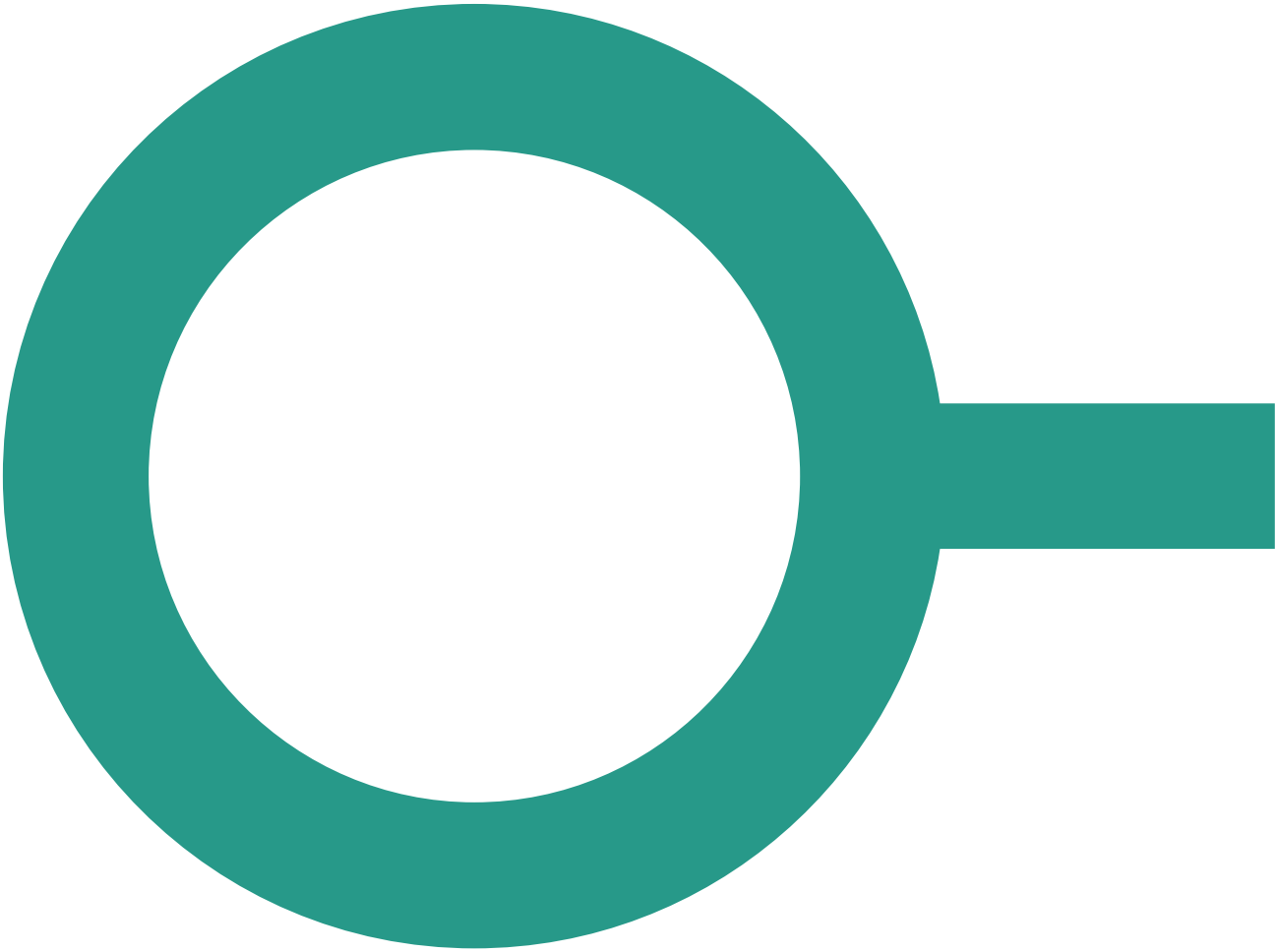


VEJLEDNING TIL ADGANGSSTYRING FOR BRUGERE

– SÅDAN IMPLEMENTERER DU SINGLE SIGN ON

Version 1.1

KOMBIT

Kommunernes it-fællesskab

Versionshistorik

Version	Dato	Kommentar
0.1	2018-06-15	Initiel udgave
0.2	2018-06-21	Opdateret efter reviewrunde
0.3	2018-06-26	Opdateret med ny struktur
0.4	2018-07-11	Opdateret efter 1. review
0.5	2018-09-04	Opdateret efter 2. review
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

INDHOLDSFORTEGNELSE

1 INDLEDNING

Adgangsstyring for brugere er en af hjørnestenene i sikkerhedsmodellen i den fælleskommunale infrastruktur. Adgangsstyring for brugere gør det muligt for kommunen 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 i selve fagløsningen, men blot håndhæves nogle brugersystemroller.

