KOMBIT

Bilag 2A

Beskrivelse af sikkerhedsmodellen i Rammearkitekturen

Indhold

1 Om dokumentet

Dette dokument giver et overblik over adgangsstyringen i Rammearkitekturen. Formålet er at give en forståelse af arkitekturen, hvilke komponenter, der er spil, deres respektive funktioner, og hvordan de interagerer med hinanden i forskellige scenarier.

Adgangsstyringen understøtter to hovedområder:

1. Adgangsstyring for brugere – som gennemgås i afsnit 4.
2. Adgangsstyring for systemer – som gennemgås i afsnit 5.

Understøttelsen af disse to hovedområder realiseres som hvert sit støttesystem i Rammearkitektur. Førstnævnte adresserer således adgang til web-baserede brugergrænseflader, mens sidstnævnte håndterer adgang til webservices (system-til-system kommunikation).

Administrationen for begge hovedområder i adgangsstyringen sker gennem Administrationsmodulet i rammearkitekturen, der udgør et selvstændigt støttesystem. Et af de bærende principper i Administrationsmodulet er, at adgang til myndighedernes data sker på baggrund af serviceaftaler (der skal ses som et supplement til databehandleraftaler) mellem myndighederne og anvenderne af data. Administrationsmodulet vil på baggrund af opsætning og indgåede aftaler provisionere information om adgange til de to adgangsstyringssystemer, som så vil anvende disse i styringen. Selve administrationen af myndighedens medarbejdere sker lokalt hos myndighederne ved genbrug af eksisterende brugeradministrationsløsninger.

Adgangsstyringen håndterer *autentifikation* og *autorisation* til systemer tilsluttet rammearkitekturen. Der findes en lang række sikkerhedsrelaterede emner, som ikke behandles her, eksempelvis fysisk sikkerhed, drift, back-up, politikker etc. Fokus i dette dokument er således udelukkende på styring af adgange for brugere og it-systemer.

Referencer:

[NSIS]	”National Standard for Identiteters Sikringsniveauer (NSIS)”, https://digitaliser.dk/group/3426134, Digitaliseringsstyrelsen.
[OIO-BPP]	”OIOSAML Basic Privilege Profile, Version 1.0.1”. http://digitaliser.dk/resource/2377872 [OIOSAML]
[OIOSAML]	”OIOSAML Web SSO Profile, Version 2.0.9”. http://digitaliser.dk/resource/2377872

2 Baggrunden for sikkerhedsmodellen

Modellen for adgangsstyring er designet ud fra en række forretningsbehov, lovkrav, arkitekturmæssige overvejelser, teknologiske tendenser, fællesoffentlige standarder samt tekniske muligheder og begrænsninger. I det følgende gennemgås de bagvedliggende overvejelser som et fundament til at forstå, hvorfor modellen ser ud som den gør.

Sikkerhedsmodellen er baseret på flg. antagelser og principper:

1. Modellen skal understøtte en effektiv brugeradministration, så myndigheder kan vedligeholde deres medarbejderes adgange lokalt - herunder ved oprettelse og nedlæggelse af brugere samt tildeling af rettigheder. Dette skal kunne ske via de forskellige brugeradministrationssystemer, som myndighederne i forvejen anvender (fx Active Directory, IdM-løsninger etc.)
2. Modellen skal understøtte, at myndighederne organiserer sig forskelligt, således at indholdet af eksempelvis jobfunktioner kan variere. Ligeledes skal myndighederne kunne have forskellige sikkerhedspolitikker, som skal kunne understøttes.
3. En medarbejder agerer på ethvert tidspunkt i kontekst af én organisation (myndighed) defineret ved et ansættelsesforhold, hvori medarbejderen kan udføre et antal jobfunktioner. Hvis personen har flere ansættelsesforhold, vil vedkommende skulle skifte aktivt mellem de forskellige kontekster.
4. De fælleskommunale systemer vil blive afviklet i et driftsmiljø, der er separat fra dels fagsystemerne (f.eks. SAPA) og dels myndighedernes egen infrastruktur. Der er med andre ord tale om en distribueret arkitektur, hvor interaktion foregår på tværs af *mindst tre adskilte sikkerhedsdomæner*.
5. Al kommunikation mellem sikkerhedsdomæner foregår via internettet (med internetprotokoller) under anvendelse af passende beskyttelse. Der etableres således ikke dedikerede netværk til at understøtte tværgående kommunikation.
6. Brugergrænseflader er web-baserede og tilgås af slutbrugerne via internettet. Traditionelle tykke klienter kan driftsafvikles lokalt hos myndigheder, men vil da tilgå den fælleskommunale infrastruktur via en web service grænseflade (se nedenfor).
7. Webservice grænseflader er SOAP- eller REST-baserede og udstilles ligeledes via internettet (herunder via den fælleskommunale serviceplatform).
8. Sikkerhedsmodellen skal funderes på fællesoffentlige standarder og være understøttet af gængse sikkerhedsprodukter og -værktøjer. Dette muliggør integration med de fællesoffentlige brugerstyringsløsninger udviklet af Digitaliseringsstyrelsen som eksempelvis NemLog-in og NemID.
9. Medarbejdere i myndighederne skal opnå single sign-on til brugervendte systemer, således at de ikke behøver at logge på hele tiden. Dette forudsætter, at de er logget på den kommunale infrastruktur.
10. Håndhævelse af adgange (*Policy Enforcement*) sker decentralt i det enkelte system.
11. Modellen skal understøtte legacy applikationer, som ikke nødvendigvis fra starten er designet til at kunne indgå i en fødereret model baseret på security tokens. Teknikker til dette beskrives senere i dokumentet.
12. Modellen skal understøtte, at myndigheder udfører jobfunktioner for hinanden via delegering.

3 Den token-baserede model

På baggrund af ovenstående principper, behov og antagelser er der valgt en *token-baseret model* for adgangsstyring. Denne indebærer, at brugere og systemer efter autentifikation får udstedt et såkaldt security token (af en betroet komponent i infrastrukturen), som herefter præsenteres overfor det system eller den service, der ønskes adgang til. Et security token indeholder information om brugerens eller systemets identitet samt tildelte adgangsrettigheder, og det er digital signeret af den betroede udsteder, så det ikke kan forfalskes eller manipuleres.

Den token-baserede model er grundlaget for en løst-koblet, fødereret arkitektur, hvor de enkelte applikationer og services kun håndhæver adgang lokalt (på baggrund af information i tokenet),

men ikke selv håndterer administration af brugere, anvendersystemer og rettigheder. Modellen indebærer således en forenkling både for brugerorganisationerne (myndigheder) og udbyderne af applikationer og services.

Af hensyn til en række legacy systemer understøtter rammearkitekturen også nogle få ikke-token baserede modeller. Disse beskrives ikke yderligere her – der henvises til integrationsvilkår i bilag 2 for detaljer om disse.

Sammenhængen i infrastrukturen sikres ved anvendelse af fællesoffentlige standarder (bl.a. OIO-SAML og OIO WS-Trust) suppleret med KOMBIT-specifikke udvidelser, som definerer hvilke attributter, der skal forefindes i security tokens (en såkaldt attributprofil).

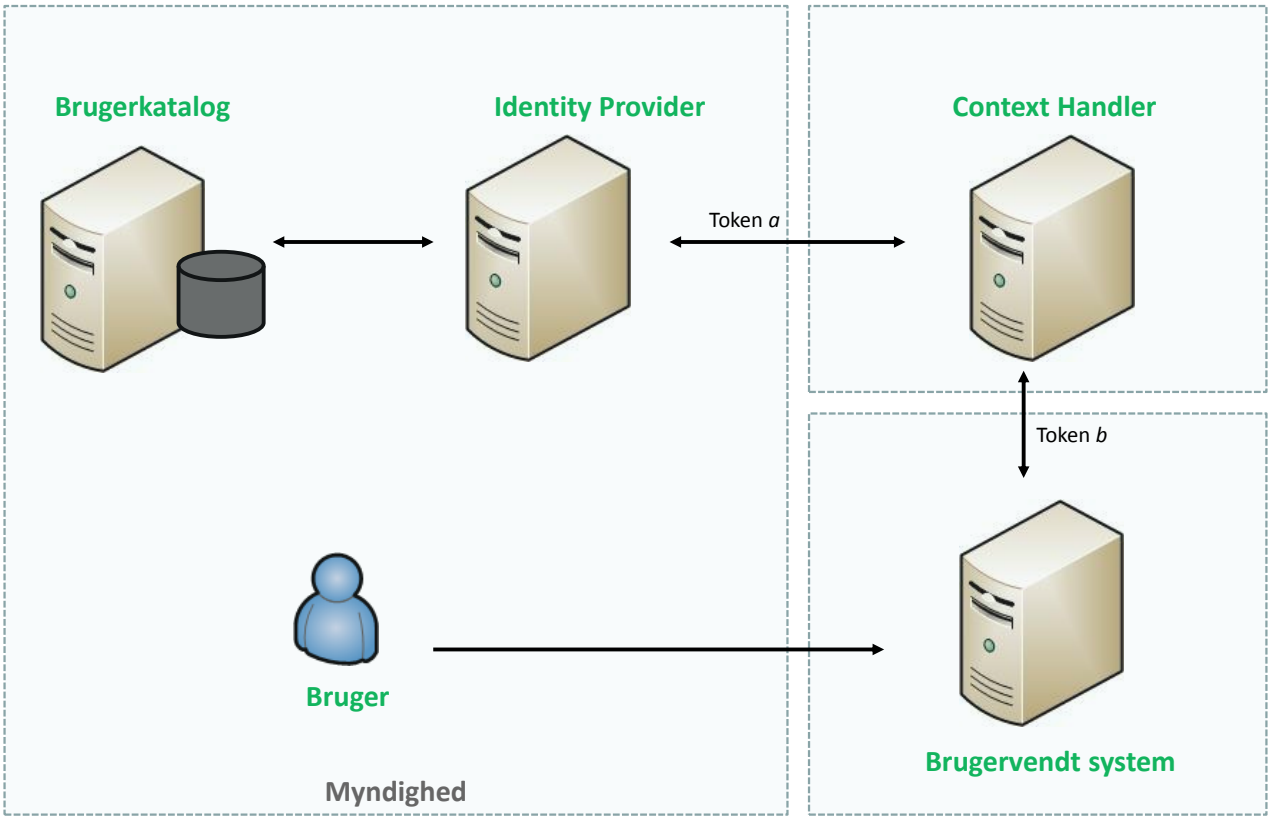
Valget af den token-baserede model er i tråd med de fællesoffentlige initiativer indenfor brugerstyring og er baseret på de samme fællesoffentlige standarder – herunder OIOSAML standarden. Som eksempel på andre offentlige initiativer, der benytter en token-baseret model, kan nævnes NemLog-in (fællesoffentlig brugerstyring), Grunddataprogrammet, Borger.dk, Virk.dk, Danmarks miljøportal, Sundhedsområdet mv. Dette giver mulighed for en række synergier eksempelvis i form af tværgående arbejdsgange mellem domæner, genbrug af fællesoffentlige komponenter (fx digitale fuldmagter), single sign-on på tværs af domæner mv.

