KOMBIT

Bilag 2

Vilkår for anvendelse af sikkerhedsmodellen i den fælleskommunale infrastruktur

1 Versionshistorik

Dokument version	Dato	Kommentarer
2.3	2024-03-18	Tilføjelse af versionshistorik Appendiks D: OIOSAML-profiler er lagt ud som selvstændige dokumenter.

2 Indledning

Nærværende dokument beskriver vilkårene for, at it-systemer kan indgå i sikkerhedsmodellen i den fælleskommunale infrastruktur, samt den daglige administration og vedligehold heraf. Vilkårene sikrer fælles spilleregler på tværs af infrastrukturen, definerer roller og ansvar, og regulerer sikkerhed samt interoperabilitet.

Vilkårene for anvendelse af sikkerhedsmodellen har overordnet/generel karakter. I konkrete udbud af it-systemer vil kravene være udmøntet i form af et bilag med detaljerede sikkerhedskrav.

Dokumentet er opdelt i en række afsnit, der afspejler de forskellige roller et it-system kan optræde i den fælleskommunale infrastruktur, nemlig ”Anvendersystem”, ”Serviceudbyder” og ”Brugervendt system”. Alle it-systemer vil ikke nødvendigvis optræde i alle roller, og det er derfor ikke nødvendigvis alle vilkår, der vil være relevante for et konkret it-system.

Dokumentet er opdelt i følgende afsnit:

- Afsnit 1: Generel introduktion til sikkerhedsmodellen
- Afsnit 2 ”Vilkår for anvendelse af Fælleskommunalt Administrationsmodul”
- Afsnit 3 ”Vilkår vedr. adgangsstyring for anvendersystemer”
- Afsnit 4 ”Vilkår vedr. adgangsstyring for serviceudbydere”
- Afsnit 5 ”Vilkår vedr. adgangsstyring for anvendersystemer med brugeradgang”
- Afsnit 6 ”Vilkår vedrørende adgangsstyring”
- Appendiks A: Begrebsmodel for Fælleskommunalt Administrationsmodul
- Appendiks B: Begrebsmodel for adgangsstyring
- Appendiks C: Navnekonvention for roller
- Appendiks D: KOMBIT Attributprofil for SAML-tokens

Afsnit 2 og **Afsnit 6** vil være relevante for alle it-systemer, der skal anvende sikkerhedsmodellen i .

Afsnit 3 beskriver krav til, hvordan anvendersystemer, der benytter services i den fælleskommunale infrastruktur, skal forholde sig til den adgangsstyring, der er implementeret af en serviceudbyder. Serviceplatformen vil eksempelvis være en sådan serviceudbyder. Disse krav er således relevante for alle systemer, der ønsker at anvende services i den fælleskommunale infrastruktur.

Afsnit 4 beskriver krav til, hvordan serviceudbydere skal håndtere adgangsstyring. Disse krav er relevante for alle systemer, der ønsker at udstille en service og ønsker at anvende den adgangsstyringsmodel, der gælder for den fælleskommunale infrastruktur.

Afsnit 5 beskriver krav til, hvordan et brugervendt system kan foretage adgangsstyring for brugere i henhold til den fælleskommunale infrastruktur føderationsmodel for adgangsstyring. Disse krav kan være relevant for alle brugervendte systemer, der tilkobles den fælleskommunale infrastruktur.

Herudover er sikkerhedsmodellen introduceret i bilag 2A.

1.1 Overblik over sikkerhedsmodellen

Sikkerhedsmodellen er en forudsætning for at benytte den fælleskommunale infrastruktur, da brugere og systemer ellers ikke vil få adgang.

Sikkerhedsmodellen handler om at styre hvilke brugere og systemer, der får adgang til it-systemer. Adgangsstyringen håndterer både, hvem der kan logge ind i et it-system og hvilken adgang, der efterfølgende gives til forskellige data og funktionalitet i it-systemet.

Infrastrukturen understøtter adgangsstyring for to forskellige scenarier:

- Når et it-system (anvendersystem) tilgår en fælleskommunal service i et andet it-system (serviceudbyder)
- Når en bruger tilgår et it-system (brugervendt system)

Disse to scenarier uddybes yderligere i det efterfølgende.

I infrastrukturens adgangsstyringsmodel kaldes et it-system, der:

- Udstiller en service for en ***serviceudbyder***
- Anvender en service for et ***anvendersystem***
- Udstiller en brugergrænseflade for et ***brugervendt system***

1.1.1 Adgangsstyring for serviceudbydere

En række it-systemer kræver myndighedsgodkendelse, før der kan opnås adgang til servicen. Myndighedens godkendelse kan eksempelvis være påkrævet, fordi servicen udleverer data, som myndigheden er dataansvarlig for, eller fordi myndigheden skal betale for anvendelse af servicen.

Adgangsstyringen i infrastrukturen understøtter sådanne services (benævnt fælleskommunale services), hvor et it-system udstiller en service, der kan anvendes i kontekst af forskellige myndigheder, men hvor adgang til servicen godkendes individuelt af hver enkelt myndighed. I adgangsstyringsmodellen kan en service benyttes til at udlevere data fra en serviceudbyder, til at indlevere data til serviceudbyderen eller til at få serviceudbyderen til at udføre en handling for anvendersystemet.

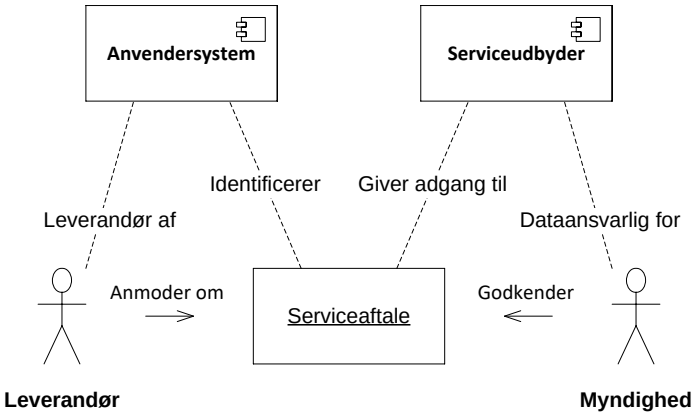
Serviceplatformen og Støttesystemerne er eksempler på serviceudbydere. Fælleskommunale fagsystemer vil ligeledes kunne optræde som serviceudbydere.

Anvendersystemer vil typisk være fagsystemer, der skal anvende en eller flere services i den fælleskommunale infrastruktur. Anvendersystemer kan også være et Støttesystem, der ønsker at anvende en service, der udstilles af et andet Støttesystem. Et givet it-system kan således optræde i flere forskellige roller samtidigt.

1.1.1.1 Serviceaftaler

Når et anvendersystem skal have adgang til en fælleskommunal service, kræves der en godkendelse fra den Myndighed, som anvenderen af it-systemet skal tilgå servicen på vegne af. Alle servicekald sker således i kontekst af en Myndighed. Denne godkendelse indhentes i form af en serviceaftale.

Indgåelse af serviceaftaler er systemunderstøttet via Fælleskommunalt Administrationsmodul. En serviceaftale indgås i praksis ved, at Leverandøren af et anvendersystem anmoder om indgåelse af serviceaftalen for en given service og Myndigheden godkender eller afviser denne anmodning.



En serviceaftale tjener som instruks til KOMBIT og serviceudbyderen om at give Anvendersystemet adgang til servicen (herunder data udstillet af denne). Herudover skal Myndigheden indgå en databehandleraftale med Anvendersystemet, hvis adgangen omfatter personoplysninger. Serviceaftalen specificerer endvidere de adgangsrettigheder (i form af systemroller med tilhørende dataafgrænsninger), som giver anvendersystemet adgang til serviceudbyderen. Derved kan serviceaftalen automatisk håndhæves, når anvendersystemet tilgår serviceudbyderen.

Det er Myndighedernes ansvar, i samarbejde med Leverandøren af anvendersystemet, løbende at ajourføre serviceaftalerne, så de hele tiden er tidssvarende, og kun giver adgang til de nødvendige data. Det er endvidere Myndighedens ansvar at sikre (gennem databehandleraftalen), at anvendervendersystemet kun henter nødvendige data for den aktuelle kontekst (fx en konkret sagsbehandling), hvilket kan være færre data end den totale adgang specificeret i serviceaftalen. Såfremt en serviceudbyder har opstillet specifikke parametre, som der i givne situationer skal tilgås med, er det Myndighedens ansvar, at anvendersystemet overholder disse parametre (via instruks).

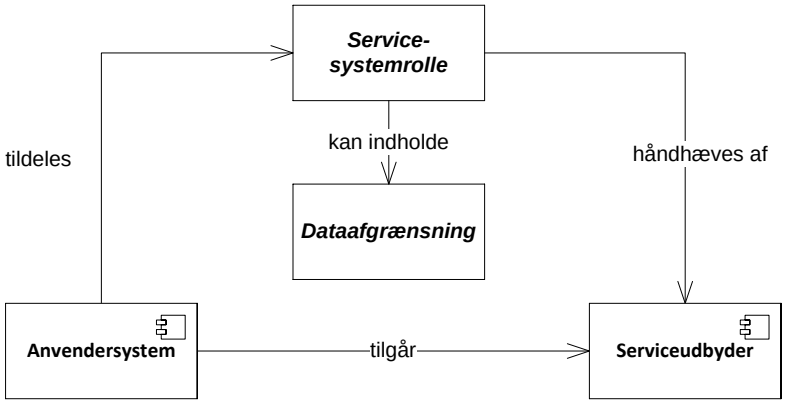
2.1.1.2 Systemroller og dataafgrænsninger

Serviceudbyderen håndhæver adgangskontrol på baggrund af et antal systemroller til Anvendersystemer gennem serviceaftaler. En systemrolle beskriver en gruppering af hvilken funktionalitet hos serviceudbyderen, som systemrollen giver adgang til.

