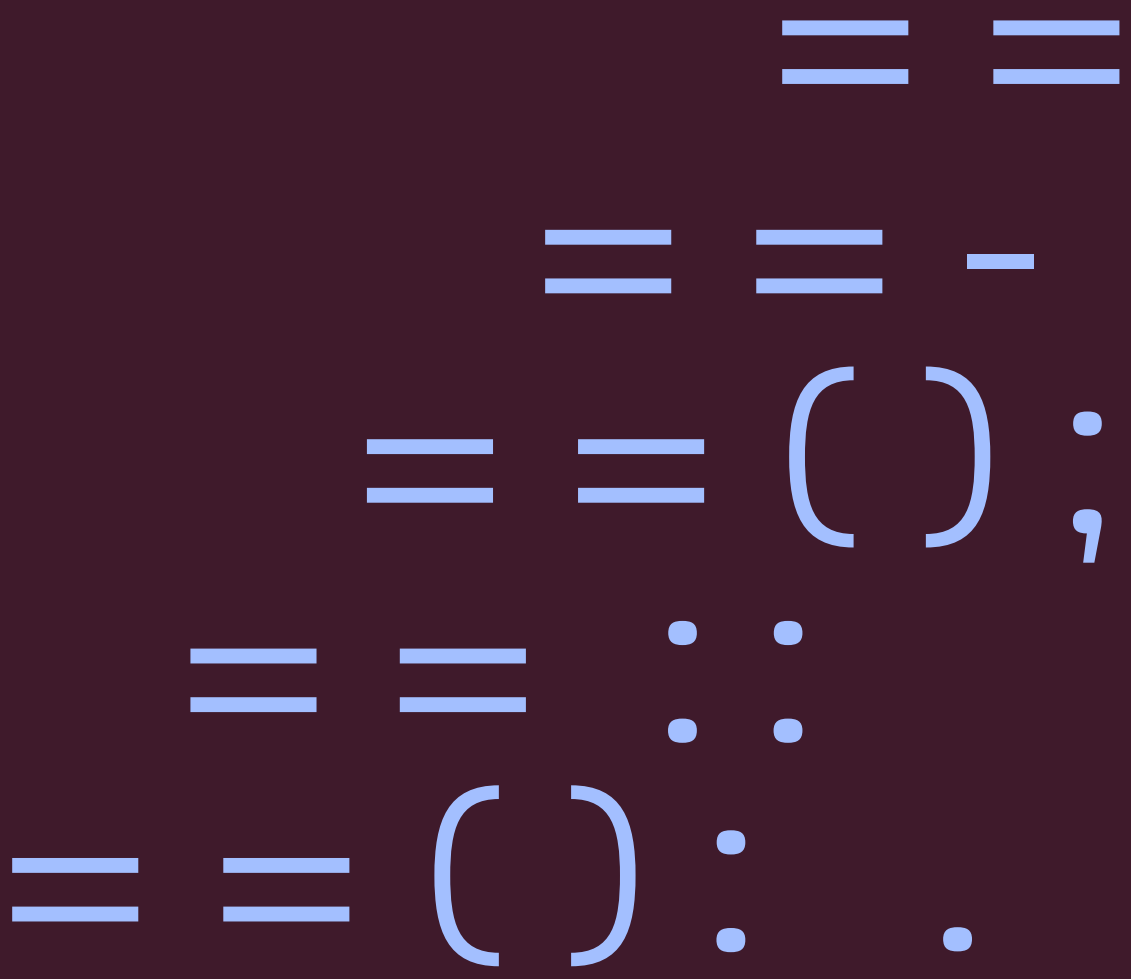
Digitaliserings-
styrelsen

Whitepaper

Borger.dk's Digital Post-klienter



Marts 2022

Indhold

1. Resumé

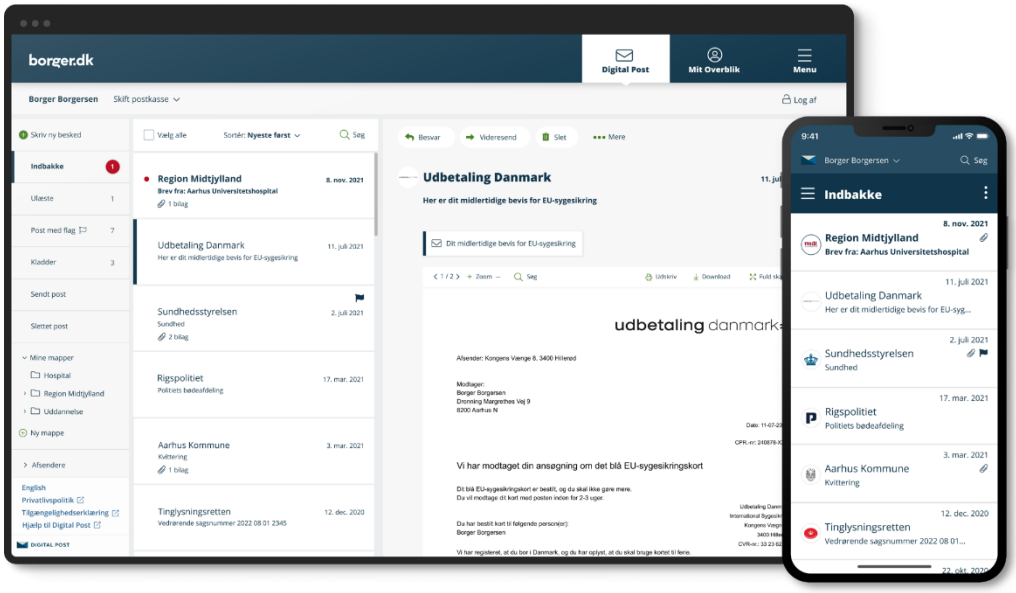
Dette whitepaper om Digital Post-klienterne giver en indføring i klienternes formål, funktioner, opbygning samt sikkerheds- og privatlivsmæssige aspekter af løsningerne.

Borger.dk's visningsklienter til Digital Post består af en webklient, der er en del af borger.dk og en Digital Post-mobilapplikation. Disse klienter er primært målrettet borgere. Erhvervsstyrelsen laver en webklient til virksomheder, mens private virksomheder udarbejder kommercielle visningsklienter, der også kan vise Digital Post-beskeder fra det offentlige.

Digital Post skal som udgangspunkt benyttes af alle med fast bopæl i Danmark, der er fyldt 15 år.

Visningsklienterne har den nødvendige funktionalitet til at borgere og myndigheder kan kommunikere med hinanden på sikker vis.

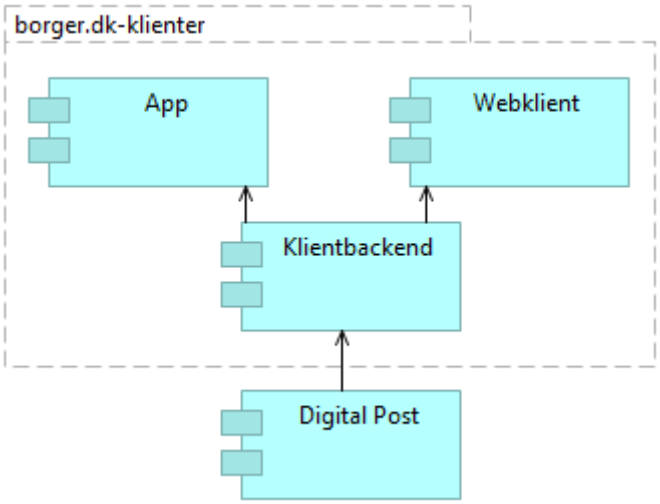
Digital Post minder på mange områder om e-mail, men Digital Post er et lukket kredsløb. Borgerne kan læse deres Digital Post og organisere denne på forskellig vis. Det er ligeledes muligt at tildele og anmode andre brugere om læseadgange til en andens Digital Post. Borgere kan skrive til myndigheder enten ved at besvare en Digital Post-besked eller oprette en ny.



Billede 1: Hovedskærmene i henholdsvis borger.dk-webklienten og Digital Post-appen.

Digital Post er en løsning, der skal benyttes af mange borgere, som har forskellige forudsætninger. Klienterne er derfor udviklet ud fra et princip om, at de skal være så brugervenlige og webtilgængelige som muligt – og løsningerne er begge blevet testet grundigt.

Både webklienten og Digital Post-appen benytter den samme bagvedliggende infrastruktur. Denne infrastruktur sørger for at kommunikere med selve Digital Post-løsningens snitflader til begge visningsklienter. Digital Post-løsningen har i sig selv ingen borger- eller virksomhedsvendt brugergrænseflade.



Figur 1: Klientbackend er den bagvedliggende infrastruktur, der kommunikerer med Digital Post på vegne af henholdsvis webklienten og appen.

Sikkerhed, sikring mod misbrug og beskyttelse af borgernes privatliv er altafgørende og drejer sig om at sikre de tekniske løsninger mod angreb, sikre at borgernes data ikke misbruges eller bliver gjort tilgængelige for uvedkommende.

Klienterne er derfor blevet grundigt testet af et eksternt sikkerhedsfirma. Der er ligeledes blevet implementeret foranstaltninger både i forhold til funktionalitet, i softwareløsningerne, driftsmiljøer og de processer, som omgiver klienterne.

2. Indledning

Formålet med dette whitepaper er at beskrive borger.dk's Digital Post-klienters funktionalitet, opbygning samt sikkerheds- og privacymæssige aspekter.

Borger.dk's Digital Post-klienter udvikles af Digitaliseringsstyrelsen.

Klienterne udgøres af henholdsvis en webklient på borger.dk, som tilgås med en browser samt en mobilapplikation, der kan benyttes på smartphones og tablets.

Webklienten på borger.dk er målrettet borgere, mens mobilapplikationen er målrettet borgere samt mindre virksomheder.

Erhvervsstyrelsen udarbejder en tilsvarende Digital Post-webklient i regi af erhvervsportalen Virk, der er målrettet virksomheder. Ligeledes udvikler private leverandører også klienter, der kan vise offentlig såvel som privat digital post.

De kommercielle klienter, der udvikles af private leverandører, giver borgerne adgang til den samme Digital Post som de offentlige klienter, som dette whitepaper omhandler. Borgerne kan dermed frit vælge, hvilken klient, de ønsker at benytte, og det er muligt at benytte sig af flere klienter.

I dette whitepaper gennemgås i afsnit 3 formålet med Digital Post og klienterne, da dette er rammesættende for de tekniske løsninger som beskrives.

Klienternes væsentligste funktionalitet i både webklienten og appen præsenteres i afsnit 4.

I afsnit 5 og afsnit 6, der omhandler henholdsvis webtilgængelighed og brugervenlighed, beskrives nogle af de tiltag, der er foretaget for at sikre, at så mange borgere som muligt kan benytte løsningerne.

I afsnit 7 gennemgås den overordnede it-arkitektur, hvor bl.a. sammenhængen mellem Digital Post-klienterne og selve Digital Post-løsningen forklares, og hvor de tekniske facetter af borger.dk's Digital Post-klienter beskrives nærmere.

Det sidste afsnit 8 omhandler de sikkerhedsmæssige aspekter af webklienterne, herunder it-sikkerhed, sikring mod misbrug og beskyttelse af borgernes privatliv – samt nogle af de foranstaltninger, som er foretaget.

Dette whitepaper er udarbejdet i forbindelse med lanceringen af Digital Post, og løsningerne beskrives derfor, som de er udformet på dette tidspunkt. Der vil forventeligt ske en videreudvikling af løsningerne efterfølgende. Den eventuelle udmøntning af denne er ikke beskrevet i dette whitepaper.

Det skal bemærkes, at de benyttede illustrationer stammer fra løsningernes testmiljøer og fremviser derfor testdata. Ligeledes vil tekster i illustrationerne ikke nødvendigvis fremstå fuldstændig som i de lancerede udgaver af visningsklienterne.

3. Formålet med Digital Post-klienterne

Digital Post er en sikker kanal til kommunikation mellem borgere og myndigheder.

Digital Post benyttes til at sende Digital Post sikkert mellem de offentlige myndigheder (fx kommunale, regionale og statslige myndigheder) og borgere og virksomheder.

Alle borgere over 15 år med bopæl eller fast adresse i Danmark har siden den 1. november 2014 været forpligtet til at have en digital postkasse tilknyttet CPR-nummeret, hvor de kan modtage post fra offentlige myndigheder. Borgere, som af forskellige årsager ikke kan benytte Digital Post, har mulighed for at blive fritaget.

Digitaliseringsstyrelsen har besluttet at hjemtage en større del af ejerskabet over it-løsningen bag Digital Post, og i den forbindelser er der blevet udviklet en ny Digital Post-infrastruktur, der kan skabe bedre sammenhæng mellem de offentlige løsninger, som er mere brugervenlig, og som er lettere at administrere.

Målet er at bane vejen for bedre kommunikation mellem borgere og myndigheder, så kommunikationen vil opleves nemmere og mere brugervenlig. Fx vil det blive tydeligere, hvem der har sendt digital post, og hvad den handler om.

