Bilag 1 - Fælles arkitekturramme for GD1-GD2-GD7

Forslag til fælles sikkerhedsmodel for   
Grunddataprogrammet

Status: Version 1.2

Version: 19.06.2014

Indholdsfortegnelse

1. Indledning 4

1.1 Baggrund 4

1.2 Dokumentet 4

1.3 Afgrænsninger 4

2. Ledelsesoverblik 6

2.1 Forretningsbehov 6

2.2 Succeskriterier 6

3. Aktører, brugerflader og services 7

4. Anbefalet sikkerhedsmodel 8

4.1 Token-baseret adgangsstyring 8

4.2 Antagelser og hypoteser 9

4.3 Løsningsmodel fase 1 9

4.3.1 Bruger logger på klient 11

4.3.2 Klient kalder service til ajourføring 13

4.3.3 Sikkerhed på beskeder 13

4.4 Løsningsmodel fase 2 (personbrugermodel) 15

4.5 Videreudviklingsmuligheder 17

4.5.1 Adgang til grunddata med fuldmagt 17

5. Forslag til krav 19

5.1 Krav til lokale brugerkataloger og IdP’er 19

5.2 Krav til klienter og serviceanvendere 20

5.2.1 Krav til tykke klienter 23

5.3 Krav til serviceudbydere 23

5.4 Krav til Grunddata STS 24

5.5 Fælleskrav 26

6. Referencer 28

7. Appendiks A: System- og personbruger 29

7.1 Model A: Adgang med personbrugere 29

7.2 Model B: Adgang med systembruger 30

8. Appendiks B: SAML Attributprofiler 32

8.1 Profil for ikke-OCES brugere 32

8.1.1 Krav til indhold af SAML Subject Element 32

8.1.2 Krav til indhold af kerneattributter 33

8.1.3 Krav til AudienceRestriction 33

8.1.4 Krav til repræsentation af roller 34

# Indledning

## Baggrund

Dette dokument har til formål at adressere behovet for en tværgående sikkerhedsmodel i Grunddataprogrammet, som understøtter single sign-on og effektiv brugeradministration. Formålet er at sikre en hensigtsmæssig understøttelse af tværgående processer, hvor en bruger eksempelvis arbejder på flere underliggende grunddataregistre samtidig. Hvert register samt Datafordeleren har hidtil opereret med hver deres sikkerhedsmodel, som isoleret set fungerer fint, men som på sigt ikke er en skalérbar model og i værste fald kan resultere i en ressourcekrævende brugeradministration.

Med henblik på at afklare og konkretisere behovene for en tværgående sikkerhedsmodel, er der i februar og marts 2014 afholdt en række workshops med deltagelse af repræsentanter fra Ministeriet for By, Bolig og Landdistrikter, Geodatastyrelsen, KOMBIT, Strand & Donslund, Optimum IT, IT Crew Consulting og Digitaliseringsstyrelsen. På disse er behovene for adgangsstyring i GD1 og GD2 diskuteret med udgangspunkt i BBR klienten.

## Dokumentet

Dette dokument beskriver et forslag til en sikkerhedsmodel for grunddataprogrammet, der er opstillet på baggrund af de identificerede behov hos GD1 og GD2. Det er dog tilstræbt, at modellen er generel og dermed anvendelig for resten af grunddataprogrammet. Der er endvidere beskrevet forslag til overordnede krav, som de enkelte projekter tager udgangspunkt i ved udarbejdelse af udbudsmateriale. De enkelte grunddataprojekter forventes dog efterfølgende at skulle foretage en detaljering og konkretisering af egne forhold i de kravspecifikationer samt øvrigt udbudsmateriale, som skal udarbejdes.

Udover dette indledende kapitel indeholder dokumentet følgende kapitler:

* **Kapitel 2 – Ledelsesoverblik**  
  Indeholder en beskrivelse samt motivering af forretningsbehov og succeskriterier for en fælles, tværgående sikkerhedsløsning.
* **Kapitel 3 – Aktører, brugerflader og services**  
  Giver et overblik over aktører, brugerflader / klienter og services i GD1 samt GD2.
* **Kapitel 4 – Anbefalet sikkerhedsmodel**  
  Indeholder en overordnet beskrivelse af den foreslåede sikkerhedsmodel inkl. de principper og logiske komponenter, som arkitekturen bygges på.
* **Kapitel 5 – Forslag til krav**  
  Indeholder forslag til overordnede krav til de forskellige komponenter i sikkerhedsmodellen, som danner udgangspunkt for efterfølgende kravspecifikationer i grunddataprogrammet. De enkelte udbud må udvælge de relevante krav og supplere med egne detailkrav, hvor det er nødvendigt.

Målgruppen for dokumentet er it-arkitekter og projektledere i grunddataprogrammet.

## Afgrænsninger

Under hensyn til de snævre tidsmæssige rammer for udarbejdelsen af nærværende dokument, er der foretaget en række afgrænsninger:

* Sikkerhedsmodellen er beskrevet på overordnet niveau.
* Fokus er på behovet for adgangsstyring for ”offentlige” snitflader i form af brugergrænseflader samt servicegrænseflader. Interne forhold og integrationer (fx dataoverførsel mellem registre og datafordeleren) behandles ikke.
* Krav er formuleret til bl.a. logiske komponenter, klienter, serviceanvendere, serviceudbydere og Grunddata STS m.fl., - som gør dokumentet relevant at inkludere i projekternes kravspecifikationer - hvorfor følgende opgaver udestår for de enkelte projekter:  
  + Identifikation af - og dokumentation af de nødvendige roller.
  + Definition af lokale brugerkataloger
  + Håndtering af modtagne Security Tokens
* Kravene er formuleret som funktionelle krav til sikkerhedskomponenter – men er ikke beregnet til at stå alene. De antages at blive indarbejdet i udbudsmaterialer, som indeholder andre krav til komponenterne, eksempelvis krav til test, drift, miljøer, SLA’er, dokumentation osv.
* Der er ikke taget stilling til governance, administrative processer, aftaleindgåelse mv. Dette omfatter eksempelvis koordinering af roller, udveksling af metadata, udformning af databehandleraftaler mv.
* Dokumentet indeholder ikke planlægningsaspekter – herunder timingen i de forskellige udbud, afhængigheder, behovet for interim-løsninger osv.

Hovedsigtet har været på at etablere en fælles sikkerhedsmodel med tilhørende krav, som kan indgå i de udbud, der gennemføres i foråret 2014. Som det fremgår af ovenstående, er der en række forhold, som skal afklares under den efterfølgende implementeringsfase.

# Ledelsesoverblik

## Forretningsbehov

I Grunddataprogrammet sker der et afgørende sceneskift, når ”silosystemer” (eksempelvis ESR) erstattes af samarbejdende grunddataregistre, hvor aktører kan ajourføre på tværs af de enkelte grunddataregistre og kan hente grunddata fra Datafordeleren.

Dette fordrer en sikkerhedsløsning, som understøtter ”Single Sign-on” på tværs af grunddataregistre og Datafordeleren. For kommunerne er der eksempelvis behov for, at løsningen hænger sammen med de løsninger til brugeradministration og adgangsstyring, der er ved at blive implementeret under den fælleskommunale rammearkitektur i regi af KOMBIT.

Situationen vil være uholdbar for den enkelte aktør - fx den kommunale medarbejder - hvis vedkommende skal logge ind individuelt på hvert enkelt grunddataregister hhv. Datafordeleren, hver gang der skal hentes eller opdateres data – eller hvis brugernes adgang skal administreres i mange forskellige systemer. Der er således behov for, at aktører i en og samme arbejdsgang og med ét log-on kan opdatere et eller flere grunddataregistre og samtidig få adgang til grunddata fra Datafordeleren. I modsat fald kan risikere, at de forventede effektiviseringer kan ikke opnås, fordi arbejdsgangene bliver mere ressourcekrævende end antaget i den opstillede business case.

## Succeskriterier

Der er identificeret flg. succeskriterier for en fælles sikkerhedsmodel:

1. Modellen skal være implementérbar og tage hensyn til tidsplanen for grunddataprogrammet – herunder fx ved kunne realiseres i forskellige faser, således at sikkerløsningen ikke introducerer en forsinkelse af tidsplanen.
2. Den nye sikkerhedsmodel skal kunne opnå mindst samme sikkerhedsniveau, som der findes på servicegrænsefladerne for de nuværende registre.
3. Brugerne skal kun skulle logge på én gang – uanset om deres arbejdsfunktion betinger en underliggende adgang til flere underliggende registre eller sammensatte services.
4. Brugeradministrationen skal være enkel og effektiv – eksempelvis skal den enkelte bruger blive administreret i den organisation, som de udfører arbejdsopgaver for.
5. Persondatalovens- og sikkerhedsbekendtgørelsens krav skal kunne opfyldes i forbindelse med adgang til personoplysninger.
6. Sikkerhedsmodellen skal kunne arbejde sammen med eksisterende brugerstyringsløsninger som fx Adgangsstyring i den fælleskommunale rammearkitektur og NemLog-in (fællesoffentlig brugerstyring) – så der ikke introduceres en ny silo med brugerstyring og brugeradministration.
7. Sikkerhedsmodellen for services skal være ens på tværs af hele grunddataprogrammet, således at der er størst mulighed ensartethed og potentiale for synergier - eksempelvis gennem fælles implementeringer.
8. Der skal etableres fuld sporbarhed for læsninger og opdateringer.

Ovenstående succeskriterier er lagt til grund for nedenstående anbefalinger og løsningsforslag.

# Aktører, brugerflader og services

Et vigtigt formål med de afholdte workshops har været af kortlægge hvilke aktører, brugerflader og services, der er i spil i GD1 og GD2, samt relationerne mellem dem. Nedenstående figur illustrerer resultatet af kortlægningen:



Figur : Aktører, brugerflader og registre

Som det fremgår af figuren, er der en række forskellige brugergrupper (illustreret som aktører), der anvender en række forskellige brugerflader / klienter, som tilgår en række forskellige registre (illustreret uden et servicelag).

På workshops blev flg. vigtige pointer fremhævet, som har været udslagsgivende for forslaget til model:

* Brugerfladerne / klienterne er et relativt faste, og der forventes ikke i fremtiden et stort antal nye klienter udviklet af tredjeparter. Det er derfor rimeligt at antage, at dataansvarlige myndigheder, som lader en klient tilgå deres services og data, kan indgå en databehandleraftale med den part, som er ansvarlig for klienten, og at en del af adgangskontrollen ud mod slutbrugerne håndhæves i klienten (jævnfør systembrugermodellen i appendiks A).
* Der er en stor mængde tværgående kald af nye ajourføringsservices, som skal håndteres.
* Flere aktører anvender mere end én klient – dette gælder eksempelvis kommunale brugere.
* Flere klienter vil evt. på sigt skulle håndtere nye brugergrupper som eksempelvis private rådgivere, borgere, konsulenter etc.

# Anbefalet sikkerhedsmodel

I dette kapitel beskrives den anbefalede sikkerhedsmodel. Der lægges op til en implementering i to faser, startende med en basal løsning baseret på systembrugermodellen, som på et senere tidspunkt kan udvides til at omfatte personbrugermodellen[[1]](#footnote-2).

Baggrunden for dette forslag er:

* Hensynet til kompleksitet, tidsplaner og økonomi for GD1 og GD2, herunder mindst mulig påvirkning af de eksisterende systemer, som er orienteret mod systembrugermodellen.
* Forretningsbehovene for GD1 og GD2 udtrykt på workshops fordrer ikke på kort sigt en personbrugermodel. Eksempelvis er der identificeret få, faste klienter med relativt faste integrationer til bagvedliggende registre, hvorfor administrationen af databehandleraftaler og trust-relationer forekommer overskuelig.