Mange it-systemer har en indbygget rettighedsmodel, der gør det muligt at detailstyre rettighedstildelinger i forbindelse med rettighedsadministration i it-systemet. Eksempelvis kan det være muligt at tildele rettigheder for specifikke objekter og specifikke handlinger i it-systemet. En systemrolle vil ofte være en gruppering af disse detailrettigheder. Mange eksisterende it-systemer opererer allerede med begreber, der giver en sådan gruppering af detailrettigheder i systemroller.

Systemroller tildeles anvendersystemer i forbindelse med indgåelsen af en serviceaftale. Anvendersystemet får derved lov til at tilgå den funktionalitet og de data hos serviceudbyderen, som myndigheden har godkendt via serviceaftalen.

Når anvendersystemet tilgår en serviceudbyder, håndhæver denne ud fra de tildelte systemroller, at anvendersystemet kun får adgang til en begrænset mængde funktionalitet og data.



Adgangsstyringsmodellen for brugere, der beskrives i det efterfølgende, er også baseret på systemroller. Der bruges derfor betegnelsen servicesystemrolle for en systemrolle, der håndhæves af en serviceudbyder for at skelne dem fra systemroller, der bliver brugt i forbindelse med adgangsstyring for brugere (de såkaldte brugersystemroller).

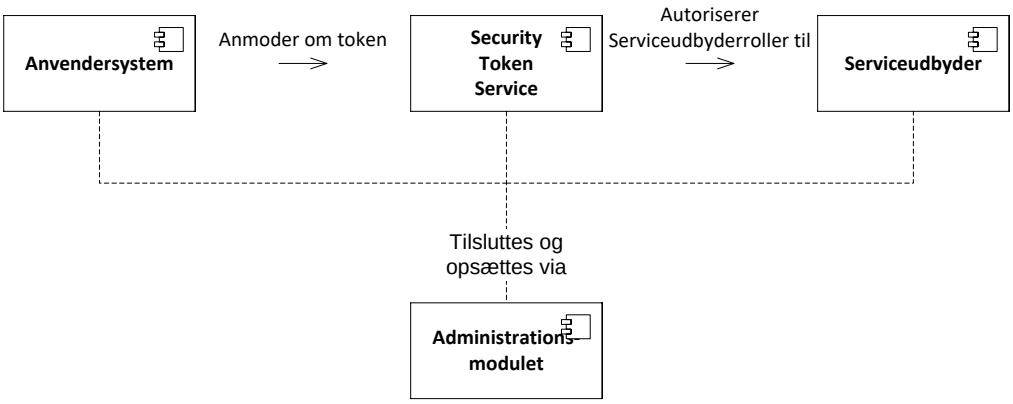
En systemrolle kan indeholde en række dataafgrænsninger, som begrænser systemrollens datamæssige virkefelt. Eksempelvis ville en systemrolle ”Hent sag” kunne indeholde en dataafgrænsning på ”sagstype” defineret som et KLE-nummer. Anvendersystemet kan så tildeles servicesystemrollen ”Hent sag”, og man kan sætte dataafgrænsningsværdien ”sagstype = 27.10.*”. Således autoriseres anvendersystemet til at hente alle sager, der har en sagstype med KLE-hovedgruppe 27 og KLE-gruppe 10.

1.1.1.3 Flow for anvendelse af en service

Når et anvendersystem tilgår en serviceudbyder, foregår adgangsstyring ved at anvendersystemet først anmoder Fælleskommunal Adgangsstyring for systemer (Security Token Service) om et security token med de servicesystemroller, som anvendersystemet er tildelt den aktuelle serviceudbyder gennem serviceaftaler.

Security Token Service har til formål at udstede security tokens, der er en signeret XML-billet, der beskriver et givet Anvendersystems adgang til en specifik service i kontekst af en specifik Myndighed. Adgangstokens er baseret på SAML-standarden og anmodninger til Security Token Service forgår ved brug af OIO WS-Trust protokollen.

Når anvendersystemet tilgår serviceudbyderen, medsendes dette token, og serviceudbyderen tillader så adgang ud fra de servicesystemroller og dataafgrænsninger, der fremgår af tokenet. For at forhindre snyd med tokens, er de alle signeret med Security Token Service digitale signatur.



Anvendersystemer og serviceudbyder tilsluttes til infrastrukturen via Fælleskommunalt Administrationsmodul. Fælleskommunalt Administrationsmodul benyttes ligeledes til at indgå serviceaftaler.

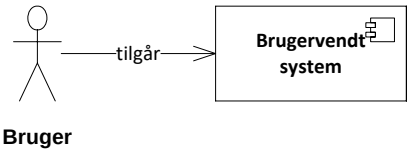
Security Token Service opdateres løbende fra Fælleskommunalt Administrationsmodul med informationer om anvendersystemer, serviceudbydere og serviceaftaler efterhånden som disse registreres. Security Token Service kan således automatisk udstede adgangstokens for de tilsluttede systemer, som direkte afspejler de indgåede serviceaftaler.

1.1.2 Adgangsstyring for brugere

It-systemer i den fælleskommunale infrastruktur skal kunne anvendes af brugere fra de forskellige myndigheder. Fælleskommunal Adgangsstyring for brugere understøtter dette ved at give brugere fra forskellige myndigheder mulighed for tilgå fælleskommunale og kommunale fagsystemer.

Fælleskommunal Adgangsstyring for brugere er baseret på en fødereret model. Dette betyder bl.a., at brugere oprettes, tildeles adgang og autentificeres lokalt hos de enkelte myndigheder. Fælleskommunal Adgangsstyring for brugere gør det muligt, at myndighedens bruger kan få adgang til de forskellige systemer, der er tilsluttet infrastrukturen, samtidig med at myndigheden administrerer de enkelte brugeres roller og rettigheder lokalt.

De systemer, som understøttes af Fælleskommunal Adgangsstyring for brugere, kaldes for brugervendte systemer:



Fælleskommunale fagsystemer er eksempler på brugervendte systemer.

It-systemer indkøbt af en eller flere kommuner til eget brug kan også bruge Fælleskommunal Adgangsstyring for brugere. Disse systemer vil så også være brugervendte systemer i infrastrukturens adgangsstyringsmodel.

1.1.2.1 Roller og dataafgrænsninger

Adgangskontrollen for brugervendte systemer håndhæves, ligesom for serviceudbydere, ud fra systemroller med tilhørende dataafgrænsninger. Disse systemroller kaldes brugersystemroller, for at skelne dem fra de systemroller, der benyttes af serviceudbydere.

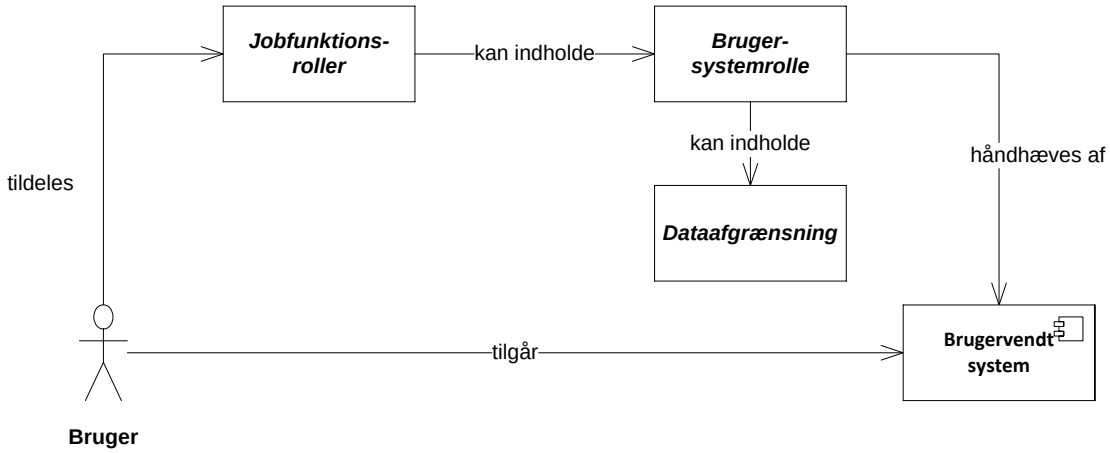
Et brugervendt system håndhæver altså brugeradgang ud fra et antal brugersystemroller med tilhørende dataafgrænsninger. Disse udarbejdes i forbindelse med designet af det brugervendte system.

For at understøtte en fødereret model for adgangsstyring, der kan anvendes af forskellige myndigheder, tillader infrastrukturens adgangsstyring, at hver enkelt myndighed kan definere deres egne jobfunktionsroller.