Digital Post-løsningen bliver udviklet, så der kan være flere Digital Post-klienter, der viser post på forskellige teknologiske platforme. Det betyder, at borgere og virksomheder i fremtiden vil få større valgfrihed om, hvor de vil læse deres Digital Post.

Det er en stor fordel, fordi:

- Det sikrer en kontinuitet for borgere, der ikke ønsker en forandring. Hvis man i dag foretrækker at læse offentlig post på e-Boks, vil man fortsat have denne mulighed.
- Det introducerer konkurrence på markedet for sikker Digital Post, hvilket forventeligt vil give bedre priser og services for de virksomheder, der gerne vil kommunikere sikkert til deres kunder. Virksomhederne e-Boks og Mit.dk vil tilbyde visning af offentlig post i tilknytning til post fra private afsendere.
- På den måde får danskerne bedre kommunikation og færre almindelige mails sendt over en ikke-krypteret forbindelse med vigtige eller fortrolige informationer.
- Selv med flere klienter, så samles borgernes Digital Post fra det offentlige ét sted. Og man vil altid kunne se al offentlig post på borger.dk, Virk og i Digital Post-appen.

Da Digital Post er obligatorisk, udvikles der en række offentlige Digital Post-klienter, der skal sikre, at borgere og virksomheder altid har mulighed for at læse deres Digital Post på en brugervenlig, tilgængelig og sikker vis i vante rammer på henholdsvis borger.dk og Virk.

De offentlige Digital Post-klienter vil udelukkende vise Digital Post fra offentlige myndigheder, og har ikke – modsat kommercielle klienter – mulighed for også at vise digital post fra private virksomheder. Se desuden afsnit 0.

I klienterne, der er tilknyttet borger.dk, vil alle nødvendige funktioner i Digital Post være tilgængelige.

3.1 Borgere og erhvervsbrugere i borger.dk's Digital Postklienter

Webklienten på borger.dk kan som udgangspunkt kun benyttes af borgere, der logger ind med deres NemID eller MitID via NemLog-in. Undtagelsen er virksomheder, der er partsrepræsentant for en borger. Disse brugere vil kunne logge ind og kunne se postkasser for borgere, som de repræsenterer.

Digital Post-appen kan benyttes af borgere, NemID til erhverv-brugere og virksomhedsbrugere, herunder virksomheder, som repræsenterer en borger.

4. Funktionalitet

Borger.dk's Digital Post-klienter indeholder mange funktioner. De væsentligste funktioner omhandler muligheder for at læse, skrive og organisere Digital Post.

4.1 Klienternes overordnede funktionalitet

Digital Post-klienterne til borgerne, henholdsvis en app og en web-løsning, indeholder samme funktionalitet med få forskelle. Eksempelvis skal indstillinger om læseadgang foretages i webklienten, mens push-notifikationer kun findes i appen.

Da Digital Post begrebsmæssigt minder om e-mails, er det naturligt, at klienterne minder om e-mail-klienter både visuelt og funktionelt. Borgerne vil derfor kunne genkende mange mønstre fra andre løsninger, som de benytter i andre sammenhænge (se desuden afsnit 6.1).

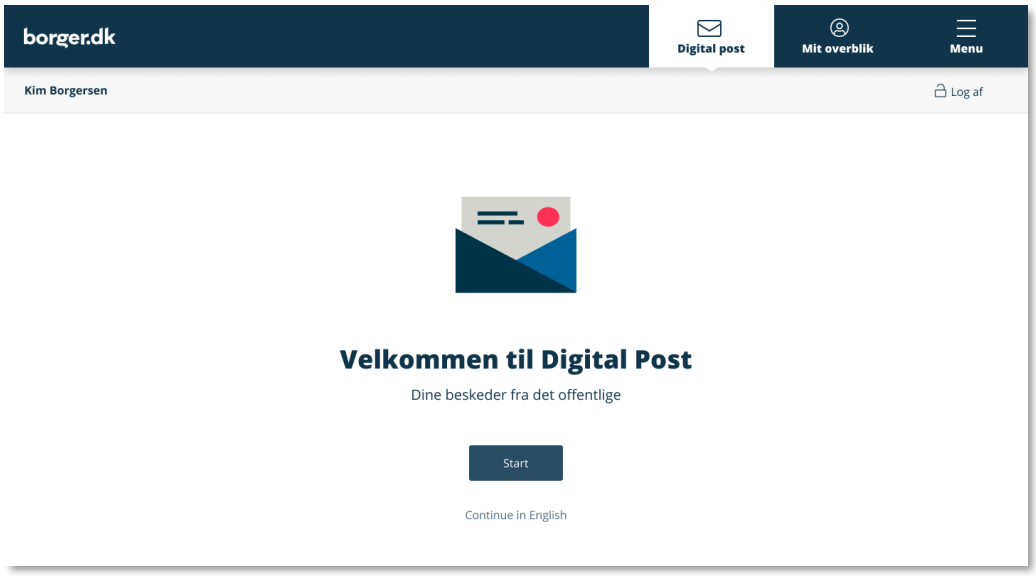
Der er dog forskelle på Digital Post og klassisk e-mail på en række områder fx:

- Digital Post er et lukket kredsløb, hvor kun oprettede parter kan sende beskeder til hinanden. Det er dog muligt for en borger at sende en Digital Post-besked til en ekstern e-mail.
- Borgere adresseres på deres CPR-nummer (modsat en e-mail-adresse)
- Borgere kan kun rette henvendelse til de kontaktpunkter, som myndigheder har oprettet.
- I Digital Post kan borgere kun videresende beskeder til andre borgere, såfremt den modtagne part har godkendt, at denne vil modtage Digital Post fra afsenderen.
- Borgere kan give læseadgang til postkasser, så andre borgere eller virksomheder kan se indholdet af disse.
- Digital Post-beskeder har flere funktioner, som adskiller sig fra normale e-mails fx *handlinger*.

I de næste afsnit gennemgås klienternes væsentligste funktionalitet i de to løsninger.

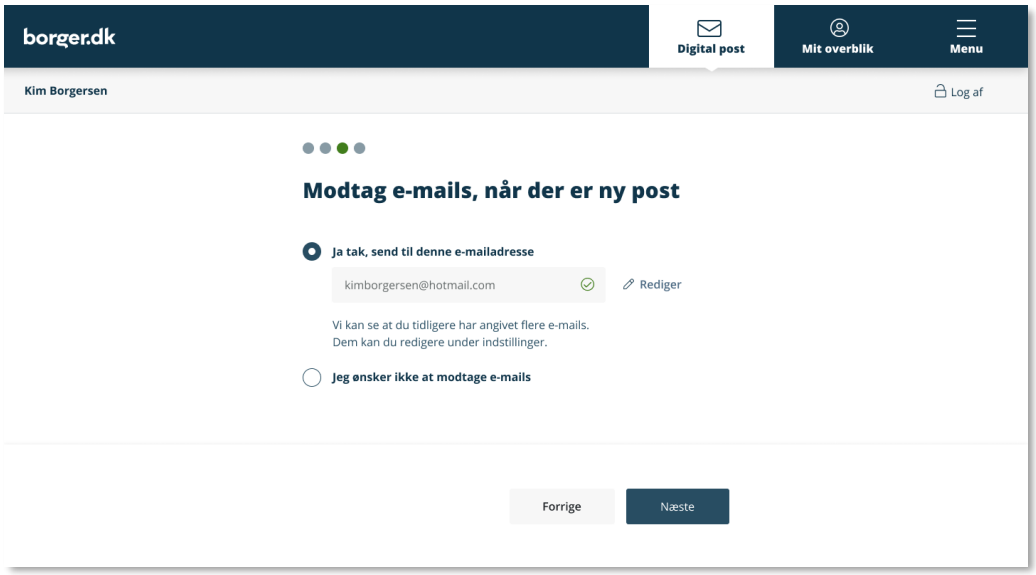
4.2 Introduktionsforløb

Første gang borgeren benytter Digital Post-klienten skal der gennemføres et introduktionsforløb. Introduktionsforløbet giver borgeren et indblik i den væsentligste funktionalitet.



Billede 2: Velkomstskærmen i webklienten som vises første gang borgeren benytter løsningen.

Som en del af introduktionsforløbet bliver borgeren bedt om at tage stilling til, hvorvidt der ønskes henholdsvis en e-mail- og/eller en SMS-advisering, når der modtages Digital Post.

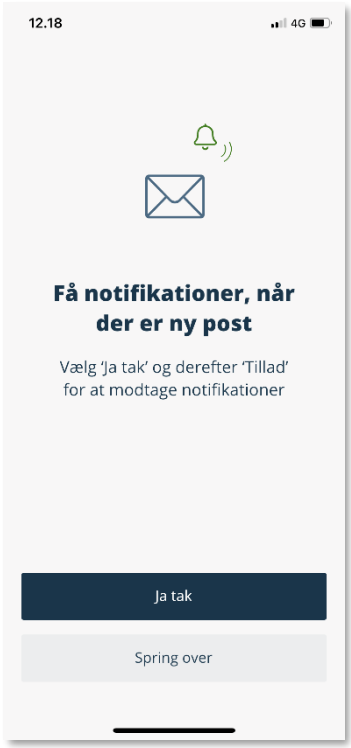


Billede 3: Borgeren skal i introduktionsforløbet i webklienten tage stilling til, om der ønskes e-mails og/eller SMS-beskeder, der adviserer om ny post.

Hvis dette ønskes, så skal e-mailadresse/telefonnummer bekræftes med en engangskode.

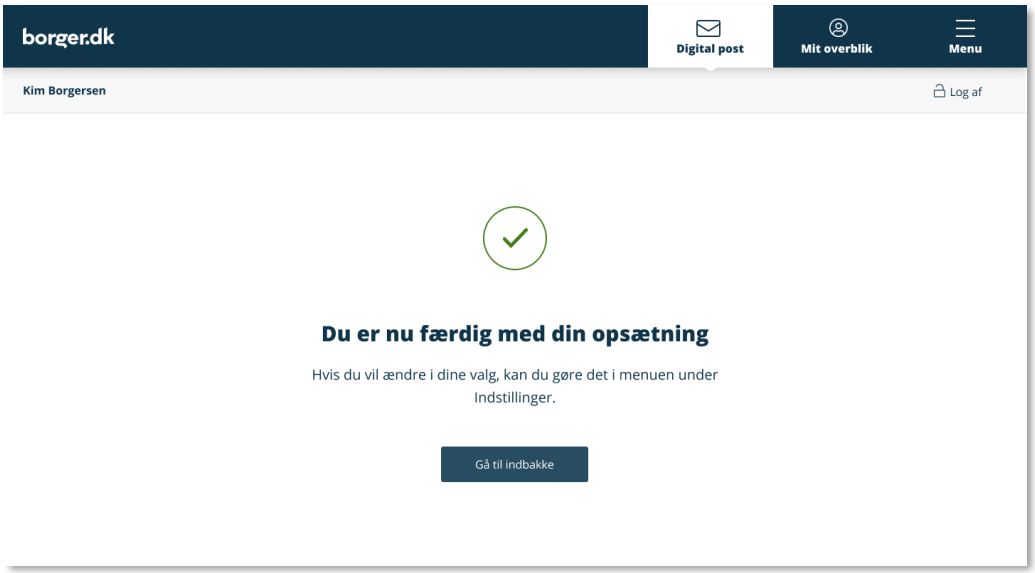
Billede 4: Bekræftelseskoden indtastes, så det sikres, at det indtastede telefonnummer er korrekt og knyttet til borgeren.

I appens introduktionsforløb skal borgeren ligeledes tage stilling til, om der ønskes push-notifikationer, som kan advisere om ny Digital Post, samt om borgeren ønsker at kunne logge ind med biometri/pinkode.



Billede 5: Borgeren skal i introduktionsforløbet i appen tage til, om der ønskes push-notifikationer, der adviserer om ny post.

Herefter er borgeren færdig med opsætningen.



Billede 6: Webklienten informerer borgeren, at opsætningen er gennemført.

