SUNDHEDSDATA-
STYRELSEN

DIGITALISERINGSSTYRELSEN

Whitepaper om coronapas-appen

Version: 29. maj 2021

2021

Indhold

1. Resumé

Dette whitepaper om coronapasset giver en indføring i coronapassets formål, funktioner, opbygning samt sikkerheds- og privacy-mæssige aspekter af løsningen.

Coronapasset bliver udviklet på baggrund af de politiske aftaler om genåbningen af Danmark 2021.

Coronapasset skal muliggøre, at borgere kan fremvise et gyldigt coronapas, der kan tilpasses til forskellige kontrolsituationer. Som udgangspunkt vises blot, at coronapasset er gyldigt, men borgeren kan vælge at tilføje navn og fødselsdag til visningen.

Det skal samtidigt være muligt for en kontrollør at få verificeret, at de fremviste oplysninger er korrekte ved at kunne scanne en QR-kode, der er dannet på baggrund af data, som er digital signeret med en signatur, der er ejet af myndighederne.

Coronapasset skal være let at benytte og let at forstå for både borgere, der fremviser det, og for kontrollanter.

Coronapasset kommer til at fungere både indenrigs og udenrigs. Den danske løsning kommer til at virke med de øvrige EU-landes løsninger. Dette er reguleret af den kommende EU Digital COVID Certificate -forordningen (DCC). Når løsningen bruges i EU-regi benyttes et aftalt og mere detaljeret datasæt, som er aftalt af landene og reguleret i forordningen.

Sikkerhedsarbejdet i løsningen har stort fokus og beskæftiger sig med alle dele af løsningen. En internationalt anerkendt virksomhed foretager sikkerhedstests og undersøgelser samt rådgiver på den baggrund myndighederne og leverandørerne til løsningen.

I appen er der flere tiltag, der modvirker misbrug, fx bevægelige dele, der reagerer på telefonens gyroskop, QR-koder, der kan verificeres og begrænsninger af, hvor mange enheder, der kan benyttes på samme tid.

Sikkerhed og tiltag mod misbrug skal dog opvejes mod behovet for, at løsningen er brugervenlig samt respekten for borgerens privatliv. Sidstnævnte sikres i appen ved at give borgeren maksimal kontrol over visningen af data, minimere mængden af data og sikre, at data ikke opbevares i systemer, der ligger uden for det i forvejen meget sikre Sundhedsdatanet.

Løsningen baserer sig på allerede eksisterende it-systemer fx den Nationale Serviceplatform og kildesystemerne MiBa og DDV, der leverer test- og vaccinationsinformation.

Foruden appen og en backend til appen etableres der en særlig webservice, CBS, der har til formål at skåne kildesystemerne for det meget store antal brugere, som vil lave kald efter data til coronapas-appen.

Løsningens arkitektur er designet til at kunne fungere med det system, der leveres af EU-kommissionen, som led i EU Digital COVID Certificate-forordningen.

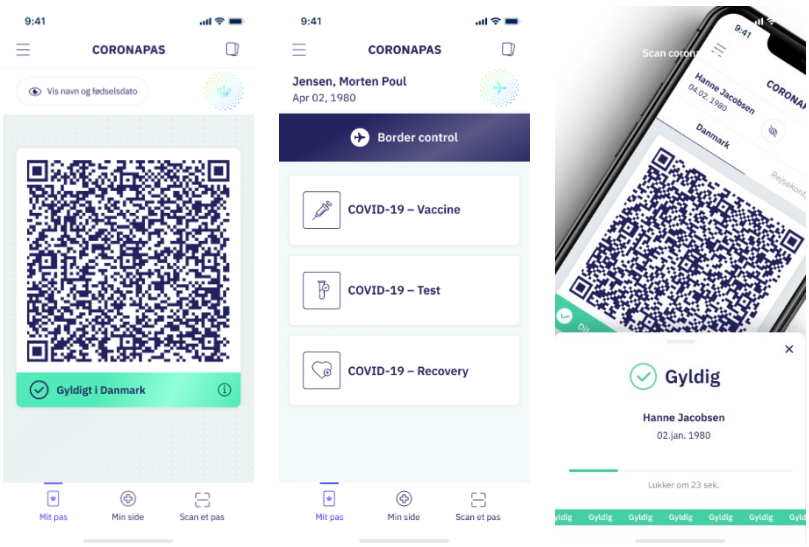

Illustration: Centrale skærmbilleder fra coronapas-appen. Fra venstre mod højre: 1) hovedskærm i indenrigsvisning. 2) Oversigt over certifikater, som kan bruges ved rejse. 3) Scanningsresultat, der vises til kontrollant.

2. Indledning

Formålet med dette whitepaper er at beskrive coronapassets funktionalitet, data, opbygning samt sikkerheds- og privacymæssige aspekter ved løsningen.

Coronapassset udvikles af Sundhedsdatastyrelsen, Digitaliseringsstyrelsen, Statens Serum Institut og Sundhedsministeriet.

Coronapas-appen er en digital løsning til borgernes mobiltelefoner, der giver mulighed for at fremvise et gyldigt coronapas både indenrigs og udenrigs.

I dette whitepaper gennemgås formålet med coronapasset herunder de politiske aftaler, som det er baseret på i afsnit 3. Disse formål er rammesættende for coronapassets funktioner, som beskrives i det følgende afsnit 4, for henholdsvis borgere, der fremviser et coronapas og kontrollanter, der foretager kontroller.

Det data, som løsningen behandler henholdsvis indenrigs og udenrigs gennemgås i afsnit 5

De sikkerhedsmæssige aspekter i løsningen er meget væsentlige og behandles i afsnit 6. De dækker både over it-sikkerhed, sikring mod misbrug og borgerens beskyttelse af borgerens privatliv.

Til sidst gennemgås løsningens overordnede it-arkitektur i afsnit 7.

Dette whitepaper er udarbejdet i forbindelse med udviklingen af coronapasset. Løsningen beskrives, som den vil se ud ved lanceringen, men der vil ske løbende videreudvikling – ligesom der tages forbehold for, at EU Digital COVID Certificate-forordningen ved udarbejdelsen af dette whitepaper endnu ikke foreligger i en endeligt vedtaget udgave.

3. Formålet med et coronapas

Det er politisk besluttet at indføre krav om coronapas, der skal bidrage til at fastholde epidemikontrollen i Danmark. Coronapasset giver mulighed for, at store dele af erhvervs- og kulturlivet kan genåbne tidligere, end hvad der ellers var muligt. Samtidigt er coronapasset en vigtig forudsætning for rejser til og fra Danmark.

3.1 Politiske aftaler

I *Rammeaftale om plan for genåbning af Danmark*[1] blev aftalepartierne[2] den 22. marts 2021 enige om, at et coronapas vil bidrage til epidemikontrollen, så store dele af erhvervene og kulturlivet kan genåbne tidligere end ellers.