Det er dog samtidig klart, at personbrugermodellen rummer en række fordele på sigt, herunder at modellen bedre skalerer til et økosystem med mange klienter, som tilgår mange services. For en yderligere beskrivelse af fordelene ved personbrugermodellen henvises til appendiks A.

Både system- og personbrugermodellen er funderet på udstedelse og konsumering af såkaldte security tokens (SAML Assertions), hvilket beskrives i næste afsnit.

## Token-baseret adgangsstyring

Det anbefales, at adgangsstyringen overordnet baseres på en **token-baseret adgangsstyring**, hvor adgang til en brugerflade eller en web service opnås ved præsentation af et security token (SAML Assertion) udstedt af en betroet tredjepart. Et security token indeholder information om klientens eller brugerens identitet samt tildelte rettigheder (fx i form af roller og dataafgrænsninger), og er signeret for at sikre dets autenticitet og integritet.

Token-baseret adgangsstyring anvendes efterhånden overalt i den offentlige sektor (NemLog-in, den fælleskommunale rammearkitektur, sundhedsdomænet (SOSI), Danmarks Miljøportal, WAYF) og giver en række fordele:

* Modellen er i tråd med de hidtidige strategier for fællesoffentlig brugerstyring.
* Modellen er teknologi-neutral.
* Brugerne kan opnå single sign-on og brugeradministration kan ske lokalt / decentralt (dvs. dobbeltadministration kan undgås).
* Der opnås fleksibilitet i forhold til at kunne sammensætte services og understøtte tværgående scenarier.
* Der er mulighed for synergi med eksisterende brugerstyringsløsninger – så eksisterende komponenter til adgangsstyring kan genbruges.
* Adgangen til services styres ud fra en rolle-baseret model.
* Arkitekturen opnår en løs kobling mellem udbydere af services og administrationen af adgange.

Security tokens kan udstedes til enten en personbruger eller en systembruger (se Appendiks A for detaljer). Forskellen mellem disse er primært, hvor og hvordan brugerstyringen foretages hhv. hvilket system, der har ansvaret for, at brugerne kun får adgang til de funktioner og data, de er berettiget til. Personbrugermodellen opfattes normalt som den mest ideelle (og moderne), men er samtidig også den mest komplekse, idet den kræver, at alle personbrugere oprettes med dertil knyttede rettigheder.

## Antagelser og hypoteser

Der ligger en række antagelser og hypoteser til grund for den foreslåede udmøntning af den token-baserede model:

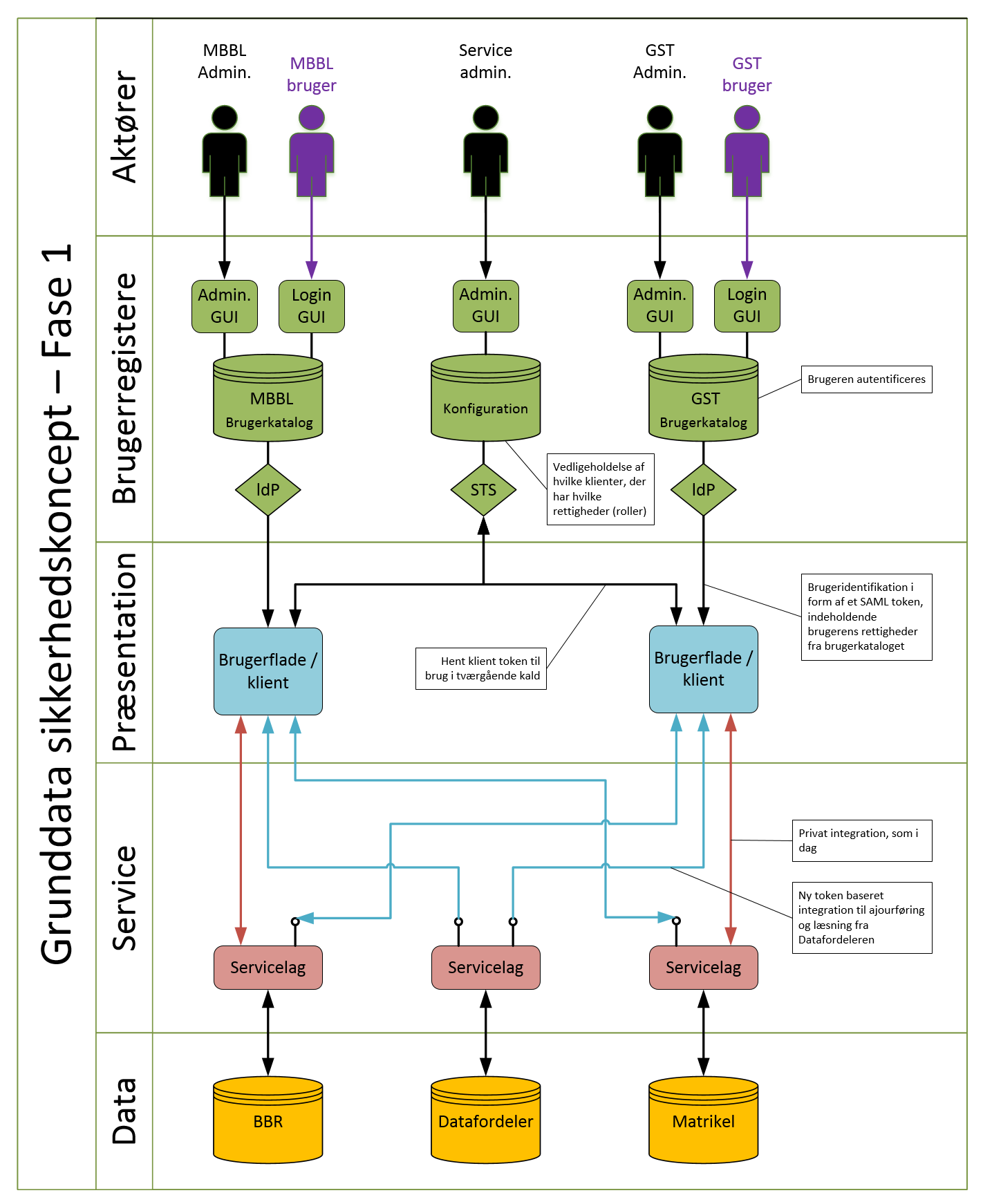
1. Der er behov for, at brugerkataloger og brugerautentifikation er løst-koblede komponenter, som ikke indbygges i de enkelte brugerflader/klienter. På den måde kan brugerne opnå single sign-on til forskellige enkelte klienter, og man undgår at skulle administrere brugerne mere end ét sted.
2. Adgangsstyring ifm. tværgående kald af ajourføringsservices kan håndteres via en ”grovkornet” sikkerhedsmodel baseret på nogle statiske roller suppleret med få dataafgrænsninger.
3. Systembrugermodellen (se appendiks A) har det umiddelbart bedste fit med det nuværende systemlandskab og vurderes derfor at kunne give den hurtigste / billigste implementering. Der er dog fordele ved personbrugermodellen, som skal kunne bruges på sigt parallelt med systembrugermodellen.
4. Der skal ske en forberedelse af infrastrukturen, så man senere kan overgå til personbrugermodellen (fase 2) uden store konsekvenser. Der skal med andre ord tages højde for denne transition i kravspecifikationer og arkitektur.

## Løsningsmodel fase 1

I den første fase af løsningen indføres selvstændige, løst-koblede brugerkataloger samt en token-baseret systembrugermodel for servicekald. Endvidere genbruges en række eksisterende fællesoffentlige brugerstyringskomponenter. De vigtigste principper ved løsningsmodellen er dermed flg.:

* Brugerne vedligeholdes i decentrale brugerkataloger hos de autoritative myndigheder, hvor de er ansat, eller hvor adgangen for eksterne naturligt administreres. Dette kan eksempelvis være kommunernes egne brugerkataloger, et GST brugerkatalog med beskikkede landinspektører, et brugerkatalog hos en myndighed med interne myndighedsbrugere etc.
  + Hvis der i forbindelse med det lokale brugerkatalog er mulighed for brugerautentifikation (fx via brugernavn og kodeord), udstilles dette som en SAML-baseret Identity Provider service til de klienter, som servicerer de pågældende brugere. Identity Provideren skal autentificere brugerne, og udstille deres roller for klienterne via udstedte security tokens.
  + For brugere, der autentificeres via NemID eller OCES certifikater (fx borgere og landinspektører), benyttes NemLog-in som SAML baseret Identity Provider. Her kan et lokalt brugerkatalog supplere brugerens centralt udstedte token fra NemLog-in med andre attributter, der vedligeholdes lokalt (fx katalog over beskikkede landinspektører). Hvis det lokale brugerkatalog anvendes af mere end én klient, skal det udstilles som en SAML Attribute Provider, så det kan genbruges via en åben snitflade.
  + Brugeradministration og -autentifikation flyttes dermed ud af klienterne, så de kan genbruges på tværs af infrastrukturen.
* Klienter med behov for fuldmagter skal anvende NemLog-in’s fuldmagtsløsninger (hhv. borger- og erhvervsfuldmagt), for brugerne med NemID / OCES certifikat. Herved undgår klienterne selv at etablere fuldmagtsfunktionalitet.
* Klienter med behov for signering skal anvende NemLog-in’s signeringstjeneste for brugere med NemID / OCES certifikat. Herved undgår klienterne at etablere egen signeringskomponent.
* Hvis der er brugerroller, som administreres af de enkelte brugerorganisationer ved en delegeret model i stedet for centralt (fx landinspektørers assistenter), skal dette ske via NemLog-in’s brugeradministrationsløsning (FBRS). Herved undgår klienterne at etablere en løsning til delegeret brugeradministration.
* Servicekald mellem eksisterende klienter og ”egne” services (fx kald fra BBR klient til BBR services) kan videreføres i de nuværende former og ændres dermed ikke i den første fase. Kaldene opfattes som en privat integration, der ikke behøver at følge den token-baserede model. Dette betyder, at myndighederne i første omgang kan fokusere på de nye ajourføringsservices, og at bestående implementeringer berøres så lidt som muligt.
* Der indføres en fælles (logisk) Security Token Service (STS) til grunddataprogrammet, som udsteder security tokens (SAML Assertions), der kan autorisere web service kald. Hensigten med denne er at have et centralt sted at administrere og autorisere tværgående kald, således at de enkelte udbydere af ajourføringsservices slipper for dette. Samtidig udgør den et samlet integrationspunkt, hvor man kan videreudvikle sikkerhedsmodellen med mere avanceret funktionalitet (se beskrivelsen af fase 2).
* ***Tværgående*** servicekald til ajourføring af grunddata autoriseres med et security token indeholdende en systembruger. Dette gælder ligeledes læseadgang til Datafordeleren. Dermed er der ét centralt sted, hvor man kan administrere klienternes/serviceanvenderes adgange; de enkelte serviceudbydere slipper altså for at udstille snitflader til klientadministration. Dette vurderes at kunne give væsentlige, administrative gevinster.

Udvalgte aspekter af løsningsmodellen er skitseret på nedenstående figur:



Figur : Løsningmodel for fase 1

Bemærk at servicekald på figuren er illustreret som udgående fra klienterne – de kan også udgå fra et servicelag hørende til klienten (back-end), men modellen er helt den samme.

Samlet adresserer modellen flg. processer for brugere og services: autentifikation, single sign-on, autorisation, administration, signering og fuldmagt. De efterfølgende underafsnit uddyber forskellige aspekter af modellen.