Med Adgangsstyring for brugere er det muligt for kommunerne at implementere Single Sign On til alle deres løsninger.

2 LÆSEVEJLEDNING

Denne vejledning giver et overblik over de aktiviteter, der skal til for, at du som leverandør kan implementere Adgangsstyring for brugere succesfuldt. Herudover beskriver vejledningen de enkelte aktiviteter trin for trin.

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 kommunens vinkel som brugere af dit it-system. Overblikket er suppleret med en tjekliste, som du kan bruge til at understøtte din implementering af Adgangsstyring for brugere.

Dele af vejledningen er teknisk funderet og er målrettet dig, som skal udføre den tekniske implementering af integrationen til Adgangsstyring for brugere. I vejledningens sidste kapitler er nogle eksempler på SAML beskeder, der kan give en bedre forståelse for den kommunikation, der indgår i integrationen med Adgangsstyring for brugere.

Vi anbefaler, at du læser de mest relevante afsnit i [VILKÅR] og [SIKKERHEDSMODEL], før du går i gang med den tekniske implementering.

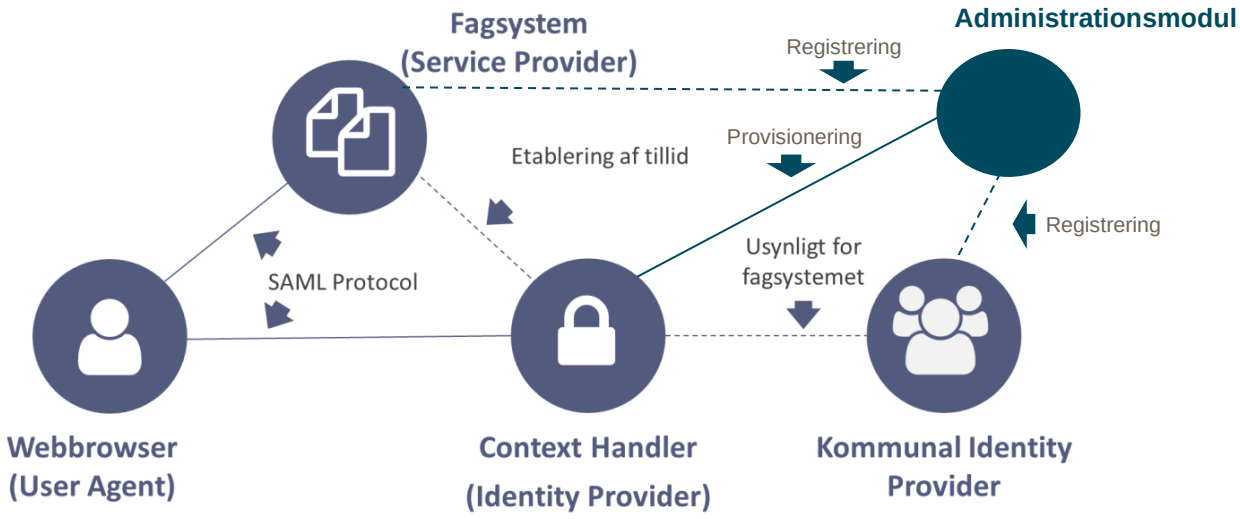
- [VILKÅR] Afsnit 1 og 5 samt appendikserne.
- [SIKKERHEDSMODEL] Afsnit 4

Du finder links til den relevante dokumentation i bilagslisten bagerst i denne vejledning.

Vær opmærksom på, at vejledningen ikke gennemgår SAML i dybden, men forudsætter at læseren allerede har kendskab til SAML frameworks eller sætter sig ind i det førend implementering af Adgangsstyring for brugere påbegyndes.

3 SÅDAN FUNGERER ADGANGSSTYRING FOR BRUGERE

Adgangsstyring for brugere er en sikkerhedsmodel rettet mod brugervendte systemer – dvs. it-systemer med en brugergrænseflade. Sikkerhedsmodellen understøttes af støttesystemerne Context Handleren og Fælleskommunal Administration. Både det brugervendte system og kommunens lokale Identity Provider integrerer til Context Handler, og begge systemer er registreret i det Fælleskommunale Administrationsmodul, hvor rettighederne modelleres.



Det betyder, at det brugervendte system ikke kommunikerer direkte med kommunens lokale Identity Provider, men at Context Handleren agerer proxy for kommunen og oversætter rettighederne mellem de to systemer.

