STAVANGER KOMMUNE

Dato: 29.01.2019
Saksnummer: 18/22230-17

Notat til egen organisasjon, fastlegene samt kommunene i innkjøpsfelleskapet for ny legemiddelavtale med Norsk Medisinaldepot AS.

Emne: Elektronisk oversendelse av resept i ny avtale

Innhold

1. Innledning

I et forsøk på å imøtekomme mange spørsmål fra fastlegene med flere i avtalen, har vi laget et notat som går litt mer i dybden på de ulike alternative, *elektroniske* oversendelsesmetodene i avtalen med Norsk Medisinaldepot som startet opp 1.1.2019.

I påvente av at e-dose skal bli en ferdig løsning for alle landets fastleger (pt. er dette en pilot), åpner avtalen med Norsk Medisinaldepot for flere ulike metoder for oversendelse av multidosereseptene. For mer informasjon om inngått legemiddelavtale og e-dose, vises det til vårt forrige notat datert 16.1.2019.

Foreliggende notat er utarbeidet i samråd med vårt personvernombud og vår sentrale IT-avdeling. Vurderingene som er gjort, gjelder formelt sett kun for Stavanger kommune. Notatet deles med øvrige kommuner i anbudet og fastlegene, men skal ikke regnes som en offisiell risikovurdering for andre parter enn rettssubjektet Stavanger kommune.

Før vi går videre inn i materien, ønsker vi å presisere følgende:

- GDPR og personvern er godt sikret i ny legemiddelavtale med Norsk Medisinaldepot.
- Avtalen som er inngått med NMD, inneholder ingen endring med hensyn til tidligere praksis for oversendelse av taushetsbelagt informasjon hos Apotek 1 og Boots (som hadde legemiddelavtalen før Apotek 1).
- Det er gjort et grundig arbeid (risiko/sikkerhetsvurdering) i både anbudsfasen samt forut for signering, herunder ved å tilpasse Databehandleravtalen til kommunenes behov og krav etter norsk rett, jf. personvernforordningen fra EU (GDPR) og personopplysningsloven (gjennomføringen av GDPR i norsk rett).

2. Regelverk

2.1. Uttalelse fra Helsedirektoratet om oversendelse av elektronisk resept

Helsedirektoratet har på forespørsel fra Statens legemiddelverk den 22.07 2016[1] tolket regelverket for elektronisk oversendelse av resept (ikke e-resept). Hovedprinsippene i Helsedirektoratets tolkning er fortsatt gjeldende også etter at GDPR ble inkorporert i norsk rett den 15.juni 2018.

[1] http://www.apotek.no/Files/Apotekregelverk/Brev/Helsedirektoratet/20160722%20Fortolkning%20av%20regelverket%20som%20gjelder%20for%20oversendelse%20av%20resepter.pdf

Da Trondheim kommune i desember 2018 tok kontakt med Helsedirektoratet og ba om tilbakemelding på om kommunens og fastlegenes bruk av telefaks ved oversendelse av multidose til apotek, fremdeles ble ansett som en kurant oversendelsesmetode, svarte direktoratet[2]:

«[…] inntil ny elektronisk løsning i Reseptformidleren er på plass er dagens praksis slik dere beskriver den akseptabel. Samtidig er det viktig å jobbe for å få etablert en elektronisk løsning for multidose i Reseptformidleren. I Utleverings – og rekvireringsforskriften som nå er til revisjon, vil det legges opp til krav om en elektronisk samhandlingskjede for alle typer resepter, også multidose.»

Per dags dato er ikke e-dose en ferdig løsning. E-dose er heller ikke en løsning virksomhetene i kommunene (sykehjem osv), kan bruke. Direktoratet «godkjenner» altså fremdeles kommunes og fastlegenes bruk av telefaks. Dette er også i samsvar også med forskrift om rekvirering og utlevering av legemidler fra apotek og tidligere uttalelser fra helsemyndighetene.

2.2. Ny personvernforordning fra EU

Personvernforordningen (GDPR) artikkel 32, 1 ledd slår fast følgende:

«Idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, ***skal den behandlingsansvarlige og databehandleren gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen,*** *herunder blant annet, alt etter hva som er egnet,»* [vår utheving].

