Godkjent av: GUKN Gyldig fra: 24.06.2021	Rapport Risikovurdering informasjonssikkerhet	Versjon 2.1

FHI

Risikovurdering

Av Koronasertifikat, Trinn 4.

Juni 2021

Gun Peggy Strømstad Knudsen, 24.06.2021
Produkteier

Endringslogg og godkjenning

Versjon	Dato for godkjenning	Godkjent av (henhold til fullmakt)	Endring
1.0	11.06.2021	Gun Peggy Strømstad Knudsen	Første versjon, omfatter scope Koronasertifikat Trinn 3.
2.0	18.06.2021	Gun Peggy Strømstad Knudsen	Tilpasset scope Koronasertifikat Trinn 4.
2.1	24.06.2021	Gun Peggy Strømstad Knudsen	Mindre endringer i risikoscenariene

Innholdsfortegnelse

1. Bakgrunn

EU-kommisjonen la 17. mars frem et lovforslag om å opprette et EU Covid-19 Sertifikat, for å legge til rette for økt bevegelighet over landegrensene i EU under covid-19-pandemien. Det foreslåtte regelverket skal etablere et felles juridisk og teknisk rammeverk for utstedelse, verifikasjon og aksept av koronasertifikater i Europa. Sertifikatet skal bli gratis tilgjengelig digitalt og analogt i papirformat. Det vil inneholde en QR-kode for å verifisere at sertifikatet er gyldig. Koronasertifikatet skal kunne verifiseres i et annet land enn i det landet der sertifikatet er utstedt, slik at den enkelte under reiser skal kunne dokumentere status for vaksinasjon, testing eller gjennomgått koronasykdom. Det vil være opp til det enkelte land å bestemme bruken av sertifikatene, og hvilke reiserestriksjoner som skal gjelde. Forslaget gjør heller ikke det å inneha et gyldig vaksinesertifikat til en forutsetning for å kunne reise i Europa. Innenlands bruk av et koronasertifikat bestemmes også av hvert land selv.

Mens denne risikovurderingen skrives, er arbeidet med den tekniske løsningen for et koronasertifikat i full gang. Helsedirektoratet, Folkehelseinstituttet, Direktoratet for e-helse og Norsk Helsenett utvikler sertifikatet slik at den tekniske løsningen er på plass innen regjeringen har vurdert og besluttet hva koronasertifikatet kan brukes til. En forenklet utgave av koronasertifikatet (Trinn 1) kom på plass i begynnelsen av mai 2021. En mellomutgave med kun innenlands bruk som formål (Trinn 3) kom på plass i midten av juni 2021. Den endelige versjonen av sertifikatet (Trinn 4), som vil være i samsvar med EUs regelverk, kommer i slutten av juni 2021. Denne risikovurderingen dekker Koronasertifikat Trinn 4 og bygger videre på risikobildet for Trinn 3.

Koronasertifikatet baserer seg på tre deler:

- Vaksinasjonsstatus (basert på informasjon fra FHI SYSVAK),
- Negativt testresultat (basert på informasjon fra FHI Labdatabasen),
- Immunitet etter gjennomgått koronasykdom (basert på informasjon fra FHI MSIS).

Trinn 4 av koronasertifikatet dekker disse delene. Sertifikatet er verifiserbart i at det kan sjekkes at informasjon i koronasertifikatet ikke er endret etter utstedelse, og at sertifikatet er utstedt av korrekt utsteder. Med identifiserende informasjon i sertifikatet (fult navn og fødselsdato) blir det mulig å kontrollere at sertifikatet tilhører bæreren.

2. Sammendrag

2.1. Risikobildet

Risikobildet for Trinn 4 av koronasertifikatløsningen viser at risikonivået for informasjonssikkerhet er totalt sett vurdert som akseptabelt, innenfor de tiltenkte bruksområdene. De mest relevante risikoområdene er:

- Det er uklarheter rundt presise bruksområder og varighet med koronasertifikatet, både innenlands og ved grensepassering. Innenlands er praktisk bruk delvis opp til private arrangører å ordne. Dette kan føre til en mangfold av anvendelser og utydelig kommunikasjon til innbyggere og videre samfunnsimplikasjoner, som for eksempel mistillit til løsningen, tilsiktet eller utilsiktet misbruk av løsningen og politiske eller tilsynsdiskusjoner.
- Kontrollørappen blir lett tilgjengelig både i Norge og i utlandet. Misbruk av appen og kontrollørfunksjonen vil kunne føre til uønsket innsamling av sensitiv informasjon, profilering og et svekket tillitssystem.
- Innbyggere som ikke er digitalt aktive eller som av andre grunner ikke benytter seg av Helsenorge kan benytte en analog kanal. Utilstrekkelig kontroll av saksbehandlere kan potensielt føre til misbruk av deres tilgang som kan føre til at et utvalg av norske innbyggeres personopplysninger kommer på avveie.

Det bør nevnes at risikobildet har høy usikkerhet av blant annet følgende årsakene.

- Faktisk bruk av innenlands koronasertifikat har ikke blitt fullstendig avklart i skrivende stund og er delvis opp til private arrangører. Det er forventet at det kommer endringer eller utvidelser i bruken av innenlands koronasertifikat i løpet av de neste ukene og månedene. Det gjør at risikovurderingen ikke kan ta utgangspunkt i alle mulige bruksscenarier og relaterte risikopunkter og kan dermed være upresis.
- Risikovurderingen har blitt gjennomført parallelt med utvikling av koronasertifikatløsningen. Det har derfor kun vært mulig å ta utgangspunkt i dokumentasjon, opplysninger og kunnskap som har vært tilgjengelig under vurderingsperioden. Det gjør at risikovurderingen muligens ikke har fanget opp detaljer som er av betydning for risikobildet.

Det er viktig at arbeidet med personvern og informasjonssikkerhet fortsetter i hele løsningens levetid, samt at tiltak iverksettes for å holde risikoen på et akseptabelt nivå. Endringer i trusselbildet kan forekomme, og det er viktig at dette fanges opp og håndteres fortløpende. Videre kan det senere gjøres endringer i løsningen, og disse endringene må også risikovurderes før de settes i produksjon.

2.2. Anbefalte tiltak

Det er identifisert tiltak knyttet til scenarier med middels og høy risiko. Det bør nevnes at en del tiltak handler om politiske avgjørelser og avklaringer som ligger utenfor FHI sitt mandat, hos HOD. De mest relevante tiltaksområdene er:

- Presisere innenlands bruk av, varighet med og kontroll av koronasertifikat og kontrollørfunksjonen;
- Gjennomføre en kommunikasjonskampanje til innbyggere og reisende om bruk av koronasertifikatet;
- Istandsette private arrangører til å anvende koronasertifikat og kontrollørfunksjonen på en riktig, konsistent, forutsigbar og tydelig måte;
- Gjennomføre aktive tiltak mot misbruk av kontrollørappen;
- Utvide kontroll på mistenkelige handlinger i analog kanal;
- Utvide monitorering over kritiske prosesser rundt (digitale) sertifikater og nøkler.

3. Scope

Denne risikovurderingen dekker det norske koronasertifikatet som kobles til EU Digital COVID Certificate Gateway (Trinn 4) og bygger videre på risikobildet for mellomutgaven av det nasjonale koronasertifikatet (Trinn 3) som er kun brukt innenlands. Løsningen bygger videre på eksisterende løsninger for *innsyn i prøvesvar* og *vaksinetjeneste* som driftes av Norsk Helsenett (NHN) på vegne av FHI. I tillegg bygger løsningen på nye komponenter, levert av NHN og NetCompany, og en integrasjon med EU Gateway.

Følgende brukerhistorier (og løsningen som støtter disse historiene) har blitt tatt hensyn til i risikovurderingen:

- Innbygger skal kunne få et digitalt fremvisbart og utskriftbart testresultat, vaksineringsbevis eller immunitetsbevis som kan verifiseres for grensepassering i EU.
- Innbygger skal kunne få et digitalt fremvisbart og utskriftbart testresultat, vaksineringsbevis eller immunitetsbevis som kan verifiseres for innenlands bruk.
- Kontrollør skal kunne verifisere et testresultat, immunitetsbevis eller vaksineringsbevis uten å ta stilling til helseinformasjon.

3.1. Løsningsbeskrivelse

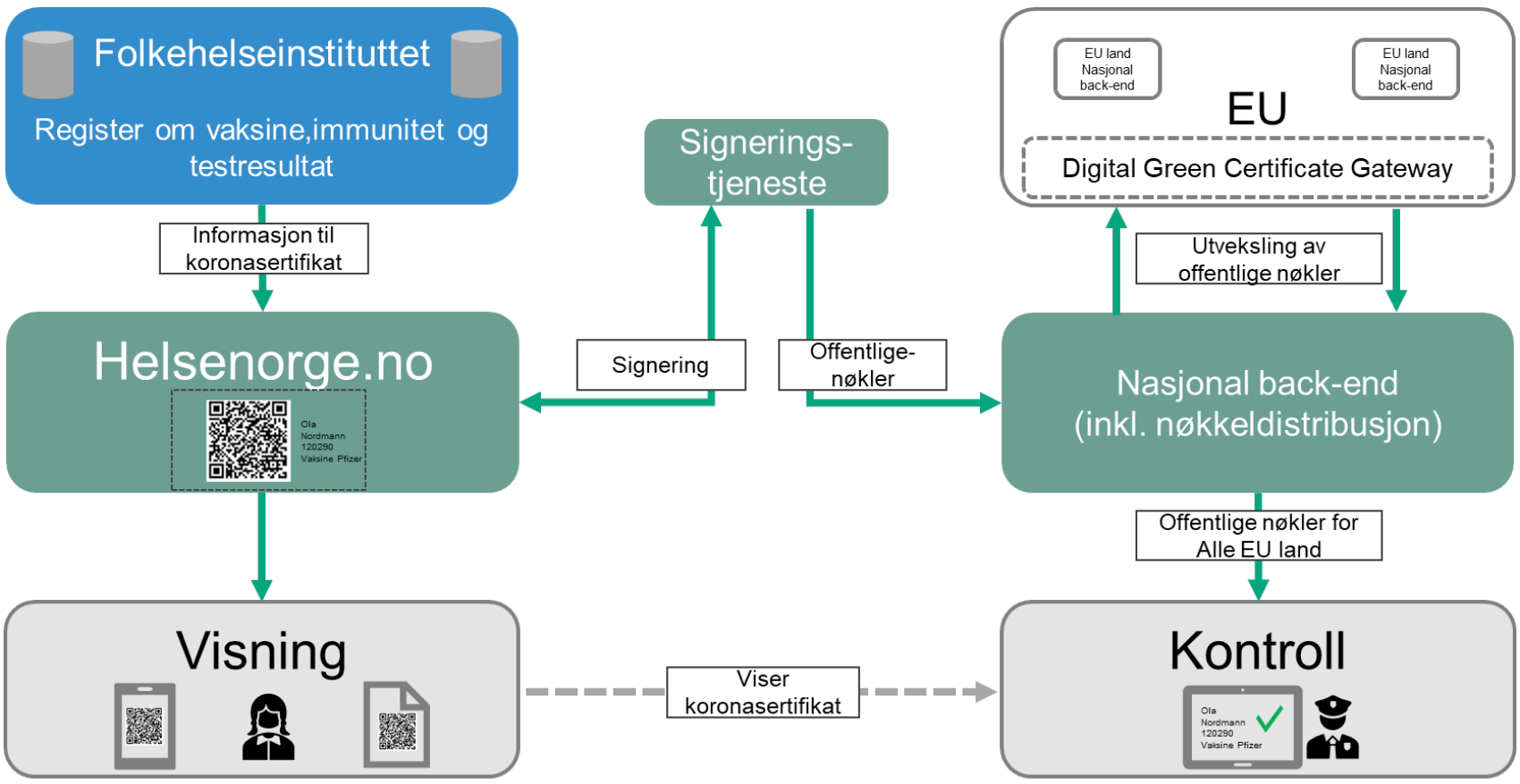
Koronasertifikatløsningen er tilgjengelig på Helsenorge etter innlogging. Den kan generere et koronasertifikat når en Innbygger er vaksinert, har en gyldig negativ prøve eller har immunitet etter gjennomgått sykdom. Prøvesvar for fremvisning hentes fra en replika av FHIs Labdatabase, vaksinestatus hentes fra FHI SYSVAK, immunitet hentes fra MSIS. FHI er eiere av databasene og er databehandlingsansvarlig, mens NHN er tjenesteleverandør og databehandler.

Helsenorge legger til rette for inngang for koronasertifikat og visning av dette for innbygger. For datautveksling er løsningen basert på eksisterende API-er og Helsenorges innsyntjeneste for prøvesvar og vaksinering. Den tekniske løsningen bygger videre på etablerte mekanismer for innsyn i prøvesvar og vaksiner, samt sikkerhetsmodell etablert mellom FHI og Norsk Helsenett (som forvalter Helsenorge). Kommunikasjonen mellom Helsenorge og FHI skjer over Helsenett.

Det brukes asymmetrisk kryptografi for signering av et koronasertifikat, det vil si med et nøkkelpar[1] bestående av en privat nøkkel og en offentlig nøkkel. Helsenorge genererer først en datapakke som inneholder identitetsopplysninger (noen bokstaver fra for- og etternavn og fødselsåret) og opplysninger om negativ test eller vaksine. Denne pakken signeres i signeringstjenesten ved bruk av en privat nøkkel. Ut ifra koden og signatur genereres det en QR-kode som kan vises frem, lastes ned og skrives ut. QR-koden vil inneholde (maskinelt) lesbare personopplysninger, den er ikke kryptert. Med at QR-koden inneholder både informasjon og signatur, blir det mulig for en kontrollør å validere at informasjonen kommer fra en troverdig part.

Tilhørende offentlige signeringsnøklene distribueres og lagres i et nøkkelregister i nasjonal back-end. Kontrollørtjenestene har tilgang til nøkkelregisteret og kan laste ned offentlige signeringsnøklene for validering av innholdet i QR-koden.

Under følger en skissering av koronasertifikatløsningen og koblingen til EU Digital COVID Certificate (tidligere Digital Green Certificate).



[1] For å unngå forvirring mellom signeringssertifikater (X.509) og koronasertifikater (QR-koder) benyttes det 'offentlige / private nøkler', 'nøkkelpar' og 'signeringsnøkkel' i stedet for 'sertifikat' når det diskuteres signeringssertifikater.

3.2. Verdivurdering

Helsenorge og FHI-koblinger

Helsenorge brukes for å laste ned eller vise et koronasertifikat og er dermed en sentral komponent. Helsenorge benytter eksisterende koblinger med FHI sine systemer for registrering av vaksine (SYSVAK), test (Labdatabasen) og smittsomme sykdomer (MSIS). Koblingene har blitt risikovurdert tidligere. Helsenorge er den primære visningstjenesten i denne fasen av samfunnsåpningen.

Helsenorge og koblingene med FHI sine systemer er av høy verdi for koronasertifikatløsningen.

Helsenorgeappen

Helsenorgeappen er nylig publisert og har en økende brukerandel. Denne appen kan benyttes for å vise frem et koronasertifikat og er dermed en del av visningstjenesten. For visning av et koronasertifikat, kan blant annet bruk av Helsenorge på nett og bruk av utskriftbart koronasertifikat på papir benyttes i stedet for appen.

Helsenorgeappen er i skrivende stund av middels verdi for koronasertifikatløsningen. Verdi kan øke med økt utbredelse og bruk av appen og walletfunksjonalitet fremover.

ID-porten

ID-porten er en portal for sikker identifisering mot offentlige tjenester i Norge og den brukes for å logge inn i Helsenorge. Ansvaret for ID-porten ligger hos Digitaliseringsdirektoratet, og de er også ansvarlige for den totale sikkerheten i tjenesten. Det ble lagt til grunn at ID-porten sikkert identifiserer brukere, og at drift og forvaltning er trygt ivaretatt.

Ikke alle innbyggere har en elektronisk ID som kan brukes for innlogging i Helsenorge, som gjør at det må tilrettelegges for alternative måter å få tak i et koronasertifikat. Med at koronasertifikatet er tiltenkt brukt i en offline-situasjon er det ikke nødvendig at en innbygger må kunne logge seg inn i en online løsning til enhver tid, men et digitalt samfunn kan ha en forventning om at en online løsning skal fungere på det tidspunktet man trenger den.

ID-porten av middels til høy verdi for koronasertifikatløsningen.

Signeringstjeneste

Signeringstjenesten sørger for at identitets- og helseinformasjon signeres ved bruk av en privat nøkkel, slik at en QR-kode kan lages. Det er også her de private nøklene lagres. Signeringsnøklene har en bestemt levetid og en bestemt antall koronasertifikater de skal brukes til. Kompromittering av en signeringsnøkkel gjør at en kan bruke nøkkelen til å generere et falsk koronasertifikat.

Signeringstjenesten er av høy verdi for koronasertifikatløsningen.

Nasjonal back-end og nøkkeldistribusjon

Verifisering av et koronasertifikat betyr i praksis validering av at en gyldig nøkkel ble brukt ved signering. Det er derfor viktig at ingen ugyldige eller falske nøkler distribueres, for å unngå at det kan utstedes falske koronasertifikater som feilaktig viser gyldighet ved kontroll. Distribusjonstjenesten er ikke en sanntidsløsning og oppdateres noen ganger per døgn. Det er kun offentlige nøkler som distribueres, de relaterte private nøklene lagres på andre steder.

De offentlige delene av nøkkelpar som blir distribuert, lagres i nøkkelregisteret. Det bør ikke lagres nøkler som ikke er gyldige, fordi det vil øke sannsynligheten for falsk bruk. Det er i skrivende stund ikke mulig å revokere et nøkkelpar, siden det finnes ikke noen revokeringsliste. Dagens måte å løse dette på har vært å fjerne en offentlig nøkkel fra nøkkelregisteret.

Nasjonal back-end og nøkkeldistribusjonsfunksjonen er av høy verdi for koronasertifikatløsningen.

Kontrollørfunksjon

Kontrollørfunksjonen består av en verifikasjonsapp og en back-end. Appen brukes av en kontrollør, for eksempel en dørvakter ved inngangen til et stort arrangement. Kontrolløren bruker appen for å scanne QR-kode i et koronasertifikat. Verifikasjonsappen validerer om QR-koden er utstedt av en troverdig aktør ved å sjekke at signatur på QR-koden stemmer med en liste over troverdige signeringsnøkler. Appen har tilgang til de troverdige nøklene gjennom app-back-end. Kontrollørfunksjonen forvalter ikke mer informasjon enn det som kan leses ut ifra en QR-kode. Appen blir tilgjengeliggjort via app stores og kan lastes ned av hvem som helst.

Uten kontrollørfunksjon vil det være umulig å validere om koronasertifikatet er ekte eller falsk. Det legges det til grunn at, ut fra en antatt lavt prosent av falske koronasertifikater, midlertidig fravær av verifikasjonsløsningen vil ha begrenset negativ effekt. Falske verifikasjonsapper vil derimot påvirke befolkingens tillit til kontrollørfunksjonen.

I tillegg er det i skrivende stund usikker om fremvisning av et koronasertifikat medfører identifikasjonsplikt for validering at sertifikatet tilhører bæreren.

Kontrollørfunksjon er av middels til høy verdi for koronasertifikatløsningen.

Kobling til EU Gateway

Kobling til EU Gateway tilrettelegger for Europeisk nøkkelutveksling. Med denne koblingen blir det mulig for andre tilkoblete land å validere at et norsk koronasertifikat er utstedt av riktig norsk utsteder, og blir det mulig for norske kontrollører å validere integritet med koronasertifikater fra andre tilkoblete land. Koblingen til EU Gateway vil ikke blir brukt ved validering av norske koronasertifikater i Norge men er nødvendig for at kontroll ved grensepassering kan gjennomføres.

Koblingen til EU Gateway er av høy verdi for koronasertifikatløsningen.