Coronapasset skal vise, om borgeren er færdigvaccineret, har overstået infektion eller er testet negativ indenfor 72 timer (både PCR-og antigen-test). Børn under 15 år vil være undtaget.

Coronapasset skal virke ved turisme, rejser og sikre den fri bevægelighed i EU ved hjælp af EU Digital COVID Certificate -forordningen (DCC), som omtales nærmere i afsnit 3.4.

Det blev aftalt i rammeaftalen, at liberale serviceerhverv kunne genåbne fra d. 6. april med krav om coronapas,

I *Aftale om udmøntning af genåbning per 21. april 2121*[3] fastlagde aftalepartierne, hvilke yderligere anvendelsesområder, der kunne genåbne med krav om coronapas. Det fremgår af aftalen, at der kræves coronapas på bl.a. museer, biblioteker, indendørs servering på restauranter og cafeer, fodboldkampe i superligaen mv.

I *Aftale om udmøntning af genåbning pr. 6. maj 2021* enedes aftalepartierne om, at konferencer, spillesteder, teatre og biografer og lignende øvrige lokaler, hvor der udøves kulturaktiviteter kunne åbnes med coronapas. Desuden åbnedes – med coronapas – for indendørs idræt for voksne over 18 år.[4]

I *Aftale om udmøntning af genåbning pr. 21. maj 2021* blev der aftalt en række yderligere genåbninger med krav om coronapas, herunder resterende idræts-, fritids-og

[1] https://www.stm.dk/media/10258/rammeaftale-om-plan-for-genaabning-af-danmark.pdf
[2] Regeringen (Socialdemokratiet) og Venstre, Dansk Folkeparti, Socialistisk Folkeparti, Radikale Venstre, Enhedslisten, Det Konservative Folkeparti, Liberal Alliance og Alternativet
[3] https://www.justitsministeriet.dk/wp-content/uploads/2021/04/Aftale-endelig.pdf
[4] https://www.justitsministeriet.dk/wp-content/uploads/2021/05/Aftale-6.-maj-2021-ENDELIG.pdf

foreningsaktiviteter, indendørs faciliteter i forlystelsesparker, zoo mv. Partierne er derudover enige om, at reglerne for gyldig dokumentation i coronapas lempes, så man som udgangspunkt 14 dage efter første vaccinationsstik kan anvende dokumentation herfor som coronapas.

3.2 Ikke digitale borgere

Aftalepartierne er enige om, at færdig-vaccinerede borgere, der ikke anvender de digitale løsninger, skal have en let og ubureaukratisk adgang til at dokumentere deres vaccination.

Ligeledes kan borgere, der ikke anvender de digitale løsninger, fortsat anvende fysisk dokumentation for en negativ test.

Det er i dag muligt at få fysisk dokumentation for negativ antigentest hos de private udbydere. Det er et krav, at disse leverandører tilbyder fysisk dokumentation til borgere, som ønsker det. Der arbejdes desuden på en løsning med hensyn til svar på PCR-test. Derudover findes der en fuldmagtsløsning på sundhed.dk, som gør det muligt for pårørende eller værger at se testsvar og hente COVID-19 testpas. Det gælder både svar fra PCR- og antigentest.

Færdigvaccinerede borgere, der er fritaget fra digital post, får tilsendt vaccinationsdokumentation (vaccinationspas) direkte via fysisk post. Færdigvaccinerede borgere kan derudover ringe og bestille et printet vaccinationspas hos supporten hos sundhed.dk.

3.3 Solnedgangsklausul

Aftalepartierne aftaler i august 2021 hvilke konsekvenser det skal have for coronapasset, at alle borgere, der ønsker det, er færdigvaccinerede. Aftalepartierne er således enige om en "solnedgangsklausul" på anvendelsen af coronapasset til andre aktiviteter end turisme og rejser.

Aftalepartierne vil desuden i maj og juni 2021 drøfte erfaringerne med anvendelsen af coronapasset og tage stilling til dets fortsatte omfang og brug.

Med *Aftale om udmøntning af genåbning pr. 21. maj 2021* blev partierne enige om, at der skal udarbejdes en plan for udfasning af coronapasset begyndende primo juni. Der igangsættes en gennemgang af de områder, hvor der i dag er krav om coronapas med udgangspunkt i de tre følgende bærende hensyn; 1) hensynet til smitterisici, 2) de givne aktiviteters medvirken til at understøtte hyppig testning samt 3) praktiske og logistiske hensyn.

3.4 EU og rejse

Den 17. marts præsenterede Kommissionen et forordningsforslag, EU Digital COVID Certificate (DCC)[5], for at sikre den fri bevægelighed under Covid-19 ved hjælp af et rammeværk, der skal gøre medlemslandenes coronapas interoperable.

DCC gør det muligt for en borger ved ind- og udrejse at præsentere verificérbare data om vaccination, (negativ) test eller immunitet på grund af overstået sygdom.

De deltagende lande forpligter sig til at anerkende korrektheden af certifikater udstedt af de øvrige lande, men det er op til det enkelte land at fastsætte kravene til indrejse i det pågældende land. Et coronapas, der er gyldigt i land A, er dermed ikke per automatik gyldigt i land B.

Lande, der deltager i samarbejdet, er forpligtet til at signere data i coronapasset med en digital signatur, ejet af en offentlig sundhedsmyndighed, der kan verificereres af de øvrige lande – i praksis ved at scanne en QR-kode i passet (se afsnit 7.2). Samtidigt er der mellem landene aftalt et fælles datasæt, der udtrykker de nødvendige metadata, som er nødvendige for at det kan afgøres, om en borger kan foretage indrejse i et land (se afsnit 5.3).

Danmark deltager i samarbejdet, og har indgået i pilotarbejdet med en række øvrige lande.

3.5 Sammenhæng mellem coronapas-app og coronapas på Sundhed.dk og i MinSundhed-appen

Fra ultimo marts har coronapas i appen "MinSundhed" og på hjemmesiden sundhed.dk fungeret som funktionelle, men simple coronapas. Da passene på sundhed.dk og i MinSundhed-appen blev udviklet, var formålet at give danskerne mulighed for at dokumentere negativ test og vaccination ved rejser på tværs af landegrænser, hvor der kan være forskellige krav om dokumentation ved indrejse. På den baggrund blev det besluttet, at der skulle fremgå en række oplysninger på passene, der gør passene fleksible ift. de forskellige krav.

Den nye og kommende coronapas-app er udviklet med særligt fokus på brug i Danmark, og derfor er appen målrettet enkel og hurtig fremvisning og kontrol af coronapasset i Danmark, og viser ikke nogle øvrige data om borgeren, når appen bruges i Danmark.

---

[5] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0130. Det skal bemærkes, at forordningsudkastet skiftede navn den 21. maj 2021 fra Digital Green Certificate til EU Digital COVID Certificate. Sidstnævnte betegnelse benyttes i dette whitepaper.