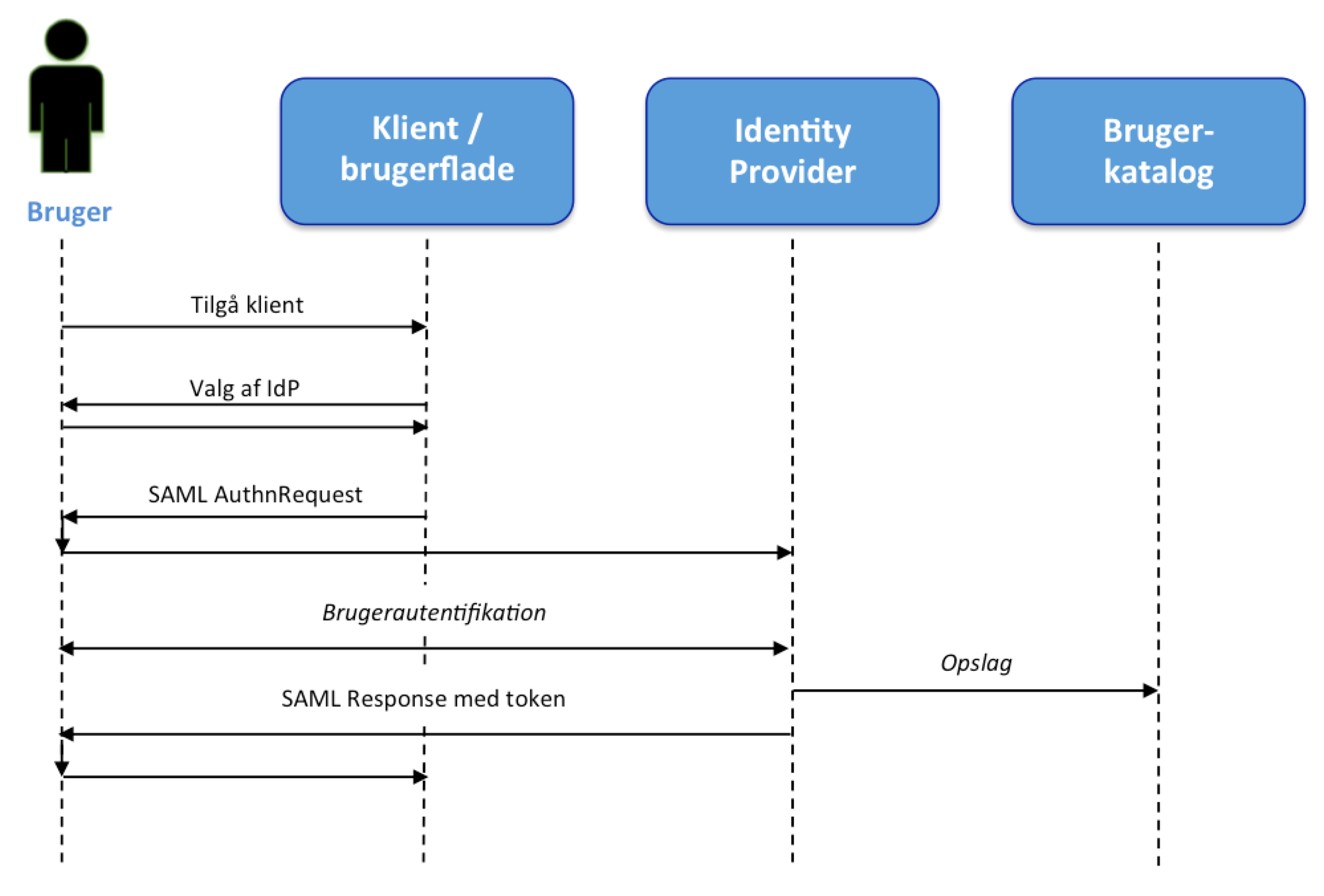
### Bruger logger på klient

Når en bruger logger på en klient, vil det i henhold til modellen ske gennem en ekstern Identity Provider service via SAML protokollen. Klienten vil derfor på forhånd skulle være konfigureret med tilslutninger til Identity Providers for de brugertyper/organisationer, den servicerer.

I eksemplet med BBR klienten vil denne skulle være konfigureret med en forbindelse til:

* KOMBIT’s centrale Identity Provider for kommunale brugere (også kaldet Context Handler).
* En MBBL Identity Provider for medarbejdere i MBBL.
* Evt. med NemLog-in’s Identity Provider for log-in for borgere/rådgivere med NemID eller medarbejdersignatur.

Når brugerens browser rammer en beskyttet side i BBR-klienten, vil den skulle bede brugeren om at vælge, hvordan han/hun vil logge på (dvs. hvor vedkommende kommer fra)[[2]](#footnote-3). Herefter videresendes browseren via SAML protokollen til den relevante Identity Provider, som autentificerer brugeren, og returnerer browseren til BBR klienten med et SAML security token, der identificerer brugeren og indeholder evt. roller til BBR klienten, som brugeren måtte være tildelt. Sekvensen er illustreret på nedenstående figur:



Figur : Sekvens ved brugerlog-in til klient

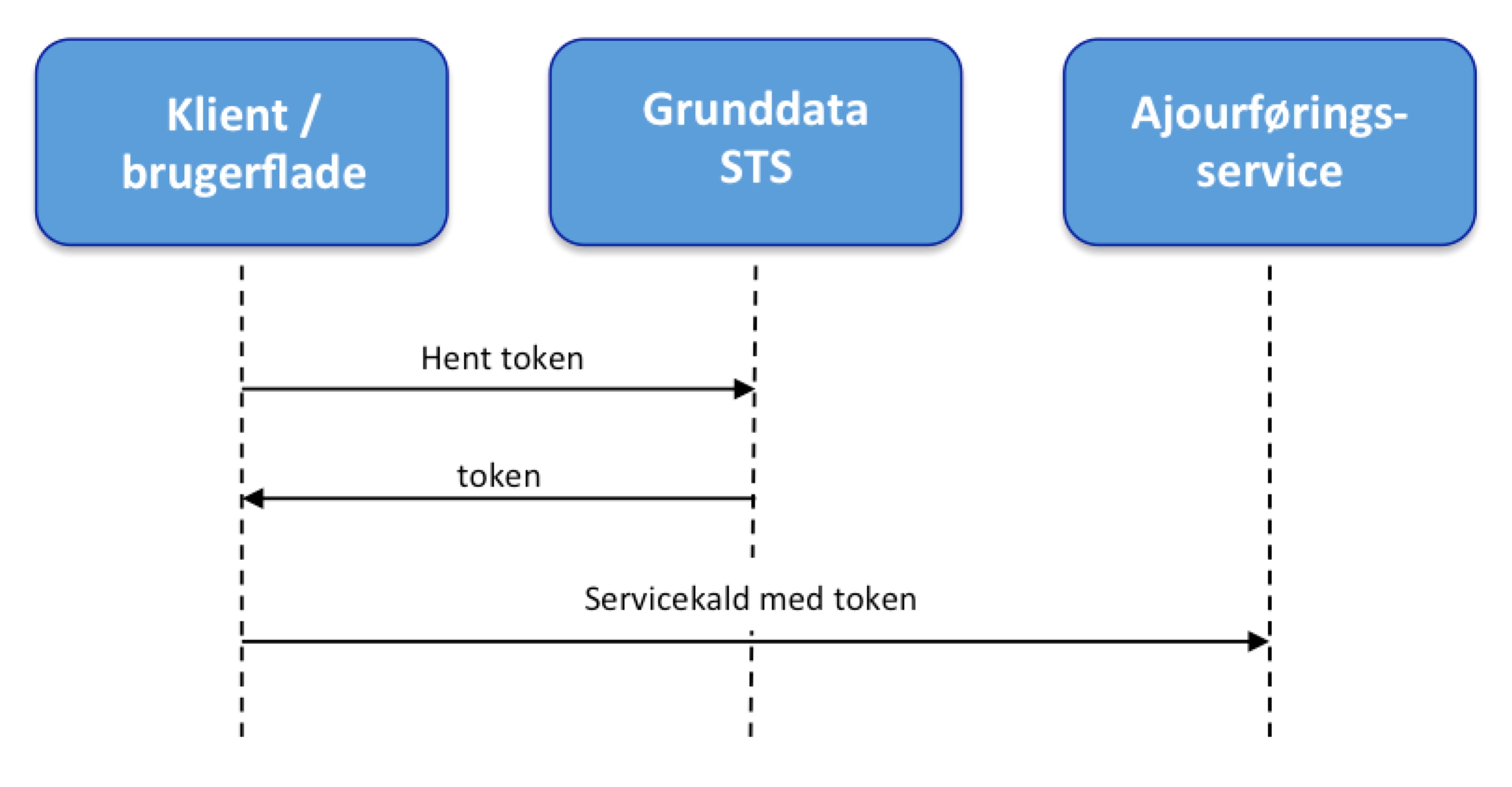
Klienten skal på forhånd have defineret de roller, som brugerne skal kunne tildeles, således at de kan medsendes i det SAML token, som Identity Provideren udsteder. Dette kan eksempelvis være i form af et antal URI’er, der kan repræsenteres som tekststrenge i henhold til OIOSAML Basic Privilege Profile.

Efter brugerlog-in opretter klienten en session med brugerens browser og håndhæver adgangskontrol på baggrund af de roller, som brugeren er tildelt (fra SAML token).

Brugerne administreres som nævnt decentralt i de brugerkataloger, hvor de enten er ansat, eller hvor det autoritative ansvar for brugeradgang er placeret. Her er det vigtigt at skabe sammenhæng mellem de roller, som klienterne udstiller, og de tildelinger der foretages decentralt. Behov for værktøjsunderstøttelse af denne koordinering vurderes på et senere tidspunkt – i første omgang kan man evt. nøjes med et rollekatalog udstillet på en passende web side.

### Klient kalder service til ajourføring

Når en klient (eller anden serviceanvender) har behov for at kalde en (fremmed) ajourføringsservice, skal den først hente et security token hos grunddata STS’en, som efterfølgende autoriserer kaldet. Dette sker ved at klienten først kalder STS’en via WS-Trust protokollen, hvori klienten autentificerer sig med et OCES certifikat, der på forhånd er registreret, hvorefter STS’en kan udstede et SAML security token til klienten. Med dette token kan klienten nu kalde den ønskede service – sekvensen er illustreret på nedenstående figur:



Figur : Kald af ajourføringsservice

Bemærk at security tokens kan have en lang levetid (fx 4 eller 8 timer) og caches, så efterfølgende kald til samme service ikke behøver kræve en ny interaktion med grunddata STS’en med det tilhørende overhead. Servicekaldet udføres i kontekst af klientens rettigheder, men man kan godt i kaldet overføre parametre (uden for security tokenet) som angiver, hvilken slutbruger kaldet udføres på vegne af (eksempelvis hvilken landinspektør, skal har foretaget en opdatering). Samme princip følges i øvrigt ved kald til Datafordeleren, hvis klienten skal tilgå ikke-offentlige data.

