

Views: 18165

# Sikker Post/Krypteret E- Mail

Vi kan sende sikker på flere måder. Hvis modtageren er på tunnellisten (se nedenfor), sker kryptering automatisk. Hvis man ikke er på tunnellisten, kan du kryptere gennem din Outlook klient/Outlook på web. Se mulighederne nedenfor.

# Indholdsfortegnelse

## e

Hvis du skal sende krypteret mail

Tunnelmail

Krypteret mail i Outlook

Sådan ser modtageren den krypterede mail

Når modtageren benytter Outlook, og mailkontoen er en Office 365 konto

Når modtagerens mailkonto ikke er en Office 365 konto

Hvis du skal modtage krypteret mail

Er de på tunnellisten

Er de ikke på tunnellisten – men bruger offentligt certifikat

Bruger afsenderen kryptering fra deres egen mail

Tekniske betegnelser

Hvad er en krypteret mail?

Hvad er en tunnelliste?

# Hvis Du Skal Sende Krypteret Mail Tunnelmail

**Når du skal sende sikker post (en krypteret e-mail) fra DMJX, kan du gøre det på følgende måde:**

1. Tjek om modtagerens domæne findes på "Tunnellisten" (vi har domænet .dmjx.dk)
  1. Du kan se tunnellisten ved at gå ind på [denne side](#) – **og vælge linket til tunnellisten.**
2. Hvis modtagerens domæne er på tunnellisten, kan du blot sende din mail som normalt.
3. Hvis modtageren IKKE er på listen, skal du gøre nedenstående. Det virker KUN, hvis modtageren har et offentligt certifikat

1. Opret din mail som normalt.
2. Start emnefeltet med **#K-sikkerpost#**
3. Send din mail.
4. Hvis modtageren ikke har et offentligt certifikat, vil du modtage en mail retur, hvori du får besked om, at din e-mail ikke kunne sendes. Dermed kan modtageren ikke modtage krypteret e-mail, og der skal findes en anden løsning på at udveksle data. Du kan søge om der er et offentligt certifikat – [Klik her >>](#) (og søg på den e-mail adresse, du vil sende til)

# Kryptér Mail I Outlook

Hvis du ikke kan sende over tunnelmail, kan du sende krypteret via din Outlook Klient/webmail. Se nedenfor hvordan.

1. Lave ny mail og vælg herefter kryptering:
  1. Outlook til **Mac**: Klik på Kladde -> Krypter (vælg én af indstillingerne nedenfor)
  2. Outlook til **Windows**: Klik på fanen Indstillinger > Kryptér (vælg din konto og vælg én af indstillingerne (se nedenfor)
  3. Outlook på **Web**: "de 3 prikker i bunden" -> Kryptér. Ændring af indstillinger, forgår i toppen af den mail, du er ved at skrive (vælg én af indstillingerne nedenfor).
2. Herefter kan du vælge mellem nedenstående muligheder.
3. Når du har valgt din indstilling, skrevet din mail, sender du den "helt normalt".

## “Kun krypteret” og “Videresend ikke”

Man kan bruge “Kun krypteret”/”videresend ikke” til alle mailadresse. Nogle modtagere kan se mailen direkte i sin indbakke – det gælder internt i DMJX i Outlook (web og klient). Og hvis man ikke har en DMJX-mail, får man en mail med et link, hvorefter man kan logge ind og se læse sin mail. Der bliver jf. Microsoft krypteret med S/MIME – [Se link >>](#)

Ved “Videresend ikke” krypteres mailen, og modtageren får ikke mulighed for at trykke på knappen “videresend”

## “DMJX - Confidential”

Kan kun bruges internt med @dmjx.dk adresser

## “DMJX - Confidential view only”

Kan kun bruges internt med @dmjx.dk adresser og man kan IKKE se vedhæftede filer.

# Sådan Ser

# Modtageren Den Krypterede Mail Når Modtageren Benytter Outlook, Og Mailkontoen Er En Office 365 Konto

Sender du en krypteret mail til en anden Office 365 bruger, så skal mailen ikke dekrypteres, da modtageren allerede er logget på Office 365. Alt sker altså automatisk.

# Når Modtagerens Mailkonto Ikke Er En Office 365 Konto

Når din krypterede e-mail er sendt til en bruger, som ikke har en Office 365 konto, vil mailen ikke straks blive vist. Modtager skal igennem en dekrypteringsproces, som beskrevet herunder:

1. Åben mailen
2. Klik på "Læs Meddelelsen"
  1. Der åbnes nu en fane i en browser.
3. Da modtager ikke har en Office 365 konto, klikkes på "Log på med en engangsadgangskode" eller log ind i din mail (afhængig af system). Hvis du er i tvivl, brug da "Log på med en engangsadgangskode"
  1. Vedkommende bliver viderestillet til en ny hjemmeside, hvor en engangskode skal indtastes.
  2. Koden sendes til indbakken, hvor man også har modtaget den krypterede mail.
4. Angiv engangsadgangskoden i feltet på hjemmesiden og klik på "Forsæt". OBS!

Engangsadgangskoden udløber 15 minutter efter den er afsendt af systemet.

Mailen vil nu være dekrypteret, og modtageren har mulighed for at læse beskeden.

# Hvis Du Skal Modtage Krypteret Mail

Her er det afsenderen, som skal sikre sig, hvordan de gør.

## Er De På Tunnellisten

Her går det af sig selv, da vi også er på den. Man kan blot sende til medarbejderen direkte.

# Er De Ikke På Tunnellisten - Men Bruger Offentligt Certifikat

1. Find vores offentlige certifikat på denne side - [Klik her >>](#)
2. Søg efter vores mail til sikker post - den er: sikkerpost@dmjx.dk
3. Afsenderen skal nu - ved hjælp af sine programmer - kryptere sin mail og sende den til os på: sikkerpost@dmjx.dk (altså IKKE direkte til medarbejderen)
4. Herefter vil modtage den sikre post, som vi kan dekryptere. Det er vigtigt, at der i den krypterede mail står, hvem der skal modtage mailen, da vi - efter dekryptering - skal sende den videre til den rette modtager her i huset.

HUSK at du altid kan kontakte Hanne Bilgrav (hab@dmjx.dk), hvis du skal have sendt sikker post, og ikke kan få ovenstående til at virke.

# Bruger Afsenderen Kryptering Fra Deres Egen Mail

Fungerer på helt samme måde, som når vi sender – så man kan se vejledningen, som er i toppen af denne artikel. Kræver dog, at afsenderen har licens/installeret det i egen organisation.

## Tekniske

# Betegnelser

## Hvad Er En Krypteret Mail?

En mail- som er krypteret betyder, at når man sender den fra DMJX bliver den kodet, så kun modtageren kan læse den.

## Hvad Er En Tunnelliste?

Tunnellisten er en liste, hvorpå en række virksomheder og institutioner har tilmeldt sig. Hvis man er på denne liste, overholder man en række sikkerhedsstandarder, der betyder, at man sender sikker post til hinanden.