Det vil si at løsningen som benyttes, skal være innenfor akseptabel risiko. Det er dertil opp til den behandlingsansvarlige å vurdere hva som er akseptabel risiko.

Kommunene er kun behandlingsansvarlige for den dataen de selv forvalter og sender fra seg. Det vil si at fastlegene eller andre private parter tilknyttet avtalen, på selvstendig grunnlag, må foreta en risikovurdering med hensyn til hvilken av avtalens *mulige* oversendelsesmetoder de ønsker å benytte seg av.

2.3. Helsedirektoratets vurdering

I følge Helsedirektoratet må følgende krav være oppfylt ved elektronisk oversendelse av resept eller rekvisisjon:

[2] Seniorrådgiver ved avdeling retningslinjer og fagutvikling i Helsedirektoratet svarte oss. For interesserte kan denne mailen videreformidles.

1. Avsender må kunne autentiseres. Brukes elektronisk signatur skal sikkerhetsnivå 4 (bruk av Bank-ID eller lignende) benyttes.
2. Taushetsplikt/personvern/konfidensialitet må sikres ved bruk av kryptering. Benyttes kryptering anses autentiseringen som godkjent.

Helsedirektoratet uttaler videre i notat datert 22.07.2016 følgende:

«Bruk av e-Resept er i samsvar med regelverket. Det samme vil gjelde for kryptert kommunikasjon per e-post. For nærmere informasjon om hvilke krypteringsmåter som er tilfredsstillende vises til Datatilsynets nettsider www.datatilsynet.no. Dersom e-posten sendes kryptert kan resepten eller rekvisisjonen være en skannet kopi med håndskrevet signatur. Ellers må det benyttes kvalifisert elektronisk signatur, som omtalt i punkt 2 foran. Ved kryptering er kravet til autentisering og sikring av resepten eller rekvisisjonens innhold oppfylt.»

Det vil si at også tvungen TLS, oppfyller kravet om kryptert e-post overføring. Dette i likhet med ovennevnte informasjon om telefaks.

3. Mer om kryptering og bruk av TLS

Av de mulige oversendelsesmetodene avtalen åpner opp for, har Stavanger kommune konkludert med at tvungen TLS er innenfor det vi anser som akseptabel risiko. For spørsmål om kryptering henviser Datatilsynet til Nasjonale sikkerhetsmyndighet.[3] Nasjonal sikkerhetsmyndighet (NSM) uttaler:

"NSM anbefaler at TLS benyttes i størst mulig grad, da protokollen er tilgjengelig i mange ulike systemer og tjenester."

TLS vil si at vi kan sende epost som vanlig, uten noe videre kryptering av selve vedlegget. Det blir som å sende en helt ordinær epost med vedlegg, bortsett fra at linjen er helt trygg. Noe den ikke vanligvis er når man sende epost. Hvis man ikke bruker tvungen TLS har man ikke garanti for at e-posten blir sendt kryptert.

Denne vurderingen bygger på uttalelse fra Helsedirektoratet, NSM, Datatilsynets, Normen for informasjonssikkerhet, Microsoft og personvernforordningen artikkel 24 & 32.

Vår vurdering er gjort med hensyn til den tekniske løsningen eller overføringen kalt «tvungen TLS 1.2 (Transport Layer Security)». Dette er med andre ord løsningen for selve oversendingen av den elektroniske resepten.

[3] Se https://nsm.stat.no/publikasjoner/regelverk/veiledninger/veiledning-for-systemteknisk-sikkerhet/sikring-av-kommunikasjon-med-tls/

Dokumentet er elektronisk godkjent og sendes uten signatur.

På bakgrunn av anbefalinger fra ovennevnte kilder har Stavanger vurdert at oversendelse av resepter i e-post med tvungen TLS 1.2 er innenfor akseptabel risiko, med den forutsetning at avsender og mottaker har rutiner for å håndtere resepter før og etter oversendelsen.

Vurderingen gjelder *dataoverføringen*, ikke reseptprosessen. Prosessen for å sende og motta resept blir opptil partene (den enkelte kommune, fastlegekontor) å utarbeide nærmere. Slike rutiner bør inneholde for eksempel hvem som har ansvaret for å sende resepten, hvem som sletter e-posten etter at den er sendt, etterkontroll og sletting av gamle resepter (her eposter) osv. Slike rutiner er lovpålagt etter personvernforordningens artikkel 32.

