# Beskrivelse av sikkerhet ved innsending av IPLOS-meldinger fra kommunen til Helsedirektoratet over helsenettet med AMQP

## Generelt

Beskrivelsen av sikkerhet gjelder overføring av meldinger fra fagsystem i kommunen til Helsedirektoratet ved bruk av PKI-løsningen i helsenettet. Denne løsningen krypterer og signerer meldinger for sikker transport i helsenettet, ved hjelp av adresser og sertifikater som distribueres via NHN sitt adresseregister.

Dette er ikke en risikovurdering av PKI-løsningen i helsenettet, en slik antas å være utført av andre. Vurderingen er avgrenset til overføring fra kommunen ved bruk av Service Bus som betinger en åpning i brannmur for trafikk til/fra sikker sone.

Beskrivelsen av sikkerhet er et grunnlag for å kunne åpne i brannmur for trafikk fra sikker sone i kommunen via AMQP. Løsningen, med bruk av AMQP - protokollen og Servicebus, er risikovurdert av Norsk helsenett[1], med en anbefaling om at den benyttes. Videre inngår løsningen i et eksisterende teknisk miljø som er risikovurdert tidligere (f.eks. i forbindelse med overføring av PLO-meldinger fra fagsystem via EDI i helsenettet ved bruk av PKI-løsningen).

For å kunne sende meldinger til helsedirektoratet er det nødvendig med følgende portåpninger

| Fra server | porter | Til Servere |
|---|---|---|
| kommunen | (sb.net): 9354, 9355, 9356<br>(AMQP): 5671, 45672 | 91.186.92.103<br>91.186.92.104<br>91.186.92.105 |

## Etterlevelse av krav til informasjonssikkerhet i "Normen"

Spesielt viktige krav i Norm for informasjonssikkerhet:

- punkt 5.5.2, stiller krav om at " Trafikk kan ikke passere direkte utenfra og inn; all slik ekstern trafikk må initieres fra virksomhetens systemer. "
    - Kravet ivaretas ved at det kun åpnes for at trafikk initieres fra kommunens sikre sone mot NHNs Servicebus.

- Punkt 5.5.3 stiller videre krav om at mottaker (Helsedirektoratet) skal "ivareta overføringskryptering ende-til-ende. "
    - Kravet ivaretas ved at informasjon holdes kryptert inntil den blir behandlet i forvaltningssonen i Helsedirektoratet.

[1] «Risikovurdering av NHN Service Bus» utført og godkjent av NHN 3.2.2015

## Vurderinger av hvordan sikkerhet ivaretas ved brannmuråpning

### Risiko for brudd på konfidensialitet

Handler om sikkerhet mot uautorisert tilgang til informasjonen som utveksles – dette ivaretas ved at:

- All informasjonsutveksling initieres fra kommunens sikre sone - det åpnes ikke for at trafikk kan initieres andre veien
- Kommunikasjonen går via Norsk helsenett som er et sikret nett
- Meldingene sendes med ende til ende kryptering

### Risiko for brudd på integritet

Handler om sikkerhet mot uautorisert endring av informasjonen – dette ivaretas ved hjelp av de samme mekanismer og forhold som er nevnt ovenfor under punktet om *Sikkerhet for konfidensialitet*.

### Risiko for brudd på tilgjengelighet

Handler om at informasjonen skal være tilgjengelig *når* det er behov for den for den/*de* som har behov for den.

Det er viktig at kommunene etablerer gode systemer/rutiner for å forsikre seg om at de har mottatt / ikke mottatt applikasjonskvittering.

Flere av tiltakene omtalt under områdene *Sikkerhet for konfidensialitet* og *Sikkerhet for integritet* er relevante også for *Sikkerhet for tilgjengelighet.*

## Konklusjon

Innsending av IPLOS-data følger krav til meldingsutveksling slik de fremkommer i Norm for informasjonssikkerhet, og åpninger i brannmur kan gjennomføres slik de er beskrevet under punktet "generelt"

# Ytterlig dokumentasjon

- E-helse link til bruk av AMQP
- https://docs.microsoft.com/en-us/windows/desktop/seccrypto/pkcs--7-concepts (Kryptering+signering)
- https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-fundamentals-hybrid-solutions (Basic om Service Bus)
- https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-messaging-overview (Oversikt over Service Bus)
- https://ehelse.no/grunndata/adresseregisteret (Adresseregisteret)