4 Adgang til brugervendte systemer

Ved styring af brugeradgange opereres med flg. komponenter:

- Medarbejderne registreres i lokale **brugerkataloger** hos de myndigheder, hvor de er ansat. Her tildeles de et antal jobfunktionsroller ud fra de arbejdsopgaver, de skal varetage.
- Myndigheder (og andre brugerorganisationer) skal etablere en såkaldt **Identity Provider** (dvs. udbyder af identitet). Identity Provideren autentificerer organisationens egne medarbejdere (f.eks. på baggrund af lokalt netværkslogin) og udsteder herefter et security token (en SAML billet), som indeholder information om brugeren som fx identitet og tildelte jobfunktionsroller. Identity Provideren udstiller således informationerne fra organisationens brugerkatalog overfor omverdenen via en standardiseret snitflade.
- Brugervendte systemer i den fælleskommunale infrastruktur indtager rollen af **Service Provider** (dvs. konsument af identitet). Disse logger brugeren på systemet på baggrund af et security token udstedt af en betroet tredjepart.
- Mellem myndighedens Identity Provider og det brugervendte systemer indskydes en **Context Handler**, der er et støttesystem i den fælleskommunale infrastruktur. Denne har til formål at agere som fælles integrationspunkt (”trust broker”), som alle Service Providers og Identity Providers integreres til. Desuden holder Context Handleren styr på, hvilken organisation brugeren aktuelt opererer på vegne af (kontekst), og veksler jobfunktionsroller til de systemspecifikke roller, der giver adgang til de bagvedliggende systemer.

Principperne er illustreret nedenfor:



Denne model giver en hensigtsmæssig ansvarsfordeling, idet brugerne kan administreres lokalt men få adgang centralt (med single sign-on), og samtidig giver den en ønskværdig arkitekturmæssig de-kobling mellem brugervendte systemer og den fælleskommunale infrastruktur. Således kan den enkelte myndighed frit vælge den teknologi og de værktøjer, man ønsker at administrere brugerne med, så længe snitfladen mod omverdenen overholdes.

Den fællesoffentlige standard på føderationsområdet er OIOSAML[1], der er en profil af den internationale SAML 2.0 standard fra OASIS. Denne standard er ligeledes hjørnestenen i den fællesoffentlige brugerstyringsløsning NemLog-in og derfor velafprøvet. Digitaliseringsstyrelsen har fået udviklet open source referenceimplementeringer af OIOSAML, som kan lette anvendelsen af standarden. Derudover anvender en række myndigheder i dag SAML via integration til WAYF-løsningen eller Danmarks Miljøportal.

Der er foretaget en subprofilering af OIOSAML profilen i form af en såkaldt KOMBIT attributprofil, der definerer indholdet af security tokens i den fælleskommunale infrastruktur. Denne er beskrevet i Bilag 2, Appendiks D.

4.1 Rollemodel

Adgangen til brugervendte systemer styres ud fra en rollebaseret model med to niveauer:

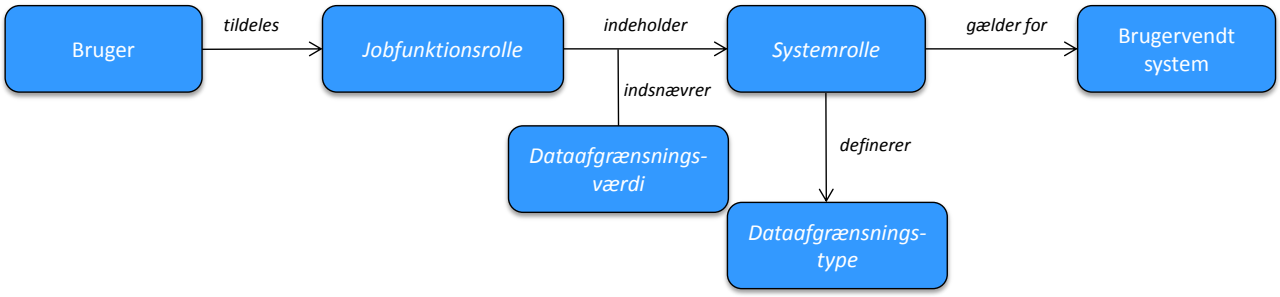
[1] http://digitaliser.dk/resource/2377872

- Jobfunktionsroller er forretningsmæssige roller, som defineres individuelt af hver myndighed og tildeledes til brugere via det lokale brugerkatalog. Disse udgør det øverste abstraktionsniveau.
- Systemroller er tekniske roller, som giver adgang til at udføre bestemte handlinger i de underliggende it-systemer. Systemrollerne er specifikke for det enkelte it-system (defineres af dette), og derved kan de roller, som mange it-systemer er født med, genanvendes. It-systemerne tvinges med andre ord ikke ind i en fælles rollemodel.

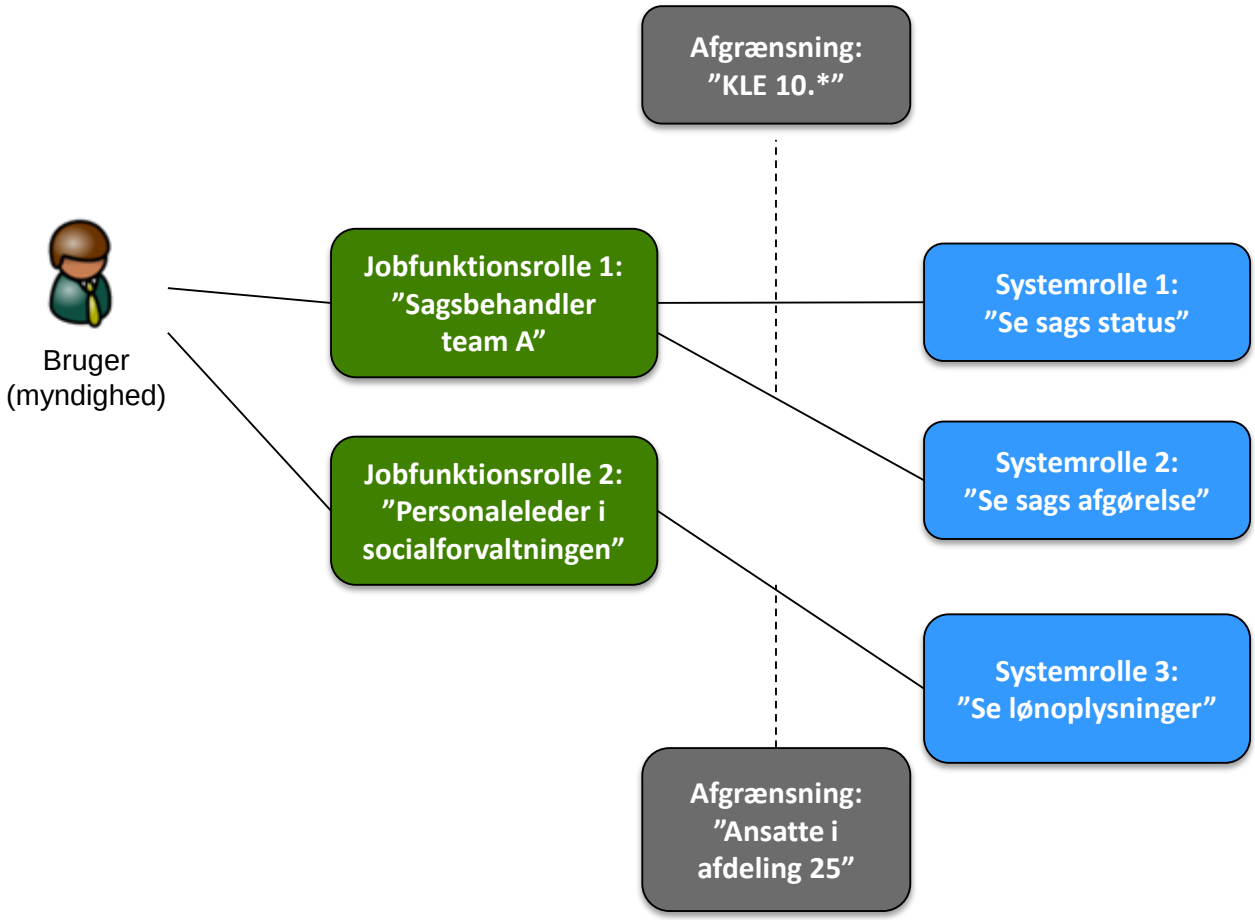
I forbindelse med definition af jobfunktionsroller opsætter en administrator i myndigheden en mapning til de underliggende systemroller. Dette sker via Administrationsmodulet i Rammearkitekturen, som beskrives senere. Ved tilknytningen mellem en systemrolle til en jobfunktionsrolle er det muligt at tilknytte en eller flere dataafgrænsninger, som angiver hvilke forretningsobjekter eller attributter af disse, systemrollen kan anvendes på. Dette forudsætter dog, at det underliggende it-system understøtter den specifikke dataafgrænsning.

De enkelte it-systemer kan håndtere forskellige typer dataafgrænsninger i deres rettighedsmodel. Eksempler på dataafgræsninger kan være KLE numre, følsomhed (ud fra en klassifikation), organisatorisk tilhørsforhold mv. Med henblik på at skabe en generel og fleksibel arkitektur, skal it-systemer udstille / deklarere deres dataafgrænsninger for infrastrukturen. Dette sker ved at it-systemet udstiller en service, som bl.a. oplyser om de understøttede dataafgrænsningstyper per systemrolle. Herved kan vilkårlige dataafgrænsninger understøttes, blot deres værdier kan udtrykkes som simple tekststrenge.

Begreberne i rollemodellen er skitseret nedenfor:



Nedenstående figur illustrerer en konkret instantiering af modellen, hvor en medarbejder er tildelt to forskellige jobfunktionsroller, som igen er koblet op på 3 underliggende systemroller med tilhørende dataafgrænsninger på disse relationer:

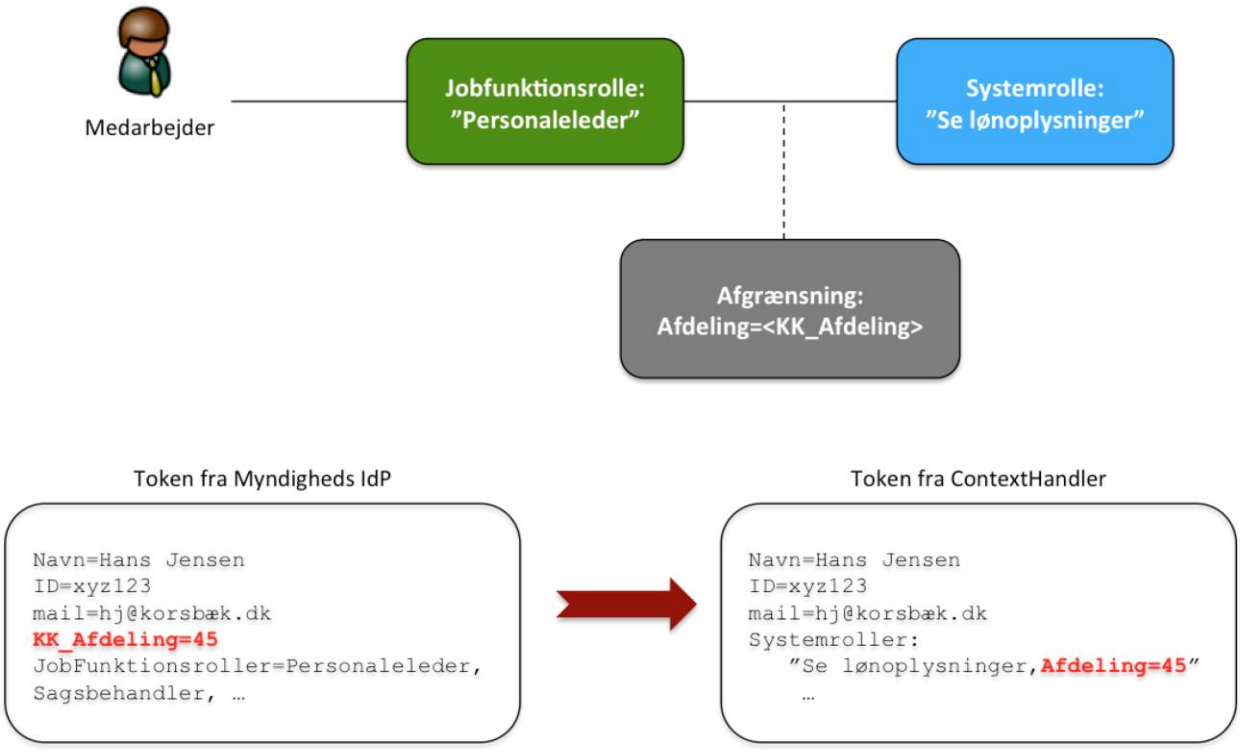

Afgrænsning:
”KLE 10.*”
Bruger
(myndighed)
Jobfunktionsrolle 1:
”Sagsbehandler
team A”
Jobfunktionsrolle 2:
”Personaleleder i
socialforvaltningen”
Systemrolle 1:
”Se sags status”
Systemrolle 2:
”Se sags afgørelse”
Systemrolle 3:
”Se lønoplysninger”
Afgrænsning:
”Ansatte i
afdeling 25”