Efter lancering af appen kan man fortsat bruge print-selv-pas fra sundhed.dk og coronapas i MinSundhed-appen, hvis man ønsker det. Derudover vil der med den kommende EU-forordning blive et krav, at medlemslandene skal stille papirbaserede certifikater til borgere, der ønsker at bruge det frem for digitale løsninger, og derfor skal det sikres, at print-selv-passene på sundhed.dk også kommer til at leve op til EU-kravene.

4. Funktionalitet

Coronapasset skal understøtte de aftalte formål. Samtidigt skal det være let, trygt og sikkert for borgerne at benytte passet, mens kontrol af passet skal kunne gøres hurtigt og med vished for, at den fremviste information er korrekt.

4.1 Coronapassets overordnede funktionalitet

Coronapas-appen kan installeres på Android-telefoner (med styresystem Android 5 eller højere) og iPhones (med styresystem iOS 9 eller højere), samt professionelle scannere/imagers af mærkerne Zebra og Newland. Appen udvikles ud fra et kriterium om, at den skal kunne fungere på så mange telefoner som muligt, herunder også ældre telefoner. Appen benytter ikke bluetooth eller NFC-teknologi og er derfor ikke afhængig af tilstedeværelsen af disse teknologier på brugerens telefon.

Det er en væsentlig forudsætning, at appen er let at benytte og let at forstå for borgerne, og at den samtidigt føles tryg og sikker at benytte. Således skal der tages hensyn til borgernes privatliv, så borgerne kun skal vise den allermest nødvendige information til kontrollanter.

For kontrollanter skal det sikres, at det er let at foretage inspektion af coronapasset, og det skal indrettes, således det understøtter forskellige former for kontrol fx visuel inspektion eller scanning og med forskellig former for data fx med og uden navn og fødselsdag på borgeren.

Det er ligeledes et mål at sikre, at appen er så tilgængelig som muligt for personer med handicap og funktionsnedsættelser.

I brugergrænsefladen i appen er indlejret to animerede vandmærker, der reagerer på telefonens gyroskop. Denne funktion beskrives nærmere i afsnit 6.4.

I de følgende afsnit gennemgås coronapasset funktioner i detaljer.

4.2 Brugeroplevelse som borger

Introduktion til coronapas

Når en borger benytter appen første gang, føres denne gennem et introduktionsforløb på engelsk eller dansk, der forklarer den væsentligste funktionalitet i appen.

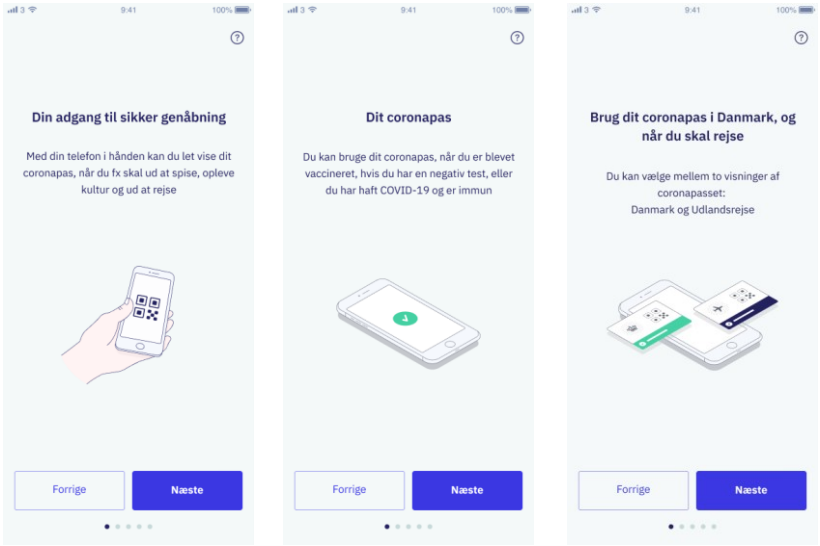

Illustration: Eksempler på skærme i introduktionsforløbet.

Samtykke

Borgeren skal afgive et samtykke, før appen kan ibrugtages.

Oprettelse af coronapas

Borgeren opretter bestilling til sit coronapas og afslutter introduktionsforløbet ved at logge ind med NemID[6].

Når borgeren er logget ind med NemID, skal der vælges en pinkode, som kan beskytte appen. Borgeren kan også tilvælge biometrisk beskyttelse, hvis dette er understøttet af den pågældende telefon. Se også afsnit 6.2.

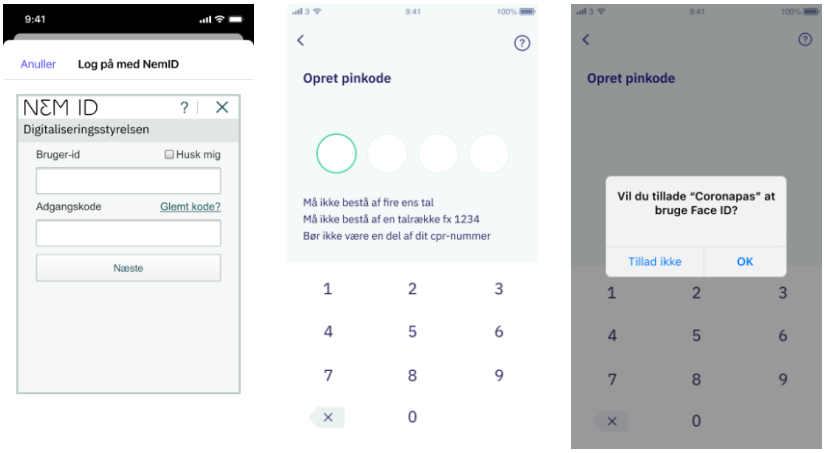

Illustration: Eksempler på skærme i oprettelsesforløbet.

[6] Borgere, der ikke benytter digitale løsninger eller har et NemID kan få et coronapas på anden vis, hvilket der står nærmere beskrevet på coronasmittte.dk: https://coronasmitte.dk/raad-og-regler/coronapas#heading3

Fremvise coronapas - indenrigs

Når borgeren benytter coronapasset indenrigs, vises alene, at borgeren har et gyldigt coronapas. Det er kontrollanten uvedkommende, hvorfor coronapasset er gyldigt.

Denne foranstaltning sikrer, at borgere, der fx ikke ønsker at modtage en vaccination, ikke indirekte afslører dette ved en kontrol.

Som udgangspunkt vises ikke navn og fødselsdag på borgeren.

Illustration: Hovedskærmen i coronapasset, hvor navn og fødselsdag ikke vises.

Borgeren skal aktivt selv vælge at vise navn og fødselsdag. Dette giver en kontrollant mulighed for at sammenstille informationerne med supplerende legitimationsbeviser. Kontrol af coronapas skal følge de til enhver tid gældende retningslinjer herfor. Dette whitepaper forholder sig ikke yderligere til de krav, som stilles til kontrol i forskellige sammenhænge men alene til de metoder, som appen understøtter.

Illustration: Hovedskærmen i coronapasset, hvor navn og fødselsdag vises.