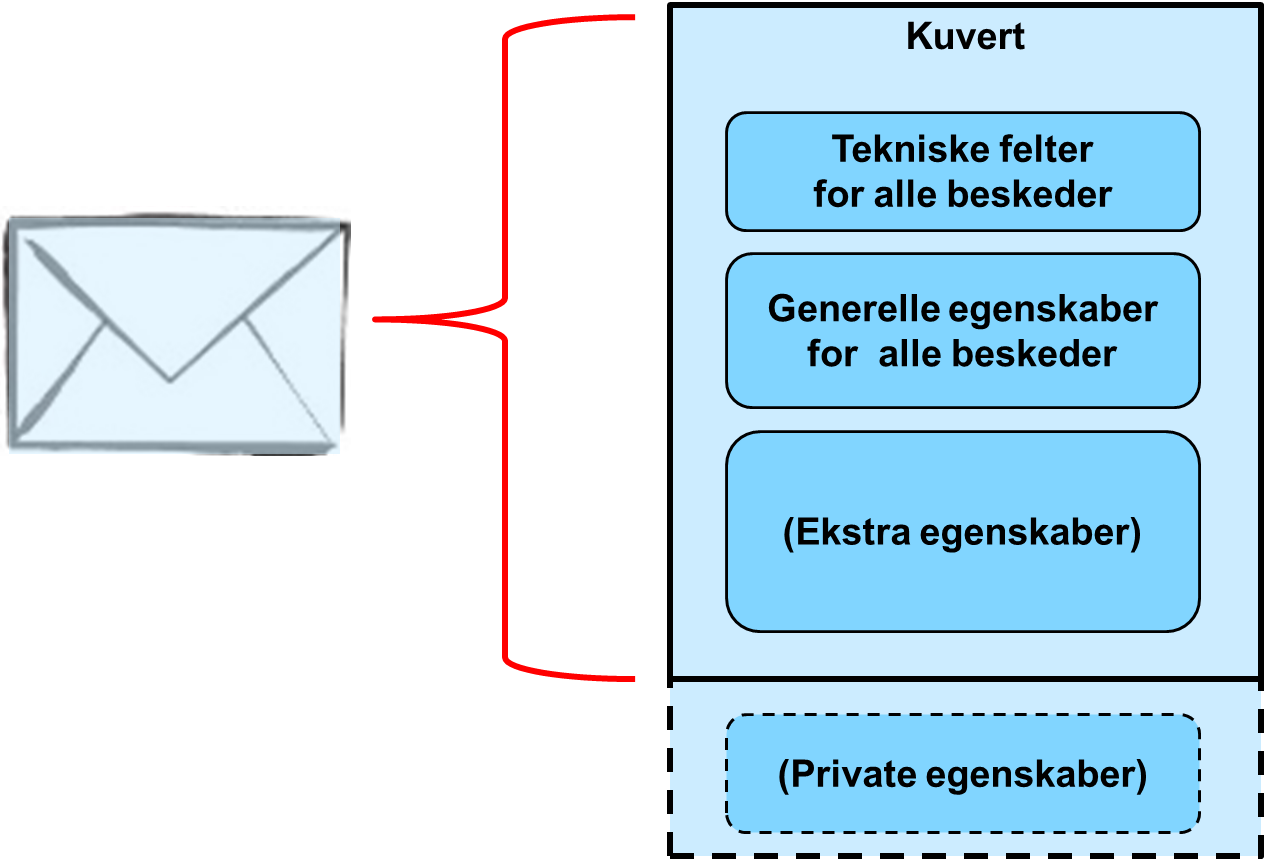
Modellen forudsætter, at de enkelte klienter på forhånd er registreret hos Grunddata STS’en med deres certifikat og de evt. systemroller, som klienterne måtte være tildelt. Her vil der være behov for en administrativ (bruger)grænseflade, hvor den enkelte serviceudbyder kan registrere sin service, angive roller som servicen forventer, og tildele roller til klienter (som ligeledes er registreret). I første fase kan administrationsgrænsefladen hos STS’en evt. undværes, og de enkelte serviceejere kan blot få oprettet klienter efter en manuel proces ved indsendelse af en formular, som angiver klient ID og roller.

### Sikkerhed på beskeder

I dette afsnit skitseres kort en sikkerhedsmodel for beskeder. Baggrunden er beslutningen om at etablere en såkaldt Beskedfordeler i regi af Datafordeleren, som skal distribuere hændelsesbeskeder, der repræsenterer forretningshændelser samt datahændelser.

Hændelsesbeskeder kan i sig selv være forretnings- eller personfølsomme, og de kan i visse tilfælde indeholde forretningsobjekter (fx ændrede data), der ligeledes skal beskyttes.

I henhold til udkastet til referencearkitektur for [EDA], forventes en hændelsesbesked at være struktureret som illustreret på figuren nedenfor:



Figur : Beskedstruktur

Nedenfor adresseres to forskellige aspekter af beskedsikkerhed:

* Sikring af beskeder under transport, herunder konfidentialitet, integritet, autentifikation af afsender og modtager.
* Adgangskontrol på beskeder – altså afgørelse af, om en given aktør må modtage (eller afsende) en besked.

Beskedsikkerheden foreslås håndteret ved brug af gængse, sikre transportprotokoller som fx SSL / TLS eller Liberty Basic SOAP Binding [SOAP Binding]. Det konkrete valg af protokol afgøres bedst under implementeringen af beskedfordeleren, men begge fordrer, at afsendere/modtagere på forhånd kan registrere X.509 certifikater til autentifikation (fx FOCES/VOCES certifikater). Uafviselighed på beskeder kan opnås ved digital signering af beskeden – fx ved brug af XML dSig standarden for digitale signaturer, som naturligt kan indlejres i XML-baserede beskeder. Beskedfordeleren skal således understøtte validering af signaturer, logning samt gensignering af beskeder.

Adgangen til at sende eller hente en besked (med PUSH/PULL) håndhæves af beskedfordeleren på dens eksterne grænseflader. I en systembrugermodel (fase 1) er det naturlige valg, at adgange til beskeder tildeles til *systemer* – dvs. afsendersystemer og modtagersystemer, som på forhånd er oprettede via en administrativ grænseflade. De pågældende systemer skal så herefter ”i andet led” foretage en adgangskontrol/håndhævelse ud mod slutbrugerne på samme måde som klienter har en lokal adgangskontrol mod deres brugere. Dette betyder ligeledes, at beskedafsendere og modtagere er ”trustede” systemer, som der på forhånd skal indgås databehandleraftaler med.

Adgangskontrollen baseres på en række oplysninger og generelle egenskaber for alle beskeder:

* Afsender/modtager-systemets identitet samt tildelte roller. Rollerne kan evt. administreres ved Grunddata STS’en og formidles til beskedfordeleren via et security token.
* Beskedens type (det forudsættes at beskeder af afsenderen opmærkes med en globalt unik type)
* Beskedens klassifikation (det forudsættes at beskeder af afsenderen opmærkes med en fælles sikkerhedsklassifikation (fx 1 - 5).
* Identifikation af kommune eller anden organisation som ejer hændelsen (kun for beskeder, hvor dette giver mening).

Fordelen ved denne tilgang er, at beskedfordeleren ikke behøver at forstå indholdet af den enkelte besked(type) for at kunne håndhæve adgangskontrollen. Omvendt er der også grænser for, hvor detaljerede adgangsregler, man kan definere – eksempelvis er det ikke muligt at foretage dataafgrænsninger indenfor en beskedtype på andet end sikkerhedsklassifikationen. I systembrugermodellen, hvor parterne er trustede, vurderes det umiddelbart, at en ”grovkornet” adgangspolitik er tilstrækkelig – men denne antagelse skal valideres i den videre proces med arkitektur for hændelsesbeskeder.

Det skal endvidere bemærkes, at opsætning af abonnementer godt kan baseres på andre typer parametre, som anvendes til filtrering af hvilke typer beskeder, et modtagersystem ønsker at modtage. Dette kunne eksempelvis være geografisk afgrænsning.

Modellen fordrer en række tiltag:

* Beskedfordeleren skal udstille en administrativ snitflade, hvor afsendere, modtagere og abonnementer kan vedligeholdes, og hvor relevant sikkerhedsinformation kan registreres som fx certifikater, tildelte roller mv.
* Der skal defineres en fælles sikkerhedsklassifikation for beskeder i grunddataprogrammet.
* Der skal defineres en fælles måde at beskrive beskedtyper og sikring af entydighed af disse.
* Der skal defineres et antal roller, som kan tildeles afsender- og modtagersystemer.
* Der skal defineres databehandleraftaler for modtagere af beskeder, som bl.a. definerer den adgangskontrol og sikkerhed, som forventes håndhævet af modtagersystemet.

Afslutningsvis skal det bemærkes, at den foreslåede sikkerhedsmodel er meget analog til den sikkerhedsmodel, KOMBIT har valgt til den fælleskommunale beskedfordeler, der udbydes som et af støttesystemerne i den fælleskommunale rammearkitektur[[3]](#footnote-4).

## Løsningsmodel fase 2 (personbrugermodel)

Den primære udvidelse i fase 2 er muligheden for personbrugeradgang dvs. web service kald udført fra en klient udføres med *brugerens* rettigheder og ikke klientens rettigheder.

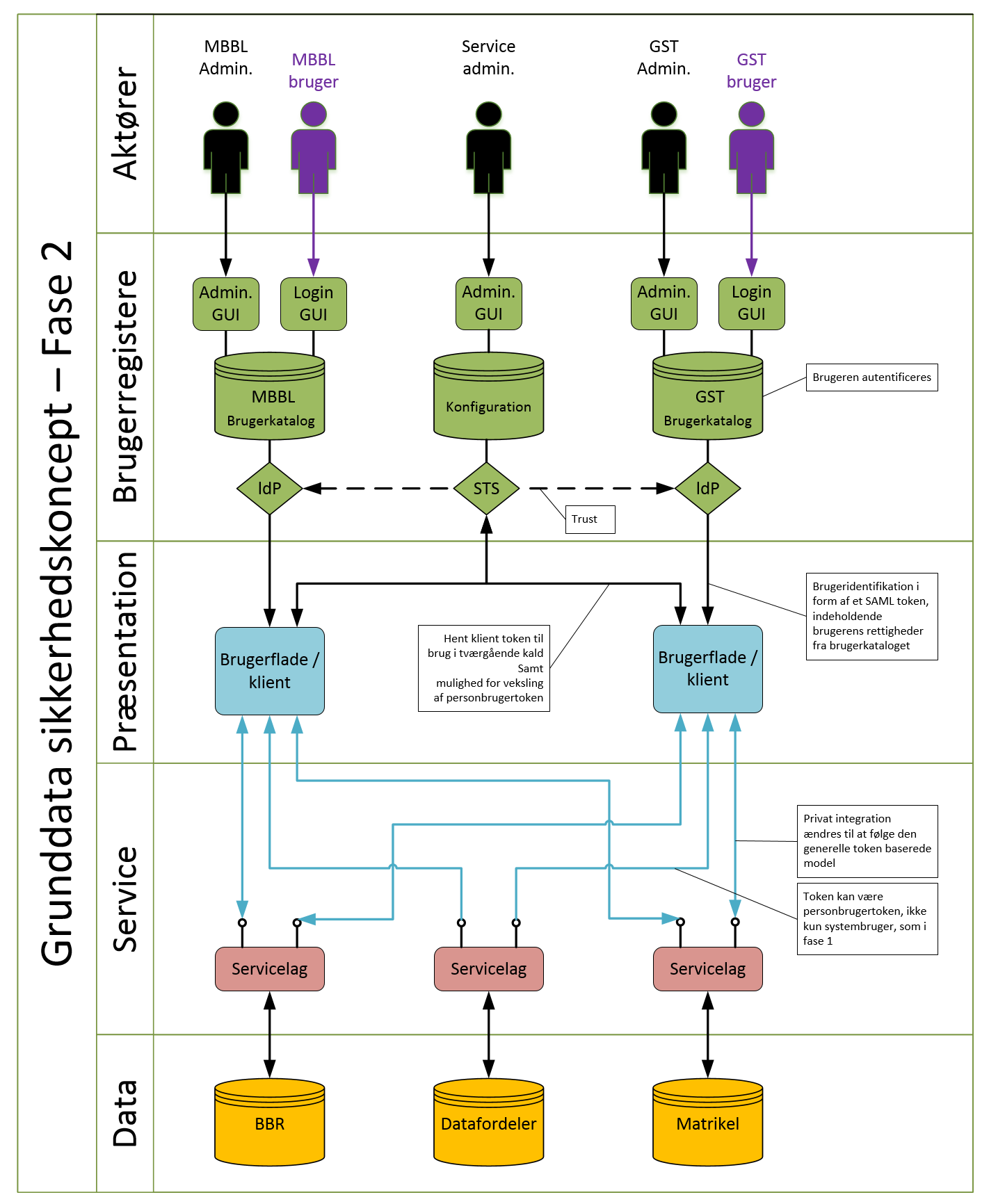
Dette betyder flg.:

* Brugere (personer) kan tildeles roller direkte til de bagvedliggende registre (udstillede ajourføringsservices).
* Grunddata STS’en kan veksle security tokens udstedt af en kendt (”trusted”) Identity Provider til nye tokens, som autoriserer klienten til at udføre kald på brugerens vegne.
* Klienterne behøver ikke længere håndhæve adgangskontrol på vegne af serviceudbydere, når kald sker på vegne af bruger. Ligeledes mindskes behovet for databehandleraftaler mellem udbydere af registre og klienter. Klienternes integration mod Grunddata STS’en forbliver stort set den samme.
* Services skal udstille nogle nye roller, som kan tildeles personbrugere. Services skal håndhæve adgangskontrol på baggrund af brugerroller (udover systemroller).
* Brugeradministratorer skal tildele nye roller til deres brugere og lade dem indgå i de tokens, som lokale Identity Provider’s udsteder.