4.1.1 Dynamiske dataafgrænsninger

Normalt fastsættes værdien af dataafgrænsninger, når en jobfunktionsrolle kobles til de underliggende brugersystemroller i Administrationsmodulet. Som et tænkt eksempel kunne jobfunktionsrollen ”Personaleleder” blive koblet til systemrollen ”Se lønoplysninger” med dataafgrænsningen ”Afdeling=23”, således at vedkommende kun kan se lønoplysninger på medarbejdere i egen afdeling. Ulempen ved at dataafgrænsningsværdien ”23” er fast defineret er imidlertid, at jobfunktionsrollen ”Personaleleder” ikke kan bruges generelt for personaleledere (for andre afdelinger), og dermed kan man ende med et behov for at definere mange udgaver af rollen, der kun adskiller sig ved værdien af dataafgrænsningen.

Til imødegåelse af ovenstående situation rummer rammearkitekturen mulighed for såkaldte ”dynamiske dataafgrænsninger” på brugerroller. Med en dynamisk dataafgrænsning gives der mulighed for at værdien af dataafgrænsninger ikke fastsættes på tidspunktet, hvor rollen defineres i Administrationsmodulet, men i stedet parameterstyres ved at myndighedens IdP medsender attributter i det udstedte token. Værdien kan ContextHandler så indsætte ”dynamisk” som værdien af dataafgrænsningen i det token, som medsendes til det brugervendte system. I forlængelse af ovenstående eksempel kunne Myndighedens IdP altså medsende værdien af brugerens afdeling (=23), og denne værdi ville så kunne bruges som værdien af dataafgrænsningen. På denne måde kan jobfunktionsrollen ”Personaleleder” være generisk.

Konceptet er illustreret på nedenstående figur:

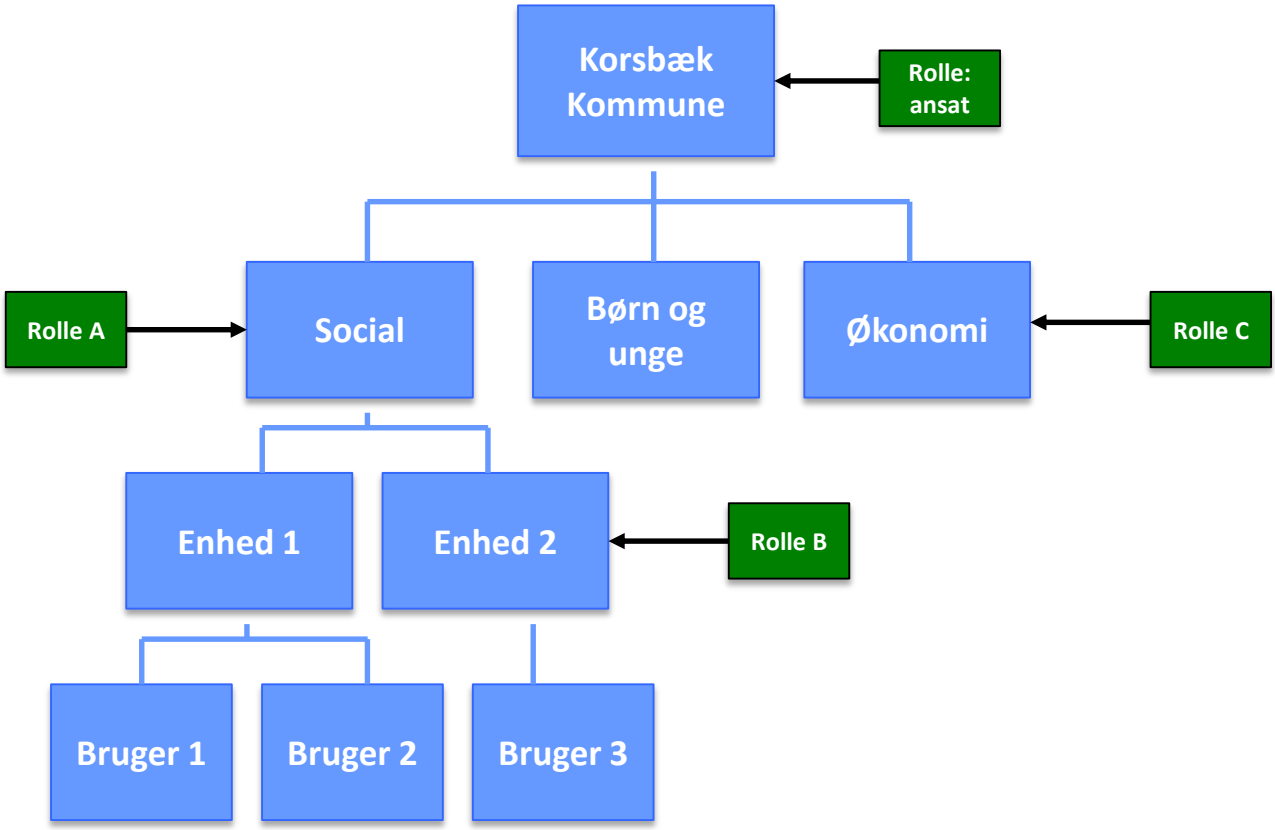


4.2 Automatiseret tildeling af jobfunktionsroller

Som nævnt administreres brugerne (herunder de tildelte jobfunktionsroller) i myndighedernes lokale brugerkataloger. Hvordan dette gøres, er helt op til den enkelte myndighed. Det kan således både gøres manuelt (fx ved at en administrator indmelder brugerne i grupper i et Active Directory, der mappes til udgående roller) eller der kan anvendes Identity Management løsninger, som automatisk eller semiautomatisk tildeler brugerne adgange på baggrund af workflows, data fra eksempelvis et HR-system med organisationsdata, eller som implementerer attestering af adgange samt såkaldt "Access Governance", hvor de faktiske adgange sammenholdes med politikker og regler med henblik på at identificere afvigelser. Alle disse ting kan opfattes som et valgfrit "automatiseringslag" ovenpå brugerkataloget.

I næsten alle organisationer er der en sammenhæng mellem de jobfunktioner, medarbejderne udfører, og den placering, de har i organisationen. Det er derfor relevant at afdække sammenhængen mellem disse begreber samt ikke mindst interaktionen mellem sikkerhedskomponenter og den fælles Organisationskomponent i Rammearkitekturen.

Figuren nedenfor illustrerer koblingen af roller til den organisatoriske placering:



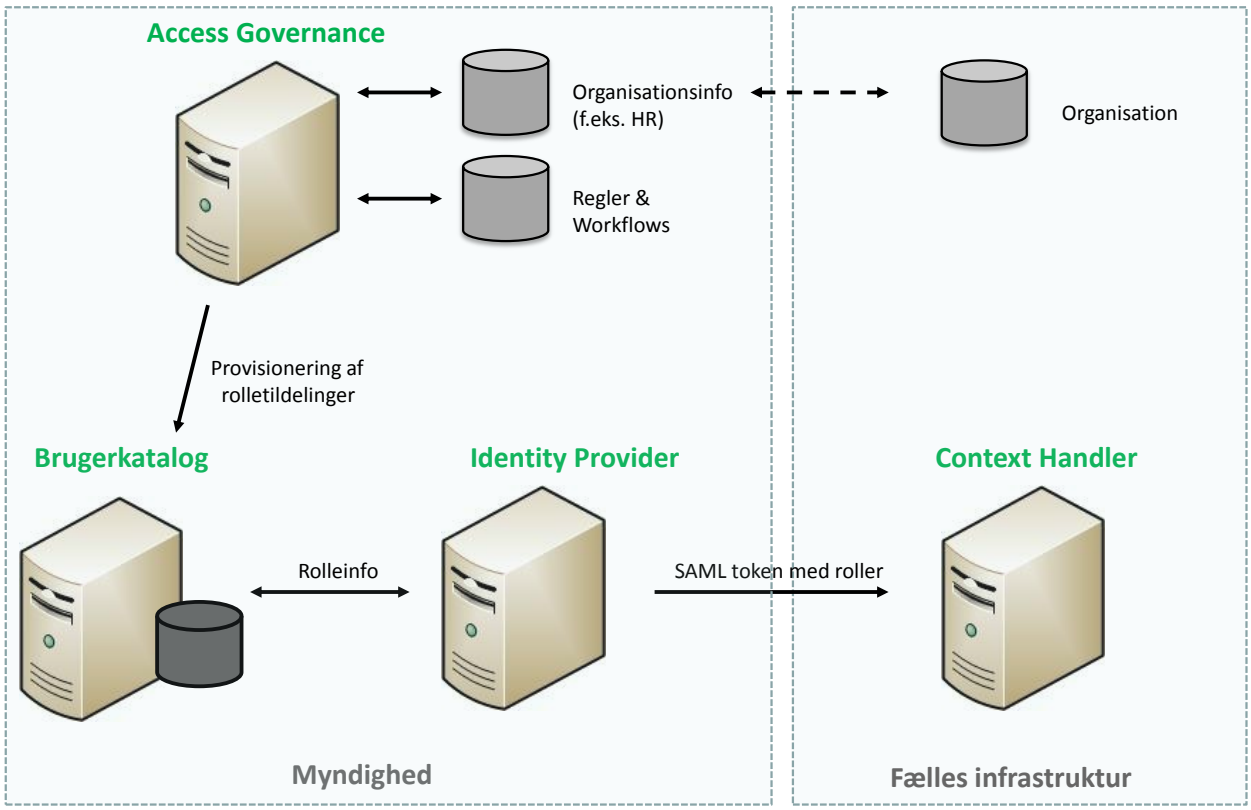
Hovedtanken i sikkerhedsmodellen er, at viden om brugerens organisatoriske tilhørsforhold kombineret med lokale regler og workflows kan danne grundlag for (evt. automatisk) tildeling af jobfunktionsroller, som adgangskontrollen herefter kan operere på. Dette betyder, at den tokenbaserede adgangskontrol kan holdes simpel, idet den kun opererer på roller og ikke skal kende organisatorisk tilknytning samt avancerede tildelingsregler, samtidig med at man kan administrere brugerne

efter avancerede regler med høj grad af automatisering. Arkitekturen opnår dermed en fordelagtig deling af ansvaret mellem en administrationskomponent (typisk et Access Governance, IAM eller IdM værktøj), der anvender organisatorisk viden og avancerede tildelingsregler[2], og en adgangskontrolkomponent, som blot agerer på de effektive roller, der er resultatet af tildelingen. En sådan opdeling er velkendt fra Identity Management software-suiter, hvor den giver mulighed for en høj grad af automatisering af brugeradministrationen kombineret med et tværgående overblik over brugernes rettigheder, selvom dette ikke er understøttet i de enkelte applikationers egen rettighedsmodel.