3.3. Databehandling

I databehandlingskapittelet presenteres et sammendrag som redegjør for lagring og innsamling av personopplysninger i koronasertifikatet. Oversikten er basert på foreløpig utkast av DPIA-en, og det henvises til DPIA-en for en fullstendig og grundig gjennomgang og vurdering av personopplysninger og data som lagres i ulike komponenter av løsningen.

Behandling av personopplysninger som er nødvendig for utstedelse og verifikasjon av koronasertifikater for å lette fri bevegelighet i EØS med Europeisk koronasertifikat. Behandlingsgrunnlaget er basert på rettslig grunnlag jf. GDPR artikkel 6 nr. 1 bokstav c (rettslig forpliktelse) og/eller bokstav e (oppgave i allmennhetens interesse), jf. nr. 3 samt artikkel 9 nr. 2 bokstav g om behandling av særlige kategorier av personopplysninger som er nødvendig av hensyn til viktige allmenne interesser.
For behandlingen av personopplysninger som gjelder nasjonalt koronasertifikat er det rettslige grunnlaget de nærmere reglene som åpner for og regulerer bruk av sertifikatet innenlands, jf. GDPR artikkel 6 nr. 1 bokstav c (rettslig forpliktelse) og/eller e (oppgave i allmennhetens interesse), jf. nr. 3, og artikkel 9 nr. 2 bokstav g, eventuelt bokstav i om folkehelsehensyn.

Formålet med behandlingen av personopplysningene er å kunne tilgjengeliggjøre et koronasertifikat for borgerne. Sertifikatet skal være i tråd med EUs Guidelines, sik at innbyggeren kan benytte sertifikatet for å ulike behov i andre EU-land, f.eks. krysse grenser eller få samme lettelser som andre EU-land tilbyr sine innbyggere på bakgrunn av et koronasertifikat. Sertifikatet skal også kunne benyttes til formål i Norge (f.eks. deltagelse i store arrangementer eller kystcruise) og andre land. Hvilke øvrige formål et sertifikat skal benyttes til er ikke klarlagt, men det vil være innbyggeren som beslutter om et koronasertifikat skal opprettes, lastes ned og benyttes. De som ønsker fremlagt et koronasertifikat vil trenge et behandlingsgrunnlag for det.

QR-koden brukes for å verifisere hvorvidt man er vaksinert, har hatt covid-19, eller har testet negativt for covid-19 de siste 24-timene. QR-koden inneholder derfor opplysninger om dette og hvor lang varighet gyldigheten har. Identifiserende informasjon i QR koden består av:

- Innenlands bruk (Trinn 3): én bokstav fra fornavnet, tre bokstaver fra etternavnet, og fødselsår;
- EU Grensepassering (Trinn 4): fult navn og full fødselsdato.

3.4. Avgrensning av risikovurdering

I arbeidet med risiko- og sårbarhetsanalysen av Koronasertifikatløsningen er det gjort avgrensninger for å fokusere innsatsen mot de mest kritiske komponentene. Samtidig har det vært essensielt at avgrensningen ikke går på bekostning av norske innbyggeres sikkerhet og personvern. Avgrensning av omfang er derfor gjort i dialog mellom FHI og NHN.

Risikoer knyttet til personvern er mer ufyllende håndtert i DPIA-en som dekker dette området. Tett samarbeid mellom prosjektgruppene som har utarbeidet DPIA-en og RoS-en har sikret at de mest fremtredende risikoene knyttet til personvern er dekket på alle områder.

I risikovurderingen av sikker utvikling hos leverandøren av nasjonalt back-end og kontrollørtjenesten til koronasertifikat, er analysen avgrenset til å omfatte intervjuer og beskrivelser fra utviklerne. Intervjuene og vurderingene er basert på ledende internasjonale sikkerhetsstandarder, som f.eks. NIST, ISO 27001 og OWASP ASVS. Risikovurderingen er hovedsakelig basert på tillit og samtaler med flere av utviklerne hos leverandøren. Det er ikke gjort risikovurderinger av eventuelle underleverandører til utviklerleverandøren av koronasertifikat.

Det er gjort avgrensninger slik at denne RoS-en ikke omfatter vurdering av økt risiko for angrep mot MSIS, SYSVAK, Helsenorge.no, eller FHI eller NHN sin motstandsdyktighet mot angrep. Det henvises til eksisterende risikovurderinger og iverksatte tiltak når det gjelder risikobilde for de individuelle løsningene.
Denne RoS-en omhandler ikke risiko knyttet til effekt og måloppnåelse av koronasertifikat som tjeneste og heller ikke omdømmerisiko.

4. Metode for risikoforståelse

Dette kapitlet redegjør for risikometodikken som er benyttet i risikoanalysen og definerer kriterier for sannsynlighet og konsekvens som danner grunnlaget for risikovurderingen av Koronasertifikat. En beskrivelse av hvordan det norske sikkerhetsmiljøet er inkludert gjennom en workshopserie, og tilstedeværelsen og bruken av usikkerhet i risikovurderingene er også inkludert.

4.1. Risikometodikk

Denne risikoanalysen er gjennomført i henhold til risikovurderingsmetodikken som benyttes i det norske helsedomenet, basert på ISO 31000 og andre relevante underliggende standarder. Risikoanalysen skal bidra til at FHI på en systematisk måte kan forutse, forebygge og redusere sannsynligheten for, og konsekvensen av, uønskede hendelser relatert til informasjonsbehandlingen i koronasertifikatet. Risikoanalysen er en iterativ prosess med formål å sikre at usikkerhet knyttet til identifiserte risikoer reduseres over tid, at risikonivåer for eksisterende risikoer er oppdatert, samt at oppdukkende risiko kan vurderes. Tre viktige komponenter finnes i en risikovurdering:

- **Verdier:** Informasjon som forvaltes av løsningen, den tekniske løsningen og verdikjeden, for eksempel helseopplysninger, en applikasjon eller sikkerhetsgradert informasjon.
- **Trusler:** Noen eller noe som kan utnytte eller skade verdiene, for eksempel en hacker eller et strømbrudd.
- **Sårbarheter:** Mangel på, eller svakheter i, sikkerhetstiltak som trusselaktørene kan utnytte, for eksempel svak tilgangskontroll eller manglende nødstrøm.

Risiko kan manifestere seg i ulik form og ulik grad av konsekvens. Typiske konsekvenser inkluderer:

- **Liv og helse**, alt fra ubetydelig personskade til dødsfall.
- **Personvern**, alt fra ubetydelig tap av personlig integritet til langvarige konsekvenser for den enkeltes personlig integritet eller anseelse.
- **Regelverk**, alt fra ubetydelig brudd til brudd som medfører vedtak, bøter eller straff.
- **Tjenesteytelse**, alt fra redusert drift til langvarig utilgjengelighet av tjenesten.
- **Omdømme**, alt fra negative oppslag til vesentlig tap av tillit hos brukere og samfunnet.
- **Økonomi**, alt fra ubetydelig økonomisk konsekvens til uopprettelig økonomisk tap.
- **Politikk**, alt fra ubetydelig politisk påvirkning til omfattende politisk påvirkning.

Risikoanalysen har blitt gjennomført som beskrevet under:

1. **Kartlegging av verdier**. Komponentene i koronasertifikatet og informasjonsverdiene som forvaltes av systemene har blitt identifisert og klassifisert. Identifiseringen av informasjonsverdiene danner grunnlag for identifisering av trusselaktører som potensielt kan skade disse.
2. **Kartlegging av trusler**. Trusselaktørene og deres motiv har blitt kartlagt, samt angrepsvektorene som kan benyttes.
3. **Kartlegging av sårbarheter**. Komponentene og verdikjeden har blitt vurdert.
4. **Etablering av risikoscenarier**. En oversikt over mulige scenarier har blitt etablert. Et risikoscenario skal bestå av en trusselaktør, en uønsket hendelse knyttet til informasjonsverdi(er) som kan få noen konsekvenser.
5. **Vurdering av sannsynlighet, konsekvens og usikkerhet**. Ved bruk av standardene for vurdering av sannsynlighet, konsekvens og usikkerhet i helsedomenet (kapittel 4) har de ulike faktorene blitt vurdert for hvert risikoscenario.
6. **Gruppering og rapportering**. Risikoscenariene har blitt gruppert slik at det blir lettere å få oversikt over de scenariene som har felles faktorer.

4.2. Workshopserie med eksternt fagmiljø

FHI holdt en workshopserie i forbindelse med Koronasertifikat Trinn 3 og Trinn 4. Formålet med workshopserien har vært å involvere fagmiljøet utenfor FHI i diskusjon rundt risikoscenariene og tiltak. FHI har fått konkrete innspill på scenarier, og tiltak forbundet med disse, fra fagmiljøet. FHI er veldig takknemlig for fagmiljøets innspill.

Workshopserien har fulgt følgende tematikk:

- Workshop 1 innledet arbeidet med en innføring i arbeidsmetode og veien så langt.
- Workshop 2 tilspisset arbeidet med fokus på «digital etikk».
- Workshop 3 fokuserer på tematikken «kryptografi».
- Workshop 4 tok for seg «personvern».
- Workshop 5 fokuserer på «informasjonssikkerhet».

Innspillene fra fagmiljøet har vært med på å prioritere og forme RoS-arbeidet, slik at der sikres en helhetlig dekning. Med åpenhet og innsikt fra flere hold har det vært mulig å bedre bevare helhetlig sikkerhet i Koronasertifikatet.

4.3. Usikkerhet i forståelse av risiko over tid

Løsningen består av mange komponenter og leverandører med gjensidige avhengigheter. Analyseresultatene i denne rapporten baserer seg på beste praksis og vurderinger etter godt faglig skjønn. Samtidig er det viktig å poengtere at dette er en løsning i en aktiv utviklingsfase, og vurderingene vil derfor inneholde varierende grad av sikkerhet basert på graden av innsikt i hvordan tiltak er implementert i løsningen som settes i produksjon. Denne risikoanalysen tar høyde for graden av usikkerhet i forståelsen av risiko. Den sanne eller objektive risikoen er det ingen som kjenner. Det er derfor tatt høyde for at vurdering av etterlevelse i henhold til beste praksis kan utføres periodisk slik at grad av usikkerhet i risikoforståelsen kan reduseres. Dette gjøres ved å tallfeste grad av etterlevelse av tiltak hvor beste praksis benyttes for å dekke løsningens behov for risikoreduserende tiltak.

4.4. Risikobehandling

Risikoscore fastsettes som et resultat av produktet sannsynlighet og konsekvens iht tabellen nedenfor.

Risikonivå	Score	Tiltak
Lav	1-3	Ingen tiltak nødvendig
Moderat	4-8	Hendelsene skal vurderes nærmere og eventuelle tiltak iverksettes eller risiko aksepteres
Høy	9-16	Risikoreduserende tiltak skal iverksettes

Behandlingen og iverksettelse av tiltak er dokumentert i en risikobehandlingsplan. Risikobehandlingsplanen inneholder:

- Beskrivelse av oppfølgingspunkter for hver risiko.
- Beskrivelse av behandlingsalternativ og ytterligere tiltak.
- Definering av tiltakseier og frist. Alle tiltak skal ha en ansvarlig tiltakseier med frist for iverksettelse.

Det er utarbeidet akseptansekriterier for risiko og usikkerhet som en del av prosessen for å behandle risiko. NHN sine etablerte matriser benyttes til dette.

4.5. Kommunikasjon og lederforankring

Risikoeier er FHI. FHI skal sørge for at risiko rapporteres regelmessig for å ivareta lederforankring. Disse skal også ivareta kommunikasjon mot andre relevante interessenter.

Risikovurderinger skal oppdateres ved endringer som kan påvirke risikobildet.

4.6. Risikotabeller

4.6.1. Tabell for vurdering av sannsynlighet

Kriterier for valg av sannsynlighet			
Verdi	**Beskrivelse**	**Erfaring/Trend?**	**Beskrivelse letthet**
4	**Meget sannsynlig**	Har skjedd hos oss og andre.	• Sikkerhet er ikke etablert. • Krever små til normale ressurser av egne medarbeidere eller eksterne for å brytes. • Ikke nødvendig med kjennskap til tiltakene. • Sikkerhetstiltak er sterkt avhengig av at en eller flere manuelle rutiner/policyer følges
3	**Sannsynlig**	Har hørt om hos andre, kunne like gjerne vært hos oss.	• Sikkerhetstiltak er ikke fullt etablert i forhold til sikkerhetsbehovet. • Sikkerhetstiltak fungerer ikke etter hensikten. • Egne medarbeidere trenger kun små til normale ressurser for å bryte tiltakene. • Eksterne trenger små/normale ressurser og normal kjennskap til tiltakene for å bryte disse.
2	**Mindre sannsynlig**	Har hørt om, men aldri hos oss.	• Sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet. • Sikkerhetstiltak fungerer etter hensikten. • Egne medarbeidere trenger små til normale ressurser og normal kjennskap til tiltakene for å bryte disse. • Eksterne trenger gode ressurser og god kjennskap til tiltakene for å bryte disse.
1	**Lite sannsynlig**	Har aldri hørt om.	• Sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet. • Sikkerhetstiltak fungerer etter hensikten. • Krever gode ressurser og godt kjennskap av egne medarbeidere for å brytes. • Eksterne kan ikke omgå tiltakene.

4.6.2. Tabell for vurdering av konsekvens

Kriterier for valg av konsekvens							
Verdi	**Beskr.**	**Personvern**	**Liv og helse** (Berører hvor mange?)	**Regelverk**	**Tjenesteytelse og tidsaspekt i forhold til tjenestekritikalitet** Ute av drift /redusert kvalitet	**Omdømme**	**Økonomi**
4	**Meget stor**	Langvarig tap av anseelse eller personlig integritet • Inngripende personopplysninger om mange personer • Fortrolig eller strengt fortrolig informasjon om mange personer • Særlig kategori personopplysninger om mange personer • Den registrertes rettigheter og personvernprinsippene er ikke ivaretatt	Dødsfall eller alvorlige personskader (flere personer) på grunn av mangel eller feil hos NHN eller underleverandører.	Regelverksbrudd som medfører vedtak, foretaksstraff/bøter og/eller fengselsstraff.	• System som benyttes av alle virksomheter og/eller har stor betydning er midlertidig ute av drift eller redusert. • Stopp/reduksjon omhandler alle brukere. • Personsensitiv informasjon kan ha gått tapt eller kan ikke stoles på.	Vesentlig tap av tillit hos brukere/kunder, eier og andre viktige interessenter. Omfattende og svært negative oppslag i media (redaksjonelle medier og sosiale medier).	Tap på over 50 mill. kroner
3	**Stor**	Tap av anseelse eller personlig integritet som er krenkende • Inngripende personopplysninger om flere personer / eller lite inngripende personopplysninger om mange personer • Fortrolig eller strengt fortrolig informasjon om en eller få personer • Særlig kategori personopplysninger om en eller få personer • Den registrertes rettigheter og personvernprinsippene er ikke tilstrekkelig ivaretatt	Alvorlig personskade (én person) på grunn av mangel eller feil hos NHN eller underleverandører.	Regelverksbrudd som medfører advarsel eller vedtak, samt mulig foretaksstraff/bøter.	• System av stor utbredelse/betydning er midlertidig ute av drift eller redusert. • Stopp/reduksjon som omhandler de fleste brukerne. • Virksomhetskritisk informasjon kan ha gått tapt eller kan ikke stoles på.	Tap av tillit hos brukere/kunder, eier og andre viktige interessenter. Negative oppslag i media over flere dager.	Tap mellom 15 og 50 mill.
2	**Mindre**	Tap av anseelse eller personlig integritet som kan oppfattes som krenkende • Lite inngripende personopplysninger om flere personer • Ingen fortrolig eller strengt fortrolig informasjon • Ingen særlig kategori personopplysninger • Den registrertes rettigheter og personvernprinsippene er i det vesentlige ivaretatt	Mindre alvorlig personskade på grunn av mangel eller feil hos NHN eller underleverandører.	Regelverksbrudd som kan medføre advarsel eller vedtak.	• System av større utbredelse/betydning er midlertidig ute av drift eller redusert. • Stopp/reduksjon som omhandler noen brukere. • Informasjon unntatt offentlighetsloven kan ha gått tapt eller kan ikke stoles på.	Mindre eller kortvarige oppslag i media som kan ved gjentatte tilfeller føre til tap av tillit.	Tap mellom 3 og 15 mill.
1	**Liten**	Ubetydelig tap av anseelse eller personlig integritet • Lite inngripende personopplysninger om få personer • Ingen fortrolig eller strengt fortrolig informasjon • Ingen særlig kategori personopplysninger • Den registrertes rettigheter og personvernprinsippene er ivaretatt	Ubetydelig personskade på grunn av mangel eller feil hos NHN eller underleverandører.	Ubetydelig regelverksbrudd.	• System av mindre utbredelse/betydning er midlertidig ute av drift er midlertidig ute av drift eller redusert. • Stopp/reduksjon som omhandler få brukere. • Åpen/tilgjengelig informasjon kan ha gått tapt eller kan ikke stoles på.	Henvendelse fra media uten negative oppslag.	Tap mellom 500.000 og 3 mill.

4.6.3. Tabell for vurdering av usikkerhet

Ettersom denne løsningen er etablert på svært kort tid og inneholder stor grad av usikkerhet benyttes følgende skala for usikkerhetsvurdering i RoS-analysen og speiler på grad av bevis som er lagt frem. Skalaen definerer *kunnskapsstyrken* bak vurderingene som beskrives og tallfestes (epistemic uncertainty), og ikke iboende «naturgitt» usikkerhet til risikohendelse og dens årsakssammenheng og konsekvensrom (aleatory uncertainty).

Usikkerhets-beskrivelse	**Grad av usikkerhet (konfidensintervaller)**	**Baysian probability [2](%)**	**IPCC skala[3]**	**Legal standard of proof**
Ingen	10 (Helt sikkert)	100-99	Virtually certain	Virtually certain
	9	90-99	Very likely	Clear and convincing evidence
Lav	8	80-90		Clear showcase
	7	67-80	Likely	Substantial and credible evidence
	6	50-67	Middels likelihood	Preponderance of the evidence
Middels	5	33-50		Clear indication
	4	20-33		Probably cause, reasonable belief
	3	10-20	Unlikely	Reasonable indication
Høy	2	1-10		Reasonable
	1	<1	Very unlikely	Inchoate hunch, fanciful conjecture
	0 (Helt usikkert)	0		Insufficient even to support a hunch or conjecture

[2] https://www.bipm.org/utils/common/documents/jcgm/JCGM_100_2008_E.pdf
[3] https://www.ipcc.ch/about/

5. Trusselvurdering

I dette kapittelet presenteres trusselvurderingen i henhold til implementeringen av koronasertifikatløsningen. En trusselvurdering analyserer og vurderer potensielle aktørers evne og vilje til å utføre angrep mot løsningen, inkludert personell, materiell og verdier (produksjon, informasjon og omdømme), samt sannsynligheten for at et angrep vil utføres. I dette kapittelet dokumenteres derfor det overordnete trusselbilde mot FHIs sektor og tjenester, ulike typer trusselaktører, eksempler på motiver for å gjennomføre ulike typer angrep eller anslag, samt aktuelle angrepsvektorer.

Omfanget av trusselvurderingen har fire hovedmål:

- Først tar det sikte på å øke FHIs situasjonsforståelse i henhold til reelle trusler mot sin sektor (både lokalt i Norge samt fra et mer globalt perspektiv) som finnes på nåværende tidspunkt, samt nye fremtredende trusler som kan bli aktuelle i nær fremtid. Dette vil gi en oversikt over potensielle trusler mot koronasertifikatløsningen samt trusselaktører som kan ha interesse av å utnytte den og hvilke formål de har.
- Basert på dette så vil trusselvurderingen gjøre det enklere for FHIs ledelse, beslutningstakere og analytikere å ta bedre og mer effektive avgjørelser for sikkerheten rundt koronasertifikatløsningen.
- Trusselvurderingen vil også benytte tidligere og nylige hendelser mot helsesektoren og lignende løsninger for at FHI skal kunne utarbeide bedre sikkerhetsstrategier for koronasertifikatløsningen.
- Til slutt vil trusselvurderingen ta sikte på å gi en forståelse for hvordan endringer i trussellandskapet kan påvirke både FHI og koronasertifikatløsningen, både direkte og indirekte, både når det gjelder eksterne og interne risikoer.

