInstant="2018-06-15T09:26:26.422Z" Version="2.0">
    <Issuer>https://saml.adgangsstyring.stoettesystemerne.dk</Issuer>
    <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
        <SignedInfo>
            <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256"/>
            <Reference URI="#id622063e2c04b49d898bfad1a8827e6fe">
                <Transforms>
                    <Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                    <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </Transforms>
                <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

<DigestValue>4WcQKfQQXHiVoD5VstIlxhrLCTwJisJsjgPRF5Bo+2M=</DigestValue>
            </Reference>
        </SignedInfo>
        <SignatureValue>ixfd...jL2</SignatureValue>
        <KeyInfo>
            <X509Data>
                <X509Certificate>MIIGHz...wCQYDV </X509Certificate>
            </X509Data>
        </KeyInfo>
    </Signature>
    <Subject>
        <NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
            C=DK,O=19435075,CN=Hans Hansen,Serial=74c08b2b-212b-4f6d-9ce6-
0fba1651087d
        </NameID>
        <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <SubjectConfirmationData InResponseTo="a13b8791058c47e138gf64ci3g81hag"
```

```
            NotOnOrAfter="2018-06-15T09:31:26.422Z"
            Recipient="https://sapa.kombit.dk/saml/SSO"/>
        </SubjectConfirmation>
    </Subject>
    <Conditions NotBefore="2018-06-15T09:26:26.422Z" NotOnOrAfter="2018-06-
15T09:31:26.422Z">
        <AudienceRestriction>
            <Audience>https://saml.sapa.kombit.dk</Audience>
        </AudienceRestriction>
    </Conditions>
    <AuthnStatement AuthnInstant="2018-06-15T09:26:26.422Z" SessionIndex="204072065">
        <AuthnContext>
            <AuthnContextClassRef>urn:4</AuthnContextClassRef>
        </AuthnContext>
    </AuthnStatement>
    <AttributeStatement>
        <Attribute Name="dk:gov:saml:attribute:CvrNumberIdentifier"
                   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
            <AttributeValue>19435075</AttributeValue>
        </Attribute>
        <Attribute Name="dk:gov:saml:attribute:SpecVer"
                   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
            <AttributeValue>DK-SAML-2.0</AttributeValue>
        </Attribute>
        <Attribute Name="dk:gov:saml:attribute:KombitSpecVer"
                   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
            <AttributeValue>1.0</AttributeValue>
        </Attribute>
        <Attribute Name="dk:gov:saml:attribute:AssuranceLevel"
                   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
            <AttributeValue>4</AttributeValue>
        </Attribute>
        <Attribute Name="dk:gov:saml:attribute:Privileges_intermediate"
                   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
            <AttributeValue>PD94bWw...0iVVRGLT </AttributeValue>
        </Attribute>
    </AttributeStatement>
</Assertion>
```

LogoutRequest

Dette er et logout request, som kan dannes af både fagsystemet, eller af Context Handler initieret af et andet fagsystem. Hvis en bruger ønsker at logge ud af fagsystemet og trykker på en ”logout” knap, så kan fagsystemet danne et LogoutRequest, der sendes til Context Handler for at bede den afslutte brugerens SAML session. Det kan også være Context Handler, der initierer logout, og her vil fagsystemet skulle modtage et LogoutRequest og foretage et logout af brugeren i fagsystemet på baggrund af dette request.

```
<saml2p:LogoutRequest
    Destination="https://adgangsstyring.stoettesystemerne.dk/runtime/saml2/issue.idp"
    ID="a32667835ihbgbgj3f1fcb23cj0i2db" IssueInstant="2018-06-15T07:55:55.783Z"
    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.sapa.kombit.dk
    </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=19435075,CN=Hans Hansen,Serial=74c08b2b-212b-4f6d-9ce6-0fba1651087d
        </saml2:NameID>
    <saml2p:SessionIndex>2038322619</saml2p:SessionIndex>
```

```
</saml2p:LogoutRequest>
```

Ovenstående logout request er dannet af fagsystemet og sendt til Context Handleren. Her beder man Context Handleren om at logge en bestemt bruger ud (identificeret via NameID). Context Handleren kan se, hvilket fagsystem der beder om at få logget brugeren ud via Issuer elementet.

Et request, der kommer fra Context Handleren til fagsystemet, vil have samme struktur blot med Context Handleren som Issuer.

SAML Bindings

I SAML specifikationen er der en række forskellige bindinger. En Binding beskriver, hvordan ovenstående SAML beskeder kommunikeres mellem Context Handleren og fagsystemet. De to Bindings, der anvendes i KOMBIT infrastrukturen, er:

• HTTP-Redirect. Denne Binding anvendes typisk når man sender mindre SAML beskeder. I denne Binding zip-komprimeres XML beskeden, hvorefter den base64-enkodes, og så sendes den via en HTTP-GET som en URL parameter. Da man ønsker så små beskeder som muligt, udføres der ikke nogen XMLDSIG signatur på XML beskeden. I stedes laves en detached signatur på beskeden, som vedlægges som endnu en URL parameter i requestet.

• HTTP-POST. Denne binding anvendes typisk, når man sender større SAML beskeder. I denne Binding tilføjes en XMLDSIG signatur på XML beskeden, og hele beskeden sendes som et body payload på en HTTP-POST.

For begge Bindings gælder, at man bruger brugerens browser til at kommunikere med. Så hvis fagsystemet vil sende en AuthnRequest via HTTP-Redirect til Context Handleren, så dannes den fornødne XML besked, og den sendes ved at lade browseren foretage et GET mod et bestemt endpoint på Context Handleren med de nævnte URL parametre.

De fleste SAML frameworks understøtter begge disse Bindings, og SAML frameworkene håndterer typisk selv at vælge den korrekte Binding (ud fra størrelsen på beskeden, konteksten m.m.). De SAML metadata, der udveksles, beskriver hvilke Bindings den enkelte part understøtter, samt på hvilke beskedtyper disse Bindings kan anvendes.

Det anbefales dog på det kraftigste at anvende HTTP-POST til logout, da browsere typisk blokerer for mange på hinanden følgende redirects, og et single logout forløb involverer, at der sendes ca. to beskeder per system, som brugeren er logget på.

Denne kommunikation via de nævnte Bindings er noget ens SAML framework typisk tager sig af.