Vi ønsker å presisere at uansett hvilken metode man velger for å sende en resept til Norsk medisinaldepot eller andre apotek for den saks skyld, vil resepten alltid på et tidspunkt bli behandlet ukryptert. Det er derfor viktig at ovennevnte «før og etter» rutiner er på plass, da dette er en forutsetning for totalvurderingen.

Det er dertil opp til hver behandlingsansvarlig å vurdere om behandlingsaktiviteten er innenfor akseptabel risiko, det vil si at tekniske og organisatoriske tiltak er på plass, jf. personvernforordningen artikkel 24 nummer 1 og artikkel 32 nummer 1.

Databehandleravtalen mellom kommunene (behandlingsansvarlig) og Norsk Medisinaldepot AS (databehandler), sikrer at NMD behandler dataen de mottar fra kommune og fastlegene etter gjeldende rett (personopplysningsloven, GDPR).

Vi ønsker å presisere at det ikke foreligger noen indikasjoner på at Norsk Medisinaldepot ikke følger inngått databehandleravtale. Avtalen er omfattende og ble signert før avtalen og leveransene startet opp. Dette i henhold til gjeldende rett og datatilsynets anbefalte prosedyre.

4. Hva er TLS?

Krypteringsprotokollen TLS er den vanligste løsningen for konfidensialitetsbeskyttelse, jf. anbefalinger fra Nasjonal Sikkerhetsmyndighet (NSM)[4].

For at denne løsningen skal fungere, forutsettes det at man inngår en gjensidig avtale, hvor begge parter setter opp tvungen TLS- kobling for utgående og innkommende meldinger.

Med tvungen TLS sendes melding kun hvis den kan overføres kryptert. Det vi si at avsender (serveren til Stavanger kommune i dette tilfellet) sjekker om mottaker (serveren hos Norsk Medisinaldepot),

[4] Nasjonal sikkerhetsmyndighet (NSM) er Norges ekspertorgan for informasjons- og objektsikkerhet, og det nasjonale fagmiljøet for IKT-sikkerhet. Direktoratet er nasjonal varslings- og koordineringsinstans for alvorlige dataangrep og andre IKT-sikkerhetshendelser.

støtter TLS. Hvis mottaker ikke støtter TLS vil ikke e-posten bli sendt og man får en feilmelding som denne:

> ***"/9/2019 1:00:01 PM - Server at HE1PR0702MB3802.eurprd07.prod.outlook.com returned '550 5.4.317 Message expired, cannot connect to remote server(451 5.7.3 STARTTLS is required to send mail)'"***

Stavanger kommune har satt opp tvungen TLS mot domenene NMD.no og Vitusapotek.no. Denne installasjonen ble gjort på få minutter av IT avdelingene hos de respektive partene (Stavanger kommune og NMD). Vi mener derfor det er god grunn til å hevde at i tillegg til å være innenfor akseptabel risiko, er denne løsningen enkel å sette opp samt svært brukervennlig for kommunen som kun behøver å sende epost som vanlig etter at installasjonen er gjort.

E-posten er kun kryptert i overføringsfasen og dekrypteres på serveren. Enkelte har i den forbindelse stilt oss spørsmål om TLS er tilstrekkelig med tanke på sikkerhet. Dette fordi tredjepart, her leverandøren av e-posttjenesten, har tilgang til e- postserveren. Vårt svar til denne bekymringen er at dersom en fastlege eller en kommune, ikke har nødvendig tillitt til sin epostleverandør, bør de vurdere å bytte epostleverandør. Det samme gjelder for skybaserte tjenester hvor det håndteres sensitiv informasjon. Her vil også leverandøren ha tilgang til sensitiv data.

Som allerede angitt reguleres dette gjennom databehandleravtaler som inngås med leverandører som håndterer slike data, jf. databehandleravtalen kommunene har inngått med NMD. Dette prinsippet gjelder for så vidt også for interne systemer som for eksempel CGM, Visma og Acos, hvor leverandørene har tilgang til systemet via sine supporttjenester

5. Skisse av TLS

Dokumentet er elektronisk godkjent og sendes uten signatur.