Samtidig skal man overveje at lade de ”private” integrationer fra fase 1 (*legacy*) overgå til den token-baserede model.

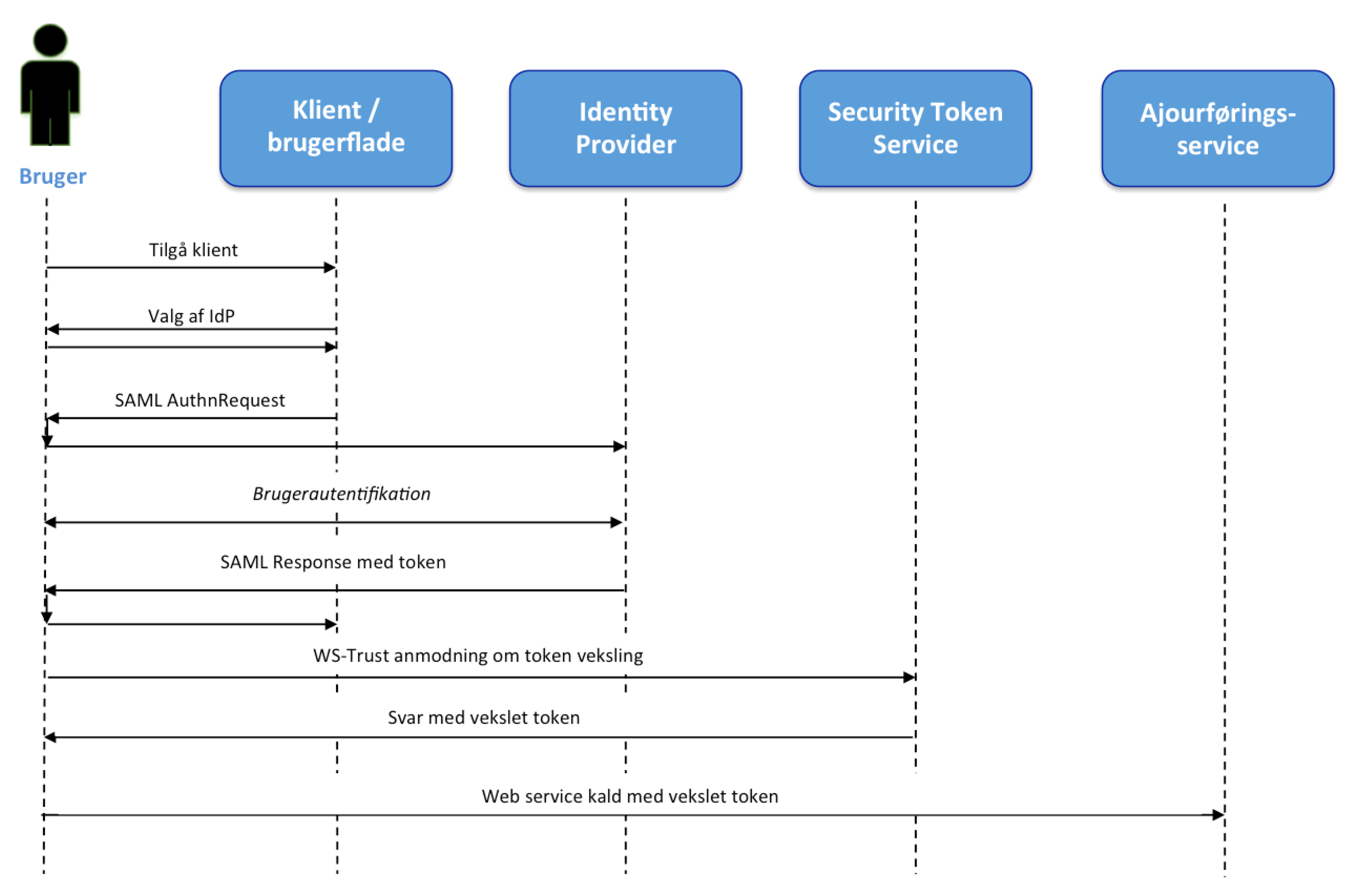
Det har ikke været muligt indenfor rammerne af nærværende arbejde at definere en sikkerhedsmodel for beskeder indenfor personbrugermodellen. Dette må derfor analyseres på et senere tidspunkt.

Modellen for fase 2 er illustreret på nedenstående figur:



Figur : Sikkerhedsmodel i fase 2

Som det fremgår af figuren, etableres der ”trust”-relationer mellem STS’er og de lokale Identity Providers, således at et brugertoken udstedt af en IdP kan veksles til et token, som klienten kan anvende på vegne af brugeren. Sekvensen i forbindelse med brugerlogin og efterfølgende web service kald på vegne af brugeren er illustreret på figuren nedenfor:



Figur : Sekvens ved tokenveksling i personbrugermodel

Som før kan security tokens caches og genanvendes indenfor deres levetid, således at ovenstående ikke udføres forud for hvert servicekald.

## Videreudviklingsmuligheder

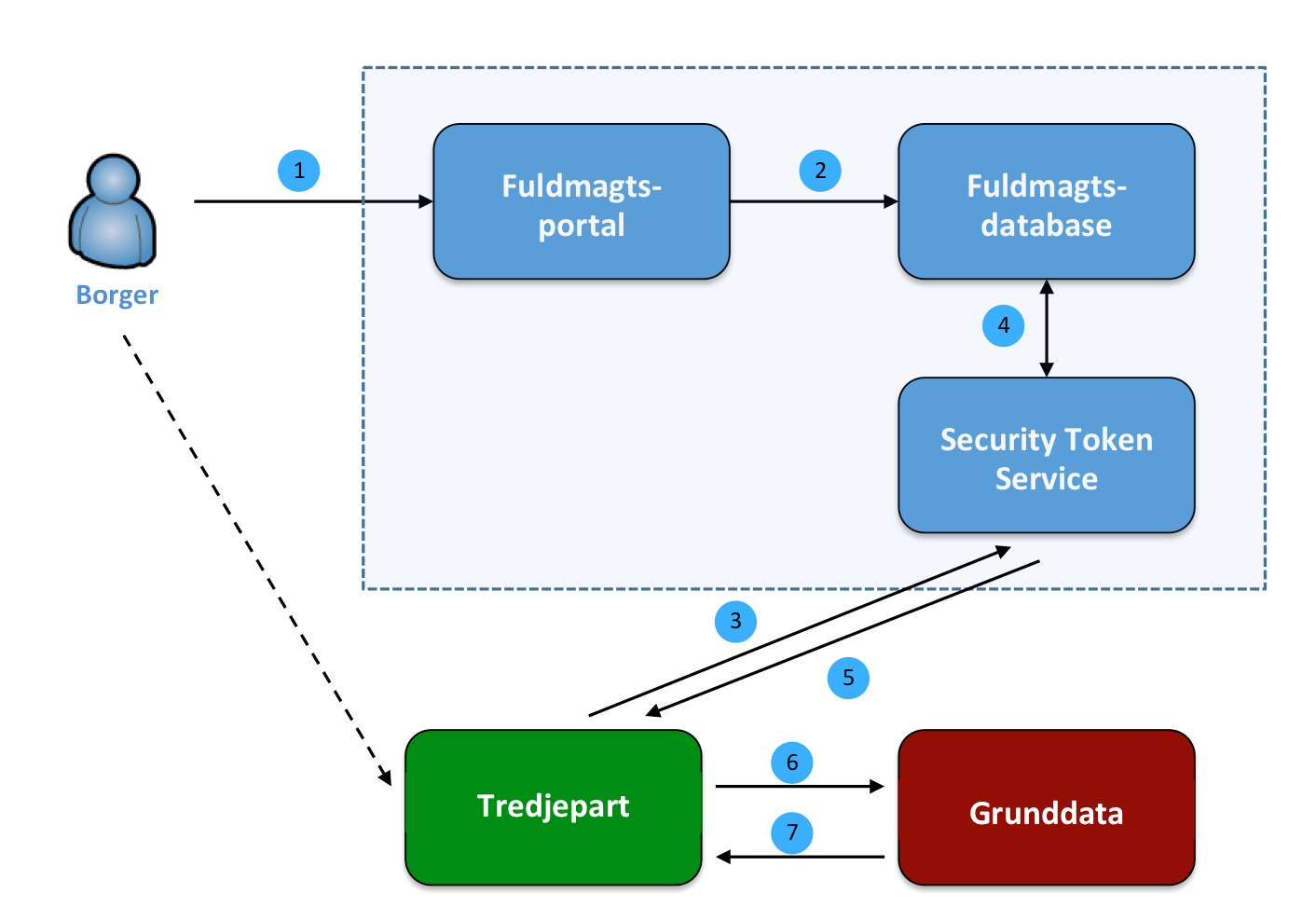
I dette afsnit beskrives kort nogle potentialer for videreudvikling af modellen, som dog ikke er kravsat nedenfor.

### Adgang til grunddata med fuldmagt

En potentiel videreudvikling af personbrugermodellen er at give ejere / borgere adgang til egne data (fx data om bygninger) direkte ved grunddataservices - herunder mulighed for at kunne udstede fuldmagter til deres data til andre personer eller systemer. En sådan funktionalitet vil kunne understøtte flg. forretningsbehov:

* Udvikling af tredjepartsklienter, som benytter brugerens grunddata på nye, innovative måder.
* Mulighed for at en borger eller virksomhed med en fuldmagt autoriserer en tredjepart (fx en bank) til at benytte vedkommendes data – fx i forbindelse med en låneansøgning.

Modellen forudsætter, at Datafordeleren samt ajourføringsservices er i stand til at operere med ”ejerforhold” samt understøtte fuldmagter i modtagne security tokens. Ligeledes forudsættes en sammenkobling af Grunddata STS’en med NemLog-in’s fuldmagtsløsning, så man kan give en fuldmagt til en tredjepart som fx en bank, som herefter kan omsættes til et security token, der kan anvendes i et web service kald.



Figur : Autorisering af tredjepart via fuldmagt

På figuren ovenfor opretter borgeren først en fuldmagt til en tredjepart via NemLog-in’s fuldmagtsløsning (fx ved at angive dennes CVR nummer). Herefter kan tredjeparten tilgå STS’en og få udstedt et security token (trin 3 – 5), der autoriserer et efterfølgende web service kald til en grunddataservice (trin 6-7).

Med en sådan model vil tredjepartsadgang til borgeres data kunne foregå på en ensartet måde (samme sikkerhedsmodel, samme protokoller) til gavn for alle anvendere og udstillere af data. En fælles model kan således nedbringe barriererne for adgang til grunddata betydeligt.