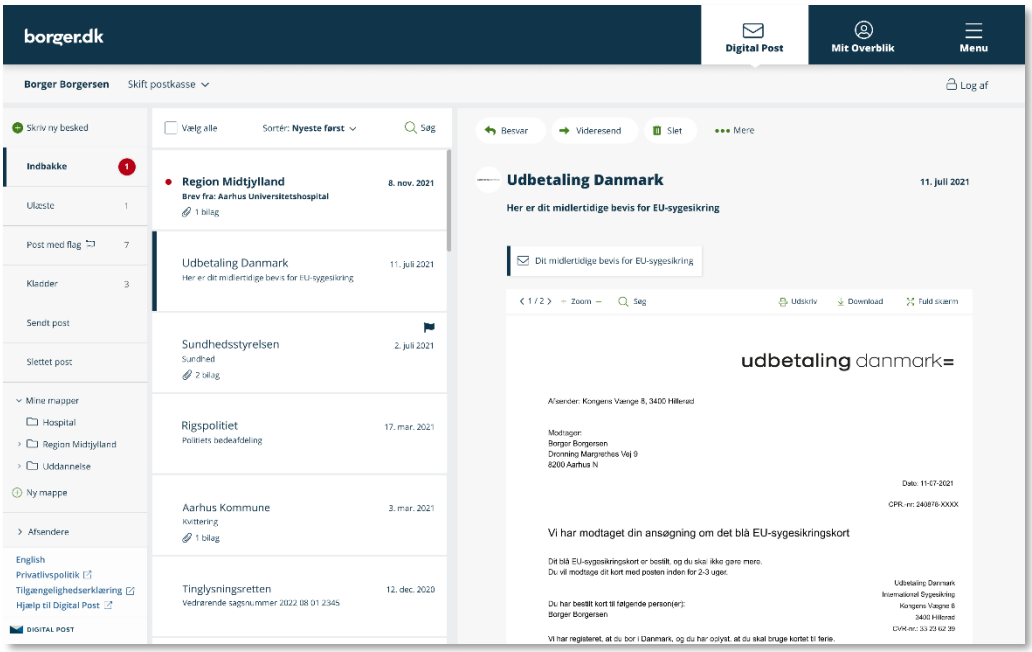
4.3 Hovedskærm

I klienternes hovedskærm er der adgang til alle de væsentligste funktioner.

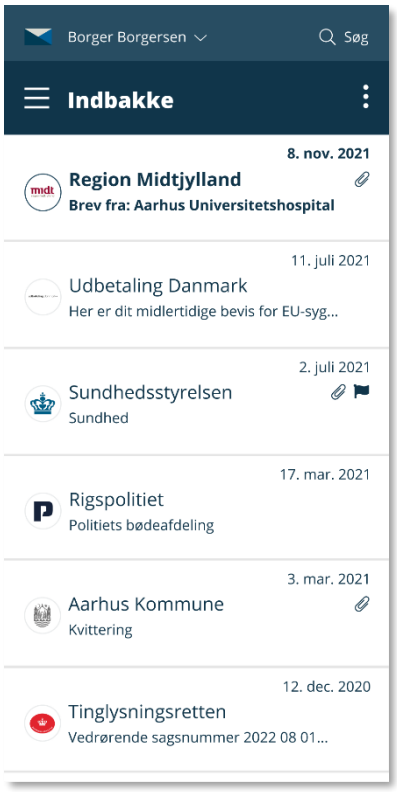
Hovedskærmen i webklienten består af en liste over mapper, en beskedsliste, der viser Digital Post-beskederne i den valgte mappe og en forhåndsvisningsrude, hvor man kan se den valgte Digital Post-besked.

Som udgangspunkt starter hovedskærmen med at vise borgerens indbakke, da det er her nye beskeder vises.

I appen vises som udgangspunkt beskedlisten, som starter med indbakken. Der er her fra adgang til mappelisten samt forhåndsvisningsruden.



Billede 7: Webklientens hovedskærm med mappeliste, beskedliste og forhåndsvisningsrude.



Billede 8: Appens hovedskærm, der viser indbakken.

4.3.1 Mapper

Klienterne har en række faste mapper, som borgeren ikke selv kan slette eller flytte. Det drejer sig om mapperne *Indbakke*, *Kladder*, *Post med flag*, *Ulæste*, *Sendt post* og *Slettet post*. Derudover er det også muligt at se mapper med de myndigheder, som man har modtaget Digital Post fra.

Borgere har ligeledes mulighed for at oprette egne mapper med undermapper og flytte Digital Post-beskeder til disse.

4.3.2 Beskedliste

I beskedlisten vises beskederne i den valgte mappe.

På den enkelte besked er det muligt at udføre handlinger fx flytte, slette eller markere med flag. I webklienten kan man højreklikke på en besked i beskedlisten for at få adgang til handlingerne, mens man i appen kan *swipe* på en besked.

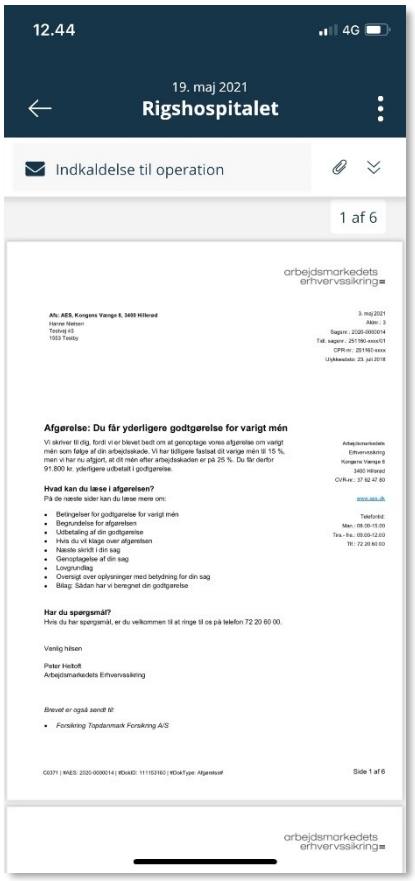
Det er også muligt at markere flere beskeder og dermed foretage handlinger på flere beskeder på samme tid.

4.3.3 Søgning

I beskedlisten er det muligt at foretage en søgning i Digital Post-beskederne. Når der søges, foretages en søgning i alle mapper og resultatet vises i beskedlisten.

4.3.4 Forhåndsvisningsruden

I forhåndsvisningsruden vises den besked, som er valgt i beskedlisten. På mindre skærme vises forhåndsvisningsruden ikke sammen med beskedlisten og mappelisten men derimod i sin egen skærmvisning. Det samme princip gør sig gældende i appen.



Billede 9: Forhåndsvisningsruden i appen.

4.4 Læse Digital Post

Borgeren kan læse sin Digital Post enten i forhåndsvisningsruden eller vælge en fuldskærmsvisning.

Det er muligt at se en forhåndsvisning af langt de fleste dokumenter, der er vedhæftet til en besked i Digital Post. På den måde behøver borgeren ikke downloade filer til sin enhed eller pc. Dette er særligt hensigtsmæssigt for borgere, der benytter pc'er, som deles med andre fx på biblioteker eller i borgerservicecentre.

Dokumenter, der ikke kan forhåndsvises, skal downloades af borgeren. Når borgeren starter et download, advares der mod at gemme på offentlige pc'er (se også afsnit 8.7).

4.4.1 Digital Post-beskedformatet MeMo

I forbindelse med lanceringen af den nye Digital Post-løsning introduceres et nyt beskedformat til Digital Post *Meddelelsesmodel* (MeMo).[1]

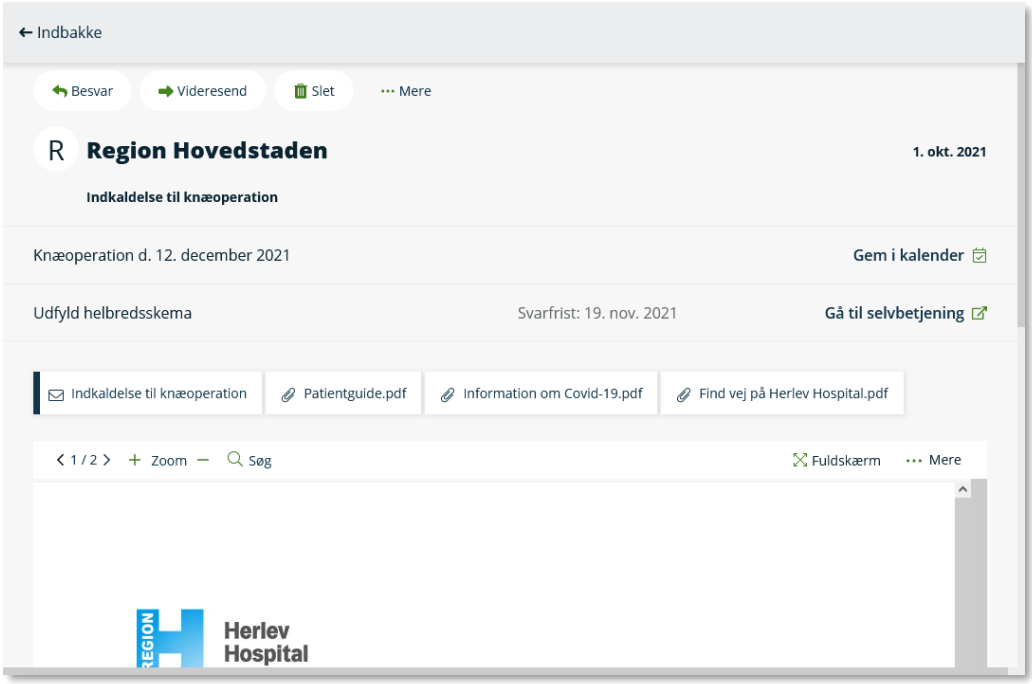
Set fra et slutbrugerperspektiv minder MeMo-beskeder meget om vanlige Digital Post-beskeder og e-mails men med en række tilføjelser, som beskrives i de følgende afsnit.

[1] https://www.digitaliser.dk/resource/5248921/artefact/IntrotilMeddelelsesModel(MeMo).pdf?artefact=true&PID=6074027

4.4.2 Handlinger

Foruden at vedhæfte dokumenter til en Digital Post-besked kan myndighederne også forsyne en besked med handlinger, som fx kan bestå af links, som leder borgeren til en selvbetjeningsløsning.

Det er også muligt for myndigheden at vedhæfte en kalenderaftale, som borgeren kan overføre til sin egen kalender – fx kalenderen på borgerens telefon.



Billede 10: En Digital Post-besked med en handling i form af et link til en selvbetjeningsløsning og en vedhæftet kalenderaftale.

4.4.3 Ekstra felter

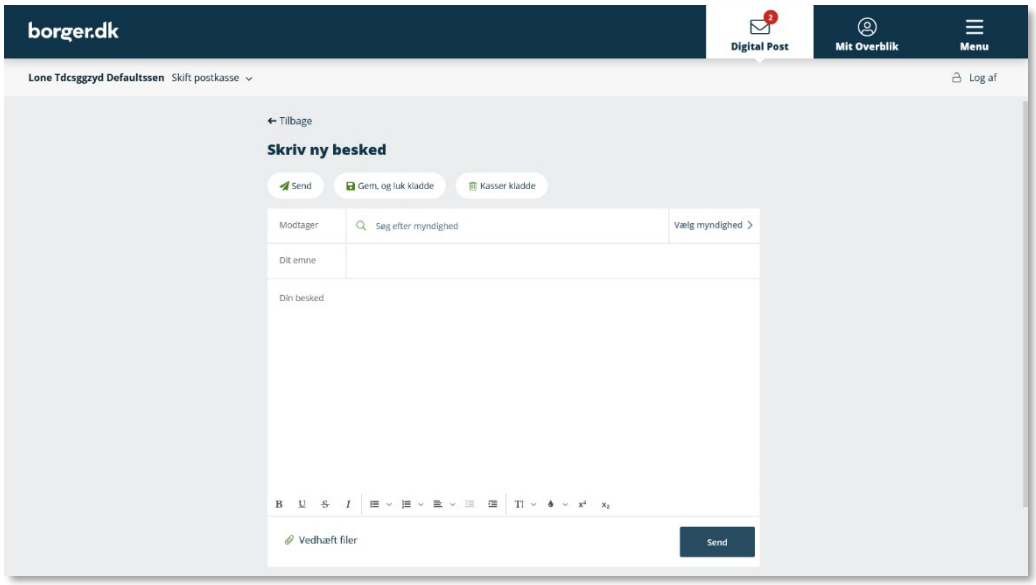
Myndigheder har også mulighed for at forsyne borgerens svarformular med en række ekstra felter, så myndigheden kan modtage data struktureret. Det kan fx være et løbenummer, et registreringsnummer eller et navn.

4.4.4 Mulighed for at besvare

Myndighederne kan angive, hvorvidt det skal være muligt for borgerne at besvare en besked. Denne mulighed kan være forsynet med en svarfrist. Hvis det er muligt at besvare en besked, så vises en besvar-knap i brugergrænsefladen.

4.5 Skriv til offentlige myndigheder

Borgere kan skrive til offentlige myndigheder via en formular og har mulighed for at gemme kladder. Til en besked kan der angives et emne og vedhæftes filer foruden selve beskedteksten.