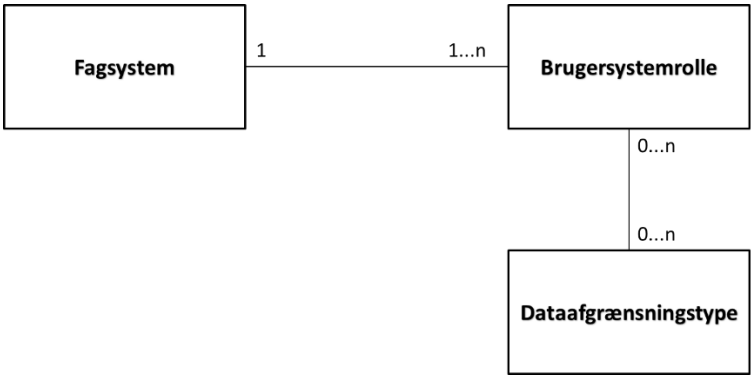
3.1 Brugersystemroller og dataafgrænsningstyper

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”.

Det vil sige, at en rettighed altid består af en rolle (hvad du må), og den kan optionelt kombineres med en eller flere afgrænsninger (hvilke data må man udføre de tilladte handlinger på).

Det er dig som leverandør af det brugervendte system, der specificerer, hvilke roller systemet understøtter, og hvilke afgrænsningstyper de enkelte roller kan kombineres med (fx kan du sige, at en given rolle kan afgrænses på KLE emneområde eller organisatorisk tilhørsforhold osv).

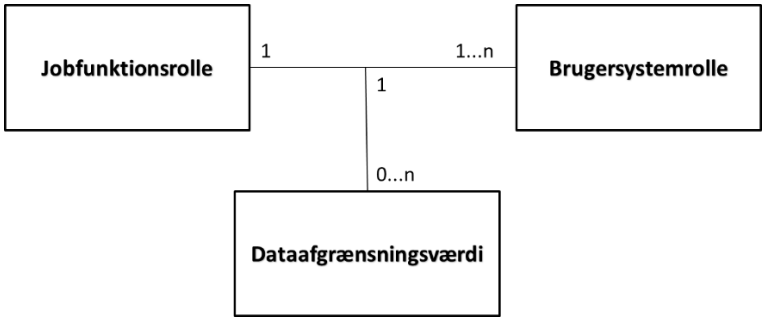
Rollerne kaldes for brugersystemroller, og afgrænsningerne kaldes for dataafgrænsningstyper. Se nedenstående illustration:



Når du har modelleret og registreret dit systems brugersystemroller, skal kommunen efterfølgende kombinere brugersystemroller (og eventuelle dataafgrænsninger) i kommunens samle-roller – også kaldet jobfunktionsroller. Denne efter-modellering af rettigheder er kommunens opgave, og den udføres lokalt i henholdsvis Fælleskommunal Administration og kommunens lokale rettighedsstyringssystem af kommunens rolleadministrator.

Som leverandører ser du aldrig jobfunktionsrollerne, men alene de brugersystemroller, som dit brugervendte it-system understøtter. Det er ikke relevant for det brugervendte system, idet jobfunktionsroller bliver vekslet til brugersystemroller og dataafgrænsningsværdier af Context Handler, inden de modtages af det brugervendte system.

Modelleringen af jobfunktionsroller er illustreret nedenfor. Bemærk at der alene er tale om en illustration af det samlede billede, og ikke at data, der er relevante for det brugervendte system.



Som det fremgår af ovenstående figur, er det på bindingen mellem en given jobfunktionsrolle og en given brugersystemrolle, kommunen skal forholde sig til de konkrete dataafgrænsninger, som er tilknyttet brugersystemrollen. Bemærk også at det er på relationen mellem brugersystemrollen og jobfunktionsrollen, at kommunen knytter egentlige dataafgrænsnings**værdier**, der matcher de dataafgrænsnings**typer**, som brugersystemrollen understøtter.

Det betyder, at du som leverandør har stor frihed til at modellere en specifik rettighedsmodel til netop din løsning. Tilgangen til modellering af rettigheder i det brugervendte system kan være på et forholdsvist højt niveau, hvor du modellerer rettigheder ud fra bruger-personaer og ender med brugersystemroller som:

Leder, Administrator, Sagsbehandler, Superbruger... osv.

Men du har også muligheden for at tilbyde kommunerne mere finkornede rettigheder og kan derfor ende med at tilbyde brugersystemroller som:

Se sager, Opret sag, Send advis, Opret Journalnotat... osv.

I begge tilfælde kan du som leverandør vælge, at rollerne skal understøtte afgrænsninger. Du kan vælge at gøre dataafgrænsningerne obligatoriske, dvs. at kommunen SKAL afgrænse rollen til et bestemt dataudsnit, eller du kan vælge at gøre dataafgrænsningerne optionelle, dvs. at kommunen KAN vælge at afgrænse rollen til et bestemt dataudsnit.

3.2 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-framework, der understøtter SAML protokollerne, og som kan generere de beskedformater, der sendes over protokollen.

Læs mere i [VILKÅR] appendix D.