QR-koden indeholder de informationer, som vises på skærmen samt signatur fra Sundhedsdatastyrelsen, der garanterer for ægtheden af data. Når der ikke vises navn, indeholder QR-koden en gyldighedsmarkering. Når der vises navn og fødselsdag, er disse også indeholdt i QR-koden.

Hvis borgeren har oprettet sig i appen, men endnu ikke har modtaget eller har forudsætningen for at modtage et gyldigt coronapas, vises følgende.

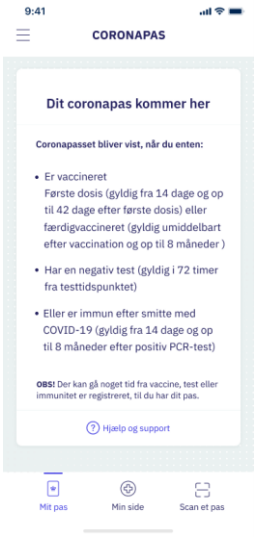

Illustration: Visning, når borgeren har oprettet sig, men der ikke er dannet et gyldigt pas.

Det skal bemærkes, at det potentielt er muligt – men formentligt meget sjældent forekommende – at have et coronapas, som kan give adgang til rejse til andre lande, men som ikke er gyldigt indenrigs fx hvis gyldigheden af en vaccine er længere end i Danmark.

Fremvise coronapas – udenrigs

Når en borger skal rejse til udlandet, så skal denne skifte til appens udenrigsside.

På rejsesiden vises de gyldige rejsecertifikater, som borgeren har. Borgeren kan have flere gyldige rejsecertifikater, hvis denne både er vaccineret, har negativ test og er immun pga. overstået infektion.

På rejsesiden er der ikke en markering af, hvorvidt coronapasset er gyldigt. Det skyldes, at regler for gyldigt coronapas kan være forskellige fra land til land. Borgeren skal derfor på forhånd – og inden afrejse – orientere sig om reglerne i de lande, som rejsen omfatter herunder transitlande.

Et rejsecertifikat indeholder detaljeret information om vaccine-, test- eller immunitet samt en QR-kode, som kan læses af de øvrige deltagende lande i DCC-samarbejdet, der er signeret af Sundhedsdatastyrelsen. Datasættet, der deles, beskrives nærmere i afsnit 5.3.

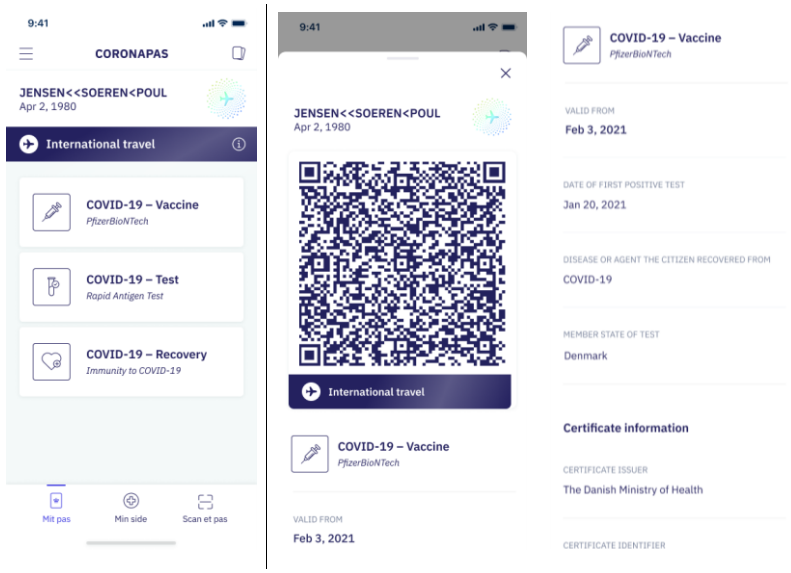

Illustration: Visning, når borgeren viser et certifikat ved rejse. I eksemplet et vaccinecertifikat

Få indblik i egne data

Det er muligt for borgeren i appens "Min Side"-sektion at se de data, der ligger til grund for coronapasset, herunder vaccine-, test eller data om overstået infektion i appen.

Oplysningerne på denne side er udelukkende ment til borgeren og skal ikke benyttes til kontrol, hvilket borgeren indledende gøres opmærksom på.

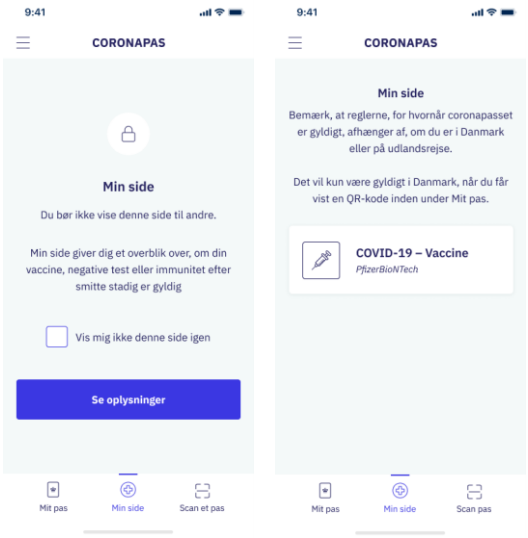

Illustration: "Min side", hvor borgeren kan se datagrundlaget for coronapasset.

Scanne et andet coronapas

En borger har mulighed for at scanne en anden borgers pas. Denne funktion gør det muligt for en borger både at agere i rollen som borger, der skal fremvise pas samt som kontrollant.

4.3 Brugeroplevelse som kontrollant

Som kontrollant kan et coronapas inspiceres på flere forskellige måder alt efter kontrolsituation.

Dette whitepaper forholder sig som nævnt i afsnit 4.2 ikke til de krav, der stilles til kontrol i forskellige sammenhænge men alene til de metoder, som appen understøtter.

Visuel inspektion

Coronapasset kan visuelt inspiceres af en kontrollør. Hvis borgeren har et gyldigt pas, så fremgår det tydeligt på brugerens skærm, at passet er gyldigt.

Hvis kontrolløren har behov for at se borgerens navn og fødselsdag kan denne bede borgeren fremvise dette, så det eventuelt kan sammenstilles med supplerende legitimationsbeviser.

Kontrolløren kan til et vist omfang afgøre coronapassets ægthed ved at konstatere, at vandmærkerne i passet reagerer på telefonens gyroskop. Se også afsnit 6.4.

Scanning

En kontrollant kan scanne QR-koderne i coronapasset. I appen er indlejret den offentlige nøgle fra Sundhedsdatastyrelsen, der gør det muligt at verificere, at de

data, som fremvises, er korrekte. Når DCC-forordningen træder i kraft, indlejres ligeledes de offentlige nøgler fra de øvrige deltagende lande. Se også afsnit 7.2.

Appen kan bruges af en kontrollant, uden at denne skal logge ind i appen. På den måde understøttes det, at kontrollanter ikke behøver logge ind på telefoner, som fx er udleveret af en arbejdsgiver, med personlige informationer.

