2021-02-02

Målarkitektur for sammenhængende brugerstyring transition 1: Overgang til MitID og NemLog-in3

Oversigt over ændringer i den nationale infrastruktur på sundhedsområdet ved overgang til MitID og NemLogin 3

Arbejdsdokument-version 0.3.9

SUNDHEDSDATA-
STYRELSEN

SUNDHEDSDATA-
STYRELSEN

Versionslog

Version	Dato	Forfatter	Beskrivelse
0.1	20.3.2020	KMMO	Første udgave
0.2	24.3.2020	HEBL	
0.3	21/4 2020	KMMO	Indarbejdet kommentarer fra HEBL. Ændret titel, beskrevet baseline, tilføjet logisk model m/ redegørelse for realisering, beskrevet faseopdelt målarkitektur, præciseret og udbygget transition 1-modeller. Redaktionelle ændringer
0.3.1	2020-04-28	KMMO	Udbygget yderligere
0.3.2	2020-05-01	KMMO	Kommentarer fra CHG (baseline) indarbejdet
0.3.3	2020-05-20	KMMO	Opdateret efter review med HEBL og EAD
0.3.3.1	2020-06-02	KMMO	Uddybet. Skilt baseline og transition 1 ud i to selvstændige afsnit
0.3.4	2020-07-02	KMMO	Opdateret efter review med Jacob Qvortrup/Arosii
0.3.5	2020-09-10	SMI	Kapitel 7 vedrørende applikationsarkitektur indsat
0.3.6	2020-10-01	SMI	Kapitel 7 klar til første interne review
0.3.7	2020-11-02	SMI	Kapitel 5, 6 og 7 revideret
0.3.8	2020-11-19	SMI	Kapitel 5, 6 og 7 justeret i henhold til review den 17. nov. 2020
0.3.9	2020-12-22	SMI	Borgerscenarier opdateret i kapitel 6 og SOSI-STS grænseflader målrettet borger i kapitel 7
0.3.10	2021-02-02	SMI	Kapitel 6 revudereret pba. review

SUNDHEDSDATA-
STYRELSEN

Indholdsfortegnelse

1. Problem

Bemærk: Dette dokument er et arbejdsdokument og ændring samt tilføjelser må fortsat forventes.

Den nationale infrastruktur på sundhedsområdet skal tilrettes i forbindelse med overgang til MitID og NemLogin 3. Denne tilretning udgør første skridt i realiseringen af målbilledet for sammenhængende brugerstyring [Målbillede brugerstyring]. Dette dokument opstiller en konkret målarkitektur, som tjener som dialogværktøj og som udgangspunkt for opgavespecificering.

2. Baggrund

Målbilledet for sammenhængende brugerstyring på sundhedsområdet [Målbillede brugerstyring] blev udarbejdet i samarbejde mellem SDS og parterne på sundhedsområdet og tiltrådt af RUSA i december 2019.

Målbilledet danner rammen for det videre arbejde med brugerstyringsløsninger på sundhedsområdet. Det beskriver, hvordan en national føderation på sundhedsområdet kan etableres med sammenhæng til fællesoffentlig samt til regionale og kommunale føderationer, blandt andet med henblik på at understøtte overgangen til MitID og NemLog-in 3.

De fællesoffentlige løsninger NemID og Nemlog-in 2 erstattes i løbet af 2020-2021 af MitID og NemLog-in3(NL3). Samtidig med dette erstattes den nuværende OCES2-certifikatløsning af en ny OCES3-løsning, hvilket blandt andet indebærer ophør af central verifikation af MOCES-certifikater. Endelig vil der med overgangen til NemLog_in3 ske en overgang til NSIS fra NIST som grundlag for trust i den fællesoffentlige føderation. Ændringerne i de fællesoffentlige løsninger medfører et behov for en række ændringer i den nationale infrastruktur for sundhedsområdet samt hos parterne.

2.1 Parternes tre løsningsscenarier

Der er opstillet tre overordnede løsningsscenarier for parternes overgang til MitID og Nemlogin 3:

1. MitID-scenarie: Anvendelse af MitID Erhverv som identifikationsmiddel
2. Certifikatscenarie: Anvendelse af MOCES som identifikationsmiddel
3. Føderationsscenarie: Anvendelse af egne identifikationsmidler

MitID-scenariet forventes først og fremmest at blive anvendt af mindre private aktører. Blandt de regionale og kommunale parter er der et ønske om at bevæge sig i en føderal retning, som også beskrevet i [Målbillede brugerstyring]. Dette understøttes i føderationsscenariet. Der er flere parter, som har udtrykt ønske om at kunne fortsætte anvendelsen af MOCES-certifikater i en periode fremover, hvilket understøttes i certifikatscenariet.

2.2 Formål

Målarkitekturen tjener to formål: dels skal den vejlede SDS i forbindelse med udvikling af den nationale infrastruktur på sundhedsområdet. I denne sammenhæng er arkitekturen konkretiseret og løsningsanvisende til et niveau, så den danner udgangspunkt for kravspecificering af de nødvendige og tilstrækkelige udviklingsopgaver. Dels skal den vejlede parterne i deres arbejde med at forberede egne løsninger. I den sammenhæng bidrager målarkitekturen til at identificere nødvendige udviklingstiltag, mens en konkretisering af disse naturligt ligger hos parterne.

2.3 Rammer og afgrænsning

Målarkitekturen for sammenhængende brugerstyring er udarbejdet i forlængelse af målbilledet for sammenhængende brugerstyring [Målbillede brugerstyring]. Målarkitekturen fokus ligger på applikationsdelen og informationsdelen, og konkretiserer de i målbilledet definerede informationsobjekter, applikationskomponenter samt flows og relationer. Målarkitekturen har desuden enkelte afstikkere til teknologilaget.

Målarkitekturen beskæftiger sig ikke med governance, supportbehov eller nonfunktionelle emner såsom skaleringsbehov, tilgængelighedskrav med videre forbundet med de applikationskomponenter, som arkitekturen baserer sig på, men tager det som en forudsætning, at disse tilgodeses i den respektive systemforvaltning.

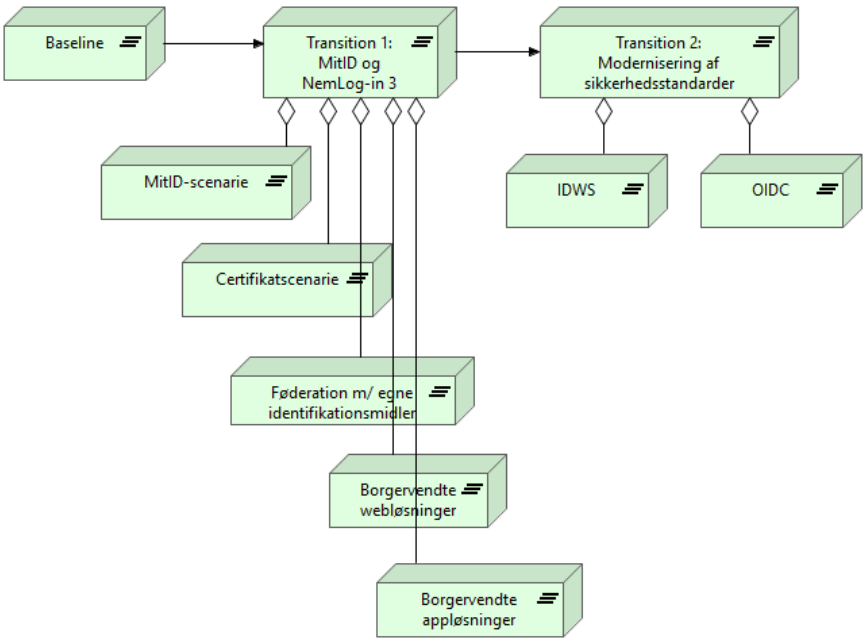
Overgangen til MitID og NemLog-in3 er en opgave, som kræver betydelige ressourcer blandt alle parter på sundhedsområdet. Målarkitekturen er derfor inddelt i transitioner, som er afgrænset ud fra et ønske om at fokusere på nødvendige tiltag af hensyn til MitID og NemLog-in3. Parternes overgang til føderale løsninger forventes på kortere sigt kun at blive delvist realiseret, og målarkitekturen for den nationale infrastruktur på sundhedsområdet vil i denne version alene blive konkretiseret i forhold til føderale løsninger ud fra parternes ambitioner på kortere sigt. Ligeledes vil ændringer som følger af strategiens mål om at modernisere sikkerhedsstandarder [Strategi] først blive konkretiseret i efterfølgende versioner af målarkitekturen.

Ud fra ovenstående følger blandt andet, at SOSI ID-kort i første omgang fastholdes hvor det er muligt, i det det forventes, at parternes løsninger dermed påvirkes mindst muligt.

3. Transitionsarkitekturer

Realisering af målbilledet for sammenhængende brugerstyring vil strække sig over en årrække fremover, og vil derfor skulle gennemføres i en række transitioner. Sikkerhedsområdet står over for to større ændringer som hver især kan tjene som motor for velafgrænsede indsatser i realisering af målbilledet. Den første af disse udgøres af overgangen til MitID og Nemlog_in3, mens den anden omfatter den planlagte modernisering af sikkerhedsstandarder på sundhedsområdet, herunder indførelse af IDWS som erstatning for DGWS.

Det vurderes, at en samtidig gennemførelse af disse to tiltag vil indebære en uhensigtsmæssig høj risiko for parterne på sundhedsområdet, dels som følge af de samlede påvirkninger, som en parallel implementering vil medføre og dels i lyset af tidshorisont for og kritikaliteten af overgangen til MitID. SDS har på den baggrund besluttet at lade overgang til MitID og modernisering af sikkerhedsstandarder udgøre henholdsvis første transition og anden transition i realisering af målbilledet, jævnfør Figur 1: Målarkitektur for sammenhængende brugerstyring, overordnede faser. Denne beslutning indebærer en fastholdelse SOSI-kortet som identitetsbevis og adgangsbillet til nationale sundhedstjenester, og er ydermere båret af en forventning om, at der dermed opnås mindst mulig påvirkning de eksisterende flows og dermed af parternes systemporteføljе i første transition. Transition 1 er desuden nedbrudt i de tre ovenfor listede scenarier, henholdsvis MitID-scenariet, certifikatscenariet og det føderale scenarie med egne identifikationsmidler samt med borgervendte løsninger.



Figur 1: Målarkitektur for sammenhængende brugerstyring, overordnede faser

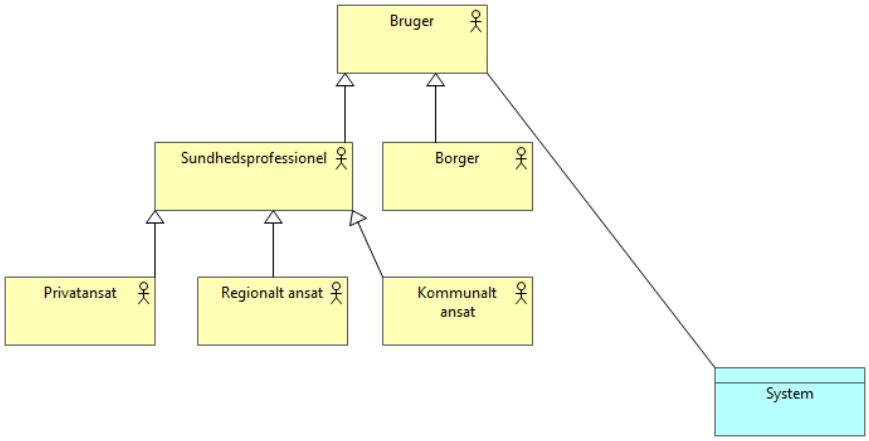
Som det fremgår af titlen, beskriver dette dokument først og fremmest første transition med henblik på at forberede den nationale infrastruktur til overgangen til MitID og NemLog-in 3. Nedbrydning og uddybning af efterfølgende transitioner udarbejdes senere.

4. Logisk model

I dette afsnit introduceres de overordnede logiske elementer i målarkitekturen.

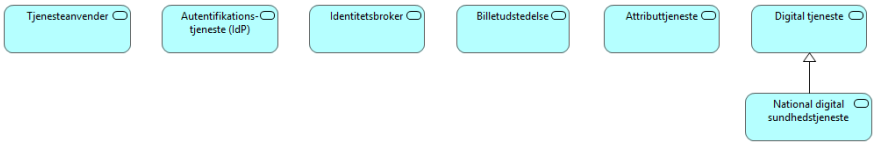
4.1 Brugere

Forretningsmæssigt skelnes der mellem to typer af brugere: sundhedsprofessionelle og borgere. For de sundhedsprofessionelle skelnes der på ansættelsessted. Desuden kan et system i visse situationer optræde som en særlig bruger (teknisk bruger).



Figur 2: Brugere

Følgende viser de centrale logiske applikationskomponenter:



Figur 3: De centrale logiske applikationskomponenter

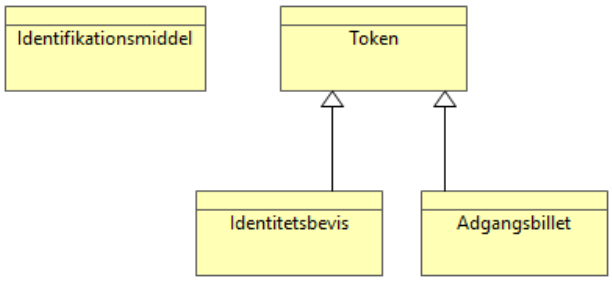
De enkelte komponenter er beskrevet i nedenstående tabel:

Komponent	Beskrivelse
Tjenesteanvender	Den klient, som brugeren anvender til at få adgang til den digitale tjeneste [DIGST 2020]
Autentifikationstjeneste	Tillidstjeneste, der udfører autentifikation af digitale identiteter [DIGST 2020]. I den fremtidige fællesoffentlige infrastruktur er MidID autentifikationstjeneste
Identitetsbroker	Tillidstjeneste som formidler en digital identitet til tredjeparter på baggrund af en autentifikation verificeret af brokeren selv eller evt. af en anden tredjepart [DIGST 2020]. I den fremtidige fællesoffentlige infrastruktur vil NemLog-in 3 være identitetsbroker for MitID
Billetudstedelse	Proces hvor en adgangsbillet udstedes til brugeren på baggrund af autentikation og attestation [DIGST 2020]

Komponent	Beskrivelse
Attributtjeneste	Tillidstjeneste, der muliggør registrering og/eller attestation af attributter [DIGST 2020]. Bemærk, at der i denne transition, foruden de ændringer som følger af MitID og NemLog-in3-overgangen, ikke ændres ved attributkilder, og det alene er berørte attributkilder, som foldes ud i denne version af arkitekturen.
National digital sundhedstjeneste	Digital sundhedstjeneste udstillet i Den nationale føderation for sundhedsområdet [SDS 2020]. Bemærk, at arkitekturen beskæftiger sig med adgang til nationale digitale sundhedstjenester jævnfør målbilledet, derfor specialiseringen.

Tabel 1: Beskrivelse af de logiske applikationskomponenter

Nedenfor ses de logiske informationsobjekter tokens og identifikationsmidler:



Figur 4: De centrale logiske informationsobjekter

De logiske informationsobjekter beskrives kort i nedenstående tabel:

Komponent	Beskrivelse
Identifikationsmiddel	Middel som en entitet får udstedt til brug for autentifikation og som benytter en eller flere autentifikationsfaktorer [DIGST 2020]
Token	Samlebegreb for identitetsbeviser og adgangsbilletter [SDS 2020]
Identitetsbevis	Et elektronisk objekt, der dokumenterer en brugers identitet. Identitetsbeviset kan anvendes overfor en billettjeneste til at få udstedt adgangsbilletter til tjenester [SDS 2020]
Adgangsbillet	Beskyttet elektronisk objekt udstedt af tillidstjeneste, der beskriver en digital identitets attributter og som giver adgang til en forretningstjeneste [DIGST 2020]

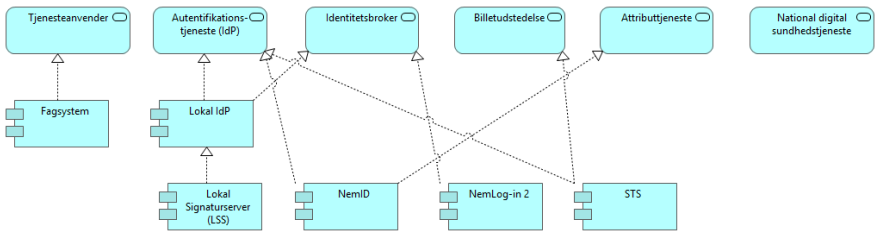
Tabel 2: Beskrivelse af de logiske informationsobjekter

5. Baseline

5.1 Ansattes adgang via rig klient

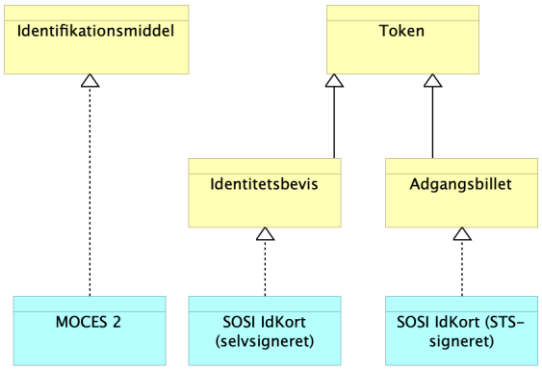
5.1.1 Komponentrealisering

Nedenstående viser de konkrete realiseringer af logiske komponenter:



Figur 5: Realisering af logiske applikationskomponenter

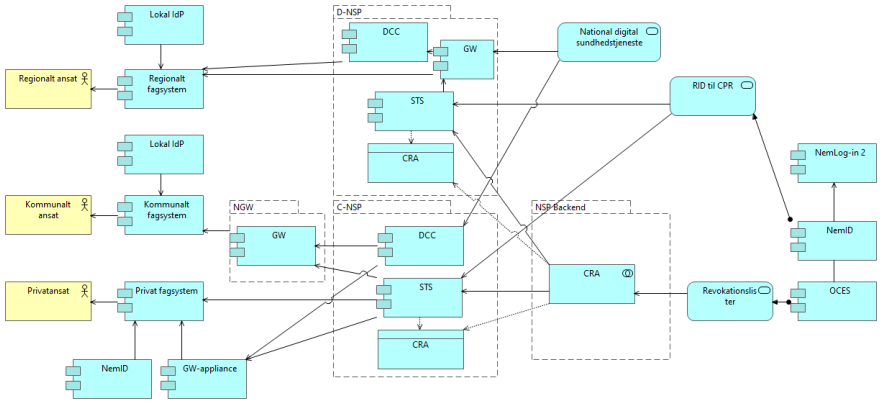
De lokale IdP'er udgøres for regioners og kommuners vedkommende typisk af lokale signaturservere. Private aktører anvender OCES-nøglefiler, og autentificerer sig op mod NemID.



Figur 6: Nuværende realisering af de centrale logiske objekter

5.1.2 Statiske sammenhænge

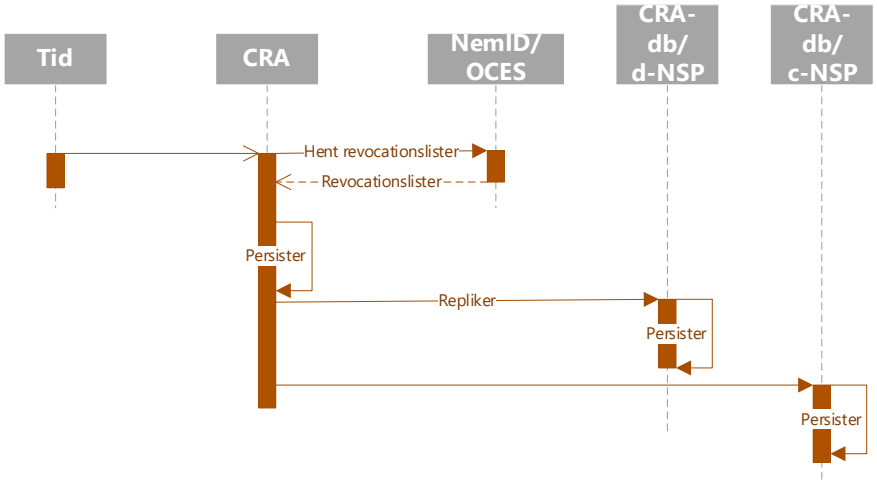
Nedenstående model viser sammenhængende mellem komponenterne i forhold til det kommunale domæne, det regionale domæne og det private domæne. Systemerne inden for det kommunale domæne interfacer med et særligt miljø, betegnet NGW. De private aktører tilgår for de flestes vedkommende STS direkte. Dog har nogle EOJ-leverandører selv installeret en GW i egen infrastruktur, en såkaldt NSP-GW-appliance, der anvendes i forbindelse med nogle private plejehjem. På det regionale område er det oprindelige mønster, at der kaldes gennem DCC. Dette mønster er ved at blive omlagt, således at også regionerne interfacer med GW.



Figur 7: Nuværende applikationslandskab med serving relations.

5.1.3 Flow ved opdatering af CRL

CRL opdateres som en forudsætning for at kunne verificere certifikater. Opdateringen foretages af CRA ud fra en tidsgivet event. Pt opdateres hvert 30. minut.



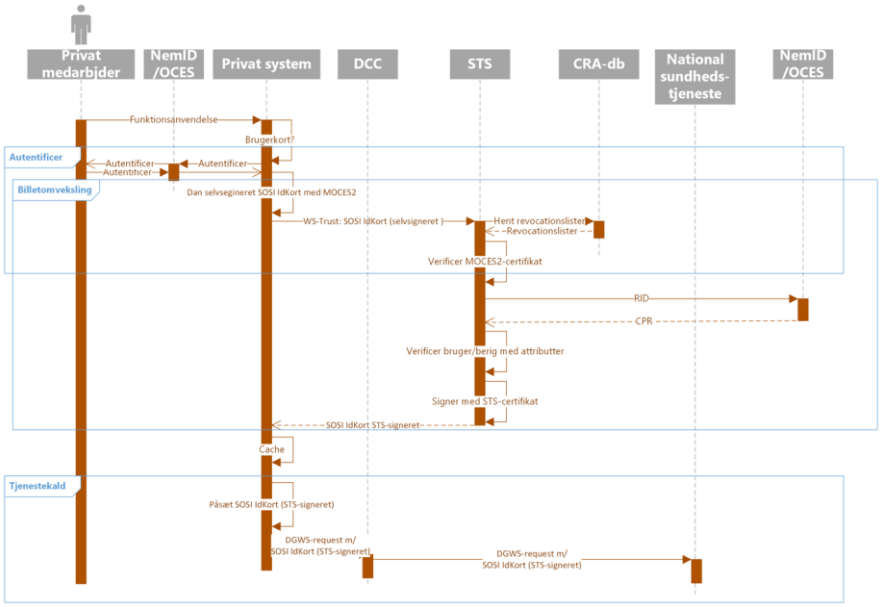
Figur 8: Batchvis opdatering af CRL

5.1.4 Autentifikationsflow

Autentifikationsflows vises henholdsvis for parter, der cacher SOSI-kort i eget system og parter, som anvender SOSI-GW til caching af SOSI-kort.

5.1.4.1 Autentifikationsflow uden SOSI-GW

Herunder vises autentifikationsflow for systemer med lokal caching af SOSI-kort.



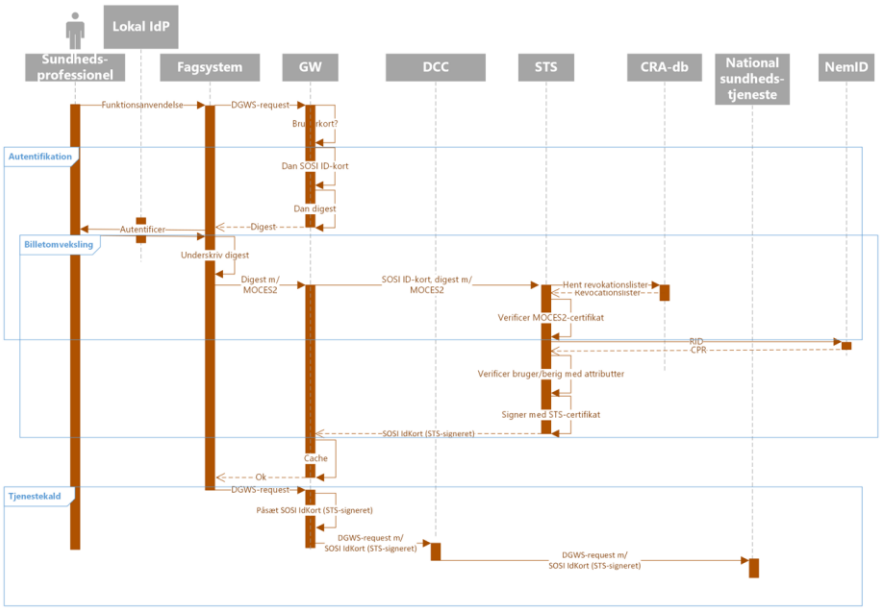
Figur 9: Autentifikationsflow fra systemer med lokal caching af SOSI-kort

5.1.4.2 Autentifikationsflow gennem SOSI-GW

Dette flow anvendes af regionale og kommunale parter samt af de private parter, som anvender en NSP-GW-appliance. Som ovenfor beskrevet, går nogle af de regionale parter igennem DCC inden de rammer SOSI-GW. Denne variant er ikke vist forneden.

Autentifikationsflowet baserer sig på, at brugerens SOSI-kort (STS-signeret) caches i SOSI-gateway i forbindelse med autentifikation. Kortet caches i GW, og vil genanvendes ved senere kald, så længe der er et gyldigt kort. Kortet har i dag en maksimal gyldighed på 24 timer, og de enkelte sundhedstjenester kan sætte yderligere krav (eksempelvis opererer FMK med gyldighed på ni timer), i hvilket fald der skal ske en genautentifikation

Autentifikation kan ske eksplicit ved at man forud for et tjenestekald forespørger på, om der findes et gyldigt SOSI-kort, og ellers får det dannet, eller det kan ske implicit ved at fagsystemet kalder en tjeneste, og givet at der ikke findes et kort får et digest tilbage, som fagsystemet dernæst anvender i et autentifikationsflow forud for, at tjenestekaldet gentages. Nedenfor vises det implicitte flow.



Figur 10: Autentifikationsflow for rige klienter med anvendelse af SOSI-GW

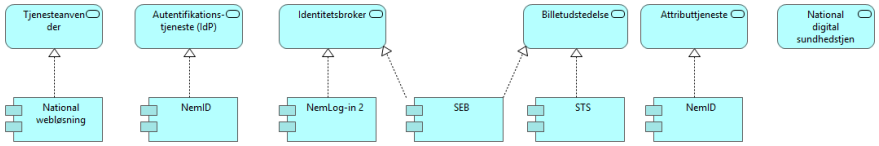
5.2 Ansattes adgang via browser

I dette afsnit beskrives ansattes adgang til nationale webløsninger via brugerens browser direkte fra brugerens enhed. For beskrivelse af browseradgang via brugerens fagsystem, såkaldt sikker browseropstart, se afsnit 5.3. De nationale webløsninger udgøres pt. af sundhed.dk, fmk-online, sårjournalen og FUT. Herunder gennemgås først sundhed.dk og fmk-online samlet og dernæst sårjournalen og FUT samlet.

5.2.1 Sundhed.dk og fmk-online

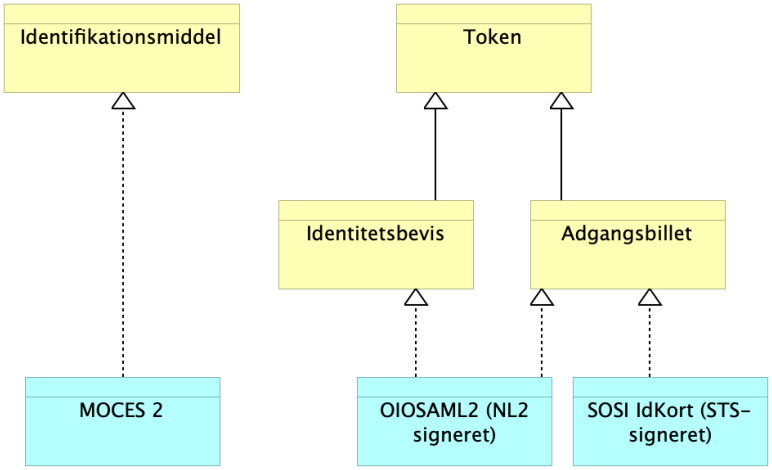
5.2.1.1 Komponentrealisering

Realisering af applikationskomponenter:



Figur 11: Realisering af applikationskomponenter

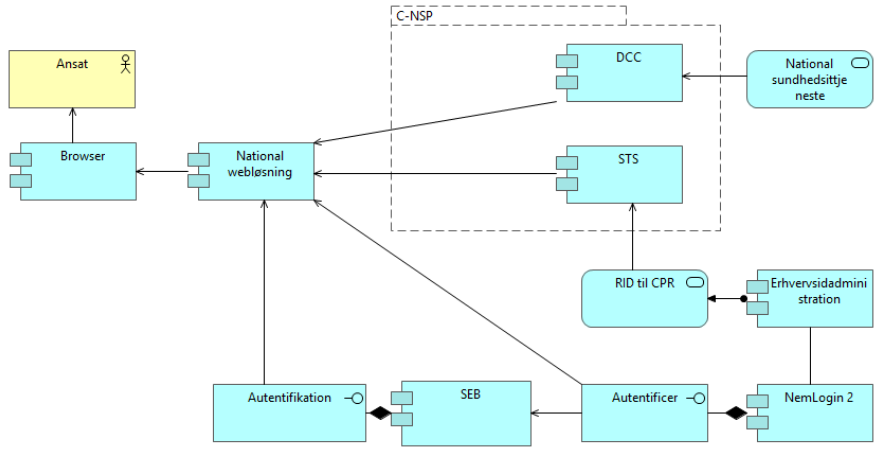
Realisering af informationsobjekter



Figur 12: Realisering af informationsobjekter

5.2.1.2 Statiske sammenhænge

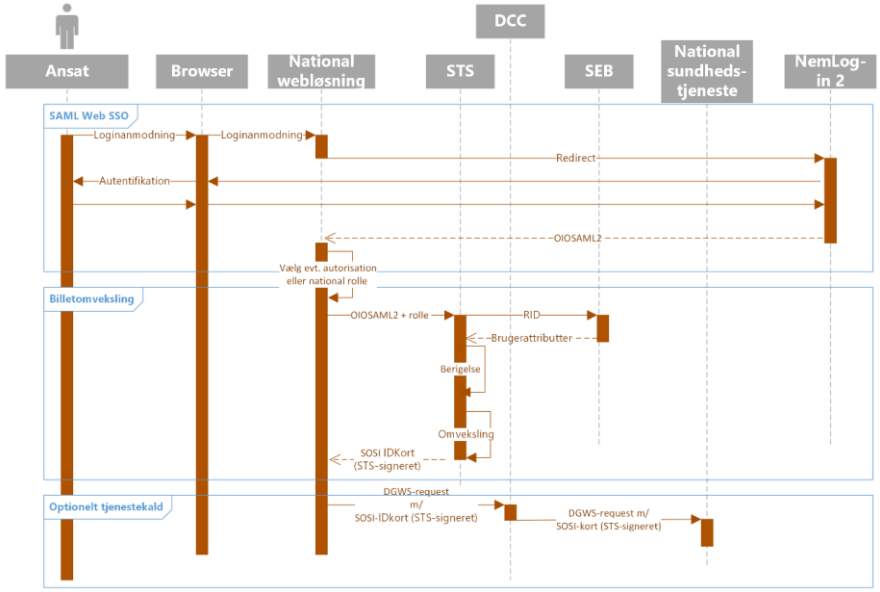
Nedenstående figur viser de statiske sammenhænge for browseradgang via nationale webløsninger. Bemærk, at både sundhed.dk og fmk-online tilgår NemLogin direkte. Begge systemer anvender STS direkte uden om GW. FUT og Sårjournalen anvender SEB.



Figur 13: Statiske sammenhænge for baselinekomponenter

5.2.1.3 Autentifikationsflow

Nedenfor vises autentifikationsflowet for en ansat, som tilgår en national webløsning. Flowet omfatter også kald til bagvedliggende nationale sundhedstjenester, som den nationale webløsning kalder på vegne af brugeren. Den første del af flowet er et standard SAML SSO Web-autentifikationsflow.

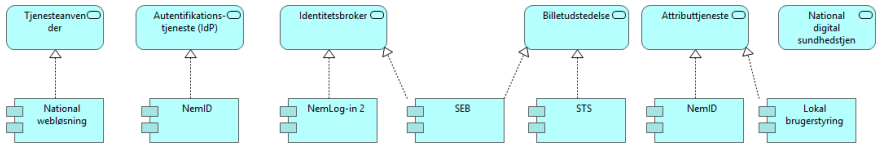


Figur 14: Autentifikationsflow for ansatte med adgang til national webløsning via browser.

5.2.2 Sårjournalen og FUT

5.2.2.1 Komponentrealisering

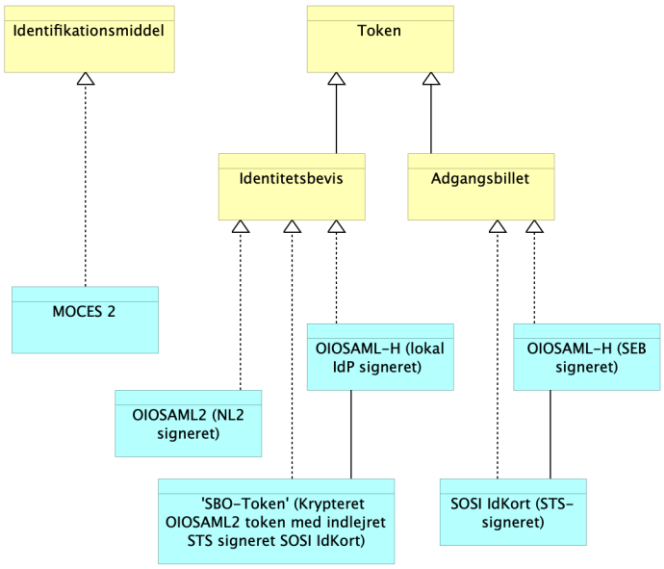
Realisering af applikationskomponenter. Bemærk, at lokal brugerstyring indgår som attributtjeneste.



Realisering af informationsobjekter fremgår nedenfor. Der introduceres to nye tokens:

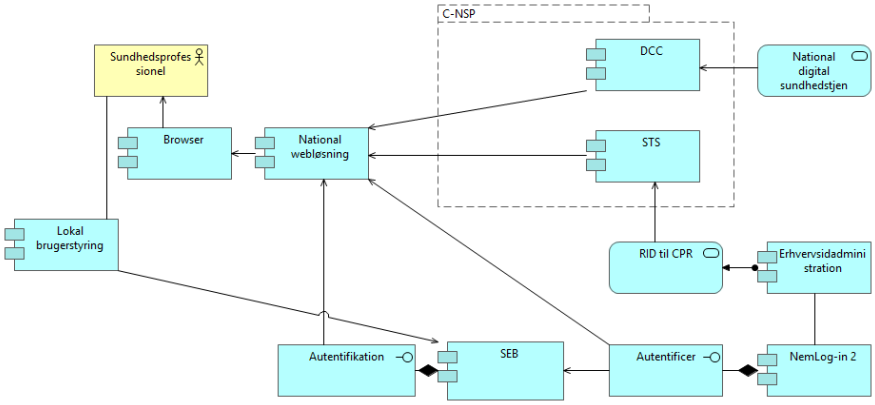
1) OIOSAML-H, der er en subprofil til OIOSAML2 målrettet sundhedsområdets (Health) behov. Tokenet har attributter til håndtering af sundhedsfaglige roller mm.
2) SBO-token (Sikker BrowserOpstart token). Tokenet er realiseret som et audiencekrypteret OIOSAML2 token med et indlejret SOSI idkort. Tokenet skabes

og signeres af SOSI STS'en. Audiencekrypteret betyder, at tokenet kun kan læses af det audience (her SEB), som tokenet er henvendt til. SBO-tokenet er primært en indpakning til udtræk og overførelse af STS signerede SOSI idkortet.