6. Bruk av brev eller telefaks vs TLS

Risikoen for brudd på informasjonssikkerheten er høyere ved bruk av brev eller telefaks, enn ved bruk av e-post.

Brev håndteres av mange ledd fra avsender til mottaker. Risikoen for uønskede hendelser er derfor høyere ved brev, enn e-post. Telefaks er gammel teknologi som medfører sårbarheter og større risiko for uønskede hendelser.

Feilsending kan skje i alle systemer, men har man gode rutiner, er risikoen minimal. Merk også at regelverket vi er forpliktet til å etterleve, personopplysningsloven og EUs personvernforordning, i utgangspunktet ikke forbyr bruk av for eksempel telefaks for oversendelse av multidoseskjema. Se i den forbindelse ovennevnte uttalelser fra Helsedirektoratet til Trondheim kommune. En viktig presisering her er at selv om en praksis ikke er «ideell» og ikke fullt ut i tråd med den veiledende normen[5], betyr ikke det dermed at praksisen innebærer ulovlig eller ikke akseptabel risiko. Merk at ingen apotekkjeder pt. er 100% i såkalt «compliance» med sikkerhetsnormen. Normen er selvsagt viktig, men den er *veiledende*. Det er viktig å ikke forveksle lovkrav knyttet til personvern med veiledende retningslinjer.

7. Konklusjon

Uansett hvilken oversendelsesmetode man velger, vil alltid avsender og mottaker håndtere informasjonen ukryptert på et gitt tidspunkt. Det er derfor viktig å utarbeide gode rutiner som ivaretar nødvendig informasjonssikkerhet og personvern. Dette er rutiner som kommunene og fastlegene selv må utarbeide. Hvilken grossist kommunene har inngått legemiddelavtale med, er således uinteressant i denne kontekst. NMD har som sagt en databehandleravtale som stadfester at de håndterer dataen korrekt på *sin side.*

NMD godtar de ovennevnte oversendelsesmetodene i henhold til inngått kontrakt. Hvilken av avtalens *alternative* oversendelsesmetoder kunden velger for multidoseskjemaene, (TLS, faks, brev, kryptert vedlegg), er den enkelte behandlingsansvarliges beslutning.

Helsedirektoratet sier: *«Taushetsplikt/personvern/konfidensialitet må sikres ved bruk av kryptering. Benyttes kryptering anses autentisering godkjent.»*

Med bakgrunn i helsedirektorats tolkning av regelverket, NSM anbefaling og Stavanger kommunes egen sikkerhetsvurdering, mener vi at kryptering (tvungen TLS 1.2) fra avsender til mottakers server

[5] Norm for informasjonssikkerhet og personvern i helse og omsorgstjenesten

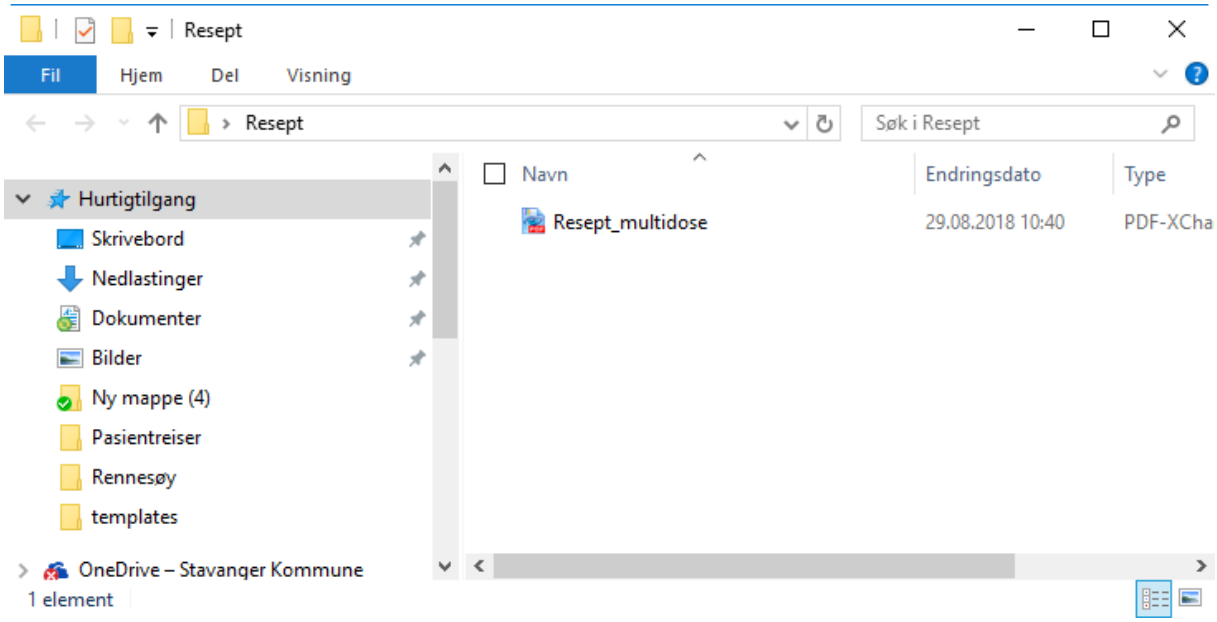
er innenfor akseptabel risiko**.** Risikoen for uønskede hendelser ved oversendelse av multidoseresept er minimal ved bruk av TLS.

