



Sikker mail – Kryptering af e-mails

Brugervejledning

Indholdsfortegnelse

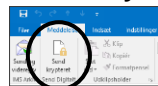
1 Introduktion	3
2 Anvendelse (Quick start)	3
2.1 Sikker e-mail	3
3 Brugergænsefladen (detaljeret)	3
3.1 Send Sikkert vinduet	4
3.2 Første opstart (Send Sikkert konfiguration)	5
3.2.1 Sikker mail konfiguration	5
3.3 Afsendelse af Sikker mail	6
3.3.1 Ændring af sikker mail afsenderinformation	8
4 Begreber	8

1 Introduktion

For at kommunikere sikkert til borgere, virksomheder eller andre myndigheder er det vigtigt, at kommunikationen foregår krypteret. Hvis modtageren skal have sikkerhed for, at afsenderen er den, der gives udtryk for, skal kommunikationen tillige signeres.

Send Sikkert er et tilføjesprogram (add-in) til Outlook, der på en enkel og intuitiv måde, anvendes til at sende sikre (krypterede og signerede) e-mails, IT-Center Syd's løsning.

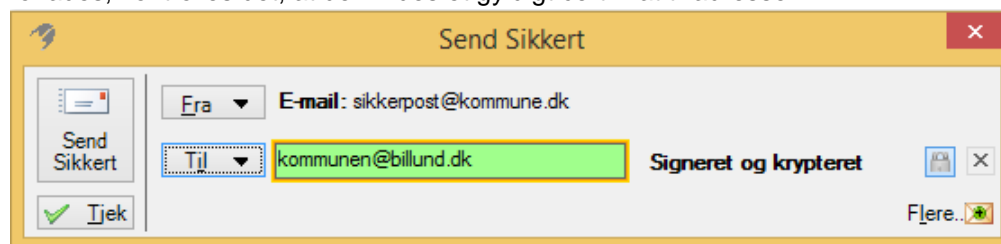
Dette betyder at du nu har fået en ny knap som sender krypteret.



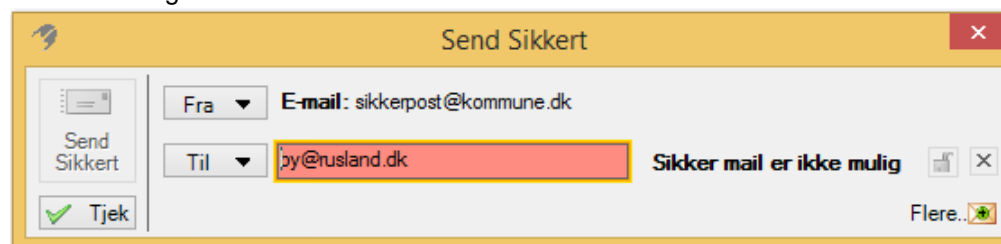
2 Anvendelse (Quick start)

2.1 Sikker e-mail

Hvis modtagerens e-mailadresse er kendt, og der er tilknyttet et DanID certifikat, kan e-mailen sendes som sikker mail. Dette gøres ved at angive e-mail adressen i adressefeltet. Når feltet forlades, kontrolleres det, at der findes et gyldigt certifikat til adressen.



Også her vil grønne indikere, at det er muligt at sende sikkert (Signeret og Krypteret). Rød indikerer, at der ikke er fundet et gyldigt certifikat, og der kan derfor ikke sendes sikkert til denne modtager.



