SUNDHEDSDATA-
STYRELSEN

Appendix 1d

Løsningsarkitektur for App Gravid_i_DK og Frameløsningen eGraviditet.dk

Projekt 'Digital løsning til Graviditetsforløbet'

Indholdsfortegnelse

Versionshistorik

Version	Dato	Hvad	Hvem
1.0	9. juni 2020	Udarbejdet ifm. udbud, der udsendes 12. juni 2020	SMI, Lakeside

1. Baggrund og formål

I efteråret 2019 blev der udarbejdet et målbillede for Digital løsning til Graviditetsforløbet. Målbilledet er nedbrudt efter FDA arkitekturreol-modellen (se Figur 1 og jf. "Appendix 1c Målbillede for digital løsning til graviditetsforløbet").

Dette dokument vedrører løsningsarkitekturen for App- og Web-løsning til Det digitale graviditetsforløb. Den mobile App (navngivet Gravid_i_DK) giver den gravide og hendes pårørende mulighed for at følge med i de sundhedsdata, der opsamles undervejs i graviditetsforløbet, samt mulighed for at få overblik over graviditetsforløbets planlagte og afsluttede aktiviteter. Webløsningen (navngivet eGraviditet.dk) giver de sundhedsfaglige mulighed for at koordinere indsatsen omkring graviditetsforløbet.
Løsningsarkitekturen afgrænses til fase 1 funktionalitet, som defineret i målarkitekturens afsnit 3.4.3 "Målbillede – faseopdeling".

Figur 1: FDA arkitekturreol

Nærværende dokument skal anvendes ifm. udarbejdelse af kravspecifikation, der sendes i udbud primo juni. Dokumentet indeholder et kapitel for hver af følgende lag i FDA arkitekturreolen.

- Opgavearkitektur: Beskriver de opgaver som Gravid_i_DK og eGraviditet.dk skal håndtere i fase 1.
- Informationsarkitektur: Beskriver de dataobjekter, der udgør graviditetsdata i fase 1.
- Applikationsarkitektur: Beskriver applikationsarkitekturen, der skal understøtte Gravid_i_DK og eGraviditet.dk i fase 1.
- Sikkerhedsarkitektur: Beskriver sikkerhedskomponenter, som skal håndtere autentifikation for henholdsvis den gravide, pårørende og de sundhedsfaglige.

1.1. Proces for udarbejdelse af løsningsarkitekturen

Nærværende løsningsarkitektur for Gravid_i_DK og eGraviditet.dk udarbejdes af projektets tekniske konsulenter i samarbejde med arkitekterne i projektets arbejdsgruppe og arkitekter i SDS.

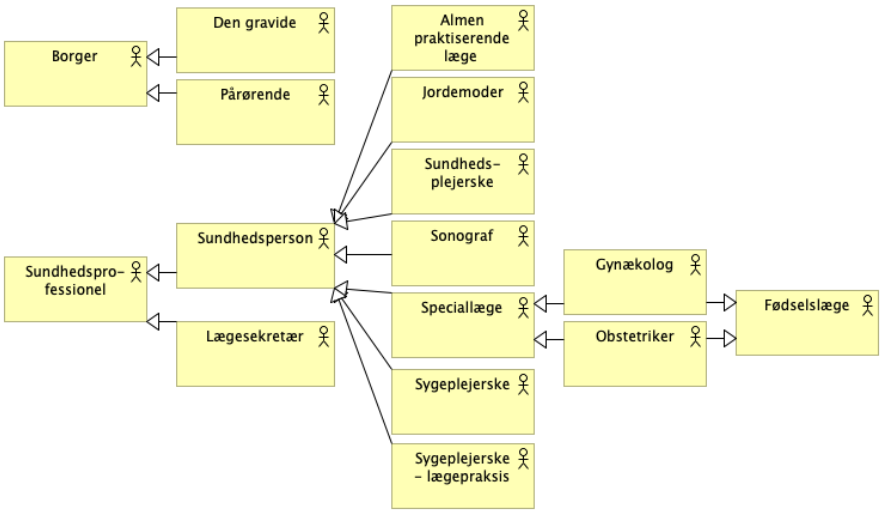
Review proces for løsningsarkitekturen for Gravid_i_dk og eGraviditet.dk:

1. Review: Review møde med arbejdsgruppen arkitekter og SDS arkitekter
2. Review: Skriftelig review i et lidt større kreds
3. Review: RUSA

2. Opgavearkitektur

Arbejdsgangene i henholdsvis Gravid_i_DK (App) og eGraviditet.dk (webløsning) er beskrevet i "Appendix 1a Use cases Gravid_i_DK App.docx" og "Appendix 1b Use cases eGraviditet.dk til Sundhedsfaglige.docx". Desuden er der udarbejdet wireframes til eGraviditet.dk (se http://letsgozebra.com/clients/vandrejournal/v2/), som er evalueret af projektets kliniske arbejdsgruppe.

Figur 2 nedenfor er hentet fra målbilledet og illustrerer de roller, der skal anvende henholdsvis Gravid_i_DK og eGraviditet.dk. Gravid_i_DK anvendes af en Borger. eGraviditet.dk anvendes af en Sundhedsfaglig.



Figur 2: Roller til Gravid_i_DK og eGraviditet.dk

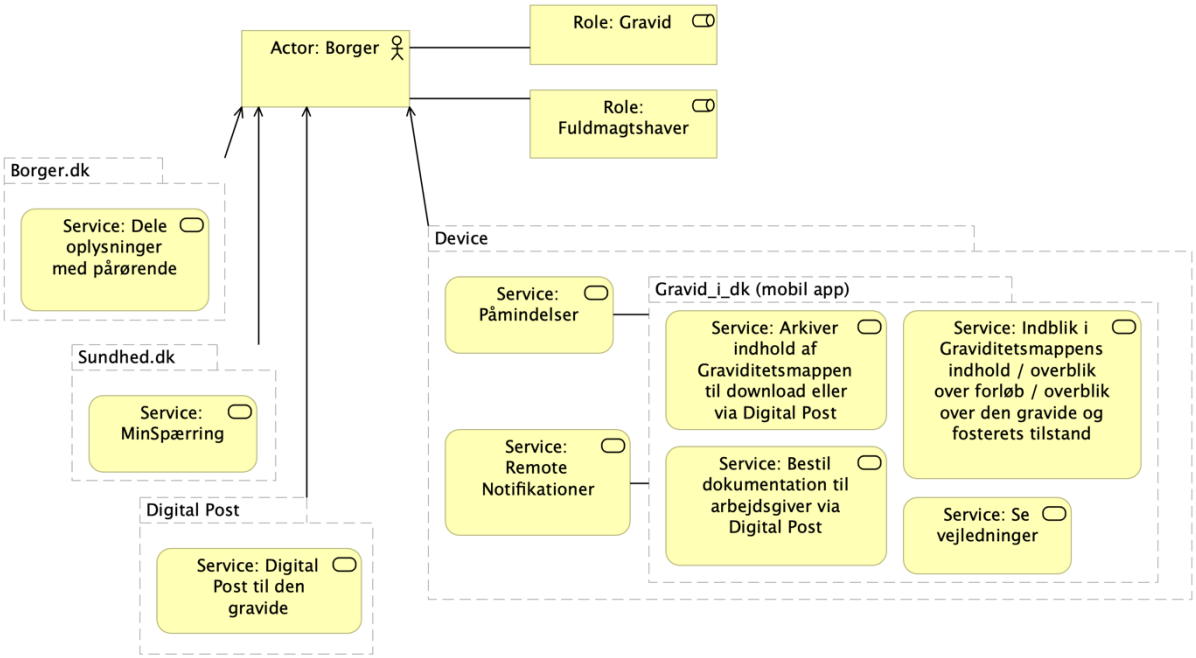
I målbilledets afsnit "5.3 Opgavekatalog" listes de opgaver, der skal varetages af det digitale graviditetsforløb. I tabellen nedenfor listes de opgave fra målbilledets opgavekatalog, der vedrører Borgeren, og som er omfattet af fase 1 i det digitale graviditetsforløb. Første kolonne navngiver opgaven. Anden kolonne beskriver opgaven. Tredje kolonne beskriver, hvordan løsnings-arkitekturen skal understøtte opgaven.

Aktør: Borger		
Opgavenavn	**Beskrivelse**	**Hvad skal arkitekturen understøtte**
Overblik over forløb	Borgeren skal kunne se planlagte og gennemførte aktiviteter i graviditetsforløbet	Gravid_i_DK skal kunne hente og præsentere den gravides graviditetsdata via DokumentDelingsServicen, hvor data ligger fordelt på en række CDA dokumenter

		(Graviditetsplan, Graviditetskort, Aftaler, Målinger, Resuméer).
Se vejledninger	Standardvejledninger. Borgeren skal have adgang til nationale vejledninger vedrørende graviditet via Gravid_i_DK	Gravid_i_DK skal kunne præsentere graviditetsvejledninger, som ligger lagret i et backend system.
Dele oplysninger med pårørende	Den gravide skal kunne give fuldmagt til adgang til Graviditetsmappen for pårørende	Fuldmagt opsættes via den fællesoffentlige digitale fuldmagtsløsning. Ved login skal arkitekturen understøtte OIO-IDWS tokens med fuldmagt.
Spærring af data	Den gravide skal have mulighed for at spærre for adgang til Graviditetsmappen for specifikke sundhedsfaglige personer og organisationer.	MinSpærring håndteres via Sundhed.dk.
Digital Post til den gravide	Vejledning vedrørende brug af Gravid_i_DK og hentning af denne	Der sendes et NAS advis når Graviditetskort oprettes. En services skal opfange denne advis og sende en Digital Post til den gravide
	Information om lukning af Gravid_i_DK i forbindelse med afsluttet graviditet	Der sendes en NAS advis når Graviditetskortet skifter status til afsluttet. En services skal opfange denne advis og sende en Digital Post til den gravide
Dokumentation til arbejdsgiver	Som dokumentation på Graviditet.	Kan aktiveres af borgeren via Gravid_i_DK. Dokumentationen sendes til den gravides private Digital Post konto. Den gravide står selv for den videre formidling til arbejdsgiver
Arkiver indhold af Graviditetsmappen	Der er to use cases med arkivering af indhold af Graviditetsmappen: -Sende indhold som PDF til Digital Post efter behov. -Automatisk job, der ved afslutning af graviditetsforløb, sender indhold som PDF til Digital Post	Løsningen skal kunne udtrække og generere en PDF med indholdet af graviditetsforløbet. Udtrækket skal kunne initialiseres fra Gravid_i_DK efter behov samt automatisk ved afslutning af graviditetsforløbet.
Indblik i Graviditetsmappens indhold / overblik over den gravide og fosterets tilstand	Borgeren skal kunne danne sig et overblik over relevante data, målinger og journalnotater vedrørende graviditetsforløbet.	Gravid_i_DK skal kunne hente og præsentere den gravides graviditetsdata via DokumentDelingsServicen, hvor data ligger fordelt på en række CDA dokumenter (Graviditetsplan, Graviditetskort, Aftaler, Målinger, Resumer).

Notifikationer NB: Det er besluttet at udskyde App notifikationer til en senere fase, da der er en række udfordringer: 1) konceptet skal sammentænkes med øvrige notifikationer, der udsendes fra sundhedsvæsenet 2) Det vil være et ukomplet billede af notifikationer, da DDS ikke udsender notifikationer ved oprettelse/ændring af dokumenter	Borgeren skal kunne modtage notifikationer om ændringer og nye aktiviteter i Graviditetsmappen	Remote notifikationer, som sendes fra backendsystemer til borgerens device, Notifikationerne sendes ved bestemte hændelser i backendsysterne. Dette kan fx være ændringer i Graviditetsplan eller hvis der foretages nye målinger eller bookes aftaler
Påmindelser NB: Det er besluttet at udskyde App påmindelser til en senere fase, da der er en række udfordringer: 1) konceptet skal sammentænkes med øvrige notifikationer, der udsendes fra sundhedsvæsenet 2) Hvis en aftale flyttes notificeres brugeren ikke	Den gravide skal kunne modtage påmindelser om forestående aftaler.	Lokale notifikationer som den gravide kan opsættes via Gravid_i_DK. Fx påmindelser om kommende aftaler

Figur 3 nedenfor illustrerer opgaverne fra tabellen fordelt på de klientapplikationer, hvor opgaverne varetages.