Første gang kontrollanten benytter scanningsfunktionen, gives en kort introduktion til funktionaliteten.

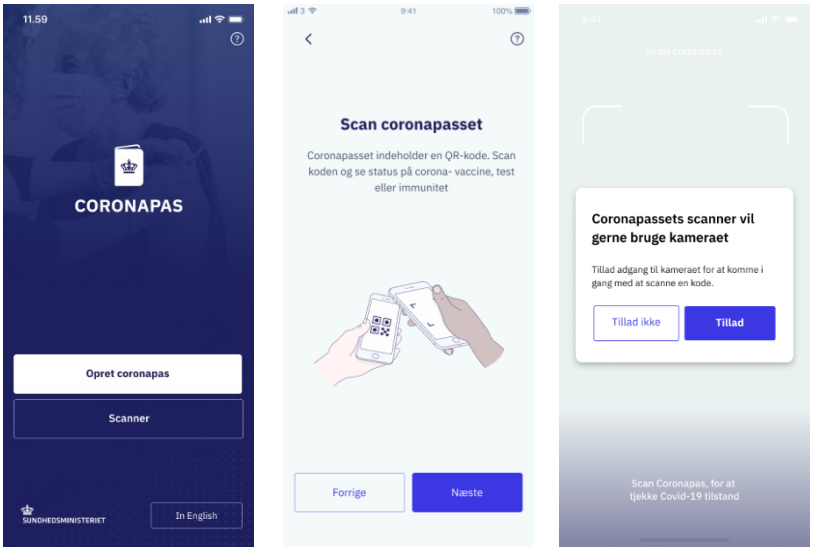

Illustration: Scanneren kan benyttes uden kontrollanten opretter sig. Kontrollanten får en kort introduktionen til funktionen.

Herefter kan kontrollanten scanne ved hjælp af telefonens kamera. Scanningsskærmen i appen indeholder de samme informationer, som vises på skærmen, da disse også er indlejret i QR-koden.

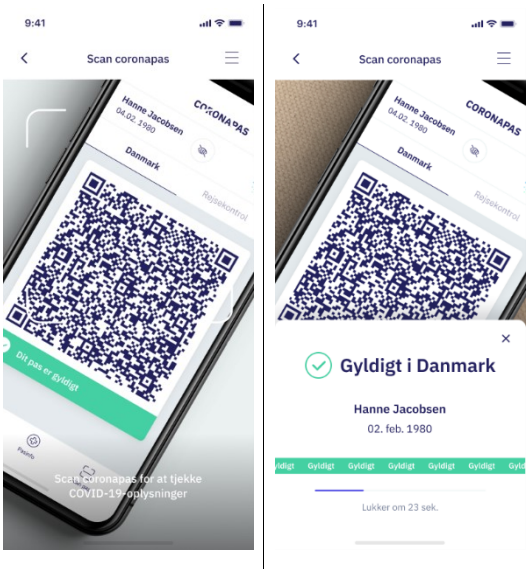

Illustration: Scanneren benyttes til at scanne QR-koden. Kontrollanten får på sin skærm svar med resultatet.

Scanningsresultatet forsvinder automatisk efter et antal sekunder. Scanning omtales også i afsnit 6.4.

Scanning med professionelle scannere og imagers

Appen kan installeres på professionelle scanningsenheder, som er udstyret med særligt udstyr til effektiv scanning af QR-koder. Her understøttes som udgangspunkt mærkerne Zebra og Newland.

Scanning med øvrige enheder

Det undersøges pt., hvorvidt enheder, der ikke benytter appen, også vil kunne indlejre den offentlige nøgle, så data i QR-koden kan verificeres. Funktionen vil dog ikke være understøttet ved lanceringen af appen.

4.4 Øvrige funktioner

Mulig for at skifte mellem dansk og engelsk

Det er muligt for brugeren at skifte mellem engelsk og dansk.

Offline

Coronapas-appen kan fungere offline i en periode, når først QR-koden er hentet ud i appen. Som udgangspunkt har QR-koderne til indenrigsbrug en levetid, der tillader, at man kortvarigt kan være offline, mens QR-koderne til udenrigsbrug har en levetid på 72 timer.

En kontrollant behøver som udgangspunkt heller ikke være online. Scanneren er dog afhængig af at kunne opnå forbindelse til internettet med visse mellemrum for at kunne hente offentlige nøgler, der er beskrevet i afsnit 4.3.

5. Data i coronapasset

Coronapasset indeholder forskellige datasæt, der svarer til de understøttede kontrolscenarier.

5.1 Generelt om data i coronapas-appen

De data, som behandles i coronapas-appen, er opdelt i flere datasæt, der modsvarer de understøttede kontrolscenarier. Det er Statens Serum Institut, der er dataansvarlig.

Data i indenrigsvisningen er, ud fra et princip om dataminimering, reduceret til alene at angive gyldighed evt. suppleret med navn og fødselsdag.

Data i udenrigsvisningen er aftalt mellem EU-landene og er detaljeret til en grad, der muliggør, at landene har forskellige informationer til rådighed for at afgøre, om en EU-borger ved indrejse vurderes at have et gyldigt coronapas. EU-forordningen er ikke endeligt vedtaget, hvorfor den endelige data i udenrigsvisningen kan ændre sig.

5.2 Data i indenrigsvisning

Datafelter, der medtages i standardvisning

a) Gyldig

Datafelter, der medtages i visning med navn og fødselsdag

a) Gyldig
b) Navn
c) Fødselsdato

5.3 Data i udenrigsvisning

Datafelter, der skal medtages i vaccinationscertifikatet

a) navn: efternavn(e) og fornavn(e) i nævnte rækkefølge
b) fødselsdato
c) målsygdom eller -agens
d) vaccine/profylakse
e) vaccinelægemiddel
f) indehaver af markedsføringstilladelsen for vaccinen eller vaccineproducent
g) nummer i en række af vaccinationer/doser

h) dato for vaccination, med angivelse af datoen for den seneste dosis
i) medlemsstat, hvor vaccinen er givet
j) udsteder af certifikat
k) en unik certifikatidentifikator.

Datafelter, der skal medtages i testcertifikatet

a) navn: efternavn(e) og fornavn(e) i nævnte rækkefølge
b) fødselsdato
c) målsygdom eller -agens
d) testtype
e) testnavn (valgfrit i forbindelse med NAAT-test. Feltet er ikke understøttet ved lancering)
f) testproducent (valgfrit i forbindelse med NAAT-test. Feltet er ikke understøttet ved lancering)
g) dato og klokkeslæt for prøveudtagning
h) testresultat
i) testcenter eller -facilitet
j) medlemsstat, hvor testen er taget
k) udsteder af certifikat
l) en unik certifikatidentifikator.

