Rådet for Digital Sikkerheds principper for udvikling af et corona-pas

Der er igangsat et arbejde med at udvikle et digitalt coronapas, hvor man som borger kan tilgå status for PCR-test og vaccine. Rådet for Digital Sikkerhed har formuleret en række principper, Rådet mener bør ligge til grund for den videre udvikling.

Baggrund og formål

For at understøtte en sikker åbning af samfundet er der fra 6. april krav om brug af coronapas, når man fx skal til frisør, på restaurant i teater eller på rejser. I den forbindelse er der en række sikkerhedsmæssige og databeskyttelsesmæssige hensyn man skal tage, og en række funktionaliteter og etiske overvejelser, der bør gøres. Et coronapas skal kunne fremvises som dokumentation for, at man er vaccineret eller indenfor 72 timer er testet negativ. Via sundhed.dk kan man se sit coronapas, ligesom det også er muligt at downloade app'en Min Sundhed, og se svaret herinde. Der igangsat et arbejde med at udvikle en mere avanceret og brugervenlig app, der lanceres ultimo maj.

En sådan app kan indeholde mulighed for smitteopsporing (fx ved videreudvikling af eksisterende smittestop-app), hvilket der kan være behov for, da der i en negativ test kan indeholde usikkerhed, med mulighed for europæisk interoperabilitet, således danskerne kan bruge passet, når de skal rejse i udlandet.

Der kan også være tilfælde, hvor der er behov for at kunne scanne passet, fx i tilfælde at meget store arrangementer – eksempelvis ved brug af brug af QR kode, hvor det registreres, at man har været til stede til et givent arrangement. Der er altså forskellige krav afhængig af, hvad formål passet skal tjene.

Rådet for Digital sikkerhed, har formuleret en række principper, der bør anvendes, når et coronapas skal udvikles.

Rådet for Digital Sikkerhed
Vester Farimagsgade 37B, 1. th., 1606 København V
Telefon: +45 2041 4685 mail: info@digitalsikkerhed.dk web: www.digitalsikkerhed.dk

Principper for passet:

Privatlivsbeskyttelse

1. Dataminimering i design af løsningen - anvendelse af så få data om borgeren som muligt (fx grønt pas kan være udtryk for både vaccination/negativ test, der er max 72 timer gammel) Der vises alene en simpel markør fx grøn/rød (vaccineret- negativ test, der er max 72 timer gammel /ikke vaccineret) Passet indeholder ikke andre oplysninger fx lokationsoplysninger og data lagres decentralt på de enkelte enheder
2. Det bør være frivilligt for borgeren at hente passet– selvom det vil begrænse borgeren ikke at have det
3. De tekniske komponenter og de designmæssige overvejelser skal bygge på et privacy venligt design
4. Individets rettigheder og principperne i GDPR skal sikres gennem it-løsningens design (forudbestemt formål, kun indsamling af nødvendige data, indsigt, oplysningspligt, kontrol over egne data, sletning m.v.)
5. Data i passet skal alene bruges til formålet: at borgeren kan fremvise en markør af om vedkommende er vaccineret / inden for 72 timer er testet negativ
6. Tilfælde hvor fx restauranter eller museer skal lagre information om, hvem der har været til stede – bør minimeres – i tilfælde af behov for dette, bør det ske ved brug af fx QR kode

Sikkerhed

7. De tekniske komponenter og de designmæssige overvejelser skal bygge security by design og best practise (fx review, sikkerhedstest, krypteret kommunikation, code review, styring af adgangsrettigheder mv.) i stil med, hvad der er anvendt i smittestop app'en

Politisk proces

8. Der tages stilling til konsekvenserne af løsningen på lang og kort sigt
9. Der skal være en solnedgangsklausul – brug af coronapas skal afvikles så snart muligt
10. Klarhed om ansvarsplacering, løbende tilsyn og klageadgang
11. Det skal virke på alle smartphones Krav om coronapas ved indgang til fx restauranter, museer mv. skal alene følge myndighedernes anbefalinger
12. Passet skal være interoperationelt dvs. det skal kunne bruges på tværs af landegrænser

Rådet står naturligvis til rådighed for en uddybelse af ovenstående synspunkter.

På bestyrelsens vegne

Henning Mortensen
Formand, Rådet for Digital Sikkerhed