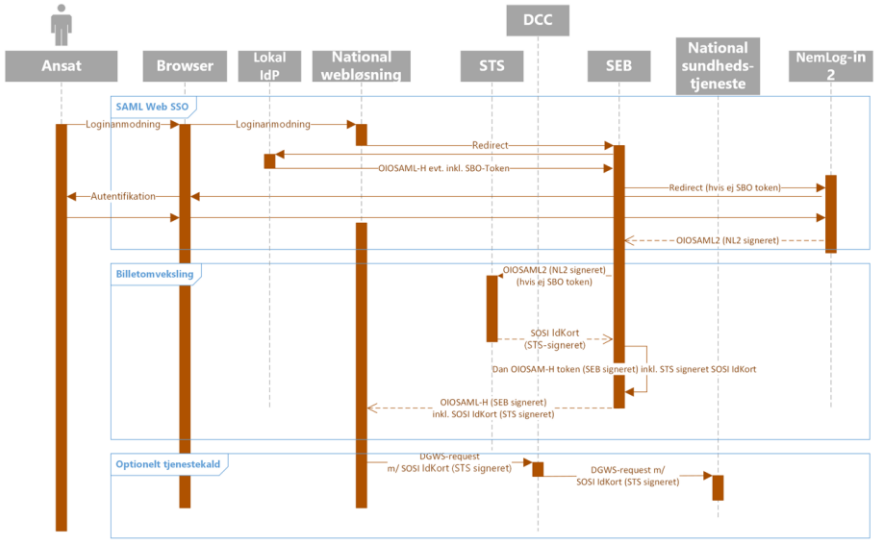
Figur 15: Realisering af informationsobjekter

5.2.2.2 Statiske sammenhænge



Figur 16: Statiske sammenhænge

5.2.2.3 Autentifikation via SEB for FUT og Sårjournal



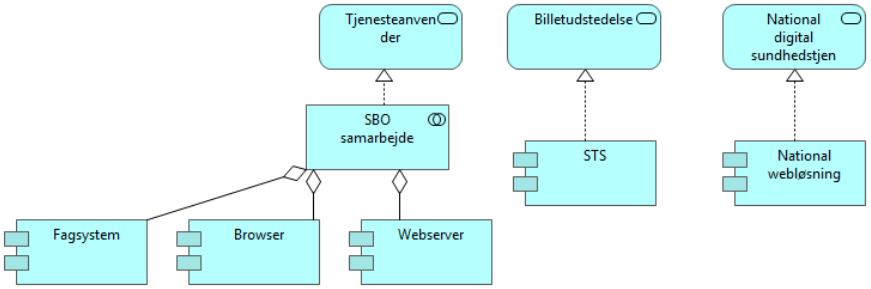
Figur 17: Autentifikationsflow for sårjournal

5.3 Ansattes adgang via browser og fagsystem (Sikker browseropstart)

Ansatte kan fra deres rige klient starte en browser med brug af samme identifikationsmidler, som ved kald af den rige klient. Udgangspunktet er, at man allerede har skaffet sig et gyldigt SOSI idkort (STS signeret).

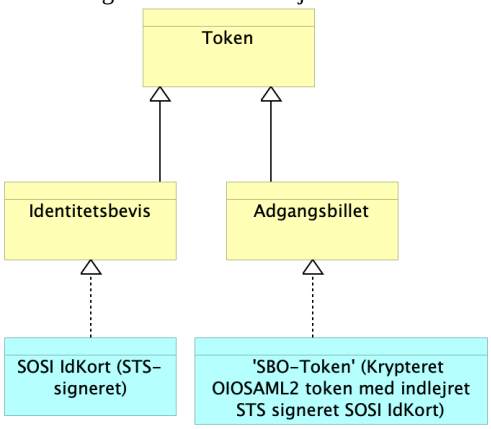
5.3.1 Komponentrealisering

Realisering af applikationskomponenter:



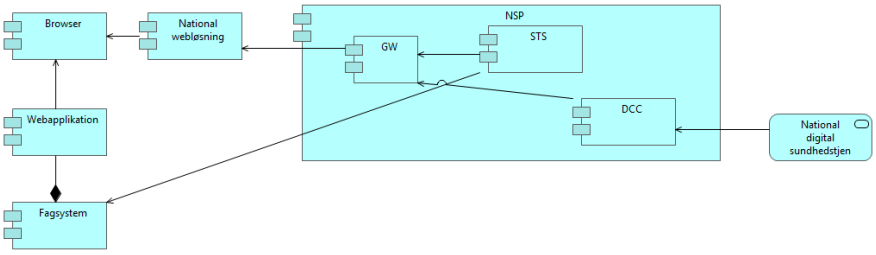
Figur 18: Realisering af applikationskomponenter

Realisering af informationsobjekter:



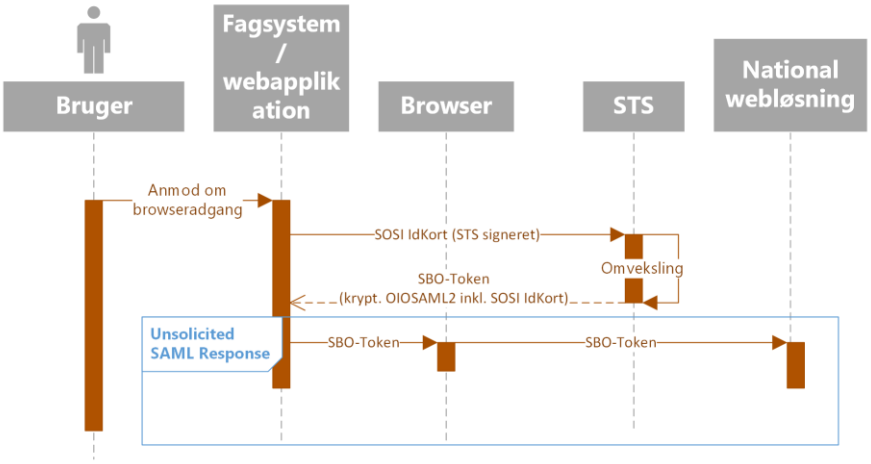
Figur 19: Realisering af informationsobjekter

5.3.2 Statiske sammenhænge



Figur 20: statiske sammenhænge

5.3.3 Flow



Figur 21: Flow ved sikker browseropstart

Ud over 'SBO-Token' overføres typisk også information om den konkrete brugerkontekst i fagsystemet. Eksempelvis den patient, som webløsningen skal opstartes med.

5.4 Systemadgang via webservices

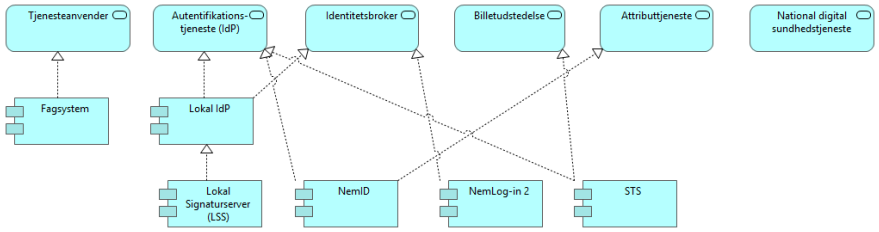
I visse situationer kan en tjenesteanvender få adgang til en sundhedstjeneste på baggrund af tokens, der alene identificerer tjenesteanvenderen og dermed ikke en fysisk bruger.

Det kan være et batch-job, der automatisk henter data fra en sundhedstjeneste, og hvor sundhedstjenesten ikke kræver, at kaldet skal initieres af en identificerbar person.

Der kan også være trust-baseret adgang. Det vil sige en trustaftale mellem tjenesteanvender og sundhedstjeneste, hvor det defineres, at det er tjenesteanvenderens ansvar at kontrollere og administrere bruger-identitet og -adgang.

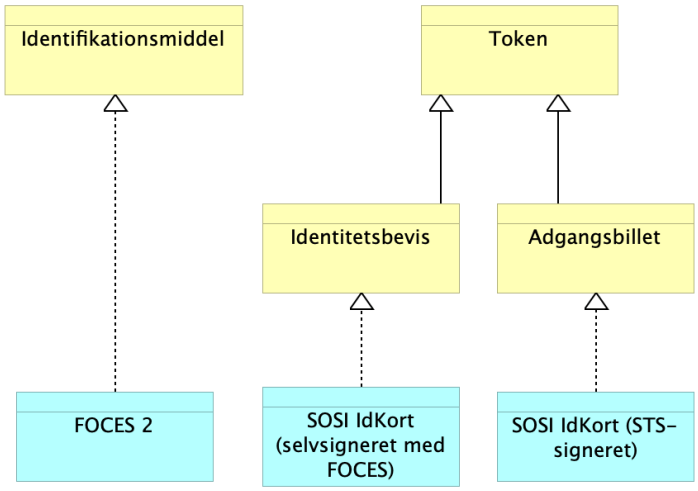
5.4.1 Komponentrealisering

Applikationskomponenter (svarer til baseline for rige klienter):



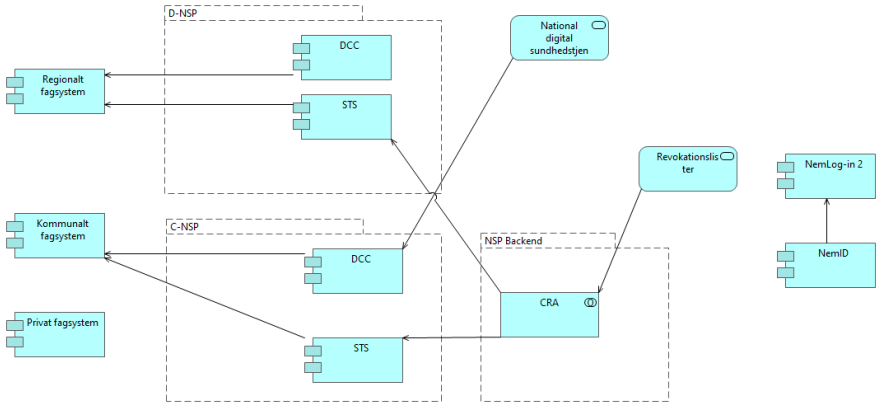
Figur 22: Realisering af applikationskomponenter

Informationsobjekter er realiseret som vist nedenfor:



Figur 23: Realisering af informationsobjekter ved systemadgang

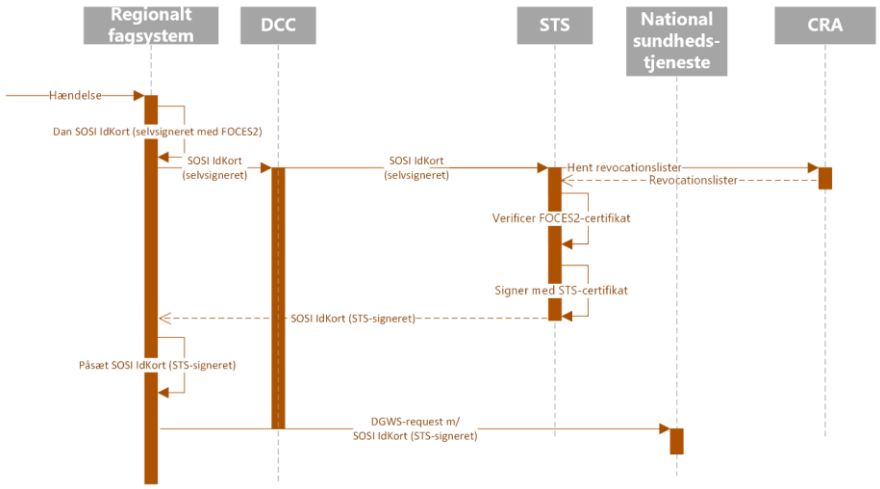
5.4.2 Statiske sammenhænge



Figur 24: Statiske sammenhænge

5.4.3 Autentifikationsflow

Nedenstående viser flow for systemkald fra rige klienter. Bemærk, at det ikke ligger fast, om SOSI idkortet caches, eller der dannes et nyt ved hvert kald. Levetiden for SOSI idkort er 24 timer. De enkelte tjenester kan have skærpede krav til SOSI idkortes levetid. Bemærk, at DCC ikke kalder GW hvis der er tale om et kald på niveau 3.

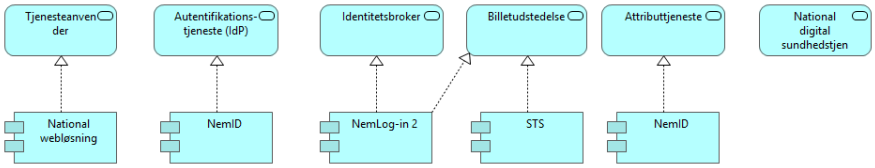


Figur 25: Autentifikationsflow

5.5 Borgers adgang til nationale webløsninger via browser

5.5.1 Komponentrealisering

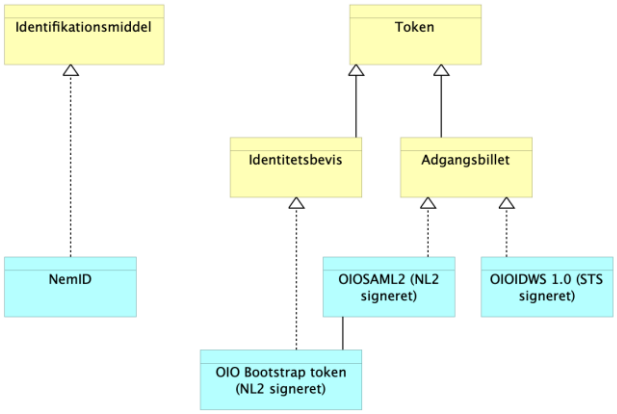
Applikationskomponenter er realiseret tilsvarende ansattes adgang via browser:



Figur 26: Realisering af applikationskomponenter

De nationale webløsninger omfatter sundhed.dk, fmk-online og FUT (borgeradgang til Sårjournal er baseret på NemID, og omfatter ikke opslag i de Nationale sundhedstjenester)

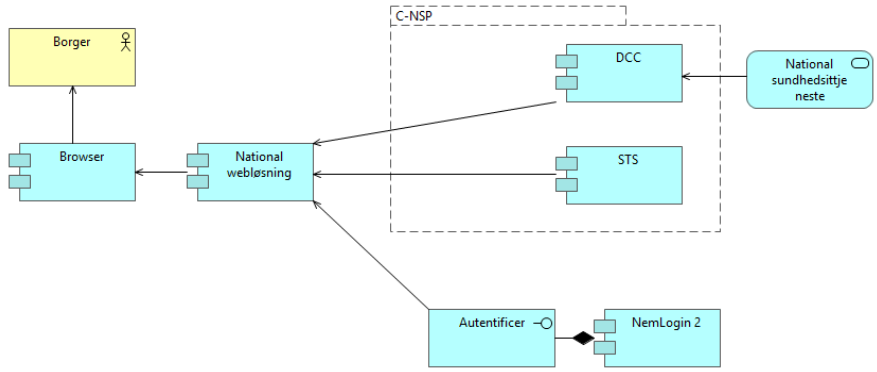
Informationsobjekter ses nedenfor. Bemærk, at services på NSP alene accepterer OIO IDWS-billetter, som er udstedt af STS'en på NSP.



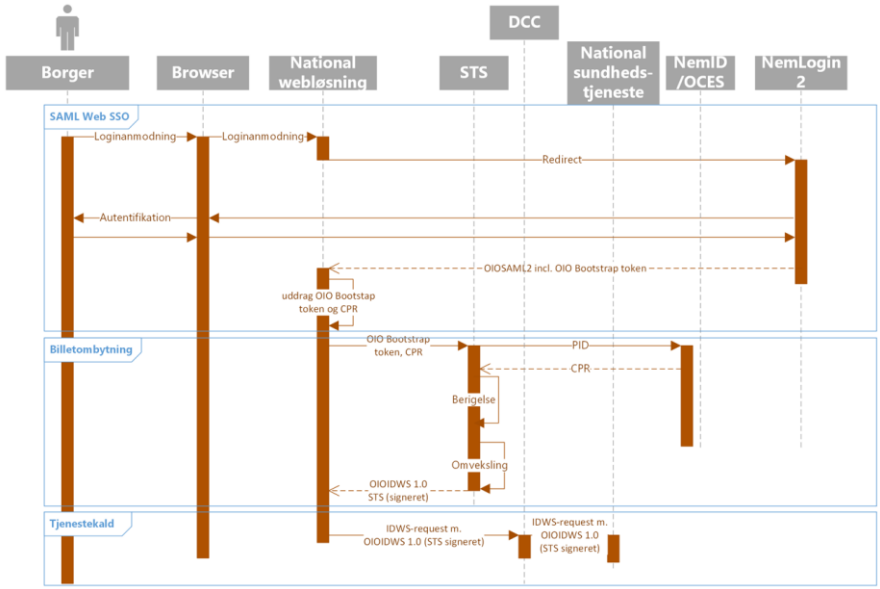
Figur 27: Realisering af informationsobjekter

5.5.2 Statiske sammenhænge

Statiske sammenhænge er de samme som for ansattes adgang med browser:



5.5.3 Autentifikationsflow



Figur 28: Autentifikationsflow

Webløsninger, der ikke tilgår borgerens egne sundhedsdata i de nationale sundhedstjenester, kan nøjes log-in til webløsningen og dermed med den første del af autentifikationsflowet på Figur 28 (dvs. SAML Web SSO delen).

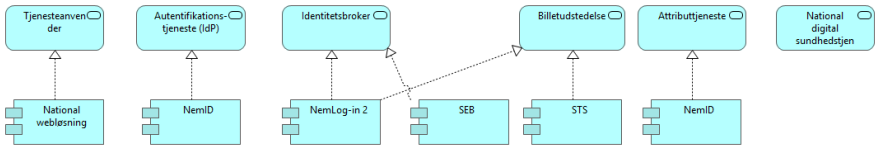
5.6 Borgers browseradgang via private webløsninger

Borgeres adgang via private webløsninger omfatter de situationer, hvor en privat part har en webløsning, som kalder en national sundhedstjeneste på vegne af borgeren.

Borgeres adgang via private webløsninger omfatter webapoteker og portaler tilknyttet lægepraksissystemer.

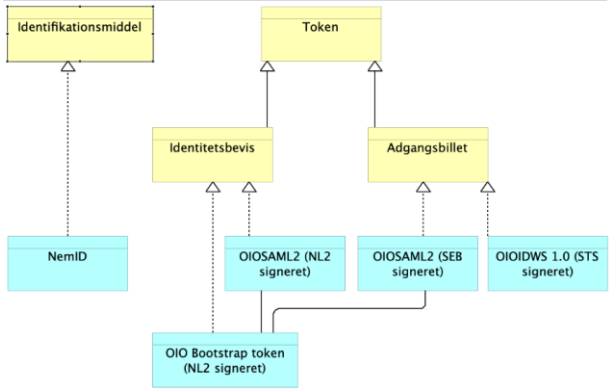
5.6.1 Komponentrealisering

Realisering af applikationskomponenter:



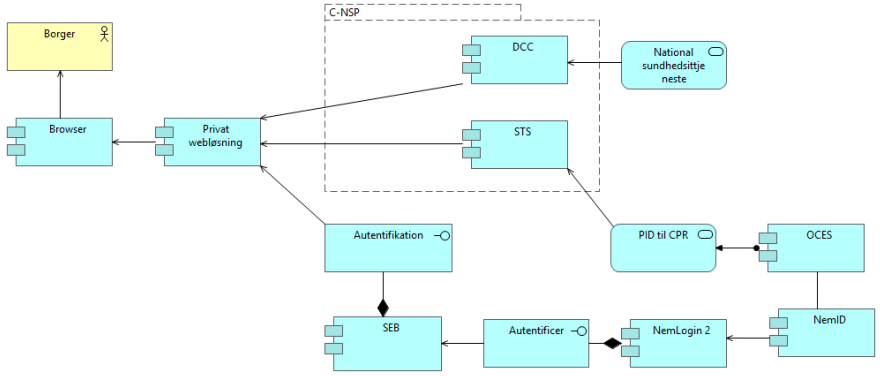
Figur 29: Realisering af applikationskomponenter

Realisering af informationsobjekter:



Figur 30: Realisering af informationsobjekter

5.6.2 Statiske sammenhænge

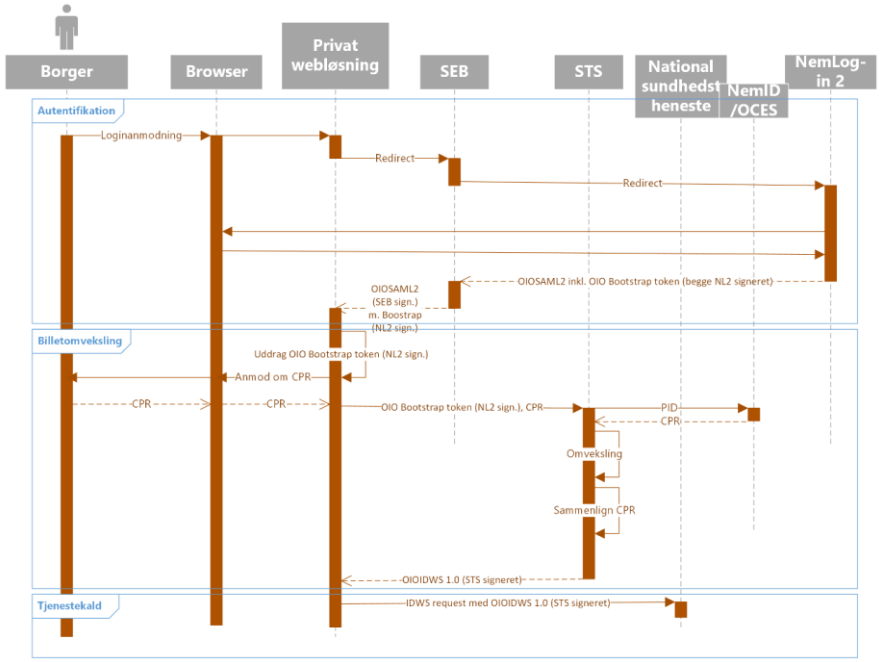


Figur 31: Statiske sammenhænge

5.6.3 Autentifikationsflow

Selve autentifikationen svarer til borgeres adgang til nationale webløsninger, som dog for nuværende foregår igennem SEB som proxy for NemLog-in2 (idet private aktører ikke må kobles direkte på nuværende NemLog-in2).
Desuden kan en privat webløsning ikke uddrage CPR-nummer fra OIOSAML2 tokenet, men må bede borger om at afgive dette.

I udgangspunkt er det resterende flow ens for alle webapoteker og LPS-portaler. Dog kalder nogle webapoteksløsninger den gamle PEM-snitflade (med system-trust), hvilket ikke afspejles i nedenstående flow. PEM-snitfladen lukkes meget snart.



Figur 32: Autentifikationsflow

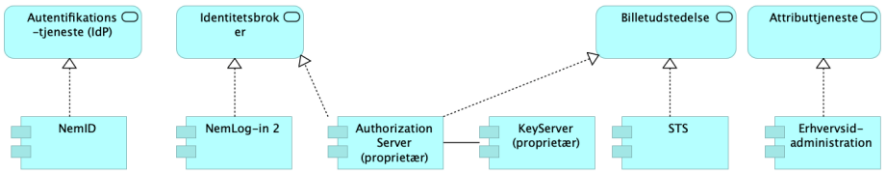
Private webløsninger, der ikke tilgår patientdata i de nationale sundhedstjenester, kan nøjes med den første del af autentifikationsflowet på Figur 32(dvs. autentifikations-delen).

5.7 Borgers adgang via apps

Diverse komponenter målrettet OpenId-Connect autorisation er ikke del af den nationale infrastruktur. De eksisterende apps (minLæge og FMK) anvender proprietære OpenId-Connect infrastruktur-komponenter. I gennemgangen nedenfor fremgår hvilke komponenter, der er proprietære og dermed ikke del af den nationale infrastruktur.

5.7.1 Komponentrealisering

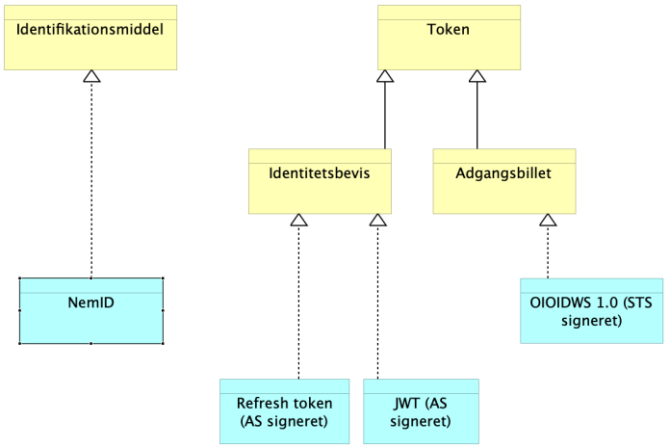
Realisering af centrale applikationskomponenter:



Figur 33: Realisering af centrale applikationskomponenter

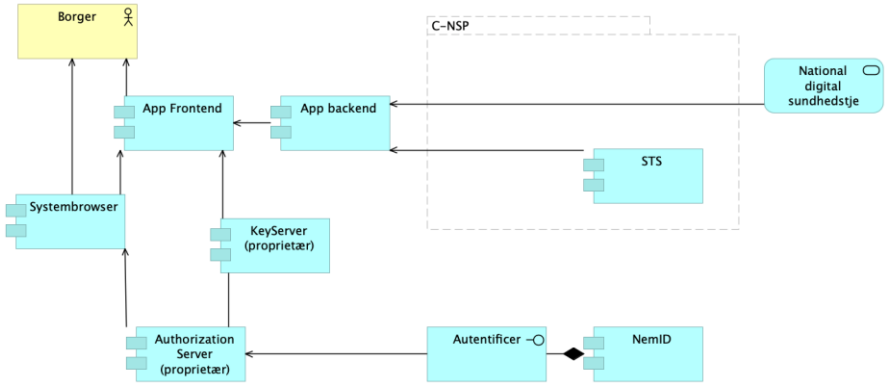
Realisering af informationsobjekter:

- JWT (JSON Web Token). I regi af OpenId Connect/OAuth også omtalt i Access Token. Har typisk kort levetid.
- Refresh token. Token anvendt til at hente nyt Access token. Har typisk lang levetid.



Figur 34: Realisering af centrale informationsobjekter

Statiske sammenhænge:



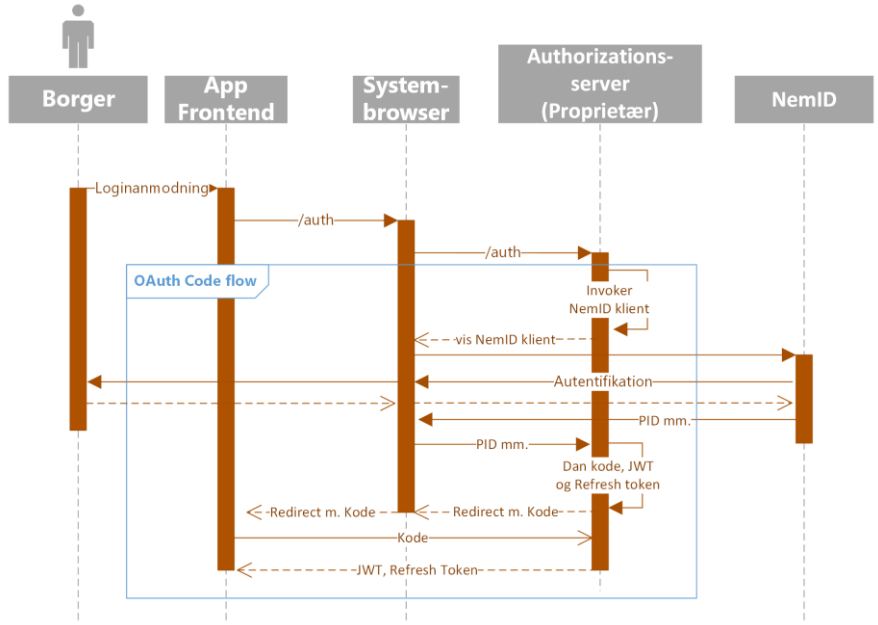
Figur 35: Statiske sammenhænge

5.7.2 Autentifikationsflow

Autentifikationsflowet falder i fire dele:

1) autentifikationen fra app frontend
2) valg af pinkode samt caching af refresh token
3) omveksling af access token og kald af tjeneste
4) genoptagelse af session

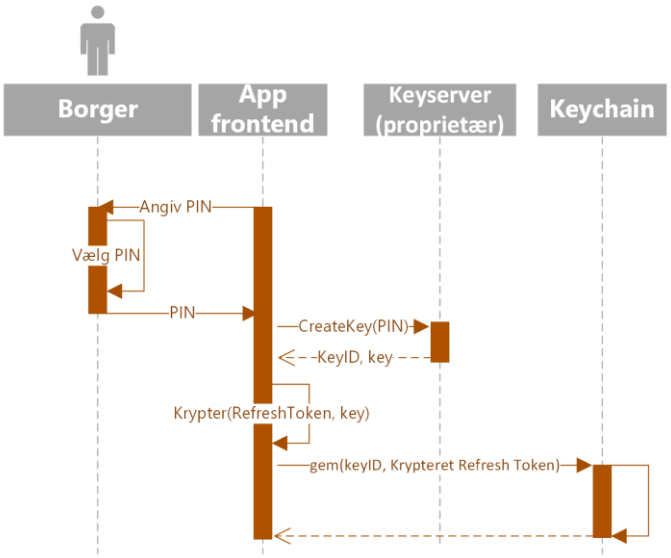
5.7.2.1 Autentificering fra app front end



Figur 36: Autentifikationsflow fra app frontend

5.7.2.2 Afslutning på førstegangsautentificering m/ valg af PIN-kode

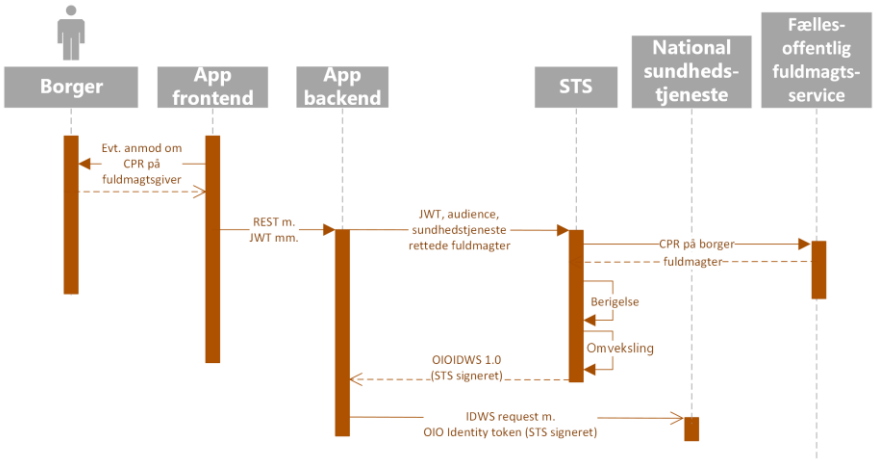
Flowet viser, hvordan sessionsbeviset, i form af refreshtoken, gemmes i keychain på device efter kryptering.



Figur 37: PIN-kode og anvendelse af keychain til opbevaring af sessionsbevis i form af refresh token

5.7.2.3 Omveksling af access token og kald af tjeneste

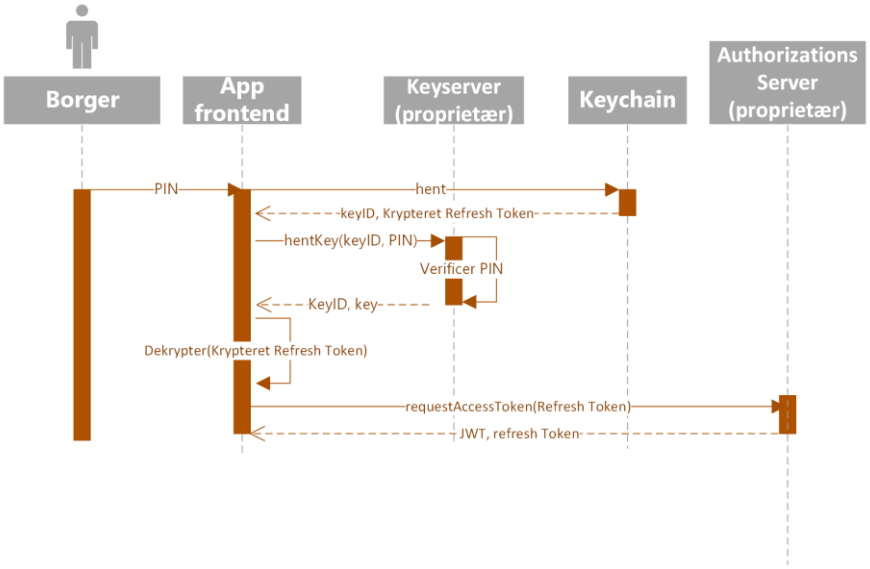
Flowet viser, hvordan APP henter data fra en national sundhedstjeneste. Enten borgers egne data eller en fuldmagtsgivers data. I det sidste tilfælde anmodes om CPR på fuldmagtsgiver, og STS'en validere om borger har en fuldmagt fra fuldmagtsgiver via den fællesoffentlige fuldmagtsservice.



Figur 38: Omveksling af access token og kald af service

5.7.3 Sessionsgenoptagelse med refreshtoken

Nedenstående flow viser hvordan sessionen genoptages med anvendelse af refreshtoke-net. Flowet vil herefter gå over i lagring af tokens samt omveksling og kald af tjeneste (se ovenfor).



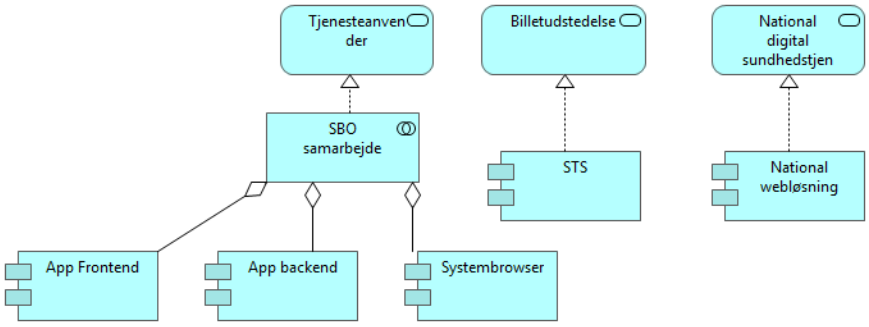
Figur 39: Genoptagelse af session

5.8 Borgers adgang til webløsninger via app (SBO)

Der er i forbindelse med MinLæge-appen etableret en løsning, som kan overføre en brugerkontekst fra appen til en given webløsning tilsvarende det som kendes fra sikker browserstart initieret fra en fagapplikation. Løsningen forudsætter, at brugeren har logget ind i appen, og appen derfor har et access token (JWT). Løsningen skal i første omgang anvendes til at vise forløbsplaner fra Minlæge, men anvendes endnu ikke i produktion.