VEDLEGG 1: Hva gjør man hvis man ikke har oppsett for tvungen TLS?

Dersom du ønsker ekstra sikkerhet eller ikke har TLS, kan filer enkelt krypteres og sendes via e-post. Enkelte har hevdet at TLS ikke er tilstrekkelig og at vedlegget også må krypteres. Stavanger kommune er ikke av denne oppfatning, men det er selvsagt ikke noe i veien for å kryptere vedlegget i tillegg til TLS forbindelse dersom man ønsker det.

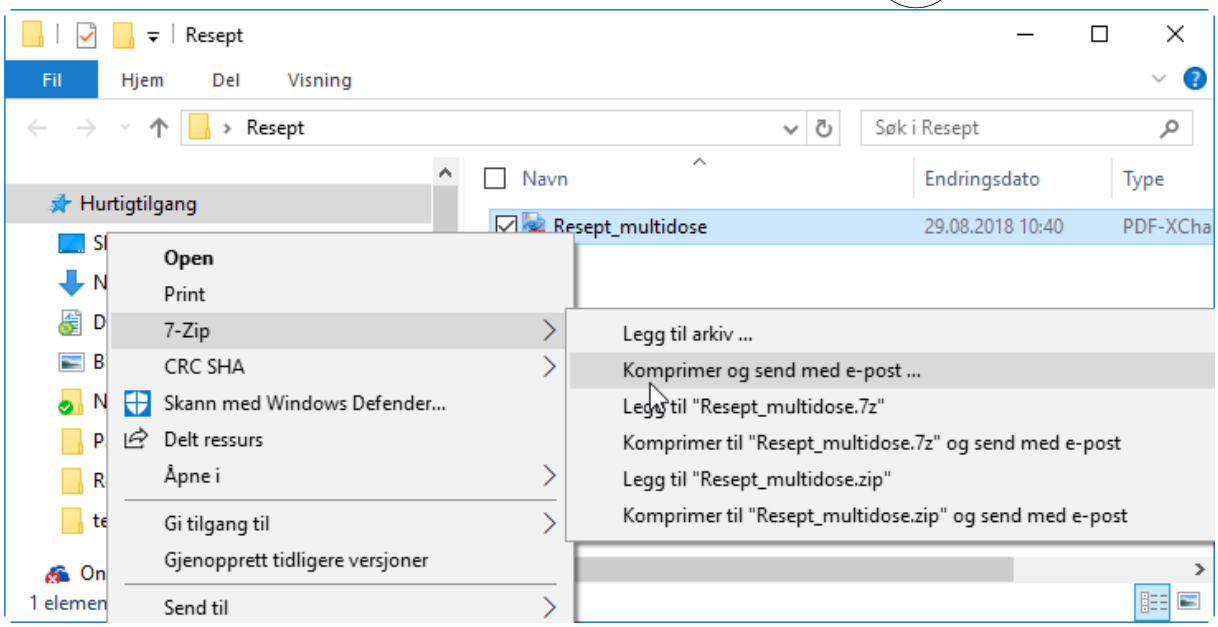
Hvordan (enkelt) kryptere en fil?