En jobfunktionsrolle er en samling af brugersystemroller, hvor de tilhørende dataafgrænsninger endvidere er tildelt en dataafgrænsningsværdi. Jobfunktionsroller giver således myndighederne mulighed for at samle brugersystemroller i nogle overordnede roller, og vil derved gøre den daglige administration med at tildele roller til brugere lettere for myndigheden.

Jobfunktionsroller bør udarbejdes af myndigheden, så de svarer til de jobfunktioner, den enkelte myndighed har – eller på anden måde repræsenterer de sæt af brugersystemroller, der ønskes givet samlet. En jobfunktionsrolle kunne eksempelvis svare til en jobfunktion som ”Borgerservicemedarbejder”, ”Udbetaler for kontanthjælp” eller som ”Sagsbehandler for børn og unge”.

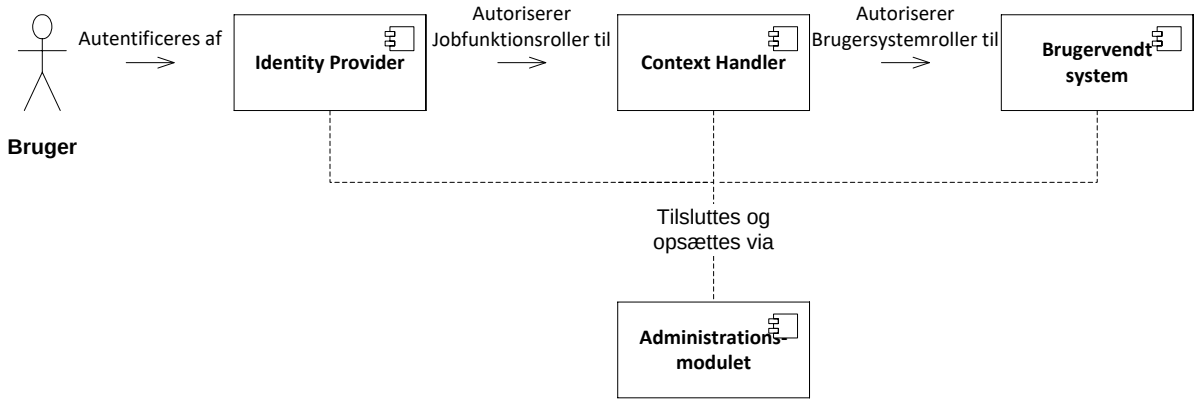
Idet jobfunktionsroller kan defineres forskelligt for hver enkelt myndighed, giver det myndighederne mulighed for at organisere deres arbejde forskelligt, selv om de anvender de samme brugervendte systemer – og uden at de brugervendte systemer skal kende myndighedernes jobfunktioner, da infrastrukturen oversætter mellem de to rollemodeller (se nedenfor).



I praksis administreres jobfunktionsroller af Myndigheden i Fælleskommunalt Administrationsmodul. Selve tildelingen af jobfunktionsroller til brugere foregår derimod lokalt hos myndigheden ved brug af dens egen brugeradministrationsløsning.

1.1.2.2 Flow for bruger log-in

Når en bruger skal logge ind på et brugervendt system, der understøttes af infrastrukturens adgangsstyring, foregår det overordnet set som beskrevet nedenfor:



Bemærk: Kommunikation mellem det brugervendte system, Context Handler, og IdP forgår med redirects via brugerens browser

Når en bruger tilgår et brugervendt system, og endnu ikke er logget ind, sender det brugervendte system brugeren videre til myndighedens egen Identity Provider (IdP). En IdP er et system, der kan autentificere brugeren, og som ved hvilke jobfunktionsroller brugeren er tildelt. I praksis vil IdP'en være et system, der er integreret med myndighedens eksisterende brugeradministrationsløsning. Man kan herunder også integrere til myndighedens eksisterende single sign-on løsning således, at brugeren ikke oplever at blive spurgt om eksempelvis brugernavn og password i forbindelse med autentifikation for det brugervendte system, hvis brugeren allerede er logget ind på andre af myndighedens systemer.

Når brugeren er autentificeret, udsteder myndighedens IdP et SAML-token, der indeholder oplysninger om brugerens identitet, hvilken myndighed brugeren kommer fra, samt hvilke jobfunktionsroller brugeren er tildelt.

SAML-tokenet fra IdP'en sendes videre til Fælleskommunal Adgangsstyring for brugere (Context Handler). Context Handleren omveksler SAML-tokenet til et andet SAML-token, der indeholder brugersystemroller for det specifikke brugervendte system, som brugeren ønsker at logge ind på.

Dette SAML-token med brugersystemroller og dataafgrænsninger videresendes til det brugervendte system, der opretter en session med brugeren. I denne session håndhæver det brugervendte system, at brugeren kun får adgang til den funktionalitet og data, som brugeren er autoriseret til i henhold til det medsendte SAML-token.

Hele det ovenstående log-in flow er rent teknisk baseret på den eksisterende OIOSAML-standard. Dog har KOMBIT udarbejdet ny attributprofiler for SAML-tokens (Appendiks D), så disse kan indeholde dataafgrænsninger. Dette er nemlig ikke understøttet i den eksisterende OIOSAML-standard.

Context Handler opdateres løbende fra Fælleskommunalt Administrationsmodul med informationer om IdP'er, brugervendte systemer og definitioner af jobfunktionsroller efterhånden som disse registreres. Context Handler kan således automatisk omveksle SAML security tokens for de tilsluttede myndigheders brugere på baggrund af de jobfunktionsroller, som myndigheden har defineret.

3 Vilkår for anvendelse af Fælleskommunalt Administrationsmodul

For at et it-system kan anvende infrastrukturen, skal leverandøren af it-systemet (Leverandøren) oprettes som ”Organisation” i Fælleskommunalt Administrationsmodul, og Leverandøren skal oprette It-systemet i Administrationsmodulet.

3.1 Krav til oprettelse som ”Organisation”

Leverandøren skal først tilslutte sin virksomhed som organisation af typen ”Leverandør” i Fælleskommunalt Administrationsmodul for at kunne tilslutte systemer til infrastrukturen og redigere aftaler og roller for disse. Leverandøren skal yderligere udpege en eller flere medarbejdere, der kan agere som administratorer i Leverandørens organisation.

Administratorerne skal varetage forskellige administrative roller på vegne af Leverandøren, herunder vedligeholde organisationens stamdata og kontaktoplysninger, anmode om serviceaftaler og foretage teknisk administration af it-systemer.

Disse administratorer skal kunne logge på Fælleskommunalt Administrationsmodul ved anvendelse af et OCES-medarbejdercertifikat.

Leverandøren skal løbende ajourføre de udpegede administratorer med eventuelle ændringer af ansvarlige personer i Leverandørens organisation.

3.2 Tilslutning af it-systemer

Leverandøren er ansvarlig for at tilslutte sine it-systemer til infrastrukturen via Fælleskommunalt Administrationsmodul. Leverandøren skal anvende brugergrænsefladen i Administrationsmodulet til dette formål.

Leverandøren er ansvarlig for at overholde de generelle vilkår, der gælder for it-systemer tilsluttet til den fælleskommunale infrastruktur.

Leverandøren skal oprette (og løbende vedligeholde) alle relevante konfigurationsoplysninger for It-systemet, eksempelvis navn, beskrivelse, SAML-metadata, OCES-certifikat til identifikation af It-systemet og systemroller. En del af dette består i at sikre, at certifikater opdateres inden udløb. Konfigurationsoplysninger vil variere afhængigt af systemtype.

3.3 Krav til certifikater på Anvendersystemer

For Anvendersystemer gælder der, at det OCES-certifikat, der registreres på Anvendersystemet, skal være et System- eller Organisations-certifikat, og at det ikke må genbruges af andre Anvendersystemer.

4 Vilkår vedrørende adgangsstyring for Anvendersystemer

Hvis it-systemet er et Anvendersystem, jævnfør afsnit 1, skal nedenstående krav opfyldes af Leverandøren.

4.1 Krav til oprettelse og vedligehold af aftaler

En serviceaftale beskriver hvilken adgang et givet Anvendersystem får til data, og funktionalitet, hos en given serviceudbyder, jævnfør afsnit 1.

Rent praktisk foregår indgåelse af en serviceaftale i Fælleskommunalt Administrationsmodul, hvor Leverandøren af et anvendersystemopretter anmodningen om indgåelse af en serviceaftale. Denne anmodning fremsendes til den eller de Myndigheder, der identificeres i anmodningen, og såfremt denne/disse godkender aftalen, vil anvendersystemet automatisk blive tildelt de forespurgte rettigheder til serviceudbyderen på de pågældende myndigheders vegne (udtrykt som servicesystemroller med tilhørende dataafgrænsninger).

Leverandøren kan i Administrationsmodulet desuden anmode om indgåelse af en serviceaftale for en Fælleskommunal service på vegne af en Myndighed, men med et ønske om at tilgå en anden Myndigheds data. Dette benævnes en serviceaftale med videregivelse af data. I dette scenarie vil begge Myndigheder skulle godkende serviceaftalen, inden anvendersystemet bliver tildelt de nødvendige rettigheder til at tilgå serviceudbyderen.