Datafelter, der skal medtages i restitutionscertifikatet

a) navn: efternavn(e) og fornavn(e) i nævnte rækkefølge
b) fødselsdato
c) sygdom eller agens, som borgeren er kommet sig over
d) dato for første positive testresultat
e) medlemsstat, hvor testen er taget
f) udsteder af certifikat
g) certifikat gyldigt fra
h) certifikat gyldigt indtil
i) en unik certifikatidentifikator.

5.4 Data på Min Side

Data på Min Side, der udelukkende er til borgerens egen information, er udledt af datasættet til udenrigsvisning.

6. Sikkerhed, privacy og sikring mod misbrug

It-sikkerhed, sikring af brugerens privatliv og sikring mod misbrug er essentiel for coronapassets succes og er derfor en forudsætning for projektets gennemførsel. Samtidigt er det væsentligt at finde den rette balance mellem de tre faktorer.

Sikkerheds- og privacy-mekanismer indbygges i designet af coronapassets funktionalitet og processer samt i de tekniske foranstaltninger til beskyttelse af data og kommunikationskanaler.

Ligeledes indbygges der funktionalitet, der har til formål at mindske misbrug af appen og svindel med coronapas.

Sikkerheden bliver forankret hele vejen gennem udviklingsprocessen og i den efterfølgende overvågning og drift af løsningen.

6.1 Sikkerhed i den samlede løsning

I det følgende gennemgås en række af de områder, som indgår for at sikre tilgængeligheden, fortroligheden og integriteten i den samlede coronapasløsning.

Tilgængelighed

Da coronapasset bliver et væsentligt instrument i samfundet i forbindelse med genåbningen er det vigtigt at sikre løsningen mod ondsindede angreb, der kan medføre nedetid på løsningen, hvilket kan betyde, at det kan være vanskeligt for borgerne at få et coronapas.

Fortrolighed

Da løsningen behandler borgerens data, der har sundhedsmæssig karakter, er det kritisk, at disse kun bliver gjort tilgængelige for rette vedkommende, og at data i det hele taget minimeres til det absolut nødvendige, for at løsningen kan fungere.

Integritet

Det skal ligeledes sikres, at data ikke kan manipuleres eller forfalskes i selve it-løsningen med henblik på misbrug, så brugeren opnår at modtage et gyldigt pas ved, at forudsætningerne for dets udstedelse er blevet ændret.

Lige så væsentligt er det at indbygge et vist niveau af tiltag mod misbrug af coronapasset i forskellige brugssituationer. Disse behandles nærmere i afsnit 6.4.

Ekstern sikkerhedstest

Et internationalt anerkendt sikkerhedsfirma har foretaget en grundig test af systemet. Det overordnede formål med testen har været at sikre, at der tages tilstrækkelige tiltag til netop at sikre tilgængelighed, fortrolighed og integritet.

Testen har bl.a. beskæftiget sig med og taget udgangspunkt i velafprøvede metodikker fx OWASP[7]:

- Gennemgang og sårbarhedsscanninger af løsningens backend og infrastruktur.
- Analyse med henblik på at identificere logiksårbarheder og applikationsspecifikke problemer.
- Analyse af beskyttelse af data i alle stadier af løsningen – både når data er i bevægelse eller opbevares baseret på en "*least privilege*"-model – samt at sikre, at der er politikker og processer på plads som er i overensstemmelse med GDPR og øvrige krav fra myndighederne. Gennemgang af dataflow i løsningen både internt i løsningens komponenter og mellem komponenterne.
- Review af selve appen både til iOS og Android herunder evt. tiltag til hærdning af appen. Se afsnit 6.2.

6.2 Sikkerhed i appen

Sikker brugerautentifikation ved indrullering

Som tidligere beskrevet foretages indrulleringen på baggrund af NemID, hvilket skaber en meget høj grad af sikkerhed for identiteten af den person, som får udstedt et coronapas.

Selve autentifikationen sker i en browser, der sikrer, at appen ikke får adgang til brugerens log ind-informationer.

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

Hvis borgeren ikke benytter coronapas appen i 30 dage, så skal borgeren dog logge ind igen.

[7] https://owasp.org/

Oplåsning af app

Coronapas-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.

Hærdning af appen

I forbindelse med udvikling af appen har indgået en række overvejelser om ibrugtagning af teknikker, der kan hærde appens sikkerhed. Disse overvejelser, som ligeledes indgik i forbindelse med sikkerhedsanalysen, inkluderer bl.a.:

Obfuskering (tilsløring) af appens kodebase

Ved at obfuskere koden, besværliggøres det for offentligheden at læse appens kildekode med henblik på fx at identificere hardcodede keys og API endpoints, 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.

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 man kan advare borgeren om sikkerhedsrisikoen ved, at en ondsindet app på borgerens rootede telefon opfanger pasdata fra coronapas-appen.

Root detection er implementeret i appen.

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, hvor en borger eksempelvis vil kunne få et "forkert" coronapas ned på deres telefon.

SSL-pinning er ligeledes implementeret i appen.

6.3 Forhold mellem sikring mod misbrug og privacy

I udviklingen af coronapasset har løbende indgået overvejelser om at sikre den rette balance mellem at hindre misbrug og samtidig respektere for borgerens privatliv.

De mål, der gerne vil opnås, foruden at løsningen er meget sikker, inkluderer:

- At løsningen til et vist niveau er modstandsdygtig over for misbrug
- At løsningen kun viser nødvendige data om borgeren.

Til disse kommer også et ønske om at lave en app, der er brugervenlig og en infrastruktur, der er robust over for, at der skal dannes mange coronapas.

Målene kan imidlertid være vanskelige at opnå på samme tid.

Eksempelvis er et middel til at mitigere misbrug med passet, at borgerens navn og fødselsdag indgår i en visning i coronapasset. Dette tvinger dog borgeren til at afgive nogle oplysninger om sig selv.

Hvis en større grad af vished skal opnås, vil det være nødvendigt at supplere med endnu mere information om borgeren fx billede, som det kendes fra det Digital Kørekort, eller CPR-nummer. Hermed vil borgeren dog skulle afgive endnu flere oplysninger om sig selv. Blandt andet derfor er dette fravalgt.

QR-koder med en kort levetid forhindrer, at disse deles med andre borgere med henblik på misbrug.

Kortlevende QR-koder kræver dog, at borgeren ofte har forbindelse til appens backend, hvorfra data modtages, og det betyder, at borgeren ikke kan være offline i længere perioder. Dette kan være uhensigtsmæssigt særligt ved rejse, hvor man ikke nødvendigvis har konstant forbindelse til internettet. I QR-koden til udenrigsbrug er navn og fødselsdag på borgeren dog indlejret og vil formentligt blive sammenholdt med supplerende identifikation, hvorfor risikoen for misbrug er mindre. Af den årsag kan QR-koden til udenrigsbrug have en længere levetid.

Det er vigtigt at understrege, at det ikke alle tiltag mod misbrug, der har potentielle konsekvenser for privatliv, hvilket fremgår af afsnit 6.4.