Det er viktig å påpeke at vurderingene som blir fremhevet i dette kapittelet er skrevet med forbehold om at det er et høyt usikkerhetsmoment knyttet til koronasertifikatløsningen da den ikke er ferdigutviklet, bruksområder ikke er definert, og man ikke har eksempler på lignende løsninger fra tidligere. Sannsynligheten i disse vurderingene kan dermed endre seg over tid.

Trusselvurderingen har blitt utarbeidet blant annet ved bruk av trusseletterretning. Trusseletterretning er informasjon om trusler og trusselaktører som samlet gir en god nok trusselforståelse til å kunne effektivt identifisere tiltak for å forhindre eller minske skadeomfanget. Informasjonen og vurderingene som er utredet i dette kapittelet er basert på ulike typer åpne kilder, inkludert norske myndigheters årlige åpne trusselrapporter, eksempelvis fra Nasjonal Sikkerhetsmyndighet (heretter NSM), Politiets Sikkerhetstjeneste (heretter PST) og Etterretningstjenesten. Essensen i trusseletteretningsarbeid er å sette rett informasjon i rett kontekst, og at dette er med på å effektivt utbedre sikkerheten til FHI sin koronasertifikatløsning. Trusseletterretning skal skille ut handlingsbar etterretning fra den store og støyende informasjonsmassen som finnes. Dette for å forstå trusselaktører i kontekst, slik at trusseletterretning kan innlemmes i FHIs måte å gjøre sikkerhet på en effektiv måte som gjenkjenner og responderer til mulige trusler. For å sette trusseletterretning i kontekst benyttes ulike nivå og mål for trusseletterretning som vil bli videre definert i seksjonen under.

5.1. Metode

I denne rapporten vil implementering av koronasertifikatet og trusler knyttet til dette vurderes på tre nivå; Strategisk, Operasjonelt, og Taktisk. Hvert nivå tar for seg ulik type informasjon og målgrupper. Målet med denne inndelingen er at trusselvurderingen blir kategorisert på en mer hensiktsmessig og effektiv måte for de ulike interessenter involvert i arbeidet med koronasertifikatløsningen, dette for å bedre kunne støtte oppunder deres respektive ansvarsområder. Man kan også identifisere gap og gjøre sikkerheten i henhold til koronasertifikatet mer tilpasningsdyktig.

Strategisk nivå: På dette nivået fokuserer FHI på overordnede risikoer og implikasjoner assosiert med trusler som kan påvirke FHIs virksomhet og koronasertifikatløsningen. Informasjon på dette nivået fokuserer altså på *hvem* og *hvorfor*, og hjelper ledelsen og ulike beslutningstakere til å ta informerte beslutninger og sikre samsvar mellom strategi for løsningen og den reelle risikoen FHI står ovenfor. Et hypotetisk eksempel på dette kan være at en statlig aktør ønsker å få tilgang til FHI og koronasertifikatløsningens systemer og data. Kilder som den strategiske trusseletterretningen baserer seg på inkluderer norske myndigheters årlige åpne trusselrapporter, eksempelvis fra NSM, PST og Etterretningstjenesten.

Operasjonelt nivå: På dette nivået fokuser FHI på trusselaktørenes motivasjon, intensjon og kapabilitet. Informasjon på dette nivået fokuserer altså på *hvordan* og *hvor.* Overordnet så gir dette analytikere og andre på SOC team eller CSIRT teams en inngående forståelse av det reelle trusselbildet mot løsningen, og hjelper med utbedringen av hendelseshåndtering. På dette nivået kan vi for eksempel se at den statlige aktøren som ønsker å få tilgang, vil oppnå dette gjennom et leverandørkjedeangrep mot leverandøren av kontrollørtjenesten. Kilder som den operasjonelle trusseletterretningen baserer seg på inkluderer blant annet dybderapporter fra ulike sikkerhetsleverandører og analytikere som omhandler aktuelle trusselaktører, deres metoder og tidligere angrep.

Taktisk nivå: På taktisk nivå fokuserer FHI på identifikasjon av indikatorer på eksisterende eller fremvoksende trusler mot koronasertifikatløsningen. Informasjon på dette nivået fokuserer altså på *hva.* Dette kan være for eksempel IP-adresser, domener, og e-post adresser, og hjelper analytikere å forbedre og finjustere defensive systemer i henhold til deteksjon av potensielle trusler. Dette vil for eksempel kunne være spesifikke e-post adresser som den statlige aktøren bruker til å sende phishing e-poster til FHIs underleverandør for å initiere leverandørkjedeangrepet. Kilder som den taktiske trusseletterretningen baserer seg på inkluderer rapporter og artikler fra ulike sikkerhetsleverandører som utreder spesifikke indikatorer assosiert med en gitt trusselaktør eller spesifikke nettverksoperasjoner.

5.2. Overordnet trusselbilde

5.2.1. Trusler mot Norge

Trussellandskapet innenfor cyberdomenet har alltid vært i stadig endring og reflekterer ofte de endringene eller hendelsene som man ser i samfunnet, både på nasjonalt og globalt nivå. De årlige åpne trusselrapportene fra NSM, PST og Etterretningstjenesten fremhever noen sentrale vurderinger av det nåværende trusselbilde mot FHIs sektor og tjenester. Disse vurderingen danner et godt og bredt grunnlag for vurderinger av potensielle trusler mot koronasertifikatløsningen.

NSM har bemerket seg at trusselaktører tilpasser seg endrede situasjoner raskt og utnytter nye sårbarheter som oppstår. Dette har ikke minst vært tilfellet det foregående året da Covid-19 pandemien har ført til flere store samfunnsendringer. Ifølge NSM har det blant annet ført til raskere digitaliseringstakt i flere områder under pandemien, noe som har åpnet opp for nye og flere potensielle sårbarheter og ført til et skjerpet digitalt risikobilde. NSMs rapport vurderer at dette har gjort at risikoen har økt det siste året for flere ulike sektorer, inkludert helsesektoren, og at denne økte risikoen forventes å vedvare i 2021. Risikoer inkluderer blant annet personellmessige- og IKT sårbarheter som følge av endrede arbeidsmønstre og raskere digitalisering. Det blir også bemerket i rapporten at deler av helsesektoren har fått høyere verdi som følge av sin avgjørende rolle i håndteringen av Covid-19 pandemien.

Overordnet så vil de største og mest alvorlige truslene mot Norge og norsk helsesektor komme fra statlige aktører ifølge Etterretningstjenestens FOKUS rapport. Under pandemien har ulike statlige aktører gjennomført ulike typer påvirkningsoperasjoner. Statlige aktører har blant annet gjennomført desinformasjonskampanjer siktet mot vaksiner utviklet i vesten, som Pfizer og Moderna, med mål om å forbedre konkurransegrunnlaget for sine egne vaksiner. Ifølge Etterretningstjenesten har påvirkningsoperasjonene også fokusert på å påvirke ulike politiske prosesser. I tillegg til påvirkningsoperasjoner har statlige aktører ifølge Etterretningstjenesten også evnen til å utføre destruktive operasjoner for sabotasje og avskrekking. Etterretningstjenesten rapporterer at det er sannsynlig at utenlandsk etterretning vil gripe inn i helsesektoren da helseinformasjon generelt har høy etterretningsverdi og er av interesse. PST vurderer at nettverksoperasjoner vil utgjøre den største delen av utenlandsk etterretning mot Norge.

Trusler mot FHIs sektor stammer ikke bare fra nettverkoperasjoner som blir utført av statlige aktører men også av andre trusselaktører, som for eksempel organiserte cyberkriminelle, samt enkeltindivider. I følge NSM har det vært en endring i type nettverksangrep disse trusselaktørene benytter seg av, og har merket seg en generell økning av økonomisk motivert aktivitet, særlig løsepengevirusangrep. Telenor har bemerket at angrep som løsepengevirusangrep ikke lenger bare blir initiert av mer tradisjonelle metoder som phishing e-post på data, men også at det er blitt mer av løsepengevirusangrep (og andre typer skadevarer) mot mobiler.

PSTs rapport fremhever også en utvikling i mer sammensatte trusler, som for eksempel leverandørkjedeangrep hvor tredjeparter eller underleverandører blir utsatt for angrep, som da kan få alvorlige konsekvenser for virksomhetens kunder samt for andre virksomheter i forsyningskjeden[4]. Denne typen angrep er muliggjort ettersom de fleste virksomheter er avhengig av digitale komponenter eller tjenester som ofte leveres fra eller har forgreininger i utlandet. NSM fremhever i sin rapport at dette sårbarhetsbildet er blitt tydeliggjort under Covid-19 med tanke på norske virksomheters avhengighet av leverandørkjeder, inkludert virksomheter og tjenester innenfor helsesektoren. Det finnes også potensial for innsidetrusler i henhold til både tilsiktede og utilsiktede handlinger, som for eksempel utilsiktet deling av sensitiv informasjon og spionasje.

5.2.2. Europa og resten av verden

Ser man litt utover Norges grenser så rapporterer også European Union Agency for Cybersecurity (heretter ENISA) mye av de samme observasjonene som NSM og PST hva angår digitale trusler mot helsesektoren i Europa. ENISA fremhever at helsesektoren i Europa generelt har i større grad blitt digital og mer sammenkoblet under pandemien. Pasienthelsejournaler er tilgjengelig som elektronisk informasjon for medisinsk personell, data fra medisinsk utstyr blir lastet opp i skytjenester, ulike helsetjenester er tilgjengelig for pasienter via applikasjoner, og flere oppgaver og områder blir automatisert. Denne økte avhengigheten av sammenkoblede systemer og enheter har introdusert en rekke nye utfordringer og potensielle trusler som må imøtekommes av hver enkelt Europeisk land.

Nå da det arbeides med en felles europeisk koronasertifikatløsning og retningslinjer for medlemslandene blir etablert, fremheves også flere andre potensielle risikoområder. Dette inkluderer blant annet personvern samt faren for forskjellsbehandling mot dem som ikke kan bli vaksinert grunnet medisinske eller økonomiske årsaker. Når FHI implementerer koronasertifikatløsningen i Norge er det sannsynlig å tro at FHI vil treffe på de samme risikoene. Videre, når Norges koronasertifikatløsning blir koblet opp mot resten av Europa og globale koronasertifikatløsninger vil disse risikoområdene og den totale angrepsflaten øke, og trusselbilde mot Norge og koronasertifikatet utvides. Sikkerheten til den norske løsningen vil da også bli mer avhengig av andre lands sikkerhetsledelse og tiltak i henhold til deres helsesektor og helseinstitusjoner, koronasertifikatløsning og underleverandører.

[4] Info Security, “Codecov Supply Chain Attack May Hist Thousands:Report”, https://www.infosecurity-magazine.com/news/codecov-supply-chain-attack-may/
We Live Security, “Lazarus supply-chain attack in South Korea”, https://www.welivesecurity.com/2020/11/16/lazarus-supply-chain-attack-south-korea/
Security Boulevard, “Sodinokibu Ransomware Gang Extorts Apple Through Supply Chain Attack”, https://securityboulevard.com/2021/04/sodinokibi-ransomware-gang-extorts-apple-through-supply-chain-attack/

FHIs trusselvurdering for koronasertifikatløsningen:

- Ut fra egenarten til koronasertifikatløsningen vil det overordnet være **høyst sannsynlig** at den fanger interessen til eksterne **etterretningstjenester**, samt profesjonelle internasjonale **cyberkriminelle** individer og grupper som vil forsøke å utnytte løsningen med spionasje, påvirkningsoperasjoner, eller økonomisk vinning som formål**.** Dette er basert på de nåværende vurderingene til norske myndigheter av utenlandske etterretningstjenester og internasjonale kriminelle, med forbehold om at det er et **høyt usikkerhetsmoment** knyttet til koronasertifikatløsningen da den ikke er ferdigutviklet, bruksområder ikke er definert, og man ikke har eksempler på lignende løsninger fra tidligere. Sannsynligheten i denne vurderingen kan dermed endre seg over tid.

5.3. Trusselaktører

I sine rapporter peker NSM, PST og Etterretningstjenesten særlig mot fremmede staters etterretningsmiljøer og internasjonale kriminelle miljøer, og deres aktiviteter mot norske interesser i det digitale rom, som reelle trusler mot Norge. I henhold til helsesektoren spesifikt, og implementeringen av koronasertifikatløsningen, kan andre typer trusselaktører som nevnes i rapportene også utgjøre potensielle trusler. I tabellen under vises en oversikt over de vanligste typer trusselaktører, hva de ulike trusselaktørene vanligvis har som mål, samt noen tiltenkte eksempler på hvordan ulike verdier i koronasertifikatløsningen kan samsvare med de ulike trusselaktørenes mål.

	Motivasjonsfaktorer	Kapabilitet (Kapasitet og TTP)	Kjente hendelser
Organisert kriminalitet og cyberkriminelle grupper – nasjonal og internasjonalt	• Økonomisk vinning • Rennommé/Rykte (blant cyberkriminelle)	• Phishing • Social engineering • Business email compromise (BEC) • Botnet • Skadevare/løsepengevirus • Passord angrep • Utnyttelsessett	• Tilgang til persondata • Tilgang til helseopplysninger • Tilgang til brukerkontoer • Stjeling av finansdata • Ulovlige/falske transaksjoner • Utpressing og bruk av IT ressurser
Stater og statssponsede grupper	• Spionasje (politisk, økonomisk, eller militært) • Forhindring/ødeleggelse av prosesser • Påvirkning av prosesser	• Spear-phishing • Passordangrep • Social engineering • Manipulering/eksfiltrering av data • Fjerntilgang Trojanere (RAT) • Skadevare/Løsepengevirus • Leverandørkjedeangrep	• Strategisk planer • Angrep på underleverandører • Arkitekturskisser (system, nettverk, applikasjon) • Forretningshemmeligheter • Informasjon om fusjon og oppkjøp • Informasjon om kritisk infrastruktur
Hacktivister	• Politisk, sosial eller ideologisk motivasjon	• Manipulering av publikasjoner/nettsider • Doxing • DDoS angrep	• Spredning av politisk/ideologisk ladet budskap • Stopp/nedetid av tjenester
Innsideaktør – tilsiktede og utilsiktede handlinger	• Personlige økonomiske motiver • Hevn mot personer eller arbeidsplass • Spionasje (om innsider er affiliert med statlig eller kommersiell aktør)	• Eksfiltrering av data • Misbruk av privilegier/tilgang til systemer, nettverk eller informasjon • Social engineering (som fører til at en ansatt utilsiktet deler sensitiv informasjon)	• Utilsiktet deling av sensitiv informasjon om løsningen og/eller brukere til trusselaktører • Stjele, sabotere, lekke, offentliggjøre sensitiv informasjon • Forberede spionasje, eller manipulasjon av beslutningsprosesser og/eller handlinger. Bistand til avlytting, hacking etc. • Stopp av tjenester/nedetid
Cyberterrorister	• Propaganda • Økonomisk vinning • Spionasje • Politisk, sosial eller ideologisk motivasjon	• Lekking av data • Manipulering av nettsider • Tjenestenektangrep mot nettsider • Angrep mot samfunnskritiskfunksjoner	• Stopp av tjenester/nedetid • Spredning av politisk/ideologisk ladet budskap • Stjele, sabotere, lekke, offentliggjøre sensitiv informasjon

FHIs trusselvurdering for koronasertifikatløsningen:

- Det er **sannsynlig** at statlige aktører kommer til å ha koronasertifikatet som angrepsmål. Det er **sannsynlig** at statlige aktører vil utnytte potensielle sårbarheter i løsningen til å utføre spionasje- og kartleggingsaktiviteter ved å gjennomføre sofistikerte angrep og innhente sensitiv, strategisk data fra FHI og/eller NHN. Det er **lite sannsynlig** at statlige aktører vil utføre sofistikerte angrep mot den norske koronasertifikatløsningen for å innhente helseopplysninger om norske innbyggere.
- Det er **sannsynlig** at organiserte kriminelle aktører kommer til å utnytte ulike komponenter av, og potensielle sårbarheter i koronasertifikatløsningen som plattform for kriminell økonomisk vinning. Slike trusselaktører vil **sannsynlig** ha som formål å få tilgang til persondata, helseopplysninger eller brukerkontoer for å tjene profitt ved å selge dataen, eller for å utføre videre cyberangrep.

5.4. Digitale operasjoner og andre anslag: motiv, angrepsvektorer og typer angrep

Digitale operasjoner og andre typer angrep mot norske myndigheter og virksomheter kan komme i mange ulike former. Som tabellen ovenfor viser, så har ulike trusselaktører forskjellige mål, og disse målene er basert på hva de har som motiv. Motiv, samt trusselaktørenes kapabiliteter og ressurser avgjør i stor grad hvilke type angrep de har mulighet til, og ønsker å utføre, samt angrepsvektorer de benytter. Denne seksjonen vil utrede de ulike motivene til trusselaktørene, samt gjennomgå de vanligste angrepsvektorene og relevante typer angrep man har observert i nyere tid.

5.4.1. Motiv

Etterretnings- og kartleggingsaktivitet er ofte motivet for særlig stater og statssponset grupper som har som mål å innhente mest mulig informasjon om norske verdier. Både virksomheter og enkeltpersoner kan være i søkelyset, og under pandemien har særlig helsesektoren og ulike helseorganisasjoner, som for eksempel European Medicines Agency (EMA), vært av interesse for statlige aktører. Under pandemien har flere statlige aktører blitt anklaget for å ha forsøkt på ulike måter å stjele verdifull forskning og informasjon om vestlige vaksiner som Moderna, Astra Zeneca og Pfizer.

Økonomisk vinning kan være drivkraften for mange ulike trusselaktører, inkludert cyberkriminelle med mindre ferdigheter, individuelle hackere, organiserte kriminelle, statsstøttede grupper og stater. Under pandemien har helsesektoren vært utsatt for et økende antall angrep fra ulike trusselaktører med økonomisk vinning som mål. Ofte så driver trusselaktørene enten med pengeutpressing, stjeling av verdifull data og selge det for profitt på ulike cyberkriminelle plattformer, eller på andre måter lure sine mål til å betale for noe eller oppgi andre opplysninger som for eksempel kredittkortinformasjon.

Påvirkningsoperasjoner blir ofte brukt til å påvirke beslutninger eller demokratiske prosesser, både mot virksomheter og myndigheter på både lokalt og nasjonalt nivå. Dette er også et motiv som ofte er forbundet med særlig statlige aktører som har som mål å påvirke ulike prosesser i Norge til deres fordel.

Industrispionasje kan gjennomføres for økonomisk vinning, og/eller som middel for å avansere egen forskning og utvikling gjennom tyveri av intellektuelle verdier. Overordnet så er industrispionasje et motiv for både statlige aktører og blant konkurrerende virksomheter og organisasjoner. I Norge har risikoen for industrispionasje særlig blitt fremhevet i henhold til norske utdannings- og forskningsinstitusjoner som ansetter utenlandske arbeidere fra land Norge ikke har sikkerhetssamarbeid med.

Digital sabotasje kan brukes som ledd i hybrid krigføring og/eller benyttes som et pressmiddel i en påvirkningsoperasjon. Digital sabotasje blir brukt som et verktøy for å ødelegge, forsinke, eller stoppe ulike prosesser hos norske virksomheter. Større og mer omfattende digitale sabotasjer blir gjerne utført av trusselaktører som har både sterke kapabiliteter og ressurser, inkludert statlige aktører eller andre godt organiserte og ressurssterke kriminelle grupper. Mindre operasjoner, som manipulering av nettsider («defacement»), kan potensielt bli utført av mindre ressurssterke aktører som politisk- eller ideologisk motiverte hackergrupper.