- Last ned 7Zip(gratis) og installer programmet. Gjøres kun en gang pr. maskin
- 7Zip benytter AES 256 kryptering(sikkert). Anbefales også av datatilsynet.
- Skann resepten
- Navigere deg frem til filen



Høyre klikk på flien og velg: 7-zip →Komprimer og send med e-post

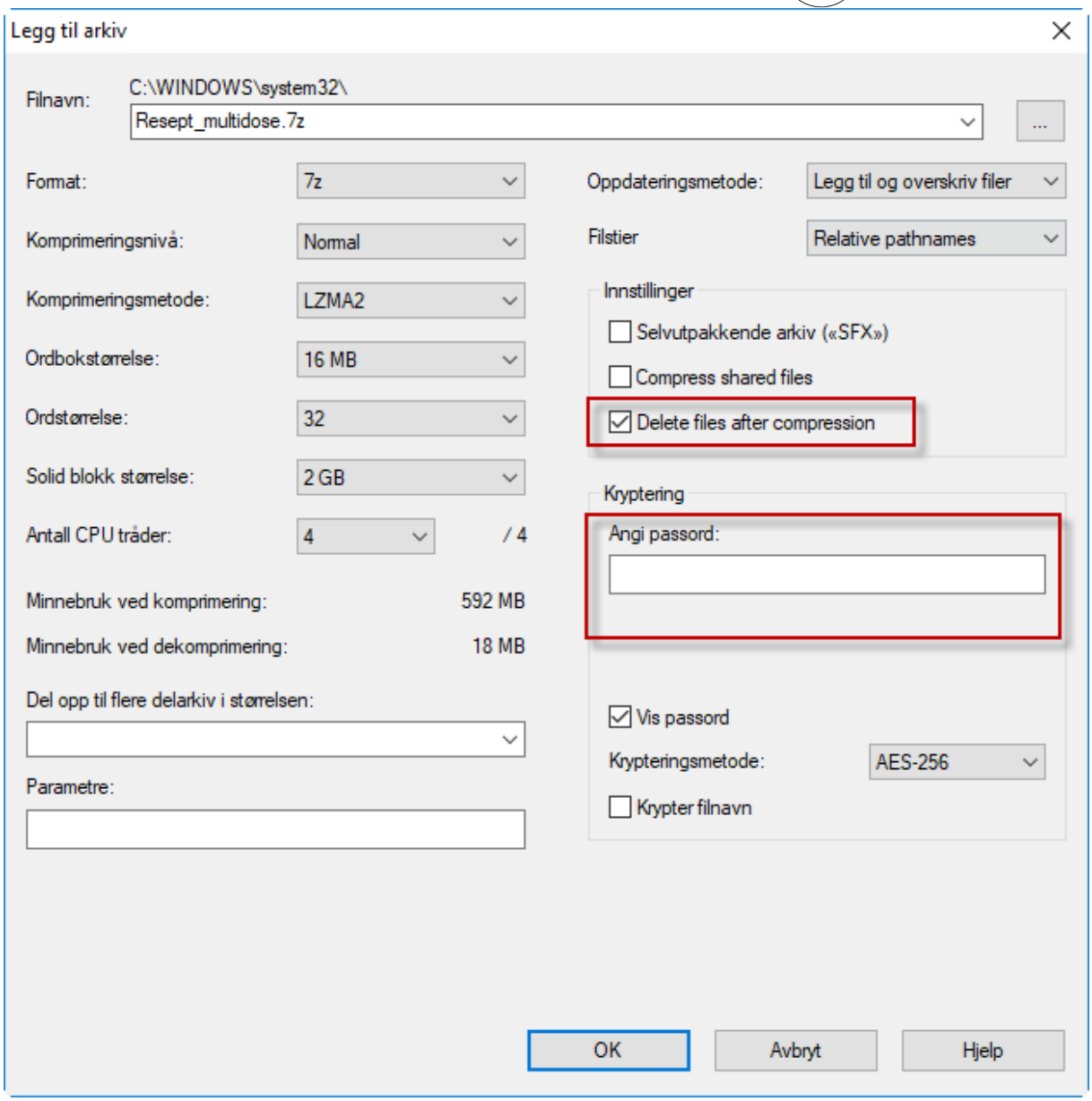
Dokumentet er elektronisk godkjent og sendes uten signatur.