# Forslag til krav

Dette kapitel indeholder forslag til overordnede, funktionelle krav til de forskellige komponenter i sikkerhedsmodellen, som danner udgangspunkt for efterfølgende kravspecifikationer i grunddataprogrammet. Hver myndighed må udvælge de relevante krav og supplere med egne detailkrav, hvor det er nødvendigt. Dette dokument kan evt. vedlægges som informationsmateriale til leverandører, således at de får en introduktion til tankerne bag den fælles sikkerhedsmodel.

## Krav til lokale brugerkataloger og IdP’er

Dette afsnit indeholder krav til lokale brugerkataloger som fx MBBL’s myndighedsbrugere, GST’s myndighedsbrugere, og GST’s katalog med beskikkede landinspektører. Kravene går således ikke på centrale brugerkataloger og IdP’er som fx NemLog-in.

| Krav ID | Titel | Beskrivelse |
| --- | --- | --- |
| BK-1 | Lokale brugerkataloger med autentifikation | Lokale brugerkataloger, som autentificerer brugerne, skal udstilles som en Identity Provider, som kan anvendes af de respektive klienter ved brug af SAML protokollen. |
| BK-2 | Lokale brugerkataloger uden autentifikation | Lokale brugerkataloger, der kun indeholder brugerattributter og roller (men ikke tilbyder brugerautentifikation), skal udstille disse som en SAML Attribute Provider, som kan anvendes af de respektive klienter. |
| BK-3 | Indhold af tokens | Udstedte SAML tokens skal indeholde brugernes identitet samt de roller, brugeren er tildelt til den klient, der anmoder om tokenet. |
| BK-4 | Integrationer, standarder og snitflader | Identity Providers og Attribute Providers skal anvende flg. fællesoffentlige profiler af SAML standarden af hensyn til interoperabilitet:   * OIOSAML 2.0.9 Web SSO Profile * OIO Basic Privilege Profile 1.0.1 for repræsentation af roller. * Attributprofilen i appendiks B for brugere uden OCES certifikat.   Se <http://digitaliser.dk/resource/2377872> for detaljer. |
| BK-5 | Logning, sporbarhed | Identity Providers skal logge alle modtagne admodninger og svar (request / response) samt selve brugerautentifikationsprocessen (herunder afviste adgangsforsøg). Dette skal sikre sporbarhed fra brugerens log-in hos ekstern IdP til de underliggende opdateringer i grunddataregistre. |
| BK-6 | Publicere metadata | Identity Providers og Attribute Providers skal publicere deres metadata, så de er tilgængelige for anvenderne (udviklerne af klienterne). Dette skal ske som en SAML Metadatafil, som overholder kravene i OIOSAML profilen (se ovenfor). |
| BK-7 | Brugeradministration | Brugerkataloger skal udstille en administrativ grænseflade, hvormed brugerne og deres rolletildelinger kan administreres. |

Bemærk: processerne for brugeradministration samt tildeling af akkreditiver er uden for scope af dette dokument.

I fase 2 skal brugerkatalogerne overholde flg. krav:

|  |  |  |
| --- | --- | --- |
| BK-8 | Brugerroller til services | Brugere skal kunne tildeles roller direkte til grunddataservices frem for klienter. |

## Krav til klienter og serviceanvendere

Nedenstående krav er målrettet de web-baserede klienter og andre serviceanvendere i første fase af sikkerhedsmodellen:

| Krav ID | Titel | Beskrivelse |
| --- | --- | --- |
| KL-1 | Brugerautentifikation via ekstern IdP | Autentifikation af brugere skal ske via en ekstern Identity Provider med OIOSAML protokollen (se integrationskrav). Klienter bør ikke implementere egen brugerautentifikation eller brugeradministration, med mindre der er tale om ganske få brugere. |
| KL-2 | Integrationer til IdP’er | Klienter integreres med de SAML-baserede Identity Providere, som repræsenterer de brugertyper, der skal kunne logge på:   * For brugere, som logger på via NemID eller medarbejdersignatur, vil Identity Provideren være den fællesoffentlige NemLog-in løsning. * Klienter med kommunale brugere skal tilsluttes som brugervendt system til KOMBIT’s rammearkitektur for at kunne anvende KOMBIT’s Identity Provider (benævnt ”Context Handler”). * Derudover kan der være IdP’er tilknyttet lokale brugerkataloger fx med myndighedsbrugere. |
| KL-3 | IdP Discovery | Hvis klienten er integreret til mere end én Identity Provider, skal klienten ved log-in spørge brugeren, hvordan/hvor vedkommende ønsker at logge ind (valg af IdP). Klienten skal herefter tilbyde brugeren at huske valget fremover fx via en browser cookie. |
| KL-4 | Definere og udstille brugerroller | Der skal for klienten defineres et antal statiske brugerroller, som repræsenterer de adgange, brugere tildeles til klienten (RBAC). Rollerne 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 klienten.  Rollerne er specifikke for klienten og modelleres som URI’er i et for klienten lokalt namespace, som sikrer entydighed. Rollerne kobles internt til et sæt af rettigheder til funktionalitet og data i klienten.  Rollerne udstilles for brugerorganisationerne med en præcis og dækkende beskrivelse.  Roller versioneres, og de opdateres ved at oprette en ny version af roller. |
| KL-5 | Adgangskontrol | Adgangskontrol i klienten håndteres på baggrund af modtaget SAML token fra en ekstern Identity Provider indeholdende brugerens identitet samt evt. de brugerroller, brugeren er tildelt. Hvis brugerens roller findes i et brugerkatalog, der er separat for Identity Provideren (dvs. autentifikation og autorisation er de-koblede), hentes brugerens rolle fra brugerkataloget med SAML Attribute Query protokollen eller tilsvarende.  Klienter skal håndhæve adgangspolitikker på vegne af de underliggende ajourføringsservices i henhold til de indgåede databehandleraftaler. |
| KL-6 | Tværgående servicekald | Klientens kald til eksterne ajourføringsservices autentificeres med et OCES funktions- eller virksomhedscertifikat og autoriseres med et SAML token hentet fra Grunddata STS’en.  I servicekald skal der medsendes en unik ID for kaldet, som logges lokalt af klienten og kobles til en unik ID for den evt. personbruger, som kaldet udføres på vegne af. Derved vil servicekaldet kobles til brugeren ved at sammenligne servicens log med klientens log (se også logningskrav).  Bemærk: servicekald mellem eksisterende klienter og ”egne” services (fx kald fra BBR klient til BBR services) opfattes ikke som tværgående, og kan videreføres i de nuværende former. Kaldene opfattes mao. som en privat integration, der ikke behøver at følge den token-baserede model. |
| KL-7 | Logning, sporbarhed | Klienter skal logge modtagne SAML tokens (ukrypteret) fra Identity Providers samt koble en entydig brugerID på brugerens handlinger i klienten samt de web servicekald, der sker til ajourføringsservices. Dette skal sikre sporbarhed fra brugerens log-in hos ekstern IdP til de underliggende opdateringer i grunddataregistre.  Ligeledes skal tokens modtaget fra Grunddata STS logges i klar tekst. |
| KL-8 | Signering | Klienter med behov for signering skal anvende NemLog-in’s signeringstjeneste for brugere med NemID / OCES certifikat. |
| KL-9 | Fuldmagt | Klienter med behov for fuldmagter skal anvende NemLog-in’s fuldmagtsløsninger (hhv. borger- og erhvervsfuldmagt), for brugerne med NemID / OCES certifikat.  Klienter, som understøtter fuldmagter, skal ved log-in detektere, om brugeren har modtaget fuldmagt fra andre. I givet fald skal klienten spørge brugeren, om hvorvidt vedkommende ønsker at agere som sig selv eller vil anvende fuldmagt fra en af de pågældende fuldmagtsgivere. |
| KL-10 | Integrationer, standarder og snitflader | Klienten skal anvende flg. protokoller og integrationer:   * Integration til Identity Providers sker med OIOSAML 2.0.9 standarden samt OIO Basic Privilege Profile 1.0.1. Se <http://digitaliser.dk/resource/2377872> for detaljer. * Integration til Grunddata STS sker med OIO WS-Trust Profile 1.0.1 og OIO WS-Trust Deployment Profile 1.0. Se <http://digitaliser.dk/resource/526486> for detaljer. * Integration til serviceudbydere sker med Liberty Basic SOAP Binding 1.0. Se <http://digitaliser.dk/resource/526486> for detaljer. * Evt. integration til NemLog-in fuldmagtsløsning sker enten via OIOSAML eller NemLog-in’s web service grænseflade. Se <http://digitaliser.dk/fuldmagt> for detaljer. * Evt. integration til NemLog-in’s signeringstjeneste sker via grænsefladen beskrevet her: <https://test-nemlog-in.dk/Testportal/dokumenter/NemLog-in2%20-%20signing%20service.pdf> |

Bemærk at udbyderen af klienten formentlig skal indgå en (juridisk) databehandleraftale med udbydere af services, før der opnås adgang. Disse aftaler skal specificere, hvilken adgangskontrol klienten skal håndhæve på vegne af den bagvedliggende ajourføringsservice, herunder hvilke brugerroller, der giver hvilken adgang i relation til servicen.

I fase 2 skal klienterne overholde flg. krav:

|  |  |  |
| --- | --- | --- |
| KL-11 | Veksling af brugertokens | Ved kald af en web service efter personbrugermodellen, skal klienten først veksle det modtagne brugertoken fra IdP’en hos grunddata STS’en fremfor at kalde STS’en med eget certifikat som i systembrugermodellen. |
| KL-12 | Ændret adgangskontrol | I takt med at brugeradgang håndhæves i bagvedliggende services efter personbrugermodellen, skal klientens egen håndhævelse slås fra. |

### Krav til tykke klienter

For tykke klienter (ikke browser-baserede), er det ikke givet, at man kan anvende ovenstående krav. Dette gælder i reglen kun, hvis klienten er i stand til at starte en browser på brugerens PC, hvor brugeren gennemfører en log-in forløb, hvorefter den tykke klient uddrager SAML tokenet fra browseren og lukker denne.

For klienter, hvor browser-baseret log-in ikke er en mulighed, må der aftales en passende snitflade med de relevante brugerkataloger, der autentificerer brugeren. Dette kan eksempelvis være baseret på LDAP eller lignende. For brugere med et OCES certifikat, kan det være en mulighed at benytte NemLog-in’s Security Token Service i den såkaldte ”signature case” mode – dvs. hvor log-in til STS’en sker ved, at brugeren signerer requestet med sin medarbejdersignatur.

Den optimale integrationsform til brugerkataloger / IdP’er vil afhænge af de specifikke forhold, og må derfor vurderes ud fra omstændighederne.