5.4.2. Angrepsvektorer

Angrepsvektorer er metoden en trusselaktør velger å initiere et angrep på. NSM, PST og Etterretningstjenesten peker i sum på følgende angrepsvektorer som benyttes for å gjennomføre digitale operasjoner og andre typer anslag:

- **E-post som angrepsvektor:** PST og NSM beskriver at den vanligste måten for en trusselaktør å komme seg på innsiden av et nettverk på er ved å sende skadevare via målrettede e-poster. Et slikt angrep utnytter både digitale og personellmessige sårbarheter.
- **Sårbare internettjenester som angrepsvektor:** PST og NSM peker på at servere som er koblet mot internett brukes som inngangsport til virksomheters nettverk. Et slikt angrep utnytter digitale sårbarheter.
- **Personell som angrepsvektor:** PST beskriver hendelser der trusselaktører bryter seg inn i datanettverk ved å få ansatte bevisst eller ubevisst til å plassere skadevare via f.eks. minnepinner. Etterretningstjenesten og PST peker særlig på faren for innsidetrusler ved at sentrale personer i virksomheter og hos myndigheter kultiveres og rekrutteres til etterretningsformål. Et slik angrep utnytter personellmessige sårbarheter
- **Digitale verdikjeder som angrepsvektor:** NSM, PST og Etterretningstjenesten peker alle på utfordringen med lange digitale verdikjeder. Trusselaktører angriper virksomheter som ikke er mål i seg selv, men som vil fungere som brohode for videre tilgang til andre mål. Et slikt angrep utnytter både digitale og personellmessige sårbarheter, samt sårbarheter i virksomheters sikkerhetsstyring.
- **Svakheter i sikkerhetsstyringen:** NSM peker på at svak sikkerhetsstyring fører til ubalanse mellom håndteringen av digitale, personellmessige, virksomhetsmessige og fysiske sikringstiltak. Denne ubalansen leder til sårbarheter som kan utnyttes som angrepsvektorer.

5.4.3. Angrepstyper

Løsepengevirus, hvor trusselaktører krypterer deler av inneholder på en infisert datamaskin for så å kreve løsepenger for å gjøre innholdet tilgjengelig igjen, har blitt svært hyppig brukt under Covid-19. Helsesektoren har vært den tredje mest utsatte sektoren for løsepengevirus under Covid-19. Løsepengevirus blir brukt av både av statlige aktører og sofistikerte kriminelle grupper som utvikler egne løsepengevirus, eller kriminelle som kjøper ferdige «løsepengevirus-pakker» på cyberkriminelle plattformer.

«Account takeover» er en populær angrepstype blant trusselaktører hvor de bruker ulike metoder for å få kontroll over brukerkontoer og så enten selger disse videre, eller bruker tilgangen til virksomheters nettverk for videre angrep, som for eksempel løsepengevirusangrep eller for å stjele verdifull informasjon.

Leverandørkjedeangrep er en angrepsform som har blitt fremhevet av NSM i deres trusselvurdering for 2021. Leverandørkjedeangrep utnytter lange, digitale verdikjeder og omfatter et innledende angrep mot en tredjepart eller underleverandør som kan gi trusselaktører videre tilgang til leverandørens kunder eller andre virksomheter i leverandørkjeden. Særlige sofistikerte leverandørkjedeangrep kan gi trusselaktørene muligheten til å overvåke virksomheters nettverk og systemer i lengre perioder uten å bli oppdaget. Oftest er det ulike statlige aktører som har blitt assosiert med store, sofistikerte leverandørkjedeangrep.

Man in the Middle (MITM) angrep er en metode trusselaktører kan bruke til å «lytte» til nettverkskommunikasjon som blir sendt mellom to parter (data og server) og på den måten fange opp og stjele informasjon. Når større deler av arbeidsstyrken til virksomheten jobber hjemmefra som følge av pandemien er de mer utsatt for slike typer angrep som MITM hvor trusselaktører enten avlytter legitime nettverk (som hjemmenettverk eller åpne WiFi forbindelser) eller skaper falske nettverk og lurer sine mål til å benytte seg av denne for å overvåke nettverkskommunikasjonen.

“Social engineering”, eller sosial manipulering, går ut på at trusselaktører forsøker å skaffe seg ulike tilganger ved å manipulere personer til å oppgi verdifull personlig informasjon eller utføre handlinger. Under Covid-19 har man sett eksempler på statlige aktører fra som benyttet seg av sosial manipulasjon for å få tilgang til forskningsdata for koronavaksiner. Trusselaktørene brukte falske sosiale medier profiler for å kontakte forskere med tilbud om å samarbeide på prosjekt, for så å sende dem linker som inneholdt ondsinnede koder. Når forskerne trykte på disse linkene fikk trusselaktørene tilgang til forskernes maskin.

Desinformasjonskampanjer er en form for påvirkningsoperasjon hvor trusselaktører sprer desinformasjon, som regel gjennom ulike digitale plattformer, fora og sosiale medier hvor de kan nå ut til et stort antall individer. Hensikten med å spre desinformasjon er å forsøke å påvirke menneskers oppfatning av et gitt tema, hendelse, politikk, eller annet, i en negativ retning. Under Covid-19 har det vært eksempler på ulike statlige aktører som har spredd desinformasjon om vestlige vaksiner, sannsynligvis i et forsøk på å gi deres egenutviklede vaksine et konkurransefortrinn.

Innsideangrep er en aktivitet hvor en innsider, en nåværende eller tidligere ansatt, konsulent eller kontraktør som har eller har hatt legitim tilgang til virksomhetens systemer, prosedyrer, objekter og informasjon, misbruker denne kunnskapen og tilgangen for å utføre handlinger som påfører virksomheten skade eller tap. Innsideaktivitet kan gjennomføres direkte og på egenhånd, eller på vegne av en ekstern aktør. Eksterne aktører kan være statlige, ikke-statlig eller andre enkeltindivider. Innsideaktivitet kan både være tilsiktede handlinger (f.eks. stjeling av konfidensiell informasjon eller åndsverk) eller utilsiktede handlinger (f.eks. åpning av ondsinnet e-post, bruk av ondsinnet USB). Denne type trussel har vært et kjent fenomen også i Norge, da spesielt fra utenlandske aktører som får innpass i norske virksomheter, og har oftest vært rettet mot forsknings- og utdanningsinstitusjoner.

Tjenestenektangrep, eller distribuert tjenestenektangrep, er når trusselaktører hindrer at noen eller noe får tilgang til informasjon eller ressurser de vil ha tilgang til. Den vanligste formen for tjenestenektangrep er å oversvømme nettstedet med trafikk. Ofte er tjenestenektangrep økonomisk motivert og utført av organiserte kriminelle grupper. Herunder finner man både grupper som har høy kapasitet og utvikler egne, sofistikerte tjenestenekt angrep, samt grupper og individer av lavere kapasitet og som gjerne kjøper tjenestenektangrep «as-a-service» fra andre trusselaktører på kriminelle nettplattformer. Tjenestenektangrep kan også bli brukt av statlige aktører for å sette viktige prosesser og tjenester ute av spill hos virksomheter eller hos myndigheter i andre land. Tjenestenektangrep har blitt mer intense og sofistikerte under COVID-19-pandemien ettersom mange virksomheter hadde vanskeligheter med å støtte den eksterne arbeidsstyrken i løpet av arbeidet hjemmefra.

FHIs trusselvurdering for koronasertifikatløsningen:

- Det er **lite sannsynlig** at statlige aktører vil utnytte potensielle sårbarheter i verifiseringsprosedyren til å utvikle falske kontrollørapper og signeringsnøkler med formål om å spre falske sertifikater til utvalgte personer og sikre dem tilgang til arrangementer og tjenester. Dette kan medføre at det skapes uro blant innbyggere og tilliten til løsningen blir svekket.
- Det er **lite sannsynlig** at statlige aktører eller ressurssterke og kapable kriminelle grupper vil utføre et leverandørkjedeangrep mot underleverandørene knyttet til koronasertifikatløsningen og oppnå tilgang med formål om etterretningsarbeid og kartleggingsaktivitet. Selv om det er lite sannsynlig, vil en slik situasjon kunne få svært alvorlige konsekvenser for FHI og koronasertifikatløsningnen om det skulle oppstå.
- Det er **sannsynlig** at organisert kriminelle grupper og individer vil utnytte potensielle sårbarheter i koronasertifikatløsningen og løsningens verifiseringsprosedyre for å forsøke å utvikle falske koronasertifikat for økonomisk vinning. Dette kan igjen medføre at falske koronasertifikater kommer i omløp.
- Det er **sannsynlig** at organiserte kriminelle vil utnytte potensielle sårbarheter i verifiseringsprosedyren til å utvikle falske kontrollørapper og signeringsnøkler. Slike trusselaktører vil **sannsynligvis** ha som formål å få tilgang til persondata, helseopplysninger eller brukerkontoer for å tjene profitt ved å selge dataen, eller for å utføre videre cyberangrep.

- Det er **sannsynlig** at utenlandske etterretningstjenester vil utnytte følelsen av forskjellsbehandling mellom dem som har koronasertifikat og dem som ikke har, til å utføre påvirkningsoperasjoner og desinformasjonskampanjer for å skape ustabilitet og svekke tilliten til løsningen blant Norges befolkning, med formål om å forbedre konkurransegrunnlaget for sine egne vaksiner, løsninger og politikk.
- Det er **sannsynlig** at statlige aktører kan benytte seg av falske utsendelser av SMS eller e-post (Smishing/Phishing) for å utnytte folks uvitenhet om koronasertifikatløsningen. Formålet til slike aktører vil **sannsynligvis** være å gjennomføre ulike påvirkningskampanjer for å påvirke det norske demokratiet gjennom å skape usikkerhet i befolkningen og redusere tilliten til myndighetene.
- Det er **sannsynlig** at organiserte kriminelle kan benytte seg av falske utsendelser av SMS eller e-post (Smishing/Phishing) for å utnytte folks uvitenhet om koronasertifikatløsningen. Formålet til slike aktører vil **sannsynligvis** være økonomisk vinning gjennom å tilegne seg informasjon som kan benyttes til utpressing, eller omsettes ved salg.
- Det er **sannsynlig** at innsideaktivitet fra statlige aktører kan forekomme i norske virksomheter som FHI og som innehar strategisk viktig og/eller sensitiv informasjon. Statlige aktørers innsideangrep vil **sannsynligvis** kunne rette seg mot ansatte i slike virksomheter som enten har direkte eller indirekte tilgang til sensitiv informasjon, med formål om å innhente informasjon og påvirke beslutninger.
- Det er **høyst sannsynlig** at phishing e-poster vil være en av de mest brukte angrepsvektorene i potensielle angrep eller anslag mot koronasertifikatløsningen, på tvers av alle typer trusselaktører, motiver, angrepstype og formål.

5.5. Diskusjon og konklusjon

I denne trusselvurderingen har FHI sett på de overordnede egenskapene til FHIs nye koronasertifikatløsning, og vi har gjort en betraktning av hva slags type data som vil bli forvaltet i løsningen. Ut fra norske sikkerhetsmyndigheters åpne trusselvurderinger har vi analysert hvordan koronasertifikatløsningen kan ha en effekt på innbyggere, og hvordan den kan være av interesse for trusselaktører. FHI har også gjort en vurdering av sikkerheten for løsningen med tanke på å koble den opp mot EUs overordnede koronasertifikatløsning og medfølgende standarder.

Ut fra egenarten til koronasertifikatløsningen, og særlig med innsikten fra Etterretningstjenestens Fokus 2021, vil det være nærliggende å tro at utenlandske etterretningsmiljøer vil være spesielt opptatt av hvordan de kan benytte koronasertifikatet til å blant annet få tak i personlig informasjon om norske innbyggere samt se på muligheten til å gjennomføre ulike påvirkningsoperasjoner mot koronasertifikatet for å potensielt svekke tilliten til løsningen og prosessen bak. Det finnes flere nyere eksempler på at utenlandske etterretningsmiljøer sannsynligvis har utført dataangrep mot norske myndigheter[5], noe som støtter oppunder vurderingene til Etterretningstjenesten. Organiserte kriminelle vil sannsynligvis også være interessert i å få tak i personlig informasjon for økonomisk vinning da helseinformasjon har fått økt verdi blant kriminelle på ulike digitale plattformer som kriminelle benytter seg av. Organiserte kriminelle vil sannsynlig ha som mål å hente ut persondata som er lagret i den nye digitale koronasertifikatløsningen gjennom sofistikerte digitale angrep.

Ved tilkobling opp mot EUs koronasertifikatløsning tar FHI utgangspunkt i at trusselaktørene, motiv, og angrepsvektorene bak potensielle handlinger forblir det samme. Til nå har sikkerhetsaspektet, kontroll og styring ved smittestoppapplikasjonen kun berørt den norske løsningen. Ved oppkoblingen mot EU vurderes det at sikkerhetsaspektet, kontroll og styring potensielt endres ved at angrepsvektorene brer seg utover et mye større geografisk område som ligger utenfor norsk kontroll. Land med en annen geopolitisk posisjon, andre styringstradisjoner og sikkerhetskultur kan således bli utsatt for en trusselaktør, og enten direkte eller indirekte ramme norske interesser. Det kan skje uten norske myndigheters kontroll, og det kan ta tid før et slikt sikkerhetsbrudd er identifisert. Det vil kunne gi en økt risiko i gitte scenarier ved at sannsynligheten øker i takt med eksponeringsflaten. En trusselaktør vil kunne benytte seg av flere verktøy og utnytte svakheter som:

- Andre nasjoners sikkerhetsimplementering hos nasjonale helsemyndigheter og i deres nasjonale back-end løsninger.
- Kommunikasjon og åpenhet rundt utfordringer, oppdatering og koding.
- Sikkerhetskultur og styringstradisjoner.

Ved en gjennomgang av tilgjengelig informasjon er det ikke funnet indikatorer som bekrefter at digitale koronasertifikatløsninger i andre land har vært offer for slike angrep per dags dato. Dette er mest sannsynlig fordi de fleste land er på et relativt tidlig stadium hva gjelder utarbeidelsen av koronasertifikatløsninger. På den andre siden har det allerede vært rapportert at produksjon av falske vaksinekort har blitt en lukrativ virksomhet for kriminelle, og det er sannsynlig at dette vil fortsette fremover etter hvert som koronasertifikatløsningen utarbeides.

Utenom trusselaktørene og deres respektive motivasjoner og kapabilitet som er beskrevet ovenfor i trusselvurderingen, kan det vurderes at koronasertifikatet også vil ha effekt på ulike norske aktører (innbyggere, virksomheter og politikere), prosesser og verdier. Disse igjen vil potensielt kunne påvirke det overordnete risikobildet, inkludert følgende:

- Risikoen for forskjellsbehandling mellom innbyggere som får koronasertifikat og dem som ikke har det.
- Risikoen ved lagring av persondata/helseopplysninger hos ulike aktører som benytter seg av løsningen.
- Risikoen ved bruk av eventuelle alternative, analoge løsninger.

Potensielle anslag mot disse risikoområdene fra tradisjonelle trusselaktører som organiserte kriminelle kan blant annet føre til at tilliten til løsningen svekkes, og at sensitive personopplysninger kan komme på avveie. Innbyggere kan også reagere på bestemmelsene til norske myndigheter innenfor disse risikoområdene og potensielt føre til handlinger blant norske innbyggere og andre aktører som kan påvirke løsningens mulighet til å effektivt oppfylle sin tiltenkte funksjon.

[5] https://www.digi.no/artikler/pst-etterforsker-it-angrepet-stortinget-vil-ha-ekstern-evaluering/508249

6. Risiko

Dette kapitlet beskriver risikoscenarier og tiltak knyttet til ulike komponenter av koronasertifikatløsningen. Scenarienes sannsynlighet, konsekvens og usikkerhet vurderes, i tillegg til at etterlevelse av foreslåtte tiltak gjennomgås. For å illustrere viktigheten av risikoene totalt og for hver komponent, er risikoene kategorisert i risikomatriser.

Risikoscenarier deles opp i 6 områder:

1. **Hele løsningen**: risikoscenarier som går på bruk av koronasertifikatet og kontrollørfunksjonen i samfunnet.
2. **Digital etikk**: risikoscenarier som går på bruk av teknologi med helserelatert formål.
3. **Kryptografi**: risikoscenarier som går på digitale sertifikater og signaturløsninger.
4. **Personvern**: risikoscenarier som går på beskyttelse av sensitiv informasjon.
5. **Informasjonssikkerhet**: risikoscenarier som går på konfidensialitet, integritet og tilgjengelighet med løsningen.
6. **Analog kanal**: risikoscenarier som går på å bestille et koronasertifikat uten digitale midler.

6.1. Vurdering av risiko – Hele løsningen

ID#	Tittel	Scenario	Beste praksis	Vurdering før ytterligere tiltak		
	Scenariotittel	Scenariobeskrivelse	Tiltak	S	K	U
R1-1	Uklarheter rundt bruksområder og varighet med korona-sertifikatet	For å starte gjenåpningen av samfunnet har regjeringen besluttet å ta i bruk et koronasertifikatet som dokumentasjon for å gi lettelser til vaksinerte, personer med immunitet etter gjennomgått koronasykdom eller negativt testresultat. Dette vil kunne bidra til å legge til rette for en gradvis og kontrollert gjenåpning av samfunnet og senere også grensekryssinger mellom EU-land. Regjeringen definerer noen bestemte bruksområder hvor det kan være aktuelt å kreve et koronasertifikat ved tilgang. Samtidig blir (private) arrangører gjort ansvarlig for å ordne bruk av koronasertifikat ved arrangement. En arrangør mangler kompetanse og veiledning i å gjøre det og får dermed utfordringer i å tilrettelegge for sømløs bruk av koronasertifikat. I tillegg klarer ikke arrangøren å tydeliggjøre til deltagere at koronasertifikat kreves, som fører til at mange deltagere står ved døren uten sertifikat. Dette svekker tillit til sertifikatet og fører til misnøye og uro i samfunnet. Helse- og omsorgsdepartementet foreslår et nytt midlertidig kapittel 4A i smittevernloven om koronasertifikat. Lovendringene vil gi et lovgrunnlag for å etablere et tidsbegrenset system for verifisert dokumentasjon av vaksinasjonsstatus, immunitet etter gjennomgått koronasykdom og testresultat. En tid etter innføring av koronasertifikatet er det god oppslutning rundt koronasertifikatet, vaksinasjonsprogrammet går som planlagt og flere og flere innbyggere benytter seg av løsningen. Myndighetene ser et mulighetsrom til videre økt bruk av koronasertifikatet og ønsker en mer permanent ordning, og legger en strategi for å utvide bruken, selv om det strekker seg utover den tidsbestemte perioden eller det opprinnelige formålet. Det fører til mistillit blant innbyggerne til myndighetenes	A) Tidsbegrensning, bruksbegrensning i prosjektet, sett opp mot Helseregisterloven. B) Informasjon til innbygger om rettigheter og lover relatert til koronasertifikatet. Informasjonskampanjer rettet mot forskjellige samfunnsgrupperinger. Informasjonen må være lett tilgjengelig. C) Stortingsvedtak ved utvidet bruk og forlengelse av koronasertifikatløsningen D) Visuelt fremvisbart tidsbegrensning E) Monitorer utviklingen nasjonalt og internasjonalt F) Tydelige forventningsavklaringer med (private) arrangører som ble gjort ansvarlig for bruk av koronasertifikat ved sine arrangement rundt krav, kommunikasjon til deltagere og problemløsning G) Etablering av kontaktkanal for private arrangører for råd og avklaringer fra myndighetene	3	3	Høy