Adgangsstyringsmodellen, der er implementeret i denne fælleskommunale infrastruktur, kan således rumme statisk funktionsadskillelse - altså at en bruger ikke er tildelt specifikke roller samtidig som f.eks. rollerne "anvis betaling" og "godkend betaling".

Adgangsstyringsmodellen understøtter ikke dynamisk funktionsadskillelse, altså at en bruger er tildelt begge roller, men ikke kan bruge dem på samme dataobjekt. En sådan dynamisk funktionsadskillelse vil skulle løftes af det enkelte fagsystem, der kender til de lokale dataobjekter, samt brugernes relation til disse. Dette ville komplicere kravene til den del af adgangsstyring, der skal implementeres af alle fagsystemerne, og er derfor fravalgt.

Figuren nedenfor illustrerer, hvorledes arkitekturen kunne se ud:



[2] Eksempelvis omkring separation of duties.

Myndigheden har i eksemplet et brugerkatalog, hvor medarbejderne og deres jobfunktionsroller er registreret. Dette brugerkatalog er baggrunden for udstedelse af SAML tokens ved log-in til brugervendte systemer via Identity Provideren. Ovenpå har myndigheden etableret en Access Governance / IAM / IdM løsning, der provisionerer brugernes roller til brugerkataloget på baggrund af viden om brugernes organisatoriske tilhørsforhold, adgangsregler og workflows (eksempelvis godkendelser fra afdelingsledere etc.). Endvidere kunne man forestille sig at en brugeradministrator kan tildele jobfunktionsroller direkte til en bruger via brugerkataloget, idet man erfaringsmæssigt ikke (kost-effektivt) kan automatisere alle rolletildelinger.

Det skal understreges, at det er valgfrit for myndigheder at etablere den automatiserede overbygning i form af et IdM eller Access Governance værktøj (herunder valg af værktøj). For mindre organisationer kan det således være acceptabelt at vedligeholde brugere og roller manuelt.

Det har været overvejet hvorvidt der skulle etableres en central Identity Management komponent i Rammearkitekturen. Dette er fravalgt idet:

- Komponenten vil formentlig kræve avancerede integrationer tilbage til myndighedernes sikkerhedsdomæner, hvilket kan være dyrt samt kunne give sikkerhedsmæssige udfordringer.
- En KOMBIT-løsning vil kunne dække en brøkdel af de systemer, som myndigheder kunne have behov for at integrere mod, og dermed ville værdien være begrænset. Eksempelvis kan man forestille sig, at myndigheden ønsker at integrere et Access Governance / IAM / IdM værktøj med deres HR system, så ansættelser, afskedigelser og jobændringer automatisk slår igennem, at der skal laves integrationer med bestillingssystemer, så nye medarbejdere får bestilt adgangskort, mobiltelefon, PC mv., tildeles en e-mail konto og får adgang til myndighedens interne fagsystemer. Ved at den enkelte myndighed kan indkøbe og konfigurere deres egne værktøjer til Access Governance / IAM / IdM opnås en stor fleksibilitet, som en central løsning ikke vil kunne honorere.

4.3 Model for delegering af jobfunktionsroller

Der er et behov for, at myndigheder kan udføre jobfunktioner for hinanden, hvilket er løst ved at give mulighed for delegering af jobfunktionsroller fra en myndighed til en anden. Dette sker delvist under anvendelse af Administrationsmodulet i den fælleskommunale infrastruktur.

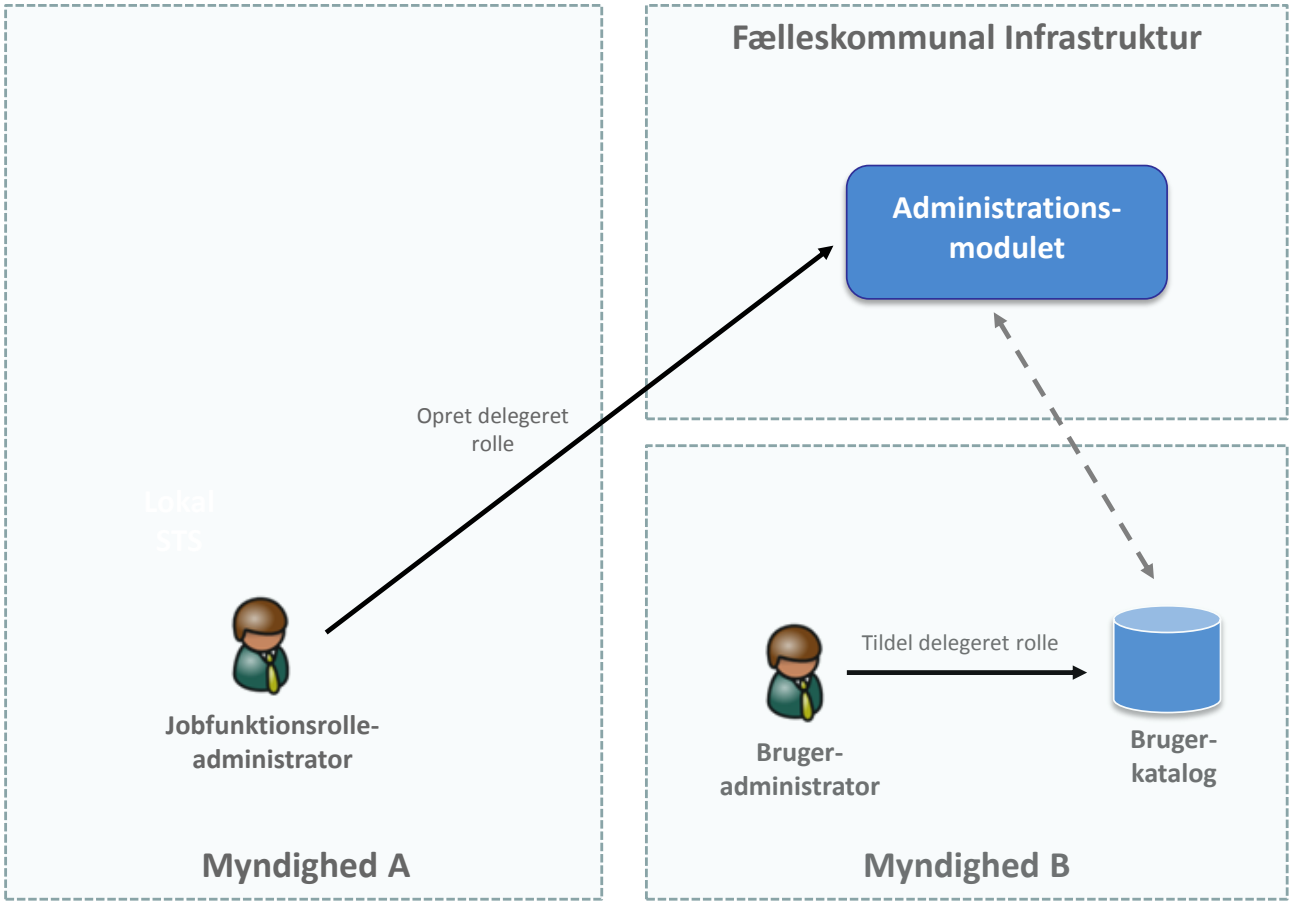
Delegeringen foregår på flg. måde:

1. Myndighed A opretter via Administrationsmodulet en jobfunktionsrolle (i egen kontekst) og tildeler den et antal systemroller til de underliggende it-systemer.
2. Myndighed A angiver i Administrationsmodulet, at jobfunktionsrollen A delegeres til myndighed B.
3. Jobfunktionsrolle A bliver nu synlig for myndighed B, og en brugeradministrator (eller et IdM-system) for myndighed B kan derfor tildele jobfunktionsrolle A til medarbejdere i myndighed B.
4. Når medarbejdere i myndighed B, som har fået tildelt jobfunktionsrolle A, logger ind via den lokale Identity Provider, inkluderes jobfunktionsrolle A i det udstedte SAML token (på lige fod med de jobfunktionsroller, medarbejderen er tildelt for sin egen myndighed).
5. Context Handleren accepterer dette (qua viden om delegeringen provisioneret fra Administrationsmodulet), og mapper jobfunktionsrolle A til de underliggende systemroller.
6. Det brugervendte system modtager systemrollerne hørende til jobfunktionsrolle A – på samme måde som ville have været tilfældet, hvis en medarbejder fra myndighed A

havde logget på. I det udstedte token fremgår dog, at brugerens kontekst stadig er myndighed B.

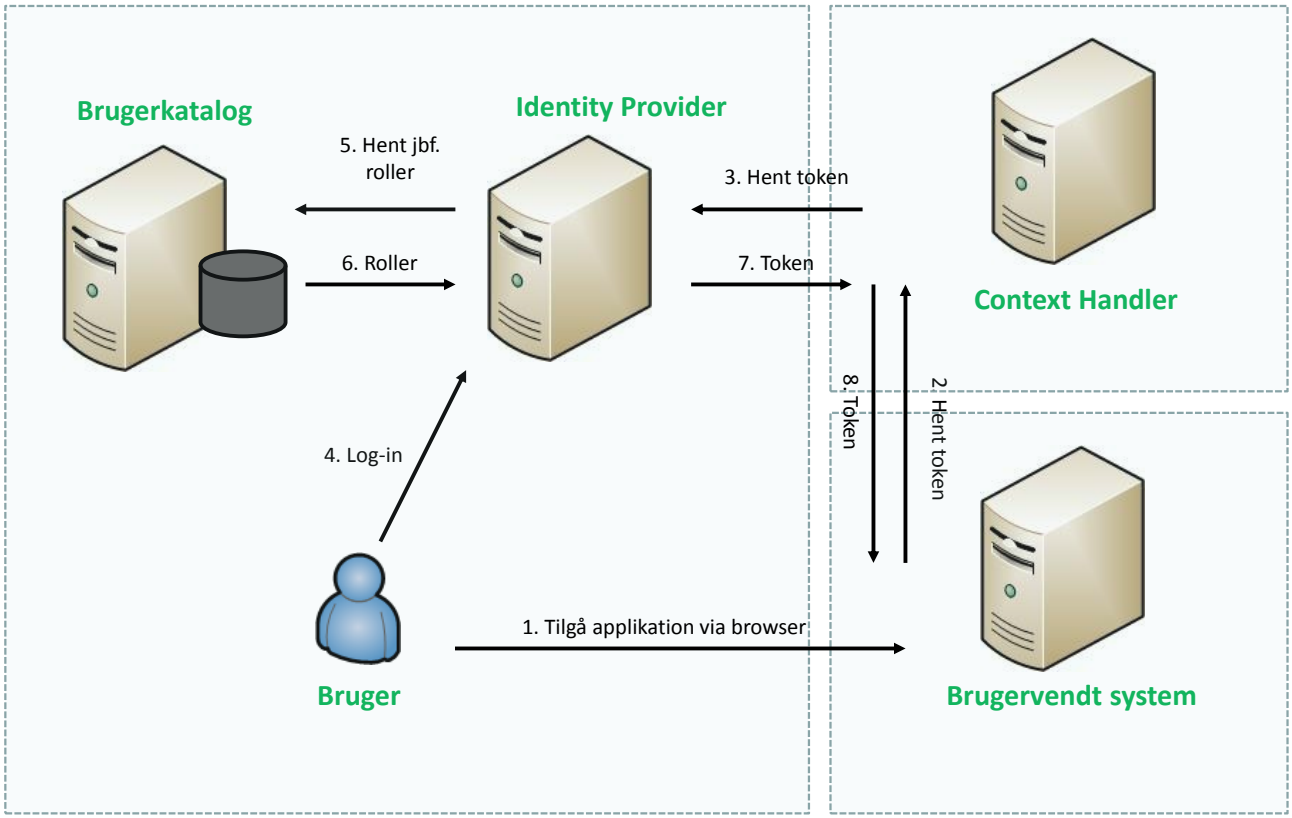
Dermed opnår man samlet, at myndighed A styrer hvilke jobfunktioner og dermed underliggende rettigheder som delegeres, mens myndighed B stadig selv håndterer administration af egne medarbejdere.