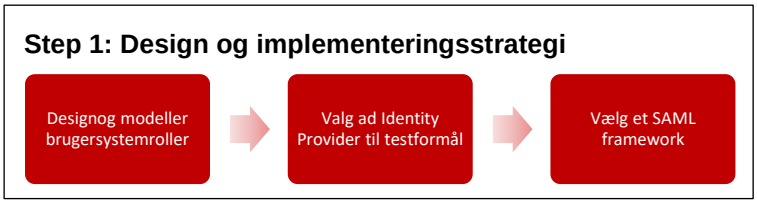
4 IMPLEMENTERING AF ADGANGSSTYRING FOR BRUGERE

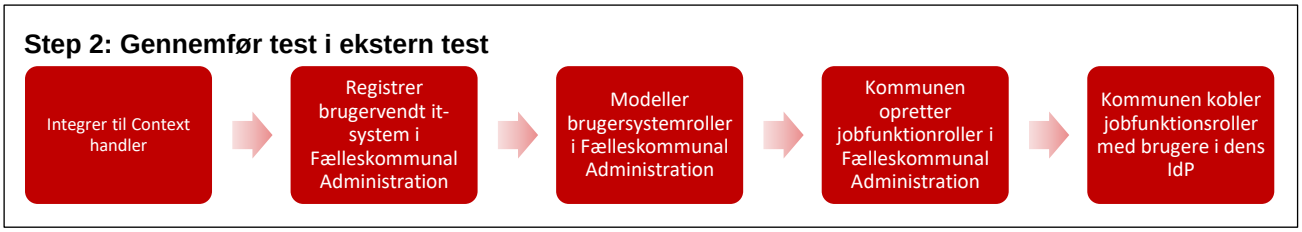
Til implementering af Adgangsstyring for brugere hører en række aktiviteter. Nogle skal udføres af leverandøren af det brugervendte system. Andre skal udføres af kommunen.

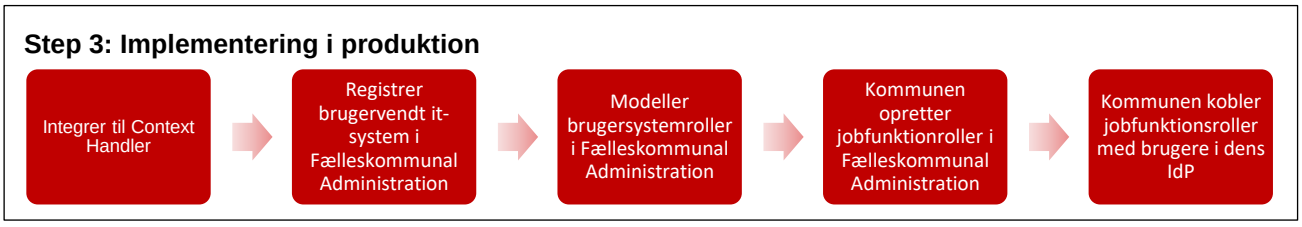
Vær opmærksom på, at aktiviteterne hos kommunen i nogle tilfælde er fordelt på flere personer i organisationen. Derfor er det vigtigt, at du sammen med relevante kolleger i kommunen tidligt fastlægger jeres fælles test- og implementeringsstrategi og beslutter, hvem der udfører de konkrete aktiviteter.

Når du skal planlægge forløbet, skal du have kontakt til kommunens STS projektleder. Hvis du er i tvivl om, hvem der har dén rolle i kommunen, kan du kontakte KOMBIT og få oplysningerne. Du kan kontakte os på KDI@kombit.dk.

I hovedtræk kan implementeringsforløbet beskrives med nedenstående hovedaktiviteter. De sidste fem skal du udføre først i det eksterne testmiljø, og dernæst gennemføres de samme fem aktiviteter igen i produktionsmiljøet:







4.1 Step 1: Design og implementeringsstrategi

Før du går i gang med implementering af Adgangsstyring for brugere, skal du træffe nogle designvalg og vælge et SAML framework. Herudover skal du vælge, hvilken Identity Provider du vil bruge til testformål.

4.1.1 Design og modellér brugersystemroller

Design og modeller de brugersystemroller, din løsning understøtter og beslut, hvilke dataafgrænsningstyper der er relevante for de enkelte roller.

Du kan hente inspiration i [ROLLEDESIGN] – dokumentet er rettet mod kommuner, som giver et godt indblik i den proces, et it-systems brugersystemroller indgår i.
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.

4.1.2 Valg af Identity Provider til testformål

Brug af kommunens Identity Provider
Du kan vælge at anvende en af dine kommunale kunders Identity Provider, da alle kommuner har etableret en Identity Provider i det eksterne testmiljø. De allerede oprettede Identity Providers i det eksterne testmiljø vil du sandsynligvis kunne bruge til testformål. Det skal du afklare direkte med den enkelte kommune, uden om KOMBIT.

Opsætning af din egen Identity Provider
Hvis du i stedet vælger at opsætte din egen Identity Provider og tilslutte den til den fælleskommunale infrastruktur, skal du gennem nedestående trin.