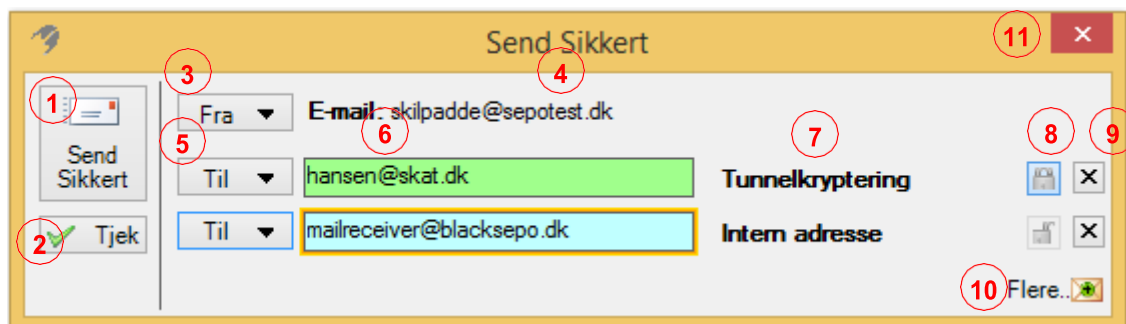
Hvis feltet bliver gult, kan der være opstået en forbindelsesfejl. Vent et øjeblik og forsøg igen. Der kan også være tale om en systemfejl. Hvis fejlen gentager sig, bør du kontakte systemadministratoren.

3 Brugergrensefladen (detaljeret)

Denne version af Send Sikkert introducerer en ny brugergrenseflade. Det primære mål med denne, er at give en enkel og intuitiv betjening.

Modtagere angives på hver sin linje. Når feltet forlades, eller der klikkes på Tjek, vil det blive valideret, om der kan sendes til den pågældende modtager. Resultatet af valideringen angives både med farver og en tekst ud for adressen.

3.1 Send Sikkert vinduet



Elementerne i Send Sikkert vinduet

1. **Send Sikkert** knappen anvendes til at afsende meddelelsen til de valgte modtagere. (Alt-S)
2. **Tjek** kan anvendes til at kontrollere, om der kan sendes til de indtastede modtagere. (Dette tjek udføres automatisk hver gang et adressefelt forlades) (Alt-T)
3. **Fra** anvendes til at korrigere afsenderinformation. Det er kun nødvendigt at ændre afsenderinformation, hvis de valgte standard værdier ikke skal bruges for netop denne afsendelse. (Alt-F) (se de følgende afsnit)
4. Ud for **Fra** knappen vises relevant **afsenderinformation**. Den viste afsenderinformation tilpasses den valgte modtager.
5. **Til (Cc, Bcc)** anvendes i forbindelse med opslag af en modtager adresse og definition modtagerens prioritet. Ved klik på denne knap vises fire funktioner: <Til>, <Cc> og <Bcc> anvendes til at bestemme hvilken prioritet den pågældende modtager har (Digital Post og Brev post vil dog altid blive sendt som primær modtager ("Til"). Den sidste funktion "**TunnelListe...**" er beskrevet i afsnit 3.3.
6. **Adressefeltet** anvendes til indtastning af modtageradressen. Her kan indtastes én e-mail adresse. Feltet skifter farve ved validering til **Grøn** (for afsendelse mulig), **Rød** (for afsendelse ikke sikker/ikke mulig), **Lysblå** (for intern adresse) og **Gul** (for fejl/validering ikke mulig).
7. Ud for **adressefeltet** vises **afsendelsesstatus**. Denne status angiver i tekst resultatet af valideringen.
8. Denne hængelås angiver om der anvendes kryptering (låst) eller ej (ulåst). I de fleste tilfælde vil denne lås være skrivebeskyttet, hvilket indikerer at den viste tilstand ikke kan ændres. Hvis ikke er påkrævet at kryptere signerede e-mails, vil det være muligt at ændre låsens tilstand ved at klikke på den.
9. **Krydsknappen** anvendes til at fjerne adresselinjer der ikke skal anvendes. (Alt-X)

10. **Flere...** anvendes til at tilføje flere adresselinjer så der kan tilføjes flere modtagere. (Alt-L)

11. Hvis e-mailen ikke ønskes sendt (endnu), klikkes på krydset i øverste højre hjørne.

3.2 Første opstart (Send Sikkert konfiguration)

For at forenkle den daglige brug af Send Sikkert, er der en række standardindstillinger, der skal vælges første gang man tager Send Sikkert i brug, og som derefter anvendes hvis intet andet angives.