Delegeringskonceptet er illustreret på nedenstående figur:



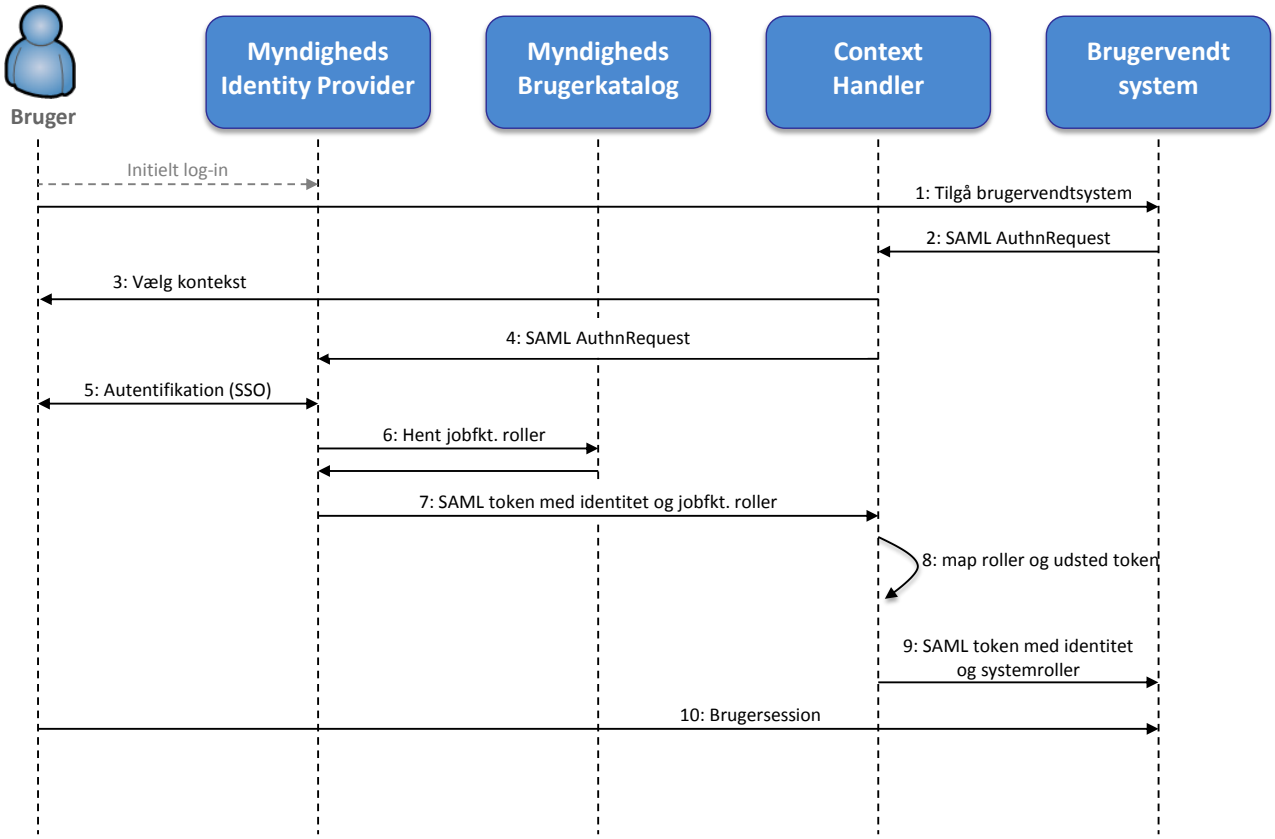
4.4 Detaljeret forløb ved log-in til brugervendt applikation

Nedenstående figur illustrerer for løbet ved log-in til en brugervendt applikation, hvor de forskellige komponenter og roller kommer i anvendelse:



1. Brugeren tilgår det brugervendte system med sin browser.
2. Det brugervendte system anmoder Context Handleren om et token til brug for log-in.
3. Context Handleren afgør hvilken Identity Provider, der kan autentificere brugeren, og anmoder denne om et token. Valget af Identity Provider kan ske ved at spørge brugeren eller ved at se på gemte præferencer (f.eks. i cookies), IP-adresse eller andet.
4. Brugeren autentificerer sig overfor den lokale Identity Provider. Hvis denne står på brugerens domæne kan processen være usynlig for brugeren (fx single sign on via Kerberos).
5. Identity Provideren validerer brugerlog-in og henter brugerens jobfunktionsroller fra det lokale brugerkatalog.
6. Jobfunktionsroller returneres på baggrund af opslag.
7. Identity Provideren udsteder et token til Context Handleren med brugerens identitet og jobfunktionsroller.
8. Context Handleren udsteder et nyt token til det brugervendte system, hvor brugerens jobfunktionsroller er omvekslet til systemroller (med tilhørende dataafgrænsninger) relevante for det brugervendte system.
9. Det brugervendte system etablerer en session med brugeren og foretager lokal adgangskontrol på baggrund af indholdet i det modtagne security token.

Den beskrevne dialog implementeres som nævnt via SAML protokollen. Interaktionen er detaljeret i nedenstående sekvensdiagram:



4.5 Revokering af adgange og roller

Når en medarbejder bliver spærret i myndighedens lokale brugerkatalog, vil vedkommende ikke længere kunne få udstedt et nyt SAML token (via den lokale Identity Provider), der giver adgang til brugervendte systemer. Dette betyder, at der ikke umiddelbart er behov for yderligere spærring af brugere, end hvad der må forventes at eksistere i forvejen. Tilsvarende gælder for brugere, som får adgang via en digital signatur (NemLog-in) frem for det lokale brugerkatalog: her vil spærring af certifikatet blokere for yderligere adgang.

Der bliver i støttesystemudbuddets implementeringsfase defineres en konkret timeoutpolitik, som definerer hvor længe SAML tokens kan være gyldige, før de skal fornys. I fællesoffentlig brugerstyring (NemLog-in føderationen) er gyldigheden normalt 30 minutter, mens det i sundhedssektoren er udbredt praksis med en gyldighed på 8 timer. Værdien skal under alle omstændigheder være konfigurérbar til forskellige værdier per autentifikationsmekanisme.

Ændringer af rettigheder slår igennem, når brugeren skal forny sit SAML token. Derfor gælder helt de samme overvejelser omkring timeoutpolitik etc. Der findes i Rammearkitekturen mekanismer, som kan gennemtvinge et log-out for brugere, men dette kan være stærkt generende for brugerne og bør derfor anvendes med omtanke.

4.6 Synergier med fællesoffentlig brugerstyring

Ved anvendelse af en fødereret sikkerhedsmodel baseret på OIOSAML opnås som nævnt en arkitekturmæssig de-kobling af fagsystemerne fra selve brugerautentifikationen. Dette vil gøre det let at skifte autentifikationsmekanismer til eksempelvis medarbejdersignaturer, mobiloptimerede loginmekanismer etc. uden påvirkning af de enkelte fagsystemer. Endvidere udstiller den fællesoffentlige brugerstyringsløsning (NemLog-in) en SAML-baseret Identity Provider komponent, som kobles til Context Handleren, hvilket kan give flg. fordele:

- Borgere vil kunne logge på Context Handleren via NemLog-in og opnå single sign-on til og med andre borgerrettede løsninger. Dette er eksempelvis relevant, hvis man i fremtiden får brug for at udstille borgervendte services på borger.dk (f.eks. indblik i egne sager). Rammearkitekturen håndterer ikke rettighedsstyring for borgere, men vil evt. kunne integrere med fællesoffentlig fuldmagtsløsning, såfremt der måtte være behov for det.
- Medarbejdere vil kunne logge på Context Handleren via NemLog-in med deres medarbejdersignatur. Dette kan benyttes ved betroede medarbejderes adgang til Administrationsmodulet.

4.7 Sikkerhed for brugerens identitet (AssuranceLevel)

Autentifikationen af medarbejdere sker lokalt og indenfor myndighedens eget sikkerhedsdomæne via de Identity Providere, som myndighederne skal etablere. Dermed vil det samlede niveau af sikkerhed for brugerens identitet (AssuranceLevel) være afhængigt af den lokale sikkerhed i organisationen - herunder de etablerede procedurer for indrullering af medarbejdere, politikker for kvalitet af kodeord eller andre credentials, låsning af konti ved afviste adgangsforsøg, begrænsning af login til det interne netværk etc. Den enkelte Identity Provider er forpligtet til at vurdere det niveau af AssuranceLevel (sikringsniveau), som er opnået (på skalaen 1 - 4) i henhold til NSIS standrden og påstemple værdien i de tokens, der udstedes, således at modtageren kan tage højde for det i adgangsbeslutninger.

Mekanismerne til beskyttelse af security tokens (digital signatur) vurderes at kunne understøtte AssuranceLevel 3[3] tilsvarende brug af OCES certifikater, hvilket normalt er det niveau, der kræves for at få adgang til personfølsomme oplysninger via internettet. Dette forudsætter naturligvis, at Identity Provideren initielt opnår AssuranceLevel 3.

4.8 Håndtering af legacy applikationer

I beskrivelsen er det hidtil antaget, at applikationer kan modtage SAML tokens fra Context Handleren indeholdende brugerens identitet og systemroller - og på baggrund af disse foretage en lokal adgangskontrol. Imidlertid kan der forekomme legacy-applikationer, som ikke er designet til at håndtere en fødereret brugerstyring – typisk ved at applikationen er født med sit eget brugerkatalog og database med rettigheder.