## Krav til serviceudbydere

Nedenstående krav relaterer sig til udbydere af tværgående ajourføringsservices. Interne services behøver som nævnt ikke følge den token-baserede sikkerhedsmodel, selvom dette dog klart anbefales.

| Krav ID | Titel | Beskrivelse |
| --- | --- | --- |
| SU-1 | Adgangskontrol | Adgangskontrol på udstillede services baseres på kalderens præsentation af et SAML token (systembrugertoken) udstedt af Grunddata STS. Tokenet angiver kalderens identitet samt tildelte roller til servicen. |
| SU-2 | Validering | Kun tokens digitalt signeret af Grunddata STS’en (eller andre eksplicit godkendte STS’er) må accepteres af servicen. Der skal altså valideres op mod en white-list. |
| SU-2 | Definere og udstille systemroller | Til servicen defineres et antal statiske systemroller, som repræsenterer de adgange, klienter/serviceanvendere tildeles til servicen (RBAC). Rollerne 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 servicen.  Rollerne er specifikke for servicen og modelleres som URI’er i et for servicen lokalt namespace, som sikrer entydighed. Rollerne kobles internt til et sæt af rettigheder til funktionalitet og data i servicen.  Rollerne udstilles for serviceanvenderne med en præcis og dækkende beskrivelse.  Roller versioneres, og de opdateres ved at oprette en ny version af rollen. |
| SU-3 | Logning, sporbarhed | Serviceudbydere skal logge modtagne SAML tokens (ukrypteret) modtaget i kaldet fra serviceanvenderen samt koble en entydig identifikation af anvenderen samt servicekaldet på logningen af kaldet. Dette skal sikre sporbarhed på tværs af infrastrukturen. |
| SU-4 | Integrationer, standarder og snitflader | Serviceudbydere skal anvende flg. protokoller og integrationer:   * Services udstilles og beskyttes i henhold til Liberty Basic SOAP Binding 1.0. Se <http://digitaliser.dk/resource/526486> for detaljer. |
| SU-5 | Oprettelse hos Grunddata STS | Servicen skal registreres hos Grunddata STS’en med et sigende navn, beskrivelse, servicens certifikat samt de systemroller, anvenderne af servicen tildeles. Dette sker via de administrative grænseflader, som STS’en stiller til rådighed. |

Som nævnt forventes udbyderen af en service at indgå databehandleraftaler med alle serviceanvendere. Når en aftale med en ny anvender er indgået, tildeles anvenderen de tilhørende roller til servicen via den administrative grænseflade i Grunddata STS’en (se afsnit 5.4). Herefter vil den pågældende anvender kunne få udstedt adgangsgivende tokens med de angivne roller til servicen.

Bemærk at et konkret it-system, der optræder som serviceudbyder, også kan optræde som serviceanvender. I givet fald skal kravene i afsnit 5.2 også overholdes for denne del.

I fase 2 skal serviceudbyderne overholde flg. krav:

|  |  |  |
| --- | --- | --- |
| SU-6 | Udstilling af brugerroller | Der skal defineres og udstilles nye roller, som tildeles personbrugere. |
| SU-7 | Håndhævelse af brugerroller | Adgangskontrollen skal opdateres til at kunne tage højde for tokens udstedt efter personbrugermodellen – dvs. hvor klienten præsenterer et token indeholdende brugerroller. |

## Krav til Grunddata STS

Dette afsnit beskriver de overordnede, funktionelle krav til Grunddata STS’en i fase 1 af sikkerhedsmodellen.

| Krav ID | Titel | Beskrivelse |
| --- | --- | --- |
| STS-1 | Token-udstedelse | Grunddata STS’en skal udstille en WS-Trust baseret Security Token Service, der udsteder security tokens til klienter og serviceanvendere.  Der er flg. krav til tokenudstedelsen:   * Tokens udstedes kun, hvis serviceanvenderen på forhånd er autoriseret til den pågældende service. * Tokens er SAML 2.0 Assertions overholdende kravene i OIO SAML Profile for Identity Token Profile. Se <http://digitaliser.dk/resource/526486> for detaljer. * Tokens udstedes til en specifik service (via SAML AudienceRestriction). * Tokens bindes til serviceanvenderen (via SAML holder-of-key elementet) * Tokens indeholder de roller, som serviceanvenderen er tildelt til den pågældende service. |
| STS-2 | Autentifikation | Serviceanvendere autentificerer sig med et OCES funktions- eller virksomhedscertifikat, der på forhånd er registreret hos STS’en. |
| STS-3 | Logning, sporbarhed | Alle anmodninger og svar skal logges med entydig identifikation af anvenderen. Se krav til den administrative snitflade herunder for detaljer. |
| STS-4 | Integrationer, standarder og snitflader | Snitfladen til tokenudstedelse skal overholde:  OIO WS-Trust Profile 1.0.1 og OIO WS-Trust Deployment Profile 1.0. Se <http://digitaliser.dk/resource/526486> for detaljer. |
| STS-5 | Administrativ grænseflade | STS’en skal indeholde en administrativ grænseflade, som understøtter flg. arbejdsopgaver:   * Serviceudbydere skal kunne registrere metadata om deres service som fx navn på service, ID, certifikat, endpoint, servicens roller mv. * Serviceanvendere skal kunne registreres inkl. navn på service, ID, certifikat mv. * En serviceudbyder skal kunne tildele serviceanvendere adgang til sin service – herunder tildele dem roller til servicen. Herefter skal dette slå igennem på tokenudstedelsen. * Alle parter skal kunne udskifte certifikater rullende således at nedetid ved certifikatudløb undgås. Dette kan eksempelvis ske ved at tillade flere versioner af et certifikat per service at være oprettet. |

Der vil formentlig være behov for, at serviceanvendere og serviceudbydere skriver under på en aftale / vilkår, inden de får adgang til at anvende Grunddata STS’en. Aftalehåndtering er dog uden for rammerne af dette dokument at beskrive.

I fase 2 skal STS’en overholde flg. krav:

|  |  |  |
| --- | --- | --- |
| STS-6 | Veksling af brugertokens | Der skal udstilles en service, som klienter anvender til at veksle et ”bootstrap token” udstedt af en lokal IdP /STS til et nyt token, der autoriserer et web service kald med brugerens rettigheder.  Vekslingen skal følge modellen for identitetsbaserede web services beskrevet på Digitaliser.dk (http://digitaliser.dk/resource/526486) |
| STS-7 | Registrering af lokale IdP’er | Der skal udstilles en administrativ grænseflade til registrering og vedligehold af metadata vedrørende lokale Identity Providere, som er trustede af STS’en. Registreringen skal indeholde information om, hvilke attributter (herunder roller), som den enkelte Identity Provider må udstede i tokens, IdP’en certifikat mv. |
| STS-8 | Validering af IdP-tokens | STS’en skal validere bootstrap tokenet fra IdP’en inden veksling, herunder signaturen på tokenet, at IdP’en kun udtaler sig om egne brugere, og at den kun medsender lovlige attributter. |
| STS-9 | Registrering af serviceanvendere | Registreringen af serviceanvendere skal udvides med muligheden for at angive, om en given serviceanvender må veksle brugertokens som beskrevet ovenfor. |

## Fælleskrav

Standarder, logning, sikkerhed, navnekonvention for roller mv.

| Krav ID | Titel | Beskrivelse |
| --- | --- | --- |
| FK-1 | Anvendelse af systemroller | Systemroller til adgangsstyring i webservices skal defineres i en forretningsmæssig passende granulering, eksempelvis pr. forretningsobjekt.  Systemrollerne navngives efter følgende konvention:  CRUD\_begrænsning  Eksempelvis:   * CreateBPFG * ReadBFE * UpdateKoordinat * DeleteEjerskab |
| FK-2 | Udstilling af roller via profiler | For ikke at udstille systemrollerne, skal der oprettet systembrugerprofiler, som serviceanvendere skal tildeles, for at tilgå de udstillede services.  Systembrugerprofilerne er den eksterne repræsentation (abstraktion) af systemrollerne og vil typisk indeholde flere systemroller.  Systembrugerprofilerne sammensættes efter anvendelsesmønster.  Eksempelvis:   * BBRbruger (hos Matriklen)   + Bestående af systemrollerne:     - CreateBFE     - CreateBPFG * DARbruger (hos BBR)   + Bestående af systemrollerne:     - UpdateEnhedsAdresse     - UpdateBygningsAdgangspunkt |
| FK-3 | Navngivning af profiler | Brugerprofilerne skal overholde følgende navnekonvention:  <system><brugertype> |
| FK-4 | Miljøer | Alle komponenter i sikkerhedsmodellen skal realiseres i både et integrationstestmiljø og et produktionsmiljø.  Integrationstestmiljøet skal gøre det muligt at teste integrationer på tværs af organisationer og systemer (både til og fra komponenten). |
| FK-5 | Brugeridentifikation | Alle servicekald skal indeholde identifikation af slutbrugeren som en særskilt parameter i et web service request. Der aftales et fælles format som en del af implementeringsfasen. |

# Referencer

[DT-STÆRK-KRYPT] Stærk kryptering, Datatilsynet, http://www.datatilsynet.dk/offentlig/sikkerhed/staerk-kryptering/

[OIO-A-LEVEL] ”Vejledning vedrørende niveauer af autenticitetssikring, IT- og Telestyrelsen”. <http://digitaliser.dk/resource/363424>

[OIO-BPP] ”OIOSAML Basic Privilege Profile, Version 1.0.1”. <http://digitaliser.dk/resource/2377872>

[OIO-IDT] ”OIOSAML Profile for Identity Tokens, Version 1.0”. <http://digitaliser.dk/resource/516724>

[OIOSAML] ”OIOSAML Web SSO Profile, Version 2.0.9”. <http://digitaliser.dk/resource/2377872>

[PDL] ”Lov om behandling af personoplysninger”; Justitsministeriet. <https://www.retsinformation.dk/Forms/r0710.aspx?id=828>

[SBK] ”Sikkerhedsbekendtgørelsen”; Justitsministeriet. <https://www.retsinformation.dk/Forms/R0710.aspx?id=842>

[SOAP Binding] Liberty Basic SOAP Binding. <http://digitaliser.dk/resource/414852>

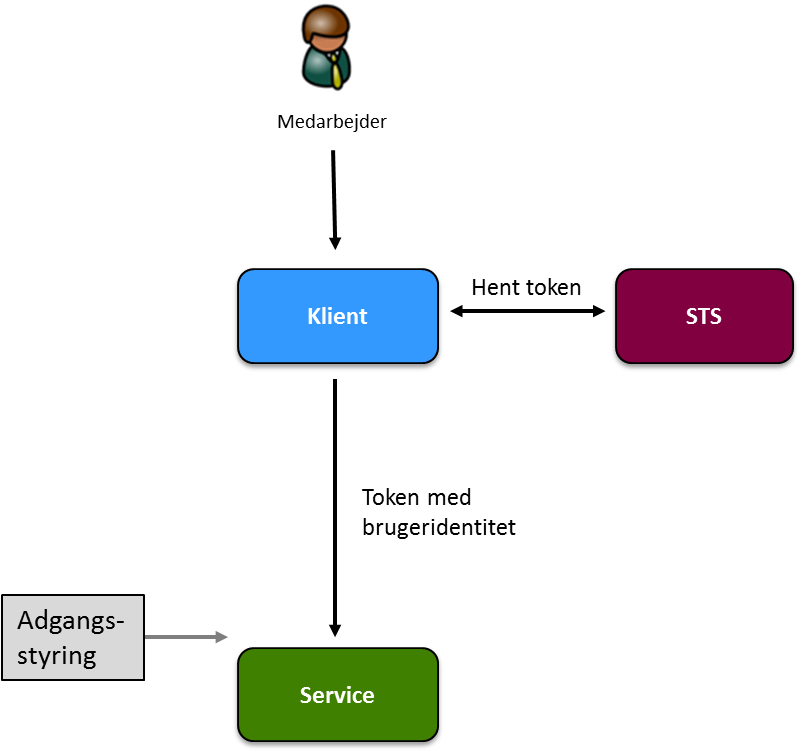
[EDA] “Referencearkitektur for håndtering af hændelser”, Version 0.4, Digitaliseringsstyrelsen.

# Appendiks A: System- og personbruger

## Model A: Adgang med personbrugere

Den første model er baseret på, at web service kaldet sker i kontekst af en personbruger. Den klient eller applikation, som betjener brugeren, skal således indhente et security token på vegne af brugeren, som præsenteres ved kaldet. Tokenet indeholder med andre ord brugerens identitet og adgangsrettigheder, og disse afgør, om klienten opnår adgang.

Modellen kaldes ofte for identitetsbaserede web services og er udbredt eksempelvis på sundhedsområdet (SOSI/DGWS) samt understøttes af NemLog-in[[4]](#footnote-5).