Figur 3: Borgerens opgaver fordelt på klient-applikationer

Som det fremgår håndteres:

- Opsætning af fuldmagt via borger.dk
- MinSpærring via sundhed.dk
- Post til den gravide via Digital Post

Gravid_i_DK håndterer primært opgaver, der giver den gravide (og eventuelt fuldmagtshaver) indblik i graviditetsmappens indhold samt vejledninger vedrørende graviditeten. Desuden er det muligt fra Gravid_i_DK at bestille to forskellige PDF-dokumenter, som leveres via Digital Post. En PDF med alt information registreret i graviditetsforløbet, samt en PDF der kan anvendes som dokumentation overfor arbejdsgiver. På det device (mobiltelefon), hvor Gravid_i_DK installeres, kan der opsætte påmindelser fra Gravid_i_DK, samt modtages Remote Notifikationer fra backendsystemerne[1].

I tabellen nedenfor listes de opgave fra målbilledets opgavekatalog, der vedrører den Sundhedsfaglige, og som er omfattet af fase 1 i det digitale graviditetsforløb.

Aktør: Sundhedsfaglig		
Opgavenavn	**Beskrivelse**	**Hvad skal arkitekturen understøtte**
Registrering af konsultation	For hver konsultation skal relevante oplysninger deles med de andre aktører. - Resume - Målinger	eGraviditet.dk skal kunne gemme et Resume og en Måling i form af et CDA dokument i XDS infrastrukturen
Etablering af visitationsgrundlag	Etablering af indhold i Graviditetskort; tidligere svangerskabs- og vandrejournal.	eGraviditet.dk skal kunne opstarte et Graviditetskort (via Graviditetskort-registeret) og gemme visitationsgrundlag heri. I samme proces vil der blive

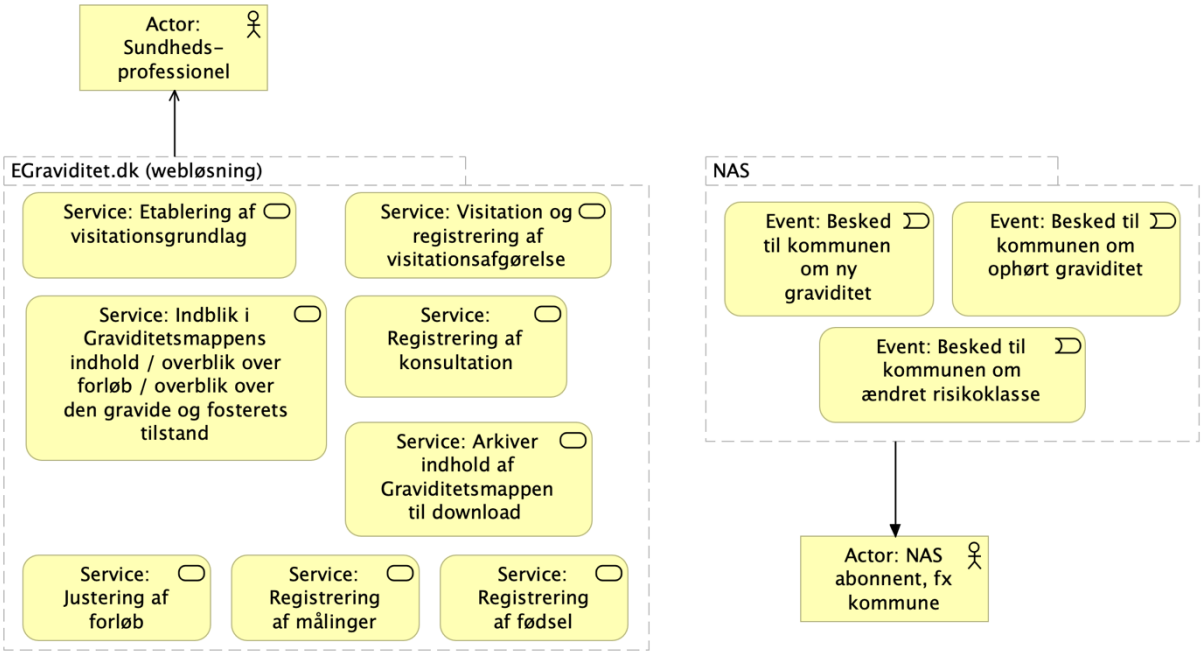
[1] NB: Fjernet fra fase 1.

	Etablering af visitationsgrundlag ved egen læge	opstartet en Graviditetsplan (via Graviditetsplan-registeret)
Visitation og registrering af visitationsafgørelse	Visitationen foregår på baggrund af de oplysninger, der findes i Graviditetsmappen. I visitationen tilknyttes de relevante ressourcer, og evt. justeringer af forløbet foretages. Visitatorens afgørelsen gemmes i Graviditetskortet	eGraviditet.dk skal kunne gemme visitationsafgørelse i Graviditetskort (via Graviditetskort-registeret) samt justere Graviditetsplan (via Graviditetsplan-registeret)
Registrering af målinger	Simple målinger skal fremgå af Graviditetsmappen. Ved en simpel måling forstås målinger og prøver som laves lokalt til en konsultation. Eks. herpå: - Symfyse-fundus måling - Vægt - Blodtryk - Urinprøve - Blodprøve analyseret lokalt	eGraviditet.dk skal kunne gemme en måling i form af et CDA dokument i XDS infrastrukturen
Overblik over forløb	Alle involverede parter skal kunne se planlagte og gennemførte aktiviteter i graviditetsforløbet	eGraviditet.dk skal kunne hente og præsentere den gravides graviditetsdata via DokumentDelingsServicen, hvor data ligger fordelt på en række CDA dokumenter (Graviditetsplan, Graviditetskort, Målinger, Resumer).
Justering af forløb	Sundhedsfaglige skal kunne justere forløbet ud fra en sundhedsfaglig vurdering på et hvert givet tidspunkt. Dette følges op af en henvisning, hvis justeringen medfører aktiviteter udenfor eget regi. Henvisningen foregår via egne systemer, men henvisningsårsagen og metoden registreres i Graviditetsmappen i et resume.	eGraviditet.dk skal kunne justere Graviditetsplanen (via Graviditetsplan-registeret)
Registrering af fødsel	Selve fødslen håndteres i egne systemer. I Graviditetsmappen registreres et resume af fødslen til deling med andre aktører.	eGraviditet.dk skal kunne gemme et Resume i form af et CDA dokument i XDS infrastrukturen

Dele vejledninger	Standardvejledninger. Der skal være adgang til nationale vejledninger via en GraviditetsApp for den gravide og hendes pårørende.	Det skal være muligt at oprette samt vedligeholde et sæt af nationale vejledninger vedr. graviditetsforløbet (håndteres evt. af en redaktørrolle). Vejledningerne formidles til Borgeren via Gravid_i_DK. Til vedligehold og distribution af vejledninger er der behov for et system med "Content management" funktionalitet
Besked til kommunen om ny graviditet	Kommunen får en besked om ny graviditet, så kommunen kan planlægge den del af graviditets- og barselsforløb, som ligger i kommunalt regi.	Kommunen abonnerer på NAS (National Advis Service) og modtager NAS advis, når et graviditetsforløb initieres. Kommunen kan herefter selv tilgå graviditetsdata via fx eGraviditet.dk eller backend services. Det udestår at få undersøgt om kommunerne har fagsystemer, der kan abonnere på NAS. Hvis ikke, skal det overvejes om der skal etableres en komponent, der lytter på NAS på vegne af kommunerne, og som kan transformere beskederne til et format, som kommunerne kan modtage – Fx Medcom beskeder eller integrere til den kommunal beskedfordeler.
Besked til kommunen om ændret risikoklasse (ny opgave – ikke med i målbilledet)	Kommunen får en besked, hvis risikoklasse ændres, så kommunen kan planlægge den del af graviditets- og barselsforløb, som ligger i kommunalt regi.	Kommunen abonnerer på NAS (National Advis Service) og modtager NAS advis, hvis risikoklasse ændres. Kommunen kan herefter selv tilgå graviditetsdata via fx eGraviditet.dk eller backend services. Kommentaren i rækken ovenfor vedr. en proxy-komponent er også relevant her.
Besked til kommunen om ophørt graviditet	Kommunen får en besked om, at gravidteten er ophørt, så kommunen kan justere sine planer (aflyse ressourcer eller booke aftaler)	Kommunen abonnerer på NAS (National Advis Service) og modtager NAS advis, når et graviditetsforløb ophører. Kommunen kan herefter selv tilgå graviditetsdata via fx eGraviditet.dk eller backend services. Kommentaren i rækken ovenfor vedr. en proxy-komponent er også relevant her.

Indblik i Graviditetsmappens indhold / overblik over den gravide og fosterets tilstand	Sundhedsfaglige skal kunne danne sig et overblik over relevante data, målinger og journalnotater vedrørende graviditetsforløbet	eGraviditet.dk skal kunne hente og præsenterer den gravides graviditetsdata via DokumentDelingsServicen, hvor data ligger fordelt på en række CDA dokumenter (Graviditetsplan, Graviditetskort, Målinger, Resumer).
Arkiver indhold af Graviditetsmappen (ny opgave – ikke med i målbilledet)	Den sundhedsfaglige skal efter endt graviditetsforløb kunne downloade graviditetsforløbet som PDF med henblik på arkivering	Løsningen skal kunne udtrække og generere en PDF med indholdet af graviditetsforløbet. Udtrækket aktiveres fra og downloades til eGraviditet.dk

Figur 4 nedenfor illustrerer opgaverne fra tabellen fordel på de klientapplikationer, hvor opgaverne varetages.



Figur 4: De Sundhedsfagliges opgaver

eGraviditet.dk håndterer primært opgaver, der giver den sundhedsfaglige et overblik over graviditetsmappens indhold samt mulighed for at initialisere, ændre og justere indholdet.

De tre beskeder til kommunen formidles via den Nationale Advis Service (NAS). Backend registrene sender Advis via NAS ved bestemte hændelser. Dette kan eksempelvis være, når et graviditetsforløb initieres, når risikoklassen i Graviditetskort ændres eller når et graviditetsforløb ophører.
Som nævnt i tabellen, så skal det undersøges om kommunerne har fagsystemer, der kan abonnere på NAS. Hvis ikke, skal det overvejes om der skal etableres en komponent, der lytter på NAS på vegne af kommunerne, og som kan transformere beskederne til et format, som kommunerne kan modtage – eksempelvis Medcom beskeder eller integration til den kommunale beskedfordeler.

3. Informationsarkitektur

I målbilledets afsnit ”6.2 Centrale forretnings- og dataobjekter” defineres de centrale forretnings- og dataobjekter i det digital graviditetsforløb. I fase 1 er dette afgrænset til dataobjekterne i tabellen nedenfor. Hvert dataobjekt mapper til et CDA dokument, og tilsammen udgør dokumenterne, det der omtales Graviditetsmappen.

Dataobjekt	Beskrivelse	Format
Aftale	En Aftale er en planlagt social- eller sundhedsrelateret aktivitet. Det kan eksempelvis være en booking, som er fastlagt via et bookingsystem. En Aftale indeholder tidspunkt, sted og nøgledeltagere ved et møde mellem den gravide (borgeren), eventuelt pårørende og sundhedsfaglige.	Dansk HL7 CDA profil – APD-DK.
Graviditets-plan (HL7 Care Plan)	En Graviditetsplan er en HL7 Care plan målrettet et graviditetsforløb. Dvs. en individuel handlingsplan bestående af en liste af Aktiviteter, samt en beskrivelse af sundhedsmålet med planen. En Aktivitet kan i Graviditetsplanen udmøntes i fx en Konsultation hos jordemoder eller en ultralydsscanning hos en sonograf. En Aktivitet kan have en vejledende tidsramme (fx graviditetsuge 28-29), et fastlagt tidspunkt (dato-tid), en fastlagt udførende aktør (fx navngivet organisatoriskenhed og evt. jordemoder), en titel (fx 1. jordemoderkonsultation) samt en status. Graviditetsplanen giver den gravide og sundhedsfaglige anvendere af informationen et overblik over planlagte aktiviteter i hendes graviditetsforløb. Ved initiering består graviditetsplanen af de aktiviteter, som indgår i et fælles nationalt basis-graviditetsforløb. Opstår der komplikationer undervejs i graviditetsforløbet tilføjes de aktiviteter der iværksættes til Graviditetsplanen. Graviditetsplanen giver de sundhedsfaglige et tværorganisatorisk, koordineret overblik over planlagte aktiviteter i graviditetsforløbet. De sundhedsfaglige fastholder og kommunikerer nye tiltag over for den gravide. Fx ved at tilføje eller fjerne planlagte aktiviteter.	Dansk HL7 CDA profil - CPD. Til pilotafprøvningen laves et udkast til en implementerings-vejledning for Graviditetsplanen[2]. Denne profileres efterfølgende af Medcom.
Graviditets-kort	Indeholder de stamoplysninger, som i dag ligger i svangerskabsjournalen og til dels vandrejournalen. Informationen anvendes i forbindelse med visitation samt den løbende opsamling på og risikovurdering af graviditetsforløbet	Til pilotafprøvningen udarbejdes et udkast til en CDA profil for