		vurderinger for bruk av koronasertifikatet og resulterer i at en stor andel av befolkningen velger å ikke ta i bruk tjenesten. Dette vil også kunne føre til at Datatilsynet anser videreføringen av koronasertifikatet utenom opprinnelig formål som brudd på personopplysningsloven som kan føre til at de kan kreve bruken avsluttet.				
R1-2	Bruk av korona-sertifikat oppfattes som obligatorisk og mange føler seg presset til å ta i bruk en digital tjeneste	Tjenesten Helsenorge er i dag samtykkebasert og i realiteten frivillig i henhold til personopplysningsloven. Koronasertifikatet skal kun tilgjengeliggjøres for innbygger via Helsenorge. Innbyggere som er vaksinert eller som har tatt en koronatest kan derfor bli satt i et avhengighetsforhold til Helsenorge når tilgangen til ulike aktiviteter i samfunnet kun er tilgjengelig for dem med en Helsenorge profil, med negativt prøvesvar, immunitet eller vaksinert. Innbygger får negative konsekvenser ved å ikke bruke Helsenorge.	A) Tydelig kommunikasjonsplan som fo kuserer på grad av frivillighetsaspektet ved bruk av Helsenorge plattformen. B) Endre behandlingsgrunnlaget for Helsenorge plattform eller for koronasertifikatdelen. C) Etablere en analog kanal som tilrettelegger for at innbygger kan motta et koronasertifikat innen rimelig tid uten å bruke digitale midler.	2	2	Middels
R1-3	Innbyggere som ikke er digitalt aktive får ikke tilgang til korona-sertifikat	Koronasertifikatet skal kun tilgjengeliggjøres for innbygger via Helsenorge. Ikke alle innbyggere vil kunne få et koronasertifikat via Helsenorge, fordi de ikke er digitalt aktive, eller at de ikke ønsker en elektronisk identitet eller av andre årsaker ikke har tilgang til Helsenorge. Det kan føre til at en ikke-digitalt-aktiv innbygger som ønsker et koronasertifikat ikke får tilsvarende mulighet som en digital aktiv innbygger med tilgang til Helsenorge. Dette kan potensielt føre til at en viss andel av befolkningen viser stor misnøye til løsningen. Videre kan det svekke den bakenforliggende intensjonen til selve løsningen.	A) Etablere en analog kanal som sikrer at innbygger kan motta et koronasertifikat innen rimelig tid. B) Benytte fullmaktordning i Helsenorge for å tilgjengeliggjøre koronasertifikat. C) Godkjent koronatestbevis levert av testsenter som kan brukes utenfor koronasertifikat og aksepteres av en kontrollør.	2	3	Lav
R1-4	Økt press på testkapasiteten forårsaker at test informasjonen blir foreldet og "ferske prøvesvar" ikke vises i korona-sertifikat.	Når koronasertifikatløsning er på plass, og bruken får større utbredelse, øker etterspørselen etter koronatester og det legges stort press på testkapasiteten. De som har behov på grunn av helsetilstanden får ikke testet seg grunnet sprengt testkapasitet pga andre formål som festivaler, konserter og lignende kultur arrangementer. Nettsider for timebestilling overbelastes og reisevirksomhet til testsentre øker som resulterer i lange køer. Til slutt sprenges testkapasiteten og testinformasjon i koronasertifikat vil være eldre enn 72 timer når det dukker opp i sertifikatet. Koronasertifikat kan derfor ikke benyttes til bevis på negativ koronaprøve, som får følger for tilliten til koronasertifikatet og systemet for å ivareta løsningen som en helhet.	A) Tilgjengeliggjøre hurtigtester med en form for registrering i koronasertifikatløsningen B) Utdanne flere autoriserte testere og plassere dem der det er størst behov, som for eksempel i tilknytning til transport og arrangementer. C) Begrense/avlyse antall/størrelse arrangement som bruker koronasertifikat når testkapasiteten forventes å bli overbelastet D) Monitorere testkapasitet og øke antall testsentre ved behov.	1	2	Lav
R1-5	Innbyggere lar seg smitte for å benytte fordelene av et	Ungdommer er nedprioritert i vaksinerekkefølge og er lei av å måtte teste seg hver gang de ønsker tilgang til et arrangement. De benytter heller mulighetsrommet et	A) Kommunikasjon rundt koronasertifikatløsningen og	1	2	Middels

	korona-sertifikat	koronasertifikat gir ved immunitet etter gjennomgått sykdom, og lar seg bevisst smitte. Dette kan utsette helsetjenesten for økt press og føre til økt smittespredning, ikke bare blant unge innbyggere men også blant ikke-vaksinerte eldre. Denne samfunnsrisikoen kan i tilfeller føre til lokale nedstenginger og økonomisk skade.	ulemper med (gjennomgått) sykdom B) Forenkle testmuligheten ved arrangement for å senke terskelen C) Endre vaksinerekkefølge D) Frivillig vaksine (Johnson)			
R1-6	Den offentlige tilgjengelige kontrollør-appen misbrukes og svekker integriteten til kontrollør-funksjonen	En sofistikert trusselaktør benytter seg av den offentlige tilgjengelige kontrollørappen til å skape en replika og legge inn (flere) egne nøkler, i tillegg til de nasjonale nøklene som er offentlig. Ettersom replika-appen ser lik ut som den legitime appen fører dette til at mange kontrollørfunksjoner laster den ned og replika-appen blir brukt i økende grad. Dette svekker tillit til kontrollørsystemet. En kommersiell aktør, som en norsk virksomhet, kan også replisere en del av kontrollørappen og integrere det i en eksisterende app, for eksempel butikkadgang kombinert med kunderegistrering, eller adgang til fly kombinert med frequent-flyer fordeler. Dette fører til tap av sensitive helseopplysninger, uønsket innsamling av data og tapt tillit til koronasertifikatløsningen.	A) Monitorering av App stores og oppfølging med App stores dersom det oppdages falske apper a. Apple b. Google c. Huawei B) Stikkprøver på kontrollørlokasjoner C) Klare regler rundt bruk av kontrollørfunksjonen	3	3	Høy
R1-7	Helse-opplysninger som fremvises av korona-sertifikat er for kompleks og vanskelig å tolke for kontrolløren	Koronasertifikatløsningen som lanseres inkluderer en app som fremviser en QR kode som inneholder helseopplysninger om individet som fremviser den. Denne QR koden skal avleses av en kontrollørapp som kontrollerer koronassertifikatet. Det er et bredt spekter av virksomheter og individer som forventes å benytte seg av kontrollørappen, inkludert politi, toll, vektere, samt andre individer som arbeider for eksempel i event-, eller restaurant bransjen. Når koronasertifikatet blir lansert viser det seg at QR-kodene fremviser altfor medisinteknisk informasjon når de avleses av kontrollørappen. Kontrollørene har ikke nok kunnskaper om det medisintekniske til å kunne validere koronasertifikater på korrekt måte. I tillegg blir smittevernreglene endret i løpet av tiden og varierer fra land til land (og kanskje fra kommune til kommune), som gjør at både innbyggeren og kontrolløren må orientere seg kontinuerlig om sitt koronasertifikat gir fordeler ut ifra de gjeldende reglene eller ikke. Dette fører til at en kontrollør kan måtte foreta skjønnsmessige vurderinger som ikke alltid er korrekte, noe som fører til at innbyggere som burde fått godkjent koronasertifikatet ikke får det, og innbyggere som ikke burde fått godkjent koronasertifikatet sitt får det godkjent. Når koronasertifikatet ikke valideres på korrekt måte øker smittenivået igjen blant innbyggere, og man går mot nye restriksjoner og potensielt en ny nedstenging.	A) En regelmotor i kontrollørappen appen bør tolke informasjon fra koronasertifikat og fremvise konklusjonen på en tydelig måte, e.g. gjennom å vise «rød/grønn». B) Kontrollørfunksjoner må få opplæring i hvordan man på korrekt måte kontrollerer informasjonen som koronasertifikatet fremviser C) Det bør være tydelig og enkel informasjon om «reglene» rundt koronasertifikatet som hjelper innbyggeren med å tolke om sitt koronasertifikat er gyldig i en gitt situasjon, en kommune, et land eller tids periode.	3	2	Middels

		Konsekvensen av de skjønnsmessige vurderingene foretatt av kontrollørene og de nye restriksjonene er at innbyggere raskt mister tillit til både løsningen og norske myndigheter. Det fører også til at organiserte kriminelle utnytter kontrollørenes mangel på kunnskap til å utvikle egne QR koder/falske koronasertifikater som de selger til innbyggere som er misfornøyd med løsningen.				
R1-8	Statlig aktør utfører påvirkningskampanje mot koronasertifikatet i den hensikt å påvirke stortingsvalget høsten 2021	En avansert statlig aktør ønsker å påvirke Norges politiske prosesser. Gjennom langsiktige påvirkningsoperasjoner på flere nivåer ønsker en statlig aktør å skape uro opp mot stortingsvalget høsten 2021. Ved å monitorere open-source kilder og media så observerer aktøren at det er stor uenighet i det norske samfunnet rundt bruken et koronasertifikat. Aktøren bestemmer seg for å utnytte en allerede gryende splid i det norske samfunnet rundt koronasertifikatet til å utføre målrettede påvirkningskampanjer. Gjennom å diskreditere koronasertifikatet utvikler trusselaktør en strategi for falske nyheter gjennom å manipulere rangeringer av publikasjoner og kommentarer på sosiale medier som omhandler koronasertifikatløsningen. Aktøren utfører dette gjennom bruk av falske profiler på sosiale medier som brukes til å dele sladder, kontroversielle historier, konspirasjonsteorier, publisere flere uavhengige falske artikler, samt diskreditere koronasertifikatløsningen, FHI, og regjeringens manglende evne til å håndtere situasjonen. Etter en lengre periode med disse perifere angrepene starter trusselaktøren med direkte falske nyhetsangrep mot FHI og regjeringen. Dette fører til svekket tillit til regjeringens håndtering av pandemien, og spesielt koronasertifikatløsningen. Innbyggerne stoler ikke lengre på regjeringens og stortingets evne til å ivareta innbyggernes beste interesser. På bakgrunn av blant annet den statlige aktørens påvirkningskampanjer kan innbyggere, men særlig individer som er spesielt misfornøyd med regjeringen, bli påvirket til å stemme i en annen retning enn de vanligvis ville. Dette kan da potensielt gi utslag på stortingsvalget høsten 2021, som kan direkte påvirke Norges fremtidige politiske linjer og stilling i internasjonale samarbeidsarenaer.	A) Åpenhet rundt prosesser, formål, og samarbeid mellom etater. B) Monitorere etter falske medieoppslag og innføre «fact-checking» funksjoner på sosiale medier C) Jevnlige informasjonskampanjer knyttet til koronasertifikatløsningen	1	4	Middels
R1-9	Feil i kontrollørapp medfører at koronasertifikatet ikke kan valideres	Parallelt med lanseringen av koronasertifikatet lanseres også en kontrollørapp som skal brukes til å kontrollere QR-koden i sertifikatet. Den relativt raske prosessen med å utvikle og implementere bruken av kontrollørappen har ført til at en feil i appen/appens kildekode har blitt forbigått av utviklerne. I begynnelsen da bruken av appen er relativt begrenset og ikke så mange innbyggere har fått koronasertifikat merkes det ikke noe til denne feilen. Men etter hvert som kontrollørappen blir tatt mer og mer i bruk av	A) Prosedyrer for sikker utvikling (OWASP ASWS) og gjennomgang og jevnlig revidering av at prosedyrene følges. B) Monitorere og logge feilmeldinger i kontrollørappen C) Automatisk innsamling av feilmeldinger hos NetCompany for å detektere	2	3	Middels

		ulike kontrollfunksjoner blir det tydelig at appen ikke fungerer som den skal da den ikke alltid klarer å lese av QR kodene på korrekt måte og enkelte ganger er veldig treig eller stopper helt opp. Innbyggere får da ikke validert sine koronasertifikater og kontrollørene blir tvunget til å vise dem bort fra for eksempel arrangement som de har betalt billett for. Konsekvensen av feil i kontrollørappen blir særlig kritisk ved grenseoverganger hvor innbyggere som har gyldig koronasertifikat ikke får den kontrollert og verifisert når de returnerer fra utlandet. Dette fører til at kontrollørene (som politi og tollvesen) ser seg nødt til å slippe innbyggere inn i landet eller sette de i karantenehotell da de ikke kan få verifisert koronasertifikatene. Det skapes uro, sinne og forvirring blant befolkningen som har satt sin lit til koronasertifikatet for å kunne delta på arrangement og reise til utlandet, og tilliten til hele løsningen og norske myndigheter svekkes.	indikatorer på systematiske feil i appen. D) Etablere beredskapsplaner for å rette feil i appen.			
R1-10	Problemer med å validere utalandske koder fører til at utenlandske sertifikat ikke kan valideres	Under Covid-19 pandemien er det et stort antall norske statsborgere som studerer, arbeider, eller av andre grunner bor i utlandet, både innenfor og utenfor EU. Mange land er kommet godt i gang med vaksineringen av sine innbyggere, men vaksinetype som brukes og type vaksinesertifikat man får utsted varierer. I mange land har det vært mulig for nordmenn som bor der å få satt vaksine og få et digitalt vaksinesertifikat som bevis. Koronasertifikatløsningen som er utviklet i Norge har ikke kunnet tatt høyde for alle ulike typer utenlandske sertifikat og kontrollørfunksjoner får derfor problemer med å kontrollere utenlandske sertifikat. Når nordmenn som er vaksinerte så bestemmer seg for å returnere til Norge, enten for ferie eller for å flytte tilbake, blir de derfor stoppet ved grenseovergangen da deres utenlandske sertifikat ikke lar seg valideres og blir tvunget til å oppholde seg på et karantenehotell. Det er ikke bare nordmenn bosatt i utlandet som opplever dette problemet. Utenlandske borgere som av ulike grunner ønsker seg innreise til Norge, og som har tatt vaksine og fått vaksinesertifikat i sitt hjemland, blir også stoppet ved grenseovergangene. Da disse ikke er norske statsborgere og ikke har fast bopel i Norge blir de tvunget til å reise tilbake til hjemlandet sitt. Det skapes uro, sinne og forvirring blant befolkningen og andre EU borgere som har satt sin lit til koronasertifikatet for å kunne delta på arrangement, reise til og fra Norge, og tilliten til hele løsningen og norske myndigheter svekkes.	A) Prosedyrer for sikker utvikling (OWASP ASWS) B) Testing av ulike scenarier og JSON-skjemaer. C) Jevnlig kommunikasjon mellom deltagere i EU-Gateway om tekniske varianter, utfordringer og lærdom D) Etablere beredskapsplaner for å rette feil i appen.	1	3	Middels

6.2. Vurdering av risiko – Digital etikk

ID#	Tittel	Scenario	Beste praksis	Vurdering før ytterligere tiltak		
	Scenariotittel	Scenariobeskrivelse	Tiltak	S	K	U
R2-1	Forskjells-behandling mellom norske innbyggere	Parallelt med utrullingen av vaksiner ventes det også lettelser av restriksjoner utover sommeren og resten av året. Myndighetene har brukt lang tid på å vurdere juridiske utfordringer opp mot samfunnsøkonomiske fordeler i en gradvis gjenåpning av samfunnet. Innføringen av koronasertifikatet er tiltenkt som et mulig ledd og sikkerhetstiltak under gjenåpningen av samfunnet. Det har vært knyttet stor usikkerhet i henhold til nøyaktig hvilket formål norske myndigheter vil benytte et koronasertifikat til ved lansering. Ved lanseringen av koronasertifikatet viser det seg at myndighetene ilegger større begrensninger for innbyggere uten et koronasertifikat enn forventet over hele Norge. Innbyggere uten et koronasertifikat blir hindret fri ferdsel over kommunegrenser og får adgangsnekt og blir utelatt fra å delta i samfunnsmessige viktigere arenaer og på alle typer større arrangementer, som fredelige møter, diverse kulturarrangement, samt fysisk deltagelse ved utdanningsinstitusjoner. Kommuner som har et lavt smittetrykk men ikke mange vaksinerte innbyggere begynner også å føle at de bli ilagt et unødvendig strengt regime på bakgrunn av storbypolitikk. Begrensningene som blir ilagt innbyggere fører også til økt skam og skyld knyttet til sykdom, det å bli smittet, eller å være syk, og skaper digitale skiller mellom dem som benytter seg av digitale plattformer slik at de kan få koronasertifikat, og dem som ikke kan eller ønsker å benytte seg av digitale plattformer. Når slike begrensninger innføres er det altså fare for systematisk forskjellsbehandling når dette legitimeres av norske myndigheter. Tilliten til myndighetenes ønske om velferd til folket svekkes raskt på grunn av opplevd urettferdighet.	A) Formålet og bruksområdet til koronasertifikatet må tydeliggjøres, blant annet gjennom rettede informasjonskampanjer B) Sørge for at formål og bruk av koronasertifikat ikke er i konflikt med grunnlovsparagraf §106 som tilsier at de som oppholder seg lovlig i riket, kan fritt bevege seg innenfor rikets grenser og velge sitt bosted der C) Begrense restriksjoner til å ikke gjelde samfunnskritiske institusjoner og kritisk infrastruktur, samt begrense tiden og områder hvor koronasertifikatet kan brukes. D) Avvente med å innføre koronasertifikat frem til vaksine er blitt tilgjengeliggjort til alle over 18 år E) Gjøre vaksinasjonsprosessen og digital kommunikasjon enklere for mer vanskeligstilte grupper og dem som har mindre digital kompetanse, samt tilby papirversjon av sertifikatet for disse gruppene	2	2	Middels
R2-2	Forskjells-behandling mellom norske innbyggere og EØS-borgere med fast opphold og D-nummer	Ved implementering av koronasertifikatet i Norge viser det seg at EØS-borgere som bor og arbeider i Norge (som har folkeregisteradresse og D-nummer), og som bruker Helsenorge, men som er vaksinert i et annet EØS-land ikke får tilgang til norsk koronasertifikat grunnet manglende prosesser for verifisering og registrering av vaksine tatt i utlandet. Innbyggere med fast opphold i Norge med D-nummer blir heller	A) Sørge for at formål og bruk av koronasertifikat ikke er i konflikt med unionsborgerdirektivet, artikkel 29 B) Begrense restriksjoner til å ikke gjelde samfunnskritiske institusjoner og kritisk infrastruktur, samt begrense tiden og	2	2	Middels

		ikke prioritert i vaksineprogrammet og får dermed ikke tilgang til et koronasertifikat. Dette fører til at vedkommende ikke får adgang til ulike sosiale og kulturelle arrangementer i Norge, og EØS-borgere får følelsen av å ikke kunne få delta i samfunnet på lik linje med norske innbyggere selv om de bor og arbeider i landet. Det kan også påvirke vedkommende sitt arbeidsliv og inntekt om deres rolle blant annet innebærer mye reising og at de da må ha et koronasertifikat for å kunne utføre jobben sin.	områder hvor koronasertifikatet kan brukes C) Oppdatere/etablere rutiner for dokumentering og etterregistrering i SYSVAK av vaksiner tatt i utlandet, og vurdere det samme for gjennomgått sykdom.			
R2-3	Forskjellsbehandling mellom norske innbyggere og EØS borgere	Ved implementering av koronasertifikatet og den videre oppkobling mot EU løsningen viser det seg at innføringen av nasjonalt koronasertifikat hindrer adgangen til norske arrangement for EØS-borgere uten adresse i Norge (uten folkeregisteradresse eller D-nummer), men med gyldig koronasertifikat fra et annet land i Europa. Dette er grunnet manglende prosesser for innenlands verifisering av sertifikater tatt i andre land.. Vedkommende får da ikke tilgang til ulike sosiale og kulturelle arrangementer i Norge, eller unntak for enkelte restriksjoner. Det kan også påvirke vedkommende sitt arbeidsliv og inntekt om begrunnelsen deres for å reise til Norge er relatert til en arbeidsreise (engangstilfelle). Videre kan dette også påvirke norsk reiselivsnæring som går glipp av inntekt fra utenlandske turister som ikke får adgang til norske aktiviteter og derfor velger et annet reisemål.	A) Etablere prosesser og rutiner for godkjenning av EU-sertifikatet for innenlands bruk. B) Målrettet informasjon om bruk av koronasertifikat i Norge for innreisende fra andre EU land	2	2	Lav
R2-4	Uklare definisjoner av formål og bruksområder fører til misbruk av koronasertifikatet	Ved lansering av koronasertifikatet er formål og bruksområder for sertifikatet fortsatt uklare og ikke godt definert eller kommunisert av norske myndigheter. I tillegg kommer nyheter om formål og bruk i Danmark og andre EU-land som skaper uklarhet om norsk formål og bruk. Det kan tolkes som at myndighetene prioriterer samfunnsøkonomiske forhold i stedet for å vurdere helsemessige konsekvenser. Dette åpner potensielt for både tilsiktet og utilsiktet misbruk av koronasertifikatløsningen, både blant norske virksomheter og innbyggere. Enten basert på misforståelser eller ved å identifisere smutthull vil virksomheter som restauranter, forsikringsselskaper, festarrangører, arbeidsplasser, samt innbyggere selv begynne å bruke både koronasertifikatløsningen langt utover tiltenkt bruksområder. Dette gjelder både i henhold til å kreve koronasertifikat når de ikke har rett på det og på den måten utelukke visse grupper mennesker, samt å la være å validere koronasertifikater med	A) Sette krav til hvem som skal kunne kontrollere og validere koronasertifikat. Dette bør være basert på formelle prosesser for risikoforståelse ved innføring av nye formål og bruksområder for koronasertifikat, samt grundige vurderinger av forholdsmessighet. Her bør man også gjøre skillet mellom formelle og uformelle sammenheng tydelig. B) Kommunisere tydelig til innbyggere om hvor man kan forvente kontroll, hvilke forholdsmessige begrensinger det finnes for de uten sertifikat, samt informasjon om kontrollformer og hvem som faktisk har rett til å kontrollere sertifikatet. C) Åpne for klageadgang/varslingssystem for rapportering av misbruk av sertifikatet, og gi informasjon om hvor man skal klage, hva	2	3	Middels