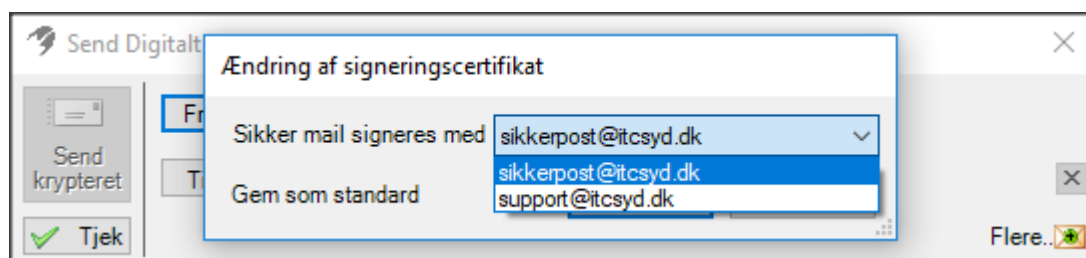
Note: Det er muligt at disse standardindstillinger allerede er valgt af systemadministratoren. I så fald behøver du ikke at ændre disse indstillinger.

Indstillingerne kan ændres, hvis dit arbejdsområde ændres. Enkelte af de indstillinger der er beskrevet i dette afsnit kan være usynlige eller skrivebeskyttet afhængig af de valg systemadministratoren har truffet i forbindelse med installationen af Send Sikkert.

Konfigurationen åbnes ved at klikke på knappen **Send Sikkert konfiguration** under fanebladet **Tilføjesprogrammer**.

Selv om værdierne kan accepteres uden ændringer, er det vigtigt at afslutte dialogen med OK for at sikre, at værdierne gemmes som dine standardindstillinger.

3.2.1 Sikker mail konfiguration

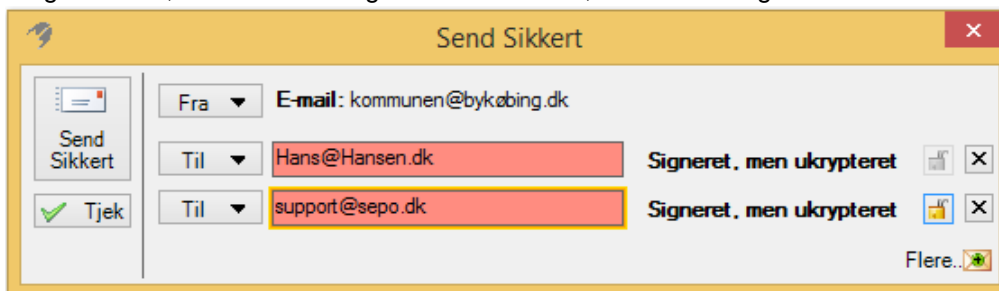


Med **Signerings-postkasse** sættes det signeringscertifikat, der skal anvendes som standard. Afhængig af SEPO konfigurationen vil det også være dette, der bestemmer afsender adressen på den sikre e-mail. Typisk vil man bruge sikkerpost@xxx.dk, men er du en af dem der ofte sender fra en af de andre vælger man den der passer til den mail adresse man sender fra. Se mere under afsnit 3.3.1