1. Hvis din virksomhed allerede er oprettet som virksomhed i Administrationsmodulet skal du søge for at din virksomhed også **tilføjes** som myndighed i KOMBITs testmiljø. Som myndighed kan I registrere jeres IdP i KOMBITs Fælleskommunalt Administrationsmodul og efterfølgende indgå en føderationsaftale med jer selv. Som myndighed får I også mulighed for at selv at oprette og teste jobfunktionsroller, uden at skulle involvere dine kommunale kommuners Identity Provider
    - Proceduren for at blive tilføjet som myndighed i testmiljøet finder du i afsnit 6.5 i [ADMINISTRATION]
    - For at kunne udføre de opgaver der gør jer i stand til at opsætte IdP, teste jobfunktionsroller mv., skal I have tildelt de nødvendige rettigheder til Administrationsmodulet. Rettigheder til Administrationsmodulet tildeles ikke i

Administrationsmodulet, men i Nem-Login. Det er jeres NemLog-in administrator der kan tildele de nødvendige rettigheder til jeres brugere. I kan læse mere om rettigheder til Administraitonsmodulet og processen for at tildele dem i [NEMLOG-IN]

2. Læs vejledning til opsætning af IdP [IDP] der er udarbejdet til kommuner vedrørende opsætning af en kommunal Identity Provider, da en leverandør-Identity Provider til testformål skal opfylde de samme tekniske krav.
3. Etablér en SAML Identity Provider lokalt i dit eget udviklingsmiljø. Du kan vælge blandt mange forskellige SAML Identity Providers, hvor nogle er Open Source, fx SimpleSAMLPhp, Shibboleth og lignende, eller du kan vælge den komponent, der er indbygget i Windows Server – Microsoft Active Directory Federation Services (AD FS).
4. Opret systemet som en Identity Provider i Fælleskommunalt Administration og upload SAML metadata fra din Identity Provider.
    a. Hvis du selv har oprettet en IdP som myndighed i testmiljøet, skal du i Administrationsmodulet anmode om føderationsaftale mellem din IdP og jeres virksomhed. Du/din virksomhed skal herefter godkende føderationsaftalen i Administrationsmodulet.
    b. Hvis du **ikke** er tilføjet som myndighed i testmiljøet, skal du anmode om føderationsaftale mellem din Identity Provider og den eller de test-kommuner, du ønsker at anvende. Føderationsaftalen skal efterfølgende godkendes. Du skal skrive til helpdesk@serviceplatformen.dk for at få den godkendt. Husk at medsende AftaleUUID.
5. Herefter er din test-Identity Provider tilsluttet, og du kan bruge den til at gennemføre logins i test-miljøet.

Vær opmærksom på, at der er **ydelser** forbundet med henvendelser til Helpdesk for hjælp med godkendelse af aftaler samt opsætning af jobfunktionsroller. Herudover er der SLA på Helpdesk-sager. Du kan derfor ikke uden videre forvente svar inden for få timer med mindre andet er aftalt. Du kan læse mere om priser og bestillingstid for de forskellige ydelser i KDI's ydelseskatalog [YDELSESKATALOG].

4.1.3 Vælg et SAML framework

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

Bemærk at du skal anvende et FOCES certifikat fra Nets/DanID til dette formål. I SAML anvendes certifikatet til både signering og kryptering af de beskeder, der sendes mellem aktørerne.

4.2 Step 2: Gennemfør test i eksternt testmiljø

I forbindelse med test i det eksterne testmiljø, som er stillet til rådighed af KOMBIT, skal du gennemføre nedenstående aktiviteter:

4.2.1 Etabler tillid til Context handler i ekstern test

Opsæt dit SAML Framework og indlæs SAML metadata fra Context Handler, så du etablerer tillid til Context Handler i det eksterne testmiljø. Du finder SAML metadata for Context handler i test [METADATA].

4.2.2 Opret brugervendt system i Fælleskommunal Administration i ekstern test

- Opret dit it-system som et brugervendt system i Fælleskommunal Administration i det eksterne testmiljø, se [ADMINISTRATION] for detaljer.
- Upload SAML metadatafilen for dit brugervendte system i Fælleskommunal Administration i ekstern test.
- Indtast de brugersystemroller og 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), og det er nu muligt at sende SAML beskeder mellem det brugervendte system og Context Handleren. De to systemer kan desuden validere hinandens beskeder.

I praksis er der dog en række ekstra trin, du skal gennemføre for at sikre, at forbindelsen er korrekt opsat.