- Krysses av i en boks: Delete files after compression.
- Filen slettes da fra katalogen når operasjonen er fullført.
- Skriv inn ønsket passord på dokumentet: Angi passord.

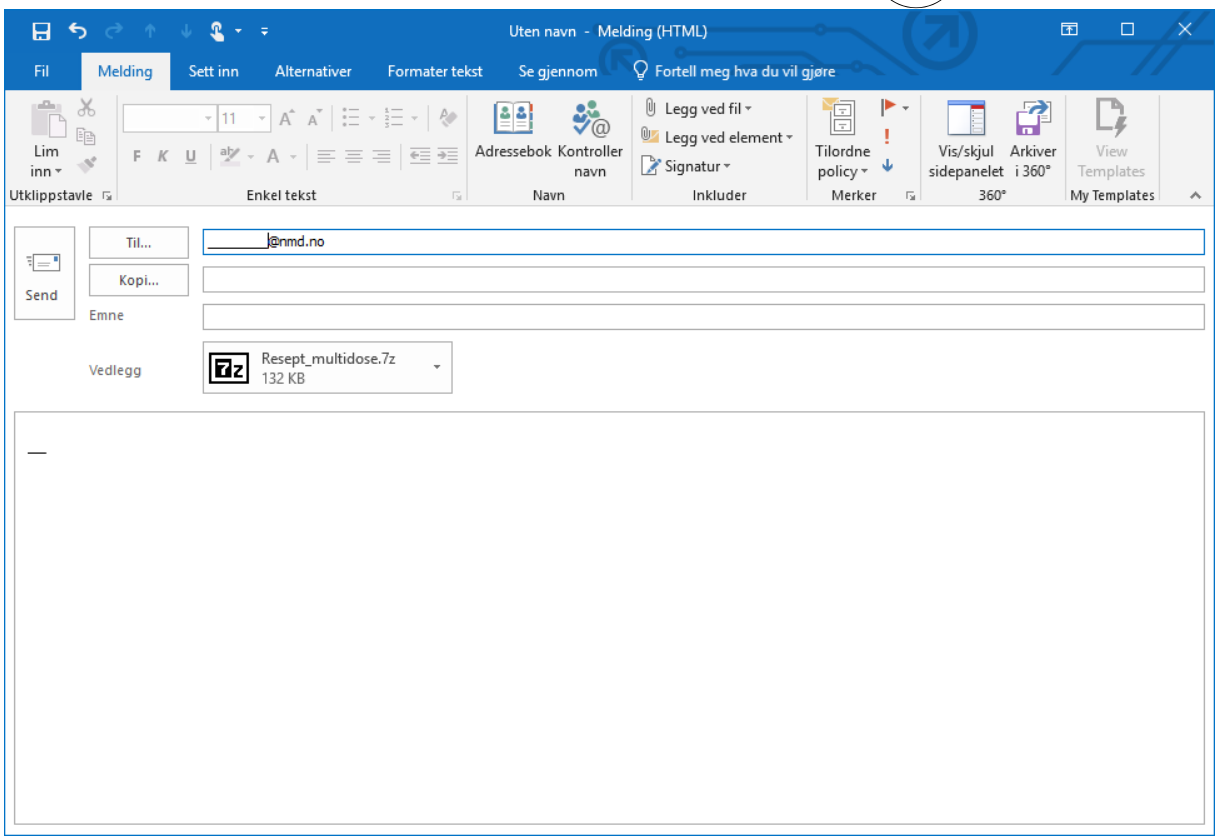
❖ Alternativ løsning er at Stavanger kommune supplerer passord til avsender og mottaker. OBS! Gjelder for virksomheter, leger tilknyttet Stavanger kommune. Passordet kan ha varighet på for eksempel 3 måneder, 6 måneder ect. Kun NMD vil ha dette passordet. Dersom en slik løsning er ønskelig, må Stavanger kommune utrede hvem i kommunen som skal supplere passord og ha ansvar for denne rutinen.

Dokumentet er elektronisk godkjent og sendes uten signatur.



- Klikk: OK
- Skriv inn mottaker adresse, emne og tekst
- Klikk Send

Dokumentet er elektronisk godkjent og sendes uten signatur.



- Husk å slett e-posten etter at den er sendt

Dokumentet er elektronisk godkjent og sendes uten signatur.