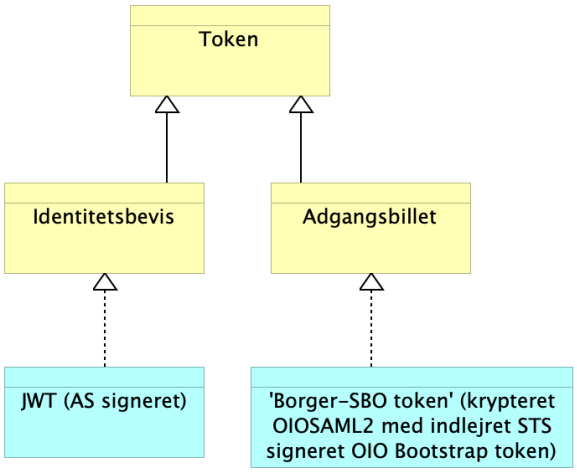
5.8.1 Komponentrealisering

Realisering af applikationskomponenter:



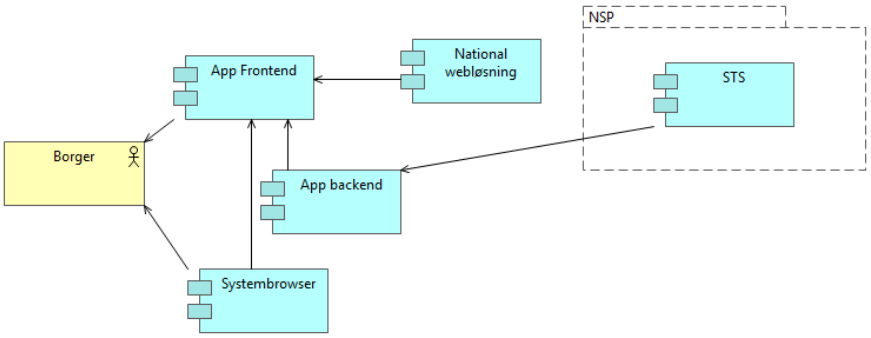
Realisering af informationsobjekter:

Borger-SBO token (Borger Sikker BrowserOpstart token). Tokenet er realiseret som et audiencekrypteret OIOSAML2 token med et indlejret OIO Bootstrap token. Tokenet skabes og signeres af SOSI STS'en. Audiencekrypteret betyder, at tokenet kun kan læses af det audience (her web-applikationen), som tokenet er henvendt til.

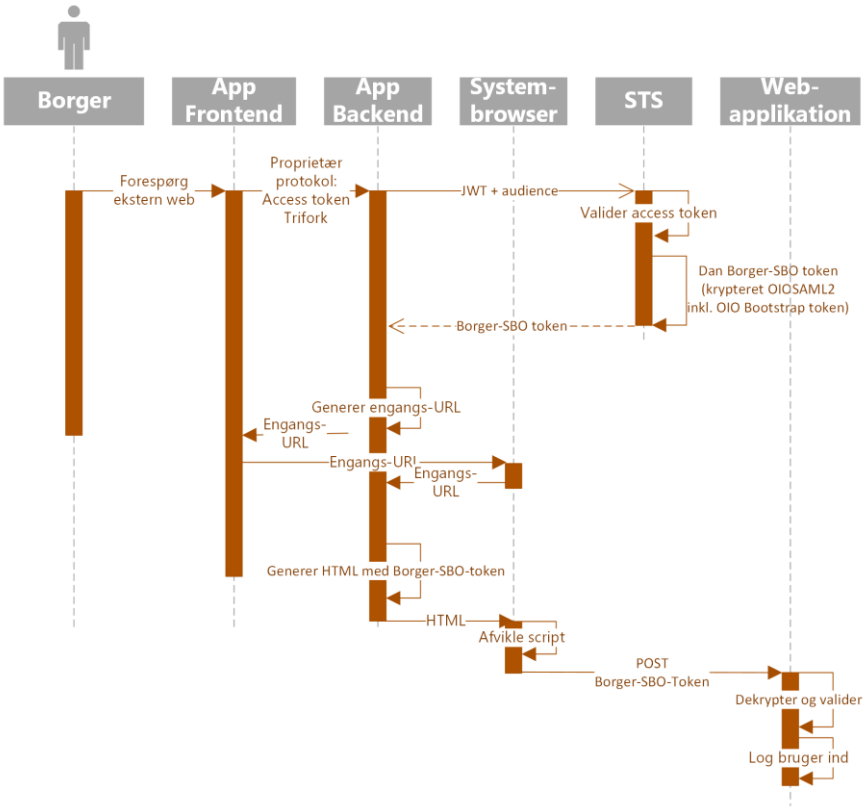


Figur 40: Realisering af informationsobjekter

Statiske sammenhænge:



5.8.2 Autentifikationsflow



Figur 41: Autentifikationsflow

6. Transition 1 - Scenarie-view

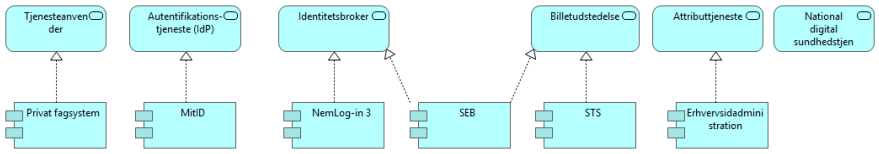
6.1 Ansattes adgang via rig klient

6.1.1 MitID-scenariet, Ansattes adgang via rig klient og MitID Erhverv

Dette flow retter sig primært mod mindre private aktører.

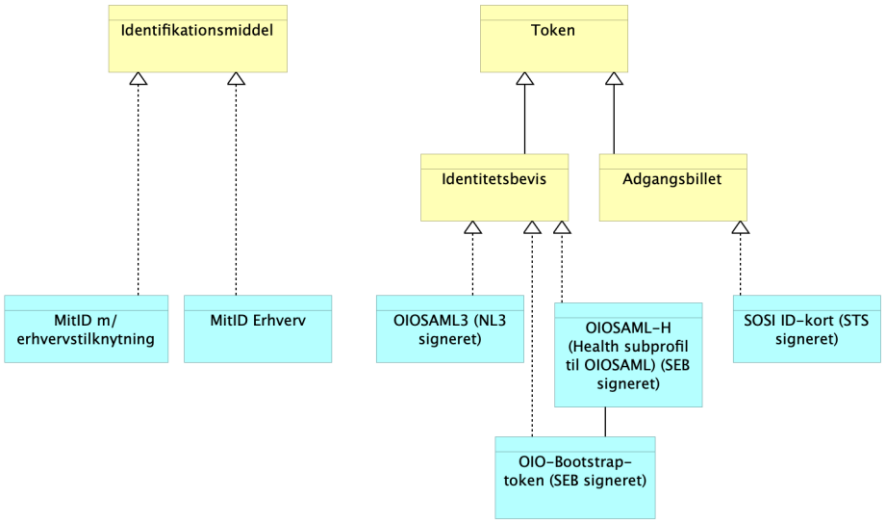
6.1.1.1 Komponentrealisering

De centrale applikationskomponenter realiseres på følgende vis:



Figur 42: Realisering af applikationskomponenterne i MitID-scenariet

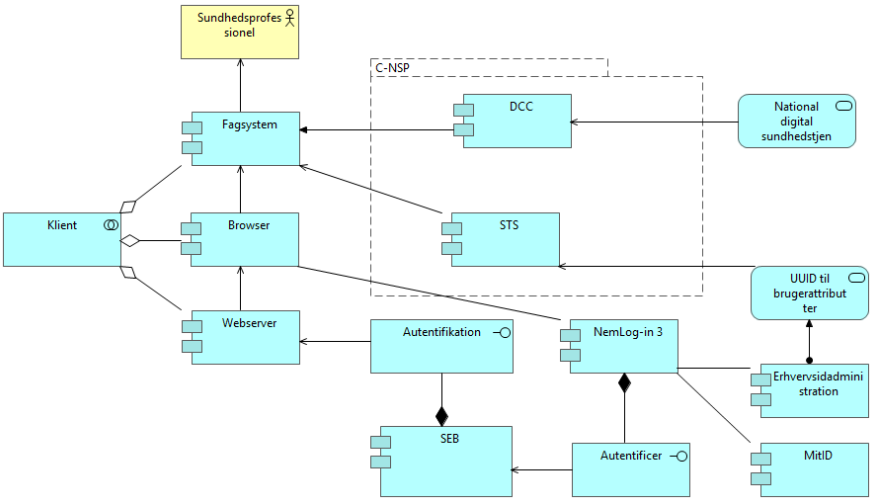
Realisering af de centrale forretningsobjekter: MitID Erhverv anvendes som identitetsmiddel. OIOSAML3 token overføres fra Nemlog-in3 til SEB, og på baggrund af dette udsteder SEB et SEB-signeret OIOSAML-H token (Health subprofil til OIOSAML) med et indlejret SEB signeret OIO-Bootstrap-token. OIO-Bootstrap-token er et identitetsbevis, som fagsystemet skal anvende i billetomvekslingen til SOSI Idkort. SOSI idkort er en adgangsbillet til de nationale sundhedstjenester.



Figur 43: Realisering af de centrale informationsobjekter

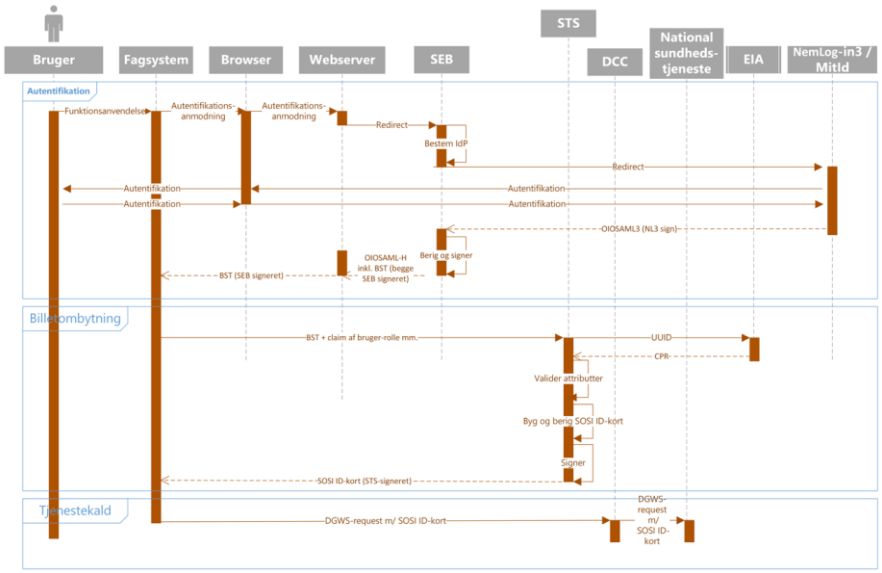
6.1.1.2 Statiske sammenhænge

Som det fremgår nedenfor, foregår autentifikationen som et standard SAML WebSSO flow. Det betyder, at de nuværende rige klienter skal autentificeres ved hjælp af browser og webserver. Den konkrete implementering er op til de enkelte systemleverandører, og er her blot angivet som et klientsamarbejde.



Figur 44: Statiske relationer for MitID-scenariet med rige klienter

6.1.1.3 Autentifikationsflow



Figur 45: Autentifikationsflow for ansat med rig klient og anvendelse af MitID Erhverv via SEB.

I ovenstående flow skal brugeren via fagsystemet hente sundhedsdata fra en nationale sundhedstjeneste (jf. svømmebanen "Tjenestekald" i sekvensdiagrammet).

Kald af en nationale sundhedstjeneste kræver en adgangsbillet i form af et SOSI idkort. SOSI idkort modtages fra SOSI STS'en på baggrund af et omvekslingskald. Input til omvekslingskaldet er et OIO-Bootstrap-token samt et 'claim', der specificerer brugerens rolle i kaldskonteksten fra fagsystemet (jf. svømmebanen "Billetombytning" i sekvensdiagrammet).

Fagsystemet iværksætter en autentifikationsproces med det formål at erhverve et OIO-Bootstrap-token. Autentifikationsprocessen er browserbaseret. Brugeren autentificeres

via MitID på NL3 og sendes omkring SEB, der udsteder OIO-Bootstrap-tokenet (jf. svømmebanen "Autentifikation" i sekvensdiagrammet).

6.1.1.4 NSP view: Gapanalyse for MitID-scenariet med ansattes adgang via rig klient

Vær opmærksom på, at der er tilknyttet en Gapanalyse-tabel til alle scenarier i kapitel 6, og at de enkelte scenarier deler mange af de samme Gap's. Af denne årsag er der tilknyttet et GapId til det enkelte Gap´s, således at læseren nemmere kan genkende de enkelte Gap's og springe teksten over.

Tabel 3: Oversigt over gaps for ansattes adgang med rige klienter i MitID-scenariet

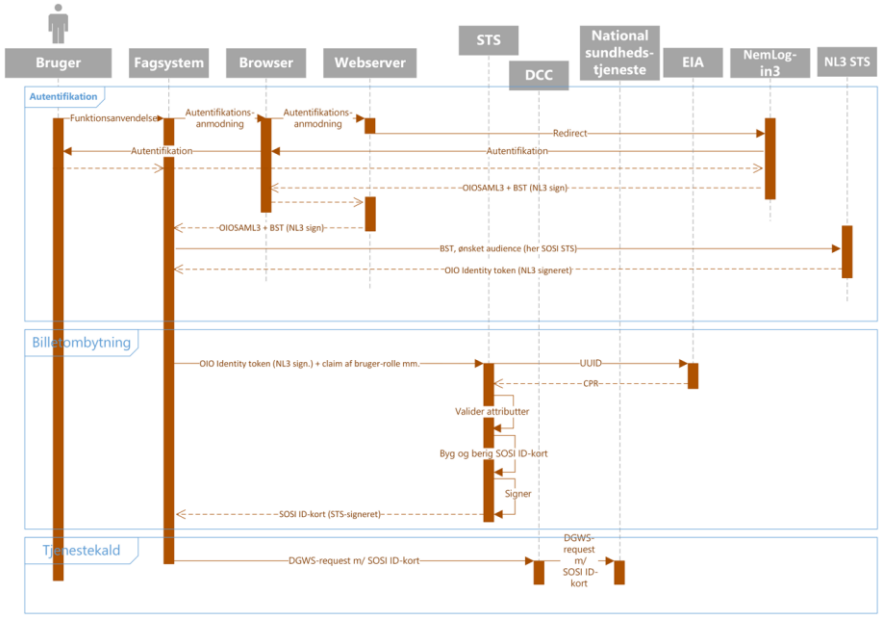
Komponent (GapID)	**Ændring**	Reference til yderligere info
Brugeradministration	Brugeren skal kunne autentificere sig via en erhvervsidentitet, der er koblet til erhvervsbrugerens private MitID elektroniske identifikationsmidler, eller via dedikerede MitID-erhvervsidentifikationsmidler. Brugerens CPR-nummer skal tilknyttes EIA-registreringen. Brugeren administreres enten manuelt via MitID administrationsgrænsefladen eller via synkronisering fra lokalt IDMS via NL3 IdM API adgangen. Sundhedsfaglige rolle til sundhedsfaglige brugere uden autentifikation administreres via SEB Classic (dvs. de 'Nationale roller').	Jf. https://migrering.nemlog-in.dk/nemlog-in-erhvervsloesning/avanceret-setup/modeller/integration-med-idm/idm-api-dokumentation/
Fagsystem	Autentifikationsprocessen er browserbaseret. Autentifikationsprocessen opstartes fra fagsystemet via en lokal webserver. Efter en succesfuld autentifikationsproces udleverer web-serveren et SEB signeret OIO-Bootstrap-token til fagsystemet, som fagsystemet skal anvende i den efterfølgende billetomveksling til SOSI idkort. Der skal etableres en tilslutningsaftale til SEB broker, således at der kan etableres et WEB-SSO kald fra lokal webserver til SEB broker.	
SEB (G1)	Der skal etableres en tilslutningsaftale med NL3.	
SEB (G2)	I SEB skal der etableres et flow, hvor SEB agerer broker mellem lokal fagsystem/webserver og Nemlog-in3/MitId. SEB omdirigerer bruger til autentifikation i NL3/MitID. Ved succesfuld autentifikation returnerer NL3 et OIO-SAML3 token til SEB. SEB validerer tokenet, udtrækker brugerens sundhedsfaglige autorisationer og nationale roller, og udsteder et OIOSAML-H token med et indlejret	SEB broker jf. afsnit 7.4.1 OIO-Bootstrap-token jf. afsnit 7.2.2.1

	OIO-Bootstrap-token. Begge tokens har listen med brugerens 'nationale roller' indlejret. OIOSAML-H tokenet har desuden listen med brugerens sundhedsfaglige autorisationer indlejret. De to SEB-signerede tokens returneres til webserveren.	
SEB (G3)	På kort sigt bliver SEB ikke NSIS registreret, og derfor udsteder SEB på kort sigt OIOSAML-H v1 tokens (Health subprofil til OIOSAML2). På langt sigt forventes SEB at blive NSIS registeret således, at SEB kan udstede OIOSAML-H v2 tokens (Health subprofil til OIOSAML3). NSIS registrering kræver blandt andet HSM-understøttelse i SEB	
SEB (G4)	Skalering: øget anvendelse af SEB nødvendiggør, at SEB gøres mere skalerbar	
STS (G5)	I SOSI STS'en skal der etableres en grænseflade der kan omveksle et OIO-Bootstraptoken til et SOSI idkort	STS omvekslingskaldet jf. 7.2.2
SEB, STS (G6)	Med MitID/NL3 indføres attributten 'Global Employee UUID' til identifikation af en erhversidentitet. MitID/NL3 udstiller en række lookup-services, der kan anvendes til at fastslå brugerens CPR-identitet ud fra Global Employee UUID. SOSI STS'en skal benytte de nye lookup-services til at udtrække brugerens CPR, da CPR er nøglen til opslag efter brugerens sundhedsfaglige autorisationer. SEB skal kun benytte de nye lookup-services i de tilfælde, hvor CPR ikke er indehold til OIOSAML tokenet fra IdP.	STS afhængigheder jf. afsnit 7.2
STS (G8)	SOSI Idkort skal justeres, da der ikke længere anvendes OCES certifikater i autentifikationsprocessen. Justeringen kan holdes indenfor DGWS standarden.	SOSI idkort justeringerne jf. 7.2.2.3

6.1.1.5 Alternative MitID autentifikationsflows

Autentifikationsflowet behandlet ovenfor tilgår MitID/NL3 via SEB. Alternativt kan fagsystemet tilgå MitID/NL3 direkte (jf. Figur 46) eller via en af de nye MitID-brokers (jf. Figur 47), som MitID åbner op for.

Fagsystem tilgår MitID/NL3 direkte:



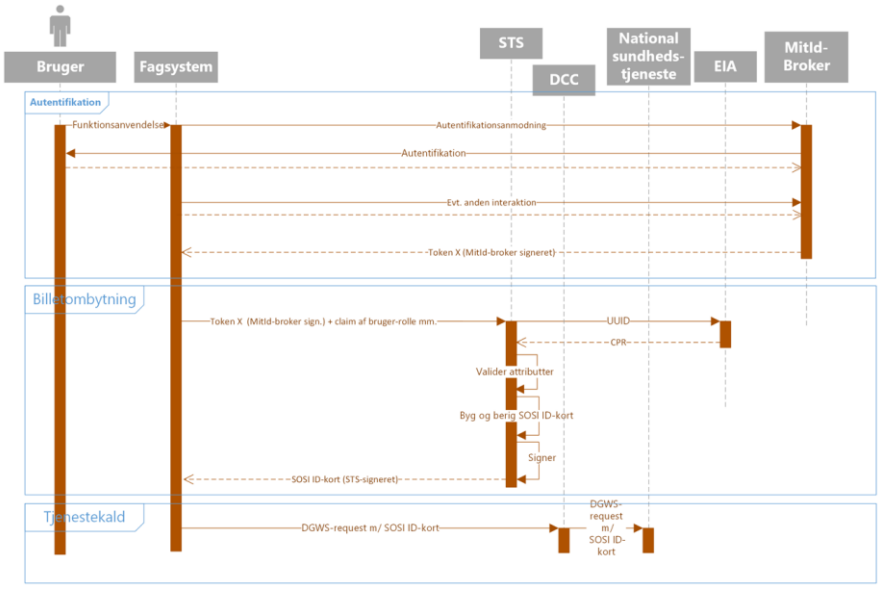
Figur 46: Autentifikationsflow for ansat med rig klient og direkte interaktion med MitID/NL3

Fagsystemet iværksætter en autentifikationsproces med det formål at erhverve et OIO-Identity-token, der giver adgang til SOSI føderationen (dvs. audience sat til SOSI STS). Autentifikationsprocessen er browserbaseret. Brugeren autentificeres via MitID på NL3, der udsteder et OIOSAML3 token med et indlejret OIO-Bootstrap-token (BST) (jf. svømmebanen "Autentifikation" i sekvensdiagrammet på Figur 46).
BST omveksles efterfølgende via NL3 STS'en til et OIO-Identity-token (audience SOSI STS).

I billetomvekslings-svømmebanen omveksles OIO-Identity-tokenet (fra NL3 STS) til et SOSI idkort. Til SOSI STS omvekslingskaldet medsendes et 'ws-trust claim' vedrørende den ansattes sundhedsfaglige rolle. SOSI STS'en validerer OIO-Identity-tokenet og den ønskede rolle, hvorefter et SOSI idkort udstedes til fagsystemet.

Tjenestekald-svømmebanen adskiller sig ikke fra de øvrige MitID-scenarier.

Fagsystem tilgå MitID via en MitID-Broker:



Figur 47: Autentifikationsflow for ansat med rig klient og MitId-broker

MitID/NL3 tillader andre og uafhængige MitID-brokere som alternativ til Nemlog-in3. Eksempelvis MitID-brokere, der adskiller sig fra Nemlog-in3 på understøttede protokoller, servicelevel eller pris.

SOSI-STS truster tokens fra MitID-brokere, der er NSIS registreret og dermed underlagt den governance, som NSIS udstikker. Samtidig vil SOSI-STS stille krav til understøttede tokenformater og tokenindhold. Kravene er endnu ikke formuleret, men det forventes, at OIO-Bootstrap og OIO-Identity tokens som minimum understøttes.

Figur 47 illustrerer autentifikationsflowet for ansattes autentifikation via en MitID-broker. Som det fremgår af autentifikations-svømmebanen, så er den nøjagtige interaktion mellem applikation og MitID-broker ukendt og vil afhænge af den konkrete MitID-broker.

Billetomveksling- og tjenestekald-svømmebanen adskiller sig ikke fra de øvrige MitId-scenarier.

6.1.1.6 NSP view: Gapanalyse for alternative MitId autentifikationsflows

Komponent (GapID)	**Ændring**	Reference til yderligere info

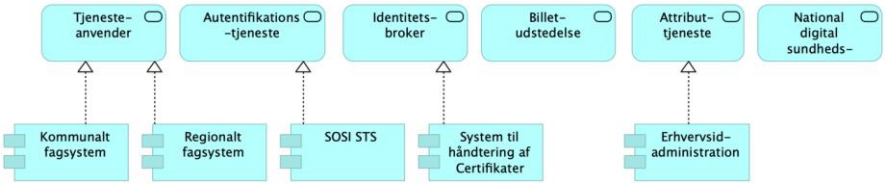
STS (G20)	I SOSI STS skal der etableres en grænseflade der kan udstede et SOSI idkort på baggrund af tokens udstedt fra NL3 STS og MitID-Broker. I første omgang afgrænses det til OIO-Identity- og OIO-bootstrap-tokens.	STS omvekslingskaldet jf. 7.2.2

6.1.2 Certifikat-scenariet: Ansattes adgang med rig klient og MOCES

Den forventede målgruppe for dette scenarie er først og fremmest regioner og kommuner. Det vil dog også kunne anvendes af private aktører.

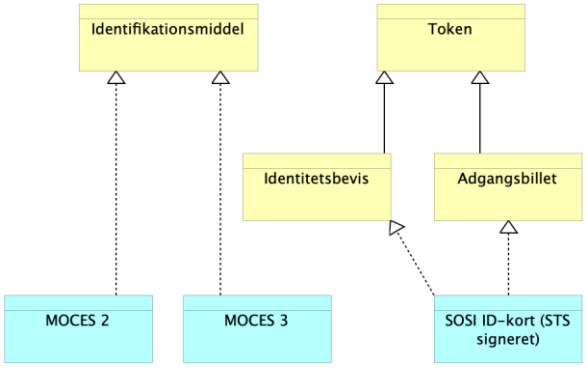
6.1.2.1 Komponentrealisering

Nedenstående viser realiseringen af de centrale applikationskomponenter.



Figur 48: Realisering af de centrale applikationskomponenter

De centrale informationsobjekter realiseres som vist nedenfor:

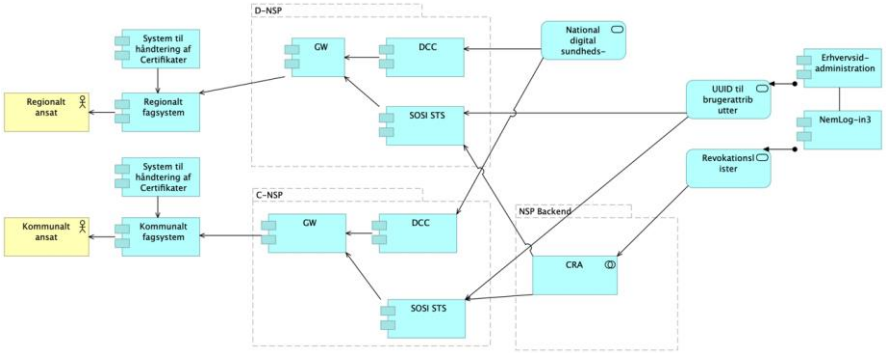


Figur 49: Realisering af de centrale informationsobjekter

Som det fremgår, understøtter scenariet såvel MOCES 2 som MOCES 3.

6.1.2.2 Statiske sammenhænge

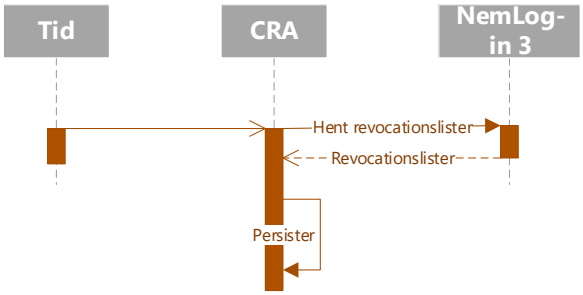
Nedenfor ses de statiske sammenhænge. Bemærk, at det nedenfor er angivet, at GW også for regioner ligger foran DCC. Denne øvelse er i gang, men er muligvis ikke færdiggjort ved scenariets start (Pt. er Region Hovedstaden og Region Sjælland overgået til dette mønster). Det har mindre betydning for scenariet.



Figur 50: Statiske sammenhænge

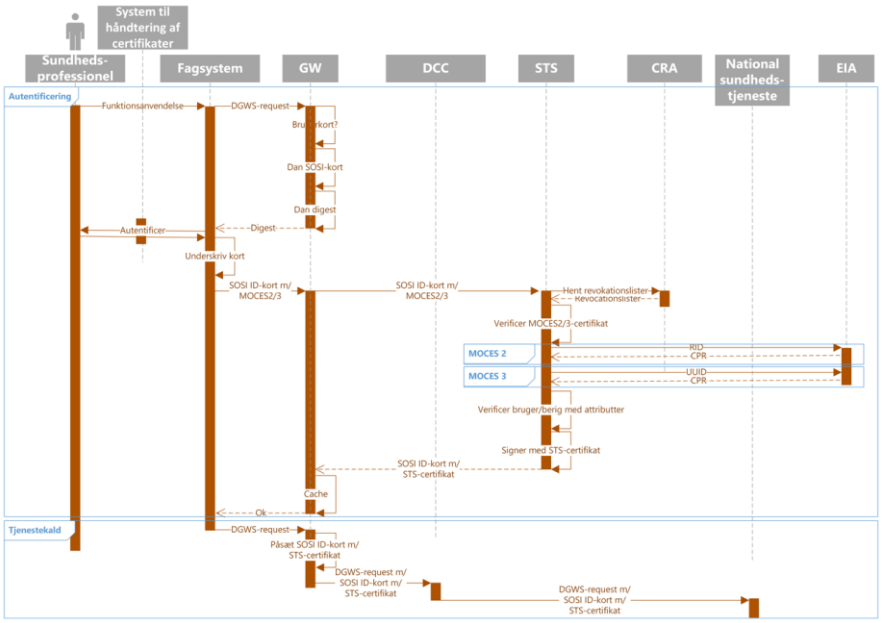
6.1.2.3 CRA-flow transition 1

CRA vil fremover opdatere revokationslister fra en snitflade på NemLogin-3.



Figur 51: Flow ved opdatering af CRA med revokationslister

6.1.2.4 Autentifikationsflow



Figur 52: Autentifikationsflow for MOCES-scenariet.

Eneste ændring til Baseline autentifikationsflowet er understøttelse af MOCES3 certifikater.

6.1.2.5 Gapanalyse for certifikat-scenariet med ansattes adgang via rig klient og MOCES

Komponent (GapID)	**Ændring**	Reference til yderligere info
Brugeradministration	Brugeren skal oprettes i EIA og havde tilknyttet sit CPR-nummer til EIA registreringen. Brugerens MOCES3 certifikat udtrækkes via en administrationsgrænseflade samt via et IdM certifikat API tilknyttet Nemlog-in3. Fremover vil understøttelse af MOCES-certifikater, med central opbevaring af nøgle hos certifikatudsteder, ophøre. Det er certifikatholderens ansvar at danne og opbevare den private nøgle på forsvarlig vis.	Jf. https://migrering.nemlog-in.dk/nemlog-in-erhvervsloesning/avanceret-setup/certifikater/

	De 'nationale roller' til sundhedsfaglige brugere uden autorisation kan, som i baseline, håndteres via to forskellige modeller 1) Via administraion i SEB Classic 2) Via trust-modellen, hvor der indgås en aftale om, at SOSI STS'en stoler på den rolle, der indskrives i det selvsignerede SOSI idkort.	
STS (G9)	Det skal sikres at SOSI STS'en kan håndtere OCES2/MOCES2 og OCES3/MOCES3 i en overgangsperiode.	Jf. afsnit 7.2.1
STS (G6)	Med MitID/NL3 indføres attributten 'Global Employee UUID' til identifikation af en erhversidentitet. MitID/NL3 udstiller en række lookup-services, der kan anvendes til at fastslå brugerens CPR-identitet ud fra Global Employee UUID. SOSI STS'en skal benytte de nye lookup-services til at udtrække brugerens CPR, da CPR er nøglen til opslag efter brugerens sundhedsfaglige autorisationer.	STS afhængigheder jf. afsnit 7.2
STS (G8)	SOSI Idkort skal justeres når MOCES3 certifikater anvendes. MOCES3 indeholder ikke CVR-RID attributten. Justeringen kan holdes indenfor DGWS standarden.	SOSI idkort justeringerne jf. 7.2.2.3
CRA (G10)	I CRA skal der etableres caching af OCES3 revocationslister	Jf. afsnit 7.7

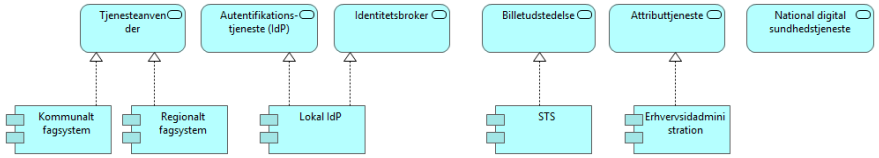
Tabel 4: Identificerede gaps

6.1.3 Føderationsscenariet med GW: Ansattes adgang via rig klient og egne identitetsmidler

Det henvender sig til parter, som ønsker at gå et stykke ad føderationsvejen, men som endnu ikke ønsker at omlægge alle flows, som involverer GW.

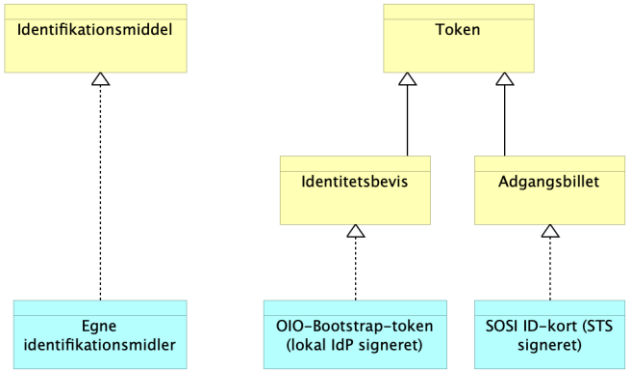
6.1.3.1 Komponentrealisering

Applikationskomponenter er realiseret som følger:



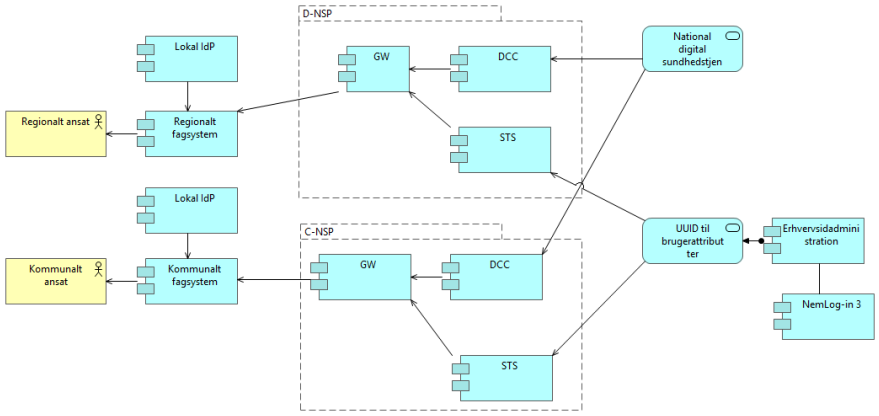
Figur 53: Realisering af applikationskomponenter i hybridscenariet for rige klienter

Informationsobjekter er realiseret som følger:



Figur 54: Realisering af informationsobjekter ved hybridscenariet for fagapplikationer

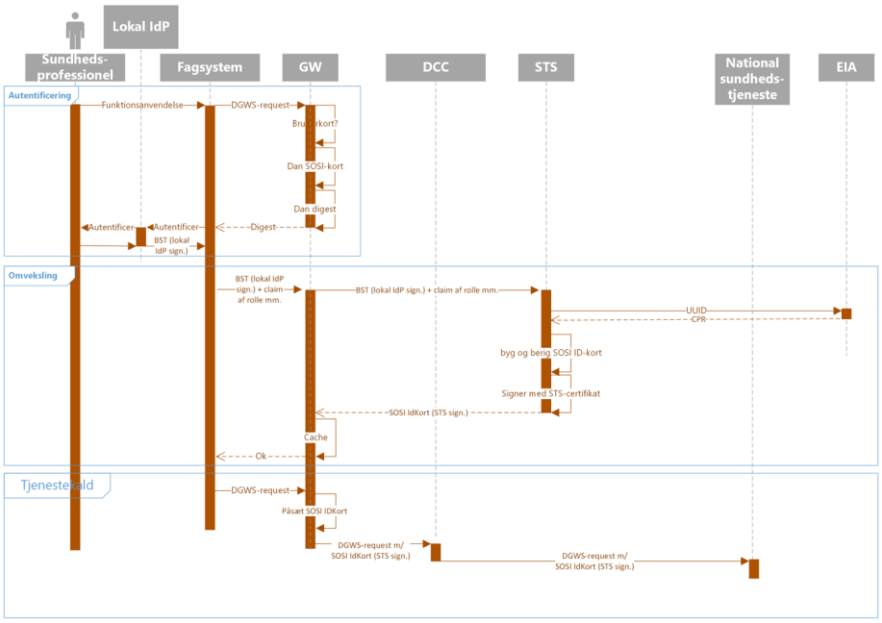
6.1.3.2 Statiske sammenhænge



Figur 55: Statiske sammenhænge for hybridscenariet

6.1.3.3 Autentifikationsflow

Autentifikationsflowet indledes på tilsvarende vis som i certifikatscenariet (og som i baseline). Men i stedet for at bygge et SOSI ID-kort ved negativt svar fra GW, dannes i stedet et lokalt udstedt OIO-Bootstrap-token, der sendes til GW sammen med et claim af brugerens rolle, tilsvarende MitID-scenariet.