4.2.3 Etablering af test-data

For at kunne teste login, skal du bruge en SAML Identity Provider. Dette kan ske ved at du:

- Opretter din egen SAML IdP
    - For at kunne gøre dette skal du være oprettet som myndighed i Fælleskommunal Administration.
    - Se Brugervejledning for administrationsmodulerne kapitel 7, http://docs.kombit.dk/loesning/adgangsstyring/betingelse
    - Alternativ du kontakte helpdesk@serviceplatformen.dk og bede dem oprette jobfunktionsroller for dig, ved at bestille ydelsen ”Hjælp til opsætning af adgangsstyring for brugere” fra KDI ydelseskatalog. Husk, at når du beder om opsætning af jobfunktionsroller

hos Heldesk, skal du specificere præcist, hvordan du vil have rollerne opsat og på hvilken kommune.

- Anvende en kommunes IdP
    - Hvis kommunen har godkendt, kan du nu få dem til at oprettet jobfunktionsroller, der indeholder dine brugersystemroller. Hvis du anvender kommunens test-Identity Provider, skal du kontakte kommunen. Det er kommunens rolleadministrator som skal foretage opsætningen.

4.2.4 Hul-igennem-test

Du er nu klar til at gennemføre hul-igennem-test, hvor du foretager et login via Context Handleren på følgende måde:

1 Du tilgår fagsystemet og vælger at starte et SAML login flow.
2 Brugeren sendes via SAML frameworket til Context Handleren.
3 Brugeren vælger, hvilken Identity Provider login skal gennemføres via (vælg her den Identity Provider, du har valgt at anvende til test-formål).
4 Brugeren ender nu på loginsiden på den valgte test-Identity Provider, hvor du gennemfører login. Husk at test-Identity Provideren udsteder jobfunktionsroller og ikke brugersystemroller.
5 Test-Identity Provideren sender brugeren tilbage til Context Handleren, der veksler jobfunktionsrollerne til brugersystemroller i henhold til den opsætning, der er lavet i Fælleskommunal Administration, og sender disse videre til det brugervendte system.
6 Det brugervendte system modtager et SAML token fra Context Handleren, som indeholder en eller flere brugersystemroller samt eventuelle dataafgrænsningsværdier knyttet til den enkelte brugersystemrolle.
7 Det brugervendte system kan nu vurdere, om den givne bruger har de fornødne rettigheder til at tilgå systemet. Bemærk at Context Handleren ikke blokerer for brugere, der ikke har nogen roller, så det brugervendte system kan modtage token, der ikke indeholder brugersystemroller og skal forholde sig til, hvordan dette skal håndteres (er der fx dele af systemet, som kan tilgås, blot man kender brugerens identitet?).

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.

4.3 Step 3: Implementering i produktion

4.3.1 Bestil FOCES certifikat til produktion

Bemærk at du skal anvende produktions-FOCES certifikat fra Nets/DanID til dette formål. I SAML anvendes certifikatet til både signering og kryptering af de beskeder, der sendes mellem aktørerne.

4.3.2 Etabler tillid til Context handler i produktion

Indlæs SAML metadata fra Context Handler i produktion i det SAML framework du har valgt, så du etablerer tillid til Context Handleren i produktionsmiljøet. Du finder SAML metadata for Context handler i produktion [METADATA].

4.3.3 Opret brugervendt system i Fælleskommunal Administration i produktion

- Opret dit it-system som et brugervendt system i Fælleskommunal Administration i produktionsmiljøet, se [ADMINISTRATION] for detaljer.
- Upload SAML metadatafilen for dit brugervendte system i Fælleskommunal Administration i produktion.
- Indtast de brugersystemroller og dataafgrænsningsværdier, som dit brugervendte system understøtter i produktion.

Når du har gennemført ovenstående trin, er der etableret teknisk forbindelse mellem dit brugervendte system og Context Handleren i produktion (via udvekslingen af SAML metadata), og det er muligt at sende SAML beskeder mellem det brugervendte system og Context Handleren. De to systemer kan nu validere hinandens beskeder i produktion.

4.3.4 Kommunen opsætter jobfunktionsroller i Fælleskommunal Administration

Tag kontakt til kommunen og bed dem opsætte jobfunktionsroller i kommunen. Det er kommunes rolleadministrator, som udfører opgaven.

Sørg for at udlevere en oversigt over de brugersystemroller du har valgt at understøtte i løsningen. Det gør det lettere for kommunen at implementere jobfunktionsrollerne.

Kommunerne har allerede erfaring med at opsætte jobfunktionsroller i forbindelse med implementering af fagsystemet BBR. Du finder et eksempel på kommunens opgavebeskrivelse [ROLLEDESIGN].

4.3.5 Kommunen tilknytter rettigheder i deres rettighedsstyringssystem

Når kommunen har opsat jobfunktionsroller i Fælleskommunal Administration, skal kommunen efterfølgende tildele rettigheder til konkrete brugere i deres rettighedsstyringssystem.

Alle kommuner har indkøbt en løsning til håndtering af rettigheder. Kommunerne har valgt forskellige løsninger til håndtere rettigheder, og derfor kan KOMBIT desværre ikke stille en generel vejledning til denne opgave til rådighed.