Leverandøren er ansvarlig for at anmode om nye serviceaftaler, der er nødvendige for It-systemets brug af en serviceudbyder. Leverandøren er ansvarlig for at vedligeholde indgåede aftaler ved at foretage nødvendige ændringsanmodninger til eksisterende serviceaftaler. Dette gælder ligeledes for opsigelse af serviceaftaler, som ikke længere er relevante. Leverandøren skal anvende Administrationsmodulets brugergrænseflade til det daglige vedligehold.

4.2 Krav til anvendelse af serviceudbydere

Når et Anvendersystem kalder serviceudbyderen, skal Anvendersystemet etablere en sikker forbindelse med serviceudbyderen, der sikrer gensidig autentifikation af systemerne, samt integritet og hemmeligholdelse af servicekaldet og dets data.

Etablering af den sikre forbindelse skal ske i henhold til de krav, serviceudbyderen udstikker for etablering af en sikker forbindelse.

Ved servicekald i infrastrukturen opereres med tre forskellige typer af adgangsstyring, der tilgodeser forskellige behov. Adgangstyperne giver forskellige muligheder for detaljering af de adgangsrettigheder, der kan håndhæves, når servicen kaldes, og understøttes på forskellig vis rent teknisk:

- **Simpel service:** Certifikatbaseret. Enten har anvendersystemet adgang til servicen eller også har det ikke adgang.
- **Simpel fælleskommunal service:** Certifikatbaseret. Et anvendersystem tilgår altid servicen på vegne af en given myndighed. Anvendersystemet har enten adgang til hele servicen (dataafgrænset til den specifikke myndigheds data) eller også har det ikke adgang.

- **Fælleskommunal service:** Tokenbaseret. Et anvendersystem tilgår altid servicen på vegne af en given myndighed. Endvidere begrænses anvendersystemets brug af servicen ud fra systemroller med tilhørende dataafgrænsninger, der tildeles anvendersystemet.

Kravene til anvendelse af disse typer uddybes yderligere i de følgende afsnit.

Det bemærkes, at KOMBIT generelt kræver at den tokenbaserede model "Fælleskommunal service" anvendes, da dette giver den mest detaljerede sikkerhedsmodel. Modellen er koordineret med fællesoffentlige standarder og fællesoffentlig brugerstyring, og kan således integreres med disse på en interoperabel måde. Det er muligt i særlige tilfælde at anvende andre sikkerhedsmodeller hvis det godkendes af KOMBIT.

4.2.1 Krav til anvendelse af simple services

Adgangskontrollen for simple services karakteriseres ved, at der enten er adgang til servicen eller ej. Det vil sige, at der typisk ikke granuleres yderligere i adgangskontrollen i forhold til den funktionalitet og de data, der gives adgang til – og i givet fald administreres dette uden for infrastrukturen.

Simple services anvendes typisk til system-system integration.

Leverandøren skal sikre, at It-systemet skal autentificere sig med det certifikat, der er angivet i den indgåede serviceaftale ved kald til simple services udstillet af en serviceudbyder.

Anvendersystemet skal autentificere serviceudbyderen via serviceudbyderens TLS-certifikat og i den forbindelse validere certifikatet for bl.a. udløb, spærrestatus mv.

4.2.2 Krav til anvendelse af simple fælleskommunale services

Simple fælleskommunale services karakteriseres ved, som for simple services, at der gives adgang til servicen uden yderligere granulering. Dog afgrænses servicen til én specifik myndighed ved, at der medsendes en anvenderkontekst.

Simple fælleskommunale services er typisk statslige grunddata eller andre eksterne systemer, der kan opnås adgang til gennem infrastrukturen.

Et anvendersystem vil således have adgang til servicen, hvis blot en enkelt Myndighed har godkendt anvendelsen på deres vegne. Der er dog krav om, at anvendersystemet medsender oplysninger om hvilken Myndighed, der ageres på vegne af, i de enkelte kald af hensyn til dataafgrænsning og logning.

Leverandøren skal sikre, at It-systemet autentificerer sig med det certifikat, der er angivet i den indgåede serviceaftale ved kald til simple fælleskommunale services udstillet af en serviceudbyder.

It-systemet skal autentificere serviceudbyder via serviceudbyderens TLS-certifikat og i den forbindelse validere certifikatet for bl.a. udløb, spærrestatus mv.

4.2.3 Krav til anvendelse af fælleskommunale services

Serviceaftaler for fælleskommunale services indgås altid i kontekst af en given Myndighed, og giver således Anvendersystemet adgang til data og funktionalitet på vegne af en specifik Myndighed (evt. flere). Når anvendersystemet i praksis skal tilgå en serviceudbyder, kræver det at Anvendersystemet har et gyldigt Security Token, der skal medsendes til kald af serviceudbyderen. Security Token'et udstedes til Anvendersystemet af Security Token Service og afspejler en indgået serviceaftalen.

Etablering af den sikre forbindelse baseret på flg. webserviceprofiler[1]:

- OIO IDWS SOAP Profile V1.1 (efterfølgeren til Liberty Basic SOAP Binding)
- OIO IDWS REST Profile V1.0

Disse profiler angiver, hvordan et webservicekald foretages med et security token, der sikrer integritet, fortrolighed og gensidig autentifikation af kommunikationen.

Leverandøren skal sikre, at It-systemet autentificerer sig over for Security Token Service med det certifikat, der er angivet i Administrationsmodulet. It-systemet skal medsende gyldige security tokens hentet fra Security Token Service ved kald til fælleskommunale services udstillet af en serviceudbyder.

Anvendersystemet skal autentificere serviceudbyder via serviceudbyderens TLS-certifikat og i den forbindelse validere certifikatet for bl.a. udløb, spærrestatus mv.

Bemærk, at et SAML-token må og bør caches og anvendes, så længe det er gyldigt, således at efterfølgende servicekald til samme serviceudbyder ikke behøver involvere forudgående kald til Security Token Service, for at etablere et nyt Security Token. Pt. sætter Security Token Service gyldigheden af tokens til otte timer.

4.2.3.1 Krav til integration med Security Token Service

Leverandøren skal sikre, at It-systemet benytter Security Token Service til at få udstedt SAML Security Tokens forud for kald af adgangsbegrænsede services, der udstilles af fælleskommunale serviceudbydere.

Security Token Service kaldes med en <RequestSecurityToken >-besked i henhold til OIO WS-Trust profilen af OASIS WS-Trust standarden.

Kald til Security Token Service signeres med et OCES-certifikat, der er tilknyttet Anvendersystemet og som forinden er registreret af Leverandøren i Fælleskommunalt Administrationsmodul.

Efterfølgende kald til samme adgangsbegrænsede service i samme myndighedskontekst skal anvende det tidligere udstedte SAML-token så længe det er gyldigt og indeholder den nødvendige

[1] Se dette link for detaljer: https://digitaliser.dk/resource/3457606

information. Dette medfører altså et krav om caching af SAML-tokens således, at kald til Security Token Service undgås, såfremt der tidligere er udstedt og modtaget et brugbart token.

5 Vilkår for adgangsstyring for serviceudbydere

Hvis it-systemet skal indgå som en serviceudbyder i infrastrukturen, jævnfør afsnit 1, skal nedenstående krav opfyldes af Leverandøren.

Ved servicekald i infrastrukturen opereres med tre forskellige typer af adgangsstyring, der tilgodeser forskellige behov. Adgangstyperne giver forskellige muligheder for detaljering af de adgangsrettigheder, der kan håndhæves, når servicen kaldes og understøttes på forskellig vis rent teknisk.

- **Simpel service:** Certifikatbaseret. Enten har anvendersystemet adgang til servicen eller også har det ikke adgang.
- **Simpel fælleskommunal service:** Certifikatbaseret. Et anvendersystem tilgår altid servicen på vegne af en given myndighed. Anvendersystemet har enten adgang til servicen (dataafgrænset til den specifikke myndigheds data) eller også har det ikke adgang.
- **Fælleskommunal service:** Tokenbaseret. Et anvendersystem tilgår altid servicen på vegne af en given myndighed. Desuden begrænses anvendersystemets brug af servicen ud fra systemroller med tilhørende dataafgrænsninger, der tildeles anvendersystemet.

Kravene til anvendelse af disse typer uddybes yderligere i de følgende afsnit.

Det bemærkes, at KOMBIT generelt kræver den tokenbaserede model ”Fælleskommunal service”, da dette giver den mest detaljerede sikkerhedsmodel. Modellen er koordineret med fællesoffentlige standarder og fællesoffentlig brugerstyring, og kan således integreres med disse på en interoperabel måde. Det er muligt i særlige tilfælde at anvende andre sikkerhedsmodeller hvis det godkendes af KOMBIT.

Serviceudbyderleverandøren skal sikre, at adgangsstyring for It-systemets services, skal foregå i henhold til adgangsstyring i den fælleskommunale infrastruktur, hvor It-systemet skal optræde som et system af typen ”Serviceudbyder”.

It-systemet skal således opfylde alle krav for en serviceudbyder. Herunder skal it-systemet opfylde krav til tilslutning af it-systemet via Fælleskommunalt Administrationsmodul, håndhævelse af adgang, samt beskyttelse af certifikater og nøgler, jf. servicens servicetype.