		vilje for å slippe inn flere grupper av mennesker enn de burde. Eksempler på dette kan være arrangører som ser bort fra aldersgrenser såfremt deltakere kan vise til koronasertifikat, barnehager, skoler og idrettslag som stiller krav om koronasertifikat, arbeidsgivere som foretrekker ansatte som har koronasertifikat, og privatpersoner som krever koronasertifikat ved private arrangement. Konsekvenser av dette inkluderer at man innfører et system som legger til rette for å forsterke og legalisere mye av den kategoriseringen man ellers ser i samfunnet. Dette medfører direkte diskriminering av innbyggere basert på helse, og at flere som ikke har koronasertifikat ser på muligheten til å benytte seg av falske koronasertifikater. I tilleg vil uklare bestemmelser for i hvilke sammenhenger koronasertifikatet kan benyttes medfører at kontroll av sertifikatet gjøres i stadig flere sammenhenger. Dette oppfattes som tidkrevende og invaderende av en stor gruppe innbyggere. Innbyggere med status beskyttet velger derfor ikke å delta i samfunnslivet og isolerer seg fra ulike aktiviteter i samfunnet. Dette gir en motsatt effekt av hva koronasertifikatet er tiltenkt å gi.	slags klageadgang man skal ha, samt tidsfrist for klage. D) Tydeliggjøre bruken av koronasertifikat innen arbeidsforhold slik at sertifikat ikke gir uforholdsmessige fordeler. E) Utforme dokumentasjon og kommunikasjonsplaner som bla viser til de etiske utfordringene rundt bruken av et koronasertifikat.			
R2-5	Korona-sertifikatet skaper ny «autoritær» normaltilstand	Da koronapandemien traff Norge og resten av verden med full styrke i mars 2020 innførte norske myndigheter de strengeste og mest inngripende tiltakene siden andre verdenskrig for å hindre spredning av viruset. Det har vært sterkt indikert hele veien at dette er unntakstilstander og at norske myndigheter vil holde seg til de minst inngripende, og mest forholdsmessige tiltakene som er tilgjengelig. Nå i pandemiens andre år tilsier smittesituasjonen at tiltak og ulike restriksjoner fortsatt er nødvendige. Samtidig planlegges det en gradvis gjenåpning av samfunnet i takt med distribusjon og andel innbyggere som har fått vaksine, og koronasertifikatet lanseres som et ledd i gjenåpningsprosessen. Men selv med koronasertifikatet opplever mange innbyggere nå at gjenåpningsprosessen går for sakte og tidsperspektivet kan være usikkert. Dette fører til at innbyggere som ikke har fått koronasertifikat at i stedet for å være et middel som hjelper samfunnet med en sikker og gradvis gjenåpning, så er det heller med på å begrense visse samfunnsgruppers mulighet til fri ferdsel og deltakelse i samfunnet generelt. Det	A) Tydeliggjør formålet og innfør sterk begrensing på hvilke områder som koronasertifikatet kan gjelde for og hvor lenge det skal vare B) Tydelig kommunisere at koronasertifikatløsningen er et midlertidig krisetiltak og ikke den nye normalen C) Formelle prosesser for nye behov og avslutning av eksisterende koronasertifikatløsningen D) Formelle risikobehandlingsprosesser som ivaretar kontinuerlig modernisering av teknologivalg.	1	3	Middels

		innbyggere først aksepterte som en unntakstilstand og en midlertidig løsning har nå blitt den nye normaltilstanden hvor et fåtall har tilgang til et koronasertifikat. Myndighetene velger å videreføre bruken av koronasertifikatet på tross av tidligere forsikringer om en midlertidig løsning. Dette fører til økt mistillit til norske myndigheter blant innbyggere og en grad av polarisering i samfunnet. En statlige aktør velger å påvirke norske myndigheters tillit i samfunnet og forsterke polariseringen ved å gjennomføre en påvirknings-, eller desinformasjonskampanje mot norske innbyggere. En slik polarisering i samfunnet oppfattes som et mulighetsrom til å skape økt splittelse og større mistillit til regjeringens håndtering av krisen. Dette kan potensielt påvirke stortingsvalget til høsten 2021, og debatten i samfunnet generelt.				
R2-6	Privilegier som gis på bakgrunn av korona-sertifikatet oppleves som urettferdig og skaper mistillit	Tidlig i januar 2021 satte norske myndigheter i gang koronavaksinasjonsprosessen for fullt hvor vaksinerekkefølgen på samfunnsgrupper ble definert ut ifra sårbarhet mot viruset og helsemessige konsekvenser. I løpet av våren og sommeren 2021 endrer myndigheten på denne «vaksinekøen» og distribusjonen av vaksiner flere ganger i henhold utviklingen av smittetilstanden i ulike regioner og blant ulike samfunnsgrupper, samt ønsket innføring av sosiale lettelser for utvalgte samfunnsgrupper. Dette er med på å gjøre situasjonen usikker både for enkeltindivider, byer og kommuner som ikke alltid er enig i fordelingen av vaksinene eller rekkefølgen på innbyggergruppene. Etter hvert som tiden går og myndighetene stadig endrer på distribusjon, rekkefølge, og tidsperspektiv, begynner innbyggere å føle at myndigheter rett og slett bare «velger» hvilke innbyggere som skal få vaksinen og gjør den utilgjengelig for visse grupper. Innbyggere er vant til å vise solidaritet ved å la de samfunnsgruppene som trenger mest, få mest, men det oppleves nå at det ikke bare er forholdsmessige goder som gis til dem som er definert som mest trengende, og store grupper av befolkningen har følelsen av å bli holdt utenfor basert på gruppeinndelinger som fremstår som tilfeldige. I løpet av tiden viser det seg for eksempel at antall testkonserter (målgruppe 18-25) blir vesentlig lavere en tenkt grunnet motstand i ulike kommuner, og at Trinn 3 vil i stedet brukes delvis for grensepassering. Dette gjør at vaksineprioriteringen for aldersgruppen 18-25 anses som en lite gjennomtenkt omprioritering.	A) Etablering av en hurtigtestprosess som er tilgjengelig for alle som ikke har koronasertifikat basert på vaksinasjon, slik at de har muligheten til å delta i samfunnet på lik linje med innbyggere som har fått koronasertifikat B) Begrense bruken av koronasertifikatet slik at den ikke gir uforholdsmessige fordeler til dem som har koronasertifikatet C) Sikre at bruken av koronasertifikatet ikke er i konflikt med menneskerettigheter, spesielt rettigheter som fri ferdsel, fri mulighet til å delta på fredelige møter og kulturarrangementer og utdanning D) Tydeliggjør formålet, innfør sterk begrensing på hvilke områder som koronasertifikatet kan gjelde for og hvor lenge det skal vare, og kommuniser tydelig at det er et midlertidig krisetiltak og ikke den nye normalen E) Oppdatere/etablere rutiner for dokumentering og etterregistrering i SYSVAK av vaksiner tatt i utlandet	2	2	Middels

		Når koronasertifikatet blir lansert blir dette sett på som enda et privilegium som gis til visse samfunnsgrupper. Dette er med på å legge et stort press på solidaritetsfølelsen blant innbyggere, som er vant til at visse grupper får flere goder men ikke at de selv mister grunnleggende rettigheter og som nå setter spørsmåltegn ved om dette er forholdsmessig. Dette igjen utfordrer den norske velferdsmodellen som er basert på en gjensidig tillit mellom norske myndigheter og innbyggere. Dette øker mistilliten i samfunnet og fører til at visse samfunnsgrupper som føler seg utenfor velger å ikke overholde myndighetenes restriksjoner og sikrer seg privileger gjennom alternative kanaler. Dette inkluderer gjennomføring av ulovlige arrangementer, møter, protester, og demonstrasjoner. Innbyggere ser også på muligheten for kjøp og salg av falske koronasertifikater og slike kriminelle aktiviteter kan bli mer organisert. Det kan også føre til at innbyggere som allerede har reist, eller planlegger å reise til utlandet for å få vaksine (vaksineturisme), ikke får dette godkjent i Norge på bakgrunn av manglende dokumentasjon og får dermed ikke benyttet et koronasertifikat.				

6.3. Vurdering av risiko – Kryptografi

ID#	Tittel	Scenario	Beste praksis	Vurdering før ytterligere tiltak		
	Scenariotittel	Scenariobeskrivelse	Tiltak	S	K	U
R3-1	Kompromittering av signeringstjenesten for å hente ut private nøkler	En trusselaktør kompromitterer signeringstjenesten til koronasertifikat-løsningen gjennom et teknisk angrep og utnyttelse av sårbarheter i konfigurasjonen eller med hjelp av en innsider. Hensikten med det tekniske angrepet er for trusselaktøren å hente ut private nøkler og bruke de til å generere falske koronasertifikater som ikke blir identifisert som falsk av kontrollørtjenesten. Det er flere typer aktører som potensielt vil kunne ha motiv og kapabilitet til å gjennomføre et slikt teknisk angrep for å hente ut private nøkler. En statlig aktør vil sannsynligvis ha som formål å spre falske sertifikater til utvalgte personer og gi dem tilgang til for eksempel ulike arrangement. Hensikten med dette vil sannsynligvis være å spre uro og svekke tillit til koronasertifikatløsningen da alle koronasertifikater blir ugyldiggjort så snart man oppdager at signeringsnøklene har kommet på avveie. Dette fører da til at sertifikathierarkiet må fornyes og alle innbyggere må fornye sertifikat.	A) Lagring av private nøkler i HSM, air-gapped (offline) eller i en løsning med tilsvarende sikkerhet (FIPS 140-2 nivå 3) B) Etablere nettverks- og sikkerhetstiltak for å hindre storskalaangrep C) Begrense antall personer som kan ha tilgang til signeringstjenesten D) Etablere Privileged Access Management og dual control på signeringstjenesten E) Etablere kontinuerlig monitorering av signeringstjenesten F) Logging av kritiske aktiviteter G) Prosess for utstedelse av sertifikater, key management og nøkkelseremoni	2	4	Middels

		Organiserte kriminelle grupper vil sannsynligvis også ha interesse av å kunne hente ut private nøkler for økonomisk vinning. En innsideaktør, enten direkte og på egenhånd eller på vegne av en ekstern aktør, vil også kunne ha motiv og kapabilitet til å utføre et slikt teknisk angrep og hente ut private nøkler for å kunne bruke dette til personlig økonomisk gevinst ved å selge falske sertifikater eller dele sensitiv informasjon til tredjeparter. Om slike falske sertifikater kommer i omløp kan dette føre til økt smitte i samfunnet igjen, og potensielt nye restriksjoner.	H) Etablere prosedyrer for å stenge ned miljøet i tilfelle det er kompromittert			
R3-2	Kompromittering av back end for å legge inn egne signeringsnøkler	En trusselaktør klarer å legge inn en egen offentlig nøkkel i nøkkeldistribusjonsprosessen eller back end registeret. Nøkkelen lastes ned til kontrollørtjenesten, uten at gyldigheten av nøkkelen verifiseres tilstrekkelig i kontrollørappen. Trusselaktøren kan benytte den tilhørende privatnøkkelen til å generere falske koronasertifikater som allikevel vil verifiseres som gyldig. En sofistikert aktør, som statlige aktører eller organiserte kriminelle grupper, vil kunne ha motiv og kapabilitet til å utføre et slikt anslag. En statlig aktør kan generere mange norske koronasertifikater for utlendinger som befinner seg i Norge og som kan være i stand til å spre viruset på et arrangement. En statlig aktør kan også brukes til å spre uro og svekke tillit til løsningen. En organisert kriminell aktør eller misfornøyd innsider hos leverandøren kan også utføre et slikt anslag for å generere norske koronasertifikater og selge dem til innbyggere som ikke ennå er vaksinert selv.	A) Signering av signeringsnøkler med et overordnet sertifikat (CA-cert eller signeringssertifikat) B) Validering av overordnet signatur i kontrollørappen C) Logging av tillegg og fjerning av nøkler fra registeret D) Monitorering og daglig validering av integritet i nøkkelregisteret mot en kontrolliste E) Sørge for at nettverks- og sikkerhetstiltak er på plass for å hindre storskalaangrep. F) Begrense antall personer som kan ha tilgang til back-end G) Etablere Privileged Access Management og dual control på signeringstjenesten	2	3	Middels
R3-3	Misbruk av manglende mulighet for tilbakekalling av signeringsnøkler	En statlig aktør har klart å kompromittere en signeringsnøkkel og kan bruke den til å generere egne sertifikater med hensikt om å enten å gi spesifikke personer tilgang til ulike steder og arrangement, eller for skape uro og øke mistillit til løsningen og myndigheter blant norske innbyggere. Koronasertifikatene som er signert med denne nøkkelen kan ikke lenger stoles på. Koronasertifikatene kan ikke trekkes tilbake og signeringsnøkkelen kan ikke revokeres på grunn av manglende revokeringstjeneste. I stedet blir den offentlige delen av nøkkelparet fjernet fra nøkkelregisteret. Selv om den offentlige delen av nøkkelparet er fjernet vil komplette versjoner av nøkkelen fortsatt eksistere på utstyr som ikke fjerner koronasertifikatene som ikke lenger finnes i nøkkelregisteret, noe FHI ikke har kontroll på. Ettersom kontrollørappen kan tas offline, får den ikke med seg at signeringsnøkkelen ikke	A) Revokeringstjenester i henholdt til eHealth Guidelines on Digital Green Certificate (mai 2021) B) Begrensning av antall koronasertifikater per signeringsnøkkel C) Kontrollørappen må oppdatere sertifikatene minst hvert døgn og det bør forhindres at appen kan brukes hvis ikke den har vært 'online' det siste døgnet D) Informasjon til innbyggere som ikke har gyldige koronasertifikat	2	3	Lav

		lenger er gyldig. Det er dermed umulig å kunne skille mellom legitime og potensielt falske koronasertifikater, noe som svekker tillit til løsningen.				
R3-4	Svakheter i sertifikathierarki utnyttes til å svekke tillitskjeden	Signeringssertifikatene utstedes av et sertifikat (Country Signing Certificate Authority sertifikat, CSCA). Disse 'root'-sertifikatene er selvsignerte. En sofistikert trusselaktør, som for eksempel en ressurssterk organisert kriminell gruppe, kan utnytte de selvsignerte sertifikatene til å kompromitter et av disse CSCA-sertifikatene, og kan med det utstede egne signeringssertifikater for økonomisk vinning. Når trusselaktøren klarer å legge inn sine egne signeringssertifikater i back-end eller i applikasjonen, kan det brukes til å generere falske koronasertifikater. Når dette oppdages må hele tillitskjeden trekkes tilbake, noe som gjør at alle koronasertifikater som ble utstedt under dette CSCA-sertifikatet ikke lenger er gyldig. Innbyggere får ikke lenger verifisert sitt koronasertifikat. Med utilstrekkelig varslingsmuligheter klarer ikke FHI å varsle de innbyggerne som nå har ugyldige sertifikater. Det gjør at alle norske innbyggere må fornye sitt koronasertifikat.	A) Lagring av CSCA nøkler i HSM, air-gapped (offline) eller i en løsning med tilsvarende sikkerhet (FIPS 140-2 nivå 3) B) Etablere nettverks- og sikkerhetstiltak for å hindre storskalaangrep C) Dele CSCA i flere (e.g. 5) «shares» og kreve et flertall tilstede for bruk av CSCA D) Logging av kritiske aktiviteter E) Kjøpe CA-tjeneste fra en godkjent tredjeparts leverandør	2	4	Middels
R3-5	Kontrollørappen misbrukes for validering av falske sertifikater	En norsk aktør som bruker kontrollørappen, i dette tilfellet en dørvakt ved et arrangement, ønsker å kunne validere koronasertifikater som ble signert med en falsk signeringsnøkkel for å slippe inn noen venner. Dørvakten benytter den eksisterende applikasjonen, for eksempel på en «jailbroken» telefon, og klarer å legge inn egne nøkler på denne. Med dette kan dørvakten gi arrangementstilgang til forhåndsdefinerte personer og svekke tillitt til løsningen.	A) Signering av signeringsnøkler med et overordnet sertifikat (CA-cert eller signeringssertifikat) B) Validering av overordnet signatur i kontrollørappen C) Hardening av kontrollørappen som forhindrer mulighet til å legge in egne nøkler	3	2	Høy
R3-6	Falske sertifikater gjennom hash kollisjoner	Innholdet i koronsertifikatet hashes før det signeres. En enkelt-aktør i et organisert cyberkriminelt miljø ønsker å bevise sine ferdigheter ved å lage ett nytt koronasertifikat via å finne en hash kollisjon med et eksisterende sertifikat. Trusselaktøren bruker store mengder CPU for å finne en kollisjon som treffer på riktig sertifikatinnhold og samme hash som et gyldig koronasertifikat som aktøren har fått tak i. Det blir stor prestisje for trusselaktøren i miljøet sitt og fører til tap av omdømme for løsningen. På større skala kan det være ett marked for salg og kjøp av genererte koronasertifikater som aktøren lager.	A) Bruke sterk hashing-algoritme med lav sannsynlighet for kollisjoner, muligens dobbel hashing. B) Standardisere innhold i QR-koden som reduserer søkeområdet for kollisjoner. C) API sikkerhet for beskyttelse av signerings-API til tredjepart	1	2	Lav