4.3.6 Valider opsætningen

Bed kommunen om at logge på det brugervendte system via brugergrænsefladen.

5 SÅDAN UDTRYKKER DU 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 du alene vil modtage brugersystemroller og dataafgrænsningsværdier, som du har valgt at modtage. Data som kommunen måtte sende med brugeren, og som ikke er relevant for ens løsning, vil blive fjernet af Context Handleren.

6 PRAKTISKE VÆRKTØJER

Da al kommunikation mellem fagsystemet og Context Handleren foregår gennem slutbrugerens browser[1], er det typisk lidt besværligt at inspicere de beskeder, der sendes frem og tilbage.

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)

7 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.

[1] 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.

8 APPENDIKS A – SAML OVERBLIK

Her kan du få et lidt dybere indblik i de begreber, der optræder i en SAML integration. Hvis du ønsker den fulde tekniske indsigt i SAML, bør du læse [SAML].

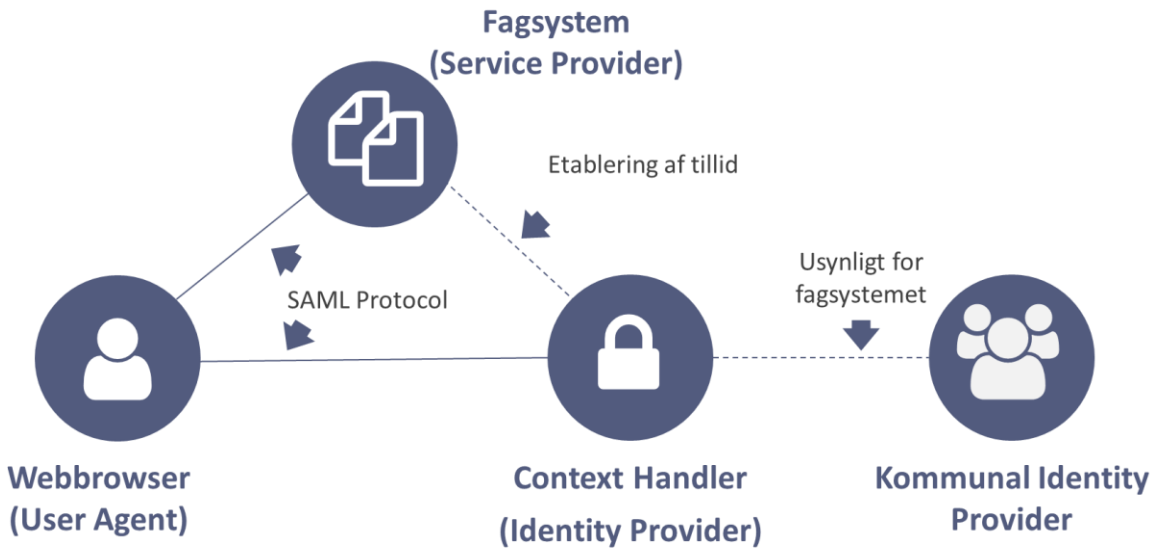
Aktører

I den fælleskommunale sikkerhedsmodel optræder der tre forskellige aktørtyper, der er beskrevet i SAML. Disse er

- User Agent
- Service Provider
- Identity Provider

En User Agent er et stykke software, der repræsenterer slutbrugeren (typisk en webbrowser). En Service Provider er selve det brugervendte system, og Identity Provideren er i KOMBIT infrastrukturen konkret implementeret via Context Handleren.

Der eksisterer flere Identity Providere i infrastrukturen. Hver kommune har tilsluttet sin egen Identity Provider, men de er ikke synlige for det brugervendte system, da de alene integrerer til Context Handleren, som agerer proxy for de kommunale Identity Providers.



Bemærk at der ikke er nogen direkte kommunikation mellem Context Handleren og det brugervendte system – det er brugerens browser, der bærer beskeder frem og tilbage mellem de to parter, enten via URL parameter i et HTTP-GET request, eller som et egentligt payload i et HTTP-POST request.

SAML beskederne

SAML specificerer en række XML-beskeder, der kan sendes mellem aktørerne. Nedenstående er relevante i forhold til den fælleskommunale sikkerhedsmodel:

AuthnRequest. Dette request er et login request, som dannes af fagsystemet og sendes til Context Handleren.

LogoutRequest. Dette er et logout request, som kan dannes af både fagsystemet og Context Handleren og sendes til den anden part. 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 Handleren for at bede den afslutte brugerens session. Det kan også være Context Handleren, der initierer logout, og her vil fagsystemet skulle modtage et LogoutRequest og foretage et logout af brugeren i fagsystemet på baggrund af dette request.