Figur 9: Model A: Adgang med systembruger.

**Modellen har følgende fordele:**

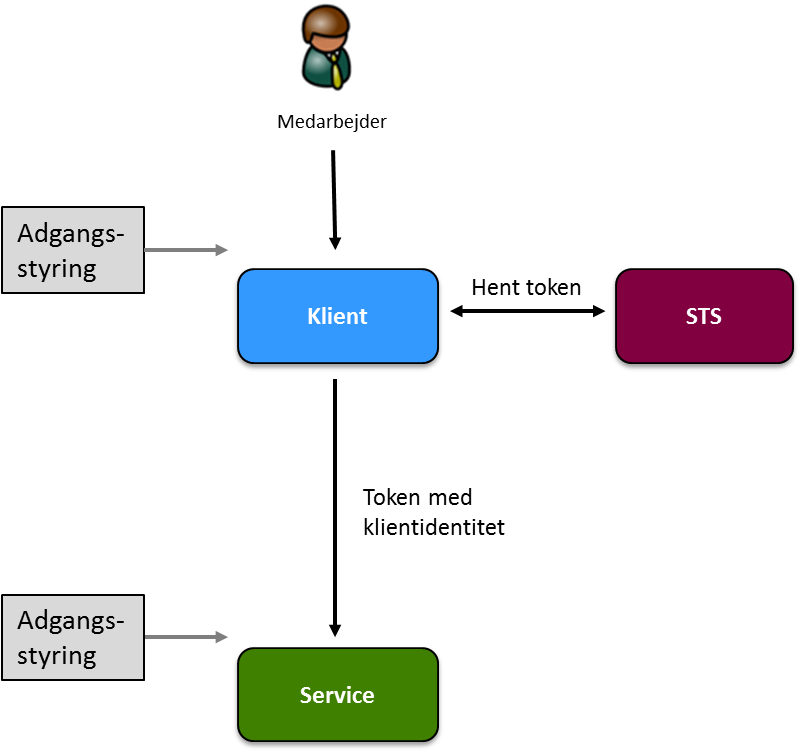
* Brugerne har de samme adgange, uanset hvilke klienter / applikationer de anvender. Dette er en fordel, hvis der er flere ”adgangsveje” til de samme bagvedliggende services.
* Det er let for servicen at dokumentere, hvem der har tilgået den. Servicen skal således blot logge de modtagne security tokens.
* Der er ikke behov for at uddelegere krav om adgangsstyring til klienter, idet håndhævelsen af adgangen alene sker i servicen. Dette er fx en fordel ved klienter som kører på mobile enheder som tablets, smart phones etc. Det er ligeledes en fordel, hvis tredjeparter skal udarbejde klienter, som skal tilgå services, uden der er mulighed for at kontrollere disse klienter (eksempelvis ved indgåelse af databehandleraftaler).

**Modellen har følgende ulemper:**

* Der skal udstedes mange tokens (ét per bruger per service), hvilket kan påvirke performance og svartider negativt. Eksempelvis bliver det vanskeligere at cache tokens, når de er unikke per bruger. Tilgængeligheden af STS for udstedelse af security tokens bliver dermed kritisk for robustheden (uden tokens ingen adgang til services).
* I brugeradministrationen skal man tildele serviceroller direkte til brugerne, hvilket kan gøre administrationen mere kompleks. Roller i det underliggende servicelag bliver således eksponeret for brugeradministrationen (direkte eller indirekte). Dette gør det samtidigt sværere at ændre eller udvikle rollemodellen.

## Model B: Adgang med systembruger

Den anden model er baseret på, at web service kaldet sker i kontekst af en systembruger. Systembrugeren modsvarer den klient eller applikation, som betjener brugeren og er tildelt sin egen adgang til de underliggende services. Klienten må nødvendigvis have en tilstrækkelig bred adgang til at kunne betjene alle sine forskellige brugere, og den udfører sin egen adgangskontrol ud mod brugerne som illustreret på figuren nedenfor:



Figur 10: Model B: Adgang med systembruger.

Modellen er anvendt i mange legacy systemer og er også valgt for web services i den fælleskommunale rammearkitektur[[5]](#footnote-6).

**Modellen har følgende fordele:**

* De enkelte services behøver normalt kun at implementere en grovkornet adgangsstyring. Den finkornede adgangsstyring foregår i klienten (mod brugerne).
* Modellen svarer umiddelbart bedst til de eksisterende sikkerhedsmodeller indenfor grunddata (fx CPR modellen, EFR).
* Modellen passer fint med paradigmet i databehandleraftaler, der er velkendt.

**Modellen har følgende ulemper:**

* Det er nødvendig at kunne stole på klienten, idet den potentielt får en bred adgang til services (og dermed data). Der skal derfor stilles en række krav til klientens sikkerhed (herunder miljøet hvor den driftsafvikles), og der skal indgås databehandleraftaler ved adgang til personoplysninger. Dette er klart en barriere for mobile klienter samt klienter, der skal udvikles af tredjeparter, som organisatorisk er langt fra udbyderne af services.
* Brugerne kan risikere at have forskellige adgangsrettigheder til de samme data og funktioner afhængigt af hvilken klient, de anvender. I disse situationer, skal der etableres mekanismer, som sikrer overensstemmelse.
* Information om hvilke personer, der har tilgået data, skal potentielt sammenstilles fra flere forskellige kilder (servicelog og klientlog).

# Appendiks B: SAML Attributprofiler

Med henblik på at sikre ensartethed og interoperabilitet på tværs af grunddataprogrammet, er det hensigtsmæssigt at standardisere indhold af security tokens (SAML Assertions).

OIOSAML profilen indeholder til formålet en OCES attributprofil, som definerer en række obligatoriske attributter for brugere, der autentificeres på baggrund af et OCES certifikat. Ligeledes indeholder OIOSAML Basic Privilege Profile en fælles måde at udtrykke roller / privilegier i SAML Assertions. Begge disse er refereret i de funktionelle krav i kapitel 5.

For brugere, der autentificeres på baggrund af et lokalt brugerkatalog (fx med brugernavn og kodeord), er der imidlertid ingen fællesoffentlig profil. Her anbefales det at tage udgangspunkt i den attributprofil for brugertokens, som KOMBIT har defineret til den fælleskommunale rammearkitektur[[6]](#footnote-7), da denne er udformet generelt nok til at dække grunddataprogrammets behov. Herunder gengives de væsentligste træk fra denne profil.

## Profil for ikke-OCES brugere

Nedenstående udgør forslag til krav vedr. SAML attributter for tokens, udstedt af lokale Identity Providere og Attribut Services, når brugeren ikke er autentificeret på baggrund af et OCES certifikat.

Alle systemer i grunddataprogrammet, som udsteder eller konsumerer brugertokens, skal overholde OIOSAML profilen [OIOSAML] af den internationale SAML 2.0 standard. Dette gælder således både regler ved udstedelse samt validering af tokens.

For indholdet af SAML tokens gælder kravene i OIOSAML afsnit 7.1 og 7.2 (”Authentication Assertion Profile”), men ikke kravene i de frivillige attributprofiler i OIOSAML kapitel 8 (”OCES attribute profile”) samt kapitel 9 (”Persistent Pseudonym Attribute Profile”). Her definerer dette afsnit i stedet kravene til de SAML attributter, der skal indlejres i tokenet.

### Krav til indhold af SAML Subject Element

Subject elementet i SAML Assertions skal entydigt identificere medarbejderen i kontekst af en organisation.

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

* Country (C) elementet skal indeholde ISO landekoden.
* Organization (O) elementet skal indeholde CVR nummeret på den organisation, som brugeren tilhører.
* Common Name (CN) elementet skal indeholde medarbejderes navn. Dette behøver ikke være unikt i sig selv.
* Serial elementet skal indeholde et ID (tekststreng), der entydigt identificerer brugeren / medarbejderen indenfor organisationen.

Formatattributten på <NameID> elementet skal sættes til urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName.

Elementerne i Subject DN skal separeres med komma, og der må ikke være white space mellem elementer.

Nedenstående udgør et eksempel på et Subject Element i henhold til ovenstående krav:

<saml:Subject>

<saml:NameID

Format=”urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName”>

**C=DK,O=20688092,CN=Hans Jensen,Serial=123abc456**

</saml:NameID>

<saml:SubjectConfirmation

Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">

<saml:SubjectConfirmationData

Recipient="https://abc\_myndighed.dk/klient\_xyz"

NotOnOrAfter="2013-12-31T12:00:00"

InResponseTo=”Authn\_request\_identifier\_1234567”>

</saml:SubjectConfirmationData>

</saml:SubjectConfirmation>

</saml:Subject>

Bemærk at Recipient URI’en i ovenstående eksempel er fiktiv.

### Krav til indhold af kerneattributter

Elementet <AttributeStatement> skal overholde indkodningsreglerne for attributter beskrevet i [OIOSAML] afsnit 7.2. Desuden skal elementet indeholde nedenstående kerneattributter beskrevet i [OIOSAML] afsnit 7.3:

* AssuranceLevel – en klassifikation af, hvor stærkt brugeren aktuelt er autentificeret (1-4) af Identity Provideren. Klassifikationen af AssuranceLevel skal følge [OIO-A-LEVEL].
* SpecVer – angivelse af hvilken version af OIOSAML, der er anvendt ved udstedelse af tokenet.

Bemærk: De øvrige kerneattributter beskrevet i OIOSAML er ikke obligatoriske i denne attributprofil.

Bemærk at den enkelte Identity Provider som følge af kravet er nødt til at klassificere det AssuranceLevel, som modsvarer styrken af den autentifikation, der foretages af brugeren – samt indlejre værdien som en attribut i udstedte tokens. I vurderingen må man tage højde for både den tekniske styrke af autentifikationsmekanismen (fx kodeord, digital signatur etc.), relaterede tekniske kontroller (fx passwordpolitik, begrænsning af log-in til interne netværk etc.) men også for de organisatoriske procedurer, der er etableret til den indledende identifikation af brugeren (indrullering). Se [OIO-A-LEVEL] for detaljer.

### Krav til AudienceRestriction

Elementet <AudienceRestriction> i den udstedte SAML Assertion sættes til EntityID for klienten.

### Krav til repræsentation af roller

Bruger- og systemroller repræsenteres ved URI’er i et namespace lokalt for den organisation, der har defineret dem.

Nedenstående ses (fiktive) eksempler på URI’er for en brugerrolle i henhold til ovenstående:

* <http://KorsbækKommune.dk/roller/socialforvaltningen/sagsbehandler>
* urn:dk:korsbækkommune:roller:socialforvaltningen:sagsbehandler

Bemærk at disse URI’er alene opfattes som identifiers, og at deres indhold i denne sammenhæng ikke er informationsbærende.

Brugerroller indkodes som privilegier i det udstedte SAML token i henhold til OIOSAML Basic Privilege Profile [OIO-BPP]. I Scope attributten på privilegiet sættes CVR nummeret for brugerens organisation.

1. Se Appendiks A for en beskrivelse af principperne bag disse modeller. [↑](#footnote-ref-2)
2. Valget kan herefter evt. huskes via en browser cookie, så brugeren ikke behøver at angive dette mere. [↑](#footnote-ref-3)
3. http://www.kombit.dk/sts [↑](#footnote-ref-4)
4. http://digitaliser.dk/resource/526486 [↑](#footnote-ref-5)
5. Iflg. de udkast til kravspecifikation, som foreligger på KOMBIT’s hjemmeside. [↑](#footnote-ref-6)
6. Denne findes i ”Underbilag 2.4 Sikkerhed, Appendiks A” i udbudsmaterialet for de fælleskommunale støttesystemer. Se <http://www.kombit.dk/sts> for detaljer. [↑](#footnote-ref-7)