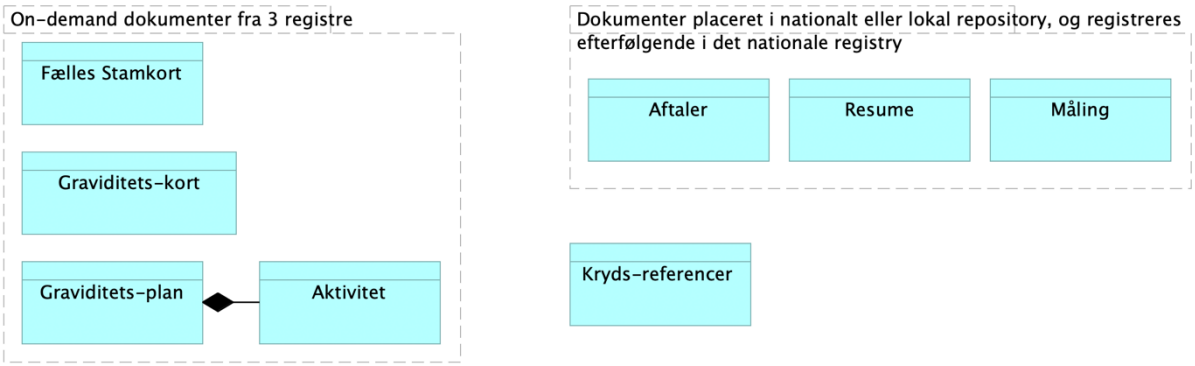
[2] https://www.nspop.dk/display/NDPV/GSR+-+Guide+til+anvendere

	Graviditetskortet indeholder relevante baggrundsdata vedrørende den gravide, som hidrører fra før graviditeten og indsamles løbende i forbindelse med det aktuelle graviditetsforløb. Eksempler på data er: vægt, BMI, tidligere fødsler, tidligere aborter, fertilitetsbehandling, terminsberegning, allergier, kroniske sygdomme, sociale forhold, arbejdsmiljøpåvirkninger, rusmidler, fertilitetsbehandling, ønsker til graviditetsforløb, screeninger og samlet sundhedsfagligvurdering af den gravides behov.	Graviditetskortet[3]. Denne profileres efterfølgende af Medcom.
Resumé	Anvendes til at opsamle de sundhedsfagliges konklusioner. Eksempelvis ved afslutning af en konsultation, ved overstået fødsel eller ved gennemgang af den gravides spørgeskemabesvarelse.	CDA profilering iværksat hos Medcom[4]
Måling	Anvendes til simple strukturerede målinger, som foretages på stedet og noteres i systemet med det samme, når den gravide er til konsultation. Fx hos jordemoder eller sonograf. Eksempler på målinger er vægt, blodtryk, symfyse-fundus samt urin. Flerfoldsgraviditet vil fremgå ved, at der internt i CDA-dokumentet for en måling ligger et måleresultat pr. foster.	Måling er en ny CDA profil, som har få afvigelser fra den eksisterende PHMR profil (Personal Health Monitoring Report) I projektet anvendes et profiludkast, som færdig profileres efter pilotafprøvningen. Information vedrørende formatet findes i **Error! Reference source not found.**.
Fælles Stamkort	Alle danskere har et stamkort. Det meste af indholdet i stamkortet er trukket fra CPR-registeret og kan ikke ændres af borgeren (fx CPR-nummer, navn og adresse). Borgeren kan via sundhed.dk tilknytte telefonnummer, sprog, pårørende samt midlertidig adresse til stamkortet. (se også servicen Fælles Stamkort (FSK))	Dansk HL7 CDA profil – Fælles Stamkort (DK-PDC 2.0).
Kryds-referencer	Formålet med Kryds-referencer er at binde kliniske oplysninger sammen. Fx binde en Aftale, Måling eller et Resume til en bestemt Aktivitet i en Graviditetsplan. Eksempelvis en Graviditetsplan, der indeholder den planlagte aktivitet ”Jordemoder konsultation i uge 22”.	SDS har nedsat en arbejdsgruppe, der skal udrede, hvordan Krydsreferencer mellem CDA

[3] https://www.nspop.dk/display/NDPV/GCP+-+Guide+til+anvendere
[4] https://www.medcom.dk/projekter/svangre-og-vandrejournal

	I forbindelse med aktivitetens planlægning laves en Aftale med mødested og dato. I forbindelse med aktivitetens gennemførelse laver jordemoder nogle Målinger og et Resume. Med Krydsreferencer vil den gravide eller de sundhedsfaglige få et overblik over afviklingen af Graviditetsplanen, og herunder det kliniske "outcome" fra de enkelte aktiviteter i Graviditetsplanen	dokumenter realiseres. Arbejdet er endnu ikke afsluttet. **Error! Reference source not found.** giver en indikation af, hvordan krydsreferencer forventes realiseret.

Figur 5 nedenfor illustrerer dokumenterne i Graviditetsmappen.



Figur 5: CDA view på datamodel i fase 1

Graviditetsplan og tilhørende Aktiviteter ligger i sammen CDA dokument. Kryds-referencer er endnu ikke fastlagt mht. løsningsmodel.

Fælles Stamkort, Graviditetskort og Graviditetsplan er realiseret via 3 centrale registre. Dokumenterne kan udtrækkes som on-demand CDA dokumenter via den nationale DokumentDelingsService.
MinSpærring kan ikke håndtere dokumenter med tværorganisatorisk ejerskab, og derfor ejer alle organisationer med den gravide i behandling, hver deres egen instans af et Graviditetskort og en Graviditetsplan. Ejerskabet medfører, at det kun er ejeren af instansen, som kan lave ændringer til informationerne i instansen. Denne opsplitning gør også, organisationerne på sigt kan hjemtage opbevaringen af eget Graviditetskort og Graviditetsplan. I fase 1 af projektet opbevares de to dokumenter dog i de centrale registre.

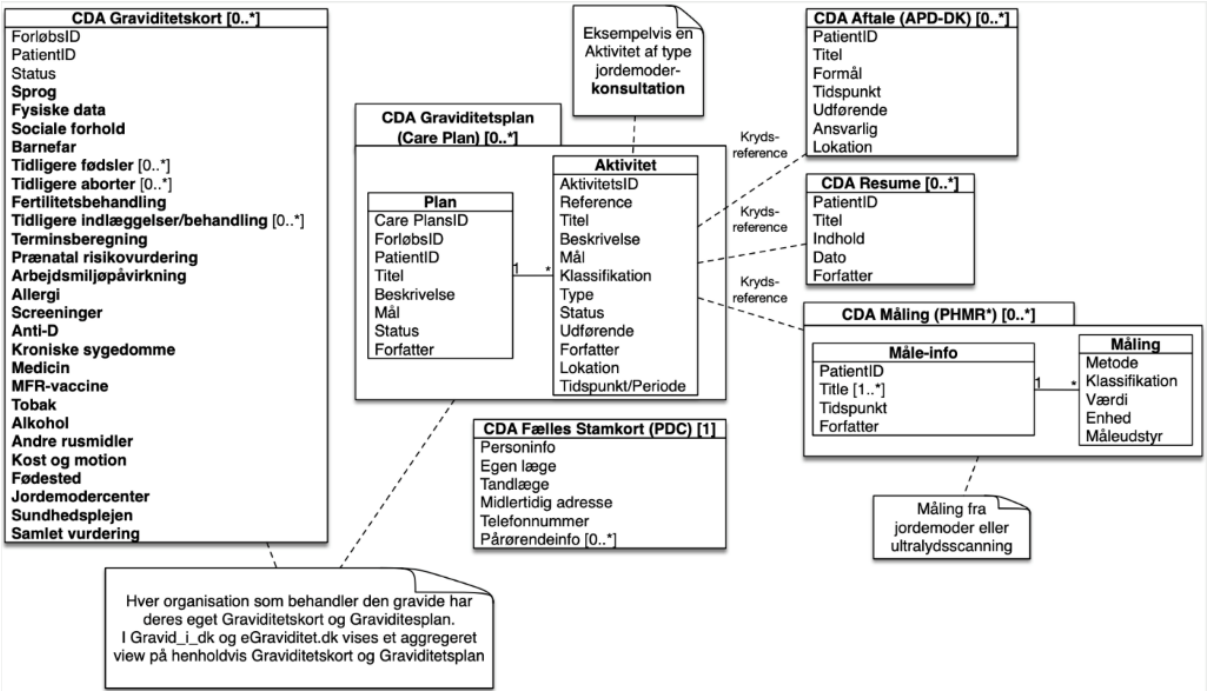
De enkelte instanser af Graviditetskort og Graviditetsplan aggregeres inden de vises i Gravid_i_DK og eGraviditet.dk, således af brugeren får det samlede overblik.

Aftale, Resume og Måling opbevares i ejerorganisationernes lokale repositories. Organisationer, der ikke har et lokalt repository eller som anvender eGraviditet.dk, opbevarer dokumenter i et nationalt repository.

I fase 1 anvendes den eksisterende nationale XDS infrastruktur, og Metadata for alle CDA dokumenter skal derfor registreres i det nationale Registry.

Det digitale graviditetsforløb er ikke en journal. De lokale systemer har fortsat journaliseringspligten, hvilket bevirker at al relevant dialog og registreringer i det digitale graviditetsforløb, som skal journaliseres – skal journaliseres i de lokale systemer. (den lokale journaliseringspligt ift. digitalt graviditetsforløb svarer til setup på Fælles Medicinkort).

På Figur 6 nedenfor illustrer det overordnede informationsindholdet i CDA dokumenterne fra Figur 5. Desuden er CDA dokumenternes multiplicitet for en gravid angivet.



Figur 6: Logisk view Informationsmodel

Før opstart af det digitale graviditetsforløb har den gravide kun et Fælles Stamkort. Efter opstart af det digitale graviditetsforløb har kvinden et Graviditetskort og en Graviditetsplan for hver involveret organisation (fx egen læge og region). Efterhånden som det digital graviditetsforløb gennemføres, oprettes der Aftaler for de konsultationer, der skal gennemføres. En gennemført konsultation kan resultere i, at Graviditetskortet og Graviditetsplanen opdateres, samt at der oprettes et Resumeer og/eller en Måling. Af selve Aftale CDA dokumentet kan det ikke aflæses, om Aftalen er gennemført, men denne information kan til gengæld sættes via Graviditetsplan Aktivitetens statusfelt.
Ligeledes kan man af statusfelter på Graviditetskort og Graviditetsplan via HL7 statuskoder angive og aflæse, om dokumenterne repræsenterer et aktivt, pauseret eller gennemført graviditetsforløb.

For yderligere information om de enkelte attributter i modellen henvises referencerne i tabellen ovenfor.