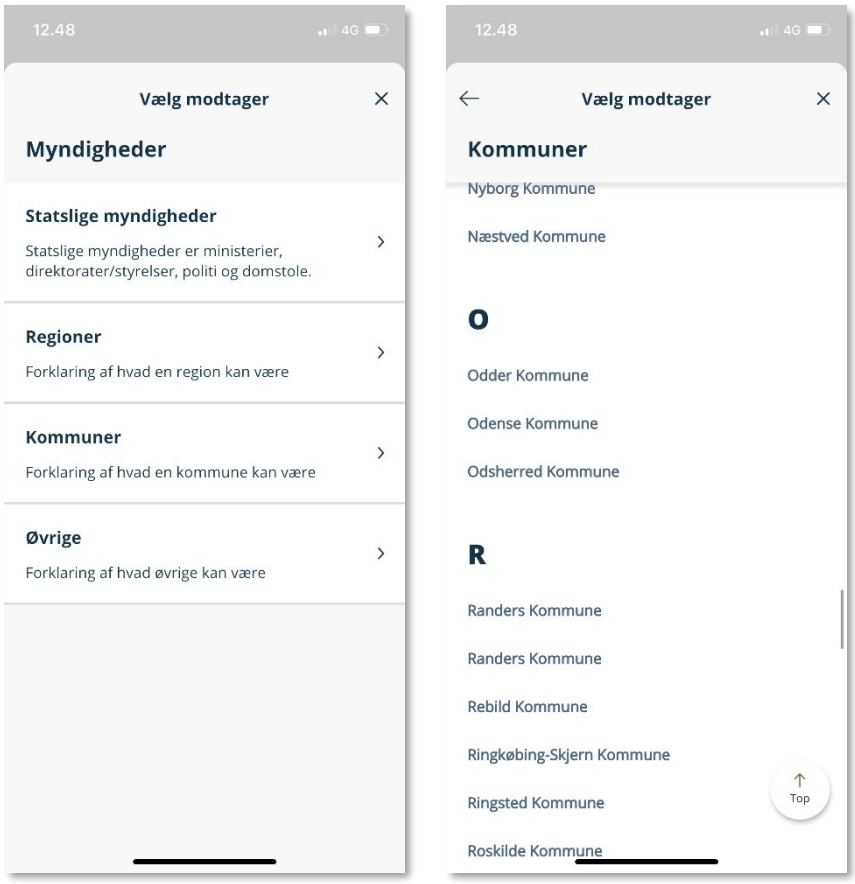


Billede 11: Illustration: Skriv til det offentlige-formular, som borgerne skal benytte, når der skriver til myndighederne.

4.5.1 Kontaktpunkter

For at hjælpe borgeren med at finde det rette kontaktpunkt hos en myndighed er det muligt både at navigere sig frem til kontaktpunkter. I webklienten kan de også fremsøges.

Nogle myndigheder vil have mange kontaktpunkter, mens andre blot vil have få.



Billede 12: Borgeren klikker sig frem til den myndighed, som skal kontaktes. På første skærm vælges, hvilken type myndighed, der er tale om, og derefter vælges den rette myndighed og til sidst et kontaktpunkt. Skærmbilleder er fra appen.

Det er muligt for myndighederne at linke direkte til en kontaktformular, hvor modtageren er forhåndsudfyldt. På den måde kan myndigheder direkte fra fx hjemmesider linke til en kontaktformular, så borgeren ikke selv behøver fremsøge det relevante kontaktpunkt.

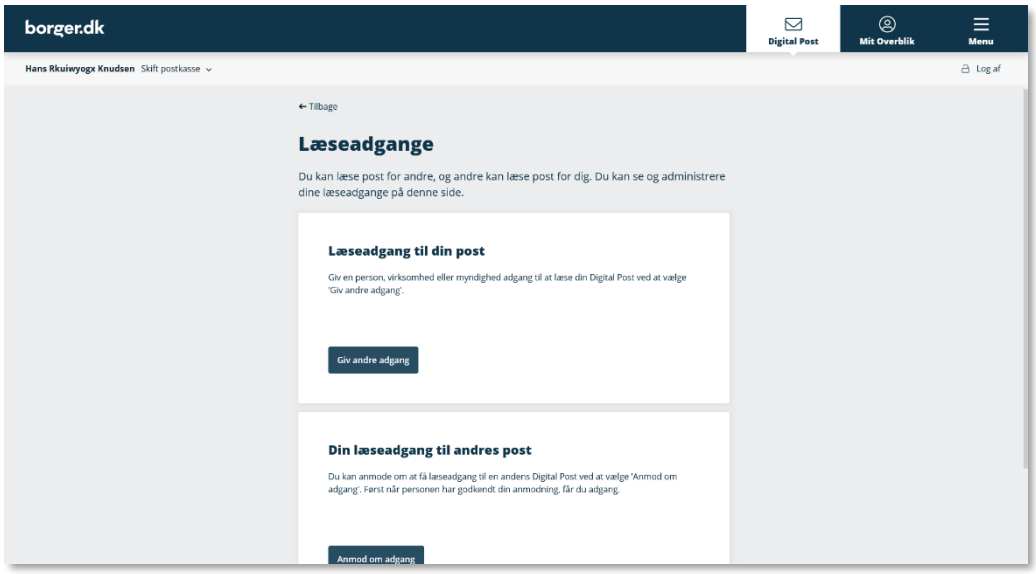
Hvis en Digital Post-besked er markeret som mulig at besvare, så er kontaktformularen også forhåndsudfyldt med modtager, når borgeren benytter besvarformularen.

4.6 Læseadgang

I Digital Post er det muligt for borgere at give andre adgang til ens Digital Post. Det er ligeledes muligt at anmode andre om adgang til deres postkasse. En anmodning skal godkendes, og det er muligt for den modtagende part at afvise en tildelt læseadgang.

Det er muligt at have adgang til flere postkasser, og man kan give flere personer adgang til sin egen postkasse.

Funktionen kan eksempelvis benyttes af ældre, der kan give børn adgang til deres postkasse, eller unge der ønsker at give deres forældre adgang.



Billede 13: Borgeren kan give og modtage læseadgang til Digital Post.

4.7 Digital Post-modtagere

Tilsvarende læseadgang er det også muligt at videresende Digital Post-beskeder til tillidspersoner, som også har Digital Post. Funktionen kan benyttes, hvis en borger ønsker at give en anden part adgang til at læse en Digital Post-besked men ikke ønsker at give adgang til hele postkassen.

For at kunne sende Digital Post-beskeder videre til Digital Post-modtagere, skal sidstnævnte acceptere dette på forhånd.

Dette medvirker til at sikre, at man ikke modtager uønskede Digital Post-beskeder fra borgere og virksomheder, man ikke kender på forhånd.

4.8 Forkyndelse

Digital post understøtter digital forkyndelse, hvor indkaldelser og andre vigtige beskeder forkyndes til dem, der skal have beskederne, så retten er sikker på, at beskederne er modtaget.

Eksempelvis kan retten sende en Digital Post-besked til en borger, som skal møde i retten, stævnes eller have en retsafgørelse. Juridisk set vil Digital Post-beskeden være modtaget og forkyndt, så snart den bliver behandlet, fx åbnet, flyttet eller slettet.

Når borgeren foretager en af disse handlinger i en Digital Post-klient, sendes en besked til Digital Post, der herefter registrerer, at Digital Post-beskeden er forkyndt.

I den forbindelse modtager borgeren en besked om, at forkyndelsen er foretaget.

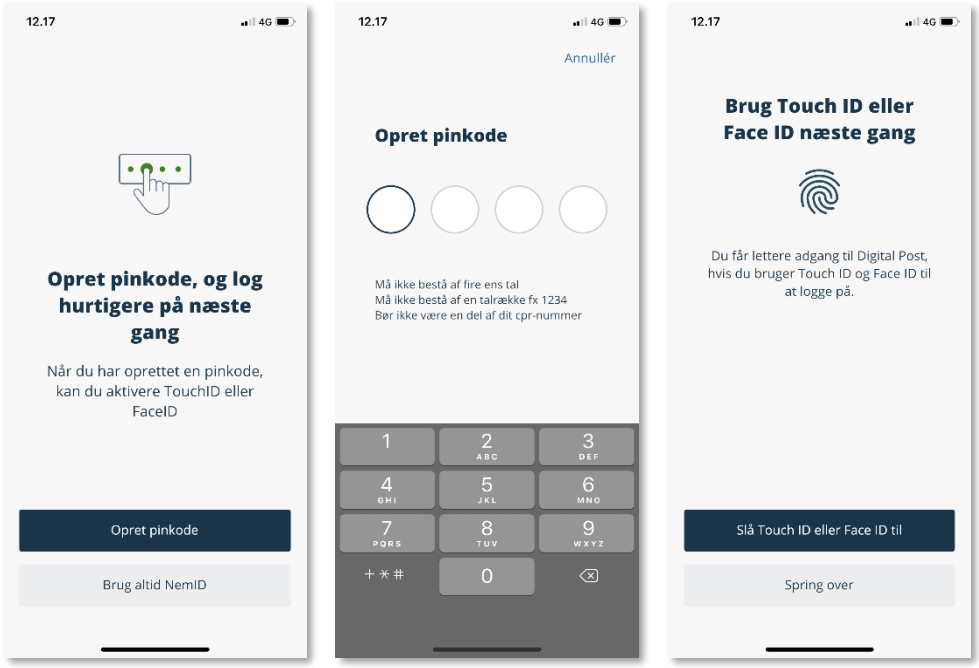
Billede 14: Forkyndelse af en Digital Post-besked i appen.

Efter forkyndelsesbeskeden er vist, kan borgeren læse Digital Post-beskeden. Hvis borgeren på et senere tidspunkt vil åbne den pågældende Digital Post-besked, kan det ses, hvornår beskeden blev forkyndt, og det er ligeledes muligt at gense forkyndelsesteksten.

Billede 15: Udsnit af forkyndt Digital Post-besked i webklienten.

4.9 Logge ind hver gang eller benytte pinkode/biometri i app

Borgerne kan i appen vælge, om de vil benytte pinkode eller biometri, eller om de vil logge ind med NemID eller MitID, hver gang appen benyttes. Se også afsnit 7.6 og afsnit 8.7.



Billede 16: Borgeren kan vælge en pinkode og eventuelt også biometri.

4.10 Gæstebruger-funktion i app

I appen er der tilføjet en mulighed for at logge på som gæst.

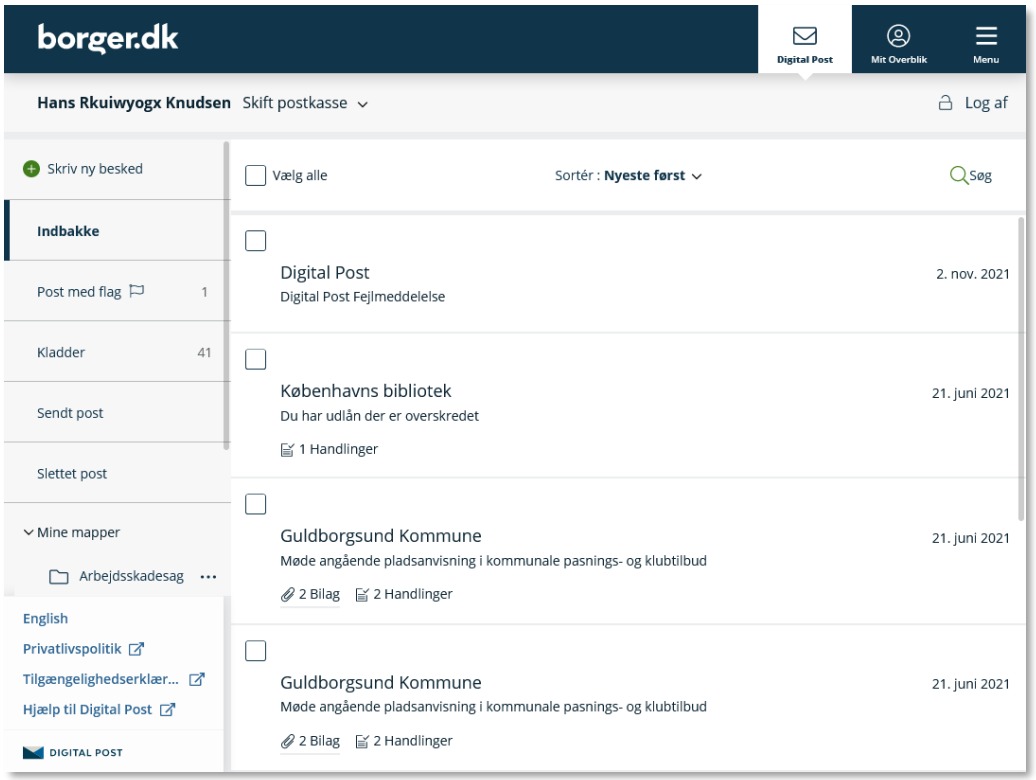
Det giver mulighed for, at en borger kan være indstillet appen, så denne kan benytte biometri og pinkode, mens en anden borger, fx en ægtefælle, midlertidigt kan låne appen og logge ind med sit NemID eller MitID.

En gæstebruger kan ikke benytte den funktion, der gør det muligt at benytte pinkode eller biometri i appen, som blev beskrevet i afsnit 4.9, og en gæstebruger kan heller ikke modtage push-notifikationer, da denne funktion er tilknyttet den oprindelige bruger af appen. Når gæstebrugerens session afsluttes, glemmes gæstebrugerens data i appen.