Figur 56: Autentifikationsflow ved føderationsscenarie med GW

Tjenestekald-flowet baserer sig på, at brugerens SOSI-kort (STS-signeret) caches i SOSI-gateway, og vil genanvendes ved kald til sundhedstjenester, så længe der er et gyldigt idkort. Kortet har i dag en maksimal gyldighed på 24 timer, og de enkelte sundhedstjenester kan sætte yderligere krav (eksempelvis opererer FMK med gyldighed på ni timer), i hvilket fald der skal ske en genautentifikation

Genautentifikation kan ske eksplicit ved, at fagsystemet forud for et tjenestekald forespørger GW på, om der findes et gyldigt SOSI-kort, og ellers får det dannet, eller det kan ske implicit ved at fagsystemet kalder en sundhedstjeneste via GW'en, og givet at der ikke findes et gyldigt idkort får en digest tilbage. Fagsystemet skal dernæst opstarte en autentifikationsproces for den ansatte, som resulterer i at fagsystemet modtager et identifikationsbevis i form at et BST token. Figur 56 viser det implicitte flow.

6.1.3.4 Gapanalyse: Ansattes adgang via rigKlient, egne identitetsmidler og GW

Komponent (GapID)	**Ændring**	**Reference til yderligere info**
Brugeradministration	Brugeren skal oprettes i EIA og havde tilknyttet sit CPR-nummer til EIA registreringen. I forbindelse med oprettelsesprocessen skal det lokale IDMS (A/D eller lign.) persistere den Globale Employee UUID, der erstatter RID og udgør brugerens primære ID i EIA. Nemlog-in3 har et IdM API til provisioneringsprocessen. Sundhedsfaglige roller, ud over de sundhedsfaglige autorisationer, administreres med fordel lokalt. Eksempelvis via lokalt IDMS.	Jf. https://migrering.nemlog-in.dk/nemlog-in-erhvervsloesning/avanceret-setup/modeller/integration-med-idm/idm-api-dokumentation
Lokal IdP	Den lokale IdP skal NSIS registreres og tilsluttes NL3. IdP'en skal udstede et OIO-Boostrap-token (lokal IdP signeret), der kan anvendes til billetomveksling i SOSI føderationen. Formatmæssigt er OIO-Boostrap-tokenet en subprofilering af OIO Bootstrap Token v1.2 (under udarbejdelse af DIGST), hvor det primære informationsindhold er; NSIS LoA, Global Employee UUID, CVR-nummer, Issuer IdP, og eventuelt en liste med medarbejderens 'nationale roller'.	Jf. afsnit 7.2.2.1
GW (G11)	I GW skal der etableres en grænseflade der kan modtage et OIO-Bootstrap-token og via STS'en få udstedt et SOSI idkort, der efterfølgende caches i GW.	Jf. afsnit 7.3.1
STS (G5)	I SOSI STS'en skal der etableres en grænseflade der kan omveksle et OIO-Bootstraptoken til et SOSI idkort	STS omvekslingskaldet jf. 7.2.2
STS (G6)	Med MitID/NL3 indføres attributten 'Global Employee UUID' til identifikation af en erhversidentitet. MitID/NL3 udstiller en række lookup-services, der kan anvendes til at fastslå brugerens CPR-identitet ud fra Global Employee UUID. SOSI STS'en skal benytte de nye lookup-services til at udtrække brugerens CPR, da CPR er nøglen til opslag efter brugerens sundhedsfaglige autorisationer.	STS afhængigheder jf. afsnit 7.2
STS (G7)	STS algoritmen til at fastslå den autorisation/'national rolle', der skal fremgå af SOSI idkort, skal justeres. Algoritmen skal medtage, at udfaldsrummet for brugerens 'nationale roller' kan fremgå af OIO-Bootstrap-tokenet.	Jf. 7.2.2.2

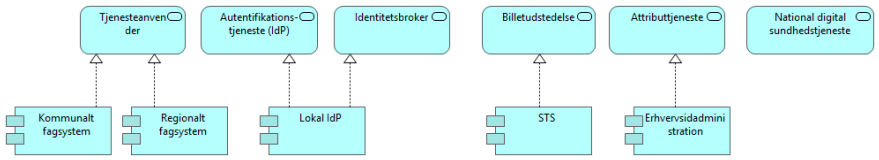
STS (G8)	SOSI Idkort skal justeres, da der ikke længere anvendes OCES certifikater i autentifikationsprocessen. Justeringen kan holdes indenfor DGWS standarden.	SOSI idkort justeringerne jf. 7.2.2.3

6.1.4 Føderationsscenariet: Ansattes adgang via rig Klient og egne identitetsmidler

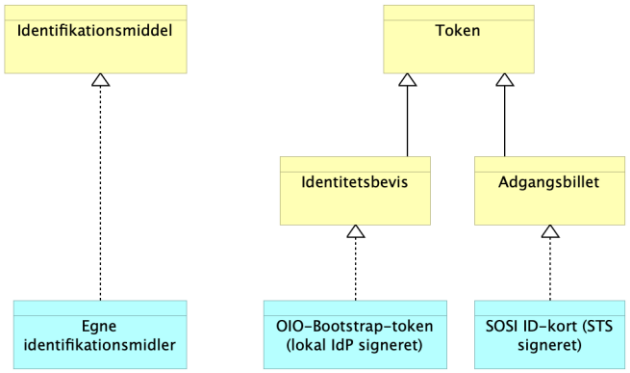
Målgruppen for dette scenarie er parter med egen lokale NSIS registrerede IdP. I modellen har anvenderorganisationen et lokalt system til caching af SOSI idkort. I scenariet ovenfor (føderationsscenarie med GW) blev caching af SOSI-idkort håndteret af SOSI-GW.
Modellen med caching i lokalt system er mere lagtidsholdbar og en godt skridt på vejen mod målbilledet (IDWS XUA), da SOSI-GW forventes udfaset ved på langt sigt (dvs. ved migration til IDWS XUA).

6.1.4.1 Komponentrealisering

Applikationskomponenter realiseres tilsvarende hybridscenariet:

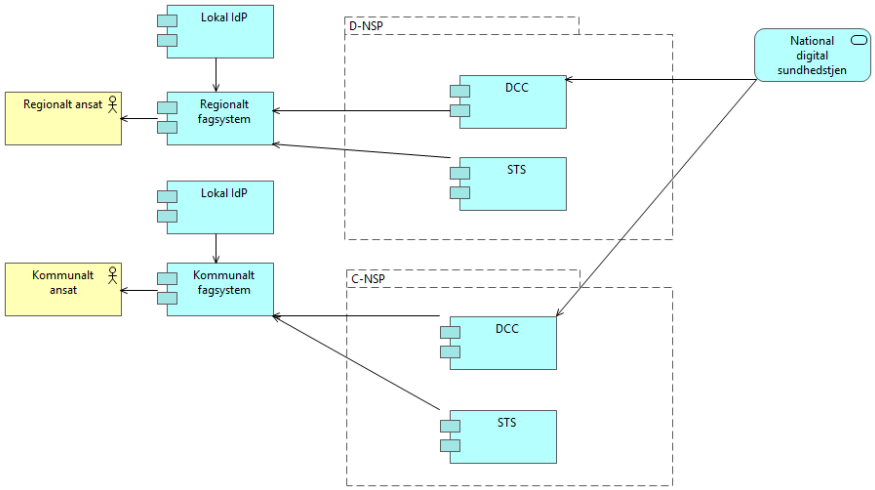


Informationsobjekter realiseres tilsvarende hybridscenariet:



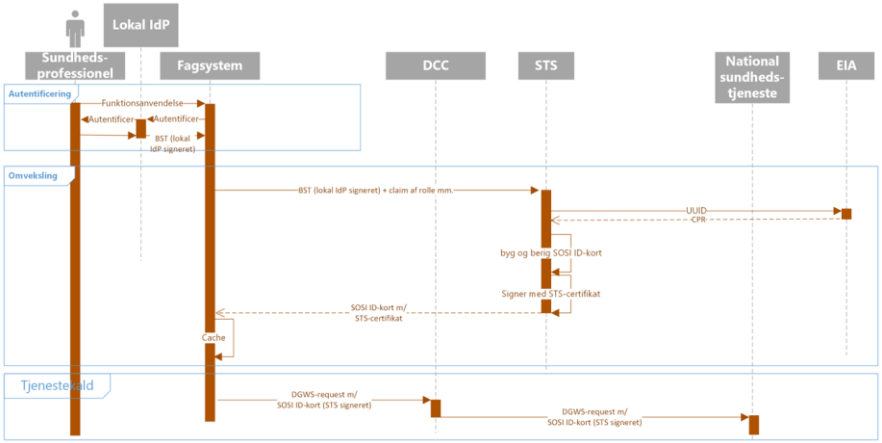
Figur 57: Realisering af informationsobjekter i hybridscenariet

6.1.4.2 Statiske sammenhænge



Figur 58: Statiske relationer ved føderationsscenariet for rige klienter.

6.1.4.3 Autentifikationsflow



Figur 59: Autentifikationsflow for ansatte med rig klient og egne identitetsmidler.

Valg af brugerkontekstens sundhedsfaglig autorisation eller nationale rolle håndteres af fagsystemet eller i forbindelse med medarbejderens netværkslogin.

6.1.4.4 Gapanalyse for føderations-scenariet med ansattes adgang via rig klient og egne identitets-midler

Kompo-nent (GapId)	**Ændring**	**Reference til yderligere info**
Bruger-admini-stration	Brugeren skal oprettes i EIA og havde tilknyttet sit CPR-nummer til EIA registreringen. I forbindelse med oprettelsesprocessen skal det lokale IDMS (A/D eller lign.) persistere den Globale Employee UUID, der erstatter RID og udgør brugerens primære ID i EIA. Nemlog-in3 har et IdM API til provisioneringspro-cessen. Sundhedsfaglige roller, ud over de sundhedsfaglige auto-risationer, administreres med fordel lokalt. Eksempelvis via lokalt IDMS.	Jf. https://mi-grering.nem-log-in.dk/nem-log-in-er-hvervslos-ning/avance-ret-setup/mo-deller/integra-tion-med-idm/idm-api-dokumentation
Lokal IdP	Den lokale IdP skal NSIS registreres og tilsluttes NL3. IdP'en skal udstede et OIO-Boostrap-token (lokal IdP sig-neret), der kan anvendes til billetomveksling i SOSI føde-rationen. Formatmæssigt er OIO-Boostrap-tokenet en subprofilering af OIO Bootstrap Token v1.2 (under udar-bejdelse af DIGST), hvor det primære informationsind-hold er; NSIS LoA, Global Employee UUID, CVR-num-mer, Issuer IdP, og eventuelt en liste med medarbejderens 'nationale roller'.	Jf. afsnit 7.2.2.1
STS (G5)	I SOSI STS'en skal der etableres en grænseflade der kan omveksle et OIO-Bootstraptoken til et SOSI idkort	STS omveks-lingskaldet jf. 7.2.2
STS (G6)	Med MitID/NL3 indføres attributten 'Global Employee UUID' til identifikation af en erhversidentitet. MitID/NL3 udstiller en række lookup-services, der kan anvendes til at fastslå brugerens CPR-identitet ud fra Glo-bal Employee UUID. SOSI STS'en skal benytte de nye lookup-services til at udtrække brugerens CPR, da CPR er nøglen til opslag ef-ter brugerens sundhedsfaglige autorisationer.	STS afhængig-heder jf. afsnit 7.2

STS (G7)	STS algoritmen til at fastslå den autorisation/'national rolle', der skal fremgå af SOSI idkort, skal justeres. Algoritmen skal medtage, at udfaldsrummet for brugerens 'nationale roller' kan fremgå af OIO-Bootstrap-tokenet.	Jf. 7.2.2.2
STS (G8)	SOSI Idkort skal justeres, da der ikke længere anvendes OCES certifikater i autentifikationsprocessen. Justeringen kan holdes indenfor DGWS standarden.	SOSI idkort justeringerne jf. 7.2.2.3

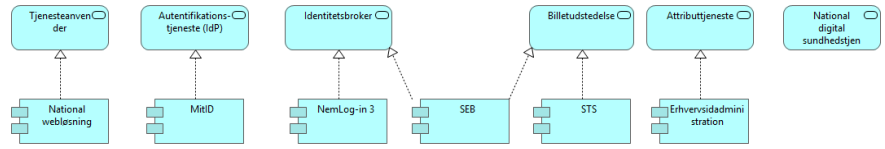
Tabel 5: Identificerede gaps

6.2 Ansattes adgang via browser

6.2.1 MitID-scenariet: Ansattes adgang via browser og MitID Erhverv

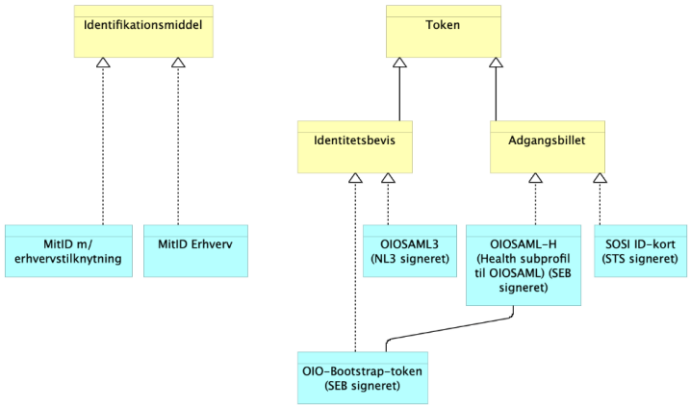
6.2.1.1 Komponentrealisering

Nedenfor vises realisering af de centrale applikationskomponenter:



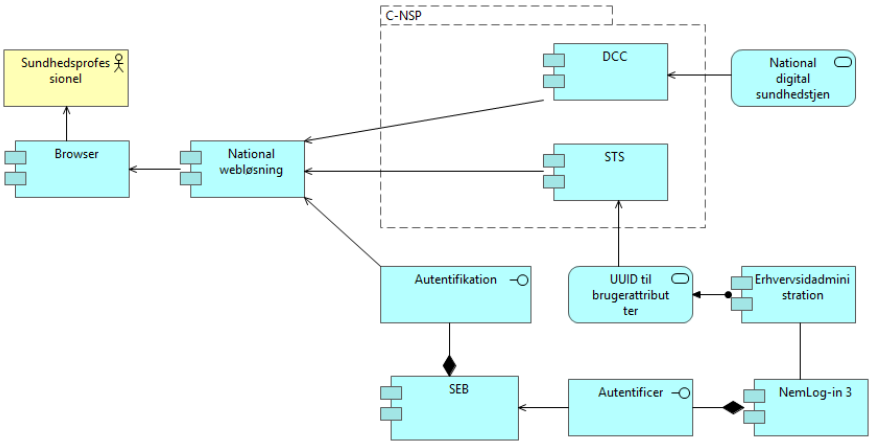
Figur 60: Realisering af de centrale applikationskomponenter

Nedenfor ses realisering af de centrale informationsobjekter:



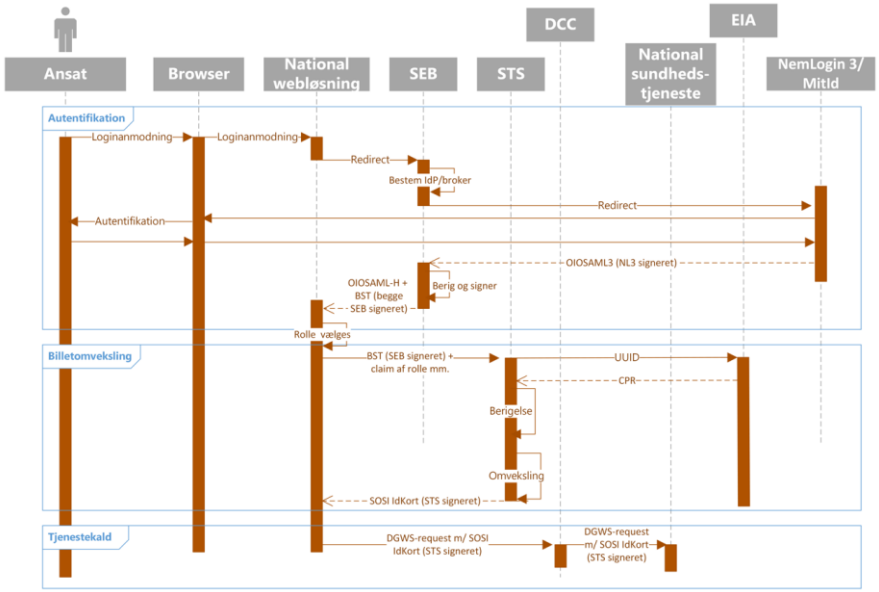
Figur 61: Realisering af de centrale informationsobjekter

6.2.1.2 Statiske sammenhænge



Figur 62: Statiske sammenhænge for ansattes adgang med browser og MitID

6.2.1.3 Autentifikationsflow



Figur 63: Autentifikationsflow for ansat, som tilgår en national webløsning via browser med MitID.

Valg af sundhedsfaglig rolle håndteres af medarbejderen umiddelbart før Billetomvekslingen. SEB udtrækker medarbejderens mulige autorisationer fra autorisationsregisteret og nationale roller fra SEB-classic, hvorefter de indlejres i OIOSAML-H tokenet. Herefter kan webløsningen lade medarbejderen vælge en rolle eller automatisk opsætte en rolle ud fra den konkrete kaldskontekst.

BST omveksles efterfølgende via NL3 STS'en til et OIO-Identity-token (audience SOSI STS).

I det illustrerede flow agerer SEB i rollen som broker mellem den nationale webløsning og Nemlog-in3/MitId. Alternativt kan den nationale webløsning vælge at tilgå Nemlog-in3/MitId direkte og efterfølgende via NL3 STS'en udtrække et OIO-Identity-token (audience SOSI STS), der kan anvendes ved adgang til sundhedsføderationen (i afsnit 6.1.1.5 anvendes dette koncept fra et fagsystem). Herved bliver den nationale Web-løsning uafhængig af SEB, men det har samtidig følgende konsekvenser:

1) Organisationer, hvis ansatte anvender MitId erhverv samt organisationer med en NSIS registreret lokal IdP, kan autentificeres via Nemlog-in3. Men organisationer, der anvender certifikatscenariet eller som anvender en ikke NSIS registeret IdP, vil ikke kunne tilgå den nationale webløsningen.
2) Organisationer, der administrerer nationale roller i egne systemer og uden kopi i SEB, kan ikke formidle rollerne til SOSI-STS'en, da Nemlog-in3 ikke videreformidler lokale roller fra tilknyttede NSIS registrerede IdP'er.
3) Organisation med lokale IdP'er bliver afhængige af Nemlog-in3, og såkaldt ø-drift udenom NL3 er ikke muligt.

6.2.1.4 Gapanalyse for ansattes adgang via browser og MitID Erhverv

Komponent (GapId)	**Ændring**	**Reference til yderligere info**
Brugeren	Erhvervsbrugeren skal kunne autentificere sig via en erhvervsidentitet, der er koblet til erhvervsbrugerens private MitID elektroniske identifikationsmidler, eller via dedikerede MitID-erhvervsidentifikationsmidler. Brugerens CPR-nummer skal tilknyttes EIA-registreringen.	Jf. DIGST.dk
SEB (G1)	Der skal etableres en tilslutningsaftale med NL3.	
SEB (G2)	I SEB skal der etableres et flow, hvor SEB agerer broker mellem lokal fagsystem/webserver og Nemlog-in3/MitId. SEB omdirigerer bruger til autentifikation i NL3/MitID. Ved succesfuld autentifikation returnerer NL3 et OIO-SAML3 token til SEB. SEB validerer tokenet, udtrækker brugerens sundhedsfaglige autorisationer og nationale roller, og udsteder et OIOSAML-H token med et indlejret OIO-Bootstrap-token. Begge tokens har listen med brugerens 'nationale roller' indlejret. OIOSAML-H tokenet har desuden listen med brugerens sundhedsfaglige autorisationer indlejret. De to SEB-signerede tokens returneres til webserveren.	SEB broker jf. afsnit 7.4.1 OIO-Bootstrap-token jf. afsnit 7.2.2.1
SEB (G3)	På kort sigt bliver SEB ikke NSIS registreret, og derfor udsteder SEB på kort sigt OIOSAML-H v1 tokens (Health subprofil til OIOSAML2). På langt sigt forventes SEB at blive NSIS registeret således, at SEB kan udstede OIOSAML-H v2 tokens (Health subprofil til OIO-SAML3). NSIS registrering kræver HSM-understøttelse i SEB	
SEB (G4)	Skalering: øget anvendelse af SEB nødvendiggør at SEB gøres mere skalerbar	

National Webløsning	Nationale webløsninger, der ikke kører SEB-vejen, skal til det (FMK og sundhed.dk mfl.). Som beskrevet under Figur 63: Autentifikationsflow for ansat, som tilgår en national webløsning via browser med MitID.Figur 63, så kan en national webløsninger alternativt tilgå NL3 direkte, men det har nogle konsekvenser.	
National Webløsning	Webløsningen kan aflæse brugerens mulige roller fra OIOSAML-H tokenet, samt lade medarbejderen vælge en rolle eller automatisk opsætte en rolle ud fra den konkrete kaldskontekst.	
STS (G5)	I SOSI STS'en skal der etableres en grænseflade der kan omveksle et OIO-Bootstraptoken til et SOSI idkort	STS omvekslingskaldet jf. 7.2.2
STS (G6)	Med MitID/NL3 indføres attributten 'Global Employee UUID' til identifikation af en erhversidentitet. MitID/NL3 udstiller en række lookup-services, der kan anvendes til at fastslå brugerens CPR-identitet ud fra Global Employee UUID. SOSI STS'en skal benytte de nye lookup-services til at udtrække brugerens CPR, da CPR er nøglen til opslag efter brugerens sundhedsfaglige autorisationer.	STS afhængigheder jf. afsnit 7.2
STS (G7)	STS algoritmen til at fastslå den autorisation/'national rolle', der skal fremgå af SOSI idkort, skal justeres. Algoritmen skal medtage, at udfaldsrummet for brugerens 'nationale roller' kan fremgå af OIO-Bootstrap-tokenet.	Jf. 7.2.2.2
STS (G8)	SOSI Idkort skal justeres, da der ikke længere anvendes OCES certifikater i autentifikationsprocessen. Justeringen kan holdes indenfor DGWS standarden.	SOSI idkort justeringerne jf. 7.2.2.3

6.2.2 Certifikat-scenariet: Ansattes adgang via browser og MOCES

Nemlog-in3 realiserer ikke en snitflade, hvorfra brugeren kan anvende sit MOCES3 certifikat til autentifikation. Dvs. en snitflade tilsvarende "Log på med nøglefil" på NemId.

For at kompenserer for dette er "Certifikat-scenariet: Ansattes adgang via browser og MOCES" realiseret. Løsningen er begrænset til autentifikation for webløsninger indenfor sundhedsområdet.

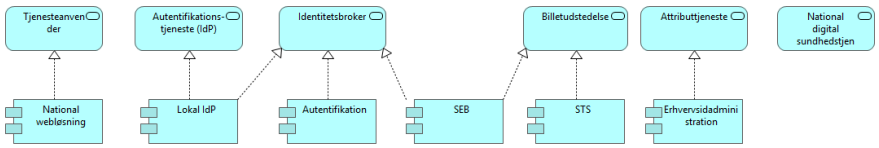
6.2.2.1 Sårjournal og FUT

I baseline for Sårjournalen og FUT (jf. afsnit 5.2.2) har det været muligt at lave en såkaldt "step-up" autentifikation. Dvs. hæve LoA-niveauet i det medsendte token fra den

lokale IdP via en supplerende autentifikation via NL2. Step-up autentifikation videreføres ikke i fase1, da step-up behovet bortfalder i og med, at de lokale IdP'er bliver NSIS-registreret.
Lokale IdP'er, der på kort sigt ikke bliver NSIS registeret, kan i stedet for anvende 'Certifikat-scenariet: Ansattes adgang via browser og MOCES', der behandles i dette afsnit.

6.2.2.2 Komponentrealisering

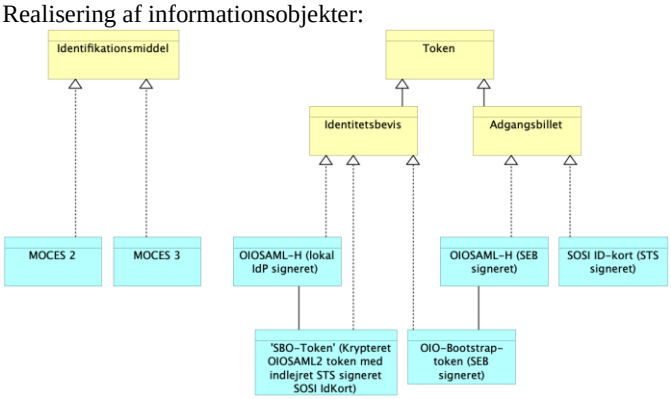
Realisering af applikationskomponenter:



Figur 64: Realisering af centrale applikationskomponenter

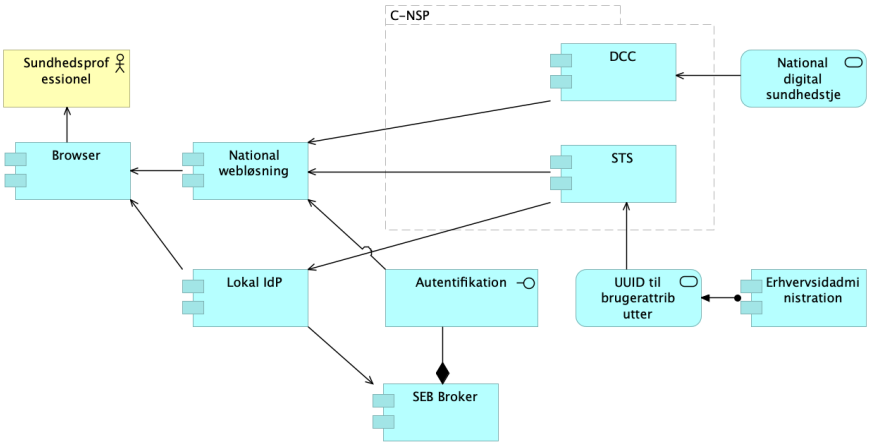
Bemærk indførelsen af en ny komponent, Autentifikation.

Realisering af informationsobjekter:



Figur 65: Realisering af centrale informationsobjekter

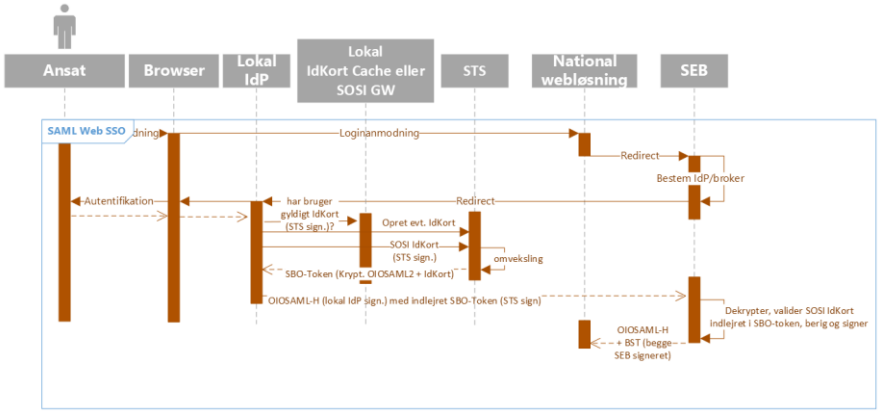
6.2.2.3 Statiske sammenhænge



Figur 66: Statiske sammenhænge ved browseradgang med certifikater

6.2.2.4 Autentifikationsflow

Herunder vises autentifikationsflowet. Billetomveksling og tjenestekald svarer til MitID-flowet, og er ikke gengivet her.



Figur 67: Autentifikationsflow for ansattes browseradgang med MOCES

I scenariet kan en lokal IdP, uden at være NSIS registreret, lave en WEB-SSO integration til SEB broker. Den lokale IdP beviser brugerens identitet overfor SEB via bruge-

rens STS signeret SOSI idkort. Den lokale IdP kan udtrække idkortet fra GW som et audience-krypteret SBO-token. Med audience-krypteret menes, at det kun er audience (her SEB), der kan dekryptere tokenet. Med SBO-token menes et krypteret OIOSAML2 token med et indlejret STS signeret SOSI idkort.
SBO-tokenet overføres til SEB via et [OIOSAML-H v1] token, der er en subprofil til OIOSAML2 med fokus på sundhedsområdet (Health).

Flow'et fra lokal IdP til 'Lokal idkort Cache eller SOSI GW' på Figur 67 er gengivet relativt overordnet. Ligger SOSI idkort i SOSI GW, så har SOSI GW forskellige services til at tjekke om der eksisterer et gyldigt idkort, samt til oprettet et nyt idkort (jf. afsnit 7.3). En lokal cache vil have behov for tilsvarende services.

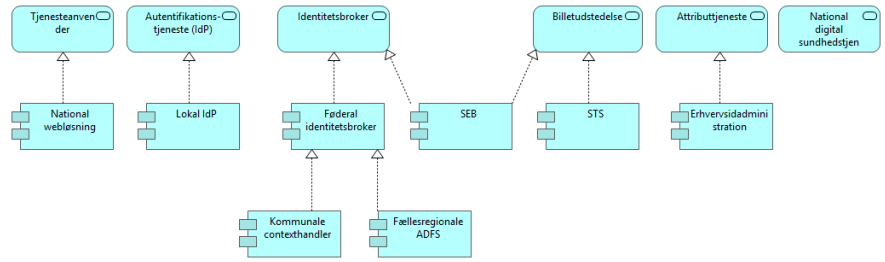
6.2.2.5 Gapanalyse for ansattes adgang via browser og MOCES

Komponent (GapID)	**Ændring**	**Reference til yderligere info**
Brugeren	Brugeren skal oprettes i EIA og havde tilknyttet sit CPR-nummer til EIA registreringen. Brugerens MOCES3 certifikat udtrækkes via et IdM certifikat API tilknyttet Nemlog-in3.	Jf. https://migrering.nemlog-in.dk/nemlog-in-erhvervsloesning/avanceret-setup/modeller/integration-med-idm/idm-api-dokumentation/
Lokal IdP	Lokal IdP autentificerer brugeren og tjekker om brugeren har et gyldigt SOSI idkort i den tilknyttede SOSI GW eller tilsvarende lokale Cache. Har brugeren ikke et gyldigt SOSI idkort, så aktiveres en proces til udstedelse af SOSI idkort på baggrund af brugerens MOCES3 certifikat (jf. afsnit 6.1.2). Efterfølgende omveksles brugerens SOSI idkort til et SBO-Token. Med SBO-token menes et krypteret OIOSAML2 token med et indlejret STS signeret SOSI idkort. Omvekslingen håndteres via SOSI STS grænsefladen SOSI2OIOSAML. SBO tokenet returnes til SEB indlejret i et OIOSAML-H token (lokal IdP signeret)	Jf. SOSI2OIOSAML STS grænsefalden i afsnit 7.2.3

Lokal id-kort Cache eller SOSI GW	SOSI idkort opbevares i en SOSI GW eller tilsvarende lokal cache.	
STS (G9)	Det skal sikres at SOSI STS'en kan håndtere OCES2/MOCES2 og OCES3/MOCES3 i en overgangsperiode.	Jf. afsnit 7.2.1
STS (G13)	Det skal sikres at SOSI2OIOSAML grænsefladen kan håndtere et SOSI idkort skabt pba. OIOSAML3/MOCES3. Dvs. et SOSI idkort uden certifikat oplysning som CVR-RID.	Jf. afsnit 7.2.3
SEB (G12)	I SEB skal der skabes understøttelse af certifikatscenariet illustreret på Figur 67. SEB omdirigerer medarbejderen til rette lokale IdP, hvorfra den certifikat baserede autentifikationsproces håndteres. Efter succesfuld autentifikation modtager SEB et OIOSAML-H v1 (Health subprofil af OIOSAML2) token med et indlejret SBO-Token (et krypteret OIOSAML2 token med indlejret STS signeret idkort). SEB dekrypterer tokenet, validerer tokenet (herunder SOSI idkortet) og udtrække brugerens sundhedsfaglige autorisationer og 'nationale roller' (med mindre de er medsendt fra lokal IdP). Herefter udstedes et OIOSAML-H token med et indlejret OIO-Bootstrap-token. Begge tokens er SEB signerede. Begge tokens indeholder listen med brugerens 'nationale roller'. OIOSAML-H tokenet indeholder desuden listen med brugerens sundhedsfaglige autorisationer. De to tokens returneres til webløsningen.	SEB broker jf. afsnit 7.4.1 OIO-Bootstrap-token jf. afsnit 7.2.2.1
National Webløsning	Webløsningen kan aflæse brugerens mulige roller fra OIOSAML-H tokenet, samt lade medarbejderen vælge en rolle eller automatisk opsætte en rolle ud fra den konkrete kaldskontekst	
STS (G5)	I SOSI STS'en skal der etableres en grænseflade der kan omveksle et OIO-Bootstraptoken til et SOSI idkort	STS omvekslingskaldet jf. 7.2.2
STS (G7)	STS algoritmen til at fastslå den autorisation/'national rolle', der skal fremgå af SOSI idkort, skal justeres. Algoritmen skal medtage, at udfaldsrummet for brugerens 'nationale roller' kan fremgå af OIO-Bootstrap-tokenet.	Jf. 7.2.2.2
STS (G8)	SOSI Idkort skal justeres, da der ikke længere anvendes OCES2 certifikater i autentifikationsprocessen. Justeringen kan holdes indenfor DGWS standarden.	SOSI idkort justeringerne jf. 7.2.2.3

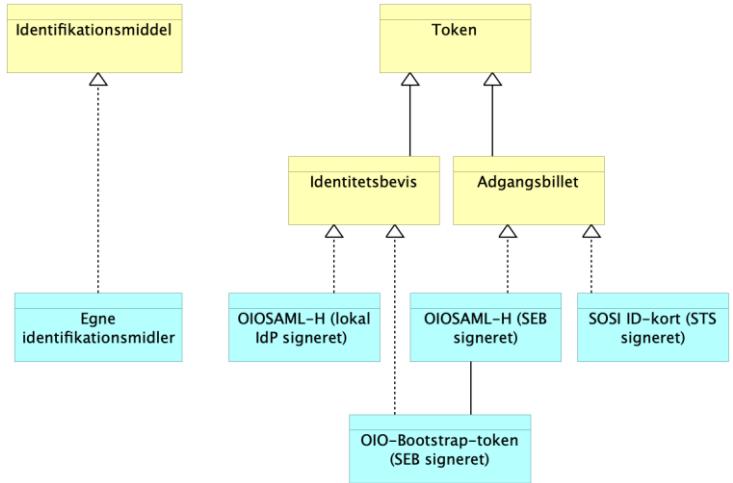
6.2.3 Føderationsscenariet: Ansattes adgang via browser og egne identitetsmidler

6.2.3.1 Komponentrealisering



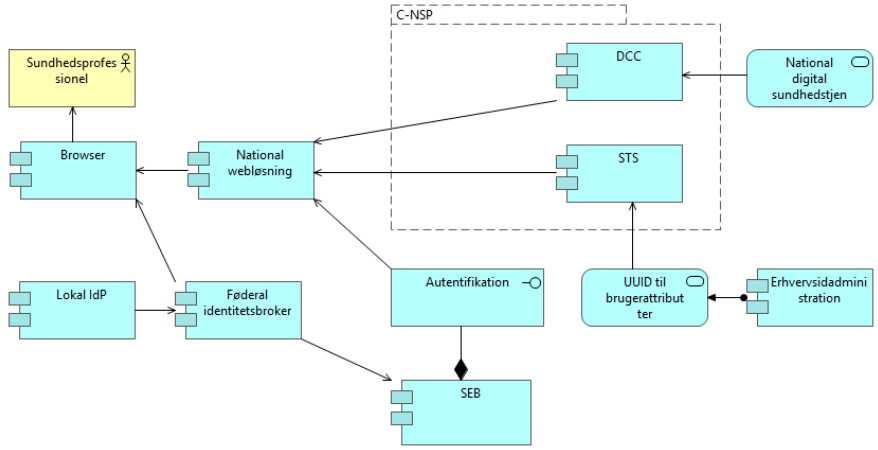
Figur 68: Realisering af applikationskomponenter

6.2.3.2 Realisering af informationsobjekter:



Figur 69: realisering af informationsobjekter

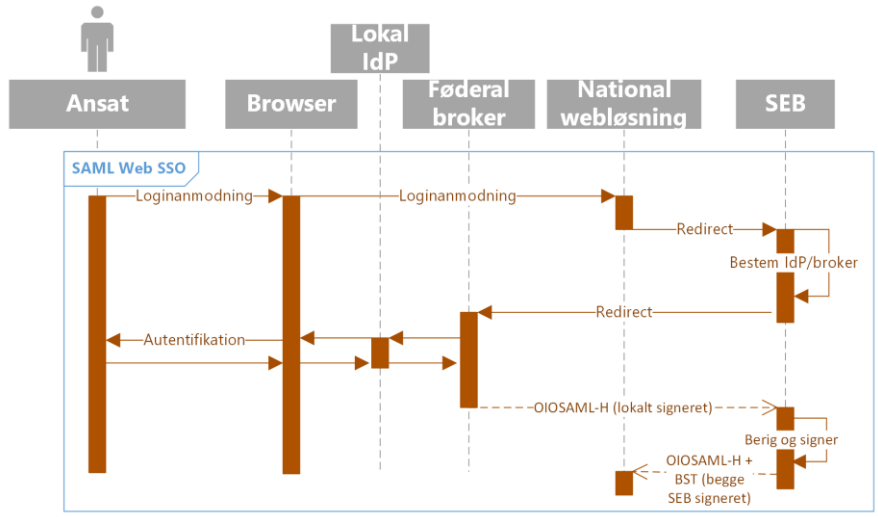
6.2.3.3 Statiske sammenhænge



Figur 70: Statiske sammenhænge

6.2.3.4 Autentifikationsflow

Herunder vises autentifikationsflowet. Billetomveksling og tjenestekald svarer til MitID-flowet, og er ikke gengivet her.