4. Applikationsarkitektur

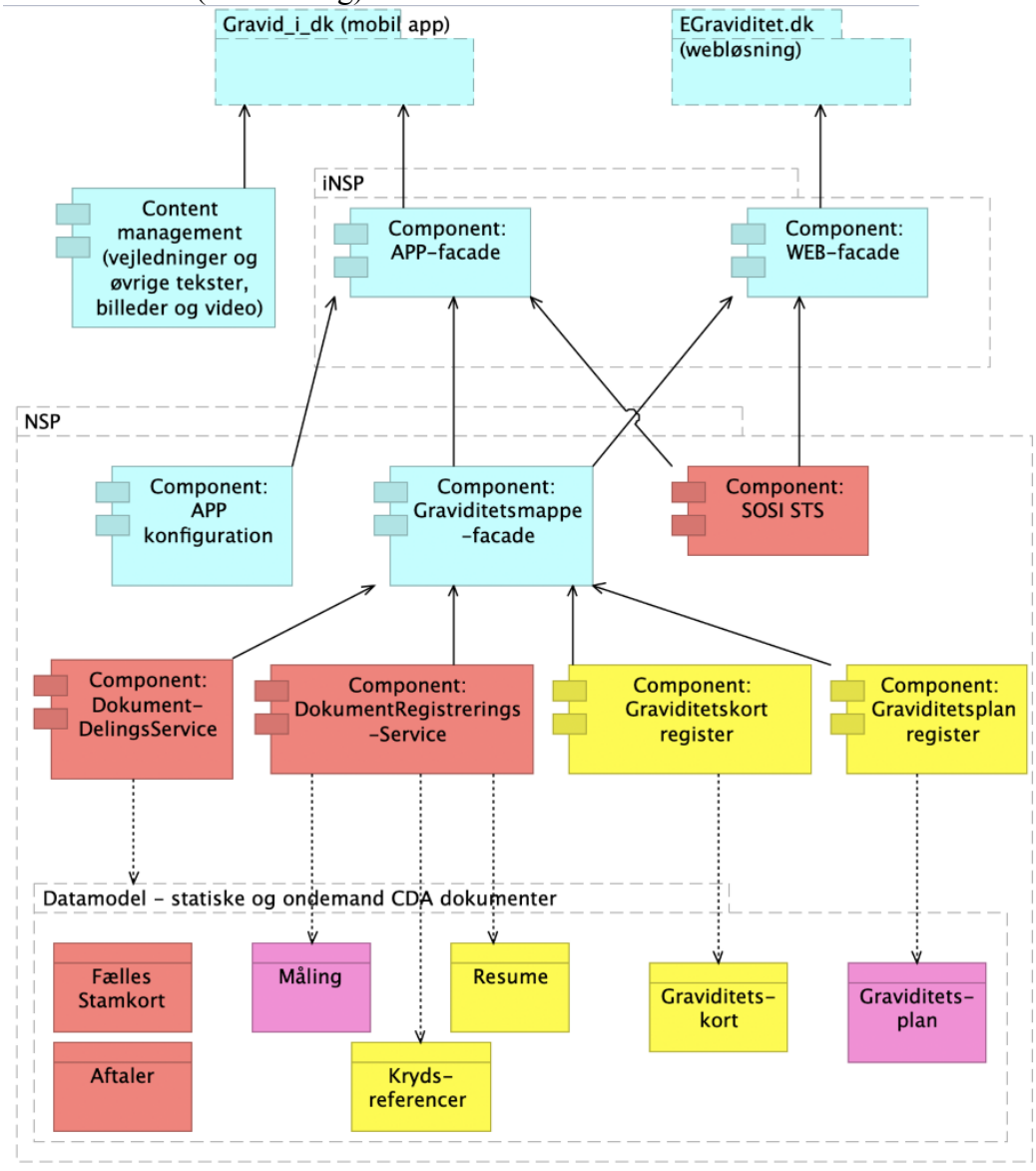
I afsnittet præsenteres applikationsarkitekturen via fire forskelle views:

1. Første view har fokus på, hvordan Gravid_i_DK og eGraviditet.dk læser og skriver til datamodellen

2. Andet view viser tre forskellige integrationsmodeller fra fagsystemer til det digitale graviditetsforløb
3. Tredje view har fokus på håndtering af remote notifikationer til borgerens mobile device
4. Fjerde view har fokus på arkivering og håndtering af digital post

4.1. View 1 – Gravid_i_DK- og eGraviditet.dk adgang til datamodel

Figur 7 nedenfor illustrerer den overordnede løsningsarkitektur for Gravid_i_DK (App) og eGraviditet.dk (webløsning).



Figur 7: Gravid_i_DK og eGraviditet.dk adgang til datamodel

Farvekoderne på figuren har følgende betydning:

- Rød: Eksisterende komponenter på NSP eller eksisterende danske HL7 CDA profiler.
- Gul: Komponenter under udvikling, der forventes tilgængelige medio 2020. Herunder HL7 CDA profiler under udvikling, der forventes afklaret medio 2020.

- Lilla: Graviditetsplan er en eksisterende profil, som skal sub-profileres til graviditetsplaner. Måling er en ny profil baseret på PHMR
- Lyseblå (Turkis): Nye komponenter og klienter.

4.1.1. Klient-laget

Øverst på figuren ses frontend klienterne:

- **Gravid_i_DK** (mobil App) målrettet den gravide og hendes behov for at skabe et overblik over eget graviditetsforløb. Der etableres understøttelse af IOS og Android mobilplatformen. Funktionalitet, som allerede ligger på borger.dk og sundhed.dk, implementeres ikke i fase 1. Borgeren henvises til de to portaler for håndtering af Digital fuldmagt, Fælles Stamkort, MinLog og MinSpærring. Sikkerhedsløsningen baseres på NemID og OpenId Connect.
- **eGraviditet.dk** er en browserbaseret webløsning målrettet de sundhedsfaglige. Fra eGraviditet.dk kan de sundhedsfaglige opstarte graviditetsforløb, justere graviditetsforløb, etablere visitationsgrundlag samt dele data fra de enkelte konsultationer og undersøgelser af den gravide (jf. use cases). eGraviditet.dk kan opstartes efter to modeller:
    - Fra et fagsystem via Sikker Browser Opstart. eGraviditet.dk opstartes via et eksternt system (fx et fagsystem) i en fastlåst patient- og brugerkontekst. Det eksterne system overfører brugerens eksisterende login-credentials til eGraviditet.dk, hvorved brugeren ikke skal lave login på ny. Fagsystemet overfører desuden information om den patientkontekst (det konkrete graviditetsforløb), som eGraviditet.dk skal opstartes med.
    - Som standalone-løsning med egen login og kontekstvalg. Fra standalone-løsningen kan den sundhedsfaglige lave NemLog-in, få tilknyttet sundhedsfaglig rolle, organisatorisk tilhørsforhold og udpege den gravide, hvis graviditetsforløb skal hentes og vises.

Sikkerhedsløsningerne til Gravid_i_DK og eGraviditet.dk er yderligere beskrevet i afsnittet ”Sikkerhedsarkitektur”.

På Figur 7 under Gravid_i_DK til venstre ses komponenten ”Content management”:

- **Content management** håndterer vejledninger målrettet den gravide og øvrige tekster, billeder og video, der skal indgå i Gravid_i_DK. Komponenten indeholder ikke følsomme informationer og forventes ikke placeret på iNSP- eller NSP-platformen. Komponenten skal udstille funktionalitet til effektiv indholdslevering over internettet samt funktionalitet til redigering og frigivelse af indhold.

4.1.2. iNSP-laget

iNSP er en ny platform i regi af NSP (den Nationale Service Platform), som er målrettet klienter på internettet. Dvs. mobile Apps og webløsninger.
iNSP-laget indeholder primært facade komponenter, som understøtter Gravid_i_DK og eGraviditet.dk, og deres behov for adgang til graviditetsdata hentet fra NSP laget. Oprindeligt var visionen at alle komponenter på iNSP-laget skulle holdes ”stateless”, og det dermed var klienternes (Gravid_i_DK og eGraviditet.dk) ansvar at holde session-state. Det har efterfølgende vist sig, at adgang via eGraviditet.dk og sikkerhedsprotokollen SBO (Sikker Browser Opstart) ikke fungere i et stateless setup. Der er derfor åbnet op for, at sundhedsfagliges adgangsgivende tokens kan gemmes i et sessionsobjekt på iNSP-laget.

iNSP komponenterne er:

- **App-facade**, som servicerer Gravid_i_DK med funktionalitet og data, og dermed er grundlaget for de skærmbilleder, den gravide tilgår via Gravid_i_DK.
    - Grænseflade: Baseres på REST og JSON og målrettes den specifikke App (Gravid_i_DK), der skal udvikles
    - Sikkerhedshåndtering: App-facaden validerer og omveksler det Access-token der modtages fra Gravid_i_DK. Omvekslingen sker for hvert kald til App-facaden via et omvekslingskald til SOSI-STS på NSP (mere herom i afsnit "Sikkerhedsarkitektur")
- **Web-facade,** som servicerer eGraviditet.dk med funktionalitet og data, og dermed danner grundlag for de skærmbilleder den sundhedsfaglige tilgår via eGraviditet.dk.
    - Grænseflade: Baseres på REST og JSON og målrettes den specifikke WEB-løsning, der skal udvikles
    - Sikkerhedshåndtering: Web-facaden validerer det audience-restricted OIOSAML token, der overføres fra klienten. Fra OIOSAML tokenet udtrækkes det indlejrede SOSI-ID kort, der skal anvendes i de videre kald til NSP-laget (mere herom i afsnit "Sikkerhedsarkitektur").

4.1.3. NSP-lag

Den Nationale Service Platform stiller national infrastruktur til rådighed for aktører på tværs af sundhedssektoren, som gør det muligt at anvende nationale registre og services direkte i patientbehandlingen ved at sikre den nødvendige tilgængelighed og driftsstabilitet.

Følgende komponenter eksisterer allerede på NSP:

- **DokumentDelingsService (DDS)**: Alt graviditetsdata fremsøges (ITI-18 Registry Stored Query) og hentes (ITI-43 Retrieve Dokument Set) som CDA dokumenter via DDS.
    - Grænseflade: IHE ITI, dog indpakket i DGWS
    - Sikkerhedshåndtering: DGWS med SOSI Idkort niveau 4[5]
- **SOSI-STS**: STS (Security Token Service) som står for omveksling til de sikkerhedstokens (SOSI-IDkort, IDWS-token og JSON Web Token), der anvendes når sundhedsfaglige og borgere skal tilgå services på NSP
- **DokumentRegistreringsService**: Service, som udstiller en "IHE ITI-41 Provide and Register", der anvendes når CDA dokumenter for Målinger, Resuméer og Aftaler registreres i det nationale Registry og persisteres i et nationalt Repository. Denne services forventes også anvendt til registrering af Krydsreferencer.
  NB: National XDS Registry tilgås direkte med "ITI-42 Register Document Set", når persisteringen håndteres i et lokalt repository, og det derved kun er metadata, der skal registreres i det nationale Registry.
    - Grænseflade: IHE ITI, dog indpakket i DGWS
    - Sikkerhedshåndtering: DGWS med SOSI Idkort niveau 3[6] eller 4

Følgende komponenter skal etableres i regi af projektet:

- **App-konfiguration,** som giver læse- og skriveadgang til konfigurationsdata. Fra Gravid_i_DK modtages forskelligt konfigurationsdata pr. bruger. Eksempelvis:

[5] Dvs. et SOSI IdKort baseret på et medarbejder-certifikat
[6] Dvs. et SOSI IdKort baseret på et funktions-certifikat (system-certifikat)

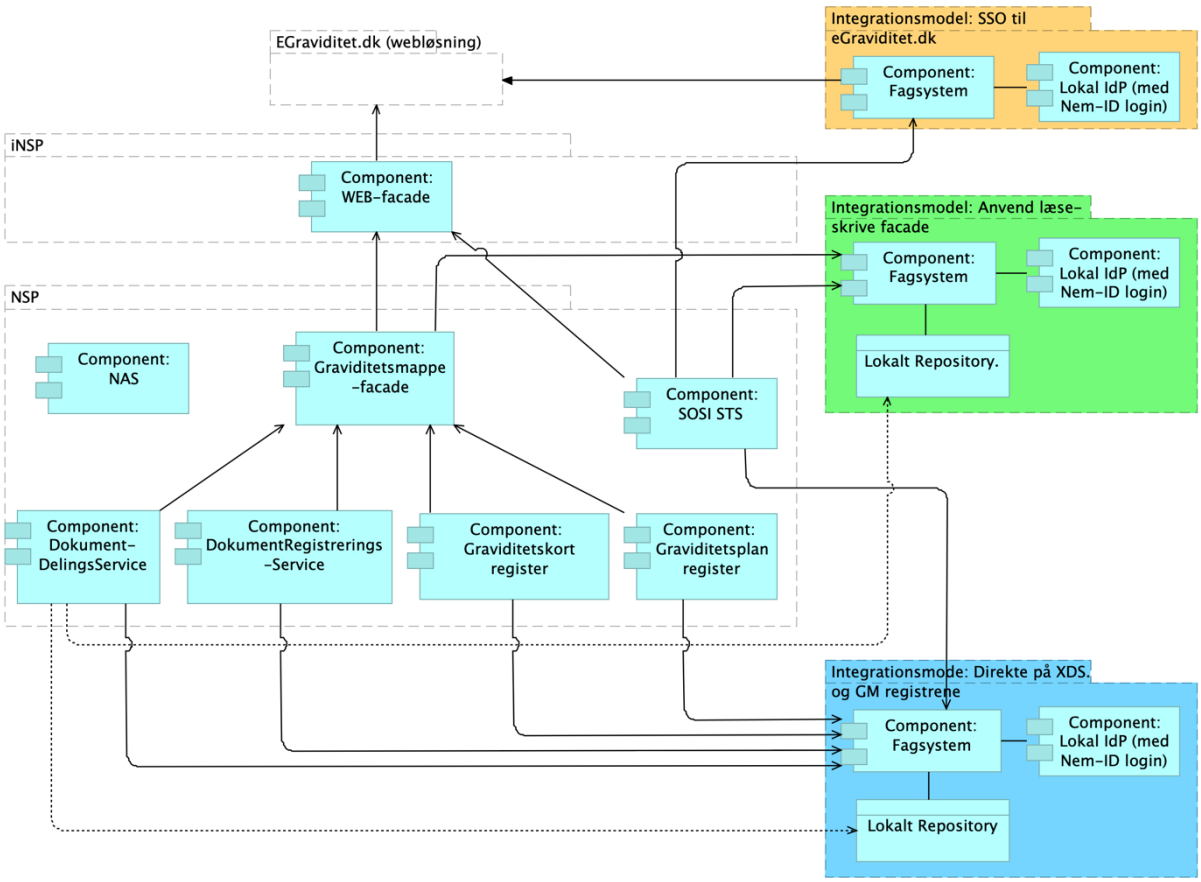
    - Identifikation af brugerens App og device, og som skal anvendes i forbindelse med udsending af remote notifikationer.
    - Diverse valg som brugeren opsætter i App-indstillingerne.