Billede 17: Gæstebrugere orienteres om, at som gæstebruger kan der modtages push-notifikationer, og at man skal huske at logge ud, inden enheden overdrages.

4.11 Store og små skærme

Appen og webklienten er designet, så de fungerer på henholdsvis små skærme (smartphones) og store skærme (tablets og pc'er). Både app og webklient supporterer også skærmrotation.



Billede 18: Webklienten på en tabletskærm, hvor kun mappelisten og beskedlisten vises pga. skærmens begrænsede størrelse.

5. Webtilgængelighed

Digital Post er en obligatorisk løsning for borgerne. Derfor er det særligt vigtigt – og et lovkrav – at sikre webtilgængeligheden i klienterne. Dette sikres ved en lang række tiltag.

Begge klienter skal overholde "Lov om tilgængelighed af offentlige og offentligretlige organers websteder og mobilapplikationer."[2] Klienterne er derfor konstrueret, så de kan benyttes af borgere med handicap.

Konkret betyder det, at løsninger eksempelvis kan betjenes med tastatur og en skærmlæser. Det er også muligt at forstørre tekst i løsningerne, og alle farver har tilstrækkelig kontrast.

Tilgængelighedstests

Løsningerne er blevet testet ved en række forskellige tests, der har haft til formål at øge tilgængeligheden af løsningerne. Disse beskrives i det følgende.

5.1.1 Test i forbindelse med udvikling af løsningen

I forbindelse med udviklingen af løsningerne har det indgået, at al brugervendt funktionalitet har skullet være tilgængeligt.

I forbindelse med udviklingen af den grafiske brugergrænseflade er det sikret, at alle farver har tilstrækkelig kontrast, og at det er muligt at forstørre indhold.

Det er ligeledes sikret, at elementerne er korrekt semantisk opmærket, og at siderne har et logisk forløb.

Der er løbende blevet foretaget tests af dette, når der er blevet udviklet ny funktionalitet. Endelig er der foretage en tilgængelighedstest, der fx sikrer, at al funktionalitet kan tilgås med en skærmlæser.

5.1.2 Automatiske tests

Løsningen skannes løbende af automatiske værktøjer, der er designet til at finde tilgængelighedsproblemer.

Disse værktøjer rapporterer løbende, så der kan tages stilling til de emner, som identificeres.

5.1.3 Eksperttest

Løsningerne er ligeledes blevet testet af tilgængelighedseksperter. Disse tests har haft tre overordnede formål:

1. At sikre at WCAG-standarden bliver overholdt, og at andre teknikker til opnåelse af større tilgængelighed benyttes korrekt fx WAI-ARIA.
2. At få en ekspertgennemgang af løsningerne med henblik på at sikre, at løsninger overholder *best practice* og undgå faldgruber og misforståelser. Som led i dette har også indgået at

[2] https://www.retsinformation.dk/eli/lta/2018/692

sikre, at navngivning af elementer er hensigtsmæssig og logisk, samt at semantikken i siderne er korrekt.

3. At identificere fejl og anvise mulige løsninger herpå

5.1.4 Handicapbrugervenlighedstest

Endelig er løsningerne blevet brugertestet af borgere med handicap for at verificere, at de også er brugervenlige i praksis og ikke bare formelt overholder WCAG-standarden.

Disse brugertest er afviklet ved, at deltagerne har fået forskellige opgaver i klienterne, som har skullet løses ved hjælp af deres udstyr fx en skærmlæser, og i den forbindelse er de blevet observeret, så uhensigtsmæssigheder har kunnet opdages og rettes.

5.2 Tilgængelighed af Digital Post-beskeder

Det er ikke muligt for Digitaliseringsstyrelsen at sikre, at de dokumenter, som vedhæftes Digital Post-beskeder, fx pdf-filer, er tilgængelige. Dette ansvar pålægger alene myndighederne, som sender disse.

5.3 Webtilgængelighedserklæringer

Klienternes webtilgængelighedserklæringer kan læses her:

- Digital post på borger.dk
- Digital Post-app

6. Brugervenlighed

Digital post-klienter skal benyttes af mange forskellige borgere. Det er derfor vigtigt, at de er lette at forstå, nemme at benytte og er genkendelige. Dette sikres bl.a. ved at brugerteste klienterne.

Det er som udgangspunkt obligatorisk for borgerne at benytte Digital Post. Samtidigt skal webklienten og Digital Post-appen benyttes af borgere med vidt forskellige forudsætninger. Nogle borgere vil foretrække at benytte webklienten og andre kun appen. Nogle vil være kompetente it-brugere, mens andre vil være mere usikre. Andre igen vil være vante med kommunikation fra det offentlige, mens det for nogle vil være en ukendt størrelse.

Som vist i afsnit 4, så er der mange forskellige funktioner i løsningen, som man som bruger kan have behov for at sætte sig ind i.

Disse faktorer stiller store krav til brugervenligheden af løsningerne.

6.1 Designkonventioner

6.1.1 Digital Post-logo

Alle Digital Post-klienter skal benytte Digital Post-logoet, der signalerer over for borgere og virksomheder, at der er tale om Digital Post fra det offentlige. Logoet indgår derfor i begge klienter.

Billede 19: Digital Post-logoet, som skal indgå i alle klienter, der viser Digital Post fra det offentlige.

6.1.2 Genbrug af mønstre fra andre e-mail-løsninger

Det har været et vigtigt designprincip ikke at opfinde nye mønstre de steder, hvor der allerede er veletablerede designkonventioner.

Der findes talrige web-, desktop- og appbaserede e-mail-klienter, som mange borgere kender fra deres hverdag, og både webklientens og appens opbygning er baseret på *best practice* herfra. Eksempelvis er webklientens opbygning med en mappeliste, beskedliste og forhåndsvisning et mønster, der benyttes i de mange kendte e-mail-løsninger.

6.1.3 Sømløshed med borger.dk

Borgerne er trygge og bekendte ved at benytte borger.dk, og det er derfor vigtigt at vise, at borger.dk's webklient er en del af borger.dk-systemet.

Det visuelle udtryk i webklienten er derfor nøje afstemt med borger.dk herunder Mit Overblik. Ligeledes er navigationsmønstre genbrugt, så borgerne oplever en sømløs brugeroplevelse i hele borger.dk-systemet.

6.1.4 Genkendelighed med Virk

Mange borgere vil også i erhvervsmæssig sammenhæng skulle benytte Virks visningsklient til virksomheder, der er integreret med Mit Virk, og som skal fungere sømløst efter samme princip som beskrevet i forrige afsnit.

Digitaliseringsstyrelsen og Erhvervsstyrelsen har derfor samarbejdet om de overordnede designmønstre og opbygning af løsningerne, så brugerne af de to webklienter let vil kunne benytte begge.

6.1.5 Digital Post-appen

Digital Post-appens design er i vid udstrækning baseret på borger.dk, men da appen også kan benyttes af visse erhvervsbrugere (se afsnit 3.1), er appens brand i højere grad Digital Post-baseret end borger.dk-baseret, da dette ellers ville kunne virke ulogisk for virksomhedsbrugerne.

6.2 Sprog

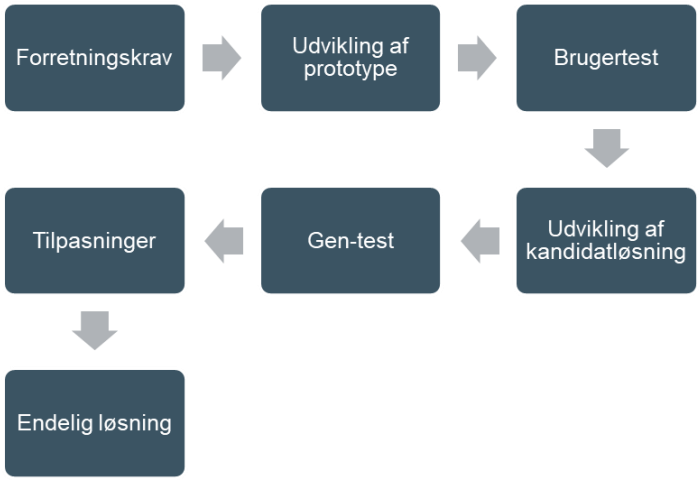
Alle tekster i klienterne er udarbejdet af brugervenlighedseksperter og borger.dk-redaktører, der har stor erfaring med borgerrettet kommunikation.

Teksterne er ligeledes, i vid udstrækning, koordineret med Virk for at sikre, at der benyttes ensartede termer på tværs af løsningerne.

6.3 Brugervenlighedstests

Begge løsninger er blevet brugervenlighedstestet af forskellige borgere og af flere omgange. Borgerne er blevet rekrutteret ved hjælp af Digitaliseringsstyrelsens brugerpanel[3], og de repræsenterer et bredt udsnit af befolkningen.

[3] https://digst.dk/digital-service/brugeroplevelse/brugerpanel/



Figur 2: Overordnet beskrivelse af design- og testproces i udviklingen af borger.dk's Digital Post-klienter. Forretningskravene giver input til en prototype, som brugertestes. På baggrund af testen foretages tilpasninger, som gentestes, indtil løsningerne er af en tilstrækkelig kvalitet.

Resultaterne fra brugertestene medfører, at klienterne er blevet tilpasset, så de er lettere at benytte. Tilpasningerne kan være i form af designmæssige ændringer af en skærm eller et flow, sproglige rettelser eller en kombination af begge dele.

Eksempelvis er begrebet "Digital Post-modtagere" (se afsnit 4.7) blevet omdøbt fra det oprindelige ord "Tillidspersoner" på baggrund af en brugertest.

Digitaliseringsstyrelsen og Erhvervsstyrelsen har løbende delt brugervenlighedsobservationer, som kan gavne både de borgerrettede klienter og den virksomhedsrettede klient.

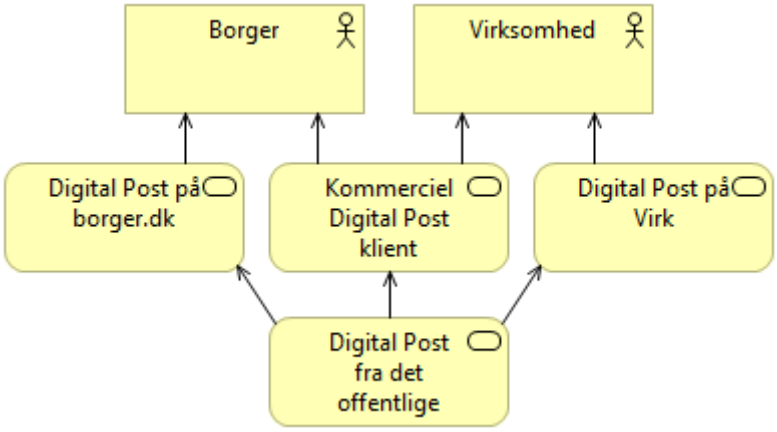
Billede 20: Billede af testopstilling fra en test af Digital Post-appen. Testpersonen interagerer med telefonen, og appen filmes og streames til observatører af testen.

7. Arkitektur

Digital Post-klienterne til borger.dk benytter den samme arkitektur. Formålet er at etablere en robust brugergrænseflade for Digital Post-løsningen.

7.1 Digital Post-arkitekturen

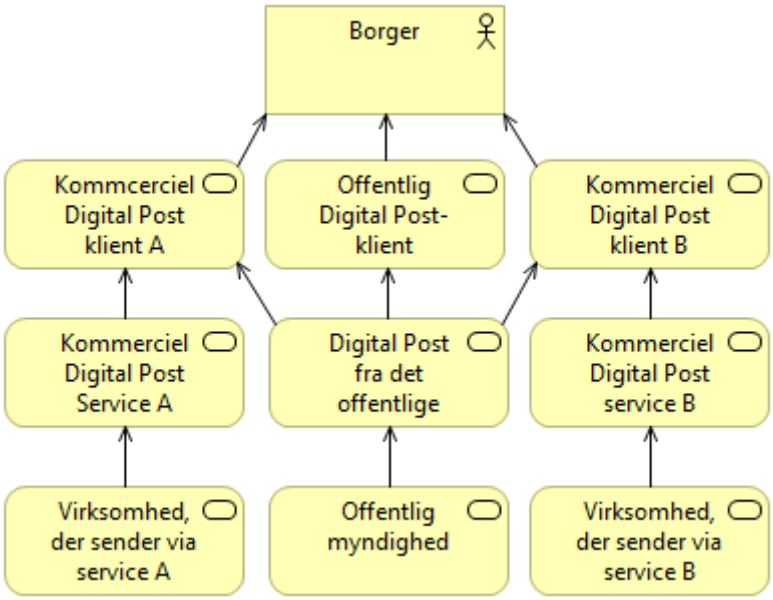
Digital Post-løsningen i sig selv har ingen borger- eller virksomhedsvendt brugergrænseflade. Denne opgave varetages i stedet af Digital Post-klienterne, der viser post fra Digital Post-løsningen.