En serviceudbyder er et it-system, der udstiller en service, hvor adgangsbegrænsning sker i henhold til en serviceaftale, som er registeret i Fælleskommunalt Administrationsmodul.

Infrastrukturen pålægger ikke direkte serviceudbyderleverandører nogen forpligtigelser i forbindelse med indgåelse af serviceaftaler, idet disse aftaler indgås mellem leverandøren af et anvendersystem og de Myndigheder, som anvendersystemet har behov for at tilgå serviceudbyderen på vegne af. Til gengæld kan serviceudbyderleverandører have nogle forpligtelser i forhold til databehandleraftaler, der er indgået med Myndigheder.

Serviceudbyderen skal håndhæve adgangskontrol, når anvendersystemet tilgår serviceudbyderen. Håndhævelsen af adgangskontrol sker ud fra den type service, der udbydes.

5.1 Krav til udstilling af services

Serviceudbyderleverandøren er ansvarlig for at registrere servicen i Fælleskommunalt Administrationsmodul og løbende vedligeholde denne registrering.

It-systemets services skal udstille funktionalitet og data via en sikker forbindelse, der sikrer gensidig autentifikation af systemerne, samt integritet og hemmeligholdelse af servicekaldet og dets data.

Ved udstilling af services med personhenførbare data, skal gældende love og regler på databeskyttelsesområdet overholdes, herunder krav til stærk kryptering, logning og kontrol med afviste adgangsforsøg. Serviceudbyder skal sikre, at anvendersystemet anvender det certifikat, der er registreret i Fælleskommunalt Administrationsmodul.

5.1.1 Krav til udstilling af simple services

Adgangskontrollen for simple services karakteriseres ved, at der enten er adgang til servicen eller ej. Det vil sige, at der ikke granuleres yderligere i adgangskontrollen i forhold den funktionalitet og de data, der gives adgang til. I givet fald administreres det uden om infrastrukturen, men denne tilgang kan generelt ikke anbefales.

Simple services vil typisk være system-systemintegration for legacy-systemer. Det er således ikke intentionen, at denne type services udbydes bredt og i større stil.

Leverandøren skal sikre, at It-systemet håndhæver adgangskontrol ved alle kald til It-systemets services. Adgangskontrollen skal håndhæves ud fra de aftaler, der er indgået i Fælleskommunalt Administrationsmodul. It-systemet skal autentificere anvendersystemet ud fra det certifikat, der er registreret i Administrationsmodulet.

It-systemet skal desuden sikre, at anvendersystemet kun får adgang til funktionalitet og data i It-systemet, hvis der foreligger en gældende serviceaftale.

5.1.2 Krav til udstilling af simple fælleskommunale services

Det anbefales, at denne type services alene udstilles af Serviceplatformen, hvorimod andre serviceudbydere anvender den token-baserede type ”fælleskommunal service”.

Simple fælleskommunale services karakteriseres ved, som for simple services, at der enten gives adgang til servicen eller ej. Dog afgrænses servicen til én specifik myndighed ved, at der medsendes en myndighedskontekst i form af et CVR-nummer.

Simple fælleskommunale services er typisk statslige grunddata eller andre eksterne systemer, der kan opnås adgang til gennem infrastrukturen. Det er dog ikke nødvendigvis altid tilfældet og kommunale data kan i visse sammenhæng også være udstillet som simple fælleskommunale services.

Et anvendersystem vil således have adgang til hele servicens funktionalitet, hvis blot en enkelt Myndighed har godkendt anvendelsen på deres vegne. Der er dog krav om, at anvendersystemet medsender oplysninger om hvilken Myndighed, der ageres på vegne af i de enkelte kald, af hensyn til logning og evt. dataafgrænsning på myndighedsniveau.

Leverandøren skal sikre, at It-systemet håndhæver adgangskontrol ved alle kald til It-systemets services. Adgangskontrollen skal håndhæves ud fra de aftaler, der er indgået i Fælleskommunalt Administrationsmodul. It-systemet skal autentificere anvendersystemet ud fra det certifikat, der er registreret i Administrationsmodulet.

Leverandøren skal sikre, at anvendersystemet kun får adgang til funktionalitet og data i It-systemet, hvis der foreligger en gyldig serviceaftale.

5.1.3 Krav til udstilling af fælleskommunale services

Udstilling af en fælleskommunal service kræver oprettelse og vedligehold af en række systemroller med tilhørende dataafgrænsninger. Disse defineres af serviceudbyderleverandøren i forbindelse med udvikling af it-systemet, og der er således mulighed for at definere disse systemroller og dataafgrænsninger, så de passer til den adgangsstyringsmodel, der allerede måtte findes i it-systemet. Systemroller med tilhørende dataafgrænsninger for serviceudbyderen oprettes og vedligeholdes af serviceudbyderleverandøren via Fælleskommunalt Administrationsmodul, så de kan tildeles til anvendersystemer, når der indgås en serviceaftale.

Serviceudbyderen skal håndhæve adgangskontrol på baggrund af Security Tokens, der udstedes af Security Token Service. Disse Security Tokens medsendes i servicekald til serviceudbyderen, og indeholder attributter, der beskriver hvilke systemroller et anvendersystem er tildelt.

Systemroller og dataafgrænsninger skal være kompatible med infrastrukturens begrebsmodellen for adgangsstyring som beskrevet i appendiks B. Systemroller og dataafgrænsninger skal defineres, så de er tilstrækkeligt finkornede til at imødegå de forretningsmæssige behov der er, for at kunne skelne mellem forskellige former for adgang til It-systemet. Systemroller og dataafgrænsninger skal repræsenteres eksternt som en unik URI med et systemspecifikt præfiks. KOMBIT har defineret en navnekonvention for roller, som skal overholdes. Denne er beskrevet i Appendiks C.

Leverandøren er ansvarlig for at registrere systemroller med tilhørende dataafgrænsninger i Fælleskommunalt Administrationsmodul og løbende vedligeholde disse. Desuden skal Leverandøren i Administrationsmodulet angive, om servicen understøtter videregivelse af data mellem myndigheder.

Bemærk, at registrering af systemroller og tilhørende dataafgrænsninger, foregår i Fælleskommunalt Administrationsmodul i forbindelse med, at it-systemet tilsluttes.

5.1.3.1 Krav til håndhævelse af adgangskontrol

Udstilling af token-baserede services baseres på flg. webserviceprofiler[2] og skal håndhæve alle valideringskrav i disse:

- OIO IDWS SOAP Profile V1.1 (efterfølgeren til Liberty Basic SOAP Binding)
- OIO IDWS REST Profile V1.0

Disse profiler angiver, hvordan et webservicekald foretages med et security token, der sikrer integritet, fortrolighed og gensidig autentifikation af kommunikationen.

Leverandøren skal sikre, at It-systemet håndhæver adgangskontrol ved alle kald til It-systemets services. Adgangskontrollen skal håndhæves ud fra de attributter, der findes i det security token (også kaldet for servicesystemtoken), der medsendes til servicekaldet.

Et security token er en SAML Assertion (en signeret XML-billet), der blandt andet indeholder attributter, der beskriver anvendersystemets tildelte systemroller og tilhørende dataafgrænsninger. Systemroller er altid tildelt i en given anvenderkontekst (CVR-nummer).

Leverandøren skal i håndhævelsen sikre, at anvendersystemet kun får adgang til funktionalitet og data i It-systemet, der svarer til de systemroller med tilhørende dataafgrænsninger, som tokenet indeholder.

Som en del af adgangskontrollen skal It-systemet validere, at SAML-tokenet er gyldigt, herunder at det er signeret af Security Token Service. Er tokenet ikke gyldigt, skal adgang til It-systemet nægtes.

Adgangskontrollen skal sikre, at der er adgangsbegrænsning mellem Myndighedernes data ved at respektere de anvenderkontekster (CVR-numre), der fremgår af det modtagne servicesystemtoken. Hvis Leverandøren i Fælleskommunalt Administrationsmodul har angivet, at en service understøtter videregivelse af data mellem Myndigheder, skal dette korrekt håndhæves ud fra de modtagne security tokens. Her vil tokenets anvenderkontekst angive den modtagende myndigheds CVR-nummer, mens CVR-scope på roller vil angive den afgivende Myndighed.

[2] Se dette link for detaljer: OIO Identity Based Web Services 1.2 (OIO IDWS) (digst.dk)

6 Vilkår for adgangsstyring for et brugervendt system

Hvis it-systemet skal udstille en brugergrænseflade i henhold til infrastrukturens føderationsmodel for adgangsstyring, skal nedenstående krav opfyldes af Leverandøren.

Håndhævelsen af brugerrettigheder sker ud fra en række brugersystemroller og tilhørende dataafgrænsninger. Disse defineres af Leverandøren af det brugervendte system i forbindelse med udvikling af it-systemet, og der er således mulighed for at definere disse brugersystemroller og dataafgrænsninger, så de passer til den adgangsstyringsmodel, der allerede måtte findes i it-systemet. Brugersystemroller med tilhørende dataafgrænsninger for et brugervendt system oprettes og vedligeholdes af Leverandøren af It-systemet via Fælleskommunalt Administrationsmodul. Her kan Myndigheder anvende disse brugerbrugersystemroller i forbindelse med administration af adgangsstyring for Myndighedens brugere.