SAMLResponse. Denne besked indeholder svaret på en request og vil typisk finde anvendelse, når en bruger logger på – her vil Context Handleren svare på et AuthnRequest fra fagsystemet med et SAMLResponse, der enten indeholder en fejlbesked (brugerens login fejlede), eller et SAML token.

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.

AuthnRequest

```
<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>
```

Ovenstående request er dannet af fagsystemet, der ønsker at logge en bruger på. Requestet indeholder en reference til fagsystemet (Issuer elementet), hvor man via dennes unikke ID (også kaldet EntityID), fortæller Context Handleren, hvilket fagsystem login requestet kommer fra.

LogoutRequest

```
<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.

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 SAMLRespones 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>f3Lybq2HKN0JmXkvs9T1CQmF7LZrNOwKt74X3KY095r1FNXTyuZk4B+aw9AS73Kz5B/sG9DFn
fA9/z/AdcRmV+eKbMrA3pExx1qGiqt0b8VcfbsEXwSMUHRTiIylPvtUNJk2lT5x9Bjcd20mxvBcboX+FfwGsZ69C
dwde4r3HD4zNedis7WCLUvcfrjYSoS+vT3VJLaroeUicojNw7hOmrH+ATDODvsZtlXWlWdvshgvibX9lKJcD9we2
Oo6C4j6vTyzMLT7ZE78PIxinYfQLiqyfhV+XFM1FbsY78DCC8WIoYbRkyjuQ6rv1OjweWZ97IFRcdVoxeqM74eVm
Rs3Wg==</e:CipherValue>
                    </e:CipherData>
                </e:EncryptedKey>
            </KeyInfo>
            <xenc:CipherData>

<xenc:CipherValue>BKw+ak9fLu+pBLtTdTU4L12ICJDIB/gumsEqLwdD7Mq89DjODzvOq3NjJKe9RX0FZupR42
0g9oCFnDKkU/xmWPrL4RR/swzr3gRzQPhwwLeU2Wj7O9VBKybluCVXpC66hDecVhCDZfryU68dovlbjs5Bx+ElT1
3SEc4CdBIXg4H+3+wuzisNU… Snip flere siders base64 data</xenc:CipherValue>
            </xenc:CipherData>
        </xenc:EncryptedData>
    </EncryptedAssertion>
</Response>
```

```
<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>ixfdjL2t8tkHaujzc0wVvmMsJ+A71z/mHD1jmkyaA1ekbzccZ5j7xEAXxqK5l33rQ...
snip lots of base64 data</SignatureValue>
        <KeyInfo>
            <X509Data>
```

```
<X509Certificate>MIIGHzCCBQegAwIBAgIEUxBEhTANBgkqhkiG9w0BAQsFADBHMQswCQYDV... snip lots
of base64 data</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>PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLT... snip
base64 data</AttributeValue>
        </Attribute>
    </AttributeStatement>
</Assertion>
```

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.

9 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.

[VILKÅR]	Bilag 2 - Vilkår for anvendelse af sikkerhedsmodellen i Rammearkitekturen v.2.2
[SIKKERHEDSMODEL]	Bilag 2A - Beskrivelse af sikkerhedsmodellen i Rammearkitekturen v.2.2
[ADMINISTRATION]	Brugervejledning til Administrationsmodulerne for leverandører
[NEMLOG-IN]	Vejledning til NemLogin
[METADATA]	Metadata Ekstern Test: https://adgangsstyring.eksterntest-stoettesystemerne.dk/runtime/saml2/metadata.idp Metadata Produktion: https://adgangsstyring.stoettesystemerne.dk/runtime/saml2/metadata.idp
[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

10 TJEKLISTE

Tjeklisten er tænkt som et ekstra værktøj til at understøtte implementeringen af adgangsstyring for brugere. Tjeklisten er en generel tjekliste, og den tager ikke højde for eventuelle lokale udfordringer. Vi modtager meget gerne input til tjeklisten, så vi hele tiden kan optimere den. Skriv til KDI@kombit.dk.		
Step 1:	**Design og implementeringsstrategi**	Done
4.1.1	Design og modellér brugersystemroller	
4.1.2	Valg af Identity Provider til testformål	
4.1.3	Vælg et SAML framework	
Step 2:	**Gennemfør test i eksternt testmiljø**	
4.2.1	Etabler tillid til Context handler i ekstern test	
4.2.2	Opret brugervendt system i FK Administration i ekstern testmiljø	
4.2.3	Etablering af test-data	
4.2.4	Hul-igennem-test	
Step 3:	**Implementering i produktion**	
4.4.1	Bestil FOCES certifikat til produktion	
4.4.2	Etabler tillid til Context handler i produktion	
4.4.3	Opret brugervendt system i FK Administration i produktion	
4.4.4	kommunen skal opsætte jobfunktionroller i FK Administration	
4.4.5	Kommunen skal tilknytte rettigheder i den rettighedsstryringssystem	
4.4.6	Valider opsætning	