

HELSE- OG OMSORGSDEPARTEMENTET  
Krisestab HOD  
Postboks 8011 Dep  
0030 OSLO

Deres ref.:  
Vår ref.: 21/44979-3  
Saksbehandler: Arve Paulsen  
Dato: 29.10.2021

## Oppdrag 548 - verifikasjon av koronasertifikat - svar til HOD

Svar på oppdrag 548 er utarbeidet med bistand fra FHI og Norsk helsenett. Vi viser til talepunkter oversendt Helse- og omsorgsdepartementet om denne aktuelle saken direkte fra FHI i går kveld, samt vedlegg fra FHI som svar på oppdrag 548. Situasjonen som ledet til utstedelse av kompromitterte koronasertifikat er ikke avklart, og saken overvåkes fortløpende. For øvrig vil vi fremholde følgende:

- Informasjonen som framkommer på nettet, konkretisert i de tre vedlagte lenkene, er misvisende. Dette var informasjon som ble delt 27.10. og som ble tilbakevist av EU kommisjonen (eHealth Network) sent samme dag.
- Det er korrekt at det er identifisert kompromitterte koronasertifikat, men grundige undersøkelser har ikke avdekket at nøklene brukt for å generere gyldige sertifikater har blitt stjålet eller kommet på avveie.
- Hendelsen er omfattet av gjeldende sikkerhetsvurdering for koronasertifikatet (ROS-analysen).
- Det er iverksatt tiltak for at identifiserte kompromitterte koronasertifikat skal avvises i den norske verifikasjonsappen.
- Det anbefales at Norge fortsetter samarbeidet gjennom EU kommisjonens Ehealth Network og ikke iverksetter tiltak utover felles anbefalinger.

## Oppdraget

Vi viser til informasjon om kompromittering av koronasertifikat på nettet i vedlagte linker.

[https://www.ansa.it/english/news/general\\_news/2021/10/27/eu-green-pass-generation-keys-stolen-sources\\_e231d1e5-8eab-429b-ae6d-c70991469d41.html](https://www.ansa.it/english/news/general_news/2021/10/27/eu-green-pass-generation-keys-stolen-sources_e231d1e5-8eab-429b-ae6d-c70991469d41.html)

<https://www.thedailybeast.com/eus-green-pass-qr-code-keys-stolen-to-make-fake-travel-certificates-including-one-for-adolf-hitler>

<https://news.ycombinator.com/item?id=29011537>

### HelseDirektoratet

Avdeling prosjekt og tjenstedesign  
Arve Paulsen

Postboks 220 Skøyen, 0213 OSLO • Besøksadresse: Vitaminveien 4, Oslo • Tlf.: (+47) 47 47 20 20  
Org.nr.: 983 544 622 • postmottak@helsedir.no • www.helsedirektoratet.no

Helse- og omsorgsdepartementet ber om at informasjonen om kompromittering av koronasertifikat verifiseres, jf informasjonen som fremkommer på nettet. Vi ber videre om en vurdering av mulige konsekvenser for Norge med en tilhørende risikovurdering, samt en anbefaling av hvordan Norge bør forholde seg til koronasertifikat fra aktuelle land hvis informasjonen verifiseres.

Kontaktperson i HOD: Bjørn Astad

Frist: 3. november kl 12:00

## **Besvarelse**

Det er gjort utførlig rede for saken i vedlagte notat fra FHI, og Helsedirektoratet støtter de vurderingene som er gjort.

Pr. 28.10. gjelder dette altså koronasertifikat knyttet til seks UVCI-koder (UVCI = Unique Vaccination Certificate Identifier), dvs. seks identifiserte koronasertifikater, men det åpnes opp for at pågående undersøkelser kan avdekke flere.

Arbeid med å endre den norske verifikasjonsapp'en startet i går (28.10.2021) og FHI antar at endringen for å avvise de kompromitterte sertifikatene raskt blir operativ.

Situasjonen overvåkes fortløpende.

Det er naturlig at denne saken følges opp på aktuelle møter mellom Helse- og omsorgsdepartementet og underliggende etater en viss tid framover.

Vennlig hilsen

Helen Brandstorp e.f.  
direktør

Arve Paulsen  
prosjektleder

*Dokumentet er godkjent elektronisk*

Kopi:

Helsedirektoratet, Beredskap @helsedir.no;FOLKEHELSEINSTITUTTET, Utbrudd Utbrudd;HELSE- OG OMSORGSDEPARTEMENTET, Bjørn Astad



COVID-19

## Oppdrag fra HOD nr. 548

Verifisering av informasjon om koronasertifikat

3. November 2021



### Oppdragstekst

*U.off.*

*Vi viser til informasjon om kompromittering av koronasertifikat på nettet i vedlagte linker.*

[https://www.ansa.it/english/news/general\\_news/2021/10/27/eu-green-pass-generation-keys-stolen-sources\\_e231d1e5-8eab-429b-ae6d-c70991469d41.html](https://www.ansa.it/english/news/general_news/2021/10/27/eu-green-pass-generation-keys-stolen-sources_e231d1e5-8eab-429b-ae6d-c70991469d41.html)

<https://www.thedailybeast.com/eus-green-pass-qr-code-keys-stolen-to-make-fake-travel-certificates-including-one-for-adolf-hitler>

<https://news.ycombinator.com/item?id=29011537>

*Helse- og omsorgsdepartementet ber om at informasjonen om kompromittering av koronasertifikat verifiseres, jf informasjonen som fremkommer på nettet.*