Figur 71: Autentifikationsflow for ansattes browseradgang med egne identitetsmidler

På figuren fremgår både en lokal IdP og en føderal broker. Et eksempel på det sidste er Kombits ContextHandler. Ofte vil der ikke eksisterer en føderal broker, og den lokale IdP vil integrere direkte med SEB.
Den nationale webløsning modtager adgangsbillet til webløsningen i form af et OIO-SAML-H token samt et indlejret OIO-Bootstrap-token. Med OIO-Bootstrap-tokenet kan webløsningen få udstedt en adgangsbillet (et SOSI idkort), der giver adgang til de nationale sundhedstjenester.

I forbindelse med billetomvekslingsflowet, som ikke er vist på figuren, skal webløsningen "claime" den sundhedsfaglige rolle, der skal fremgå af SOSI idkortet. OIOSAML-H tokenet indeholder en liste med de autorisationer og 'nationale roller', som brugeren kan anvende. De 'nationale roller' overføres fra den lokale IdP eller opsættes via SEB i det tilfælde, hvor rollerne administreres centralt i SEB classic. Autorisationerne opsættes af SEB.

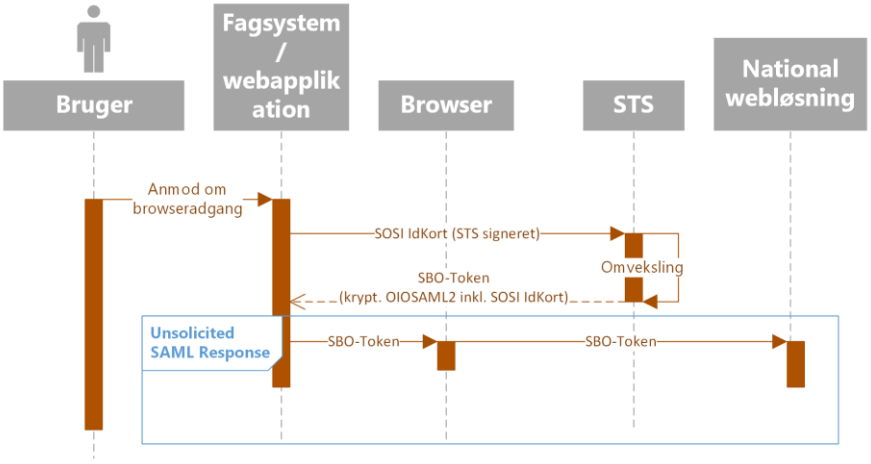
6.2.3.5 Gapanalyse for ansattes adgang via browser og egne identitetsmidler

Komponent (GapId)	**Ændring**	**Reference til yderligere info**
Brugeren	Brugeren skal oprettes i EIA og havde tilknyttet sit CPR-nummer til EIA registreringen. I forbindelse med opretsesprocessen skal det lokale IDMS (A/D eller lign.) persistere Globale Employee UUID, der erstatter RID og udgør brugerens primære ID i EIA. Nemlog-in3 har et IdM API til provisioneringsprocessen.	Jf. https://migrering.nemlog-in.dk/nemlog-in-erhvervslosning/avanceret-setup/modeller/integration-med-idm/idm-api-dokumentation/
Lokal IdP/Føderal broker	Lokale IdP/Føderal broker skal være NSIS registreret og kunne udstede et OIOSAML-H token til SEB. OIOSAML-H tokenets primære informationsindhold er; NSIS LoA, Global Employee UUID, CVR-nummer, Issuer IdP, og eventuelt en liste med medarbejderens ikke_autoriserede roller.	OIO-Bootstrap-token jf. afsnit 7.2.2.1
SEB (G14)	I SEB skal der skabes understøttelse af egne identitetsmidler-scenariet (NSIS registreret lokal IdP) illustreret på Figur 71. SEB modtager et OIOSAML-H v2 (Health subprofil af OIOSAML3) token fra lokal IdP/føderal broker, validerer tokenet, beriger med medarbejderens autorisationer og	SEB broker jf. afsnit 7.4.1 OIO-Bootstrap-token jf. afsnit 7.2.2.1

	'nationale roller', hvis ikke disse allerede er opsat fra IdP. Herefter udstedes et SEB signeret OIOSAML-H token med lejret OIO-Bootstrap-token, som returneres til den nationale webløsning.	
SEB (G3)	På kort sigt bliver SEB ikke NSIS registreret, og derfor udsteder SEB på kort sigt OIOSAML-H v1 tokens (Health subprofil til OIOSAML2). På langt sigt forventes SEB at blive NSIS registeret således, at SEB kan udstede OIOSAML-H v2 tokens (Health subprofil til OIO-SAML3). NSIS registrering kræver HSM-understøttelse i SEB	
SEB (G4)	Skalering: øget anvendelse af SEB nødvendiggør at SEB gøres mere skalerbar	
National Webløs-ning	Nationale webløsninger, der ikke kører SEB-vejen, skal til det (FMK og sundhed.dk mfl.)	
National Webløs-ning	Webløsningen kan aflæse brugerens mulige roller fra OIOSAML token, samt lade medarbejderen vælge en rolle eller automatisk opsætte en rolle ud fra den konkrete kaldskontekst	
STS (G5)	I SOSI STS'en skal der etableres en grænseflade der kan omveksle et OIO-Bootstraptoken til et SOSI idkort	STS omveks-lingskaldet jf. 7.2.2
SEB, STS (G6)	Med MitID/NL3 indføres attributten 'Global Employee UUID' til identifikation af en erhversidentitet. MitID/NL3 udstiller en række lookup-services, der kan anvendes til at fastslå brugerens CPR-identitet ud fra Global Employee UUID. SOSI STS'en skal benytte de nye lookup-services til at udtrække brugerens CPR, da CPR er nøglen til opslag efter brugerens sundhedsfaglige autorisationer. SEB skal kun benytte de nye lookup-services i de tilfælde, hvor CPR ikke er indehold til OIOSAML tokenet fra IdP.	STS afhængig-heder jf. afsnit 7.2
STS (G7)	STS algoritmen til at fastslå den autorisation/'national rolle', der skal fremgå af SOSI idkort, skal justeres. Algoritmen skal medtage, at udfaldsrummet for brugerens'nationale roller' kan fremgå af OIO-Bootstrap-tokenet.	Jf. 7.2.2.2
STS (G8)	SOSI Idkort skal justeres, da der ikke længere anvendes OCES certifikater i autentifikationsprocessen. Justeringen kan holdes indenfor DGWS standarden.	SOSI idkort ju-steringerne jf. 7.2.2.3

6.2.4 Ansattes adgang via browser og fagsystem (Sikker browser-opstart)

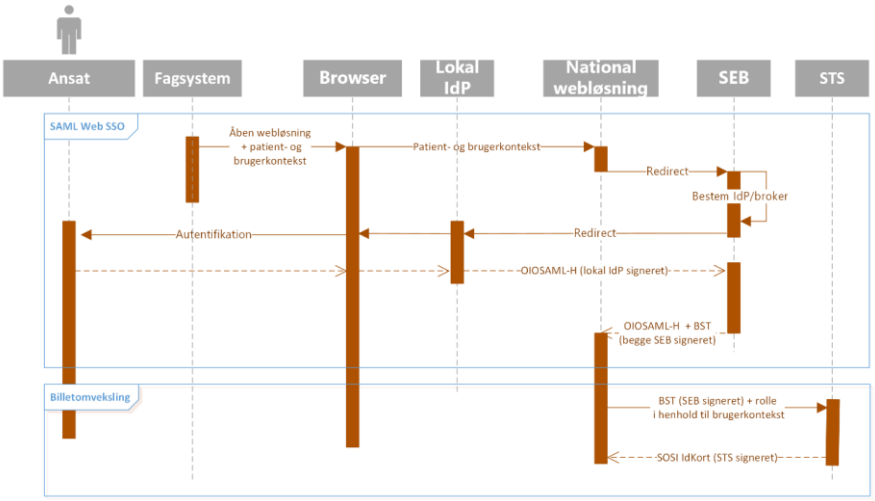
Sikker browseropstart håndteres umiddelbart som i AS-IS scenariet (jf. afsnit 5.3), hvilket er gentaget på figuren nedenfor.



Figur 72: Ansattes adgang via browser og fagsystem (Sikker browseropstart)

SBO er primært medtaget i Fase1 for at være bagud kompatibel med Baseline. Under Fase1 kan tilsvarende realiseres uden brug af STS omvekslingskaldet 'SOSI2OIO-SAML', som illustreret på Figur 73.

I Baseline udgør SOSI idkortet beviset på, at brugeren er autentificeret og godkendt af SOSI infrastrukturen. I Fase1 er der tillid til, at NSIS-registrerede IdP'er kan autentificere brugeren på tilstrækkeligt højt sikkerhedsniveau, og OIOSAML3 tokenet er bevis på brugerens identitet.
Figur 73 viser et alternativt Sikker BrowserOpstart scenarie, hvor ovenstående udnyttes.



Figur 73: Alternativ til SBO uden SOSI2OIOSAML omveksling

Hvis fagsystemet ønsker at åbne den nationale webløsning i en bestemt kontekst, fx med en bestemt patient og en bestemt sundhedsfaglige rolle, så skal denne kontekst medsendes når webløsningen åbnes (via et proprietært aftalt format). Herefter kan webløsningen lave en SAML WEB-SSO autentifikation via SEB.
SEB truster den lokale IdP, der udsteder et OIOSAML-H token og indlejre de lokalt administrerede 'nationale roller'. SEB beriger med medarbejderens autorisationer fra autorisationsregisteret og udsteder et OIOSAML-H token og OIO-Bootstrap-token til webløsning.
Webløsningen kan aflæse medarbejderes tilladte sundhedsfaglige roller via OIOSAML-H tokenet, og kan dermed tjekke om brugerkonteksten fra fagsystemet er tilladt. Webløsningen omveksler OIO-Bootstrap-token til et SOSI idkort via SOSI STS'en. Som input til omvekslingskaldet medsendes et 'claim' med den sundhedsfaglige rolle, der skal opsættes i SOSI idkortet.
SOSI STS truster OIO-Bootstrap-tokenet fra SEB og kan herfra afgøre om den ønskede (claim) rolle er tilladt.

6.2.4.1 Gapanalyse for ansattes adgang via sikker browseropstart

Nedenstående gapanalyse relaterer sig til det oprindelige SBO-flow i henhold Figur 72.

Komponent (GapID)	**Ændring**	**Reference til yderligere info**
STS (G13)	Det skal sikres at SOSI2OIO-SAML grænsefladen kan håndtere et SOSI idkort skabt pba. OIO-	Jf. afsnit 7.2.3

	SAML3/MOCES3. Dvs. et SOSI id-kort uden certifikat oplys-ning som CVR-RID.	
National Webløs-ning	Check om de Nationale Webløsnin-ger, der er konfigureret til SBO, kan opstartes med et SBO-token(krypte-ret OIOSAML2 token med indlejret STS signeret SOSI idkort), hvor OIOSAML2 er mangelfuldt udfyldt mht. CVR-RID.	Jf. afsnit 7.2.3.1

6.3 Systemadgang via web-services

I visse situationer kan en tjenesteanvender få adgang til en sundhedstjeneste på bag-grund af tokens, der alene identificerer tjenesteanvenderen og dermed ikke en fysisk bruger.

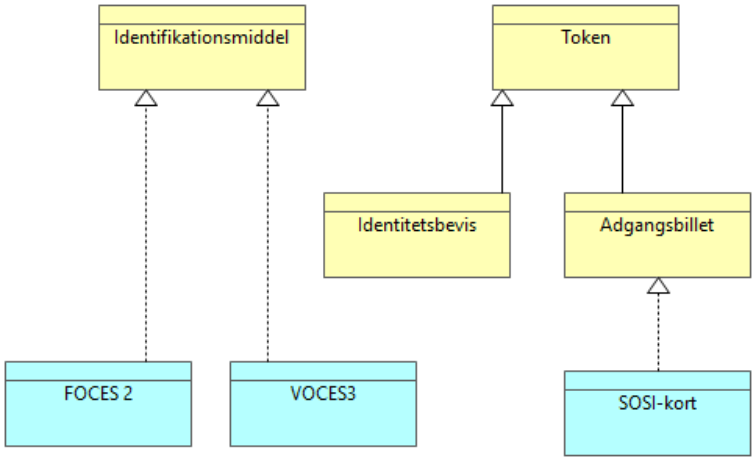
Det kan være et batch-job, der automatisk henter data fra en sundhedstjeneste, og hvor sundhedstjenesten ikke kræver, at kaldet skal initieres af en identificerbar person.

Der kan også være trust-baseret adgang. Det vil sige en trustaftale mellem tjenestean-vender og sundhedstjeneste, hvor det defineres, at det er tjenesteanvenderens ansvar at kontrollere og administrere bruger-identitet og -adgang. På sigt forventes det at disse trustaftaler udfases.

6.3.1 Komponentrealisering

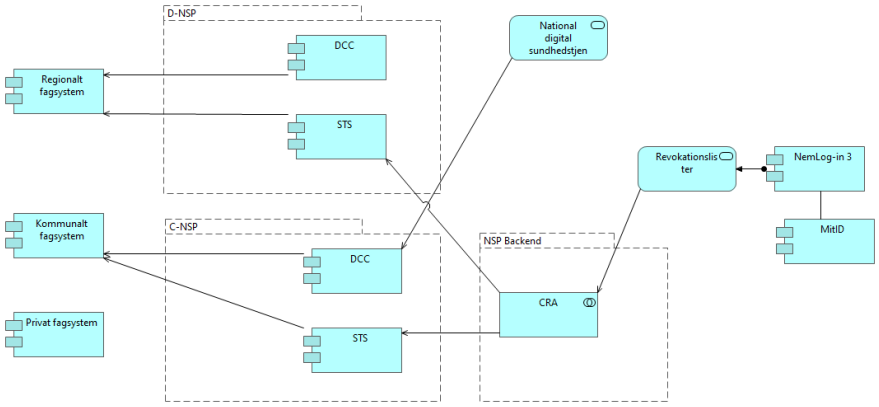
Applikationskomponenter svarer til baseline.

Informationsobjekter realiseres på følgende vis:



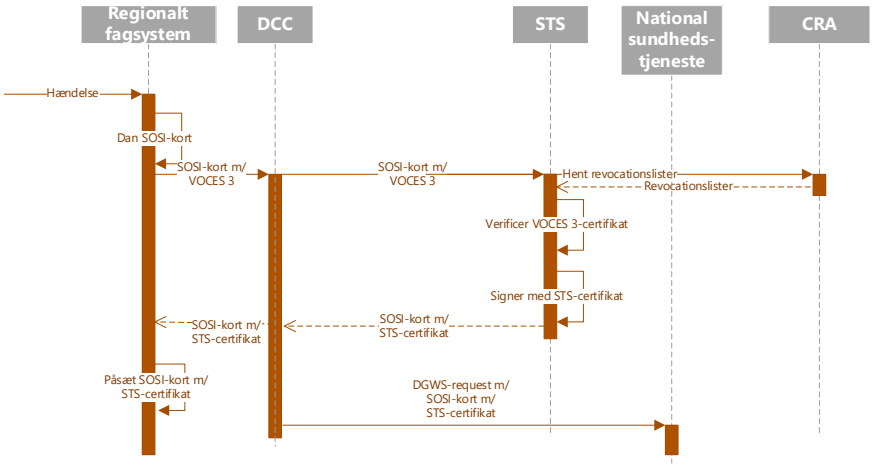
Figur 74: Realisering af informationsobjekter

6.3.2 Statiske sammenhænge



Figur 75: Statiske sammenhænge ved systemadgange

6.3.3 Autentifikationsflow



Figur 76: Autentifikationsflow

6.3.3.1 Gapanalyse for systemadgang via webservices

Kompo-nent (GapID)	***Ændring***	**Reference til yderligere info**
STS (G9)	Det skal sikres at SOSI STS'en kan håndtere OCES2 og OCES3 i en overgangsperiode.	Jf. afsnit 7.2.1
CRA (G10)	Caching af OCES3 revocationslister	Jf. afsnit 7.7

6.4 Borgeradgang model-lerne

Borgeradgangsmodellerne designes under hensyntagen til at:

1) en borgervendt web-løsning eller app skal have flere muligheder i valget af bro-ker/autentifikationsløsninger(herunder på sigt de nye MitID-brokers for private borgervendt løsninger, som MitID åbner op for). Dog under forudsætning af, at broker/autentifikationsløsning lever op til sundhedsføderationens governance-krav og understøttede tokenformater og -indhold.

2) sundhedstjenesterne ikke påvirkes. IDWS-protokollen mod sundhedstjenesterne fastholdes og sundhedstjenesterne skal udelukkende håndtere identity tokens fra SOSI STS.
3) ændringer i de eksisterende tjenesteanvender (app- eller webbaseret) holdes på et minimum. Visse ændringer er dog påkrævet, da MitID/NL3 ikke længere tillader SOSI STS omveksling af NL3 udstedte BST tokens. NL3 BST tokens bliver muligvis 'opaque' (kun læsbar for NL3 STS). Desuden overholder den eksisterende anvendelsen i baseline ikke et princip om at anvende tokens til rette formål

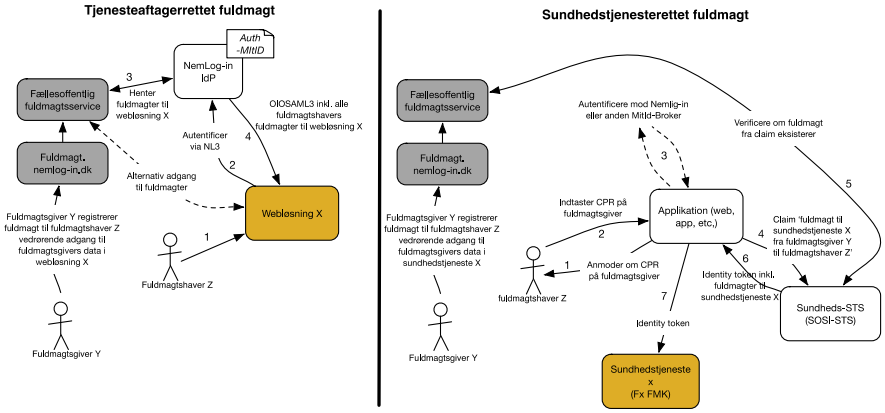
Tabellen nedenfor giver overblik over de fire borgeradgangs scenarier, som er udvalgt til viderebehandling i målarkitekturen. På grund af punkt 1 ovenfor, så kan der komme andre scenarier på sigt, efterhånden som nye MitID-brokerløsninger etableres og tages i brug.

Borgerad-gangs-scenarier	Primær målgruppe og hvad understøttes/understøttes ikke	Ændringer for tjenesteaftager fra baseline til fase1
Webløsning der tilgår Nemlog-in3 direkte	Web-løsninger, der i Baseline tilgår Nemlog-in2/NemID direkte.	Adgang til en sundhedstjeneste kræver to token-omvekslinger, hvor der i baseline kun var en. De to omvekslinger er: 1) OIO Bootstraptoken (BST) fra NL3 omveksles til et Identity token (audience SOSI STS) via NL3 STS. 2) Identity tokenet fra NL3 STS (se punkt 1) omveksles til et Identity token (audience sundhedstjeneste) via SOSI STS'en
Webløsning der tilgår Nemlog-in3 via SEB	Web-løsninger, der i Baseline tilgår Nemlog-in2 via SEB. I baseline kunne private webløsninger ikke tilgå Nemlog-in2 direkte. Sundhedsområdet frikøbte derfor autentifikation via NL2 for private sundhedsløsninger, og kontrollerede adgangen via SEB.	1) Små tilpasninger til OIOSAML2 tokenet fra SEB, da dette baseres på version 2.1.0 frem for version 2.0.9. Denne ændring er allerede trådt i kraft pr. 19. april 2021, i forbindelse med NemLog-in3 go-live. 2) Nyt BST token fra SEB
Mobil app der tilgår Nemlog_3 via Autorizations-server	Mobile app, som i forvejen tilgår en NemLog-in via en OIDC autorizations-server (AS). Nuværende AS anvendes af FMK og MinLæge APP	Ingen ændringer

Applikation (mobile apps, webløsninger mm.) der tilgår en MitID-Broker	Applikation (app, web, eller andet), der ønsker at anvende en af de nye MitId-broker frem Nemlog-in3. Autentifikation via MitId-broker er pt. forbeholdt private app's, da offentlige *skal* gå via NL3	Nyt koncept indført i forbindelse med MitID/Nemlog-in3 SOSI-føderationen stoler på tokens fra en NSIS registreret MitId-broker, og tokens herfra kan omveksles via SOSI-STS til adgangsbilletter i form af OIO Identity tokens.
Borgers adgang til webløsning via app (SBO)	App, der vil sende borger over til en webløsning via Sikker-Browser-Opstart	Ingen ændringer

6.4.1 Fuldmagt i forbindelse med borgeradgang

En borger (fuldmagtsgiver) kan give fuldmagt til, at en anden borger (fuldmagtshaver) må tilgå borgerens (fuldmagtsgivers) sundhedsdata. I målarkitekturen skelnes mellem tjenesteaftagerrettet og sundhedstjenesterettet fuldmagter, som illustreret på Figur 77.



Figur 77: Forskel på tjenesteaftager og sundhedstjeneste rettet fuldmagt

For begge typer at fuldmagter gælder, at de oprettes i den fællesoffentlige fuldmagtsløsning 'Fuldmagt.nemlog-in.dk'. En fuldmagtsgiver registrerer fuldmagt til fuldmagtshaver vedrørende adgang til fuldmagtsgivers data i et specificeret system.

Det, som målarkitekturen omtaler 'Tjenesteaftagerrettede fuldmagter', er digitale fuldmagter målrettet den klient (webløsning eller app), som borgeren tilgår. Fuldmagthavers fuldmagter til klienten overføres via OIOSAML tokenet fra Nemlog-in til klienten i forbindelse med Nemlog-in autentifikationen.

Alternativ kan klienten hente fuldmagter direkte fra den fællesoffentlige fuldmagtsservice via et SOAP-API.

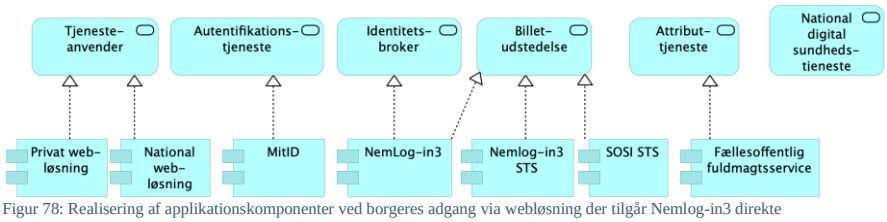
Det, som målarkitekturen omtaler 'Sundhedstjenesterettede fuldmagter', er digitale fuldmagter målrettet en sundhedstjeneste. Dvs. den bagvedliggende service, som klienten henter data fra. Fuldmagten kan anvendes fra alle klienter, der tilgår kilden. En fuldmagt til FMK-sundhedstjenesten kan eksempelvis anvendes fra klienterne MinSundhed app, MinLæge app og Medicinkort app. Sundhedstjenesterettede fuldmagter registreres formelt til systemet 'SOSI STS', og det er dermed SOSI STS'en, der validerer fuldmagtsadgang til sundhedstjenesterne i forbindelse med udstedelse af adgangstokens til de enkelte sundhedstjenester.
Tjenesteaftageren beder borgeren (fuldmagtshaveren) om at indtaste CPR på den fuldmagtsgiver, som fuldmagtshaver skal handle på vegne af. Tjenesteaftager skal i omvekslingskaldet "claime" de fuldmagter, der skal inkluderes i OIOIDWS tokenet (fx fuldmagt til sundhedstjeneste X fra fuldmagtsgiver Y). SOSI STS validere claim'et via opslag i den fællesoffentlige fuldmagtsservice og inkludere herefter fuldmagten i Identity tokenet.

Selvom det ikke fremgår af kapitel 5, så understøttes fuldmagt af baseline borger-scenarierne. I fase1 borger-scenarierne er fuldmagtsunderstøttelsen medtaget på figurerne.

6.4.2 Borgeres adgang via browser: Webløsning der tilgår Nemlog-in3 direkte

Scenariet er relevant for private og nationale web-løsninger, der ønsker en direkte integration til Nemlog-in3 og dermed igen afhængighed til SEB-broker. Scenariet er attraktivt for webløsninger, der i forvejen er integreret til Nemlog-in2.
Den direkte integration til NL3 gør desuden, at tjenesteanvenderrettede fuldmagter kan overføres via OIOSAML3 tokenet fra NL3 i forbindelse med brugerautentifikationen, fremfor igennem fuldmagts-servicens SOAP-API.

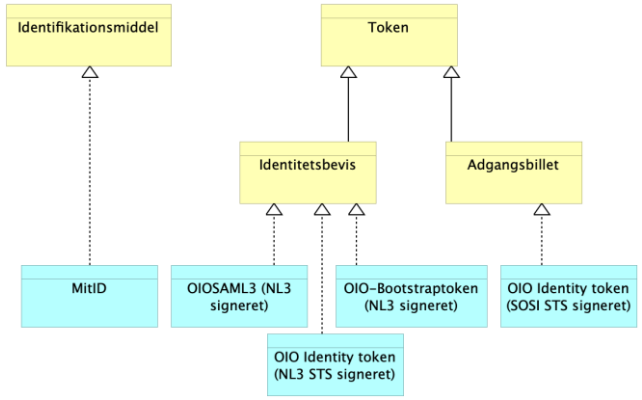
6.4.2.1 Komponentrealisering



Figur 78: Realisering af applikationskomponenter ved borgeres adgang via webløsning der tilgår Nemlog-in3 direkte

I baseline blev OIO-Bootstraptokenet fra NL2 anvendt i SOSI STS omvekslingen. Dette er ikke muligt i NL3 (jf. afsnit 6.4), og derfor er der behov for en ekstra omveksling via NL3 STS'en til et OIO Identity token, der kan anvendes til omveksling via SOSI STS'en.

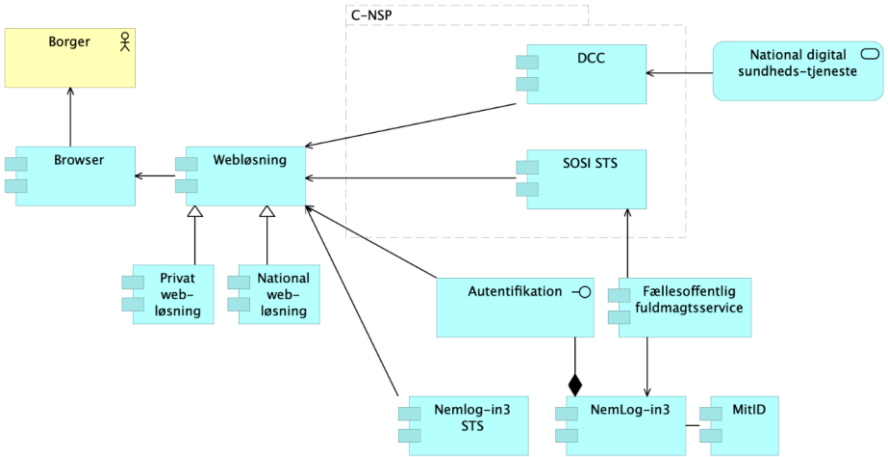
6.4.2.2 Realisering af informationsobjekter



Figur 79: Realisering af informationsobjekter ved borgeres adgang via webløsning der tilgår Nemlog-in3 direkte

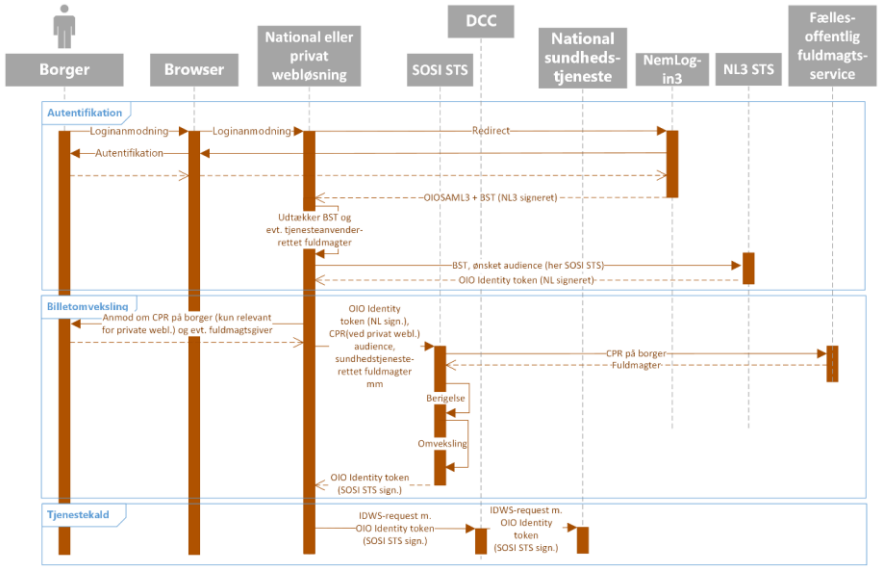
Af Figur 79 fremgår 'OIO Identity token' både som et Identitetsbevis og en Adgangsbillet. 'OIO Identity token' er en OIOSAML token profil (det præcise navn er 'OIO SAML Profile for Identity Tokens').
NL3 STS'en kan udstede et Identitetsbevis, der beviser borgerens identitet', og som tjenesteanvender kan omveksle (via SOSI-STS) til en adgangsbillet målrettet en bestemt sundhedstjeneste. Begrebsmæssigt er det desværre forvirrende, at den fællesoffentlige OIO Identity Token profil både optræder som et Identitetsbevis og en Adgangsbillet.

6.4.2.3 Statiske sammenhænge



Figur 80: Statiske sammenhænge

6.4.2.4 Autentifikationsflow



Figur 81: Autentifikationsflow for borgeres adgang til nationale webløsninger

I autentifikations-svømmebanen vises, at webløsningen kan udtrække OIO-Bootstraptoken (BST) og tjenesteanvenderrettet fuldmagter fra OIOSAML3 tokenet, der er modtaget fra NL3.
BST omveksles via NL3 STS til et OIO-Identitytoken, hvor audience er sat til SOSI STS'en.

Offentlige webløsningen kan aflæse borgerens CPR-nummer af OIOSAML3 tokenet, men CPR-nummer udleveres ikke til private web-løsninger.
Billetomvekslings-svømmebanen indledes med at webløsningen anmoder borgeren om at indtaste sit CPR (kun relevant for private webløsninger), samt CPR på evt. fuldmagtsgiver, med henblik på at få opsat sundhedstjenesterettet fuldmagter i det OIO-Identitytoken, der skal anvendes i kaldet til sundhedstjenesten. Webløsningen omveksler det OIO-Identitytoken, der er modtaget fra NL3 STS, til et OIO-Identitytoken målrette sundhedstjenesten via SOSI STS'en. Til SOSI STS omvekslingskaldet medsendes en række claims, og herunder borgers CPR (relevant for private webl.), audience (dvs. den sundhedstjeneste der ønskes adgang til) og fuldmagter. Claim af fuldmagt valideres via et opslag i den fællesoffentlige fuldmagtsservice. Handler borgeren på egne vegne, skal der selvfølgelig ikke medsendes et 'claim' vedr. fuldmagt.

Tjenesteanvendere, der ikke tilgår borgerens sundhedsdata i de nationale sundhedstjenester, kan nøjes med den første del af autentifikationsflowet på Figur 81 (dvs. autentifikations-svømmebanen). Dette forhold gælder alle borgerscenarierne.