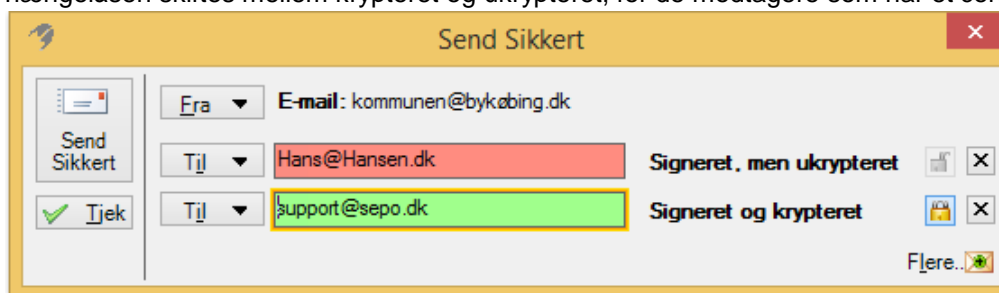
Signerede mails skal krypteres vil oftest være valgt, da dette sikrer, at der ikke kan sendes almindelige (ukrypterede) e-mails med Send Sikkert funktionen (ud over interne e-mails til

egen organisation). Denne egenskab kan dog kun ændres hvis den generelle konfiguration tillader det.

Hvis det skal være muligt at sende både krypterede og ukrypterede e-mails i samme arbejdsgang med Send Sikkert, skal dette flueben fjernes. Dette indebærer dog, at det er brugeren selv, der skal sikre sig at dette kun sker, når det er tilsigtet.



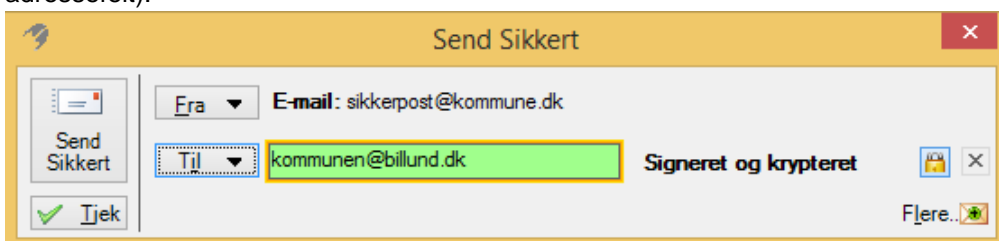
Ovenstående eksempel viser en modtager (Hans@Hansen.dk), der ikke har et certifikat og derfor kun **kan** modtage en signeret e-mail og en anden modtager (Support@sepo.dk) der har et certifikat, men hvor der **aktivt er valgt**, at e-mailen ikke skal krypteres. Ved klik på hængelåsen skiftes mellem krypteret og ukrypteret, for de modtagere som har et certifikat.



Denne valgmulighed er kun til stede, når **Signerede mails skal krypteres** ikke er sat.

3.3 Afsendelse af Sikker mail

Når du ønsker at anvende **Send Sikkert** til at sende en Sikker mail, starter du med at skrive e-mailen i Outlook som vanligt. Når du er klar til at afsende e-mailen, skriver du modtagerens e-mailadresse i adressefelt og klikker derefter på knappen **Send Sikkert**. (Alternativt kan du åbne Send Sikkert vinduet først og derefter skrive modtageres adresse ind i dette vindues adressefelt).

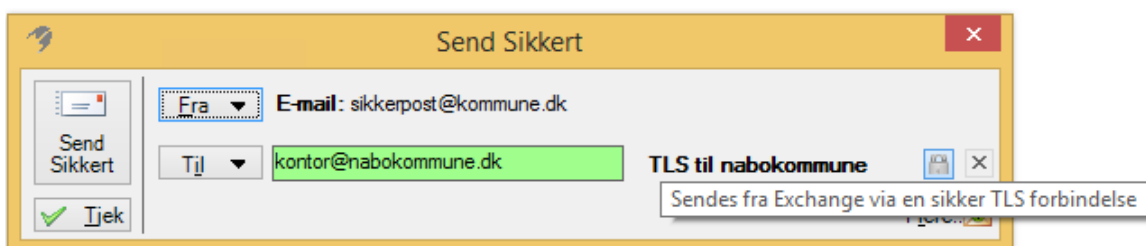


Ud for **Fra** knappen vises det certifikat, der anvendes til signering.