6.4 Tiltag mod misbrug

Som beskrevet ovenfor skal tiltag mod misbrug vægtes mod, hvilken betydning det har for borgerens privatliv samt den generelle brugervenlighed i coronapas-appen. I appen er der udviklet flere tiltag mod misbrug, men det er væsentligt at understrege, at de ikke fuldstændigt vil kunne forhindre misbrug af appen. Tiltagene beskrives i det følgende.

Autentifikation

Idet borgeren autentificerer sig med NemID ved ibrugtagning, sikres det, at det er borgerens data, som indlæses i appen. Det er dermed også borgerens navn og fødselsdag, der vises, når der foretages fremvisning med navn og fødselsdato.

QR-kode

Data i QR-koden er signeret med Sundhedsdatastyrelsens digitale signatur. Det kan derfor med fuld sikkerhed verificeres, at data stammer herfra.

Hvis scanneren benyttes på en QR-kode, hvori data er signeret med signatur, der ikke modsvares af en offentlig nøgle, som scanneren har indlejret, så vil resultatet i scanneren give kontrollanten besked om dette.

I scanneren vil der blive indlejret de offentlige nøgler fra de øvrige lande i DCC-samarbejdet foruden den danske nøgle. Se afsnit 7.2.

Illustration: Scanneren viser en fejlbesked, hvis den offentlige nøgle ikke svarer til den private nøgle/signatur.

QR-koden har endvidere en begrænset levetid, hvilket i vist omfang sikrer mod, at den videredistribueres med henblik på misbrug.

Tiltag i brugergrænsefladen

Brugergrænsefladen er forsynet med en række bevægelige elementer, der sikrer mod fx misbrug ved hjælp af screenshots.

De bevægelige dele reagerer på bevægelse, der opfanges af telefonens gyroskop og giver en effekt, som fx også kendes fra fysiske legitimationskort.

Illustration: Elementer i brugergrænsefladen med bevægelige dele, der reagerer på telefoners gyroskop.

Maksimalt antal enheder

En borger kan kun oprette coronapas på to enheder. Hvis en borger indrullerer coronapasset på en tredje smartphone, skal borgeren igen logge ind med NemID på den enhed, som brugeren først loggede ind på af de tre enheder.

Tiltaget forhindrer i et vist omfang misbrug, hvor en borger logger ind på andres telefoner og dermed potentielt giver dem adgang til borgerens gyldige pas.

6.5 Privacy

Sikring af borgernes privatliv er essentielt i løsningen. Coronapasset er derfor udarbejdet ud fra en *privacy by design*-tankegang, hvor de bærende principper er, at:

- Behandle så få data som muligt.
- Opbevare så få data som muligt i løsningens dele.
- Give borgeren kontrollen over de data, som vises.

I de følgende beskrives en række af de privatlivsbeskyttende tiltag, der er foretaget i udarbejdelse af coronapas-løsningen.

Gyldighed

I indenrigsvisningen i appen er det ikke muligt for en kontrollant at se, hvorfor coronapasset er gyldigt. Der vises alene, at der er tale om et gyldigt coronapas.

Borgeren behøver dermed fx ikke direkte eller indirekte afsløre, hvorvidt denne er vaccineret eller ønsker at blive vaccineret. Borgeren afslører heller ikke om vedkommende har haft COVID-19, og dermed at passets gyldighed skyldes immunitet.

Step up-løsning

Data, der kan identificere borgeren, hvilket vil sige navn og fødselsdag, vises som nævnt i afsnit 4.2 som udgangspunkt ikke i coronapasset til indenrigsbrug.

Dermed behøver borgeren ikke eksponere disse data i kontrolsituationer, hvor det ikke er nødvendigt. Borgeren kan selv aktivt vælge at vise sit navn og fødselsdag, hvis en kontrolsituation kræver dette.

Illustration: Hovedskærmen i coronapasset, hvor navn og fødselsdag ikke vises som udgangspunkt, og kun hvis brugeren aktivt vælger at trykke på knappen "Vis navn og fødselsdag".

Der vises heller ikke CPR-nummer, pasnummer eller andre løbenumre, der kan medvirke til at identificere borgeren.

Brugeren skal selv aktivt vælge at vise EU-minimumsdatasæt, der indeholder flere data end datasættet til indenrigsbrug, men dette er påkrævet for at kunne rejse. Se afsnit 5.3.

Opbevaring

Appens backend gemmer ikke sundhedsdata, men agerer alene som gateway mellem webservice og borgernes app. Appens backend gemmer alene kvittering for bestilling af coronapasset, så det kan hentes, når det er dannet. Se afsnit 7 for detaljer om den arkitekturmæssige opbygning af løsningen.

Scanning

Scanningsresultater gemmes ikke i appen.

Det registreres og lagres derfor ikke i forbindelse med scanning:

- resultatet af scanningen eller data herfra
- hvor passet er kontrolleret (herunder geografisk placering),
- identiteten på borgeren, der er blevet kontrolleret,
- identiteten på kontrollanten,
- tidspunkt eller
- øvrige informationer om kontrol fx oplysninger om brugerens enhed.

Logning

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

Ligeledes logges der heller ikke data, der kan benyttes til at identificere brugeren fx ip-adresse, MAC-adresse, app- eller device-id'er.

7. Arkitektur

Coronapasset er delvist baseret på allerede eksisterende it-løsninger på sundhedsområdet. Der bliver udviklet en række nye komponenter både i Danmark og EU for at understøtte coronapassets formål.

Coronapas-løsningen baserer sig på allerede eksisterende løsninger på sundhedsområdet herunder Den Nationale Serviceplatform (NSP), Det Danske Vaccinationsregister (DDV) og Den danske mikrobiologidatabase (MiBa). Det primære formål har været at skabe en robust arkitektur, der skåner de særdeles kritiske systemer i sundhedsvæsenet mod den store mængde trafik, som coronapasset vil medføre, og som disse eksisterende systemer ikke nødvendigvis er designet til at kunne håndtere.

Et andet væsenligt formål har været at designe en løsning, der allerede i sit udganspunkt er interoperabel med den løsning, som bygges på EU-plan, som skal understøtte DCC-infrastrukturen.