Sådanne applikationer håndteres i sikkerhedsmodellen ved at etablere en ”forbrænder” foran applikationen, der modtager SAML tokenet og ”just-in-time” opretter brugeren og dennes rettigheder i

[3] Det såkaldte AssuranceLevel – se http://digitaliser.dk/resource/363424 for detaljer.

applikationens interne kataloger. Komponenten oversætter altså mellem Rammearkitekturens adgangsstyringsmodel og applikationens proprietære model – på samme måde som mange web service gateways (eller ESB'er) kan indkapsle legacy systemer i en moderne web service grænseflade udadtil. Det påhviler den enkelte It-systemleverandør at levere en "forbrænder" komponent, der muliggør at applikationen kan integreres med den token-baserede brugerstyring, som anvendes i Rammearkitekturen.

Bemærk endvidere, at "just-in-time" provisioneringen sker lokalt – og ikke på tværs af sikkerhedsdomæner, og at applikationens specifikke model indpakkes i applikationens eget domæne.

4.9 Finkornet adgang

Den beskrevne model, hvor adgangsstyringen baseres på roller med tilhørende dataafgrænsninger, udgør en "grovkornet" model, som forventes at kunne dække langt hovedparten af behovet for adgangsstyring i rammearkitekturen. En af de væsentligste fordele ved modellen er, at abstraktionerne (roller og dataafgrænsninger) gør det muligt at administrere adgange eksternt for de brugervendte systemer, således at man kan få et samlet overblik over brugernes adgange og varetage brugeradministrationen ét sted.

Enkelte brugervendte systemer kan i særlige tilfælde have behov for at supplere den grovkornede adgangsstyring med mere finkornet adgangsstyring – eksempelvis hvis der er behov for at adgangsstyre individuelt på de enkelte forretningsobjekter (sager, dokumenter, organisatoriske enheder etc.). En sådan model skalerer ikke til mange forretningsobjekter og bør derfor kun anvendes i helt særlige situationer. I disse tilfælde er det brugervendte system selv ansvarligt for den supplerende, finkornede adgangsstyring, da denne typisk er tæt knyttet til systemet og forretningsdomænet. Eksempelvis kender Adgangsstyringen ikke til de konkrete forretningsobjekter (fx de specifikke sager og dokumenter), som findes i de brugervendte systemer, og derfor ville det være vanskeligt at udpege disse specifikt i forhold til administration af adgangsregler.

Et eksempel på en finkornet adgangsstyring kunne være, at kun navngivne brugere må tilgå en sag (en såkaldt ad-hoc brugergruppe, der kan tilknyttes per sag) – desuagtet disse brugeres roller. Dette behov kunne løses ved at oprette en ad hoc brugergruppe i Organisationskomponenten, melde de pågældende brugere ind i gruppen, og påstemple gruppens ID på den pågældende sag i fagsystemet, således at der kan håndhæves adgang (kun brugere der er med i gruppen får adgang). Andre systemer kan have andre behov for finkornet adgangskontrol, som skal håndteres med andre metodikker.

5 Adgang til fælleskommunale services

Ovenfor er principperne for brugeres adgange til web-baserede applikationer beskrevet. I dette afsnit gennemgås nu principperne for adgang til at kalde fælleskommunale (web) services. Som før anvendes en token-baseret model, hvor det kaldende system (Anvendersystemet) får udstedt et security token med dets identitet og tildelte systemroller. Dette token anvendes herefter ved et efterfølgende web service kald.

Den primære forskel til den brugerrettede model er den måde administrationen for adgangsstyring for fælles kommunale service foregår på. For de fælles kommunale services sker administrationen alene i Administrationsmodulet, hvor tildelingen af adgangsgivende systemroller til et anvendersystem foregår i forbindelse med indgåelse af serviceaftaler for en given service. Der er for fælleskommunale services kun ét niveau af roller for adgang til services (benævnt servicesystemroller) og altså ikke nogen jobfunktionsroller.

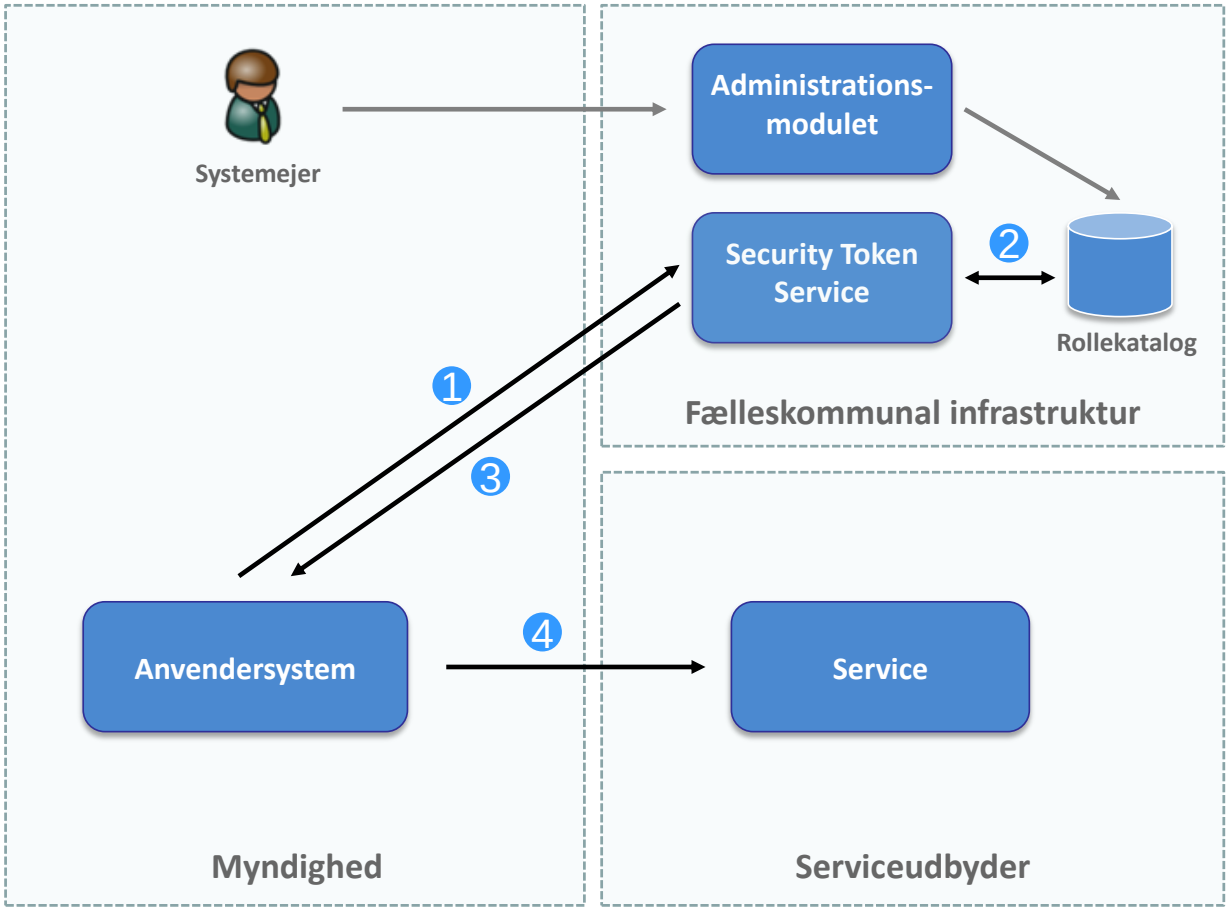
En servicesystemrolle er en gruppering af rettigheder, der definerer adgang og adgangsbegrænsninger til en given service. Servicesystemroller tildeles Anvendersystemer gennem serviceaftaler, der således beskriver hvilken adgang Anvendersystemet får til servicen.

Bemærk: udover den tokenbaserede model for adgang til services findes også modeller for simple services i Rammearkitekturen, hvor adgang gives alene på baggrund af Anvendersystemets identitet (certifikat) og ikke via tildelte roller. Disse beskrives ikke i her.

Hovedprincipperne i den token-baserede model for adgangsstyring for systemer er flg.:

- Adgang for et anvendersystem til en fælleskommunal service tildeles i Administrationsmodulet i forbindelse med indgåelse af en serviceaftale om brug af servicen.
- Adgang for et anvendersystem til en fælleskommunal service tildeles som et antal servicesystemroller med tilhørende dataafgrænsninger.
- Adgang for anvendersystemer til at kalde en web service håndhæves ved præsentation af et SAML token indeholdende et antal servicesystemroller. Tokenet bærer ikke slutbrugeridentitet men Anvendersystemets identitet (dvs. kalderens CVR nummer og et systemID).
- Der defineres nogle fælles (grovkornede) servicesystemroller, som kan tildeles Anvendersystemer og som services baserer deres adgangskontrol på.
- Et web service kald sker altid på vegne af én organisation (myndighed) identificeret ved det CVR nummer, der fremgår af kalderens OCES virksomheds- eller funktionscertifikat. For myndigheder er det kun muligt at tilgå organisationens egne data – der er med andre ord altid underforstået en dataafgrænsning på CVR nummer niveau.
- Der etableres et støttesystem i Rammearkitekturen kaldet Security Token Service (STS) baseret på WS-Trust standarden (OIO WS-Trust profilen), som Anvendersystemer kan autentificere sig mod og herefter få udstedt et SAML security token. STS'en modsvarer altså Identity Provider komponenten (Context Handleren), der servicerer browserapplikationer.
- Anvendersystemer autentificerer sig mod STS'en ved at præsentere et OCES Funktions- eller Virksomhedscertifikat. Certifikatet er forinden registreret af en betroet medarbejder fra myndigheden eller dennes It-systemleverandører i forbindelse med tilslutningen af Anvendersystemet til Rammearkitekturen.

Modellen for systemadgang via den centrale Security Token Service er skitseret på nedenstående figur:

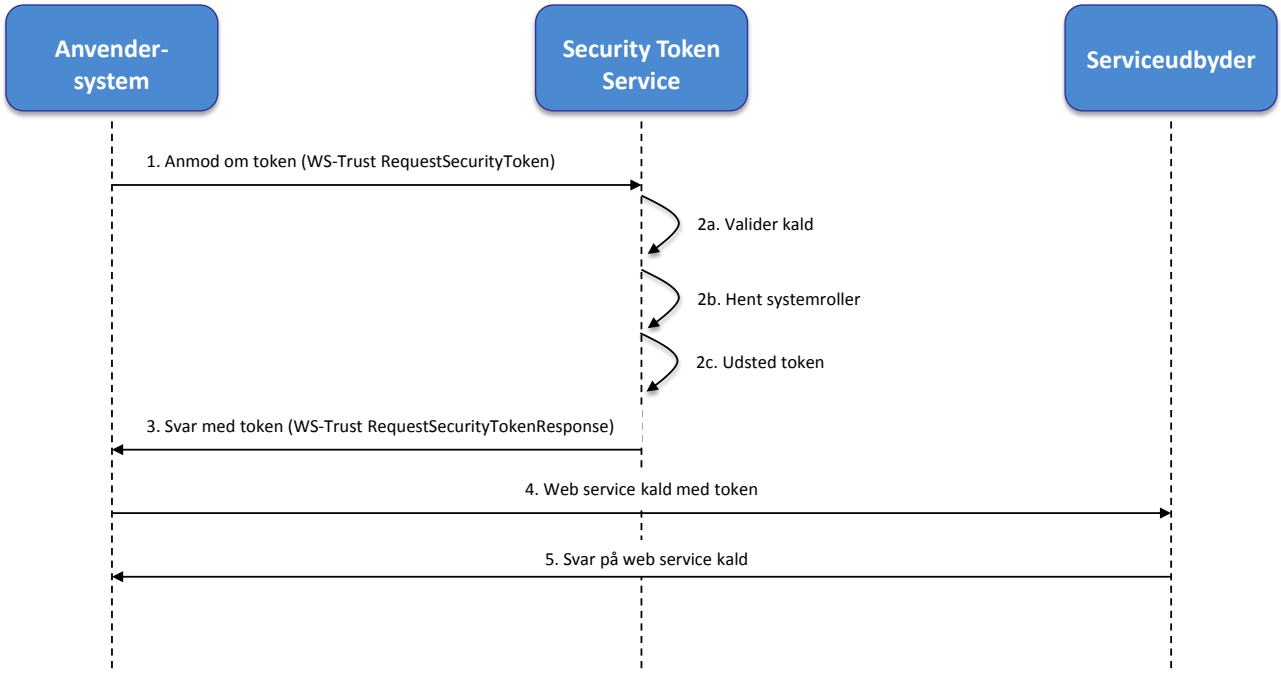


Sekvensen på figuren er flg.:

1. Anvendersystemet forespørger om et security token hos Security Token Servicen[4]. I kaldet medsendes information om hvilken web service, der ønskes adgang til, og kaldet er signeret med et OCES Funktions- eller Virksomhedscertifikat, der på forhånd er registreret via Administrationsmodulet (via de grå pile).
2. Security Token Servicen validerer kaldet, og fremfinder de servicesystemroller, som Anvendersystemet er tildelt.
3. Der udstedes et SAML token, som returneres til Anvendersystemet. Tokenet er digitalt underskrevet af STS'en, rummer information om Anvendersystemets identitet (CVR og systemID), de tildelte roller samt hvilken service (endpoint), hvor tokenet kan anvendes.
4. Anvendersystemet kan nu foretage et (signeret) web service kald mod servicen, hvori SAML tokenet medsendes. Servicen validerer signaturen og at SAML Tokenet er udstedt af Rammearkitekturens STS, hvorefter der gives adgang på baggrund af kalderens identitet og tildelte servicesystemroller, som er udtrukket af SAML tokenet. Tokenet har en gyldighed (f.eks. 1 time), så det kan caches og genbruges i efterfølgende kald, uden at STS'en skal kontaktes igen.

[4] Et WS-Trust RequestSecurityToken

Ovenstående forløb implementeres via WS-Trust protokollen som illustreret på nedenstående figur:



Modellen opnår, at den enkelte service ikke skal kende til de kaldende Anvendersystemer og deres certifikater – og blot kan stole på SAML tokens udstedt af støttesystemet STS. Dette giver en arkitekturmæssig løs kobling og fleksibilitet fremadrettet:

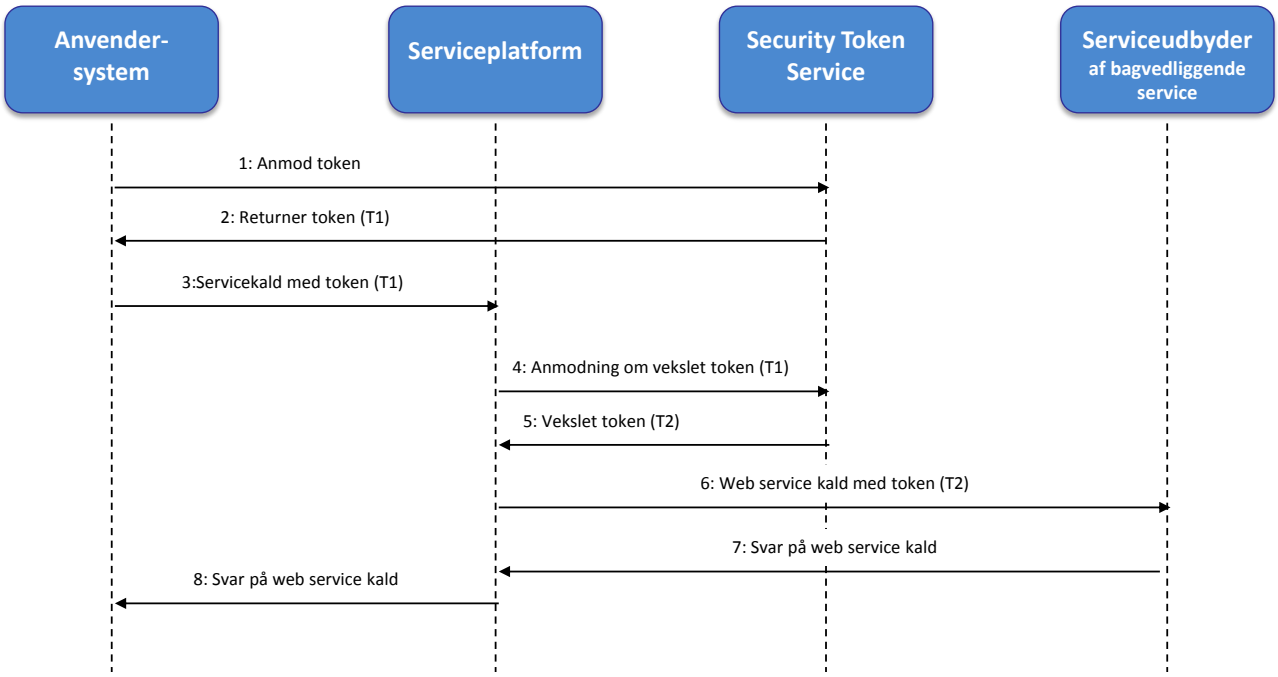
- Man kan ændre på autentifikationen uden at påvirke services, herunder autentifikationsmekanismer eller koblingen mellem credentials og systemer.
- Man kan ændre på aftalehåndtering og koblingen mellem en aftale og autentifikation uden at påvirke services.

5.1 Kald via Serviceplatformen

I praksis vil mange services blive udstillet via den fælleskommunale serviceplatform. Her vil anvendersystemet kun kende et endpoint på serviceplatformen, som herefter kalder de bagvedliggende services, indsamler / transformerer svarene og herefter returnerer svar til anvendersystemet. Herved kan serviceplatformen udføre mediering, transformationer og orkestrering af services.

I denne situation vil Anvendersystemet skulle tildeles et antal servicesystemroller til den service, der udstilles på serviceplatformen. Serviceplatform får tildelt en speciel adgang til at veksle tokens hos STS'en, hvor de indgående servicesystemroller for anvendersystemet veksles til udgående systemroller til de bagvedliggende services, så serviceplatformen kan kalde disse på vegne af anvendersystemet. Dette forudsætter, at STS'en er bekendt med sammenhængen mellem "front-end" og "back-end" services, og at serviceplatformen konfigureres som et særligt betroet system.

Princippet er illustreret på nedenstående figur:



5.2 Caching og genanvendelse af tokens

Modellen ovenfor beskriver et enkeltstående web service kald mellem Anvendersystem og service baseret på præsentation af et token. I praksis kan der være behov for at understøtte mere avancerede kaldsmønstre:

- Et Anvendersystem kan have behov for at udføre flere kald på kort tid. Her kan et token med lang levetid genanvendes, så overhead til token udstedelse undgås. Derimod vil der stadig være et overhead forbundet med validering af tokenet for det enkelte kald hos støttesystemet.
- Anvendersystem og støttesystem kan etablere en session baseret på initiel udveksling af tokens, hvorefter en længerevarende kommunikation anvender sessionen. Her er Rammearkitekturen kun involveret i udstedelse af de tokens, som anvendes til etablering af sessionen, mens resten betragtes som en privat protokol mellem Anvendersystem og støttesystem. Systemerne kan altså frit vælge protokol og teknologi til sessionshåndtering (fx WS-Secure Conversation, WS-ReliableMessaging, SSL, SSH etc.).

6 Administrationsmodulet for adgangsstyring

Den fælleskommunale infrastruktur indeholder som nævnt et Administrationsmodul, der vil være det centrale knudepunkt for at tilslutte systemer og administrere rettigheder til Rammearkitekturens systemer. Via Administrationsmodulets brugergrænseflade understøttes selvbetjening i forbindelse tilslutning af systemer til infrastrukturen samt administration af deres tilhørende aftaler og konfiguration.

Administrationsmodulet benyttes til administration af både adgangsstyring for brugere og adgangsstyring for systemer, der er beskrevet ovenfor. Administrationsmodulet håndterer de underliggende aftaler mellem Myndigheder, It-systemleverandører og KOMBIT, og provisionerer informationer til komponenterne i Adgangsstyring for hhv. brugere og systemer (Context Handler og Security Token Service), således at de kan slå igennem ved udstedelse af security tokens som beskrevet i

første del af notatet. Derved vil fagsystemerne håndhæve adgangskontrol ud fra de aftaler, der er indgået i Administrationsmodulet.

De følgende afsnit beskriver kort de administrative arbejdsopgaver, der understøttes i Administrationsmodulet.

6.1 Administration af tilslutningsparter

Enhver Myndighed og It-systemleverandør, der skal benytte den fællekommunale infrastruktur, skal oprettes som tilslutningspart i Administrationsmodulet. En tilslutningspart vil eksempelvis være de organisationer, der kan indgå som part i de aftaler, der vedrører de it-systemer, der anvender den fælleskommunale infrastruktur.

Administrationsmodulet skal understøtte tre typer af tilslutningsparter:

- Myndighed – i denne sammenhæng en organisation, der anvender et it-system og er dataansvarlig for de data, der er tilgængelige gennem Rammearkitekturen. En Myndighed vil i praksis være kommunerne eller Udbetaling Danmark.
- It-systemleverandør – den organisation, der leverer et it-system. En It-systemleverandør vil typisk være en virksomhed. Kommuner og andre offentlige Myndigheder vil dog også kunne levere it-systemer til den fællekommunale infrastruktur. Er dette tilfældet, vil Myndigheden optræde i rollen som It-systemleverandør.
- Forvalter – den organisation, der forvalter den fællekommunale Rammearkitektur. Forvalteren er eksempelvis ansvarlig for at oprette tilslutningspart og godkende tilslutninger af it-systemer. Forvalteren vil også i visse tilfælde kunne indgå aftaler på vegne af Myndigheder, hvis forvalteren har fuldmagt hertil. Som udgangspunkt indtræder KOMBIT i rollen som forvalter, men forvaltningsrollen skal kunne lægges ud til andre organisationer.

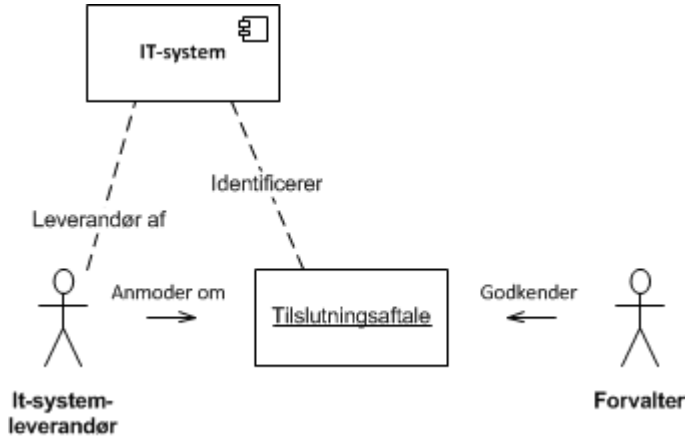
6.2 Brugeradgang til Administrationsmodulet

Som nævnt vil en række medarbejdere hos myndigheder og It-systemleverandører have behov for adgang til Administrationsmodulet. Log-in sker via NemLog-in med et OCES medarbejdercertifikat og brugerne kan tildeles et antal administrationsmodulroller, der er nogle særlige roller, der ikke vedligeholdes i myndighedernes egne brugerkataloger med derimod centralt i Administrationsmodulet. Når en organisation tilsluttes, udpeges relevante administratorer.