Brugeradgang håndteres efter en føderationsmodel. For et brugervendt system betyder det, at det ikke behøver at kende de enkelte brugere, og det brugervendte system bør ikke kræve forudgående brugeroprettelse, før der kan opnås adgang. It-systemet skal i forbindelse med bruger-login henvise brugeren til Context Handler, der sørger for, at bruger-login håndteres af brugerens egen organisation. It-systemet skal efterfølgende håndhæve adgang på baggrund af adgangstokens, der udstedes af Context Handler.

6.1 Krav til Brugertokens

I dette afsnit beskrives brugertokens – dvs. tokens udstedt til en bruger, der er en medarbejder hos en Myndighed. Der findes to varianter af brugertokens:

- Brugertokens udstedt af en Myndigheds Identity Provider eller Attributservice, som indeholder brugerens jobfunktionsroller. Disse ses kun af infrastrukturen er derfor ikke relevante for brugervendte systemer.
- Brugersystemtokens udstedt af Context Handler, som indeholder de brugersystemroller, brugeren er tildelt til et specifikt it-system. Systemrollerne fremkommer ved at oversætte de jobfunktionsroller, som brugeren er tildelt hos en Myndighed til de tilknyttede systemroller for det brugervendte system, der anmoder om tokenet. Oversættelsen mellem jobfunktionsroller og systemroller defineres af den enkelte Myndighed ved brug af Fælleskommunalt Administrationsmodul i den fælleskommunale infrastruktur. På den måde behøver et brugervendt system ikke kunne forstå andet end dets egne brugersystemroller, idet infrastrukturen står for omvekslingen.

Alle systemer i den fælleskommunale infrastruktur, som udsteder eller anvender brugertokens, skal overholde OIOSAML-profilen [OIOSAML] af den internationale SAML 2.0-standard. Dette gælder således både regler ved udstedelse samt validering af tokens. Dertil har KOMBIT defineret en række specialiseringer (underprofilering) til brug i fælleskommunal kontekst, som er beskrevet nedenfor.

Bemærk, at kravet ikke gælder eksterne Identity Providere som fx NemLog-in, hvor Context Handler vil foretage en veksling til KOMBITs format defineret i denne profil.

Subject-elementet i SAML Assertions vil entydigt identificere medarbejderen i kontekst af en Myndighed.

Subject-elementet vil indeholde et <NameID> element, der indkodes som et X.509 Distinguished Name med flg. elementer:

- Country (C) elementet indeholder ISO-landekoden.
- Organization (O) elementet indeholder CVR-nummeret på den Myndighedskontekst, som tokenet er udstedt under.
- Common Name (CN) elementet indeholder medarbejderes navn. Dette vil ikke nødvendigvis være unikt i sig selv.
- Serial-elementet indeholder et ID (tekststreng), der entydigt identificerer medarbejderen indenfor Myndigheden. Dette ID er på UUID-format, og vil være det unikke ID, der også udpeger medarbejderen i Støttesystemerne, herunder Fælleskommunalt Organisationssystem.

Formatattributten på <NameID> elementet vil være sat til `urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName`.

Elementerne i Subject DN vil være separeret med komma, og vil ikke være white space mellem elementer.

Eksempel

```
C=DK,O=19435075,CN=Hans Hansen,Serial=74c08b2b-212b-4f6d-9ce6-0fba1651087d
```

6.2 Krav til oprettelse og vedligehold af brugersystemroller

Leverandøren skal sikre, at It-systemet understøtter adgangskontrol ud fra en række brugersystemroller med tilhørende dataafgrænsninger. Leverandøren er ansvarlig for at definere en række brugersystemroller og tilhørende dataafgrænsninger til It-systemet.

Brugersystemroller og dataafgrænsninger skal være kompatible medinfrastrukturens begrebs-model for adgangsstyring, som beskrevet i appendiks B.

Brugersystemroller og dataafgrænsninger skal defineres, så de er tilstrækkeligt finkornede til at imødegå de forretningsmæssige behov, for at kunne skelne mellem forskellige former for adgang til It-systemet.

Brugersystemroller og dataafgrænsninger skal repræsenteres eksternt som en unik URI med et systemspecifikt præfiks. KOMBIT har defineret navnekonvention for disse (se Appendiks C).

Leverandøren af It-systemet er ansvarlig for at registrere og løbende vedligeholde brugersystemroller med tilhørende dataafgrænsninger i Fælleskommunalt Administrationsmodul. Herunder skal Leverandøren vedligeholde anvenderkontekster på brugersystemroller, så en given brugerbrugersystemrolle kun er tilgængelig for relevante Myndigheder, jf. begrebsmodellen i appendiks A.

6.3 Krav til bruger-login, bruger-logout og brugersessionsstyring

Log-in af brugere til It-systemets web-baserede grænseflader skal håndteres via Context Handler (SAML Identity Provider) ved brug af OIOSAML-protokollen. It-systemet skal overholde OIOSAML-profilen suppleret med KOMBITs attributprofiler beskrevet i Appendiks D. Bemærk, at infrastrukturen understøtter både OIOSAML 2 og OIOSAML 3. KOMBITs Attributprofiler for OIOSAML 2 og OIOSAML 3 findes her Adgangsstyring for brugere | Digitaliseringskataloget

It-systemet skal i sin SAML-implementering håndtere SAML AuthnRequest- og SingleLogout-protokollerne. It-systemet skal både kunne være initierende og ikke-initierende i forhold til SAML SingleLogout.

Efter log-in af brugeren, udtrækkes informationer fra SAML-token (modtaget fra Context Handler) indeholdende bl.a. de brugersystemroller, der er tildelt den aktuelle bruger af It-systemet.

Bemærk, at der ingen garanti er for at brugeren er tildelt brugersystemroller, og man derfor kan modtage SAML-tokens, der ikke indeholder brugersystemroller. Hvis fagsystemet ikke tillader, at brugere får adgang uden roller, skal Leverandøren håndtere dette scenarie ved at opsætte en fejlside til slutbrugeren, der informerer brugeren om den manglende adgang.

På baggrund af indholdet af det modtagne SAML-token, oprettes en lokal session med brugeren, og der kan evt. ”just-in-time” oprettes en lokal brugerkonto, hvis It-systemet har behov herfor. Der sker således ingen oprettelser af brugere (provisionering) forud for log-in.

Leverandøren skal sikre, at It-systemet selv håndterer sessionsstyring med brugerens browser, og herunder implementere timeout af brugersessioner ved inaktivitet i en vis periode. Det skal være muligt at konfigurere alle timeout-perioder

It-systemet skal på brugergrænseflader implementere en visuel komponent til ”Logout” (via en knap eller et link), som giver brugeren mulighed for at logge af It-systemet, samt øvrige systemer, der har en session med Context Handler.

Endvidere skal It-systemet udstille en SOAP-baseret logout-mekanisme (SAML endpoint), som kan kaldes fra Context Handler for tvungen logout af en bruger.

6.4 Krav til håndhævelse af adgangskontrol

Leverandøren skal sikre, at It-systemet håndhæver adgangskontrol over for brugere til data og ressourcer, som It-systemet udstiller via brugergrænsefladen.

Adgangskontrollen skal håndhæves ud fra de attributter, der findes i det SAML-token, der modtages ved oprettelse af brugerens session. Attributterne indeholder blandt andet oplysninger om brugerens kontekst (CVR-nummer) og tildelte brugersystemroller med tilhørende dataafgrænsninger.

Leverandøren skal ligeledes sikre, at It-systemet håndhæver, at brugeren kun får adgang til funktionalitet og data i It-systemet, der svarer til brugersystemroller med tilhørende dataafgrænsninger, som tokenet indeholder. Som en del af adgangskontrollen skal It-systemet validere, at SAML-tokenet er gyldigt, herunder at det er udstedt af Context Handler.

Er tokenet ikke gyldigt, skal adgang til It-systemet nægtes.

Det er Context Handler, der bestemmer gyldigheden af token. For assertions udstedt af Context Handler gives der et vindue på fem minutter, hvor assertion kan modtages og må behandles af It-systemet.

Adgangskontrollen skal sikre, at der er adgangsbegrænsning mellem Myndighedernes data, ved at respektere den anvenderkontekst (CVR-nummer), der fremgår af det modtagne SAML-token.

It-systemet skal understøtte infrastrukturens model for delegering af roller fra én organisation til en anden. Det betyder, at modtagne SAML-tokens kan indikere, at brugeren har modtaget en brugersystemrolle på vegne af en anden organisation, end brugeren kommer fra. Mere specifikt vil brugersystemrollen have en scope attribut, som indikerer et andet CVR-nummer.

I dette tilfælde skal It-systemet give brugeren den adgang, som defineres i brugersystemrollen på vegne af den delegerende organisation.

7 Vilkår vedrørende adgangsstyring

7.1 Sikring af systemer, der foretager adgangsstyring

Infrastrukturens adgangsstyringsmodel er baseret på anvendelse af OIO SAML, OIO WS-Trust og OCES-certifikater. Alle anvendersystemer, serviceudbydere og brugervendte systemer, der optræder som SAML end-point, skal overholde nedenstående krav til sikring. Leverandøren skal sikre dette.