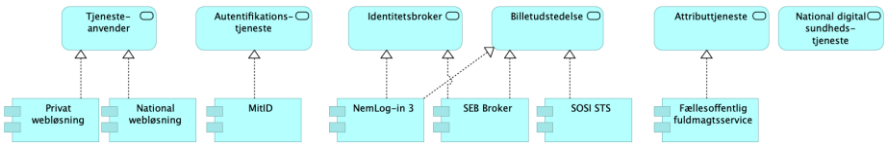
6.4.2.5 Gapanalyse for borgeres adgang til nationale webløsninger via browser og MitID

Komponent (GapID)	**Ændring**	**Reference til yderligere info**
Webløsning	Tilslutningsaftale med NL3 STS	
STS (G19)	I SOSI-STS'en skal der etableres en grænseflade, der kan udstede et OIO Identity token målrette en sundhedstjeneste pba. et OIO Identity token fra NL3 STS	Jf. afsnit 7.2.4

6.4.3 Borgeres adgang via browser: Webløsning der tilgår Nemlog-in3 via SEB

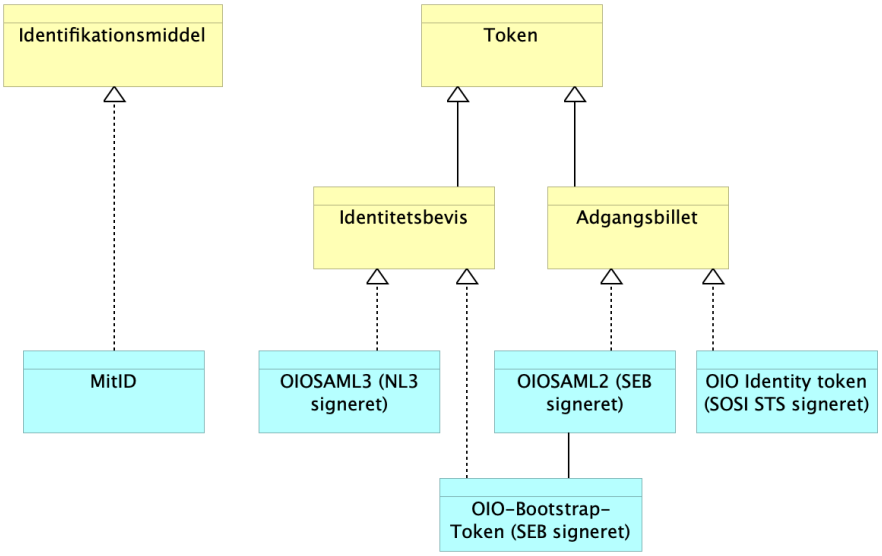
Scenariet er relevant for private og offentlige web-løsninger, der i Basline tilgår Nemlog-in2 via SEB.
I baseline kunne private webløsninger ikke tilgå Nemlog-in2 direkte. Sundhedsområdet frikøbte derfor autentifikation via NL2 for private sundhedsløsninger, og kontrollerede adgangen via SEB.

6.4.3.1 Komponentrealisering



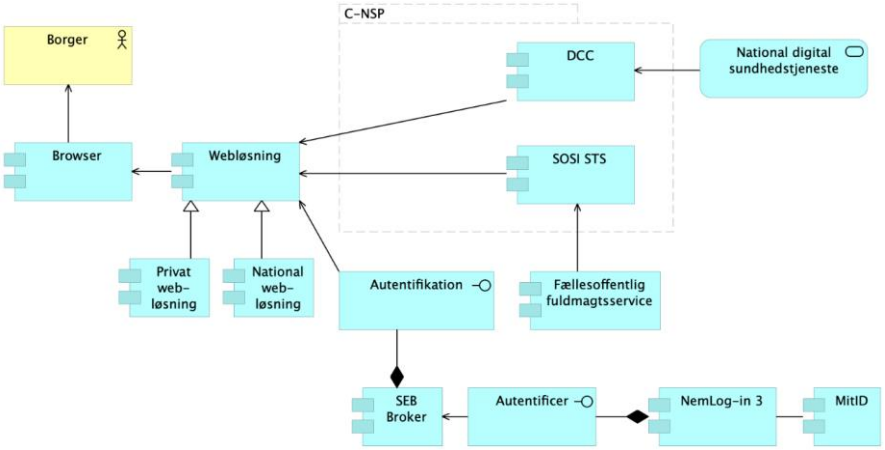
Figur 82: Realisering af applikationskomponenter ved borgeres adgang via browser med MitID

6.4.3.2 Realisering af informationsobjekter



Figur 83: Realisering af informationsobjekter ved borgeres adgang via browser og MitID

6.4.3.3 Statiske sammenhænge



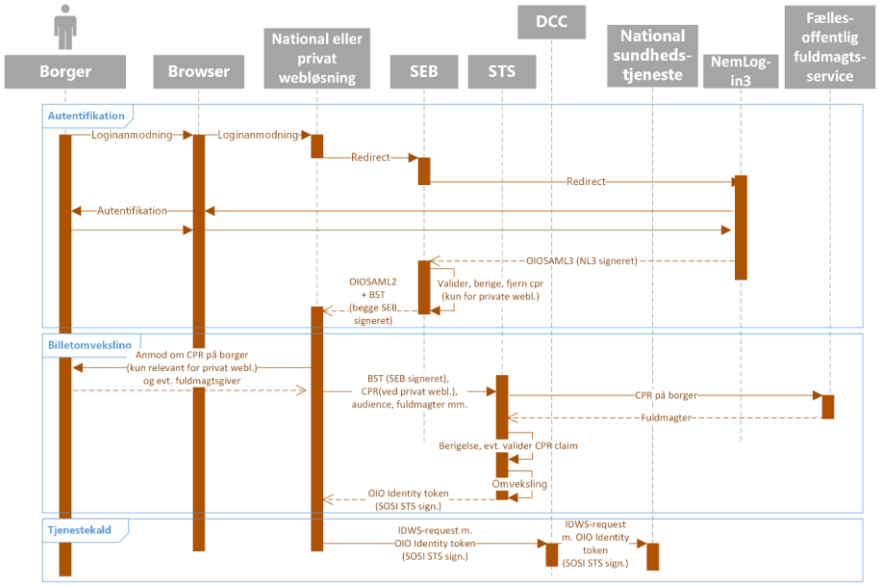
Figur 84: Statiske sammenhænge

6.4.3.4 Autentifikationsflow

For tjenesteaftagerne er der følgende ændringer til fase1 i forhold til baseline:

1) Små tilpasninger til OIOSAML2 tokenet fra SEB, da dette baseres på version 2.1.0 frem for version 2.0.9. Denne ændring realiseres den 14. juni 2021, i forbindelse med NemLog-in3 go-live.

2) Nyt BST token fra SEB



Figur 85: Autentifikationsflow for borgeres adgang til nationale webløsninger, hvor borger anmodes om indtastning af CPR

SEB skal sikre, at borgerens CPR kun udleveres til offentlige webløsninger og ikke til private webløsninger.
Private webløsninger skal anmode borgeren om at indtaste CPR (jf. Billetomvekslings-svømmebanen på Figur 85.

6.4.3.5 Gapanalyse for borgeres adgang til nationale webløsninger via browser og MitID

Komponent (GapID)	**Ændring**	**Reference til yderligere info**
SEB (G1)	Der skal etableres en tilslutningsaftale med NL3.	

SEB (G15)	SEB modtager et OIOSAML3 (borger) token fra NL3 og validerer tokenet. Herefter udstedes et SEB signeret OIO-SAML token med et indlejret OIO-Bootstrap-token. De to tokens returneres til Webserveren.	SEB broker jf. afsnit 7.4.1 OIO-Boot-strap-token jf. afsnit 7.2.2.1
SEB (G3)	På kort sigt bliver SEB ikke NSIS registreret, og derfor udsteder SEB på kort sigt OIOSAML2 tokens. På langt sigt forventes SEB at blive NSIS registeret således, at SEB kan udstede OIOSAML3.	
SEB (G4)	Skalering: øget anvendelse af SEB nødvendiggør at SEB gøres mere skalerbar	
STS (G16)	I SOSI-STS'en skal der etableres en grænseflade der kan udstede et OIO Identity token pba. det SEB signerede OIO-Bootstrap-token.	Jf. afsnit 7.2.4

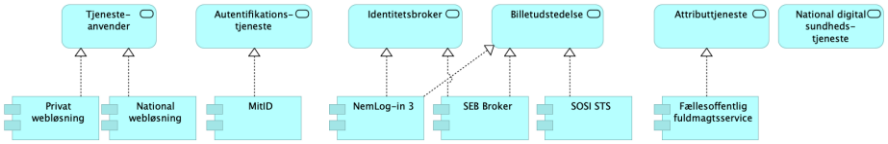
6.4.4 Borgers adgang via apps: App der tilgår Nemlog-in3 via OIDC Autorizations-server

Som beskrevet under baseline scenarierne, så falder OIDC autentifikationsflowet i fire dele:

1) autentifikationen fra app frontend
2) valg af pinkode samt caching af refresh token
3) omveksling af access token og kald af tjeneste
4) genoptagelse af session

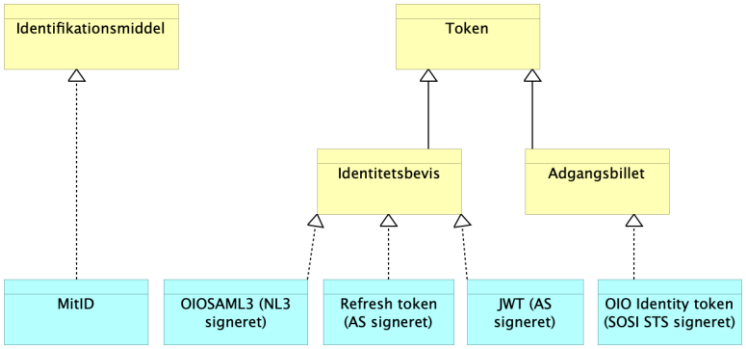
Der er kun i forbindelse med den første del, at der sker en ændring til Baseline (jf. afsnit 5.7). Autentifikation via NemID erstattes med NL3 (jf. figur nedenfor).

6.4.4.1 Komponentrealisering



Figur 86: Realisering af applikationskomponenter for borgers adgang via APP og OIDC

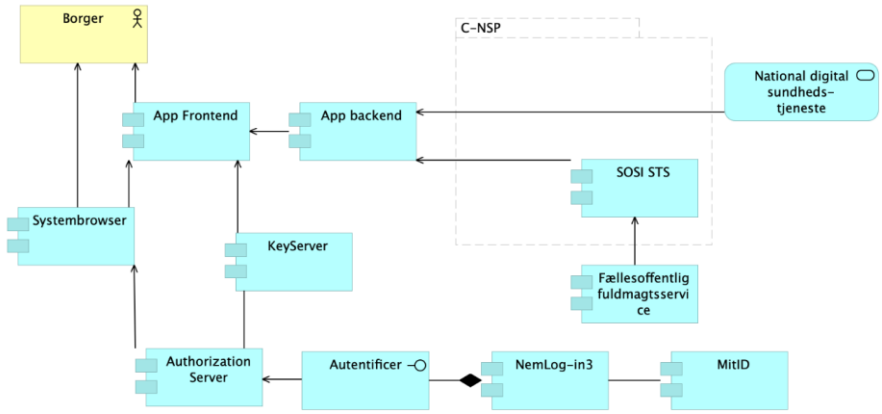
6.4.4.2 Realisering af informationsobjekter



Figur 87: Realisering af informationsobjekter for borgers adgang via APP og OIDC

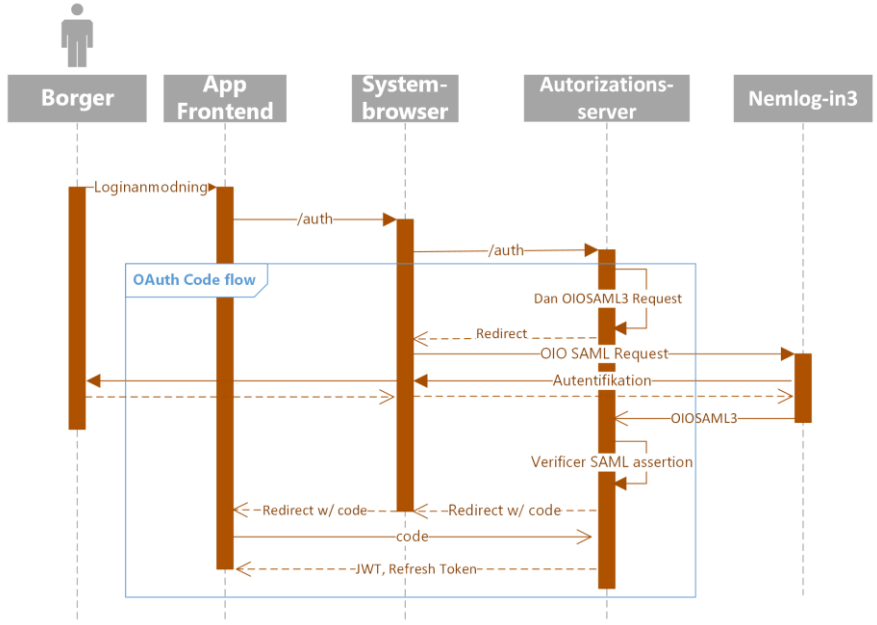
SOSI STS omveksler et JWT (JSON WEB Token) til et OIO Identity token, der skal medsendes ved adgang til en sundhedstjeneste. SOSI STS'en skal derfor have tillid (engelsk: trust) til indholdet af JWT tokenet, samt den autorizationsserver, der udsteder JWT tokenet.

6.4.4.3 Statiske sammenhænge



Figur 88: Statiske sammenhænge for borgers adgang via APP og OIDC

6.4.4.4 Autentifikationsflow



Figur 89: Autentifikationsflow for borgers adgang via APP og OIDC

6.4.4.5 Gapanalyse for borgers gang via apps

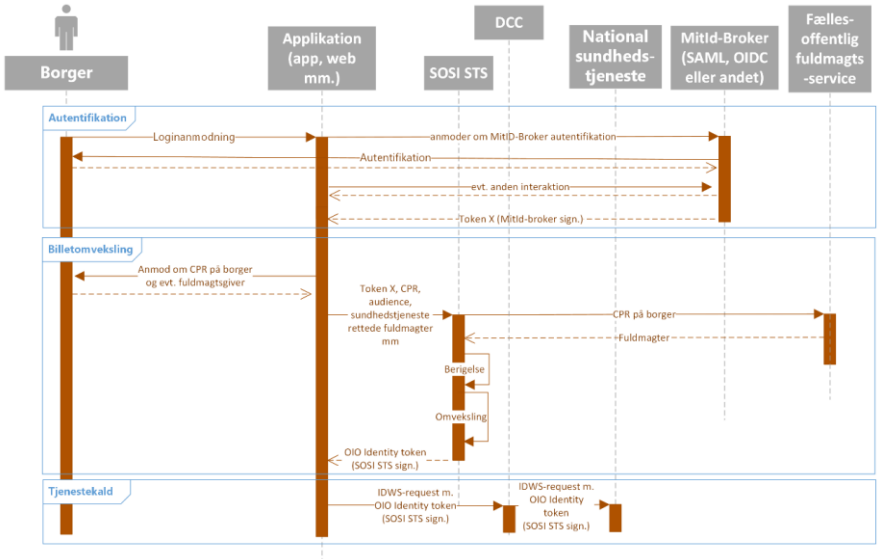
Komponent (GapID)	**Ændring**	**Reference til yderligere info**
AS eller SEB (G1)	Der skal etableres en tilslutningsaftale med NL3.	
STS (G18)	STS'en understøtter det eksisterende (baseline) proprietære JWT-format. DIGST arbejder på en fællesoffentlig OIOJWT profil, og en understøttelse af denne afventer at OIOJWT færdiggøres samt en efterfølgende stillingtagen til denne. Pt. ligger OIOJWT i version 0.3 og anses for umoden.	Jf. afsnit 7.2.4

6.4.5 Borgers adgang via applikationer der tilgår en MitId-Broker

MitID/NL3 tillader andre og uafhængige MitID-brokere som alternativ til Nemlog-in3. Eksempelvis MitID-brokere, der adskiller sig fra Nemlog-in3 på understøttede protokoller, servicelevel eller pris.

SOSI-STS truster tokens fra MitID-brokere, der er NSIS registreret og dermed underlagt den governance, som NSIS udstikker.
Samtidig vil SOSI-STS stille krav til understøttede tokenformater og tokenindhold. Pt. understøttes de tokens som SOSI-STS i forvejen tilbyder i borger-scenarierne 'Borger-adgang via browser: Webløsning der tilgår Nemlog-in3 direkte' og 'Borger adgang via app'. Dvs. et OIO Identity token (OIO SAML Profile for Identity Tokens V1.2) og et JWT token (proprietær profil).

Figur 90 illustrerer autentifikationsflowet for borgerens adgang via en MitID-broker.



Figur 90: Autentifikationsflow for borgeres adgang via en MitID-broker

Som det fremgår af autentifikations-svømmebanen, så er den nøjagtige interaktion mellem applikation og MitID-broker ukendt og vil afhænge af den konkrete MitID-broker. 'Token X' dækker over et JWT eller et OIO Identity token.

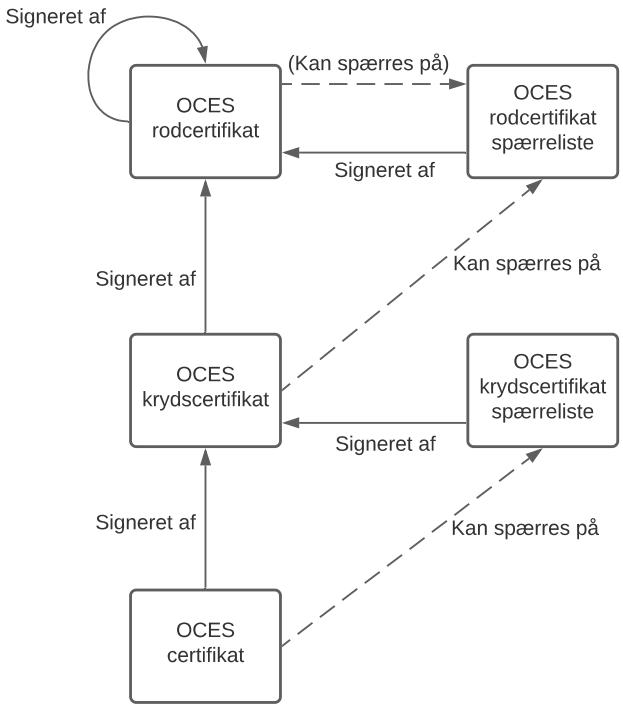
6.4.6 Borgers adgang til webløsninger via app (SBO)

SBO med app påvirkes ikke i transition 1.

6.5 Overgang fra OCES2 til OCES3 certifikater

Den kommende OCES3 infrastruktur er bygget op efter samme princip som OCES2, hvor der er et rodcertifikat (i hhv. PROD og TEST miljøerne), som udesteder en række krydscertifikater (også kaldt intermediate-certifikater eller udstedende CA'er) , der udsteder de egentlige OCES-certifikater. I og med certifikat-spærrelisterne er knyttet til det udstedende certifikat tillader afkoblingen igennem krydscertifikater, at størrelsen på spærrelisterne kan holdes lavt (hvilket var en reel praktisk udfordring i OCES1 infrastrukturen, hvor alle OCES-certifikater var udstedt af det samme rodcertifikat og den tilhørende spærreliste nåede at blive over 20 MB stor).

Forholdene mellem rodcertifikat, krydscertifikater, de egentlige OCES-certifikater og spærrelister er vist i nedenstående Figur 91.

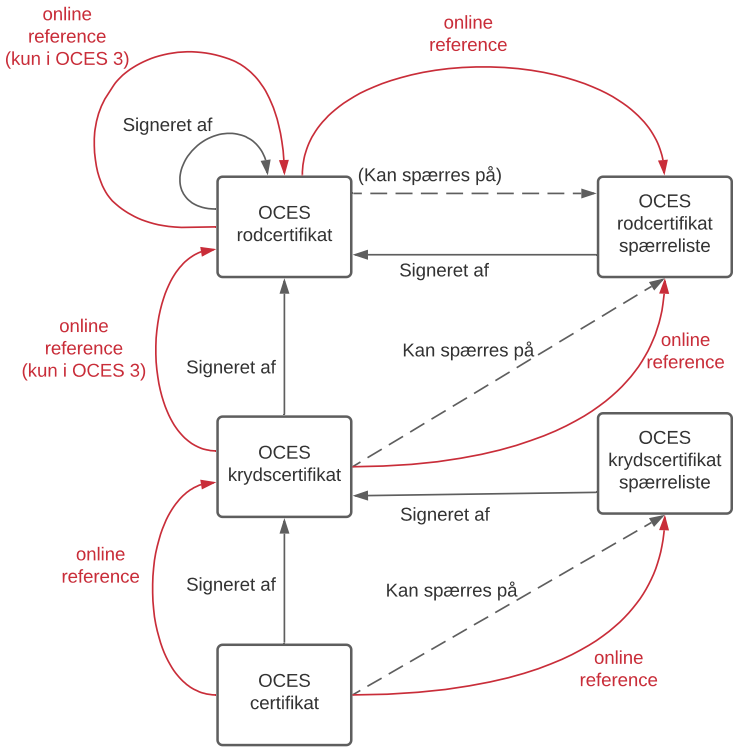


Figur 91: Sammenhængen i OCES-infrastrukturen

OCES3 certifikater er som OCES2 standard X509 certifikater, men tager nu udgangspunkt i den fælles europæiske ETSI-profilering – dette har dog så vidt vides ingen praksis betydning for anvendelsen i sundhedsvæsnet.

I forholdt til nuværende OCES2 er nøglelængder igen øget. OCES3 certifikater benytter RSA 3072 bits (rodcertifikat 4096 bits) nøgler og er signeret med RSA PSS med SHA-512, hvor OCES2 anvender RSA 2048 bit nøgler og SHA-256. En hurtig afprøvning på Java 8 platformen (som NSP baserer sig på), har ikke vist nogen udfordringer med de nye øgede nøglelængder.

Både OCES2 og OCES3 certifikater indeholder online referencer (dvs. URL'er) til henholdsvis det udstedende krydscertifikat og de tilhørende certifikat-spærreliste. Ligeledes indeholder såvel OCES2 og OCES3 rodcertifikater og krydscertifikater online referencer til deres tilhørende certifikat-spærrelister. Som noget nyt er det i OCES3 rod- og krydscertifikater også indlejrede online referencer til det udstedende certifikat. I nedenstående Figur 92 er forholdene mellem certifikaterne i infrastrukturen suppleret med de i certifikaterne indeholdte online referencer.



Figur 92: Sammenhængen i OCES-infrastrukturen med angivelse af indlejrede online referencer (med rød)

Referencer til henholdsvis udstedende certifikat og tilhørende spærreliste angives i begge OCES versioner i gennem de samme X509 extensions:

- ”CRL distribution point extension” (2.5.29.31) peger på den udstedendes certifikat spærreliste
- “Certificate Authority Information Access extension” (1.3.6.1.5.5.7.1.1) indeholder en reference til det udstedende certifikat i “CA Issuers extension” (1.3.6.1.5.5.7.48.2)

6.5.1 Ny indhold i X509 SubjectDistinguishedName i OCES3 certifikater

Med OCES3 udgår RID, FID og UID attributterne fra henholdsvis medarbejder- (MOCES), funktions- (FOCES) og virksomheds- (VOCES) certifikaterne og erstattes med at UUID attribut. (Og borger (POCES) certifikater udgår helt.)

OCES2 certifikaters "subject serial number" i SubjectDistinguishedName (ikke selve certifikatets serienummer) indeholder såvel CVR nummer og RID/FID/UID for henholdsvis medarbejder-/funktions-/virksomheds-certifikater.

Eksempel for et OCES2 medarbejdercertifikats "subject serial number" er "CVR:25450442-RID:1231593107593".

I OCES3 fremgår CVR nummeret nu af et nyt "organizationIdentifier" attribut i SubjectDistinguishedName og bliver på formen "NTRDK-XXXXXXXX".

UUID attributten (den unikke ID der erstatter RID/FID/UID) fremgår stadig af "subject serial number" og bliver i OCES på formen "UI:DK-XXXXXXX..XX".

6.5.2 Integrationer fra NSP til OCES infrastrukturen

NSP instanserne har ikke direkte adgang til internettet og OCES online ressourcer (krydscertifikater og spærrelister) tilgængeliggøres på NSP platformen via to forskellige og manuelle processer.

- Krydscertifikater bliver gjort tilgængelige for applikationer på NSP via konfiguration i en central netværkskomponent (loadbalanceren) og lokal DNS indgange på NSP.
- Spærrelister konfigureres i den central CRA-komponenten for hvert udstedende krydscertifikat og bliver periodisk opdateret og distribueret til NSP instanserne.

Der er i dag en generel udfordring i forhold til OCES operatørens ibrugtagning af nye krydscertifikater (og dermed nye spærrelister), idet Nets/DanID som nuværende OCES2-operatør ikke udsender varsler herom. NSP driftsleverandøren håndterer problemstillingen via en reaktiv udbedring igennem manuel tilføjelse i henholdsvis CRA og den centrale netværkskomponent efter alarmer i STS.

Nuværende koncept for håndtering af spærrelister og krydscertifikater på NSP videreføres for kommende OCES3 ressourcer i uændret form. (Der bør dog med fordel afdækkes om der til den nye OCES3 infrastruktur medfølger en forbedret forvaltning som indeholder varslingsmekanismer i forhold til ibrugtagning af nye krydscertifikater.)

7. Transition 1 - Applikations-view

Kapitlet beskriver applikationsarkitekturen for sikkerhedsinfrastrukturen i transition 1. Sikkerhedsinfrastrukturen udgøres af følgende komponenter og hjælpeværktøjer:

1) SOSI STS
2) SOSI Gateway
3) SEB
4) SEAL-bibliotekerne
5) NSP Accesshandler
6) CRA
7) DCC

De enkelte komponenter og hjælpeværktøjer behandles selvstændigt i hver sit afsnit. Kapitlet indledes med et afsnit, som definerer fire principper, der har været styrende i applikationsdesignet igennem kapitlet.

7.1 Principper anvendt ved design af applikations-arkitektur

Princip	**1) Forandringerne under transition 1 skal minimeres**
Formål	Transition 1 udgøres af overgangen til MitID og NL3, hvilket indebærer en fastholdelse af SOSI-idkortet som fagpersoners identitetsbevis og adgangsbillet til nationale sundhedstjenester, og er ydermere båret af en forventning om, at der dermed opnås mindst mulig påvirkning af de eksisterende flows og dermed af parternes systemportefølje i første transition.
Konsekvens	SOSI-idkortet skal bevares og kun justeres, hvor det er påkrævet grundet konceptuelle forskelle på OCES2/NL2 og MitID/NL3. Ligeledes skal forretningsregler ved omveksling og opsætning af attributindhold i SOSI-idkortet så vidt muligt bevares.

Princip	**2) Arkitekturbeslutningerne under transition 1 bør laves under hensyntagen til målbilledet og dermed transition 2**
Formål	Transition 1 skal opleves som et skridt på vej mod målbilledet og dermed transition 2 (IDWS XUA sikkerhedsprotokollen erstatter DGWS). Det skal undgås, at der indføres nye arkitekturvalg og løsninger, der går imod målarkitekturen, og dermed skal laves om under transition 2.

Konsekvens	Hvis der er flere løsninger til en arkitekturproblematik, så bør den løsning, der mest er i overensstemmelse med målbilledet vælges. Dette skal dog afvejes imod princip 1 om, at forandringer under transition 1 skal minimeres.

Princip	**3) Sikkerhedsinfrastrukturen skal overholde NSIS, før den kan udstede tokens med ophav i NSIS**
Formål	Udstedelse af tokens med ophav i NSIS (fx OIOSAML3) forudsætter at tokenudstederen/brokeren overholder NSIS kriterierne.
Konsekvens	SEB broker eller SOSI STS må ikke udstede et OIOSAML3 token med LoA-niveau "Lav", "Betydelig" eller "Høj" før SEB broker eller SOSI STS selv overholder kravene til de pågældende NSIS LoA niveauer. Ovenstående gælder også når SEB broker modtager et OIOSAML3 token fra NL3, og primært ombytter NL3 signaturen med SEB signaturen før tokenet formidles til et fagsystem eller en web-løsning i sundhedsdomænet.

Princip	**4) Sikkerhedsinfrastrukturen omveksler kun et token til et andet token på samme eller lavere sikkerhedsniveau.**
Formål	Modtageren vil forvente at laveste sikringsniveau i autentifikations- og omvekslingskæden definerer det resulterende sikringsniveau for et token. Token sikringsniveau rangordnes efter nedenstående liste fra højeste sikringsniveau til laveste sikringsniveau 1) OIOSAML3/MOCES3 NSIS LoA "Høj" 2) OIOSAML3/MOCES3 NSIS LoA "Betydelig" 3) SOSI idkort DGWS-sikkerhedsniveau 4, OCES2 og OIOSAML2
Konsekvens	Det er muligt at omveksle et OIOSAML3 token LoA "Høj" og "Betydelig" til et SOSI idkort sikkerhedsniveau 4 eller et OIOSAML2 token. Men det omvendte er ikke muligt. Det er muligt at omveksle et OIOSAML3 token LoA "Betydelig" til et OIOSAML3 token LoA "Betydelig", dog under forudsætning af, at brokeren selv overholder kravene til NSIS niveau "Betydelig" (NSIS krav). Det er derimod ikke muligt at omveksle et OIOSAML2 token eller et SOSI idkort til et OIOSAML3 token med sikringsniveau "Betydeligt".

7.2 SOSI STS

I tabellen nedenfor beskrives servicegrænsefladerne for den eksisterende SOSI STS, og det vurderes hvorvidt de enkelte grænseflader påvirkes af fase1.

Service (Brugertype)	Beskrivelse	Påvirkes af fase1 ?
SecurityTokenService og NewSecurityTokenService **(Medarbejder)**	Autentifikationsservice der udsteder af STS-signeret Idkort ud fra et selvsigneret idkort. De to services er i princippet ens og deler kode. Forskellen på de to services er at SecurityTokenService bibeholder feltet Subject.NameID fra selvsigneret til STS-signeret SOSI idkort. I NewSecurityTokenService opsættes feltet Subject.NameID med diverse certifikatoplysninger, således at idkortet efterfølgende kan omveksles til OIOSAML2.	Ja, skal kunne håndtere input i form af at MOCES3 signeret SOSI idkort, samt output uden certifkat-oplysninger i det STS-signerede IdKort
SOSI2OIOSAML **(Medarbejder)**	Ombytter et STS-signeret idkort til et OIOSAML-token rettet mod et specifikt audience (SBO), f.eks. sundhed.dk.	Ja, da SOSI idkort skabt ud fra OIOSAML3 og MOCES3 har få ændringer i forhold til Baseline SOSI idkort
OIOSAML2SOSI **(Medarbejder)**	Ombytter et OIOSAML (Nemlog-in) token til et signeret SOSI idkort. Token skal være signeret af troværdig tredjepart (Nemlog-in)	Ja, da omvekslingen fremover skal tage udgangspunkt i et SEB signeret OIOBootstrap-token frem for et NL signeret OIOSAML token. Grænsefladen OIOSAML2SOSI udfases på sigt.
BST2IDWS **(Borger)**	Ombytter et NL2 signeret OIO-Bootstrap-token til et OIO Identity Token rettet mod et givet audience, f.eks. FMK.	Ja. Grænsefladen skal fremover kunne modtage BST tokens fra NL3 STS og SEB
JWT2IDWS **(Borger)**	Ombytter et JSON Web token (JWT) til et OIO Identity token rettet mod et givet audience, f.eks. FMK	På kort sigt Nej. Grænsefladen skal på langt sigt kunne modtage tokens fra andre OIDC- og MitId-brokere
JWT2OIOSaml **(Borger)**	Ombytter et JSON Web token til et OIOSAML-token rettet mod et specifikt audience (Borger SBO), f.eks. forløbsplaner.dk	På kort sigt Nej. Grænsefladen skal på langt sigt kunne

Kommenterede [CG1]: Mangler vi ikke BST2SOSI for medarbejdere i oversigten?

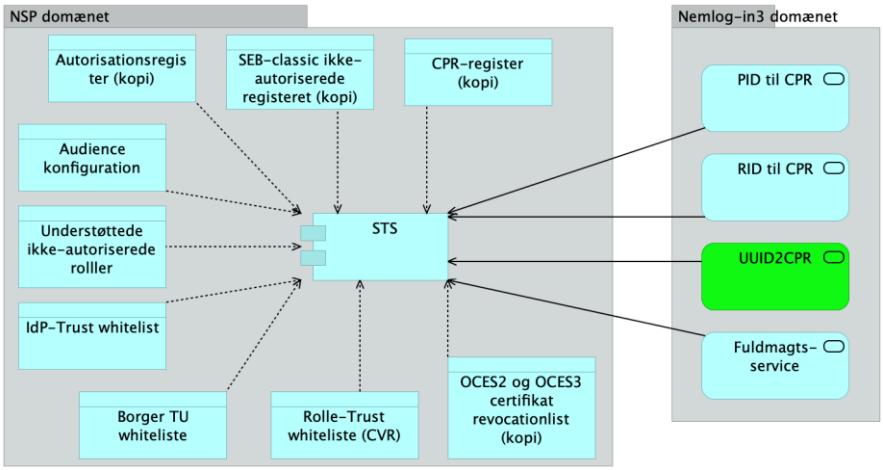
Kommenterede [SM2R1]: Det er en fremtidig grænseflade og tabellen viser kun de eksisterende grænseflader

		modtage tokens fra andre OIDC- og Mi-tId-brokere

Tabel 6: Servicegrænsefladerne for den eksisterende SOSI STS

SOSI STS'en har, som det fremgår af nedenstående figur, afhængigheder til en række konfigurationsfiler, databaser og services. UUID2CPR (markeret med grønt) er en ny services TO-BE STS'en, hvorimod alle andre afhængigheder er eksisterende (AS-IS) i STS'en.

Kommenteret [CG3]: TODO: Afventer afklaringer med Digst og internt i projektet: Muligvis er der behov for yderligere opslag hvis MOCES3 cert-specifikke UUID skal understøttes



Figur 93: SOSI STS afhængigheder til konfigurationsfiler, databaser og services

Afhængig-hed	Beskrivelse	Påvirkes af fase1
Autorisati-ons-registe-ret	Kopi af Autorisations-regi-steret fra Styrelsen for Pati-entsikkerhed.	Nej
SEB-classic 'nationale roller' regi-steret	Kopi af 'nationale roller' re-gisteret i SEB-classic.	Ja. Nøglen til opslag i dette register (CVR-RID) har status 'Depricated' i MitID/NL3. Opslag skal kunne laves med 'Global medarbejder UUID' eller CPR.
CPR-regi-steret	Kopi af CPR-registeret	CPR registeret anvendes ikke i baseline, men forventes anvendt til navneberigelse i BST2SOSI.
OCES2 og OCES3 cer-tifikat revo-cationlist	Kopi af Revocationlister for henholdsvis OCES2 certifi-kater og OCES3 certifikater.	Ja. OCES2 revocationlisten skal udvides med en OCES3 revocationlist.