*Vi ber videre om en vurdering av mulige konsekvenser for Norge med en tilhørende risikovurdering, samt en anbefaling av hvordan Norge bør forholde seg til koronasertifikat fra aktuelle land hvis informasjonen verifiseres.*

*Kontaktperson i HOD: Bjørn Astad*

*Frist: 3. november kl 12:00*

### Folkehelseinstituttets vurdering

#### Oppsummering

- Informasjonen som framkommer på nettet, konkretisert i de tre vedlagte lenkene, er misvisende. Dette var informasjon som ble delt 27.10. og som ble tilbakevist av EU kommisjonen (eHealth Network) sent samme dag.
- Det er korrekt at det er identifisert kompromitterte koronasertifikat, men grundige undersøkelser har ikke avdekket at nøklene brukt for å generere gyldige sertifikater har blitt stjålet eller kommet på avveie.
- Hendelsen er omfattet av gjeldende sikkerhetsvurdering for koronasertifikatet (ROS-analysen).
- Det er iverksatt tiltak for at identifiserte kompromitterte koronasertifikat skal avvises i den norske verifikasjonsappen.
- Det anbefales at Norge fortsetter samarbeidet gjennom EU kommisjonens Ehealth Network og ikke iverksetter tiltak utover felles anbefalinger.
- Situasjonen som ledet til utstedelse av disse kompromitterte koronasertifikatene er ikke avklart, og saken overvåkes fortløpende.

## Vurdering

Onsdag 27. Oktober ble Norge varslet om forfalskede koronasertifikat gjennom ehelsenettverket i EU. De første meldingene antydte et større omfang enn det senere undersøkelser har avdekket. Ett av de falske koronasertifikatene er utstedt i navnet til A. Hitler. Hendelsen har skjedd i Frankrike og Polen. (Dette er foreløpig ikke offentlig kjent)

Det ser ut til at koronasertifikatene ble generert av personer med gyldig legitimasjon for å få tilgang til de nasjonale IT-systemene, eller at noen har misbrukt slik gyldig legitimasjon. Ansvarlig nasjonale myndigheter i Frankrike og Polen undersøker saken, blant annet om mulig uredelig aktivitet, forfalskning av dokumenter og identitetstyveri. I henhold til tilgjengelig informasjon er ikke kryptografiske nøklene som brukes til å signere sertifikater, kompromittert.

Åpne kilder refererer til at digitale nøkler for å opprette sertifikater er stjålet. Ifølge opplysninger fra EU-kommisjonen onsdag ettermiddag stemmer ikke dette, det skal ha vært en person som har logget seg inn i et IT-system og opprettet falske koronasertifikater.

Norge er en del av det europeiske samarbeidet om koronasertifikater og deltar i ehelsenettverket i EU. E-helsenettverket (eHealth Network) koordinere sine handlinger på denne hendelsen. Som et første skritt har medlemsstatene (og EØS-landene) blitt enige om å blokkere de to falske sertifikatene slik at de blir vist som ugyldige av de bekreftende appene.

Hendelsen, slik den framstår, er dekket av gjeldene Risiko- og sårbarhetsanalyse og er omfattet av risikoscenarioene benevnt R5-2 og R5-3:

- 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

Den aktuelle risikovurdering har ikke endret seg.

Arbeid med å endre den norske verifikasjonsapp'en startet 28.10.2021 og det antas at endringen for å avvise de kompromitterte sertifikatene blir operativ samme dag. Pr. 28.10. gjelder dette koronasertifikat knyttet til seks UVCI-koder (UVCI = Unique Vaccination Certificate Identifier), dvs. seks identifiserte koronasertifikater, men det åpnes opp for at pågående undersøkelser kan avdekke flere.

Videre jobber ehelsenettverket og EU-kommisjonen på nasjonalt og europeisk nivå med å forbedre løsningen for å trekke tilbake utstedte koronasertifikater, for å kunne reagere på slike, og lignende, tilfeller enda raskere. Dette arbeidet, som også har startet opp nasjonalt er prioritert, men det er mange avveininger som skal gjøres, ikke minst personvernmessig, og arbeidet er omfattende.

Medlemsstatene og EU-kommisjonen fordømmer denne (ondsinnede) handlingen på det sterkeste, som kommer i en tid der helsetjenestene er under press for å bekjempe pandemien.

For å forhindre omdømmerisiko blokkerte italienske myndigheter noen av sertifikatene til de polske og franske borgerne som hadde blitt signert av de samme nøklene som de falske sertifikatene. Men etter koordineringen i eHealth-nettverket og som følge av informasjonen mottatt etter nærmere undersøkelse fra Frankrike og Polen, er situasjonen gjenopprettet og Italia vil igjen godta alle gyldige franske og polske sertifikater.

Det anbefales ikke å iverksette generelle tiltak knyttet til koronasertifikat fra de to land som har blitt utsatt for denne handlingen, men det vurderes som tilstrekkelig å iverksette tiltak knyttet til de konkrete koronasertifikatene identifisert som kompromitterte. Denne anbefalingen er gyldig så lenge det kun er identifisert at saken gjelder et fåtall kompromitterte koronasertifikater.

Situasjonen som ledet til utstedelse av disse kompromitterte koronasertifikatene er ikke avklart, enten det dreier seg om urettmessig tilgang til IT-systemer eller urettmessig tilgang til innloggingsdetaljer for å få tilgang til disse systemene. Situasjonen overvåkes derfor nøye gjennom det Europeiske samarbeidet og ytterligere tiltak vil bli vurdert dersom situasjonen skulle endre seg.

## Merknad

FHI ber om at vurderingen i sin helhet, inklusiv grafisk utforming, legges ved i det endelige svaret til HOD.