Tokens skal udveksles over transportmekanismer, der sikrer fortrolighed ved brug af stærk kryptering. Det henvises til Datatilsynets definition af stærk kryptering. Anvendersystemer kan anmode om et token af Security Token Service via https.

Signaturer, certifikater og security tokens skal sikkerhedsvalideres af It-systemet før brug. Der må kun accepteres SAML-tokens, som er digitalt underskrevet med Context Handlers eller Security Token Servicens certifikat. Certifikater skal generelt spærretjekkes.

Leverandøren skal definere hvilket sikringsniveau for brugeridentitet der er behov for, for at tilgå It-systemet. Infrastrukturen understøtter brug af NIST sikringsniveauer (1-4) og National Standard for Identiteters Sikringsniveauer (NSIS) (Lav, Betydelig og Høj).

Ved modtagelse af et security token skal Leverandøren sikre, at It-systemet validerer, at tokenet er udstedt på mindst samme sikringsniveau, som kræves for at opnå adgang. Eksempelvis må et token med sikringsniveau Lav ikke anvendes til at tilgå et system, der kræver niveau Betydelig. Hvis It-systemet giver adgang til følsomme personoplysninger via internettet, bør det krævede niveau sættes til mindst Betydelig.

Leverandøren er ansvarlig for at beskytte private nøgler mod uautoriseret adgang – herunder de private nøgler til de OCES-funktionscertifikater, som anvendes mod Context Handler og Security Token Service.

It-systemet skal beskytte de lokale trust stores (fx. lokale kopier af metadata og certifikater fra Context Handler og Security Token Service) mod uautoriseret adgang.

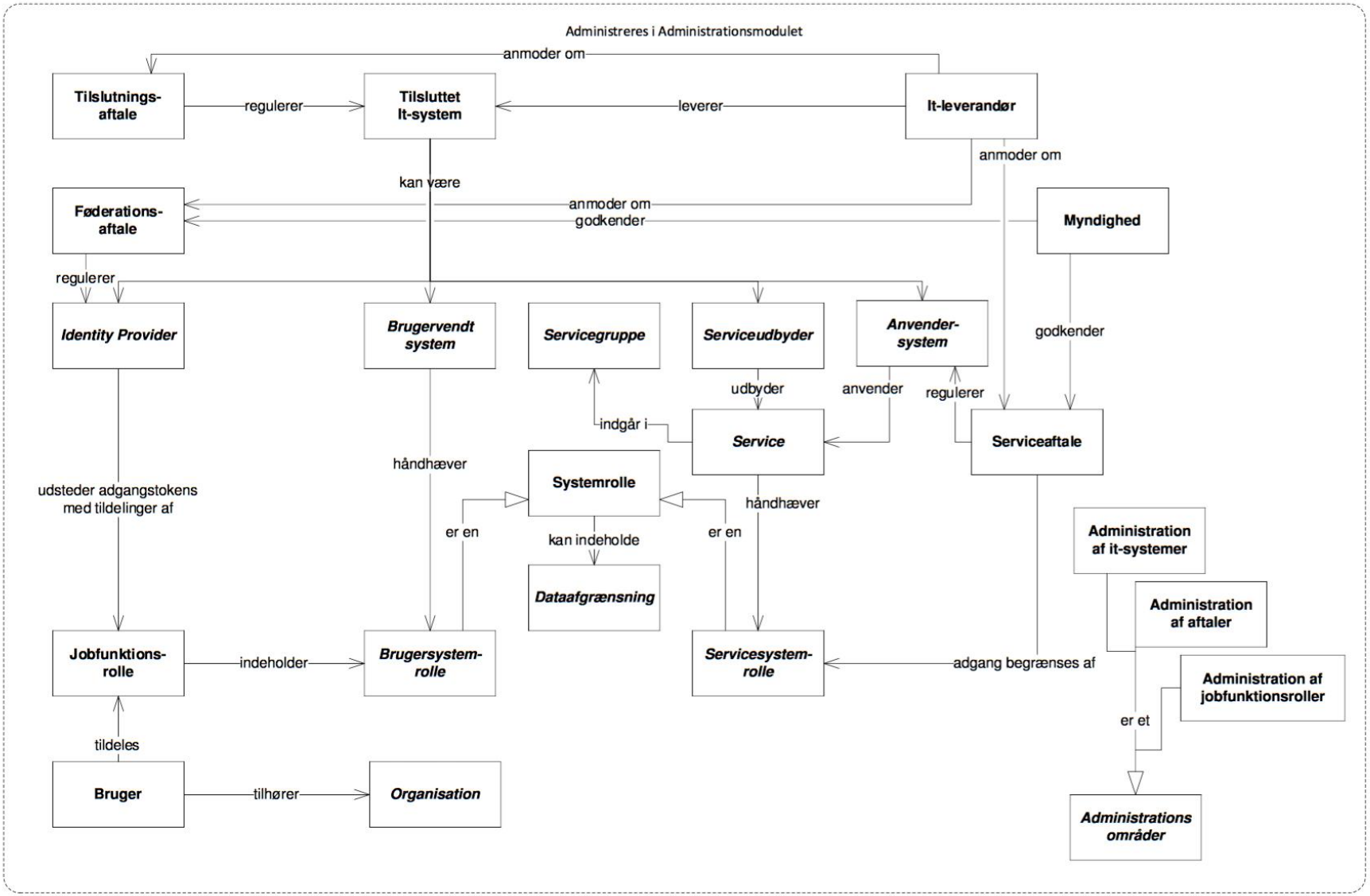
Det er Leverandørens ansvar, at trust stores beskyttes tilstrækkeligt.

Appendiks A: Begrebsmodel for Fælleskommunalt Administrationsmodul

A.1 Begrebsmodel

De centrale begreber for Fælleskommunalt Administrationsmodul er aftaler og roller. Disse styrer hvilke systemer der er tilsluttet, og hvilke rettigheder de enkelte systemer har.

Nedenfor er vist begrebsmodellen med de centrale begreber for Administrationsmodulet. KOMBIT forstår centrale begreber som forretningsbegreber, der er elementære i al kommunikation inden for opsætning og distribution af rettigheder mellem systemer.



Figur 1 Begrebsmodel for Fælleskommunalt Administrationsmodul med relationer mellem begreber

Begrebsmodellen i Figur 1 viser de centrale begreber og illustrerer deres indbyrdes relation. Diagrammet anvender notationen fra UML-klassediagrammer.

Begrebsmodellen kan læses som følger:

- En It-leverandør kan tilslutte et eller flere it-systemer som kan være:
    a. En Identity Provider, der udsteder adgangstokens for brugere bestående af Jobfunktionsroller, for de Myndigheder, der har indgået en føderationsaftale herom.
    b. Et Brugervendt system, der håndhæver adgang i henhold til Brugersystemroller.
    c. En Serviceudbyder, der håndhæver adgang i henhold til Servicesystemroller
    d. Et Anvendersystem, der anvender en Serviceudbyder i henhold til serviceaftaler, der godkendes af den dataansvarlige Myndighed.

En It-leverandør kan tilslutte systemer, og kan anmode om serviceaftaler på disse. Serviceaftaler godkendes af dataansvarlig Myndighed. I nogle tilfælde kan Forvalter godkende på vegne af en Myndighed, såfremt Myndigheden har givet Forvalter instruks til dette.