  Det komplette sæt af konfigurationsbehov er ikke afdækket og det forventes at en del af behovene først identificeres i forbindelse med udviklingsprocessen.
    - Grænseflade: Webservice/XML
    - Sikkerhedshåndtering: DGWS med SOSI IDkort niveau 3 eller 4
- **Graviditetsmappe-facade**, som udstiller en ensartet og sammenhængende "letvægts" grænseflade målrettet læsning og skrivning af graviditetsdata. Dvs. det indkapsles, at graviditetsdata udtrækkes som en række CDA dokumenter (se afsnit "Informationsarkitektur") via den nationale XDS infrastruktur (DokumentDelingsServicen), samt at graviditetsdata indlæses via forskellige formater og grænseflader. Opsætning af korrekte Krydsreferencer (se afsnit "Informationsarkitektur") mellem dokumenterne håndteres også af komponenten. Grænsefladen designes til at løse behovene fra Gravid_i_DK og eGraviditet.dk efter et generisk koncept. Andre klienter (fx fagsystemer eller andre App's) kan anvende græsefladen frem for at tilgå XDS infrastrukturen mm. direkte, hvis dette findes fordelagtigt. Der planlægges med en proces, hvor interessenter kan få indblik og indflydelse på grænsefladen i samarbejde med leverandøren.
    - Grænseflade: Webservice/XML, gerne bygget over en FHIR[7] model
    - Sikkerhedshåndtering: DGWS med SOSI IDkort niveau 4, samt niveau 3 til interne jobs.
- **Graviditetskort-registeret**: Anvendes til at oprette og opdatere et Graviditetskort. Etableres af leverandøren af Graviditetsmappen.
    - Grænseflade: Webservice/XML.
    - Sikkerhedshåndtering: DGWS med SOSI IDkort niveau 4.
- **Graviditetsplan-registeret**: Anvendes til at oprette og opdatere en graviditets-care-plan. Etableres af leverandøren af Graviditetsmappen.
    - Grænseflade: Webservice/XML.
    - Sikkerhedshåndtering: DGWS med SOSI IDkort niveau 4.

4.2. View 2 – Integrationsmodeller for fagsystemer

Figur 8 nedenfor illustrerer 3 integrationsmodeller, der kan anvendes fra et fagsystem.

[7] DGWS er et ufravigeligt krav for services udstillet via NSP, og derfor er en **ren** REST-baseret FHIR grænsefalde ikke tilladt



Figur 8: 3 integrationsmodeller fra fagsystemer til det Digitale Graviditetsforløb

Integrationsmodellerne er:

1) **SSO til eGraviditet.dk**: eGraviditet.dk opstartes fra fagsystem i en kontekstlåst sammenhæng (Sikker browser opstart). Herved kan der gives adgang til graviditetsdata for sundhedsfaglige, der har fagsystemer, hvor der ikke er lavet en dyb integration til graviditetsmappen.
2) **Anvend Graviditetsmappe-facade**: Fagsystemet kan hente og skrive graviditetsdata via facadens ensartede og sammenhængende "letvægts" grænseflade. De statiske CDA dokumenter (Aftale, Måling og Resume) kan persisteres i et lokalt repository. XDS metadata registreres i det nationale registry.
3) **Direkte på XDS og registrene**. Fagsystemet tilgår DokumentDelingsServicen, DokumentRegistreringsservicen, Graviditetskort- og Graviditetsplan-registeret direkte. De statiske CDA dokumenter (Aftale, Måling og Resume) kan persisteres i et lokalt repository. XDS metadata registreres i det nationale registry. Håndtering af Krydsreferencer via denne integrationsmodel afventer, at det besluttes hvordan Krydsreferencer realiseres.

For alle integrationsmodeller gælder, at login kan håndteres via en lokal IdP, der understøtter Nem-id (og på sigt MitID). Sikkerhedstokenet skal omveksles til et SOSI Idkort eller IDWS-token via SOSI-STS.

Komponenten NAS (National AdviseringsService), er medtaget på Figur 8, da fagsystemerne kan abonnere NAS advis, og derigennem modtage advis når graviditetsforløb oprettes, afsluttes mm.

Lokale App's (fx mitSygehus) skal selv udvikle en App-backend, og denne kan tilgå graviditetsdata via integrationsmodel 2 eller 3.

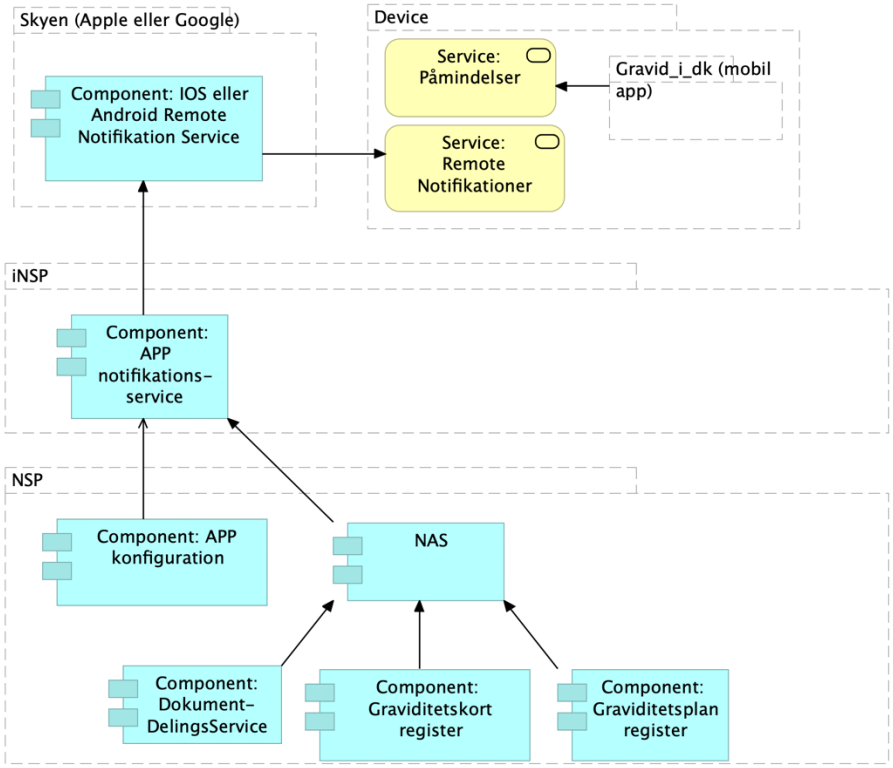
4.3. View. 3 – Notifikationer til borgerens mobile device

NB: Det er besluttet at udskyde App-notifikationer til en senere fase, da der er en række udfordringer: 1) konceptet skal sammentænkes med øvrige notifikationer, der udsendes fra sundhedsvæsenet 2) Det vil være et ukomplet billede af notifikationer, da DDS ikke udsender notifikationer ved oprettelse/ændring af dokumenter

Der skelnes mellem "lokale notifikationer" og "remote notifikationer", hvor de sidste også omtales som push notifikationer:

- **Lokale notifikationer** opsættes af Gravid_i_DK på mobiltelefonens operativsystem og kan notificere brugeren. Det er fx muligt at opsætte en lokal notifikation, som skal vises på et bestemt tidspunkt, med det formål at huske den gravide på en bestemt aftale.
- **Remote notifikationer** aktiveres fra backend systemet i forbindelse med forskellige hændelser. Det er fx muligt at sende en remote notifikation fra backend systemet, hvis der tilføjes en aktivitet til den gravides Graviditetsplan.

Sammenhængen mellem graviditetsforløb og det device, som skal modtage en notifikation, registreres, når Gravid_i_DK downloades og aktiveres til et aktuelt graviditetsforløb. Informationen persisteres via "App-konfiguration" komponenten på Figur 7.
Figur 9 nedenfor illustrerer den overordnede løsningsarkitektur for håndtering af lokale og remote notifikationer.



Figur 9: Håndtering af lokale og remote notifikationer

4.3.1. Lokale notifikationer

Lokale notifikationer håndteres udelukkende af Gravid_i_DK og device (mobiltelefonen). Når den gravide åbner Gravid_i_DK, hentes hendes aktuelle data fra DokumentDelingsServicen via backendsystemerne (se Figur 7). Dele af data vedrører opgaver, som den gravide forventes at udføre på bestemte dage eller tidspunkter. Eksempler herpå kan være at møde op til en konsultation med jordemoder eller forberede sig ved at læse en vejledning. Gravid_i_DK kan ud fra disse data, og med den gravides accept, opsætte lokale notifikationer, som skal påminde den gravide om disse emner (se pilen fra Gravid_i_DK til Påmindelser på Figur 9).
Bemærk: når de lokale notifikationer er opsat på den gravides device og når den gravide har lukket Gravid_i_DK, kan der ikke gennemføres opdateringer til de lokale notifikationer. Dvs. hvis fx en region flytter den aftale, som den lokale notifikation vedrører, vil den gravide stadig få den lokale notifikation vedrørende aftalen. Først når den gravide åbner Gravid_i_DK og data indlæses fra backendsystemerne, vil Gravid_i_DK kunne se, at aftalen er flyttet.

4.3.2. Remote notifikationer

Remote notifikationer opstår på NSP systemerne og formidles via den Nationale AdviseringsService (NAS). På Figur 9 er der vist tre kilder til advis:

1. Advis fra DDS Registry, når nye CDA dokumenter registreres. Fx nye dokumenter indenfor et graviditetsforløb (aftaler, målinger, resuméer). Advis via DDS Registry har været afprøvet[8], men er endnu ikke realiseret.
2. Advis fra Graviditetskort-registret. Advis sendes ved tilstandsskifte i registeret. Fx "Graviditetsforløb afsluttet".
3. Advis fra Graviditetsplan-registret. Advis sendes ved tilstandsskifte i registret. Fx når nye aktiviteter oprettes.

NAS sørger for, at advis'erne formidles til de klienter, der abonnerer på de rette "advis topics".

På Figur 9 er "App-notifikationsservice" en ny komponent, som abonnerer på NAS og reagerer på advis'er, der skal formidles til den gravides device (mobiltelefon). Via komponenten "App-konfiguration" hentes information om de devices, der er tilknyttet et graviditetsforløb, og dermed skal modtage notifikationerne. "App-notifikationsservice" videresender advis'en, som en remote notifikation, til en IOS eller Android notifikationsservice, der ligger i skyen og ejes af Apple eller Google. Den gravides device tjekker med en fastlagt frekvens (flere gange i timen), om der ligger en notifikation i IOS eller Android notifikationsservicen. Ligger der en notifikation, vises denne til den gravide på device'et.

"App-notifikationsservice" renser notifikationerne for følsom information inden de formidles via de skybaserede kanaler uden for Sundhedsdatastyrelsens kontrol, og som ejes af Apple eller Google. Det udestår at finde det rette niveau for, hvilke NAS advis'er, der skal formidles

[8] I regi af PRO projektet blev IHE DSUB teknologien afprøvet. Konklusionen var, at OpenText (den eksisterende repository leverandør) DSUB implementeringen har en række uhensigtsmæssigheder og kan derfor ikke anbefales. PRO-projektet anbefaler at der bør anskaffes/udvikles og testes en anden implementering af DSUB NotificationBroker

til borgerens device, samt hvordan notifikationerne kan formidles i "ikke følsomme" formuleringer.