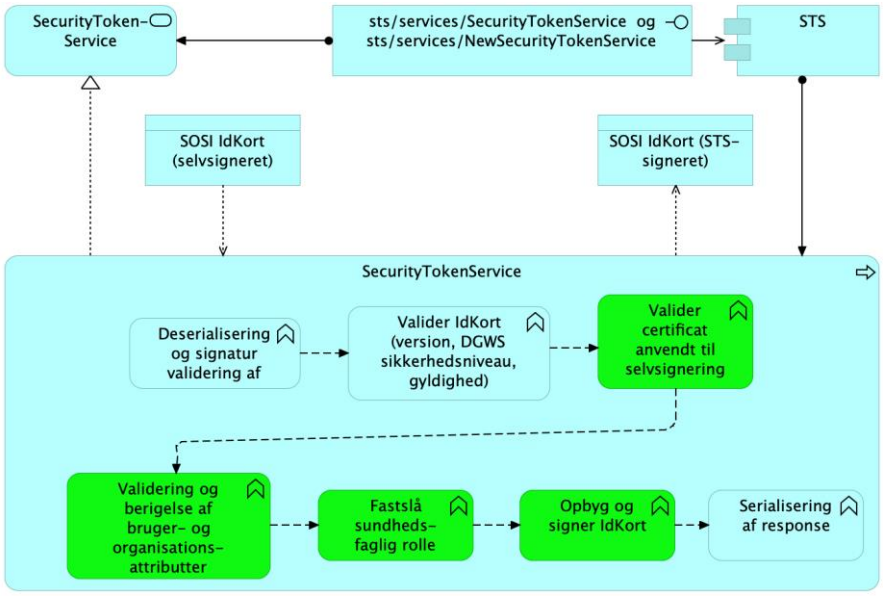
Rolle-Trust whitelist (CVR)	Liste med CVR-numre som Trustes til at kunne claime en ikke-autoriseret rolle i STS omvekslingskaldet. Der er en liste til hver STS grænseflade Trustede organisationer vedligeholder de 'nationale roller' i lokalt system for centralt i SEB-Classic, og derfor kan STS'en ikke validere en claim'ed rolle, men må stole på, at organisationen anvender de 'nationale roller' korrekt.	Nej. Rolle-Trust listen vil forsat være relevant for organisationer uden MitID/NL3 eller lokal IdP, og som derfor anvender MOCES2 eller MOCES3 autentifikation. Organisationer med egen lokale IdP forventes at udtrække de 'nationale roller' fra det lokale IDMS og via et OIO-Bootstrap-token formidle rollerne til SOSI STS'en.
IdP-Trust whitelist (medarbejder)	Liste over IdP'er som trustes mht. medarbejder autentifikation	Ja. Der skal være separate lister per service (eksisterende OIOSAML2SOSI skal ikke dele trust-liste med BST2SOSI)
Borger TU whitelist	Liste over borgerrettede tjenesteudbydere, der må lave BST/JWT TO IDWS omveksling.	Ja. Whitelisten udgår, da de eksisterende NL2 signerede BST tokens erstattes af NL3 STS eller SEB signerede BST tokens (begge HoK). Listen er alene oprettet til at kompensere for, at et NL2 BST token anvendes mod SOSI domænet.
IdP-Trust whitelist (borger)	Liste over IdP'er som trustes mht. borger autentifikation. Der er en liste pr. borgerrettet STS grænseflade	Nej.
Understøttede 'nationale roller'	Liste over gyldige 'nationale roller'.	Nej
Audience-konfiguration i forbindelse med SOSI2OIOSAML servicen	SBO tokens (OIOSAML med evt. indlejret SOSI idkort) udstedes med såkaldt audience-restriction. Dvs. tokenet må kun anvendes af den web-løsning, som det er udsted til. Pr. Audience konfigureres det, om SOSI idkort skal indlejres i OIOSAML, samt den offentlige-nøgle, der skal anvendes til kryptering af token, således at det kun er audience (web-løsningen), der kan læse tokenindholdet.	Nej

UUID-2CPR også omtalt SubjectSerialNumber2CPR	Opslagstjeneste i regi at MitID/NL3, som kan omveksle et global employee UUID til et CPR. Servicen er også omtalt som SubjectSerialNumber2CPR, da certifikater håndterer UUID fra attributten SubjectSerialNumber	Ja, ny integration
Fuldmagtsservice	Den fællesoffentlige fuldmagtsservice. Er udelukkende relevant for borgere.	Nej

Tabel 7: SOSI STS afhængigheder til konfigurationsfiler, databaser og services

I det følgende gennemgås de enkelte SOSI STS'en grænseflader der tilføjes eller ændres.

7.2.1 SecurityTokenService og NewSecurityTokenService



Figur 94: Archimate illustration med applikations-arkitektur for TO-BE grænsefladen NewSecurityTokenService

Justeringerne fra Baseline til Fase1 ligger primært indenfor funktionerne markeret med grønt på Figur 94.

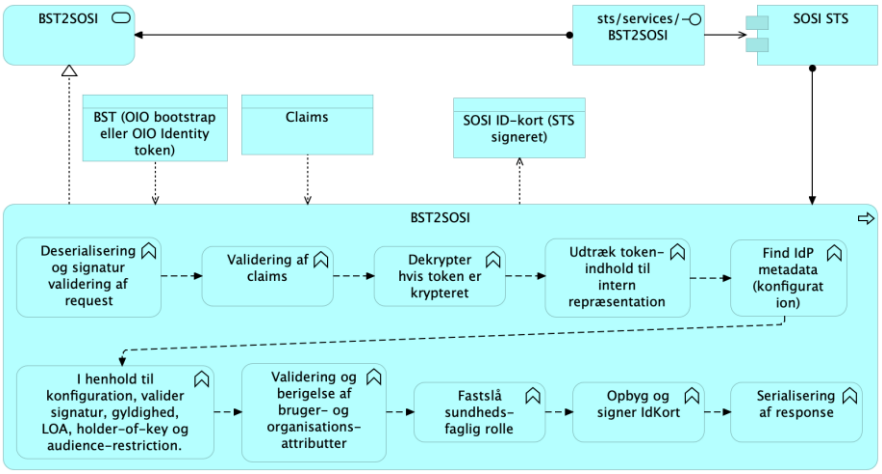
Service	**TO-BE NewSecurityTokenService**
Protokol	WS-TRUST 1.4

Interface	/sts/services/SecurityTokenService /sts/services/NewSecurityTokenService
Anvendersystemer	Alle som har SDN netværksmæssig adgang
Bruger	Medarbejder
Input	SOSI idkort (selvsigneret med MOCES3)
Output	SOSI idkort signeret af SOSI STS
Beskrivelse	De to services SecurityTokenService og NewSecurityTokenService anvender samme kode og adskiller sig kun på indholdet af Subjet.NameID feltet i output. SecurityTokenService bibeholder Subject.NameID fra input til output. NewSecurityTokenService udfylder Subject.NameID med diverse certifikatinformationer. Det er en autentifikationsservice, der tager et selvsigneret SOSI idkort som input, validere og beriger dette og returnerer et STS signeret SOSI idkort. Den primære forskel mellem Baseline og Fase1 SecurityTokenService er: • Input SOSI idkortet er selvsigneret med MOCES3 (Baseline anvendes MOCES2) • CPR-nummer findes ud fra MOCES3 SubjectSerialNumber attributten efterfulgt af et opslag i MitId/NL3 UUID2CPR opslagstjenesten (Baseline laves opslag pba. CVR-RID i MOCES2 certifikatet). • MOCES3 har ikke RID-CVR attributten og derfor skal der anvendes en ny nøgle til opslag i registeret med de 'nationale roller' (jf. Tabel 7) • Output (det STS-signerede idkortet) indeholder altid CPR-nummer i Subject.NameID feltet (jf afsnit 7.2.2.3)
Migreringsovervejelser	TO-BE logikken realiseres via en videreudvikling af de eksisterende to services. Ud fra input (certifikat version anvendt til signering af SOSI Idkort) til servicen afgøres det, om Fase1 eller Baseline logikken skal aktives.

7.2.2 BST2SOSI (medarbejder) erstatter OIOSAML2SOSI

Nedenfor vises realisering af Fase1 grænsefladen BST2SOSI, der på sigt erstatter Baseline grænsefladen OIOSAML2SOSI. Med dette skridt anvendes tokens i henhold til deres rette formål i henhold til det fælles offentlige og sundhedsområdets målbillede, og samtidig etableres et grundlag for højere sikkerhed. OIOSAML tokens anvendes som

adgangstokens til webløsninger, hvorimod BST (OIO Bootstrap eller OIO Identity tokens) anvendes til tokenomveksling og muliggør kryptografisk låsning til tjenesteanvender og audience.



Figur 95: Archimate illustration med applikations-arkitektur for grænsefladen BST2SOSI

Service	**BST2SOSI**
Protokol	WS-TRUST 1.4
Interface	sts/services/BST2SOSI
Anvendersystemer	Alle som har SDN netværksmæssig adgang
Bruger	Medarbejder
Input	- Bootstraptoken (BST) (OIOSAML-baseret) - En liste af claims • En angivelse af det kaldende it-system (en påkrævet attribut i DGWS/SOSI-idkortet) • En (frivillig) angivelse af fagpersonens sundhedsfaglig autorisation • En (frivillig) angivelse af fagpersonens 'nationale rolle' • En (frivillige) angivelse af et ID for fagpersonen, der ønskes som 'Subject NameID' i SOSI-idkortet AS-IS håndteres Claims via en proprietær claim-dialekt navngivet HealthcareContexToken. Fremover anvendes traditionelle WS-TRUST Claims.
Output	SOSI idkort signeret af SOSI STS
Beskrivelse	I Baseline omveksles et OIOSAML (Nemlog-in) token til et STS signeret SOSI idkort.

	I Fase1 er input til omvekslingen et OIO-Bootstrap-tokens fra SEB-broker eller en lokal NSIS registreret IdP, samt OIO Identity tokens fra NL3 STS. Krav til attribut-indhold for OIO-Bootstrap token findes i afsnit 7.2.2.1. OIO Identity token følger det som NL3 STS udsteder ("OIO SAML Profile for Identity Tokens" version 1.2) Den primære forskel mellem Baseline og Fase1 er: • Input er et BST-token (input i Baseline er et OIO-SAML2 token). BST er af typen Holder-of-Key med audience-restriction og begge forhold skal validres af SOSI-STS'en. Håndhævelse af HoK skal dog pr. konfiguration kunne slås fra. • Det resulterede SOSI idkort har CPR i Subject.NameID elementet. Modsat det eksisterende SOSI idkort, der har certifikat oplysninger i Subject.NameID (jf. afsnit 7.2.2.3) • OIO-Bootstrap-tokenet kan indeholde en liste af de 'nationale roller' brugeren må anvende. "Algoritme til at fastslå medarbejders sundhedsfaglige rolle" (jf. afsnit 7.2.2.2) skal medtage rolle-listen i algoritmens beslutningsgrundlag. • Baseline håndteres Claims via en proprietær claim-dialekt navngivet HealthcareContexToken. Fremover bør traditionelle WS-TRUST Claims understøttes. I udviklingen af fase1 skal fokuseres på at gøre koden generisk og fleksibel, således at nye IdP'er/Brokere nemmere kan tilkobles.
Migrationsoverve-jelser	For at synliggøre at input- og outputformatet er ændret, så laves Fase1 servicen som en ny service.

7.2.2.1 Krav til OIO-Bootstrap-token (medarbejder)

Tabellen nedenfor definerer krav til attributindholdet i OIO-Bootstrap-tokenet. Der skelnes mellem om OIO-Bootstrap-tokenet formidler NSIS eller NIST LoA. Som følge af princip 4 i afsnit 7.1 må SEB broker eller en lokal IdP kun udstede NSIS LoA tokens, hvis de selv er NSIS registreret. Dette betyder eksempelvis at SEB broker på kort sigt altid udsteder et OIO-Bootstrap-token baseret på NIST. Dette gælder også når SEB broker selv har modtaget et OIOSAML3 token (NSIS baseret) fra NL3 eller en lokal IdP.

Relevante attributter i OIO-Bootstrap-token	OIO-Bootstrap-token med op-hav NSIS	OIO-Bootstrap-token med op-hav NIST
SpecVersion	Ja	Ja
Level of Assurance (lav, betydelig, høj) NSIS	NSIS baseret skala (lav, betydelig, høj)	NIST baseret skala (1, 2, 3, 4)
Email	(gerne)	(gerne)
CPR	Nej	Ja
Persistent Identifier (Global Employee UUID), som er ens tværs af offentlige SP'er)	Ja	Nej
CVR-RID	Nej	Nej
Certifikat specifik information som SubjectSerialNumber	Nej	Nej
CVR number	Ja	Ja
Organization name	Ja	Ja
Liste af medarbejders 'nationale roller'	Kan	Kan
Issuer	Ja	Ja
Assertion Signatur	Ja	Ja

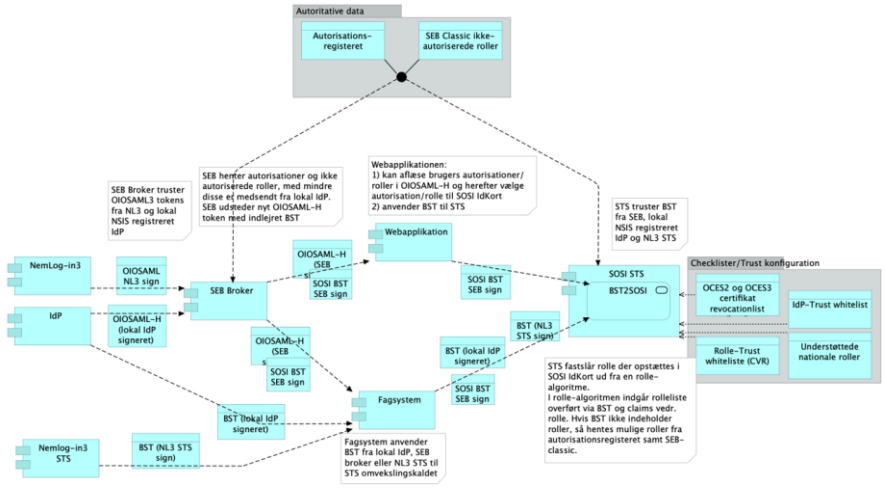
Det udestår at specificerer OIO-Bootstrap-tokenet. Som følge af princip 2 i afsnit 7.1, så skal OIO-Bootstrap-tokenet tage udgangspunkt i specifikationerne fra OIOIDWS profilen (konkret OIO Bootstrap token profile).

OIO-Bootstrap-tokenet bliver et Audience-restricted Holder-of-Key token:

- Med **Holder-of-key** menes, at tokenet er kryptografisk låst til det system, der har nøglen (her tjenesteanvenderen). Dvs. tokenet kan ikke anvendes af andre systemer, og derfor kan et holder-of-key token have lang gyldighed, uden at sikkerheden kompromitteres.
  Der åbnes dog op for, at HoK-politikken først håndhæves i forbindelse med Fase2 (dvs. ved udrulning af IDWS XUA), da HoK-politikken stiller betydelige krav til tjenesteanvenderen, samt fordi effekten ved HoK er ubetydelig så længe SOSI idkort anvendes.
- Med **Audience-restricted** menes, at tokenet udelukkende kan anvendes til kald af en STS med det specificerede audience (her SOSI STS'en)

7.2.2.2 STS, tillid (trust) og algoritme til at fastslå medarbejders sundhedsfaglige rolle

Figuren nedenfor illustrerer vejene fra NL3 og lokale IdP til grænsefladen BST2SOSI på STS'en.



Figur 96: Token og trust flow fra IdP til SOSI STS

På figuren ses 6 token-flows (veje) fra IdP til STS:

1) NL3->SEB broker->Webapplikation->SOSI STS
2) Lokal IdP->SEB broker->Webapplikation->SOSI STS
3) NL3->SEB broker->Fagsystem->SOSI STS
4) Lokal IdP->SEB broker->Fagsystem->SOSI STS
5) Lokal IdP->Fagsystem->SOSI STS
6) NL3 STS->Fagsystem->SOSI STS

Flow 4 forventes ikke anvendt, da et lokalt fagsystem forventes at anvende flow 5 mod en lokal IdP.

SEB broker truster:

- OIOSAML3 tokens fra NL3.
- OIOSAML-H v2 (subprofil til OIOSAML3) tokens fra lokale NSIS registrerede IdP'er, der har en tilslutningsaftale til SEB-broker.
- OIOSAML-H v1 (subprofil til OIOSAML2) tokens med indlejret SBO-token (dvs. et krypteres OIOSAML2 token med indlejret STS signeret SOSI idkort) fra lokal IdP, der har en tilslutningsaftale til SEB-broker (ikke vist på figur).

SEB broker udfører følgende, når et OIOSAML token modtages fra NL3 eller lokal IdP:

1) Udtrækker en liste over medarbejderens sundhedsfaglige autorisationer fra autorisationsregisteret.
2) Udtrækker en liste over medarbejderens 'nationale roller' fra SEB-Classic, hvis en sådanne liste ikke er medsendt fra IdP.
3) Udsteder et SEB signeret OIOSAML-H token med et indlejret OIO-Bootstrap-token. OIOSAML-H token indeholder liste med autorisationer og 'nationale roller'. OIO-Bootstrap-token indeholder liste med 'nationale roller'

SOSI STS'en truster:

- OIO-Bootstrap-tokens fra SEB broker
- OIO-Bootstrap-tokens fra lokale NSIS registrerede IdP'er
- OIO-Bootstrap-tokens fra NL3 STS

SOSI STS'en truster følgende attributter fra OIO-Bootstrap-tokenet, der beskriver medarbejderen:

- medarbejder CPR eller global employee UUID
- CVR-nummer
- Organisationsnavn
- Liste over 'nationale roller' som medarbejderen må anvende i organisationen

STS BST2SOSI omvekslingskaldet aktiveres af tjenesteanvenderen (et fagsystem eller en webløsning), der skal anvende et SOSI idkort for at lave DGWS kald til nationale digitale sundhedstjenester.

Hvis medarbejderen har flere autorisationer og/eller 'nationale roller', så kan der være situationer, hvor SOSI STS'en ikke selv kan afgøre den rolle, der skal fremgå af det udstedte SOSI idkort. I denne situation kan tjenesteanvenderen via OIOSAML-H tokenet aflæse de mulige roller, og lade brugeren eller kaldskonteksten afgøre den rolle, der skal anvendes. Tjenesteanvenderen kommunikerer rolle-valget til SOSI STS'en via et 'claim' (ws-trust protokollen anvendes ved kald til SOSI STS).

SOSI STS'en anvender en algoritme til at fastslå den autorisation eller 'nationale rolle', der skal fremgå af det udstedte SOSI-IdKort. I diagrammet nedenfor illustreres algoritmen via et flowdiagram. Med blåt er markeret de tilføjelser, der er lavet til baseline fastslå rolle algoritmen for at understøtte BST2SOSI. Yderligere forklaringer til algoritmen findes i bilaget 'Fastslå rolle algoritme_v2.docx'.


Start for grænsefladerne SecurityTokenService OIOSAML2SOSI og BST2SOSI
Der er en liste pr. endpoint - dvs. pr. STS grænseflade
Er der i input angivet national rolle (1)
Er den nationale rolle på NSP-listen med gyldige nationale roller
Er CVR (medarbejdens org. tilknytning) på listen af trust ede organisationer
Kaldes BST2SOSI og er den nationale rolle på rolle-liste indleveret i BST
Har medarbejderen den nationale rolle i SEB
Success: Id-kort med den angivne nationale rolle
Fejl: Fortæl at den ønskede nationale rolle er ugyldig
Success: Id-kort med den angivne nationale rolle
Success: Id-kort med den angivne nationale rolle
Fejl: Fortæl at medarbejderen ikke har den ønskede nationale rolle.
Er der i input angivet et autorisations-id
Er der i input angivet en gyldig uddannelseskode
Har medarbejderen en autorisation i autorisationsreg. der matcher de to input
Success: Id-kort med den angivne autorisation
Har medarbejderen en autorisation i autorisationsreg. der matcher autorisations-id
Har medarbejderen autorisationer i autorisationsreg.
Success: Id-kort med den angivne autorisation
Fejl: Fortæl at der ikke findes nogle autorisationer
Er der i input angivet en gyldig uddannelseskode
Har medarbejderen en enkelt autorisation i autorisationsreg. med den angivne uddannelseskode
Har medarbejderen flere autorisationer i autorisationsreg. med den angivne uddannelseskode
Har medarbejderen autorisationer autorisationer i autorisationsreg.
Fejl: Fortæl hvilke autorisationer der kan vælges
Success: Id-kort med den angivne autorisation
Fejl: Fortæl hvilke autorisationer der matchede uddannelseskoden
Fejl: Fortæl at der ikke findes nogle autorisationer
Er det i input angivet at autorisation ikke ønskes anvendt (2)
Har medarbejderen autorisationer i autorisationsreg.
Har medarbejderen en enkelt autorisation i autorisationsreg.
Success: Id-kort med denne autorisation
Kaldes BST2SOSI og har BST indlejret liste med nationale roller
Er der en enkelt national rolle i BST-listen
Har medarbejderen nationalle roller i SEB
Fejl: Fortæl hvilke nationale roller der kan vælges
Success: Id-kort med den denne nationale rolle
Success: Id-kort med den rolle der er angivet (3)
Har medarbejderen en enkelt national rolle i SEB
(1) På formen "urn:dk:healthcare:national-federation-role:code:XXXX:value:YYYY" i userRole
(2) Angives med "urn:dk:healthcare:no-role" i userRole
(3) Fritekst-roller som f.eks. "Astronaut" - Kan være tom.

7.2.2.3 SOSI idkort med ophav i OIO-SAML3/MOCES3

Designkriteriet for et SOSI idkortet med ophav OIOSAML3/MOCES3 er, at det skal indeholde så få ændringer til Baseline SOSI Idkortet som muligt således, at aftagerne af idkortet helst ikke påvirkes.

OIOSAML3/MOCES3 indeholder ikke RID og derfor kan felter med RID ikke udfyldes. OIOSAML3 indeholder, modsat OIOSAML2, ikke nogen information om nogen certifikat, der er anvendt til autentifikation (som ikke behøver at være certifikat basere).

Kommenterede [CG4]: RID fastholdes i hvert kun i en overgangsperiode …

Ovenstående påvirker primært udfyldelsen af SOSI idkortets Subject.NameID felt, som illustreret nedenfor.

Baseline udfyldelse af Subject.NameID feltet i SOSI idkortet:

```
<saml:NameID Format="medcom:other">SubjectDN={SERIALNUMBER=CVR:30808460-RID:42634739 + CN=TU GENEREL MOCES M CPR gyldig, O=NETS DANID A/S // CVR:30808460, C=DK},IssuerDN={CN=TRUST2408 Systemtest XXII CA, O=TRUST2408, C=DK},CertSerial={1538078558}</saml:NameID>
```

Fase1 udfyldelse af Subject.NameID feltet i SOSI idkortet:

```
<saml:NameID Format="medcom:cprnumber">1802602810</saml:NameID>
```

Den illustrerede udfyldelse af fase1 Subject.NameID feltet ligger indenfor det lovlige i DGWS standarden, og ændringen forventes ikke at give udfordringer for SOSI idkort aftagerne. Det sidste skal dog verificeres.

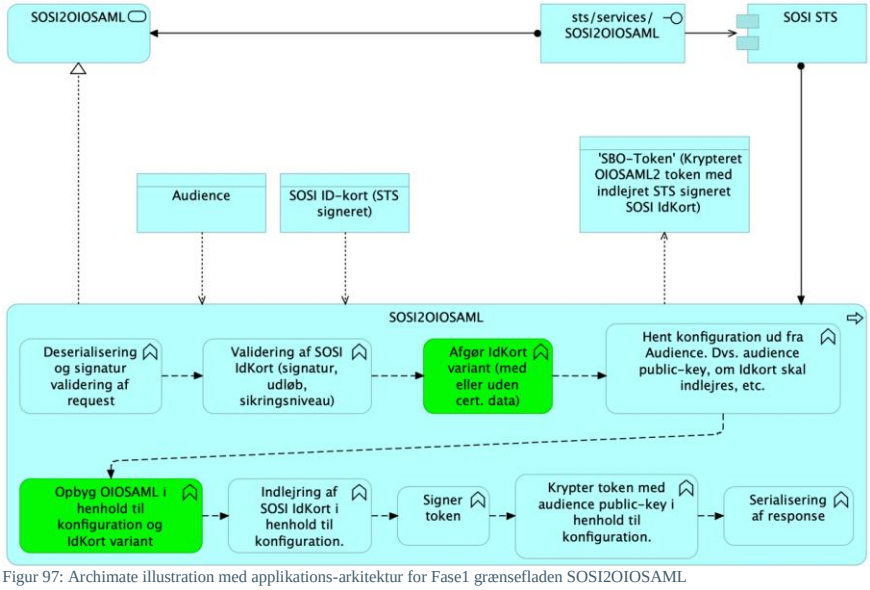
Nedenfor ses et eksempel på medarbejder SOSI idkort med ophav i OIOSAML3/MOCES3.

```
<?xml version="1.0" encoding="UTF-8"?>
<wst:RequestSecurityTokenResponse Context="www.sosi.dk">
  <wst:TokenType>urn:oasis:names:tc:SAML:2.0:assertion:</wst:TokenType>
  <wst:RequestedSecurityToken>
    <saml:Assertion IssueInstant="2020-03-03T16:12:20Z" Version="2.0" id="IDCard">
      <saml:Issuer>NSP-STS </saml:Issuer>
      <saml:Subject>
        <saml:NameID Format="medcom:cprnumber">1802602810</saml:NameID>
        <saml:SubjectConfirmation>
          <saml:ConfirmationMethod>urn:oasis:names:tc:SAML:2.0:cm:holder-of-key</saml:ConfirmationMethod>
          <saml:SubjectConfirmationData>
            <ds:KeyInfo>
              <ds:KeyName>OCESSignature</ds:KeyName>
            </ds:KeyInfo>
          </saml:SubjectConfirmationData>
        </saml:SubjectConfirmation>
      </saml:Subject>
      <saml:Conditions NotBefore="2020-03-03T16:12:20Z" NotOnOrAfter="2020-03-04T16:12:20Z"/>
      <saml:AttributeStatement id="IDCardData">
        <saml:Attribute Name="sosi:IDCardID">
          <saml:AttributeValue>tMyjQVcvbnqDMGo4dYtmJg==</saml:AttributeValue>
        </saml:Attribute>
        <saml:Attribute Name="sosi:IDCardVersion">
          <saml:AttributeValue>1.0.1</saml:AttributeValue>
        </saml:Attribute>
        <saml:Attribute Name="sosi:IDCardType">
          <saml:AttributeValue>user</saml:AttributeValue>
        </saml:Attribute>
```

```
            <saml:Attribute Name="sosi:AuthenticationLevel">
               <saml:AttributeValue>4</saml:AttributeValue>
            </saml:Attribute>
            </saml:AttributeStatement>
            <saml:AttributeStatement id="UserLog">
            <saml:Attribute Name="medcom:UserCivilRegistrationNumber">
               <saml:AttributeValue>1802602810</saml:AttributeValue>
            </saml:Attribute>
            <saml:Attribute Name="medcom:UserGivenName">
               <saml:AttributeValue>Anders</saml:AttributeValue>
            </saml:Attribute>
            <saml:Attribute Name="medcom:UserSurName">
               <saml:AttributeValue>And</saml:AttributeValue>
            </saml:Attribute>
            <saml:Attribute Name="medcom:UserEmailAddress">aand@andeby.dk</saml:Attribute>
            <saml:Attribute Name="medcom:UserRole">
               <saml:AttributeValue>7170</saml:AttributeValue>
            </saml:Attribute>
            <saml:Attribute Name="medcom:UserAuthorizationCode">
               <saml:AttributeValue>ZXCVB</saml:AttributeValue>
            </saml:Attribute>
            <saml:Attribute Name="medcom:UserOccupation">
               <saml:AttributeValue>coolDuck</saml:AttributeValue>
            </saml:Attribute>
         </saml:AttributeStatement>
         <saml:AttributeStatement id="SystemLog">
            <saml:Attribute Name="medcom:ITSystemName">
               <saml:AttributeValue>SOSITEST</saml:AttributeValue>
            </saml:Attribute>
            <saml:Attribute Name="medcom:CareProviderID" NameFormat="medcom:cvrnumber">
               <saml:AttributeValue>30808460</saml:AttributeValue>
            </saml:Attribute>
            <saml:Attribute Name="medcom:CareProviderName">
               <saml:AttributeValue>orgName</saml:AttributeValue>
            </saml:Attribute>
         </saml:AttributeStatement>
         <ds:Signature id="OCESSignature">
            <ds:SignedInfo>
               <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
               <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
               <ds:Reference URI="#IDCard">
                  <ds:Transforms>
                     <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                     <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                  </ds:Transforms>
                  <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                  <ds:DigestValue>mJyl9smLtypQDYCk/jSzZMc7A4c=</ds:DigestValue>
               </ds:Reference>
            </ds:SignedInfo>
            <ds:SignatureValue>...</ds:SignatureValue>
            <ds:KeyInfo>
               <ds:X509Data>
                  <ds:X509Certificate>...</ds:X509Certificate>
               </ds:X509Data>
            </ds:KeyInfo>
         </ds:Signature>
      </saml:Assertion>
   </wst:RequestedSecurityToken>
   <wst:Status>
      <wst:Code>http://schemas.xmlsoap.org/ws/2005/02/trust/status/valid</wst:Code>
   </wst:Status>
   <wst:Issuer>
      <wsa:Address>TEST2-NSP-STS</wsa:Address>
   </wst:Issuer>
</wst:RequestSecurityTokenResponse>
```

7.2.3 SOSI2OIOSAML (medarbejder)

Nedenfor vises realisering af STS-grænsefladen 'SOSI2OIOSAML'.



Figur 97: Archimate illustration med applikations-arkitektur for Fase1 grænsefladen SOSI2OIOSAML

Justeringerne fra Baseline til Fase1 ligger primært indenfor funktionerne markeret med grønt på Figur 97.

Service	SOSI2OIOSAML
Protokol	WS-TRUST 1.4
Interface	Sts/service/SOSI2OIOSAML
Anvendersystemer	Alle som har en SDN netværksmæssig punkt til punkt aftale til NSP
Bruger	Medarbejder
Input	SOSI idkort (med ophav i MOCES2 eller MOCES3/OIO-SAML3) Audience (dvs. identifikation af den web-løsning der ønskes adgang til)
Output	Krypteret OIOSAML2 adgangstoken, evt. med indlejret STS signeret SOSI idkort. Igennem dokumentet omtales tokenet som "SBO-Token" eller SBOT, da tokenet ofte anvendes til Sikker Browser Opstart. Bemærk: Servicen kan ikke omveksle til et OIOSAML3 token pga. princip 4 i afsnit 7.1 ' Sikkerhedsinfrastrukturen omveks-

	ler kun et token til et andet token på samme eller lavere sikkerhedsniveau'. En konsekvens heraf er, at SBO aktiverede webløsninger under fase1 forsat opstartes med OIOSAML2, og ikke OIOSAML3
Beskrivelse	Anvendes ved Sikker Browser Opstart (SBO) mm., hvor fagsystemet ønsker brugerkontekst og brugerrettigheder overført til web-løsning. Pr. Audience konfigureres det, om SOSI idkort skal indlejres i OIOSAML2, samt den offentlige-nøgle, der skal anvendes til kryptering af token, således at det kun er audience (SBO webløsningen), der kan læse tokenindholdet. Input er et SOSI idkort med ophav i MOCES2 eller med ophav i MOCES3/OIOSAML3. Dvs. et SOSI idkort med certifikatdata (herunder CVR-RID) eller CPR-data i Subject.NameID feltet. Et SOSI idkort med certifikat data i Subject.NameID kan uden videre omveksles til et OIOSAML2 token. Dette er desværre ikke muligt for et SOSI idkort med CPR-data i Subject.NameID, da OIOSAML2 OCES profilen kræver CVR-RID. Den primære forskel mellem Baseline og Fase1 SOSI2OIOSAML er: • Servicen kan modtage et SOSI Idkort med ophav i MOCES2 eller med ophav i MOCES3/OIOSAML3 • Ved omveksling fra et SOSI idkort med ophav i MOCES3/OIOSAML3 vil der opstå nogle mangler i OIOSAML2 tokenet. Det antages ikke, at disse mangler vil volde aftagerne problemer, men det udestår at få antagelsen valideret. Afsnit 7.2.3.1 beskriver indholdet af OIOSAML2 felterne, når input er et SOSI idkort med ophav i MOCES3/OIOSAML3
Migreringsovervejelser	Fase1 SOSI2OIOSAML håndteres som en videreudvikling af Baseline SOSI2OIOSAML. Servicen skal holde styr på, om input SOSI idkort har ophav i MOCES2 eller MOCES3/OIOSAML3 og håndtere de få forskelle skitseret ovenfor. Det skal undersøges om SBO web-løsningerne er afhængige af MOCES2-informationerne i OIOSAML2 tokenet. Hvis dette ikke er tilfældet, så bør web-løsningerne kunne køre uændret videre med Fase1 SOSI2OIOSAML.

7.2.3.1 Håndtering af OCES specifikke attributter i OIOSAML2 (SBO-Token)

Nedenfor behandles de enkelte OCES2 specifikke attributter fra OIOSAML2 OCES profilen. For hver attribut beskrives først det korrekte OCES2-indhold efterfulgt et forslag til dummy-data, når OCES2 data er utilgængelig.

Det vurderes at implikationerne ved at indsætte dymmy data er begrænset, da OIOSAML2 tokenet med dummy-data kun anvendes fra 2 scenarier:

1. Certifikat-scenariet: Ansattes adgang via browser og MOCES (jf. afsnit 6.2.2)
2. Ansattes adgang via browser og fagsystem (Sikker browseropstart) (jf. afsnit 6.2.4)

I det første scenarie er det SEB, der er modtager af tokenet, og felterne med dummy-indhold er ikke relevante for SEB.
I det andet scenarie er det de få webløsninger, der kan opstartes med Sikker Browser Opstart, der er modtager af tokenet (dvs. FMK-online, Sundhedsjournalen, Graviditetsmappen mm.). SBO-webløsningerne antages ikke at afhænge af felterne med dummy-indhold. Denne antagelse bør dog bekræftes via kontakt til de ansvarlige for de enkelte webløsninger.
For begge scenarier gælder, at det primært er, det indlejrede SOSI idkort, der er interessant for modtageren.

Subject feltet
Korrekt indhold med ophav i OCES2-certifikatet:

```
<?xml version="1.0" encoding="UTF-8"?>
 <ns2:Subject xmlns:ns2="urn:oasis:names:tc:SAML:2.0:assertion"> <ns2:NameID
    Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName"
    xmlns:ns2="urn:oasis:names:tc:SAML:2.0:assertion">c=DK,o=IT- og Telestyrelsen // CVR:26769388,cn=Brian Nielsen,Serial=CVR:26769388- RID:1203670161406</ns2:NameID>
    <ns2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer" xmlns:ns2="urn:oasis:names:tc:SAML:2.0:assertion">
       <ns2:SubjectConfirmationData InResponseTo="B59A949A6BA2D9CBBD1233317006316" NotOnOrAfter="2009-01-30T12:09:33Z" Recipient="https://logintst.virk.dk/brs-sp-ref/SAMLAssertionConsumer"/> </ns2:SubjectConfirmation>
 </ns2:Subject>
```

Indhold ved omveksling fra SOSI idkort med ophav i MOCES3/OIOSAML3. Bemærk at kun RID-delen ikke længere udfyldes, øvrige del-elementer (CVR, organisationsnavn, personens navn) kan stadig udfyldes med korrekte værdier:

```
<?xml version="1.0" encoding="UTF-8"?>
 <ns2:Subject xmlns:ns2="urn:oasis:names:tc:SAML:2.0:assertion"> <ns2:NameID
    Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName"
    xmlns:ns2="urn:oasis:names:tc:SAML:2.0:assertion">c=DK,o=IT- og Telestyrelsen // CVR:26769388,cn=Brian Nielsen,Serial=CVR:26769388- RID:NONE</ns2:NameID>
    <ns2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer" xmlns:ns2="urn:oasis:names:tc:SAML:2.0:assertion">
       <ns2:SubjectConfirmationData InResponseTo="B59A949A6BA2D9CBBD1233317006316" NotOnOrAfter="2009-01-30T12:09:33Z" Recipient="https://logintst.virk.dk/brs-sp-ref/SAMLAssertionConsumer"/> </ns2:SubjectConfirmation>
 </ns2:Subject>
```

Certificate Serial Number feltet
Korrekt indhold med ophav i OCES2-certifikatet:

```
<saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" Name="urn:oid:2.5.4.5" Friend-
lyName="serialNumber"> <saml:AttributeValue xsi:type="xs:string">234-2345-76745-23</saml:AttributeValue>
 </saml:Attribute>
```

Indhold ved omveksling fra SOSI idkort med ophav i MOCES3/OIOSAML3:

```
<saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" Name="urn:oid:2.5.4.5" Friend-
lyName="serialNumber"> <saml:AttributeValue xsi:type="xs:string">NONE</saml:AttributeValue>
 </saml:Attribute>
```

RID feltet
Korrekt indhold med ophav i OCES2-certifikatet:

```
<saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" Name="dk:gov:saml:attribute:Rid-
NumberIdentifier">
    <saml:AttributeValue xsi:type="xs:string">1203670161406</saml:AttributeValue>
 </saml:Attribute>
```

Indhold ved omveksling fra SOSI idkort med ophav i MOCES3/OIOSAML3:

```
<saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" Name="dk:gov:saml:attribute:Rid-
NumberIdentifier">
    <saml:AttributeValue xsi:type="xs:string">NONE</saml:AttributeValue>
 </saml:Attribute>
```

UID – CORE feltet
Korrekt indhold med ophav i OCES2-certifikatet:

```
<saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
Name="urn:oid:0.9.2342.19200300.100.1.1">
    <saml:AttributeValue xsi:type="xs:string" FriendlyName="Uid">c=DK,o=IT- og Telestyrelsen // CVR:26769388,cn=Brian
Nielsen,Serial=CVR:26769388- RID:1203670161406</saml:AttributeValue>
 </saml:Attribute>
```

Indhold ved omveksling fra SOSI idkort med ophav i MOCES3/OIOSAML3:

```
<saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
Name="urn:oid:0.9.2342.19200300.100.1.1">
    <saml:AttributeValue xsi:type="xs:string" FriendlyName="Uid">c=DK,o=IT- og Telestyrelsen // CVR:26769388,cn=Brian
Nielsen,Serial=CVR:26769388- RID:NONE</saml:AttributeValue>
 </saml:Attribute>
```

Certificate Issuer feltet
Korrekt indhold med ophav i OCES2-certifikatet:

```
<saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
    Name=" urn:oid:2.5.29.29">
    <saml:AttributeValue xsi:type="xs:string">CN=TDC OCES CA,O=TDC,C=DK</saml:AttributeValue>
 </saml:Attribute>
```

Indhold ved omveksling fra SOSI idkort med ophav i MOCES3/OIOSAML3:

```
<saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
    Name=" urn:oid:2.5.29.29">
    <saml:AttributeValue xsi:type="xs:string">NONE</saml:AttributeValue>
 </saml:Attribute>
```

7.2.4 BST2IDWS og JWT2IDWS (borger)

BST2IDWS og JWT2IDWS er 2 SOSI-STS grænseflader, der kan omveksle fra et token, der identificerer borgeren, til et OIO Identity token, der kan anvendes ved kald til sundhedsføderationens sundhedstjenester.