7.1 Coronapassets arkitektur

Coronapasløsningen består overordnet af følgende byggeblokke:

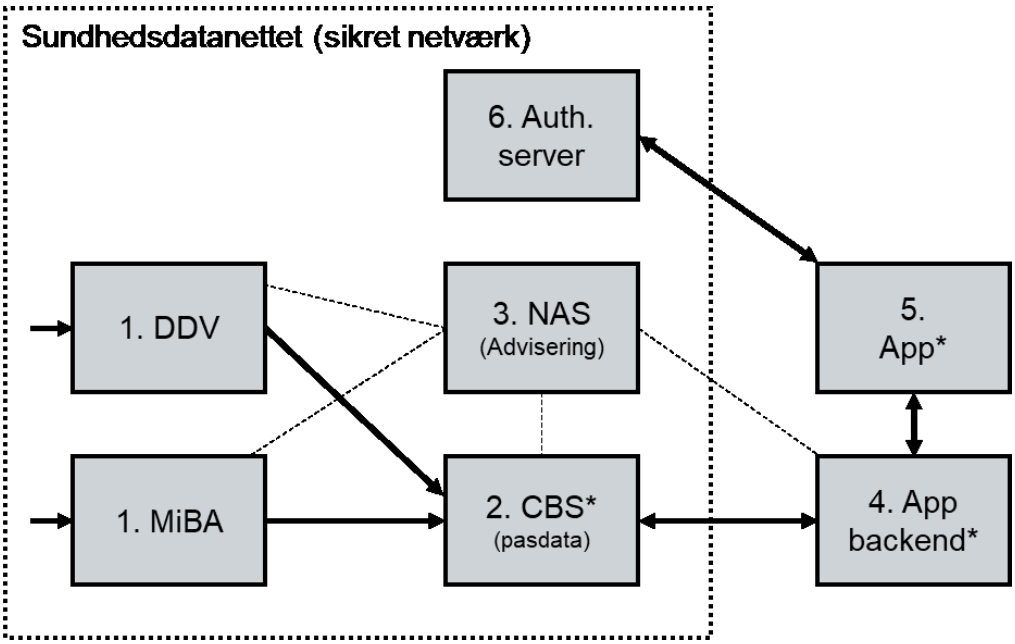

Illustration: Løsningens væsentligste byggeblokke. Byggeblokke med * er byggeblokke, der etableres i forbindelse med projektet.

Byggeblokkene beskrives i det følgende:

1. **Det Danske Vaccinationsregister (DDV) og Den danske mikrobiologi-database (MiBa)**
   Det Danske vaccinationsregister (DDV) og Mikrobiologidatabasen (MiBA) er de kernesystemer, som leverer data til løsningen. Når en borger bliver vaccineret eller testet, bliver informationerne registreret i disse systemer.

2. **Covid-19 Borgerstatus (CBS)**
   Covid-19 Borgerstatus (CBS) er en webservice, der etableres på den nationale serviceplatform (NSP) til coronapasset. Formålet med servicen er primært at skåne DDV og MiBA mod den meget store mængde trafik, som coronapasset vil medføre. Dette hånderes ved, at data sendes fra DDV og MiBA og caches i komponenten. En anden væsentlig egenskab ved CBS er, at det er i denne komponent, at regelsættet for, hvad der udgør et gyldigt pas, vedligeligholdes samt appliceres på data, inden den formidles til appens backend.

3. **National Adviseringsservice (NAS)**
   National Adviseringsservice (NAS) er en eksisterende service på den nationale serviceplatform (NSP), hvis primære formål i coronapsløsningen er at orkestrere, at de forskellige komponenter notificeres, når der ændringer i statusændringer i forhold til et coronapas, fx når et testresultat er klart.

4. **App-backend**
   App-backendens primære formål er at være gateway mellem CBS og appen, herunder stå formidlingen af data. Det er app-backenden, der modtager signerede data fra CBS og videreformidler disse til appen..

5. **App**
   Coronapas-appen som installeres af borgere og kontrollanter. Appen er brugergrænsefladen i løsningen og benyttes til fremvisning og kontrol af coronapas. I appen dannes QR-koderne på baggrund af de data, som modtages fra App-backend.

6. **Autorisationsserver**
   Autorisationsserverens rolle er at autentificere borgeren. Autorisationsserveren udsteder et langtlevende token til appen, der gør, at borgeren ikke behøver logge ind med NemID ved hvert brug. Se desuden afsnit 6.2 og 6.2.

7.2 EU-arkitektur

Digital Green Certificate Gateway'en (DGCG)[8], der etableres af EU-Kommissionen i samarbejde med medlemslandene har til formål at sikre, at de enkelte landes coronapas, hvad enten disse er digitale eller papirbårne, kan fungere sammen.

[8] Er endnu ikke blevet omdøbt, så den reflekterer, at forordningen nu omtaler EU Digital COVID Certificates frem for Digital Green Certificates.

Samarbejdet sikrer også i vid udstrækning interoperabilitet med andre internationale initiativer på området fx i regi af WHO.

Løsningen er baseret på, at landene udveksler offentlige nøgler, så det bliver muligt at verificere ægtheden af data og er illustreret ved nedenstående figur:

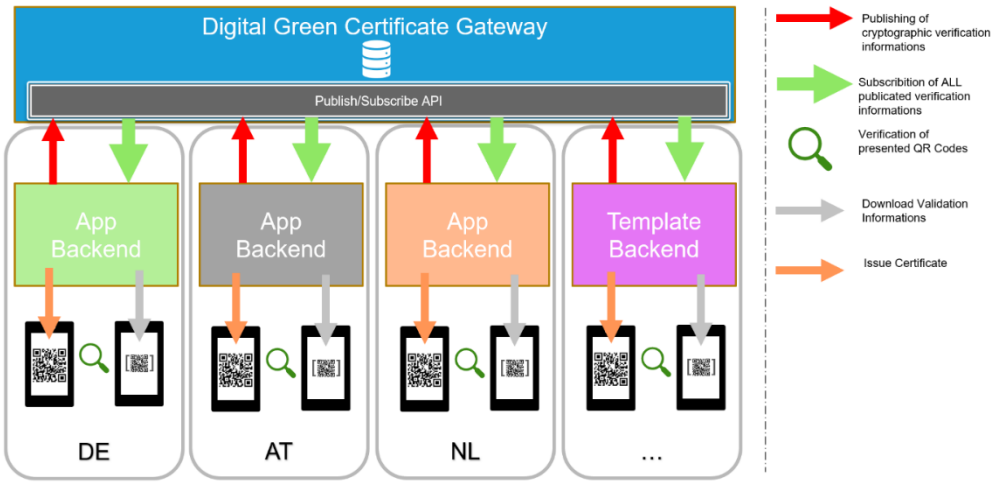

Illustration: Digital Green Certificate Gateway, der viser hvorledes offentlige nøgler deles mellem landene og distribueres til de tekniske løsninger i de respektive lande.

Den offentlige nøgle, der bliver udledt af den private nøgle, som de danske coronapas-data signeres med, publiceres til en fælles gateway. De øvrige lande gør det samme.

Den danske løsning henter de øvrige landes offentlige nøgler, som videredistribueres til den dansk coronapas-app, der dermed har indlejret alle de deltagende landes nøgler, hvilket medfører, at scanneren i den danske app, kan verificere data ved hjælp af QR-koder, som er signeret af de andre lande.

Det er vigtigt at understrege, at der ikke sendes sundhedsdata om alle – eller enkelte – danskere til den fælles gateway. Det er alene i en scanningssituation ved en grænseovergang eller lignende, at brugeren skal fremvise data. De relevante data er beskrevet i afsnit 5.3.

Formålet med dette whitepaper er at beskrive coronapasset funktionalitet, data, opbygning samt sikkerheds- og privacymæssige aspekter ved løsningen.

digst.dk / sundhedsdatastyrelsen.dk