"App-notifikationsservice" er på Figur 9 placeret i iNSP-laget. Det skal overvejes om komponenten skal flyttes ned i NSP-laget af performance hensyn, så den herved får direkte adgang til konfigurations-data.

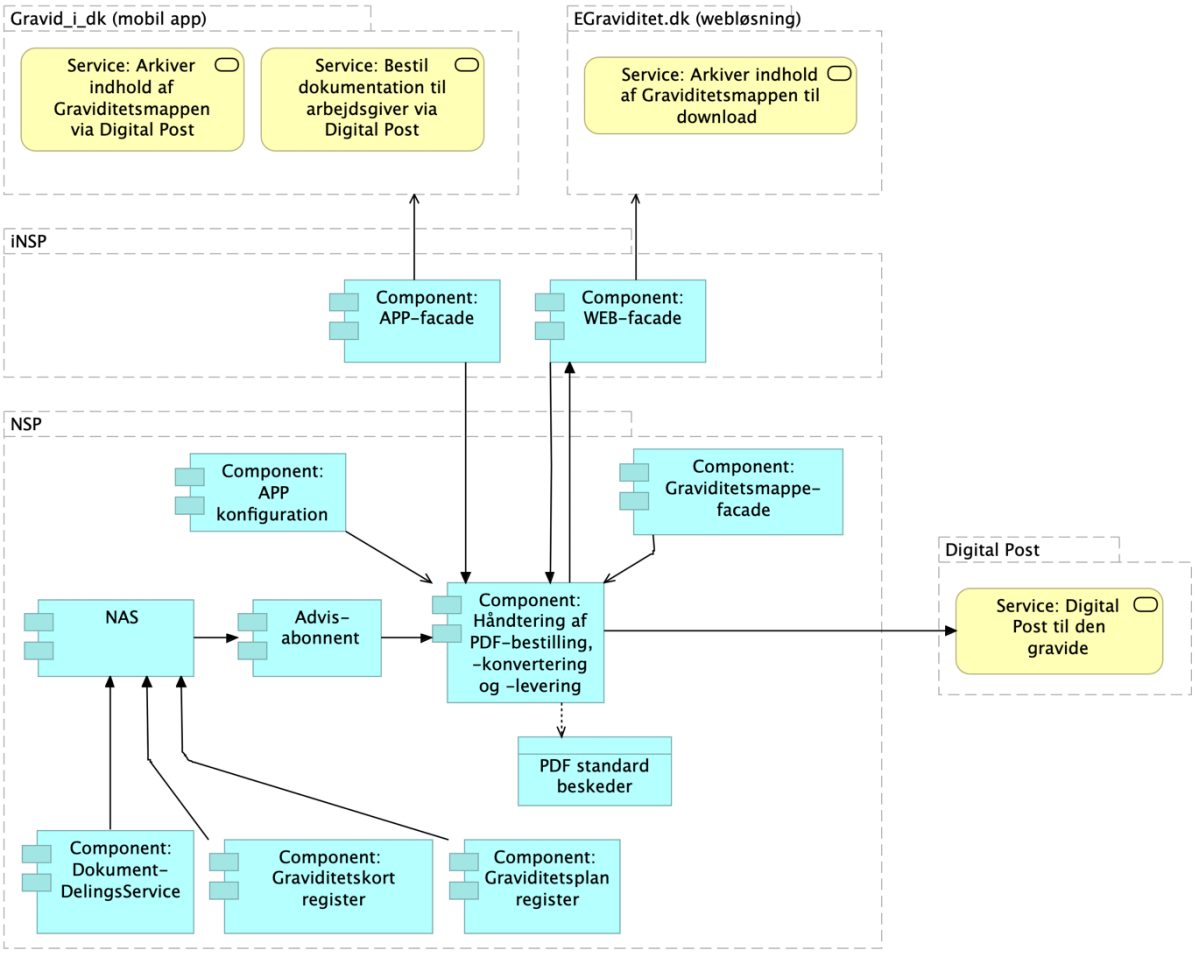
4.4. View 4 – Håndtering af arkivering og digital post

I afsnittet "Opgavearkitektur" beskrives fire hændelser, der skal medføre, at der sendes en besked via digital post til den gravide:

- Ved initiering af et Graviditetsforløb sendes automatisk en App-brugervejledning via Digital Post
- Ved afsluttet graviditet udleveres den gravides graviditetsdata automatisk som PDF via Digital Post. Brugeren kan via App-indstillingerne fravælge denne automatiske udlevering.
- Den gravide kan via Gravid_i_DK bestille "Dokumentation til arbejdsgiver", som anvendes til at dokumenterer graviditeten overfor arbejdsgiver. "Dokumentations til arbejdsgiver" leveres som et PDF-dokument via Digital post.
- Den gravide kan via Gravid_i_DK og efter behov bestille graviditetsdata udleveret, som et PDF-dokument, via Digital Post.

Desuden skal den sundhedsfaglige, via eGraviditet.dk, kunne downloade graviditetsforløbet som PDF med henblik på arkivering i lokalt fagsystem.

Figur 10 nedenfor illustrerer den overordnede løsningsarkitektur for håndtering af arkivering og Digital Post.



Figur 10: Håndtering af PDF-bestilling, - og Digital Post

På Figur 10 introduceres følgende 2 nye komponenter:

- **Advis-abonnent:** Komponenten abonnerer på udvalgte advis-topics fra NAS. Eksempler på udvalgte advis er ”Initiering af graviditetsforløb” og ”Afslutning af graviditetsforløb”, som udsendes fra Graviditetskort-registeret og formidles via NAS. ”Initiering af graviditetsforløb” advis’et skal resultere i, at der sendes en App-brugervejledning til Borgeren via Digital Post. ”Afslutning af graviditetsforløb” advis’et skal resultere i, at der genereres en PDF med den gravides graviditetsdata, som sendes via digital post.
- **Håndtering af PDF-bestilling, -konvertering og -levering:** Komponenten forventes realiseret via flere delkomponenter og det er leverandørens opgave at udfolde dette. Komponentens opgave er at håndtere PDF bestillinger, at hente eller oprette de PDF-dokumenter der bestilles, samt at levere PDF-dokumenterne via download eller Digital Post.

  1) Komponenten kan modtage PDF bestillinger fra:
  - Advis abonnement komponenten (ved initialisering og afslutning af graviditetsforløbet)
  - App-facaden (den gravides bestilling af “Dokumentation til arbejdsgiver” eller PDF med alt graviditetsdata)
  - Web facaden (den sundhedsfagliges bestilling af PDF med alt graviditetsdata)

2) Komponenten kan hente data fra:
   - App-konfiguration (herfra kan det aflæses, om den gravide har fravalgt automatisk forsendelsen af graviditetsdata).
   - Graviditetsmappe-facade (herfra kan graviditetsdata udlæses).
   - Statiske PDF-dokumenter (folder med statiske PDF-dokumenter, der skal sendes i forbindelse med initiering af et graviditetsforløb)
3) Komponenten skal konvertere hentet graviditetsdata til PDF-dokument
   - PDF-dokument med "Dokumentation til arbejdsgiver"
   - PDF-dokument med alt graviditetsdata
4) Komponenten skal levere bestillingen via
   - Digital Post (til den gravide)
   - Download (til den sundhedsfaglige)

I designet af ovenstående skal det sikres, at brugeren kun får adgang til data, som brugeren retmæssig har adgang til. Eksempelvis skal en sundhedsfaglig ikke kunne bestille et PDF-dokument, som indeholder data, som borgeren har spærret via MinSpærring.
For bestillinger, der aktiveres af en bruger (borger eller sundhedsfaglige) sikres dette ved at medsende brugers sikkerhedstoken (SOSI IdKort niveau 4 for sundhedsfaglige eller OIO-IDWS for borgere) når Graviditetsmappe-facade kaldes.

Bestillinger, der aktiveres af systemet (Advis-abonnent komponenten), laves på vegne af den gravide og resulterer i, at der sendes data til den gravides Digital Post. I disse tilfælde medsendes et SOSI IdKort niveau 3 (IdKort baseret på et system-certifikat). Samtidig skal der konfigureres en trustadgang hos DokumentDelingServicen (DDS), der er det backendsystem, der udtrækker data. DDS kræver desuden, at der medsendes en HSUID-header, hvor på-vegne-af kaldet er nærmere specificeret.

5. Sikkerhedsarkitektur

Brugerne af henholdsvis Gravid_i_DK og eGraviditet.dk skal kunne autentificeres og autoriseres i forhold til den rolle, de har.
Brugen af Gravid_i_DK er tiltænkt borgere, og brugen af eGraviditet.dk er tiltænkt de sundhedsfaglige.

5.1. Sikkerhedsløsning for borgere

Der arbejdes med to modeller vedr. login til Gravid_i_DK:

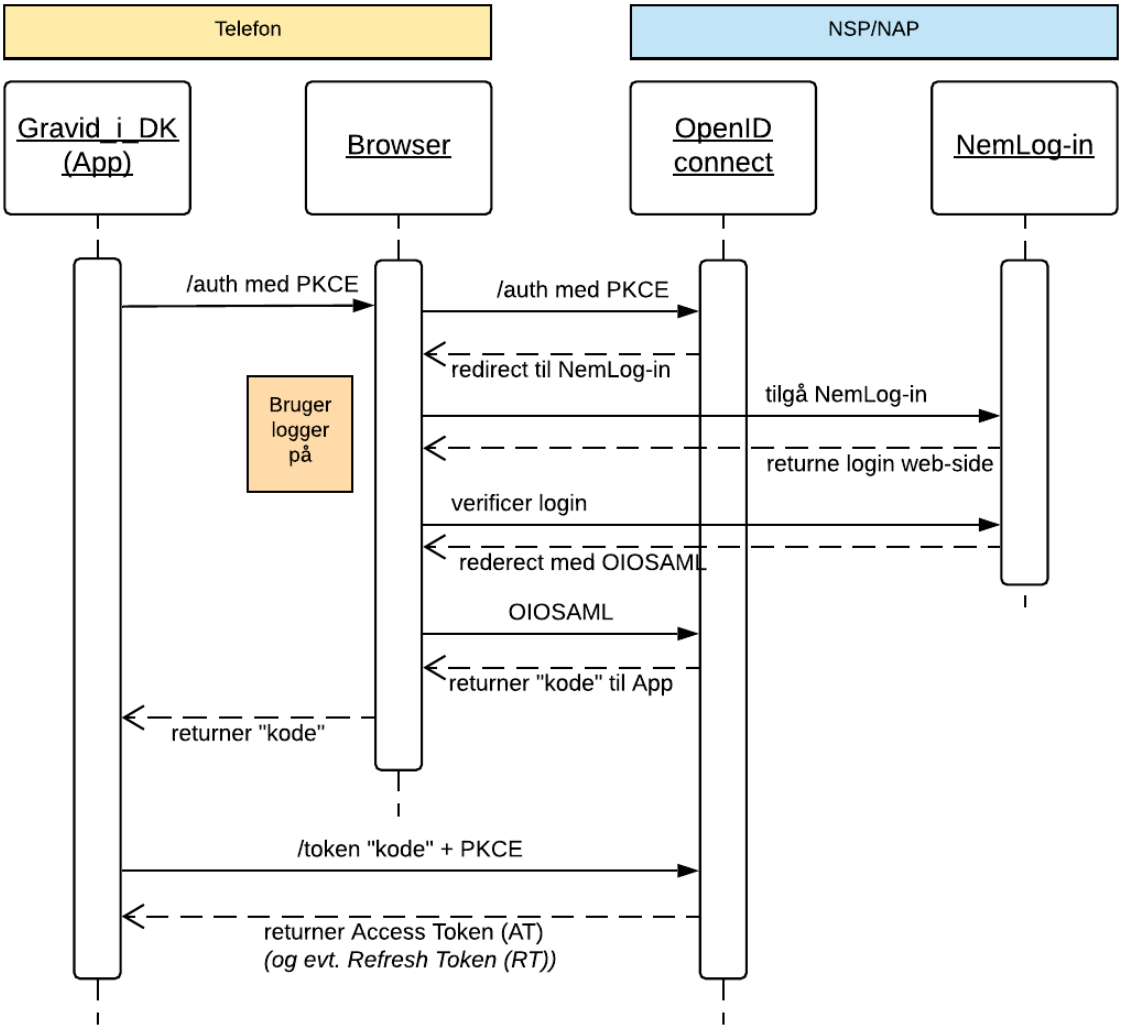
- Model Basal, hvor brugeren autentificeres via NemLog-in hver gang en Gravid_i_DK opstartes.
- Model Udvidet, hvor brugeren autentificeres med NemLog-in første gang Gravid_i_DK opstartes. Herefter kan brugeren anvende pinkode, fingerscan eller ansigtsgenkendelse ved de efterfølgende opstart af Gravid_i_DK.