SOSI STS'en har i baseline to grænseflader:

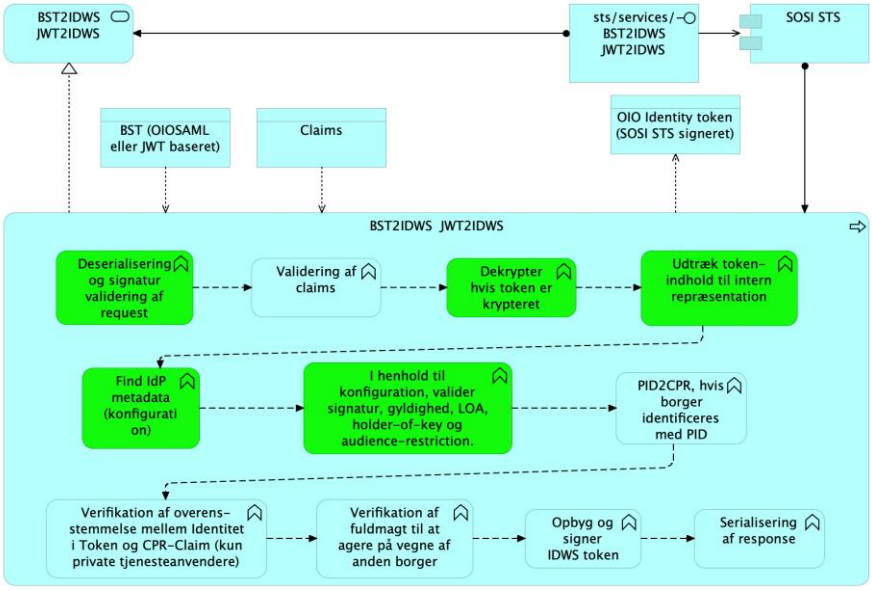
1) BST2IDWS: omveksler fra et SAML-baseret token. Konkret understøttes OIO-Bootstraptokens (NL2 signeret)
2) JWT2IDWS: omveksler fra et JSON WEB Token. Konkret understøttes tokens udsted og signeret af den Autorizationsserver, der anvendes fra FMK app og MinLæge app.

Ses der bort fra håndtering af tokenformat, så anvender grænsefladerne samme omvekslings-algoritme (illustreret på Figur 98).

I fase1 SOSI STS'en forventes de to grænseflader videreført med følgende ændringer:

1) BST2IDWS understøtter omveksling af følgende SAML-baserede tokens: 1) OIO-Bootstraptokens udstedt og signeret af SEB-broker, 2) OIO Identity tokens udstedt og signeret af NL3 STS.
2) JWT2IDWS forventes uændret fra baseline.

På sigt forventes understøttelse af tokens udstedt af uafhængige NSIS-registrerede MitID-brokere (jf. afsnit 6.4.5). Sundhedsføderationen kommer i den forbindelse til at opstille nogle restriktioner vedrørende understøttede token-formater og krævet tokenindhold. Kravene er endnu ikke formuleret og kommer til at afhænge af markedsudviklingen indenfor de uafhængige MitID-brokere.



Figur 98: Archimate illustration med applikations-arkitektur for Fase1 grænsefladen Borger-Identity-Token2IDWS

Justeringerne fra Baseline til Fase1 ligger primært indenfor funktionerne markeret med grønt på Figur 98.

Service	BST2IDWS JWT2IDWS
Protokol	WS-TRUST 1.4
Interface	sts/services/BST2IDWS og JWT2IDWS
Anvendersystemer	Alle som har SDN netværksmæssig adgang
Bruger	Borger
Input	- BorgerIdentityToken (OIOSAML eller JWT baseret) - Claim af sundhedstjenesterettede fuldmagter på formen 'fuldmagt til løsning X fra fuldmagtsgiver Y' - Claim af borgers CPR (kun relevant for private tjenesteanvendere) - Claim af audience, som output token skal udstedes til
Output	OIO Identity token v1.0 token signeret af SOSI STS
Beskrivelse	BST2IDWS og JWT2IDWS er 2 SOSI STS grænseflader, der kan omveksle fra et token, der identificerer borgeren, til et OIO Identity token, der kan anvendes ved kald til sundhedsfø-derationens sundhedstjenester. Baseline udstilles grænsefladerne: 1) BST2IDWS: omveksler fra et SAML-baseret token. Konkret understøttes OIO-Bootstraptokens (NL2 signeret)

	2) JWT2IDWS: omveksler fra et JSON WEB Token. Konkret understøttes tokens udsted og signeret af den Autorizationsserver, der anvendes fra FMK app og MinLæge app. I fase1 skal de to grænseflader understøtte: 1) BST2IDWS: 1) OIO-Bootstraptokens udstedt og signeret af SEB-broker, 2) OIO Identity tokens udstedt og signeret af NL3 STS. 2) JWT2IDWS forventes uændret på kort sigt I udviklingen af fase1 skal fokuseres på at gøre koden mere generisk og fleksibel, således at nye IdP'er/Brokere nemmere kan tilkobles.
Migrationsovervejelser	I en overgangsperiode skal baseline og fase 1 BST2IDWS grænsefladen fungere samtidig. Servicen skal holde styr på token format, version og udsteder, og ud fra dette håndtere forskellene skitseret i afsnittet. JWT2IDWS videreføres i fase1 som i baseline.

7.3 SOSI Gateway (GW)

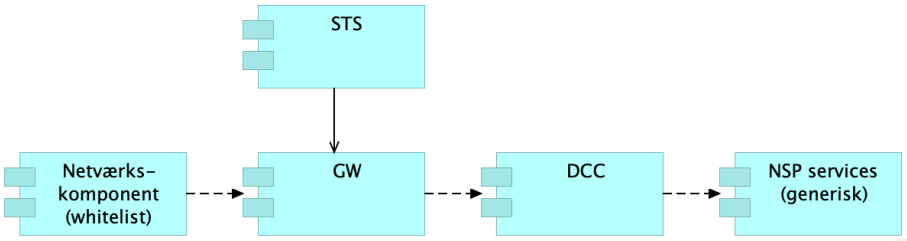
Formålet med SOSI-GW er at flytte ansvaret for signering af SOSI idkort fra de enkelte anvendersystemer til en central service. Denne service kan modtage requests og automatisk vedhæfte et STS signeret SOSI idkort inden requests sendes videre til de endelige NSP service endpoints. Dermed behøver de enkelte anvendersystemer ikke bekymre sig opbevaring af STS signerede SOSI idkort. I stedet håndteres dette af SOSI-GW.
I tabellen nedenfor beskrives servicegrænsefalden for Baseline SOSI-GW, og det vurderes hvorvidt de enkelte grænseflader påvirkes af Fase1.

Service (Brugertype)	Beskrivelse	Påvirkes af Fase1 ?
Generelt for alle services nedenfor	For at kalde NSP services igennem SOSI-GW skal der anvendes webservice-kald, der indeholder et gyldigt niveau 1 SOSI idkort i SOAP-headeren. Dette er krævet for alle kald til og gennem SOSI-GW. Det er også muligt at gennemtvinge at det medsendte idkort (som fx kan være et system-idkort) anvendes i stedet for det idkort, der ligger i GW-Cache. SOSI-GW anvender Subject.NameID fra idkortet som nøgle, når der skal mappes til de STS signerede idkort i GW-cache	Nej
RequestIdCardDigestForSigning **(Medarbejder)**	Denne operation svarer til "login". Der returneres et digest, der kan RSA-signeres med et certifikat.	Nej
signIdCard **(Medarbejder)**	Anvendes til signering af et idkort. Som input gives det RSA-signerede digest, der blev returneret til anvendersystemet af requestIdCardDigestForSigning, samt det certifikat som blev anvendt til signering. Herefter vil SOSI-GW kalde STS, som signerer med føderationens certifikat. SOSI-GW lagre det resulterende signerede niveau 4 idkort i sin cache.	Forventes ikke. Det skal via test tjekkes om signIdCard kan håndtere et MOCES3 certifikat
getValidIdCard **(Medarbejder)**	Afgør om der findes et signeret idkort. Denne operation kan kaldes af anvendersystemet, f.eks. hvert sekund, mens brugeren signerer idkortet i browseren.	Nej
Logout **(Medarbejder)**	Fjerner idkort fra cache. Operationen kan kaldes når en bruger logger af et anvendersystem, og også ønsker at logge af SOSI-GW. Vælges at kalde logout vil brugeren af anvendersystemet skulle logge på, dvs. signere idkort igen, næste gang der foretages kald til NSP services.	Nej
logoutWithResponse **(Medarbejder)**	Fjerner idkort fra cache. Denne operation er den samme som ovenfor, men der returneres "ok" eller DGWSFault, afhængigt af om pågældende id-kort blev fjernet fra cachen eller ej.	Nej
Proxy **(Medarbejder)**	SOSI-GW's gateway-operationen, som kaldes hver gang SOSI-GW skal viderestille til en NSP webservice, hedder proxy.	Nej

Tabellen nedenfor lister en ny services, der skal realiseres som resultat af Fase1.

Service (Brugertype)	Beskrivelse
CreateIdCardFromBST **(Medarbejder)**	Opretter et SOSI idkort i GW ud fra et OIO-Bootstrap-token (BST)

Figuren nedenfor illustrerer SOSI GW's afhængigheder andre komponenter. DCC kan også ligger foran GW. Dette er eksempelvis tilfælde på de dNSP'er, der anvendes af de jyske regioner. Netværkskomponenten eksisterer kun i NGW (NSP GW), hvor flere organisationer anvender samme GW. Eksempelvis kommunerne, lægepraksis og apotekerne.



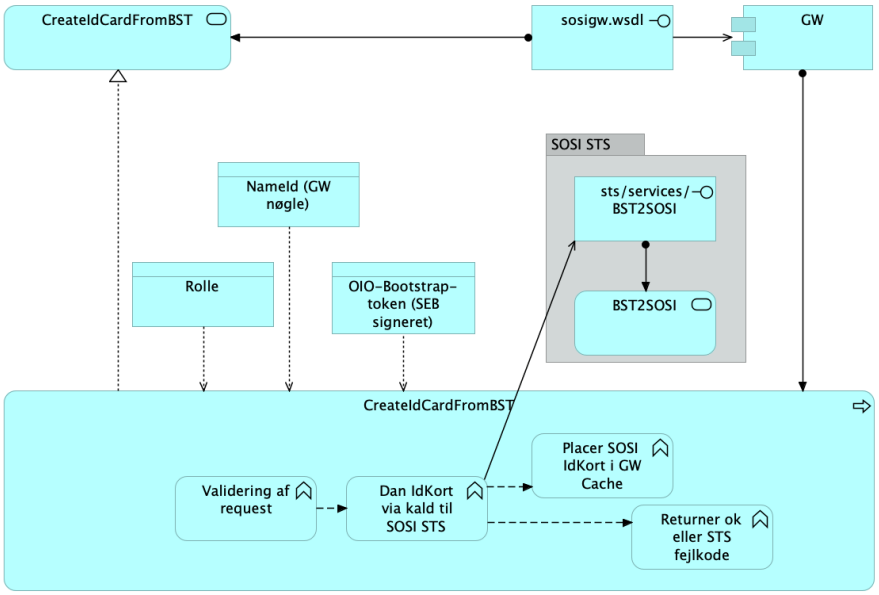
Tabellen nedenfor beskriver de enkelte komponenter, og det vurderes hvorvidt de påvirkes af Fase1.

Afhængighed	Beskrivelse	Påvirkes af transition 1
Netværks-komponent	For den fælleskommunale NSP-Gateway gælder, at anvendersystemets kald foretages med HTTPS. Komponenten sikrer, at der kaldes med et korrekt SSL-klientcertifikat, og at anvendersystemet er whitelistet til at kalde den ønskede service. Hvis dette er i orden viderestilles til SOSI-GW.	Nej
STS	SOSI STS	Ja, se afsnit 7.2.2
DCC	Som udgangspunkt kalder SOSI-GW videre til den relevante NSP service igennem en afkoblingskomponent kaldet DCC (Decoupling Component). Afkoblingskomponenten vil ud fra beskedens SOAP-action afgøre hvilket konkret endpoint, der skal kaldes. Eksempelvis vil DCC'en kalde Det Fælles Medicinkort (FMK) når SOAP action er GetMedineCard. På figuren ligger DCC bagved GW. Dette setup gælder for kommuner, Lægepraksis og apoteker, som kalder GW på den centrale NSP. Regionerne derimod anvender en decentral NSP hvor DDC'en er foranstillet GW (Sundhedsplatformens NSP har dog også GW foran DCC).	Nej

NSP service (generisk)	Den konkrete NSP service (også omtalt sundhedstjeneste), f.eks. FMK, vil oftest blive kaldt igennem DCC. Såfremt beskeden fra anvendersystemet indeholder en WsAddressing SOAP-header, hvor "To" er udfyldt, vil SOSI-GW kalde den pågældende URL direkte i stedet for at viderestille gennem DCC.	Ja, den konkrete NSP service skal kunne forstå SOSI idkort med ophav i MOCES3/OIOSAML3

7.3.1 CreateIdCardFromBST(medarbejder)

Nedenfor vises realisering af den nye GW service "CreateIdCardFromBST".



Figur 99: Archimate illustration med applikations-arkitektur for Fase1 grænsefladen CreateIdCardFromBST

Service	**CreateIdCardFromBST**
Interface	sosigw.wsdl
Anvendersystemer	Alle som har SDN netværksmæssig adgang. Anvendersystemets kald foretages med HTTPS. Det sikres, at der kaldes med et korrekt SSL-klientcertifikat, og at anvendersystemet er whitelistet til at kalde GW (gælder kun den fælleskommunale NSP-Gateway)
Bruger	Medarbejder
Input	- OIO-Bootstrap-token fra Trusted IdP (jf. afsnit 7.2.2.1) - Sundhedsfaglig rolle (der ønsket opsat i SOSI idkort)

	- NameID (nøgle der udpeger det signerede idkort i GW-cache)
Output	- OK - Eller fejlkode fra STS, hvis idkort ikke kan oprettes
Beskrivelse	Ud fra OIO-Bootstrap-token opretter eller erstatter servicen et SOSI idkort i GW-Cachen. SOSI idkort udstedelsen håndteres af SOSI STS'en.
Migreringsovervejelser	Den eksisterende SOSI GW suppleres med den nye service (CreateIdCard-FromOT). De eksisterende services i GW påvirkes ikke. Når den videreudviklede GW er sat i produktion, så vil baseline scenarierne og fase1 scenarierne fungere samtidigt.

Kommenterede [SM5]: BST - konsekvensret

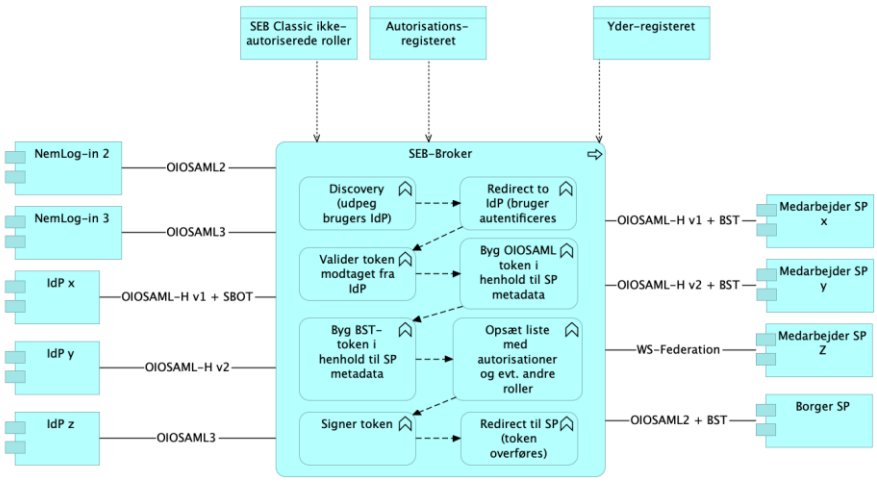
7.4 SEB (Sundhedsvæsenets Elektroniske Brugerstyring)

SEB betragtes her som to tætkoblede komponenter:

1) 'SEB broker', der er en Identitetsbroker, der håndterer billetudstedelse. Med broker menes, at SEB er et knudepunkt mellem en række tilknyttede Identitetsprovidere(IdP'er) og en række serviceprovidere (i dokumentet omtalt tjenesteanvendere), der opererer indenfor sundhedsføderationen.
2) 'SEB classic', som reelt er et IDMS (IDentity Management System) til brugere indenfor sundhedsdomænet. Dvs. et register med identiteter og tilknyttede roller, samt en række grænseflader til administration identiteter og roller.

7.4.1 SEB broker

Nedenfor illustreres realisering af Fase1 SEB broker.



Figur 100: SEB broker

På venstre siden af figuren ses de IdP'er, der kan indgå tilslutningsaftaler med SEB-broker:

- Nemlog-in2
- NemLog-in3
- Lokale IdP'er med relation til sundhedsdomænet, der
  - er NSIS registreret og dermed kan udstede OIOSAML3 tokens
  - eller den kommende OIOSAML3 subprofil 'OIOSAML-H v2', med fokus på sundhedsområdet (Health)
  - der ikke er NSIS registreret, men kan bevise brugerens identitet via et STS signeret SOSI idkort. Konkret overføres et [OIOSAML-H v1] token, der er en subprofil til OIOSAML2 med fokus på sundhedsområdet (Health). Indlejret i OIOSAML-H v1 tokenet skal der ligge et SBO-Token (dvs. et krypteret OIOSAML2 token med indlejret STS signeret SOSI idkort)

På højre siden af figuren ses de SP'er (Service Providers, i kapitel 5 og 6 omtalt tjenesteanvendere), der kan indgå tilslutningsaftaler med SEB og dermed anvende SEB som IdP-broker. Dvs. fagsystemer, webløsninger og app's. På kort sigt vil sundhedsfaglige SP'erne efter succesfuld brugerautorisation modtaget et OIOSAML-H v1 token (Health subprofil af OIOSAML2) med et indlejret OIO-Bootstrap-token (NIST baseret). Når SEB broker på længere sigt bliver NSIS registreret, så vil sundhedsfaglige SP'er modtage et OIOSAML-H v2 token (Health subprofil af OIOSAML3) med et indlejret OIO-Bootstrap-token (NSIS baseret).
På figuren ses en SP, der modtager et generiske SAML tokens (WS-Federation interfacet). Dette er medtaget for at understøtte forskellige interne legacy-løsninger.
Endeligt vises en borger SP, som modtager et OIOSAML2 token med et indlejret OIO-Bootstrap-token (NIST baseret).

I baseline for Sårjournalen og FUT (jf. afsnit 5.2.2) har det været muligt at lave en såkaldt "step-up" autentifikation. Dvs. hæve LoA-niveauet i det medsendte token fra den lokale IdP via en supplerende NL2 autentifiation. Step-up autentifkation videreføres ikke i fase1, da Step-up behovet bortfalder i og med, at de lokale IdP'er NSIS-registreres.
Lokale IdP'er, der på kort sigt ikke NSIS-registeres, kan udstede et OIOSAML-H v1 token med indlejret SBO-token til SEB-broker.

Tabellen nedenfor lister de fase1 scenarier fra kapitel 6, hvori SEB broker indgår, samt hvilke primære opgaver SEB broker håndtere i enkelte scenarier.

SEB-rolle Scenarie	Discovery service	Identitetsbroker	Billetudstedelse	Udlevering af personID (fx CPR), hvis aftager er private løsning	Beriger med medarbejderens mulige roller	Afkoblingspunkt mht. frikøb af NL3-adgang for private-løsninger
Ansattes adgang via rig klient og MitID Erhverv	Ja	Ja	Ja	Ja	Ja	Ja (for private)
Ansattes adgang via browser og MitID Erhverv	Ja	Ja	Ja	Ja	Ja	Ja (for private)
Ansattes adgang via browser og MOCES	Ja	Ja	Ja	Ja	Ja, med mindre rollerne medsendes fra lokal IdP	
Ansattes adgang via browser og egne identitetsmidler	Ja	Ja	Ja	Ja	Ja, med mindre rollerne medsendes fra lokal IdP	
Borgeres adgang via browser: Webløsning der tilgår Nemlog-in3 via SEB		Ja	Ja	Nej		Ja (for private)

Discovery service: Relevant når en web-løsning (SP) ikke på forhånd kender brugerens "hjemme" IdP.

Identitetsbroker: SEB agerer identitetsbroker på tværs af NL3-føderationen og sundhedsføderationen (SOSI-føderationen).

Billetudstedelse: Et OIOSAML WEB-SSO token er i princippet kun gyldigt til den tilgåede service (her SEB). Desuden er tokenet ikke beregnet til servicebaseret adgang. SEB omveksler tokens, der kan anvendes i NL3 føderationen til tokens, der kan anvendes i Sundhedsføderationen. Konkret udsteder SEB adgangstokens i form af OIO-SAML-H og OIOSAML, samt identitetstokens i form af OIO-Bootstrap-token (BST). Via SOSI STS'en kan tjenesteanvenderen omveksle et medarbejder BST til et medarbejder SOSI idkort, og et borger BST til et borger OIOIDWS token. SOSI idkortet skal

anvendes ved medarbejders adgang til patientdata via de nationale sundhedstjenester. OIOIDWS tokenet skal anvendes ved borgers adgang til egne data via de nationale sundhedstjenester.

Udleverer personID (fx CPR), hvis aftager er en privat løsning: SEB er juridisk set en offentlig ejet broker, og derfor har SEB adgang til brugerens fysiske identitet via NL3. For medarbejderidentiteter kræver det, at de er oprettet med CPR i NL3 erhvervs-administrationen.
Private aktører kan ikke få udleveret CPR fra NL3 og deraf følger at SEB heller ikke må udlevere CPR til private webløsninger. Private webløsninger skal selv anmode brugeren om at indtaste CPR. Det udestår at tage stilling til hvorvidt private løsninger skal have adgang til ansattes CPR via SEB.

Beriger med medarbejders mulige roller:
SEB udtrækker medarbejderens autorisationer fra autorisationsregisteret og 'nationale roller' fra SEB classic, med mindre rollerne kan udtrækkes fra tokenet modtaget fra lokal IdP. Autorisationer og nationale roller indlejres i det OIOSAML-H token, der udstedes til tjenesteanvenderen.
Nationale roller indlejres i det BST token der indlejres i OIOSAML-H tokenet.
Herved får tjenesteanvenderen adgang til ansatte autorisationer og nationale rolle og dermed mulighed for at vælge den roller der passer til kaldskonteksten.

Afkoblingspunkt mht. frikøb af NL3-adgang for private-løsninger: Borgerens adgang til deres sundhedsdata kræver autentifikation på højt niveau med MitID, eksempelvis via NL. Det frie danske sundhedsvæsen er et offentlig betalt tilbud til alle danskere, der drives i et samarbejde mellem offentlige (regioner og kommuner) og private (lægepraksis mm.) organisationer.
MitID og NL er fra fællesoffentlige side frikøbt for offentlige løsninger, men dette gælder ikke for private sundhedsløsninger. Sundhedsområdet har derfor frikøbt autentifikation via MitID/NL3 for private sundhedsløsninger. Adgangen styres via opkobling til SEB.

I tabellen specificeres fase1 SEB broker grænsefladen.

Service	SEB Broker
Interface	OIOSAML2 WEBSSO OIOSAML3 WEBSSO WS-Federation
Anvendersystemer	Web-løsninger indenfor sundhedsområdet
Bruger	Medarbejder, Borger
Input	- OIOSAML2 fra Nemlogin2 - OIOSAML3 fra NemLogin3 - OIOSAML-H v1 (Health subprofil til OIOSAML2) fra lokale IdP'er med indlejret SBO Token

	- OIOSAML-H v2 (Health subprofil til OIOSAML3) fra lokale IdP'er
Output	- OIOSAML-H v1 med indlejret OIO-Bootstrap-token - OIOSAML-H v2 med indlejret OIO-Bootstrap-token, dog først når SEB er NSIS registreret (jf. princip 1 i afsnit 7.1). - Generiske SAML tokens (WS-Federation interfacet) til forskellige interne legacy løsninger. -OIOSAML2 med indlejret OIO-Bootstrap-token (borger)
Beskrivelse	Som beskrevet i teksten ovenfor, så håndterer SEB opgaverne: 1. Discovery service 2. Identitetsbroker på tværs af føderationer 3. Billetudstedelse 4. Udleverer personID 5. Beriger med medarbejders mulige nationale roller/autorisationer 6. Afkoblingspunkt mht. frikøb af NL3-adgang for private-løsninger Mht. punkt 1, så er denne opgave kun relevant for brugere af typen medarbejder. Mht. punkt 3 skal SEB indlejre et OIO-Bootstrap-token i det OIOSAML token, der udleveres fra SEB. Det udestår at få profileret OIO-Bootstrap-tokenet (jf. afsnt 7.2.2.1). Mht. punkt 5, så er denne opgave kun relevant for brugere af typen medarbejder. Mht. punkt 6, så er denne opgave kun relevant for brugere af typen borger. Tokens udleveres under hensyntagen til Privacy. Dvs. det skal pr. serviceaftager kunne opsættes, hvilke attributter der udveksles fra SEB, således at anvenderen ikke modtager persondata, der ikke er absolut nødvendige. Den primære forskel mellem Baseline og fase1 SEB Broker er: • I fase1 indlejres OIO-Bootstrap-token i de OIOSAML tokens der udstedes fra SEB-broker. I baseline indlejres SOSI-idkort for ansatte i visse scenarier og NL2 BST token for borger. • I baseline output token indlejres medarbejderens autorisationer. I fase1 scenarierne forventes dette suppleret med de 'nationale roller'

	• Fase1 SEB-broker skal kunne håndtere en række nye tokens, der ikke håndteres i Baseline SEB-broker. De nye tokens er OIOSAML3, OIOSAML-H v2 og OIO-Bootstrap-token • Baseline SEB-broker anvender RID til identifikation af ansatte. Fase1 SEB-broker anvender både RID og Global Employee UUID. • Fase1 SEB-broker skal pr. serviceaftager kunne opsætte hvilke attributter, der må udleveres under hensyntagen til brugerens privacy.
Migrationsoverve-jelser	Det bør kunne konfigureres på begge sider at SEB om IdP eller SP anvender Baseline tokenformater eller fase1 tokenformater.

7.4.2 SEB Classic (medarbejder)

Oprettelse og administration af brugere i SEB Classic er i høj grad organiseret omkring OCES2 certifikater som identifikationsmiddel og CVR-RID som primærnøgle.
Med MitID/NL3/OCES3 udfases OCES2 og RID, og der er derfor behov for at indføre en anden autentifikationsproces og primærenøgler i SEB-Classic.

Analyse og tilpasning af SEB Classic er ikke del af denne målarkitektur og håndteres i andet regi.

7.5 SEAL-bibliotekerne

SEAL Java og .Net hjælpebibliotekerne anvendes af aftagere der anvender SOSI STS'en til omveksling og autentifikation, af DGWS-services som fx FMK og services på NSP, samt af SOSI-STS'en.

SEAL hjælpebibliotekerne skal videreudvikles således at de kan håndtere

- MOCES3/VOCES3 signerede idkort-requests
- Nye VOCES3 STS-føderationscertifikater
- OIOSAML3 baserede omvekslings-/bootstraptokens
- Request/responses til den nye STS-snitflade der kan veksle OIOSAML3 baserede omvekslings-/bootstraptokens til SOSI idkort

7.6 NSP AccessHandler

AccessHandler er en NSP-internt komponent der validerer tokens (SOSI idkort og borger IDWS tokens) i indkommende service-requests.

AccessHandler skal tilrettes således at VOCES2 og VOCES3 signaturer kan håndteres samtidig.

7.7 Certificate Revocation Authority (CRA) på NSP

CRA er en internt, centralt deployeret NSP-komponent som periodisk henter OCES spærrelister og gemmer indholdet i en database som distribueres til NSP instanserne. CRA skal kunne hente spærrelister for OCES3 certifikater på lige fod som OCES2 spærrelister hentes og gemmes i databasen i nuværende udgave af CRA.
(I og med relationerne mellem OCES3 certifikater og spærrelister er næsten identiske som i OCES2 (jf. afsnit 6.5), formodes der, at der alene skal opdateres til den nye Seal.Java med OCES3 understøttelse og tilføjes konfigurationer til CRA for at kunne håndtere OCES3 spærrelister.)

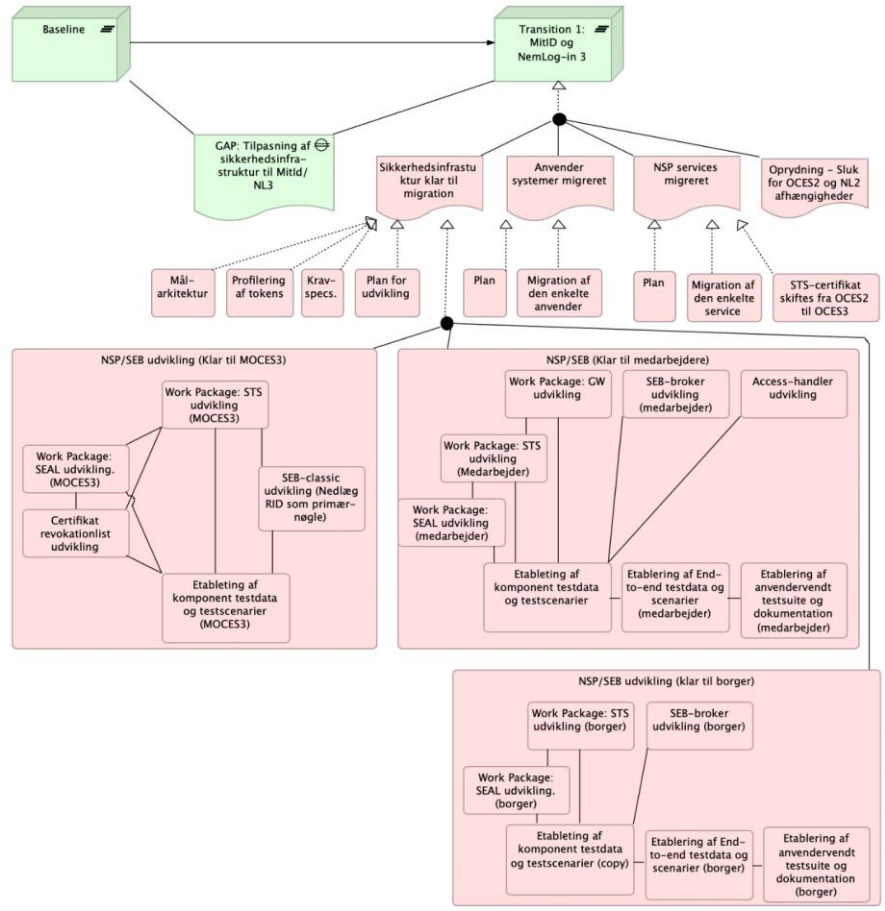
7.8 DCC

Analyse af DCC udestår.

8. Migrationsplan

I en migreringsfase skal AS-IS og TO-BE sikkerhedsarkitekturen kunne fungere samtidig.
Nedenfor illustreres arbejdspakker og leverancer frem til transition 1. Udviklingsopgaven er nedbrudt i tre skridt:

1) Klar til MOCES3. Dvs. udvikling af den nødvendige funktionalitet til realisering af STS-autentifikation med MOCES3.
2) Klar til medarbejdere. Dvs. udvikling af den nødvendige funktionalitet til realisering af alle medarbejder-scenarier
3) Klar til borgere. Dvs. udvikling af den nødvendige funktionalitet til realisering af alle borger-scenarier


Baseline
Transition 1: MitID og NemLog-in 3
GAP: Tilpasning af sikkerhedsinfra-struktur til MitId/ NL3
Sikkerhedsinfrastru ktur klar til migration
Anvender systemer migreret
NSP services migreret
Oprydning - Sluk for OCES2 og NL2 afhængigheder
Mål-arkitektur
Profilering af tokens
Krav-specs.
Plan for udvikling
Plan
Migration af den enkelte anvender
Plan
Migration af den enkelte service
STS-certifikat skiftes fra OCES2 til OCES3
NSP/SEB udvikling (Klar til MOCES3)
Work Package: STS udvikling (MOCES3)
Work Package: SEAL udvikling. (MOCES3)
SEB-classic udvikling (Nedlæg RID som primær-nøgle)
Certifikat revokationlist udvikling
Etableting af komponent testdata og testscenarier (MOCES3)
NSP/SEB (Klar til medarbejdere)
Work Package: GW udvikling
SEB-broker udvikling (medarbejder)
Access-handler udvikling
Work Package: STS udvikling (Medarbejder)
Work Package: SEAL udvikling (medarbejder)
Etableting af komponent testdata og testscenarier
Etablering af End-to-end testdata og scenarier (medarbejder)
Etablering af anvendervendt testsuite og dokumentation (medarbejder)
NSP/SEB udvikling (klar til borger)
Work Package: STS udvikling (borger)
SEB-broker udvikling (borger)
Work Package: SEAL udvikling. (borger)
Etableting af komponent testdata og testscenarier (copy)
Etablering af End-to-end testdata og scenarier (borger)
Etablering af anvendervendt testsuite og dokumentation (borger)

SUNDHEDSDATA-
STYRELSEN

Henvisning

[DIGST 2020]	UDKAST: Referencearkitektur for brugerstyring, fællesoffentlig. DIGST 2020.
[OIOSAML-H]	OIOSAML Attribute Profiles for Healthcare (OIOSAML-H) 1.0
[SDS 2020]	Målbillede for sammenhængende brugerstyring.
[CVR RID analyse]	Brugen af CVR RID i nationale tokens - v01.docx