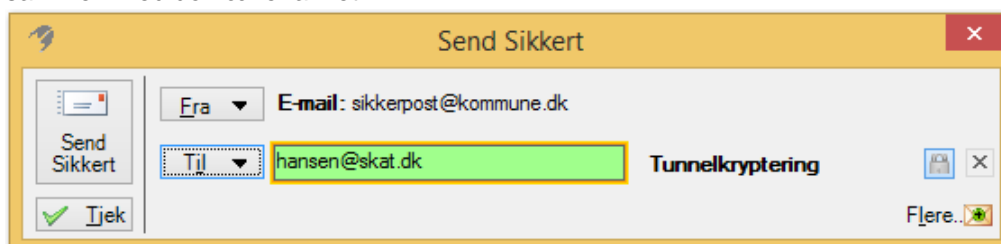
Hængelåsen indikerer om e-mailen krypteres. Denne lås kan kun ændres hvis konfigurationen tillader, at der kan sendes ukrypterede e-mails med Send Sikkert.

Hvis adresse bliver grøn når adressefeltet forlades, kan der sendes sikkert til denne modtager. Ud for adressen kan metoden e-mailen afsendes med læses som f.eks. **Signeret og krypteret** eller **Tunnel og egen kryptering**.

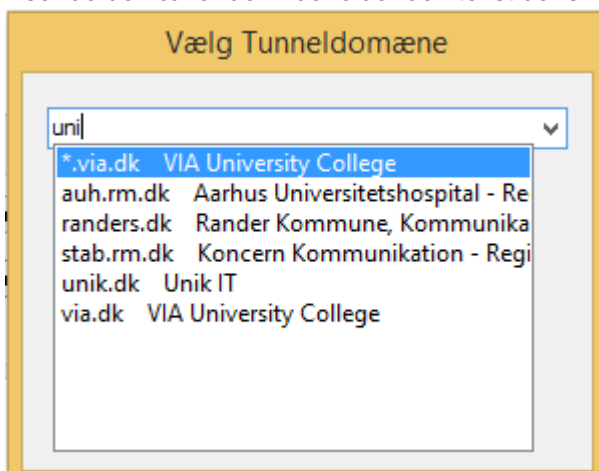
Mange virksomheder/myndigheder har etableret sikre forbindelser (udenom SEPO) til udveksling af e-mails med betroede samarbejdspartnere. Som en ny feature i Send Sikkert version 3.3.6 indikeres dette som vist herunder.



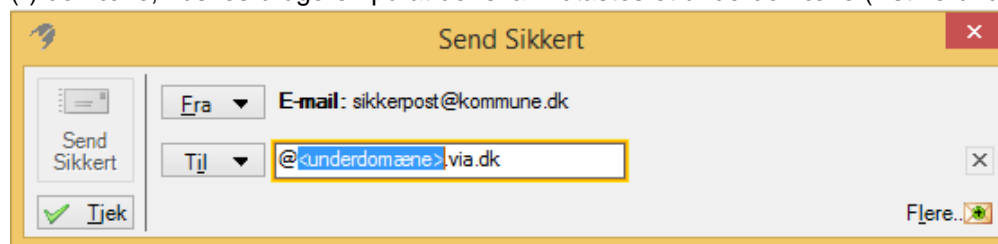
Denne feature kræver at administratoren definerer en liste med de pågældende modtagerdomæner. Teksten der vises til højre for adressen defineres af administratoren sammen med domænenavnet.



Når Send Sikkert anvendes sammen med SEPO version 3.9 eller senere, vil **Til** knappen have valgmuligheden **"TunnelListe..."**, der giver mulighed for at vælge blandt de tunnel domæner der er defineret i SEPO konfigurationen. Listen har en speed-search funktion der automatisk viser de domæner der indeholder den tekst der skrives i tekstboksen.