Model Udvidet er en overbygning på model Basal. I begge modeller håndteres brugerautentifikation via NemLog-in. NemLog-in kommer, modsat Nem-ID, til at understøtte det kommende MitID, og er dermed fremtidssikret.

NemLog-in skal anvendes med såkaldt "SAML force autentification", hvorved det sikres, at brugeren altid skal autentificere sig ved NemLog-in, og dermed ikke kan anvende automatisk login på baggrund af en eksisterende single-sign-on session med NemLog-in.

OpenId connect anvendes til udstedelse af et Acces Token, som kan anvendes når Gravid_i_DK tilgår GraviditetsData. I forbindelse med tidligere afprøvning på medicinkort-app'en, blev det besluttet at benytte OpenID Connect's såkaldte "code flow" med brug af PKCE ("Proof Key for Code Exchange" https://tools.ietf.org/html/rfc7636) i overensstemmelse med OAuth 2.0 for Native Apps (https://tools.ietf.org/html/rfc8252).

Sekvensdiagrammet på Figur 11Figur 11: OpenID Connect sekvensdiagram viser hvorledes et OpenID Connect flow fungerer med direkte brug af NemLog-in.



Figur 11: OpenID Connect sekvensdiagram

Sekvensdiagrammet afsluttes med, at der returneres et Acces Token (AT) og eventuelt et Refresh Token (RT) til Gravid_i_DK. Refresh tokenet returneres kun i Model Udvidet, hvor brugeren kan anvende pinkode, fingerscan eller ansigtsgenkendelse ved de efterfølgende opstart af Gravid_i_DK.

Access Token (AT) og Refresh Token (RT) har hver især en begrænset levetid, som kan konfigureres i OpenID Connect serveren. Typisk vil AT have en levetid der svarer til en brugersession – fx 20 minutter. Når Gravid_i_DK's AT er udløbet, benytter Gravid_i_DK (i model Udvidet) RT til at omveksle til et nyt AT. Derved vil RT normalt have en noget længere levetid end AT. For at give brugeren mulighed for at åbne Gravid_i_DK uden at skulle logge ind igen med Nem-ID, bør der gives en tilstrækkelig lang levetid til RT; fx på 1-3 måneder. Dermed vil brugeren kunne genoptage sessionen uden at skulle re-autentificere sig med Nem-ID inden for denne periode.

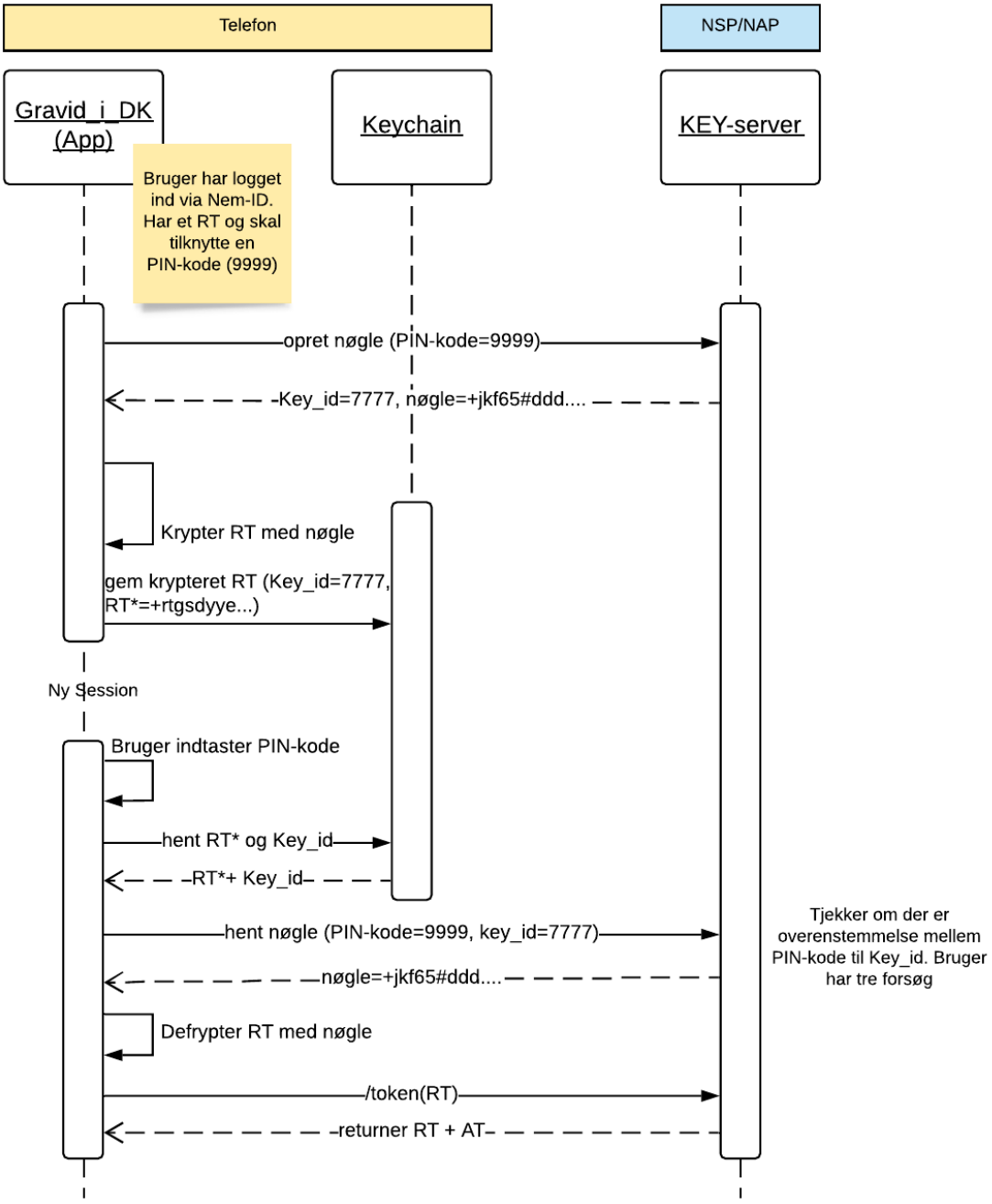
Acces tokenet skal være "sender-constrained" (jf. afsnit 2.2 og 4.8.1.1.2 i https://tools.ietf.org/html/draft-ietf-oauth-security-topics-15) som sikkerhedsforanstaltning mod Replay angreb.

5.1.1. Beskyttelse af refresh tokens (Kun relevant for model Udvidet)

Følgende er kun relevant for Model Udvidet, hvor borgeren kan anvende pinkode, fingerscan eller ansigtsgenkendelse ved efterfølgende opstart af Gravid_i_DK.

I forbindelse med at borgeren ikke skal logge ind med Nem-ID, hver gang Gravid_i_DK åbnes, er det nødvendigt at beskytte det cache'ede refresh token på devicet (mobiltelefonen).

Sekvensdiagrammet på Figur 12 illustrerer, hvordan Refresh tokenet kunne beskyttes via en Key-server.



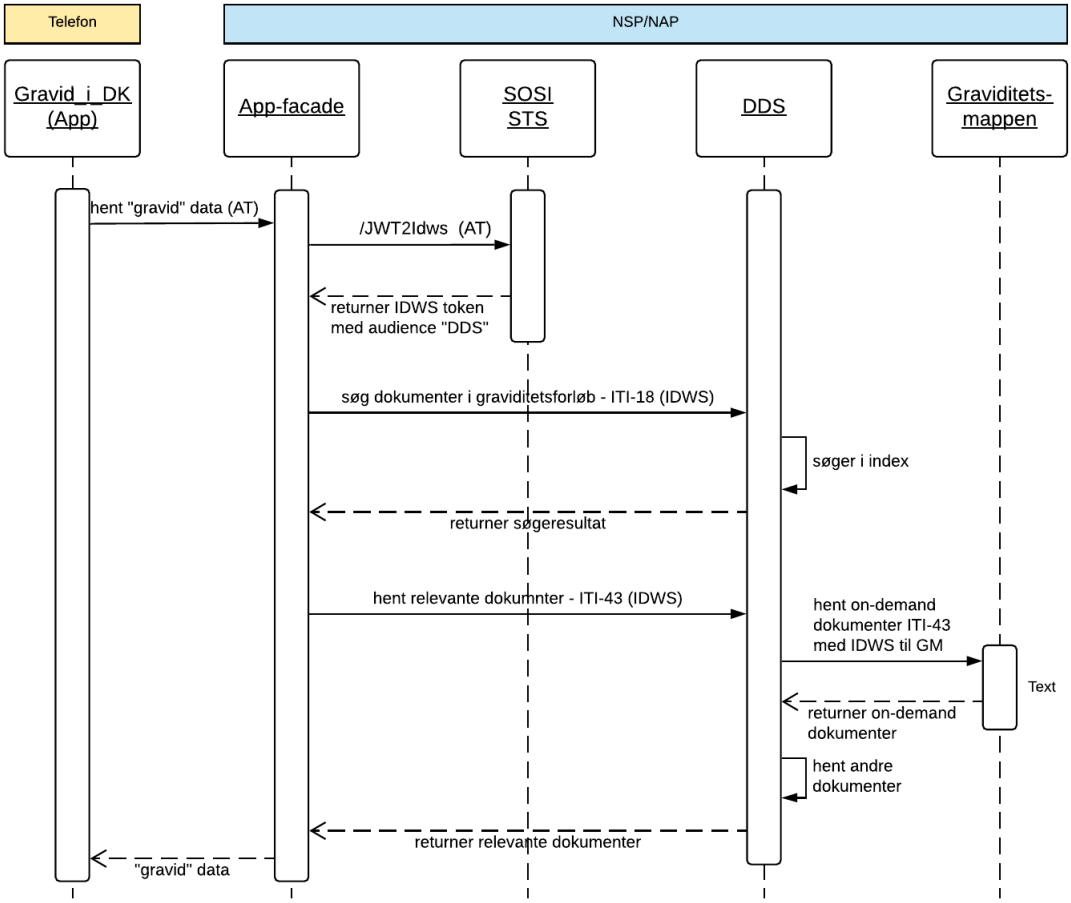
Figur 12: Beskyttelse af refresh token

Key-servicen sikre, at brugeren skal benytte PIN kode (fingerscan eller ansigtsgenkendelse) for at aktivere Refresh tokenet, og samtidig beskyttes der mod offline angreb, hvor forsøg på at gætte PIN koden udføres.

5.1.2. Adgang til Graviditetsmappen for borgere

Når først borgeren er logget ind i Gravid_i_DK, kan data om graviditeten hentes og blive præsenteret. Infrastrukturen på NSP/iNSP understøtter ikke Access Tokens (i JSON Web Token format - JWT), og disse skal derfor omveksles før Gravid_i_DK kan få adgang til data.

Sekvensdiagrammet på Figur 13 viser, hvorledes et Access Token fra Gravid_i_DK kan omveksles til et OIO-IDWS token og derved give adgang til data om den gravide gennem DokumentDelingsServicen. Omvekslingen laves for hvert kald fra Gravid_i_DK, der skal resultere i at App-facaden tilgår NSP komponenterne.



Figur 13: Sekvensdiagram vedrørende token omveksling

NB: I ovenstående sekvensdiagram eksisterer 2 udfordringer, som SDS skal finde en løsning på:
1) OIOIDWS tokenet er i princippet låst til kommunikation mellem App-facade og DDS, og kan derfor i princippet ikke anvendes til viderekald mellem DDS og graviditetsmappen.
2) Et fuldmagts claim kan ikke videredelegeres, hvis DDS laver en STS-omveksling med henblik på at få et OIOIDWS token, der matcher kommunikationen mellem DDS og Graviditetsmappen.

5.1.3. Sessioner og personfølsom data i Gravid_i_DK

Gravid_i_DK skal slette alle personfølsomme data når brugeren er inaktiv, men stadig har Gravid_i_DK åben. Pr. konfiguration skal der kunne opsættes en timeout-periode, som specificerer hvor lang tid brugeren må være inaktiv. Overskrides timeout-perioden, så skal Gravid_i_DK slette alle personfølsomme data og kræve, at brugeren re-autentificerer sig.