Figur 3: Digital Post fra det offentlige er en service, der udstilles ved hjælpe forskellige klienter, der forsyner løsningen med en brugergrænseflade. Borger.dk-klienterne løser sammen med andre klienter denne opgave. Illustrationen er forsimplet, idet den ikke afspejler, at Digital Post-klienterne i visse tilfælde, som beskrevet i afsnit 3.1, også kan benyttes af virksomheder.

En borger (og en virksomhed) har mulighed for at se den samme Digital Post fra det offentlige i flere forskellige klienter.

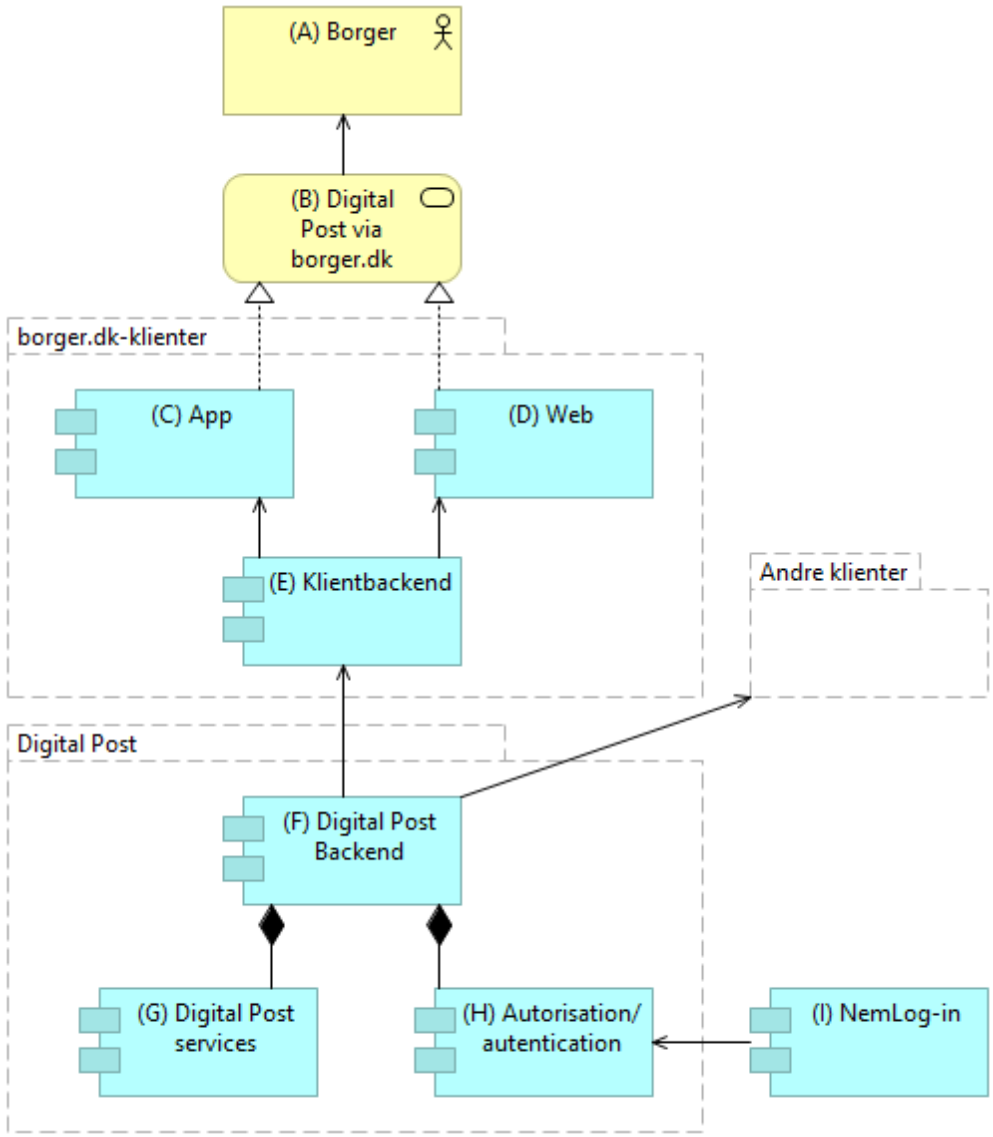
I de offentlige klienter fra borger.dk og Virk vises kun digital post fra offentlige myndigheder, mens kommercielle visningsklienter kan vise *både* digital post fra det offentlige og fra private afsendere. Forventeligt vil det dog være forskellige private afsendere, som de kommercielle visningsklienter viser digital post fra, hvilket er illustreret af nedenstående figur.



Figur 4: Digital post fra det offentlige kan vises i alle Digital Post-klienter. Kommercielle visningsklienter som e-Boks og Mit.dk kan også vise digital post fra virksomheder. Det vil dog være digital post fra forskellige virksomheder, som de kommercielle visningsklienter viser.

7.2 Arkitektur i borger.dk-klienterne

Den overordnede arkitektur for borger.dk's Digital Post-klienter er illustreret i den følgende figur.



Figur 5: En borger (A) bruger Digital Post-servicen (B). Dette realiseres af enten appen (C) eller webklienten (D). Begge applikationer serviceres af en klientbackend (E), der håndterer kommunikationen med Digital Post (F). Digital Post-backenden sørger for, at borgeren autentificeres (H) via NemLog-in (I) med NemID eller MitID.

Det er tilstræbt, at begge klienter er så tynde som muligt – og at al logik afvikles i en klientbackend, mens Digital Post-data fra forskellige Digital Post-services alene behandles, når borgeren benytter en af klienterne.

I de følgende afsnit gennemgås de væsentligste dele af arkitekturen.

7.3 Digital Post-appen

Appen er bygget med open source-rammeværket Flutter, der gør det muligt at udvikle appen til både Android og iOS med samme kodebase. Dette er valgt som alternativ til at lave to dedikerede mobilapplikationer til henholdsvis Android og iOS.

Flutter gør det i vid udstrækning muligt at genbruge kode og har en god basisunderstøttelse af webtilgængelighed.

Appen fungerer både på smartphones og tablets.

Appen kommunikerer ikke direkte med Digital Post, men derimod med klient-backenden (se afsnit 7.5), hvor logikken afvikles. Eneste undtagelse er, når borgeren logges ind i appen ved hjælp af en browser, idet denne kommunikerer direkte med Digital Posts autentifikationsserver (se afsnit 8.5).

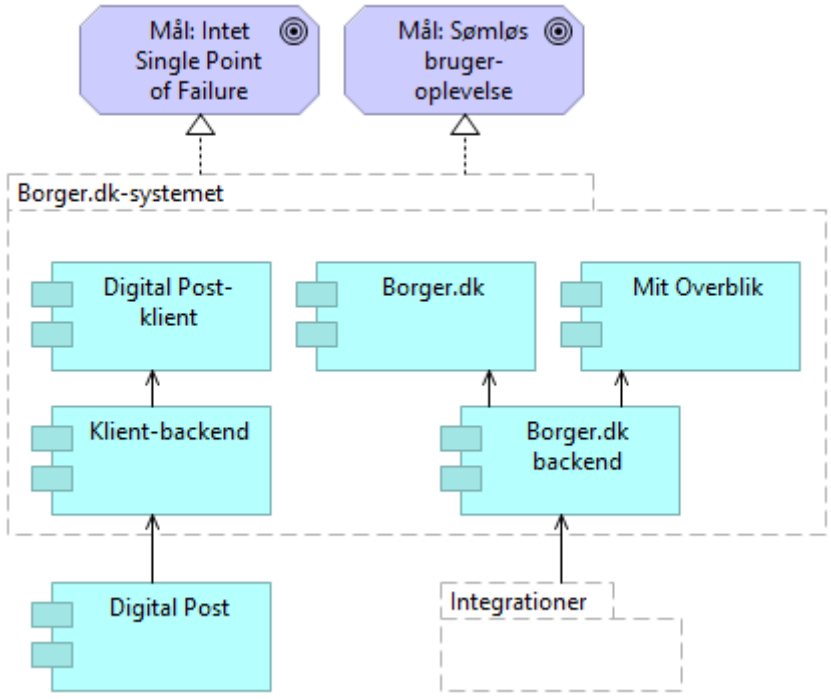
7.4 Webklienten

Webklienten er en såkaldt *Single Page Application (SPA)*, der er bygget med open sourcerammeværket Vue.js herunder Vuex, der er særligt egnet til applikationer som webklienten, hvor data hentes dynamisk på baggrund af brugerens input fremfor at genindlæse websiden, som det kendes fra typiske websteder. Store kommercielle e-mail-klienter, såsom Gmail og Outlook.com henter også data dynamisk efter samme mønster.

Webklienten tilgås i en browser på enten en computer eller mobil enhed, og det er tilstræbt, at den integrerer sømløst med borger.dk og Mit Overblik, som beskrevet i afsnit 6.1, men løsningerne kan fejle uden at påvirke hinanden. Dette sikrer, at ved et nedbrud på borger.dk-portalen, så vil Digital Post på borger.dk stadig fungere – og omvendt. For at sikre dette er komponenterne løst koblede og deler kun få ressourcer.

Webklienten er filbaseret og står alene for at vise brugergrænsefladen for borgeren. Som nævnt i afsnit 4.11 er webklienten optimeret til at virke hensigtsmæssigt i browsere både på computere og mobile enheder. Man behøver derfor ikke installere appen, hvis man ønsker at se sin Digitale Post fra det offentlige på fx en smartphone.

Webklienten kommunikerer derfor ikke direkte med Digital Post, men derimod med klientbackenden (se afsnit 7.5), hvor logikken afvikles. Dog med samme undtagelse som appen (se afsnit 7.3).



Figur 6: Systemarkitekturen realiserer målene om ikke at have et Single Point of Failure, som kan gøre begge løsninger utilgængelige på samme tid samtidigt med at målet om en sømløs brugeroplevelse understøttes.

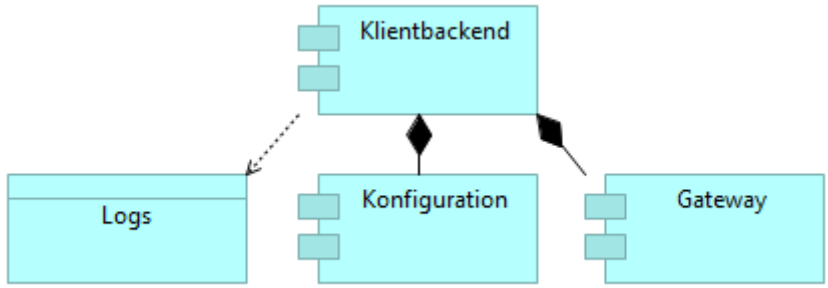
7.5 Klientbackend

Klientbackendens primære funktion er at håndtere kommunikationen med Digital Post og dermed agere gateway for webklienten og appen.

Klientbackenden håndterer derfor også sikkerhedslaget mellem klienterne og Digital Post, der baserer sig på OpenID Connect (se afsnit 7.6).

Komponenten varetager også kaldemønstre, konfigurationer og opbevarer de redaktionelle tekster, der vises i klienterne.

I klientbackenden opsamles også logs (se afsnit 8.3).



Figur 7: Klientbackenden, der består af konfiguration og en gateway samt logs, som der skrives til.

7.6 Autorisation og autentifikation

Autorisation og autentifikation af borgeren foregår i Digital Post.

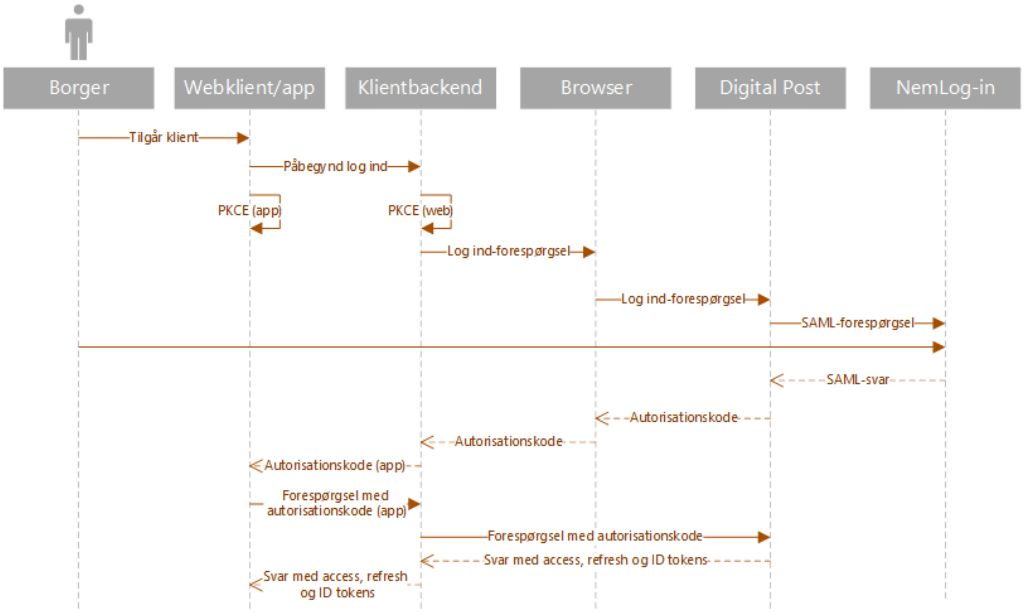
Når en borger tilgår en klient, skal Digital Post vide, hvem der tilgår ressourcen, og borgeren skal derfor identificere sig, og dette foregår ved en autentifikation. I praksis vil en borger, der eksempelvis tilgår webklienten, opleve at skulle logge ind med sit NemID eller MitID via NemLog-in.