6.4. Vurdering av risiko – Personvern

ID#	Tittel	Scenario	Beste praksis	Vurdering før ytterligere tiltak		
	Scenariotittel	Scenariobeskrivelse	Tiltak	S	K	U
R4-1	Person-opplysninger blir lekket gjennom tilgang på Helsenorge.no	Ved utrulling av koronasertifikatløsningen er det mange innbyggere som begynner å benytte seg av løsningen til å reise til utlandet. Man ser en stor økning av innbyggere som blant annet drar til Sverige	A) Gjøre koronasertifikatet direkte tilgjengelig på forsiden av Helsenorge.	2	3	Middels

	ved visning av Korona-sertifikatet	for å sjekke tilstanden til hyttene sine eller dra på «harryhandel», og innbyggere som drar til Syden for å ta sommerferie. Dette fører til økt trykk på grenseovergangene hvor blant annet politiet og tolletaten står klar til å sjekke innbyggernes koronasertifikat. Da det er flest av de eldre samfunnsgruppene som har fått tilgang på koronasertifikat grunnet vaksinering, er det også disse gruppene som reiser mest i løpet av sommeren. Mange av de eldre innenfor disse gruppene er ikke særlig digitalt aktiv og har vanskeligheter med å vise frem koronasertifikatet på mobilen sin via helsenorge.no. Dette fører til at mange spør kontrollørene (som politi og tolletat) om hjelp til å logge inn på helsenorge.no ved hjelp av innbyggers Bank-ID, slik at kontrolløren selv finner frem til vedkommendes koronasertifikat på deres Helsenorge profil. Enkelte aktører innenfor kontrollørfunksjonen (som for eksempel en politibetjent) bestemmer seg for å benytte anledningen til å utføre flere sjekker på vedkommende som egentlig er utenfor omfanget til en vanlig sjekk av koronasertifikatet. Gjennom tilgangen til innbyggerens Helsenorge-profil sjekker kontrolløren derfor blant annet hvorvidt vedkommende kan være ikke-kjørbar ved å sjekke medikamenter og/eller tidligere opphold ved rusinstitusjoner eller sykehus for bruk av rusmidler. Hvis politiet finner opplysninger som viser tidligere rusbruk kan de potensielt bestemme seg for å ta inn personen til testing. Denne handlingen kan være både tilsiktet og utilsiktet. Den kan være tilsiktet i den forstand at kontrolløren vet at de ikke har hjemmel til å sjekke vedkommende sine helseopplysninger, men gjør det likevel ettersom de for eksempel har mistanke om rusmisbruk. Handlingen kan være utilsiktet i den forstand at kontrolløren for eksempel har misforstått omfanget av verifikasjonsprosessen for koronasertifikatet eller sin egen rett som kontrollør ved grenseovergang til å sjekke innbyggeres helseopplysninger.	B) Kommunikasjon av Innbyggers rettigheter og politiets plikter ved grenseovergang. Før politiet kan starte med å hjelpe innbygger på grenseovergang må kontrollør klart gjengi hva det vil innebære å hjelpe innbygger, inkludert hva som er innbyggers rettigheter og politiets plikter. Det skal kommuniseres hvem som kan kontrollere, hva det vil si å kontrollere, hvilken informasjon som kan kontrolleres av politiet, samt hvordan man viser frem Koronasertifikatet for kontroll. C) Ivareta krav til universell utforming og ivareta et enkelt brukergrensesnitt inne på Helsenorge som gjør det enkelt for enhver å hente ut sertifikatet selv. D) Opplæring av kontrollørrollen og akseptabel fremferd for offentlig tjenestemann. E) Anbefale innbyggere til å skrive ut koronasertifikatet før planlagt reise.			
R4-2	Utvikling og bruk av falske kontrollørapper fører til lekkasje av person- og helse-opplysninger	Ved implementering av koronasertifikatløsningen lanseres det en kontrollørapp som skal brukes til å kontrollere QR koder som blir utsted til innbyggere via deres Helsenorge profil. Kontrollørappen skal være åpen og tilgjengelig for offentligheten, slik at alle som skal utøve en kontrollfunksjon kan laste den ned. Kildekoden vil også bli delt med offentligheten. Ved å dele kildekoden og gjøre den tilgjengelig for alle blir det enklere for andre tekniske brukere å oppdage	A) Begrensing av personopplysninger i QR-koden B) Tydelige krav om at scan av koronasertifikat ikke skal lagres av andre en bæreren. C) Straffeansvar for misbruk av opplysninger i koronasertifikat D) Kommunisere tydelig til innbyggere om hvor man kan	2	3	Middels

		potensielle feil og sårbarheter i kontrollørappen slik at disse raskt kan bli fikset på og appen kan oppdateres. Men å dele kildekoden åpner også for potensielle risikoer. Organiserte kriminelle grupper som har tekniske kapabiliteter og ressurser får muligheten til å laste ned kildekoden og skape sin egen versjon ved å gjøre noen endringer. Appen kan da tilnærmet se og fungere helt likt som den legetime appen, men kan potensielt ha fått tillagte egenskaper som gjør det mulig å samle inn helseinformasjonen som vises i koronasertifikatet. Organiserte kriminelle grupper vil da kunne for eksempel utstede falske kontrollører ved ulike arrangement eller andre sårbare steder som bruker den manipulerte versjonen av kontrollørappen til å lagre informasjonen til innbyggere som er til stede. Opplysningene i koronasertifikatet kan sammenstilles med tid og sted for kontrolltidspunktet. Dette kan igjen benyttes til å koble personer mot spesifikke steder, hendelser eller kontekster, som helse, religion, fagforening, seksuell legning, og til å spore enkeltinnbyggeres bevegelser i samfunnet. En slik eventuell hendelse vil altså kunne føre til lekkasje av sensitiv personinformasjon og helseopplysninger. Organiserte kriminelle kan misbruke slik informasjon i for eksempel utpressingsforsøk eller for økonomisk vinning ved å selge dem videre.	forvente kontroll, hvilke forholdsmessige begrensinger det finnes for de uten sertifikat, samt informasjon om kontrollformer og hvem som faktisk har rett til å kontrollere sertifikatet. E) Åpne for klageadgang/varslingssystem for rapportering av misbruk av sertifikatet, og gi informasjon om hvor man skal klage, hva slags klageadgang man skal ha, samt tidsfrist for klage.			
R4-3	Kontroll-funksjoner ber innbyggere å vise legitimasjon for å bekrefte eierskap til sitt norske koronasertifikat	Ved lanseringen av koronasertifikatløsningen var det først stadfestet at løsningen ikke skulle fungere som en form for identifikasjon, og heller ikke kreve identifikasjon av innbyggere som benytter seg av løsningen på grunn av at innbyggere bruker sin Helsenorge-profil til å få tilgang til, og fremvise koronasertifikatet sitt. Bruken av koronasertifikatet vil øke i takt med at befolkningen blir vaksinert. Parallelt med at flere får tilgang på koronasertifikatet verserer det også mistanke om at mange falske koronasertifikat er i omløp og blir brukt av innbyggere som ikke har tilgang på koronasertifikat. Dette fører til at kontrollfunksjoner blir redd for å slippe gjennom innbyggere som benytter seg av disse falske sertifikatene. Enkelte individer innenfor kontrollfunksjonene bestemmer seg for å kreve ytterligere identifikasjon av innbyggere ved ulike arrangementer og for ulike tjenester for å bevise at vedkommende faktisk er eiere av sertifikatet. Konsekvensen av dette er at enkelte individer innenfor kontrollfunksjonen får sett fullt navn, fødselsnummer og potensielt	A) Definere og kommunisere om legitimasjon bør vises med koronasertifikatet. B) Dynamiske elementer i en online-app som minimerer faren for forfalskning av sertifikatet.	3	2	Høy

		bankkortinformasjon av noen innbyggere når de egentlig ikke har hjemmel til det ettersom dette er mer personinformasjon enn det som er besluttet at koronasertifikatet skal kreve fra innbyggere. Denne type forskjellsbehandling av innbyggere kan potensielt være i strid med norske demokratiske prinsipper, og være med på å skape uro blant befolkningen og mistillit mot løsningen.				
R4-4	Integritets-problem ved at flere kan benytte samme koronasertifikat	Med hensyn til personvern blir dataminimering implementert i den norske koronasertifikatløsningen for å minimere mengden av personopplysninger. Dette fører til at flere kan benytte samme koronasertifikat og helseinformasjonen som blir lagt til i selve koronasertifikatet. Koronasertifikatet skal i utgangspunktet derfor bare fremvise bokstavkombinasjoner av fornavn og etternavn, samt fødselsår. Ulike samfunnsgrupper, som for eksempel ungdommer som ikke har tilgang på koronasertifikat og er misfornøyd med myndighetenes håndtering av pandemien, ser på dataminimering som en mulighet til å dele koronasertifikater seg imellom for å få tilgang til arrangementer og tjenester. Disse samfunnsgruppene benytter seg derfor av såkalt «crowdsourcing» for å identifisere andre innbyggere med sammenfallende bokstavkombinasjoner og fødselsår. Konsekvensene av dette er at flere uvaksinerte nå får tilgang til arrangementer og tjenester, noe som øker potensialet for smitte i Norge og som videre vil føre til svekket tillit til koronasertifikatet og norske myndigheter.	A) Folkeregisterøvelse for å få statistikk på sannsynlighet for at dette scenariet treffer. B) Kommunikasjon at man ikke skal dele koronasertifikatet sitt med andre. C) Forbud å lagre flere sertifikater, som gjør det straffbart å gjøre dette. D) Monitorering og "undercover actions" E) Utvikle et koronasertifikat som har navn for å kunne identifisere at du er du. F) Dynamiske elementer i en online-app som minimerer mulighet for deling.	3	2	Middels
R4-5	Arbeidsgivere benytter Korona-sertifikatet til feil formål i strid med forskrift	Det er store forventninger til mulighetene knyttet til bruken av koronasertifikat i Norge. Det er kjent at koronasertifikat kan benyttes for tilgang til arrangementer. Arbeidsgivere kan også oppfatte forskriften slik at de kan benytte koronasertifikat. En arbeidsgiver i helse og omsorg iverksetter derfor scanning av koronasertifikat som et tiltak for å beskytte sine pasienter mot mulige smittesituasjoner. Fra før har arbeidsgiveren oversikt over hvem som har gjennomgått koronasykdom og opplysningene sammenstilles til statistikkformål og for å planlegge turnus.	A) Spesifisert legitim bruk fra regjeringen. Kommunikasjon til befolkningen om legitim bruk. Kommunikasjon til de som får en kontrollørrolle om legitim bruk og sanksjonering Kommunikasjon fra arbeidsgivere at de skal aldri komme til å be om det. B) Spesifisere hvordan koronasertifikatet ikke kan brukes av arbeidsgivere.	2	2	Middels

6.5. Vurdering av risiko – Informasjonssikkerhet

ID#	Tittel	Scenario	Beste praksis	Vurdering før ytterligere tiltak		
	Scenariotittel	Scenariobeskrivelse	Tiltak	S	K	U
R5-1	DDoS-angrep fører til at hele- eller deler av korona-sertifikat løsningen er utilgjengelig.	Cyberterrorister som er politiske eller ideologisk motiverte aktører ønsker å hemme koronasertifikatet. Aktøren gjennomfører et storskala DDoS-angrep (Distributed Denial of Service Attack) hvor et BotNet med infiserte enheter benyttes som del av et zoombie angrep. DDoS angrepet benytter UDP basert DNS trafikk, med forfalsket mottaker / avsender. Målet for angrepet er backendløsningen, verifiseringsløsningen, SYSVAK eller MSIS. Konsekvensen av et slik angrepet er nedetid for løsningen. Det fører til datautveksling mellom registre berøres og at innbyggeren som ikke allerede har fått generert eller lastet ned et koronasertifikat ikke får muligheten til det. Et slik angrep vil også få en direkte innvirkning både på Helsenorge plattformen og applikasjon. Dersom det vedvarer over lengre tid, eller skjer ved flere tilfeller, kan det føre til at myndigheter og innbyggere ikke lengre stoler på FHI sin kompetanse til å ivareta en løsning som ikke innehar den funksjonaliteten, integriteten og tilgjengeligheten som kreves for den ønskede effekten av den digitale løsningen.	A) Trusselmonitorering for å avdekke planlagte angrep slik at rettede tiltak kan etableres raskt. B) Etablere kontinuerlig monitorering og varslingsrutiner slik at hendelser identifiseres og hendelsesprosesser kan igangsettes. C) Etablere kontakt med internettleverandører (ISPer) slik at uønsket trafikk kan stenges eller routes (sinkhole / blackhole). D) Etablere sikkert design. Sørge for at lagdelte nettverks- og sikkerhetstiltak er på plass for å hindre storskalaangrep. E) Etablere sikker konfigurasjon og herding av samtlige miljøer. F) Sikker drift og vedlikehold. Tydelig ansvarsfordeling og interne øvelser. G) Kontrollert ytelsestesting og verifikasjon av tåleevnen til eksponerte komponenter i infrastrukturen. H) Gjennomføre trusselmodellering av arkitekturen og herde/ etablere lagdelt sikkerhet på utsatte komponenter. I) Sikre god informasjonsflyt mellom EU-land ifm hendelser og hendelseshåndering som kan påvirke koronaretifikatet i Norge. J) Nettverkstrafikkrouting K) Isolasjon produksjon og interne systemer	1	3	Lav
R5-2	Innsideaktør med tilgang til løsningen misbruker egen tilgang for å fremme økonomisk gevinst	Etter en lengre tid som ansatt og ansvarlig for sikkerhet og tekniske løsninger knyttet til koronasertifikatet, har en ansatt hos en leverandør sett seg lei på å ikke bli hørt eller blitt tatt på alvor i sikkerhetsrettede spørsmål vedrørende systemene som ivaretar vitale komponenter hos FHI eller NHN. Den ansatte har administratortilgang til samtlige systemer og stor kjennskap til prosedyrer og produksjonsmiljøet. For å bevise sårbarhetene, velger den misfornøyde ansatte å selge eller prøver å selge stjålet nøkler eller tilganger til	A) Redusere antall brukere i FHI med tilgang til løsningen. B) Etablere dataminimering som gjør det vanskeligere å spore brukere C) Etablere tilgangsbegrensninger og opptak via PAM/PIM løsninger D) Etablere isolasjon mellom miljøer for å begrense tilgang til miljøer E) Nøkkelseremoni utføres i henhold til en nøyaktig definert protokoll. Alle deler av prosessen dokumenteres.	2	3	Lav

		systemene for egen økonomisk vinning, eller som hevn.	F) Etablere monitorering av mønstre for snoking			
R5-3	Organiserte kriminelle får tilgang til backend-løsningen og utnytter tilgangen til å gjennomføre ransomware angrep.	En sofistikert og organisert kriminell gruppe gjennomfører et phishing angrep mot ansatte hos NHN. Trusselaktøren jobber systematisk med åpne kilder for å identifisere personer i organisasjonen. Informasjonen brukes til å opprette tilpassede og målrettede phishing-e-poster (spear phishing) Via phishing hos FHI eller NHN sine ansatte og sårbarheter i systemer får en sofistikert og organisert kriminell gruppe tilgang til nøklene som generere QR-koder. Trusselaktøren Ansatte mottar en phishing-e-post som inneholder en kobling til lasteren som laster ned skadelig programvare. Den skadelige programvaren kjører kode som gir angriperen tilgang til klienten som deaktiverer sikkerhetsfunksjoner. Trusselaktøren har nå full kontroll over systemet og genererer deretter falske QR-koden som fremstår som legitime og legger de ut for salg på «The dark web». Videre velger trusselaktøren å utnytte tilgangen ved å utsette FHI/NHN for Ransomware, og krever store beløp i krypto valuta. Hvis ikke vil aktøren ødelegge, slette eller manipulere dataen i backend. lukkede internettfora (Dark Web). Trusselaktøren legger igjen tekstfiler til brukeren om at krypteringen ikke fjernes med mindre det utbetales løsepenger. Trusselaktøren krever 10 millioner € i krypto valuta. Angriperen truer med å slette eller lekke sensitiv informasjon til høystbydende, hvis løsepengene ikke betales innen kort tid. Selskapet står overfor potensielle store økonomiske tap hvis løsepengene betales, uten garanti for at systemene og informasjonen kan gjenopprettes. Utilgjengelighet av systemer og tap av data fører til tap av kontroll av operasjoner og kritiske funksjoner. Hendelsen vil påvirke selskapets omdømme, inntjening og innbyggers tillit til koronasertifikat løsningen negativt.	A) Sikre gode prosesser for tilgangsstyring og jevnlig gjennomgang av tilganger. B) Etablere tekniske, menneskelige og organisatoriske barrierer. C) Etablere sikkerhetsmonitorering D) Prosedyrer for sikker utvikling og gjennomgang og jevnlig revidering av at prosedyrene følges. E) Monitorere og logge hendelser og innlogginger for å detektere indikatorer på ikke-normal aktivitet. F) Etablere mulighet for å ta ned hele koronasertifikat-løsningen dersom man oppdager at backend er kompromittert. G) Etablere beredskapsplaner for å reetablere løsningen	1	3	Lav
R5-4	En statlig trusselaktør gjennomfører et sofistikert og målrettet angrep mot nasjonal backend	En statlig aktør med sterke ressurser og kapabiliteter gjennomfører rekognosering av nettverket til nasjonal backend over lengre tid. Aktøren benytter seg av åpne og offentlige tilgjengelige rekognoseringsverktøy som Shodan og nmap til å detektere potensielle sårbarheter. Aktøren utnytter sårbarheter de oppdager til å oppnå tilgang til nasjonal backend, og benytter tilgangen til å korrumpere innholdet i databasene. Ettersom nasjonal backend blir brukt til validering og nøkkeluteksling for koronasertifikatløsningen fører dette til at	A) Sikre gode prosesser for tilgangsstyring og jevnlig gjennomgang av tilganger. Etablere tekniske, menneskelige og organisatoriske barrierer. B) Prosedyrer for sikker utvikling og gjennomgang og jevnlig revidering av at prosedyrene følges. C) Logge hendelser og innlogginger for å detektere indikatorer på ikke-normal aktivitet. D) Etablere mulighet for å ta ned hele koronasertifikat-løsningen	1	4	Lav

		kontrollørfunksjonen settes ut av spill og kan ikke lengre utøve sin funksjon. Når kontrollørene ikke lenger kan utøve sin funksjon vil ikke innbyggere få tilgang til ulike sosiale og kulturelle arrangement, eller å reise inn og ut av landet. Dette fører til uro blant innbyggerne og svekker tilliten til løsningen og norske myndigheters ivaretagelse av innbyggernes interesser. Dette kan også få videre konsekvenser for samarbeidet rundt et europeisk koronasertifikat. I verste fall må hele tillitskjeden bygges på nytt.	dersom man oppdager at backend er kompromittert. E) Etablere gode rutiner og prosedyrer for en analog-kanal. F) Etablere beredskapsplaner for å reetablere løsningen			
R5-5	En trusselaktør utfører et leverandørkjede-angrep mot Netcompany	Netcompany er leverandør av flere Covid-19 relaterte IT løsninger til EU land, blant annet England, Danmark, Norge. Netcompany er dermed del av en digital verdikjede som omfatter flere tjenester og helsesektorer i ulike land. En avansert statlig aktør med gode ressurser og kapabiliteter velger å angripe Netcompany sin leverandørkjede ved å infisere flere ledd i deres systemer. Ved å få initiell tilgang til Netcompany's systemer utnytter trusselaktøren mulighetsrommet til å nå Netcompany's kunder som benytter seg av Covid-19 relaterte IT løsninger. Dette kan skje både gjennom avanserte, tekniske angrep eller ved hjelp av social engineering angrep. Når trusselaktøren har fått tilgang benytter aktøren seg av ulike metoder for å unngå å bli detektert, slik at aktøren kan drive spionasje og kartleggingsaktivitet over lengre tid uten å bli oppdaget. Under spionasje og kartleggingsaktiviteten vil trusselaktøren være særlig interessert i å få tilgang til strategiske planer og potensielt sensitiv informasjon fra kundene som benytter seg av Netcompany's Covid-19 relaterte IT løsninger, inkludert FHI/Helsenorge og koronasertifikatløsningen. Konsekvensene av et slikt leverandørkjedeangrep er at Netcompany blir nødt til å ta ned sine systemer, noe som fører til at Norge ikke får distribuert sine nøkler til EU og at norske innbyggere da ikke får mulighet til å gjennomføre reiser til EU ettersom deres koronasertifikat ikke kan bli verifiserte. Det vil også føre til at tilliten til løsningen svekkes blant norske innbyggere.	A) Etablere en analog kanal for ikke-digitale brukere som sikrer at innbyggere kan motta et koronasertifikat innen rimelig tid (innen 24/72 timer). B) Opplæring, trening og bevissthet rundt innsidertrusler C) Trusselovervåking av diskusjonsfora, lukkede internettfora, passordlekkasjer og falske domener D) Oppdatering av sårbarheter E) Adgangsadministrasjon F) Detaljert klientovervåking G) Sonedelt arkitektur-Nettverkssegmentering A) PAM (Privileged Access Management) B) Prosesser for hendelsesrespons, tidlig varsel om hendelse	2	3	Medium
R5-6	En sofistikert trusselaktør oppretter en Falsk versjon av Helsenorge sin plattform (applikasjon og nettside)	En sofistikert trusselaktør lager falsk versjon av Helsenorge sin koronasertifikat applikasjon som innbygger laster ned ved en feiltagelse. Applikasjonen ekstraherer informasjon om innbygger for økonomisk vinning, i form av identitetstyveri. NHN er en av mange mål for opportunistiske kriminelle for å få tilgang til innbyggers kredittkortinformasjon eller høste påloggingsdetaljer. En ukjent aktør sender ut ukjent antall phishing eposter, og har	A) Monitorering av App stores og oppfølging med App stores dersom det oppdages falske apper A) Apple B) Google C) Huawei B) Monitorer etter falske Helsenorge internettsider	4	2	Lav