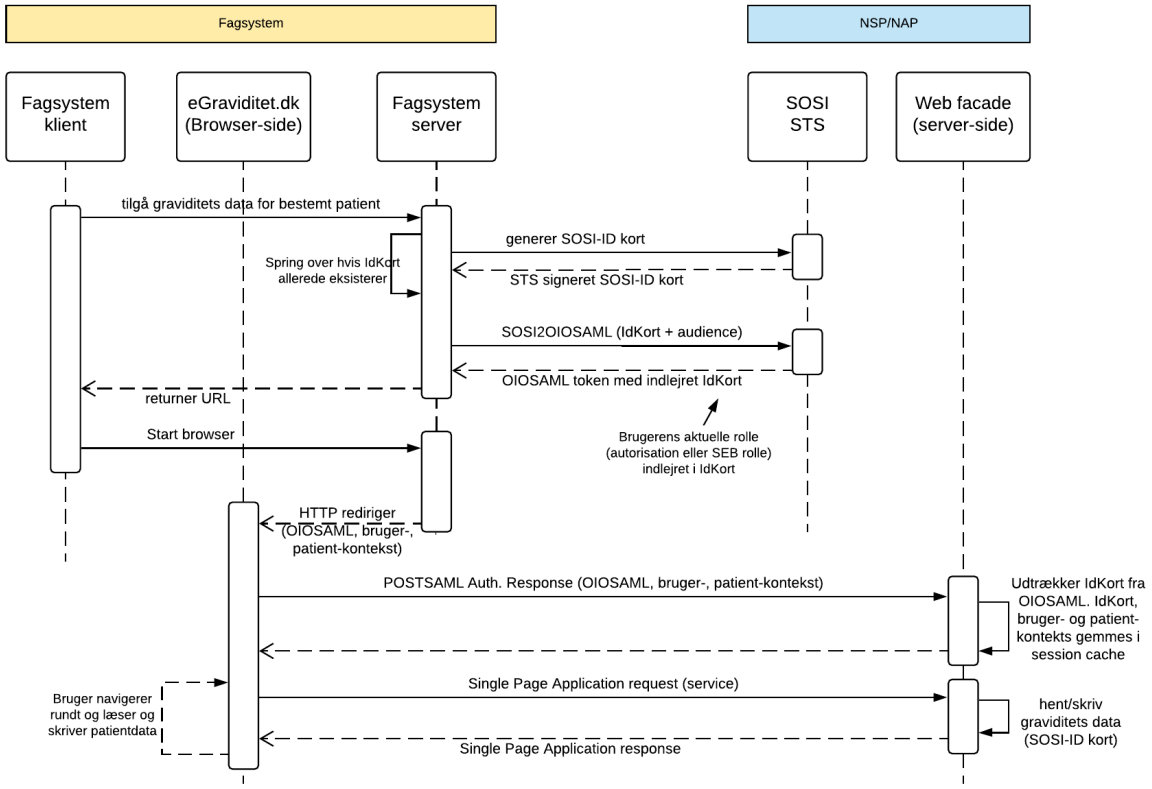
5.2. Sikkerhedsløsning for sundhedsfaglige

Den sundhedsfaglige kan enten tilgå eGraviditet.dk som en "Knap" løsning fra et fagsystem via Sikker Browser Opstart (SBO), eller som en Standalone løsning. De to modeller beskrives i det følgende.

5.2.1. Sikker Browser Opstart (SBO)

Ved SBO opstartes eGraviditet.dk via et eksternt fagsystem i en fastlåst patient- og brugerkontekst. Fagsystemet overfører brugerens eksisterende login-credentials til eGraviditet.dk, hvorved brugeren ikke skal lave login på ny. Fagsystemet overfører desuden information om den kontekst, som eGraviditet.dk skal opstartes med. Et eksempel på dette er patient_id for patienten, som brugeren ønsker at se graviditetsdata på, samt SOR-ID for den afdeling, hvor brugeren er ansat.
eGraviditet.dk er låst til den overførte bruger- og patient-kontekst. Dvs. brugeren må og kan ikke skifte patient- eller brugerkontekst via eGraviditet.dk. Hvis der skal skiftes kontekst, så skal eGraviditet.dk opstartes på ny fra fagsystemet.

Sekvensdiagrammet på Figur 14 viser hvorledes den sundhedsfaglige får åbnet en browser via sit fagsystem, og derved får adgang til data om den gravide. Flowet startes ved at den sundhedsfaglige har aktiveret "knappen" til graviditetsmappen i fagsystemet.
Fagsystem genererer først et SOSI IDkort via SOSI STS, med mindre IDkortet allerede eksisterer i fagsystemet. SOSI IDkortet er oprettet med den brugerkontekst (rolle), som den sundhedsfaglige arbejder under på det pågældende tidspunkt. Efterfølgende omveksles IDkortet til en OIOSAML billet med indlejret Idkort. OIOSAML billetten er anvendelsesmæssigt låst (audience-restricted) til Web-facaden.
eGraviditet.dk opstartes via et http-redirect fra Fagsystem-serveren, hvor OIOSAML billet, bruger- og patient-kontekst medsendes. Browseren redirectes til Web-Facaden. Web-facaden udtrækker IDkortet fra OIOSAML billetten, og gemmer IDkort samt bruger- og patient-kontekst i et sessionsobjekt. Web-facaden udfører den ønskede forretningsfunktion og returnere data. Ved efterfølgende kald fra eGraviditet.dk til Web-facade benyttes den etablerede session, som også opbevarer IdKortet. IdKortet medsendes ved kald til de bagvedliggende forretningskomponenter på NSP'en.



Figur 14: Sekvensdiagram for sikkehedsløsning i SBO eGraviditet.dk

5.2.2. Standalone

Den primære forskel mellem Standalone og SBO sikkerhedsløsningen er den indledende fase, hvor login-credentials, bruger- og patientkontekst oprettes. Ved SBO overlades dette til fagsystemet, hvorimod Standalone løsningen selv står for oprettelsen.

Sekvensdiagrammet på Figur 15 viser hvorledes den sundhedsfaglige autentificerer sig mod SEB-IdP (Sundhedsvæsenets Elektroniske Brugerstyring IdentityProvider), vælger bruger- og patient-kontekst, og derved får adgang til data om den gravide. Flowet startes ved, at den sundhedsfaglige tilgår Standalone løsningens URL via en browser.

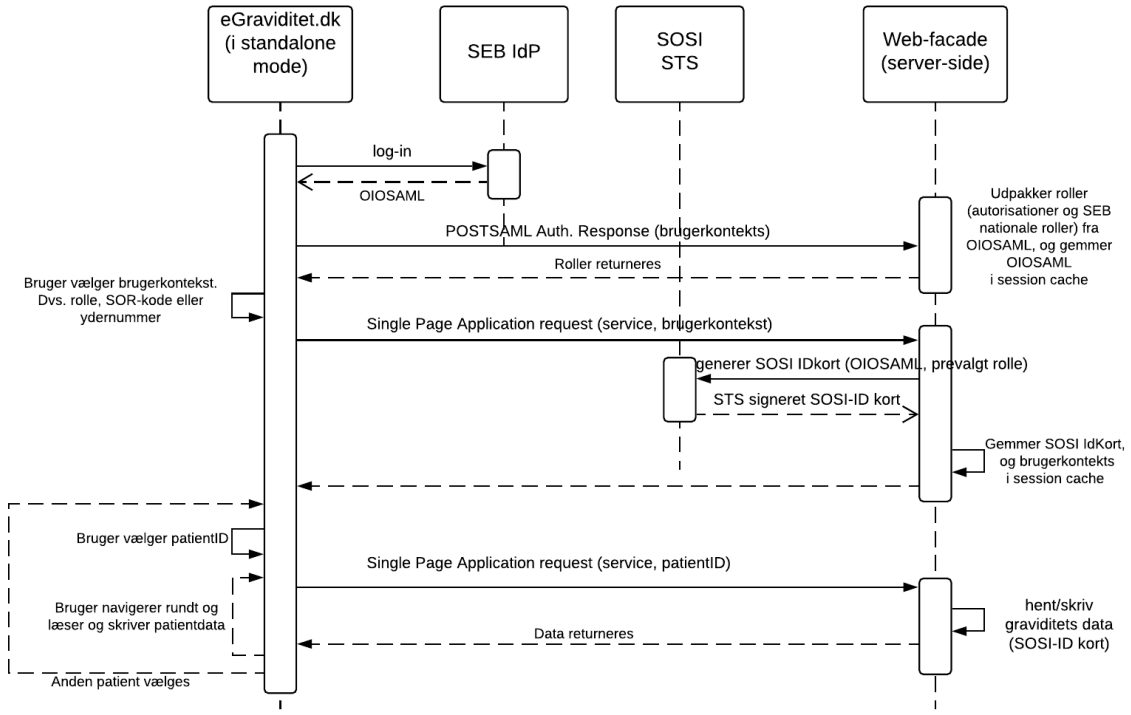
Den sundhedsfaglige sendes først til SEB IdP, som håndterer brugerens autentifikation. SEB IdP'en videresender brugeren til autentifikation hos NemLogin eller en lokal IdP (fx i en region). Dvs. SEB IdP'en introducerer en afkobling til eksisterende og fremtidige nationale og lokale autentifikationssystemer.
Fra SEB IdP'en returneres et OIOSAML token med indlejret SOSI IdKort. Af OIOSAML tokenet fremgår desuden brugerens mulige roller i form af sundhedsfaglige autorisationer og nationale SEB roller.
NB: SDS skal konfigurere/videreudvikle SEB IdP'en til at indlejre brugerens mulige nationale SEB roller i OIOSAML billetten. I dag indlejres kun brugerens mulige sundhedsfaglige autorisationer.

Da OIOSAML billetten er anvendelsesmæssigt låst (audience-restricted) til Web-facaden, så er det kun Web-facaden som kan udtrække de indlejrede roller.

eGraviditet.dk laver et “POSTSAML Auth. Responese" mod Web-facaden. Web-facaden tjekker OIOSAML tokenet og gemmer det i et sessionsobjekt. De indlejrede roller returneres til eGraviditet.dk.

Herefter skal den sundhedsfaglige vælge brugerkontekst. Dvs. den rolle, som vedkommende ønsker at arbejde under, samt SOR-ID eller ydernummer for den afdeling/praksis, som brugeren arbejder under.
Den sundhedsfaglige kan i princippet have flere sundhedsfaglige autorisationer og/eller flere nationale SEB rolle. Den sundhedsfaglige skal vælge den rolle, der matcher det ansættelsesforhold, som den sundhedsfaglige arbejder under, og som har medført behovet for at tilgå graviditetsdata for en gravid.

Ud fra den valgte brugerkontekst kan Web-facaden få SOSI IDkortet oprettet. I den forbindelse tjekker SOSI STS’en via Autorisations-registeret eller SEB-registeret, om brugeren må benytte den valgte rolle. SOSI Idkort og brugerkontekst gemmes i sessionsobjektet.
NB: SDS skal konfigurere SOSI STS til at truste’e SEB IdP’en og evt. tjekke for et HSM signeret IDKort.



Figur 15: Sekvensdiagram for sikkerhedsmodel i Standalone eGraviditet.dk

I den sidste del af sekvensdiagrammet illustreres, at brugeren skal vælge patientkontekst (cpr på den gravide), hvorefter brugeren kan læse eller skrive patientdata.
Fra Standalone løsningen kan brugeren skifte patient indenfor samme brugersession. Dvs. ny patient kan vælges uden, at den sundhedsfaglige afkræves re-autorisation.

5.3. Autorisation

Autorisation vedrører hvilke informationer borgeren eller den sundhedsfaglige må læse eller opdatere. I løsningsarkitekturen (se Figur 7) ligger autorisationsbeslutningerne nede hos de

backend komponenter, der udleverer eller gemmer data. Dvs. autorisationen vedr. læseadgang ligger hos DDS'en og autorisation vedr. skriveadgang ligger hos Graviditetskort-registret, Graviditetsplan-registret, i Fælles Stamkort-registret og DokumentRegistreringsServicen.

Der har i forbindelse med Gravid_i_DK use case arbejdet været ønske om, at en fuldmagtshaver ikke nødvendigvis har samme adgang til data som den gravide. Fx et ønske om at fuldmagtshaver ikke må se de følsomme dele af Graviditetskortet (fx tidligere aborter). Dette ønske kan ikke honoreres da Graviditetskortet er ét samlet CDA dokument, og DDS'en kan og må ikke klippe i og dermed fjerne information fra et CDA dokument.

Hvis ønsket skal honoreres, så vil det kræve et ekstra Policy Enforcement Point (PEP) oppe i App-facaden. Dvs. App-facaden vil skulle tage stilling til roller og på baggrund af disse fjerne data hentet fra backenden. PEP tilknyttet App-facaden etableres ikke i fase 1.