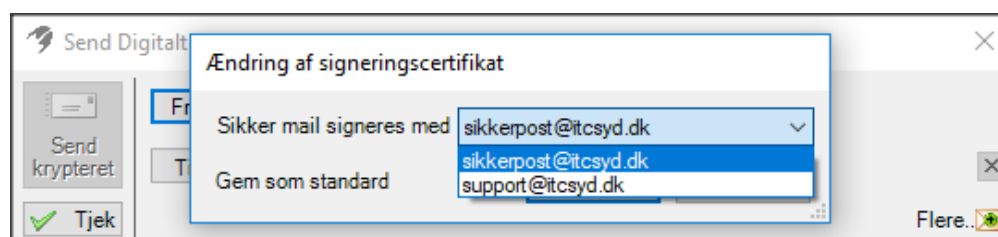
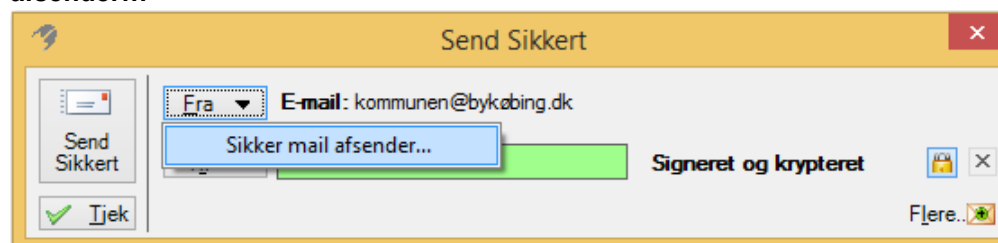


Det valgte tunnel domæne overføres automatisk til adressefeltet. Hvis der er tale om et stjerne (*) domæne, huskes brugeren på at der skal indtastes et underdomæne (vist herunder).



3.3.1 Ændring af sikker mail afsenderinformation

Hvis der er defineret flere certifikater, der kan signeres med i afdelingen, kan signeringscertifikatet ændres ved at klikke på knappen **Fra** efterfulgt af **Sikker mail afsender...**



Der kan tilføjes flere modtagere med knappen **Flere..**, og alle e-mail vil blive sendt med samme signeringscertifikat.

Denne ændring vil dog kun gælde for denne ene e-mail. Næste gang Send Sikkert anvendes, vil det oprindelige signeringscertifikat blive anvendt igen. Hvis ændringen skal bevares, skal standard indstillingerne ændres (se afsnit 3.2.1)

4 Begreber

Digital Post	Meddelelser der sendes til/fra borger eller virksomhed ved hjælp af e-boks' Dokumentboks løsning. Ofte tilgået af borgere via Borger.dk eller af virksomheder via Virk.dk , men også tilgængeligt fra e-boks.dk
Svar-postkasse	E-Boks betegnelse for et kontaktpunkt for borgeren til at sende meddelelser til myndigheden. Meddelelser til svar-postkasser videresendes til en sikker mailboks i SEPO og derfra videre til den tilhørende afdelings/fordelings-postkasse.

Svar-emne	E-Boks betegnelse for et fast defineret emne der kan/skal påføres meddelelser, der sendes til myndigheden.
Sikker mail	Fælles betegnelse for e-mails der sendes eller modtages via SEPO.
SEPO	Secure E-mail Post Office. Dette er navnet på DSI-NEXTs løsning til afsendelse og modtagelse af sikker post.
Kryptering	Metode til at sikre at en e-mail ikke er læsbar under transmissionen. E-mails der er krypteret skal de-krypteres, før de kan læses. (obs. Normalt er emnefeltet ikke krypteret. Derfor må følsomme data ikke placeres i emnefeltet)
Signering	En digital underskrift der beviser, at afsender er indehaver af den signatur, der er knyttet til e-mailadressen.
Certifikat	Et digitalt "nøglepar" der entydigt beskriver ejeren, og som anvendes til kryptering og/eller signering. Nøgleparret består af en privat og en offentlig nøgle. (En e-mail krypteret med en offentlig nøgle, kan kun dekrypteres af den tilhørende private nøgle).