		opprettet en falsk nettside som er tilnærmet identisk med Helsenorge sin. Dette angrepet benyttes til å få innbygger til å logge inn med BankID innloggingsdetaljer, kredittkortnummer, utløpsdato og sikkerhetskode (CVC). Innbygger kan potensielt blir utsatt for tap av sensitiv personinformasjon, så vel som økonomiske tap. Ettersom at det er et høyt press på Helsenorge sin plattform tar det tid før angrepet blir identifisert, og det viser seg at flere innbyggere har blitt rammet av angrepet. Dette fører til et enormt media fokus hvor kritikken rettes mot FHI, og NHN sin manglende evne til å ivareta innbyggers interesser. Dette fører til at Helsenorge sin plattform mister sin troverdighet og at innbygger ikke lengre stoler på fremtidige eposter fra Helsenorge, som videre får innbygger til å vegre seg for å bruke denne kommunikasjonskanalen.	C) Kommunikasjon til innbyggere om riktige nettsider og apper			
R5-7	Angrep mot SYSVAK eller MSIS for å korrumpere vaksine- eller smittedata.	En avansert statlig aktør ønsker å sabotere koronasertifikatløsningen for å skape uro i samfunnet og skape mistillit blant norske innbyggere mot myndighetene og løsningen. Aktøren identifiserer en sårbarhet i systemet til SYSVAK/MSIS og utnytter denne til å få tilgang til SYSVAK/MSIS databasen som inneholder registrering av innbyggeres vaksine- eller smittestatus. Aktøren korrumperer så dataen i databasen ved å manipulere og fjerne innhold, noe som fører til nedetid av registreringsprosessen. Konsekvensen av dette det fører til nedetid av SYSVAK/MSIS, noe som fører til at innbyggere som har fått registrert vaksine- eller smittestatus potensielt ikke får hentet denne informasjon ut av Helsenorge plattformen. Videre vil nyvaksinerte og personer som nylig har testet seg for korona ikke får registrert sin status i SYSVAK eller MSIS, som igjen fører til at vedkommende ikke får tilgang til koronasertifikat.	A) Sikker håndtering av nøkler til grensesnittet gjennom beste praksis på området, eksempelvis ISFs Crypto Key Management. B) Herding av integrasjonsgrensesnitt (MSIS API) og testing av ytelse. C) Gjennomføre penetrasjonstester av eksponerte grensesnitt for å kartlegge sårbarheter og mulige angrepsmønstre fra trusselaktører D) Benytte/innføre prosedyrer for manuell registrering av vaksine- og testresultater E) Opprett analog kanal for utstedelse av koronasertifikat	2	3	Lav
R5-8	Kompromitterte koronasertifikat-løsninger fra andre EU land fører til økt importsmitte i Norge	En organisert kriminell aktør som opererer i et EU land klarer å kompromittere landets koronasertifikatløsning som er koblet opp mot den overordnete EU-løsningen. Aktøren utnytter tilgangen til å produsere falske koronasertifikater og selger dem for økonomisk vinning. Dette fører til at falske sertifikater kommer i omløp i landet, og blir brukt av landets innbyggere som reiser til andre land i Europa, blant annet til Norge, både på sommerferie og på grunn av arbeid. De falske koronasertifikatene blir sett på som gyldige ved grensepassering til Norge og gir vedkommende rettigheter i Norge. Konsekvensen ved at flere benytter seg falske koronasertifikater på reiser er at man ser en økning av importsmitte i Norge og kan føre til flere store smitteutbrudd blant dem som ikke er vaksinerte. Dette kan da føre til store konsekvenser for Norges reiselivsbransje som blir kan bli nødt til å	A) Etablere prosesser for å blokkere enkeltland ved at ved grensepasseringer ikke godtar sertifikat B) Etablere hendelsesprosesser for å håndtere denne type situasjoner C) Styrke NSM & PST til å kartlegge mulige kompromitteringer i tilknyttede land D) Jevnlig kommunikasjon mellom deltagere i EU-Gateway om tekniske varianter, utfordringer og lærdom	1	4	Lav

		innføre strengere restriksjoner eller stenge ned delvis eller helt. Dette kan også føre til konsekvenser for enkelte deler av arbeidsnæringen i Norge som er særlig avhengig av utenlandsk arbeidskraft. Etter hvert som flere organiserte kriminelle ser muligheten for økonomisk vinning ved å kompromittere koronasertifikatløsning i andre land vil potensielt enda flere falske koronasertifikat komme i omløp også utenfor EU. Mange arbeidsinnvandrere fra andre land, som for eksempel høyt utdannede ingeniører fra land som India, kan potensielt også benytte seg av falske sertifikater når de reiser til Norge. Dette åpner opp for importsmitte og nye virusmutasjoner fra land som har høyt smittetrykk.				

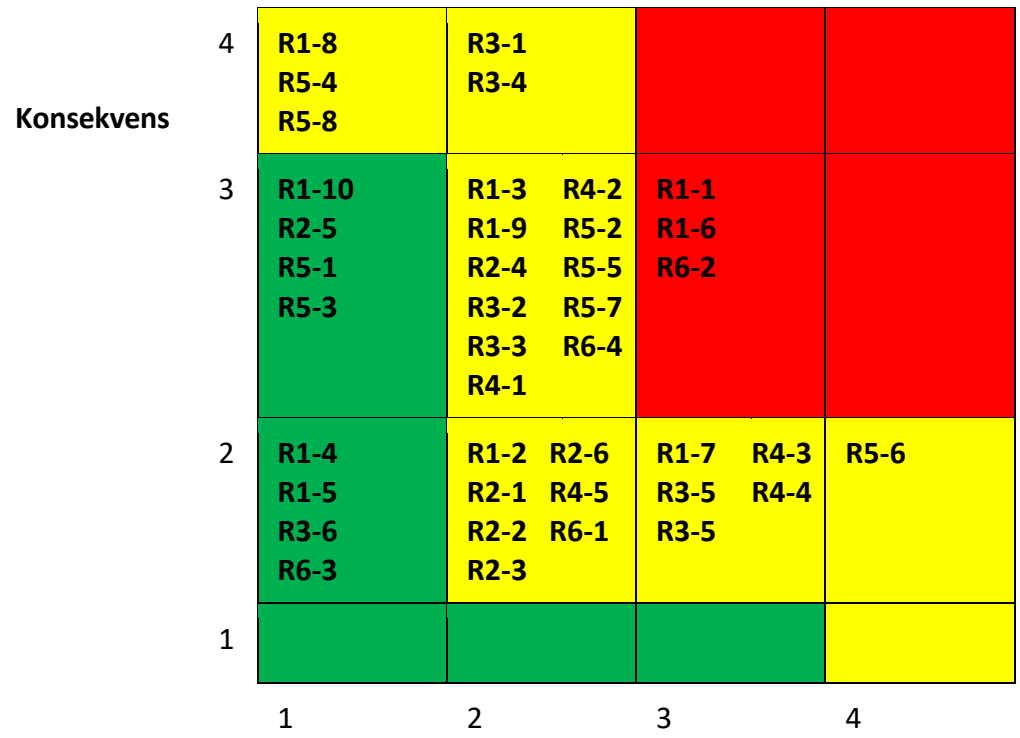
6.6. Vurdering av risiko – Analog kanal

ID#	Tittel	Scenario	Beste praksis	Vurdering før ytterligere tiltak		
	Scenariotittel	Scenariobeskrivelse	Tiltak	S	K	U
R6-1	Saksbehandler verifiserer en innbygger feilaktig	En trusselaktør gjennomfører et social engineering angrep mot saksbehandler ved å lure vedkommende til å utføre en utilsiktet handling hvor saksbehandler deler sensitive opplysninger om en annen innbygger. Trusselaktøren bruker sosiale medier til å samle informasjon om sårbare grupper og innbyggere som er tiltenkt som bruker for analog kanal. Aktøren bruker deretter denne informasjonen i samtale med saksbehandler for å innhente flere personopplysninger om innbyggere. På grunn av svak/manglende verifiseringsprosess klarer ikke saksbehandleren å gjennomskue trusselaktøren og verifisere at innbygger ikke er den de påstår at de er. Trusselaktøren får derfor tak i sensitive opplysninger om innbyggere (som for eksempel vaksineringsstatus) og kan benytte dette til å få tilgang til et koronasertifikat, eller selger opplysningene videre for økonomisk vinning.	A) Saksbehandlere må benytte et tilstrekkelig antall verifikasjonskriterier for å bekrefte innbyggers identitet. B) Trengs kontakt med tiltenkte brukergrupper for å forstå mulige utfordringer i å identifisere seg. C) Saksbehandlere må gjennomgå grundig opplæring i håndtering av innbyggere og være informert om diverse sårbare gruppers utfordringer. D) Saksbehandlere må kurses i og øke bevissthet rundt social engineering angrep. E) Helfo må håndtere flere språk.	2	2	Middels
R6-2	Saksbehandler misbruker tilgang til sensitive person-opplysninger og selger videre for økonomisk vinning	En saksbehandler benytter sin posisjon og tilgang til å hente ut sensitive personopplysninger om innbyggere som har tilgang på et koronasertifikat. Saksbehandleren samler opp, tar bilder av eller laster ned/printer ut personopplysninger og/eller koronasertifikater i papirformat og velger deretter å enten sende disse til en egendefinert adresse eller tar dem med seg hjem. Saksbehandleren velger deretter å selge både personopplysninger og koronasertifikat gjennom ulike internett	A) Krav til taushetserklæring og opplæring rundt konfidensialitet B) Kode 6/7 blir sperret C) Monitorere og logge hendelser og innlogginger for å detektere indikatorer på ikke-normal aktivitet. D) Stikkprøver i for validering at det finnes	3	3	Middels

		fora. Dette kan føre til at et utvalg av norske innbyggeres personopplysninger kommer på avveie, samt at gyldige koronasertifikater blir brukt av innbyggere de ikke hører til.	E) Saksbehandlere skal ikke jobbe individuelt (e.g. hjemmekontor) men i et overvåket areal. F) Fjerne mulighet for saksbehandler å i det hele tatt ha innsyn / tilgang til sertifikatet			
R6-3	Printløsningen for utskrift av koronasertifikat fører til at feil dokumenter ender opp i feil hender	Den analoge løsningen for koronasertifikatet innebærer prosesser for utskrift og postforsendelse av koronasertifikatets papirversjon. Da det er stor pågang på den analoge løsningen blir et begrenset antall printere brukt til å skrive ut et stort antall koronasertifikater. I prosessen fra å bli skrevet ut til å bli sendt ut til innbyggere er det mulighet for en feilaktig forveksling av koronasertifikater. Dette fører til at hele eller deler av en innbyggers koronasertifikat blir sendt til en annen innbygger. Konsekvensen av dette er at innbyggeres personopplysninger kommer på avveie, samt at innbyggere ikke vil motta koronasertifikatet sitt i tide.	F) Etablerte rutiner for håndtering av utskrifter og postforsendelse. G) Overvåking av kapasitet og kvalitet med prosessene H) Kontroll av riktig innhold i hver konvolutt før at konvolutten blir seglet.	1	2	Lav
R6-4	Overbelastning av analog løsning fører til at innbyggere ikke får utstedt koronasertifikat innen rimelig tid	Når det etableres analog kanal for koronasertifikatet er det mange innbyggere som benytter seg av dette. Ettersom Helsenorge er samtykkebasert er det ikke bare de typer brukere fra vanskeligstilte grupper som benytter seg av den analoge løsningen, men også innbyggere som av ulike grunner har valgt å ikke bruke Helsenorge plattformen. Dette fører til stor pågang på saksbehandlerne hos Helfo, noe som resulterer i ekstraordinær lang ventetid og at innbyggere som er tiltenkt primærbrukere av analog kanal ikke får tilgang til koronasertifikatet sitt i tide. I tillegg kan økt press føre til sviktet kvalitet, menneskelige feil og tap av sensitive opplysninger.	A) Øke bemanning av saksbehandlere B) Overvåke kapasitetsbruk, trender i pågang og belastning av saksbehandlere og justere der nødvendig C) Rettet informasjonskampanje om bruk av analog kanal mot tiltenkte brukergrupper D) Implementere call-in funksjoner (tastevalg) for ulike brukergrupper E) Printforespørsel på Helsenorge som alternativ for analog ganal for innbygger med digital tilgang uten printer.	2	3	Høy

6.7. Risikomatrise før ytterligere tiltak

Risikomatrisen viser risikoscenarioene og plassering basert på sannsynlighet og konsekvens før at ytterligere tiltak er på plass.



Hele løsningen

R1-1 Uklarheter rundt bruksområder og varighet med koronasertifikatet
R1-2 Bruk av korona-sertifikat oppfattes som obligatorisk og mange føler seg presset til å ta i bruk tjenesten
R1-3 Innbyggere som ikke er digitalt aktive får ikke tilgang til koronasertifikat
R1-4 Økt press på Testkapasiteten forårsaker at test informasjonen blir foreldrett og «ferske prøvesvar» ikke vises i koronasertifikat.
R1-5 Innbyggere lar seg smitte for å benytte fordelene av et koronasertifikat
R1-6 Den offentlige tilgjengelige kontrollørappen misbrukes og benyttes til å svekke kontrollørsystem
R1-7 Helseopplysninger som fremvises av koronasertifikat er for kompleks og vanskelig å tolke for kontrolløren
R1-8 Statlig aktør utfører påvirkningskampanje mot koronasertifikatet i den hensikt å påvirke stortingsvalget høsten 2021
R1-9 Feil i kontrollørapp medfører at koronasertifikatet ikke kan valideres
R1-10 Problemer med å validere utalandske koder fører til at utenlandske sertifikat ikke kan valideres

Digital Etikk

R2-1 Forskjells-behandling mellom norske innbyggere
R2-2 Forskjellsbehandling mellom norske innbyggere og EØS borgere med fast opphold og D-nummer
R2-3 Forskjellsbehandling mellom norske innbyggere og EØS borgere
R2-4 Uklare definisjoner av formål og bruksområder fører til misbruk av koronasertifikatet
R2-5 Koronasertifikatet skaper ny «autoritær» normaltilstand
R2-6 Privilegier som gis på bakgrunn av korona-sertifikatet oppleves som urettferdig og skaper mistillit

Kryptografi

R3-1 Kompromittering av signeringstjenesten for å hente ut private nøkler
R3-2 Kompromittering av back end for å legge inn egne signeringsnøkler
R3-3 Misbruk av manglende mulighet for tilbakekalling av signeringsnøkler
R3-4 Svakheter i sertifikathierarki utnyttes til å svekke tillitskjeden
R3-5 Kontrollørappen misbrukes for validering av falske sertifikater
R3-6 Falske sertifikater gjennom hash kollisjoner

Personvern

R4-1 Personopplysninger blir lekket gjennom tilgang på Helsenorge.no ved visning av Koronasertifikatet
R4-2 Utvikling og bruk av falske kontrollørapper fører til lekkasje av person- og helseopplysninger
R4-3 Kontrollfunksjoner ber innbyggere å vise legitimasjon for å bekrefte eierskap til sitt norske koronasertifikat
R4-4 Integritetsproblem ved at flere kan benytte samme koronasertifikat
R4-5 Arbeidsgivere benytter Koronasertifikatet til feil formål i strid med forskrift

Informasjonssikkerhet

R5-1 DDoS-angrep fører til at hele- eller deler av korona-sertifikat løsningen er utilgjengelig.
R5-2 Innsideaktør med tilgang til løsningen misbruker egen tilgang for å fremme økonomisk gevinst
R5-3 Organiserte kriminelle får tilgang til backend-løsningen og utnytter tilgangen til å gjennomføre ransomware angrep.
R5-4 En statlig trusselaktør gjennomfører et sofistikert og målrettet angrep mot nasjonal backend
R5-5 En trusselaktør utfører et leverandørkjedeangrep mot Netcompany
R5-6 En sofistikert trusselaktør oppretter en Falsk versjon av Helsenorge sin plattform (applikasjon og nettside)
R5-7 Angrep mot SYSVAK eller MSIS for å korrumpere vaksine- eller smittedata.
R5-8 Kompromitterte koronasertifikat-løsninger fra andre EU land fører til økt importsmitte i Norge

Analog kanal

R6-1 Saksbehandler verifisere en innbygger feilaktig
R6-2 Saksbehandler misbruker tilgang til sensitive person-opplysninger og selger videre for økonomisk vinning
R6-3 Printløsningen for utskrift av koronasertifikat fører til at feil dokumenter ender opp i feil hender
R6-4 Overbelastning av analog løsning fører til at innbyggere ikke får utstedt koronasertifikat innen rimelig tid

7. Intervjuobjekter

RoS-arbeidet omfatter blant annet intervjuer med sentrale personer i NetCompany, Norsk Helsenett og FHI. En oversikt over intervjuobjekter og områder for dekning følger.

Navn	Område for dekning
NetCompany	Utviklingsmetodikk, monitorering, forvaltning, arkitektur
NHN	Utviklingsmetodikk, arkitektur, monitorering, forvaltning
FHI (teknisk)	Arkitektur, utviklingsmetodikk, EU Gateway
FHI (juridisk)	Personvern, rettslig grunnlag

8. Tester benyttet inn i RoS-analysen

Flere tester har blitt gjennomført i løpet av RoS-arbeidet, og danner grunnlaget for deler av RoS-analysen.

Oversikt tester	Ansvarlig for test
Penetrasjonstest	NHN
Ytelsestest	FHI, NHN, NetCompany

9. Bidragsytere

Gjennom RoS-arbeidet av Koronasertifikat har nøkkelpersoner og fageksperter bidratt gjennom prosjektmøter og workshops med det norske sikkerhetsmiljøet. Oversikten viser bidragsytere og deres funksjoner i RoS-arbeidet.

Kjernegruppe:
- Pål Jakob Solerød, informasjonssikkerhetsleder FHI
- Line Sæle, leder arkitektur FHI
- Sindre Alvær, Infrastruktur FHI
- Tor Gaute Indstøy, sikkerhetsleder NHN

Eksternt fagmiljø i arbeidsmøter om digital etikk, kryptografi, personvern og informasjonssikkerhet:
- Anders Moen Hagalisletto
- Anne Siri K. Bekkelund
- Christopher Bach
- Derya Køse
- Eirik Larsen
- Eivind Arvesen
- Espen Andersen
- Kjetil Smith
- Maren Magnus Voll
- Martin Strand
- Michelle Hagen-Ellingsen
- Nils Norman Haukås
- Randi Gjerde
- Snorre Lothar von Gohren Edwin
- Øivind Høiem

10. Akronymer

Akronym	Beskrivelse
CSCA	Country Signing Certificate Authority sertifikat
DDoS	Distributed Denial of Service Attack
DPIA	Data Protection Impact Assessment
DSC	Document Signer Certificate
EDPB	European Data Protection Board
EFGS	European Federation Gateway Services/EU Gateway
ENS	Exposure Notification System
GAEN	Google Apple Exposure Notification
GDPR	General Data Protection Regulation
ISO	International Standards Organization
MSIS	Meldingssystem for Smittsomme Sykdommer
NHN	Norsk Helsenett
NIST	National Institute of Standards and Technology
NSM	Nasjonal Sikkerhetsmyndighet
OWASP	Open Web Application Security Project
PST	Politiets Sikkerhetstjeneste
RoS	Risiko- og Sårbarhetsanalyse
SYSVAK	System for registrering av Vaksinering

folkehelseinstituttet

Godkjent av: GUKN Gyldig fra: 24.06.2021	Rapport Risikovurdering informasjonssikkerhet	Versjon 2.1

FHI