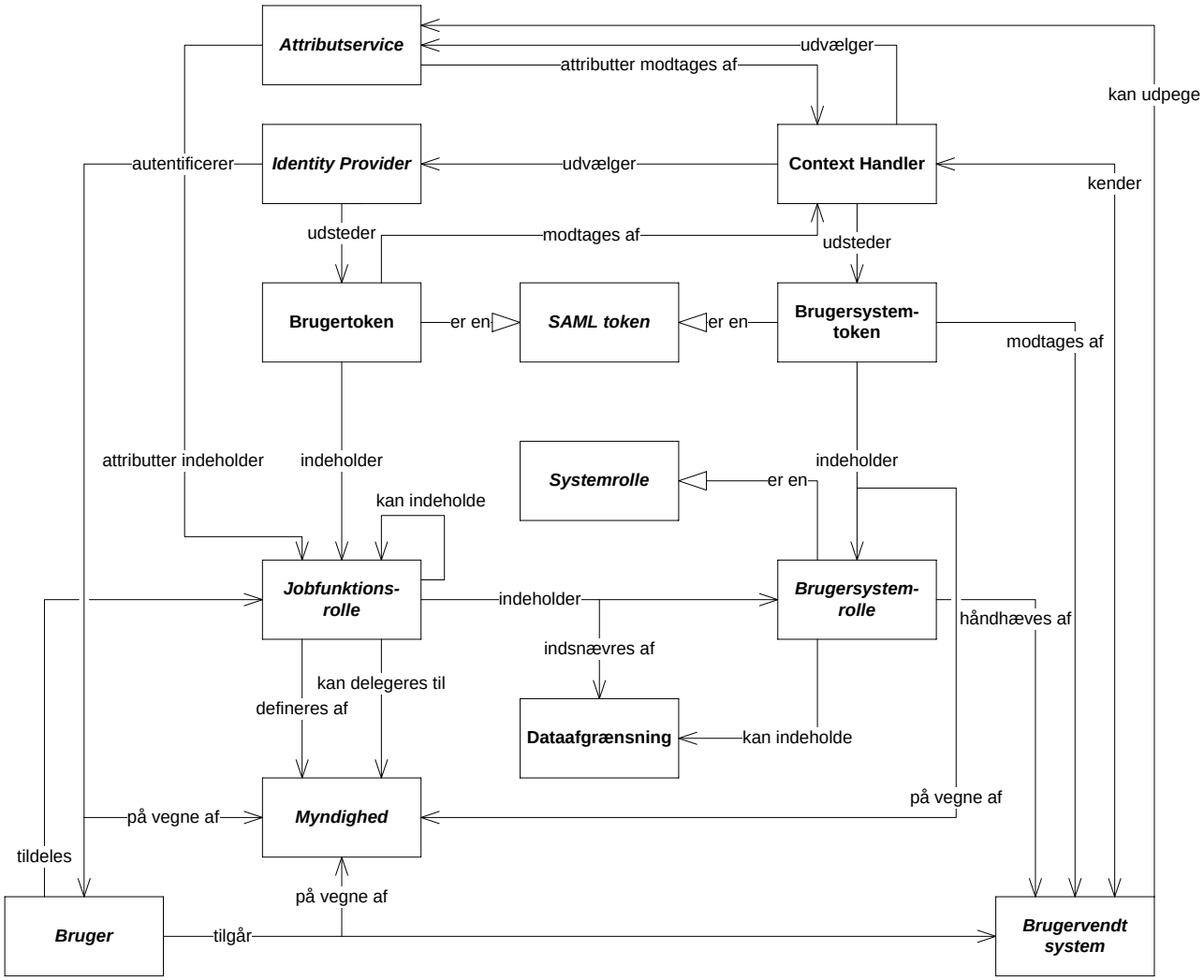
Bemærk: Tilslutningsaftalen er blot en accept af vilkår for at tilslutte et system til den fælleskommunale infrastruktur.

Appendiks B: Begrebsmodeller for adgangsstyring

B.1 Begrebsmodel for brugeradgang

Nedenfor er vist begrebsmodellen med de centrale forretningsbegreber og systemmæssige begreber for brugeradgang. KOMBIT forstår centrale forretningsbegreber som begreber, der er elementære i al kommunikation inden for Adgangsstyring for brugere og Brugervendte systemer.

Begrebsmodellen for adgangsstyring for de Brugervendte systemer er vist herunder:



Figur 2 Begrebsmodel for adgangsstyring for Brugervendte systemer

Begrebsmodellen for adgangsstyring for Brugervendte systemer skal læses således:

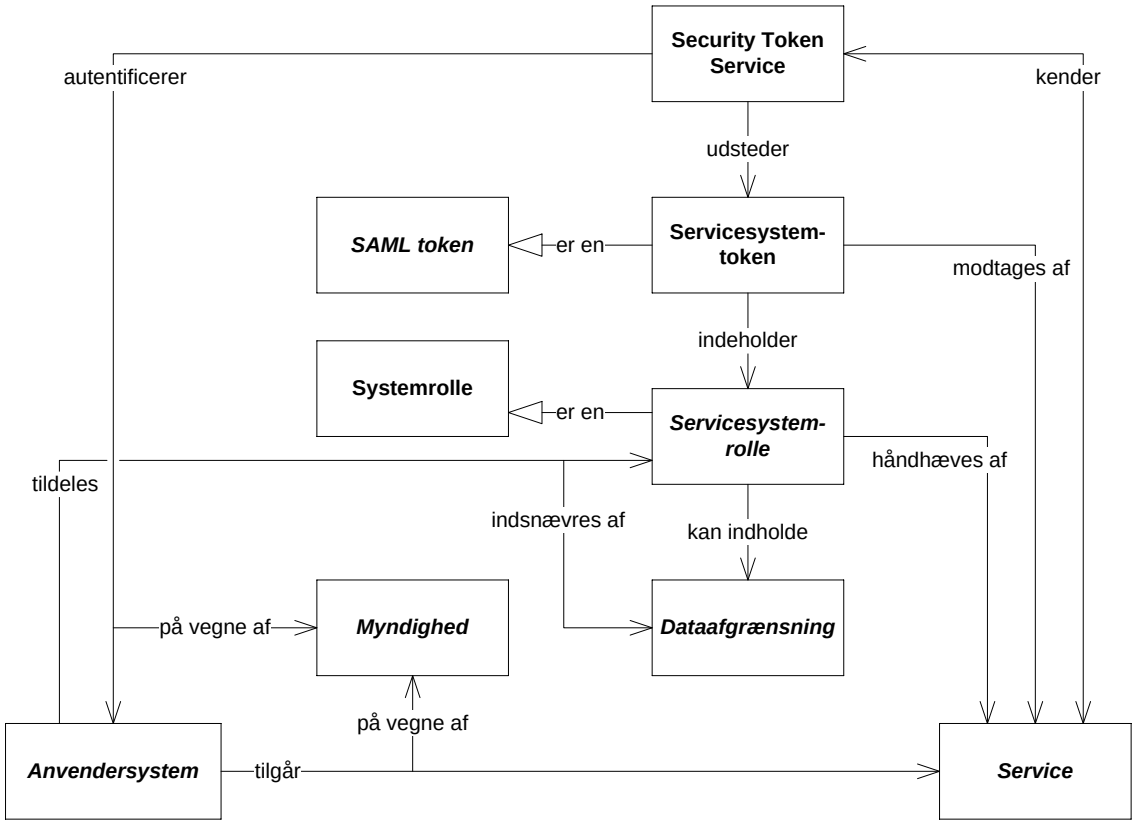
- En bruger tilgår et Brugervendt system på vegne af en Myndighed.
- Brugeren er forinden tildelt Jobfunktionsroller, der autoriserer brugeren. Jobfunktionsroller indeholder en række Brugersystemroller, som håndhæves af et specifikt Brugervendt system.

- Adgangsstyringen foregår i praksis ud fra en fødereret model, hvor brugeren autentificeres af en Identity Provider, der udsteder brugertokens indeholdende Jobfunktionsroller. Alternativt kan Jobfunktionsroller hentes fra en Attributservice.
- Brugertokens omveksles af Context Handler til brugersystemtokens, der indeholder Brugersystemroller.
- Det Brugervendte system modtager brugersystemtokens og håndhæver adgang ud fra de Brugersystemroller tokenet indeholder.

B.3 Begrebsmodel for systemadgang

I Figur 5 er begrebsmodellen for adgangsstyring med fælleskommunale services vist med de centrale forretnings- og systemmæssige begreber for Security Token Service. KOMBIT forstår centrale forretningsbegreber som begreber, der er elementære i al kommunikation inden for adgangsstyring for fælleskommunale services.

Begrebsmodellen for adgangsstyring for fælleskommunale services er vist herunder:



Figur 3 Begrebsmodel for adgangsstyring for fælleskommunale services.

Begrebsmodellen for adgangsstyring for fælleskommunale service skal læses således:

- Et Anvendersystem tilgår en service på vegne af en Myndighed. Serviceudbyderen er det it-system, der udstiller en fælleskommunal service.
- Anvendersystemet er forinden tildelt Servicesystemroller, der autoriserer Anvendersystemet. Servicesystemroller håndhæves af den specifikke service.
- Adgangsstyringen foregår i praksis ud fra en fødereret model, hvor Anvendersystemet autentificeres af en Security Token Service, der udsteder servicesystemtokens indeholdende Servicesystemroller.

Servicen modtager servicesystemtokens og håndhæver adgang ud fra de Servicesystemroller tokenet indeholder.

Appendiks C: Navnekonvention for roller

I henhold til OIO Basic Privilege Profile skal rollenavne indkodes som en URI, der er unik for systemet. På baggrund af dette krav, har KOMBIT defineret nedenstående navnekonvention.

Rollenavne skal overholde flg. syntaks:

• http://<systemnavn>.<domæne>.<landekode>/roles/<roletype>/<rolename>/<version>

hvor

• <roletype> enten er "usersystemrole" (for brugersystemroller) eller "servicesystemrole" (for servicesystemroller).

• <version> er et forløbende nummer (1, 2, 3...)

Eksempler
Brugersystemrolle og servicesystemrolle for et system:

• http://sapa.kombit.dk/roles/usersystemrole/se_udbetalinger/8
• http://sapa.kombit.dk/roles/servicesystemrole/servicesystemrole/4

Navnekonvention for dataafgrænsninger

Ligesom roller er der behov for entydig navngivning samt versionering af Dataafgrænsningstyper, således at det fx fra et system er muligt af referere (og dermed bruge) dataafgrænsningstyper defineret i andre systemer.

Der gælder flg. navnekonvention for dataafgrænsninger:
• http://<systemnavn>.<domæne>.<landekode>/constraints/<constraintname>/<version>

Eksempler:
• http://organisation.kombit.dk/constraints/KLE/2
• http://klassifikation.kombit.dk/constraints/Følsomhed/3

Appendiks D: KOMBIT Attributprofiler for SAML tokens

KOMBITs Attributprofiler for OIOSAML 2 og OIOSAML 3 findes her Adgangsstyring for brugere | Digitaliseringskataloget.