Arbejdsgangene vil blive lagt ind i dette dokument på et senere tidspunkt.

6.3 Administration af tilsluttede systemer

Alle it-systemer, der skal tilsluttes den fællekommunale infrastruktur, skal oprettes i Administrationsmodulet. Tilslutning af et system sker ved at it-systemleverandøren af it-systemet anmoder om en tilslutningsaftale for dette specifikke system. Tilslutningsaftaler visiteres og godkendes af Forvalteren af den Fællekommunale Rammearkitektur, som illustreret på figuren nedenfor.

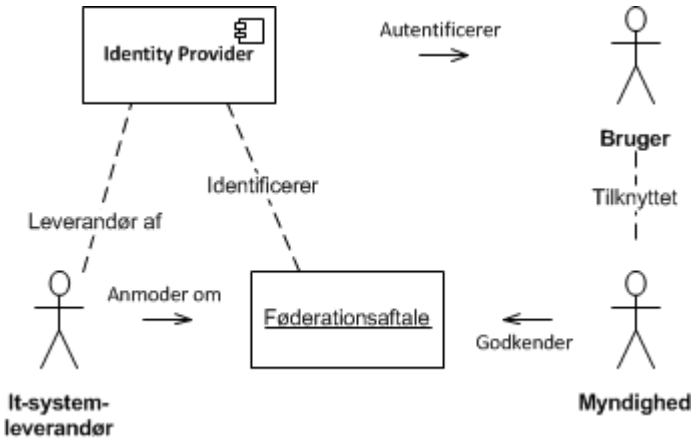


I Administrationsmodulet optræder et it-system med en eller flere systemtyper, der bestemmer hvilken type af funktionalitet it-systemet udstiller. Administrationsmodulet understøtter følgende systemtyper: Identity Provider, Brugervendt system, Anvendersystem og Serviceudbyder.

Afhængigt af it-systemets type kan man indgå forskellige typer af aftaler for it-systemet og Administrationsmodulet udstiller forskellige tekniske systemparametre, der er nødvendige for implementering og håndhævelse af disse aftaler. Disse systemparametre vedligeholdes i Administrationsmodulet af it-systemleverandøren af it-systemet. Et givet it-system ville kunne optræde med mere end en systemtype.

6.3.1 Administration af adgangsstyring for brugervendte systemer

Rammearkitekturen har en fødereret model for adgangsstyring af brugere, som beskrevet ovenfor. Her er en Identity Provider er det it-system, der udsteder tokens som attesterer, at en given bruger er autentificeret af en given Myndighed. Administrationsmodulet understøtter indgåelse af føderationsaftaler mellem en Leverandør af en Identity Provider og en Myndighed, der giver It-systemleverandøren lov til at autentificere og udstede adgangstokens for Myndighedens brugere.



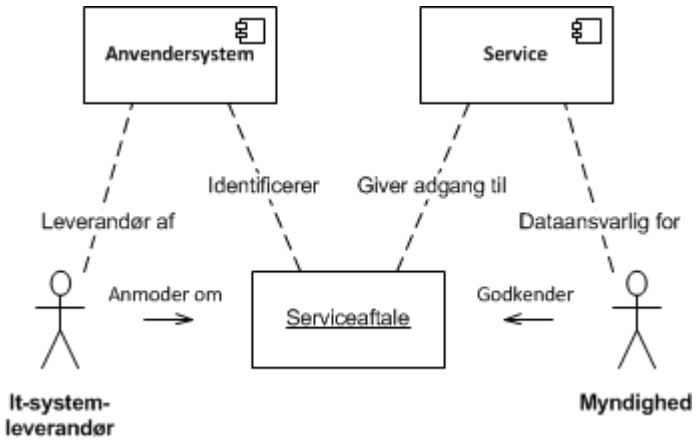
Figur 1 Indgåelse af Føderationsaftale

Administrationsmodulet er endvidere det fælles modul, der benyttes til at administrere alle oplysninger, der skal deles mellem de forskellige systemer i denne fødererede adgangsstyringsmodel. Administrationsmodulet understøtter følgende opgaver i forbindelse med adgangsstyring til det brugervendte systemer:

- Tilslutning af Identity Providere.
  - Herunder registreres certifikater til brug for kryptografiske signaturer på tokens.
- Tilslutning af brugervendte systemer.
  - Herunder registreres de Brugersystemroller, som det brugervendte system understøtter håndhævelse af.
- Administration af Jobfunktionsroller.
  - Hver Myndighed kan redigere egne Jobfunktionsroller, der passer til Myndighedens jobfunktioner. Herunder opsættes en afbildning mellem Jobfunktionsroller og Brugersystemroller, som beskrevet i afsnit 4.1.
- Provisionering til Støttesystem Adgangsstyring for brugere.
  - Føderationsaftaler og Jobfunktionsroller provisioneres til Støttesystem Adgangsstyring for brugere. Støttesystem Adgangsstyring for brugere udsteder så kun tokens i henhold til disse aftaler og opsætninger af Jobfunktionsroller.

6.3.2 Administration af adgangsstyring for Serviceudbydere

Serviceudbyderne er it-systemer, der kan indeholde Myndigheders data og udstille dem gennem en servicesnitflade, hvor andre systemer kan få adgang til disse data. Via Administrationsmodulet er det muligt for It-systemleverandøren af et Anvendersystem at indgå en serviceaftale med Myndigheden, der giver It-systemleverandøren tilladelse til at benytte servicesnitfladen til at tilgå Myndighedens data i Serviceudbyderen.



Figur 2 Indgåelse af Serviceaftale

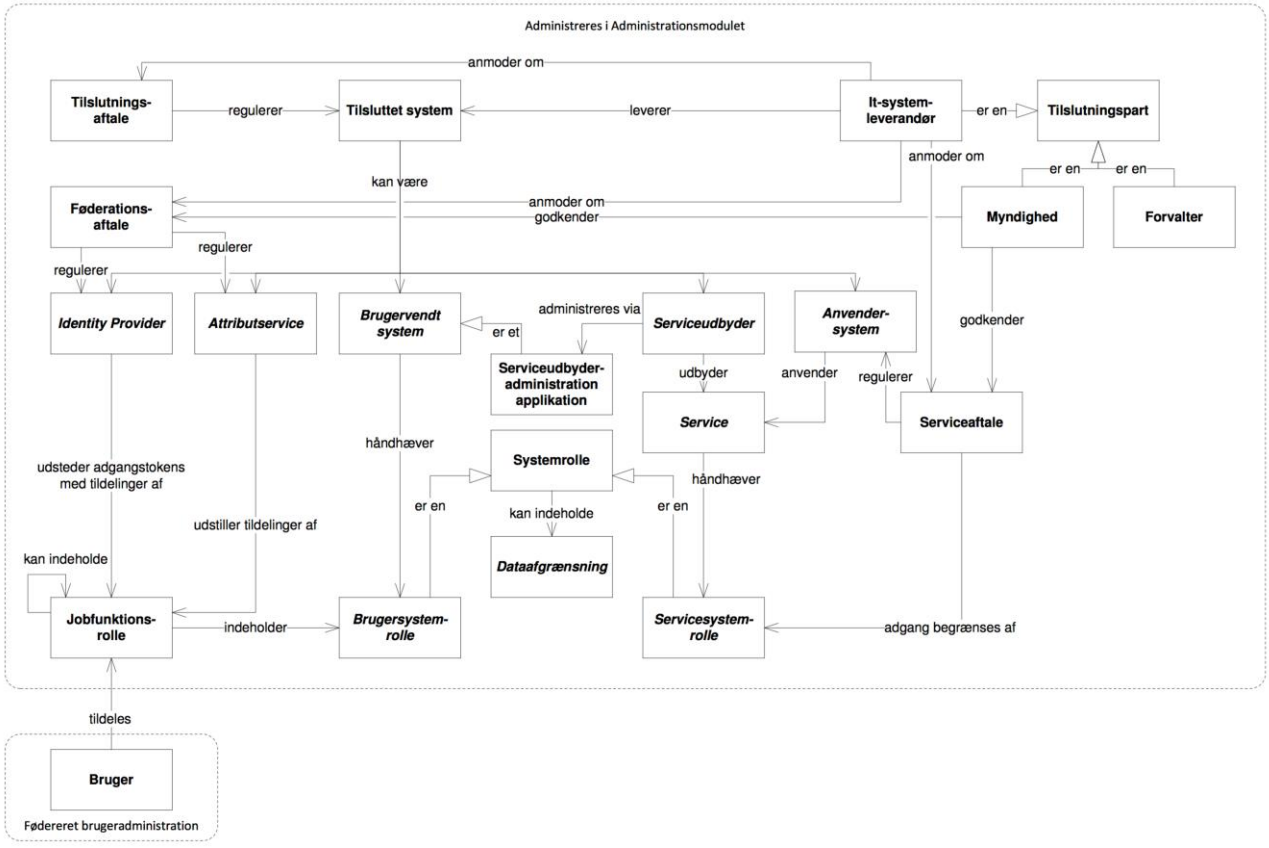
En serviceaftale er et supplement til en databehandleraftale, der giver It-systemleverandøren af Anvendersystemet en instruks om at måtte behandle Myndighedens data og overfører dem mellem Anvendersystemet og Serviceudbyderen. Serviceaftalen indeholder endvidere de adgangsrettigheder (i form af Servicesystemroller), som giver Anvendersystemet adgang til Serviceudbyderen. Derved kan serviceaftalen automatisk håndhæves, når Anvendersystemet tilgår Serviceudbyderen.

Administrationsmodulet er det fælles system, der benyttes til at administrere alle oplysninger, der skal deles mellem de forskellige Tilsluttede systemer i denne fødererede adgangsstyringsmodel. Herunder understøtter Administrationsmodulet følgende opgaver:

- Tilslutning af Serviceudbydere.
  - Herunder registreres certifikater til signering af tokens samt de Servicesystemroller, der understøttes
- Tilslutning af Anvendersystemer
  - Herunder registreres certifikater til signering ved anmodning om tokens
- Provisionering af rolletildelinger til Security Token Service.
- Udtræk af rapporter over indgåede aftaler, metadata for it-systemer, mv.

6.4 Begrebsmodel for Administrationsmodulet

Begrebsmodellen for de tilslutningsparter, it-systemer, aftaler, mv. der administreres i Administrationsmodulet er vist herunder. Denne begrebsmodel illustrerer sammenhængen mellem de forskellige begreber. I de følgende afsnit beskrives kort de primære arbejdsopgaver, der kan udføres i Administrationsmodulet.



Begrebsmodellen kan læses som følger:

- En tilslutningspart kan enten være en It-systemleverandør, en Myndighed, eller en Forvalter.

- En It-systemleverandør kan tilslutte et system ved at indgå en tilslutningsaftale med Forvalteren. Et tilsluttet system 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-systemleverandør kan tilslutte systemer, og kan anmode om aftaler på disse. Aftaler godkendes af Myndighed eller Forvalter