Den autentificerede borger kan have forskellige autorisationer til at kunne tilgå forskelligt indhold i Digital Post. Dette kan eksempelvis dreje sig om læseadgang til en anden borgers postkasse.

7.6.1 OpenID Connect

Når en borger benytter en klient til at tilgå Digital Post, så benyttes OpenID Connect (OIDC) til adgangsstyring.

Når borgeren har foretaget en autentifikation med NemID eller MitID via NemLog-in, så udsteder Digital Post først en kode til klienten, som klienten kan veksle til en kortlevende *access token* (en adgangsbillet) hos Digital Post, som klienten skal benytte for at kunne få adgang til Digital Post. Klienten modtager også en længerelevende *refresh token*, der skal benyttes, hvis klienten skal benytte en ny *access token*. Derudover udstedes også en *ID token*, der indeholder information om, hvilken borger, der forsøger at tilgå Digital Post. Når både *access token* og *refresh token* er udløbet, skal brugeren autentificere sig via NemID eller MitID igen.



Figur 8: Overordnet OIDC-flow, som gennemløbes, når en borger logger ind i en klient.

Selvom både webklienten og appen begge benytter OIDC, er der en væsentlig forskel på, hvorledes borgeren oplever dette. Dette gennemgås i de følgende afsnit.

7.6.2 Session i webklient

Når borgere skal logge ind i offentlige webbaserede løsninger, benyttes NemLog-in. Når man logger ind i NemLog-in er der mulighed for at foretage et *single sign on* i andre tjenester, der er tilknyttet

NemLog-in – fx skat.dk og sundhed.dk. Tilsvarende foretages et *single sign out*, når en borger logger sig ud af en løsning i andre tjenester tilknyttet NemLog-in.

En borger kan derfor ikke være logget ind i webklienten uden også samtidigt at have en NemLog-in-session. Af sikkerhedshensyn udløber NemLog-in-sessioner, når brugeren har været inaktiv i et antal minutter.

Tilsvarende kan den *access token*, som webklienten har fået udstedt fra Digital Post udløbe. Hvis borgeren i dette tilfælde har en gyldig NemLog-in-session vil borgeren få udstedt en ny *access token*, ellers vil borgeren blive bedt om at logge ind i gen. NemLog-in-sessioner udløber efter en time, men kan fornyes, hvis borgeren stadig er aktiv.

7.6.3 Indrullering i app

I appen er det for en borger, som nævnt i afsnit 0, muligt at vælge, hvorvidt man ønsker at identificere sig hver gang, appen benyttes, eller om man ønsker at *indrullere* sig i appen, så den får adgang til at tilgå Digital Post i længere tid ved brug af pinkode eller biometri.

Hvis man vælger at logge ind hver gang, vil en session have samme levetid, som sessionen i webklienten, der er beskrevet i ovenstående afsnit.

Hvis en borger vælger den sidste mulighed, skal appen beskyttes med en pinkode og – hvis det ønskes – biometri om fx faceID. I dette tilfælde udnyttes, at et *refresh token* har en lang levetid, og at appen derfor i tilsvarende lang tid kan få udstedt gyldige *access tokens*.

Dette mønster kendes fra en lang række offentlige apps fx MinSundhed, Kørekort-appen og Coronapas-appen.

8. Sikkerhed, sikring mod misbrug og privacy

It-sikkerhed, sikring af brugerens privatliv og sikring mod misbrug er essentielt for Digital Posts succes, og det er derfor emner, som har meget høj prioritet.

Sikkerhed, sikring mod misbrug og beskyttelse af borgerens privatliv er emner, som er nært beslægtede, og som kan påvirke hinanden – og som også kan påvirkes af de samme faktorer.

I dette afsnit gennemgås en række af de tiltag, som er foretaget.

8.1 Sikkerhed

Sikkerhed drejer sig om at beskytte den tekniske løsning mod forskellige typer af angreb.

Som udgangspunkt går sikkerhed ud på at sikre løsningens:

- Fortrolighed
- Integritet
- Tilgængelighed[4]

Fortrolighed betyder, at informationer skal beskyttes mod uautoriseret adgang eller videregivelse, således at uvedkommende ikke kan gøre sig bekendt med oplysningerne. Fortrolighed er derfor også tæt relateret til at sikre borgernes privatliv, som beskrives i afsnit 8.8.

Integritet betyder, at informationer skal beskyttes mod uautoriseret ændring eller ødelæggelse, og dermed sikre løsningen mod at fx Digital Post-beskeder manipuleres. Dette kan derfor også være relateret til sikring mod misbrug, som beskrives i afsnit 8.7

Tilgængelighed betyder, at informationer skal beskyttes mod en uautoriseret adgangsbegrænsning for personer, som har retmæssig adgang (f.eks. nedbrud så systemer ikke er tilgængelige). Det kan eksempelvis være DDOS-angreb, hvor serverne overbelastes af kald.

8.2 Driftsmiljø og processer

Driftsmiljøet, herunder infrastruktur og processer, er baseret på ISO-27001 og *best practice*.

8.2.1 Privileged Access Management

Driftsmiljøet benytter Privileged Access Management (PAM), der er en metodik til at sikre og overvåge adgange for brugere, der har særlige privilegier.

8.2.2 Overvågning

Alle løsninger bliver konstant overvåget, og i overvågningen indgår detektion af DDOS[5]-angreb.

[4] https://www.datatilsynet.dk/media/7697/vejledende-tekst-om-risikovurdering.pdf
[5] Distributed Denial Of Service

8.2.3 Processer

Der er faste processer, der følger et årshjul. Disse inkluderer eksempelvis løbende adgangstjek, penetrationstests, overholdelse af svar- og oppetider samt test af disaster recovery-plan.

8.3 Sikkerhed i klientbackenden

Klientbackenden er designet til at være *stateless*. Det betyder, at den ikke holder en tilstand om borgeren, der benytter den, fx en serversession.

Det betyder også, at den ikke indeholder persisteret information om borgerens identitet eller eksempelvis persisterede Digital Post-beskeder. Der caches heller ikke persondata eller personhenførbar information ud over IP-adressen, der logges (se næste afsnit).

Klientbackendens API'er beskyttet efter principperne i *OWASP Application Security Verification Standard (ASVS)*,[6] der er *best practice* til at sikre webapplikationer.

Derudover overholder Klientbackend OIDC-standarden, som nævnt i afsnit 7.6, med en OIO-profil, som Digitaliseringsstyrelsen har udgivet.[7]

Certifikater og API-sikkerheden skal have en A+-rating hos SSLLabs[8], der er den højeste mulige rating. SSLlabs er et online testværkstøj, der tester og vurderer konfigurationer af webservere ud fra et sikkerhedsmæssigt perspektiv samt tester mod kendte sårbarheder – og derefter rater disse.[9]

8.3.1 Logning

Brugerens identitet logges ikke i forbindelse med logning af hændelser til fejlfinding. Der logges heller ikke indhold fra borgernes postkasse fx Digital Post-beskeder.

Klientbackenden logger hændelser i applikationen fx fejl. Log-meddelelser kan forbindes ved hjælp af et korrelations-ID (se afsnit 8.4).

Webserveren har, som det er standard for webapplikationer, også en log – i dette tilfælde en IIS-log, der fx logger IP-adresse og *User-agent*.

Log-data i klientbackenden opbevares i maksimalt 90 dage.

Digital Post indeholder en aktivitetslog, der registrerer handlinger, som borgere foretager på tværs af alle visningsklienter. Denne log er en del af Digital Post-løsningen (se afsnit 0) og ikke borger.dk's klienter, men den bliver udstillet i webklienten.

8.4 Sikkerhed i webklienten

Sikkerhedsniveauet i webklienten er ligeledes baseret på OWASP ASVS.

Webklienten er ligesom klientbackenden designet til at være *stateless* og opbevarer derfor heller ikke information om borgerne eller Digital Post-beskeder ud over kortvarigt i browseren – fx mens et dokument er åbent. Dog benyttes der sessionscookies bl.a. til at verificere en brugers adgang.

Informationen findes i browseren, så længe borgeren har en aktiv session med Digital Post. Når sessionen udløber, fx ved timeout eller ved at borgeren logger ud, så fjernes informationen i

[6] https://owasp.org/www-project-application-security-verification-standard/
[7] https://digst.dk/media/24669/oio-oidc-profiles-v091.pdf
[8] https://www.ssllabs.com/ssltest/analyze.html?d=post.borger.dk
[9] https://github.com/ssllabs/research/wiki/SSL-Server-Rating-Guide

browseren. Eneste undtagelse er følgende cookies: cookie-samtykke, kommunevalg samt statistikcookies. Sidstnævnte sættes dog kun, hvis borgeren accepterer det.

8.4.1 Hærdning af webklienten

8.4.1.1 Cross Site Request Forgery

Der kan ikke laves CRUD-operationer[10] i webklienten fra eksterne kilder, hvilket forhindrer *Cross Site Request Forgery* (CSRF), som er en sårbarhed, der kan være i webløsninger, hvor en angriber lokker en bruger til at afvikle uønskede kommandoer på en hjemmeside, som denne er logget ind på fx fra en ekstern (ondsindet) hjemmeside.

8.4.1.2 Cookies

Cookies er som udgangspunkt *samesite*-cookies og *http-only*, hvilket betyder, at cookies ikke kan udlæses fx fra et ondsindet javascript. *Samesite* medfører, at der ikke kan sættes eksterne cookies i webløsningen. Eneste undtagelser er en cookie, der af CSRF-hensyn sættes for at bevise, at en forespørgsel kommer fra klientens domæne, en cookie med borgerens cookie-samtykke, en cookie der indeholder et eventuelt kommunevalg, samt en cookie med et korrelations-ID og – hvis borgeren accepterer det – en statistikcookie.

8.4.1.3 Sikkerhedsheaders

Der er ligeledes definerede hærdede sikkerhedsheaders ud fra et *least priviledge* -princip fx *Content Security Policy* (CSP) og *Cross Origin Ressource Sharing* (CORS).

8.4.2 Autentifikation

For at få adgang til webklienten skal borgeren logge ind med sit NemID eller MitID via NemLog-in som ved de fleste andre offentlige løsninger som fx skat.dk eller sundhed.dk

8.5 Sikkerhed i appen

Sikkerhedsniveauet i webklienten er baseret på *OWASP Mobile Application Security Verification Standard*.[11]

Appen er ligesom webklienten *stateless* og indeholder heller ikke persisteret information om borgernes identitet uden for brugernes egne enheder. Alt gemt data på brugernes enheder fx *refresh* og *access tokens* er krypteret og med automatisk tidsudløb.

8.5.1 Sikker autentifikation ved indrullering

Som beskrevet i afsnit 7.6 foretages indrulleringen på baggrund af NemID eller MitID via NemLog-in.

Selve autentifikationen sker i en browser inde i appen. Dette sikrer, at appen ikke får adgang til brugerens log ind-informationer. Tilsvarende kan browseren i appen heller ikke få adgang til borgerens Digital Post-beskeder.

Når en borgeren er logget ind, behøver denne ikke logge på med NemID i en periode på seks måneder.

8.5.2 Oplåsning af app

Digital Post-appen kræver oplåsning af appen med biometri eller indtastning af pinkode, så det kun er brugeren selv, der kan åbne appen, som dermed beskyttes mod utilsigtet adgang. Hvis borgeren ikke er indrulleret skal der foretages en fornyet autentifikation med NemID eller MitID.

[10] Create (skriv), Read (læs), Update (ændr), Delete (slet)
[11] https://owasp.org/www-project-mobile-security-testing-guide/

8.5.3 Hærdning af appen

I forbindelse med udvikling af appen har indgået overvejelser om ibrugtagning af teknikker, der kan hærde appens sikkerhed. Disse overvejelser inkluderer bl.a.:

8.5.3.1 Obfuskering (tilsløring) af appens kodebase

Ved at obfuskere koden, besværliggøres det for offentligheden at læse appens kildekode med henblik på fx at identificere indkodede nøgler og API-endepunkter, men det kan ikke forhindres.

Appens sikkerhedsmodel beror dog ikke på hemmeligholdelse af kildekoden men på den kryptografiske model, der ikke umiddelbart påvirkes af adgang til kildekoden.

Obfuskering er derfor blevet fravalgt.

8.5.3.2 Root Detection

Ved at implementere *root detection* gøres det muligt for appen at reagere på om brugerens telefon er "rootet" eller "jailbreaket", hvilket muliggør, at der kan installeres kode på telefonen udenom appstores, hvilket kan udgøre en sikkerhedsrisiko.

Når *root detection* er aktiv kan det forhindres, at borgeren kan benytte appen, eller at man kan advare borgeren om sikkerhedsrisikoen ved, at en ondsindet app på borgerens rootede telefon opfanger data fra Digital Post-appen.

Root detection er implementeret i appen ved, at borgeren advares med en dialog, men brug af appen forhindres ikke. Det skyldes, at *root-detection* kan medføre falske positiver, hvorfor enkelte borgere ellers ville kunne opleve uretmæssigt ikke at kunne benytte appen.

8.5.3.3 SSL pinning

Med *SSL pinning* sikres det, at appen validerer, at den backend, den kommunikerer med, rent faktisk også er den forventede backend og ikke en anden ondsindet backend, der udgiver sig for at være den rette.

Dette medvirker bl.a. til at forhindre *man-in-the-middle*-angreb.

SSL-pinning er ligeledes implementeret i appen.

8.6 Ekstern sikkerhedstest

Et eksternt sikkerhedsfirma har foretaget en test af begge klienter, klientbackenden samt det driftsmiljø, hvor løsningerne afvikles for at verificere og afprøve de sikkerhedsmæssige tiltag, der er foretaget.

Sikkerhedsfirmaet har ligeledes rådgivet om yderligere sikkerhedstiltag.

Det overordnede formål med testen har været at sikre, at der tages tilstrækkelige tiltag til netop at sikre fortrolighed, integritet og tilgængelighed.

Testen har bl.a. beskæftiget sig med og taget udgangspunkt i velafprøvede metodikker som fx OWASP:

- Gennemgang og sårbarhedsscanninger af løsningens backend og infrastruktur herunder logisk arkitektur, processer, driftskonti, kommunikationskanaler, tilgængelighed og logning.
- Analyse med henblik på at identificere logiksårbarheder og applikationsspecifikke problemer i de to klienter.
- Analyse af beskyttelse af data i alle stadier af løsningen – både når data er i bevægelse eller opbevares baseret på en *"least privilege"*-model.

- Gennemgang af dataforløb i løsningen både internt i løsningens komponenter og mellem komponenterne.

8.7 Sikring mod misbrug

Sikring mod misbrug handler om at beskytte borgerne mod, at deres oplysninger relateret til Digital Post kan misbruges.

I det følgende nævnes nogle eksempler på de tiltag, der er foretaget for at modgå misbrug af borgernes digitale post.

8.7.1 Lukket kredsløb

Som nævnt i afsnit 0 er Digital Post et lukket kredsløb. Dette er i meget høj grad med til at sikre borgerne mod misbrug.

Borgere kan være sikre på, at den Digital Post, som de modtager fra myndigheder rent faktisk kommer fra de pågældende myndigheder, fordi det kun er oprettede myndigheder, der kan sende Digital Post-beskeder.

8.7.2 Digital Post-modtagere

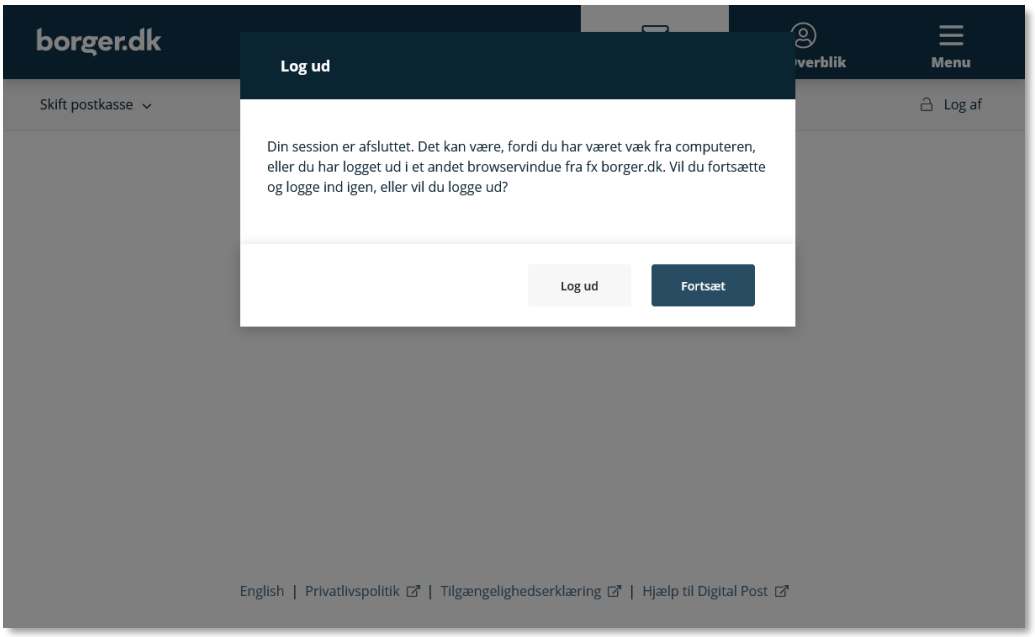
Tilsvarende kan man som borger udelukkende få videresendt beskeder fra andre borgere, hvis man på forhånd har godkendt, at man vil modtage beskeder fra den pågældende borger og dermed blive "Digital Post-modtager".

Det medvirker til at sikre mod *phishing*-lignende angreb i Digital Post-løsningen, og mod at en borger kan modtage uønskede beskeder fra andre borgere.

8.7.3 Timeout af sessioner

Hvis en borger, der benytter webklienten, ikke foretager nogle handlinger, så vil borgerens session udløbe efter tyve minutter. En session har desuden en maksimal længde på én time.

Tidsintervallet er en afvejning mellem, at en borger skal kunne have tilstrækkelig tid til at læse en Digital Post-besked uden at blive logget ud af løsningen – og samtidigt bl.a. mindske risikoen for, at en borger, der benytter en offentlig pc på fx et borgerservicecenter eller bibliotek, og som ikke får logget ud af løsningen, ved et uheld eksponerer sine data til den næste person, der benytter pc'en.



Billede 21: Når en session er udløbet, vises en besked om dette. Samtidigt fjernes alt indhold i browseren, så det ikke er muligt at se postkassen længere.

Smartphones er typisk mere personlige enheder, der også ofte er beskyttet med en pinkode eller biometri. Alligevel kræver appen, at borgeren skal indtaste sin pinkode til appen eller benytte biometri, når appen har været i baggrunden i ti minutter.

8.7.4 Download af filer / forhåndsvisning

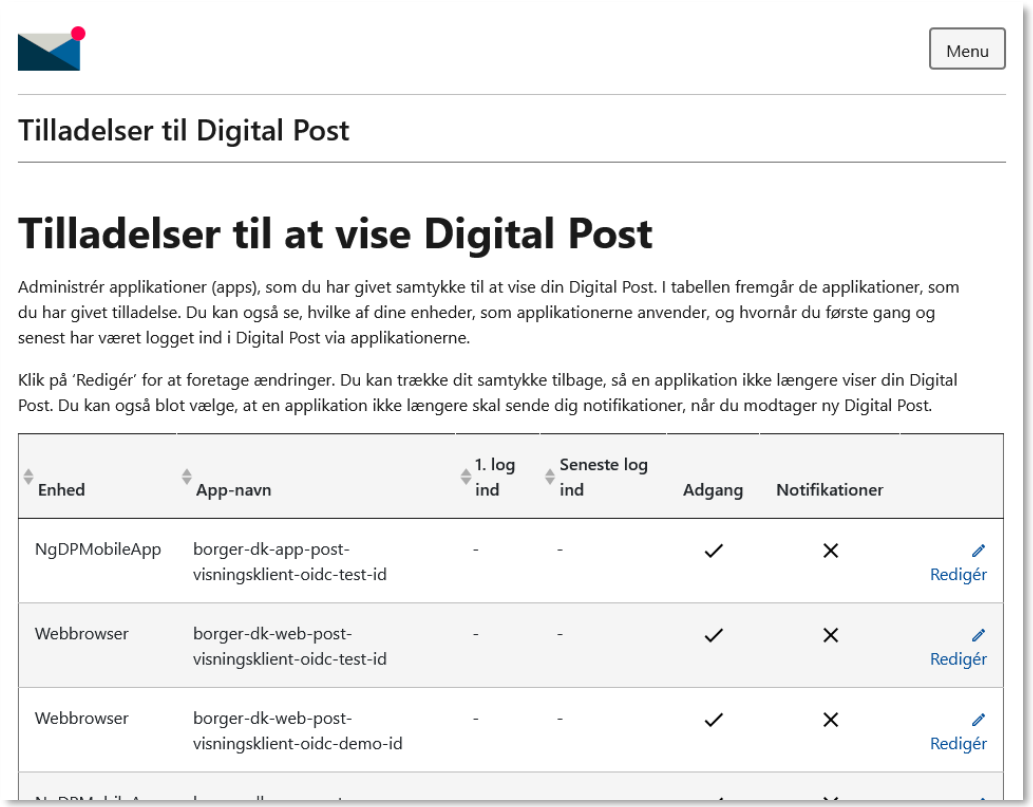
Når en borger ønsker at downloade et dokument fra en Digital Post-besked, bliver borgeren gjort opmærksom på, at det kan være forbundet med risici, da filen kan blive lagret på den pågældende enhed, fx i en mappe med overførsler, hvorefter andre kan få adgang til den. Dette vil i nogle tilfælde kunne ske på delte computere.

Billede 22: Dialog, som gør borgerne opmærksomme på, at man skal være forsigtig, hvis man vælger at downloade et dokument fra en Digital Post-besked.

8.7.5 Tilbagetrækning af app-adgange

Borgere, der eksempelvis får stjålet deres telefon eller har fået en ny telefon, kan fjerne appens adgang til Digital Post, så der ikke længere kan logges ind med pinkode eller biometri på den pågældende enhed.

Denne proces foregår via indstillingsuniverset i webklienten, men det er en løsning, der stilles til rådighed af Digital Post, da den vedrører både de offentlige og kommercielle visningsklienter.



Billede 23: Digital Posts selvbetjeningsløsning, hvor borgere kan fjerne apps, som de har givet adgang til.

8.8 Privacy

Privacy omhandler at beskytte borgernes privatliv og er helt essentielt i løsningen. Der er derfor en tæt kobling mellem privacy og sikring mod misbrug, hvorfor det også i vid udstrækning er de samme foranstaltninger, der er relevante.

Digital Post-klienterne er udarbejdet ud fra en *privacy by design*-tankegang, hvor de bærende principper er, at:

- Behandle og opbevare så få data som muligt i løsningens dele.
- Give borgeren kontrollen over de data, som vises, så de ikke tilgås af andre.
- Undgå personhenførbar sporing

I det følgende beskrives en række af de privatlivsbeskyttende tiltag, der er foretaget for at opnå dette.

8.8.1 Opbevare så få data som muligt

Klienterne og klientbackenden behandler kun de data, som borgeren gennem sin interaktion med brugergrænsefladen selv anmoder om. Når en borger fx beder om at få fremvist en mappe med digital post, så hentes mappen på det pågældende tidspunkt, hvor borgeren trykker på et element i brugergrænsefladen.

Klientbackenden lagrer derfor heller ikke data om borgernes Digital Post-beskeder og lignende, men agerer alene gateway mellem klienterne og Digital Post.

I klienterne, som er under borgerens kontrol, lagres ligeledes så få data som overhovedet muligt. I webklienten lagres, kun de data, som borgeren kan se samt sessionscookies, og kun indtil borgeren afslutter sessionen. Eneste undtagelse herfra er eventuelle statistikcookies og cookiesamtykke samt kommunevalg, som borgeren dog aktivt skal godkende via cookiebanneret (se også afsnit 8.4).

I appen lagres data, der muliggør, at borgere kan logge ind med pinkode eller biometri (se afsnit 7.6) og eventuelt borgerens navn, hvis borgeren vælger at indrullere sig i appen.

8.8.2 Give borgeren kontrollen over data

I den udstrækning det kan lade sig gøre, benyttes der forhåndsvisning af data i appen, som beskrevet i afsnit 8.7.

Dette er med til at sikre, at borgernes data ikke uforvarende bliver mulige at tilgå for uvedkommende – fx hvis de downloades til en mappe på en delt pc.

8.8.3 Undgå personhenførbar sporing

Brugerens identitet og data logges ikke i forbindelse med logning af hændelser til fejlfinding.

Det er værd at bemærke, at selve Digital Post-løsningen, som nævnt i afsnit 8.3, indeholder en aktivitetslog, der viser en borgers aktivitet på tværs af de forskellige visningsklienter.

Digitaliserings-
styrelsen