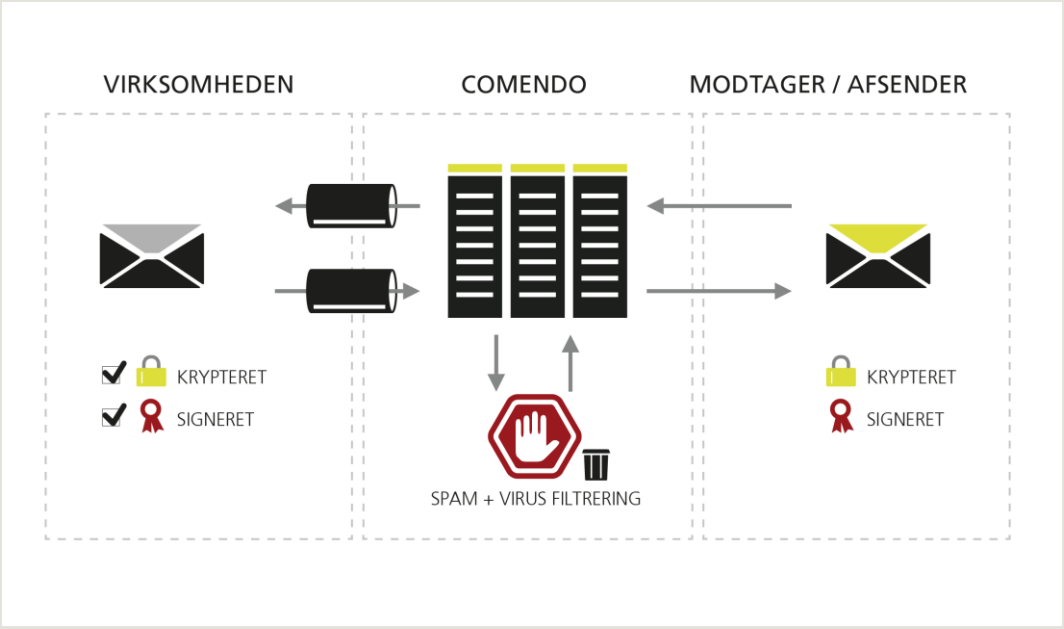
comendo
a j2 Global Company

Manual
Comendo SikkerMail

VERSION 19-06-2015



INDHOLDSFORTEGNELSE

OPSÆTNING AF SIKKERMAIL

For at få opsat produktet SikkerMail korrekt, skal der følges nogle få enkelte skridt.

TLS

SikkerMail kræver, at der oprettes en TLS (Transport Layer Security) forbindelse mellem Comendo og virksomheden.

For at oprette en TLS forbindelse til Comendo kræves et SSL-certifikat. Certifikater kan købes direkte hos en anerkendt Certificate Authority (CA) eller fra en autoriseret certifikatforhandler. TLS skal aktiveres i jeres mailserver og knyttes til et SSL certifikat.

Se bilag 1 for yderligere information vedr. MX Records, SMTP Relay og TLS.

MX-records, udgående SMTP og firewall indstillinger

Ligeledes skal virksomhedens MX-records og udgående SMTP relay ændres.

MX-records skal ændres til:

- MX 10 gw1-sec.net.comendo.com
- MX 20 gw2-sec.net.comendo.com
- MX 30 gw3-sec.net.comendo.com

Udgående smtp relay / smarthost sættes til:

- smtprelay-sec.net.comendo.com

Vi anbefaler også, at jeres firewallindstillinger ændres, så der kun kan modtages e-mail fra følgende IP-ranges:

- 89.104.216.0/24
- 89.104.217.0/24

Anskaffelse og installation af certifikater

Har I i dag ikke et virksomhedscertifikat, er det vigtigt at dette bestilles hos DanID.

DanID certifikater anskaffes ved at følge gældende procedure for virksomhedscertifikat anskaffelse.
Pt. findes anskaffelsesproceduren på flg. link:

https://www.nets-danid.dk/produkter/virksomhedssignatur/bestil_virksomhedssignatur/

Det er meget vigtigt, at virksomhedscertifikatet bestilles med den e-mailadresse som funktionspostkassen har.

Når certifikat link (e-mail) samt pinkode brev er modtaget skal certifikatet hentes fra DanID i PKCS#12 format. Dette gøres på flg. måde:

1. Kald certifikat link fra e-mail vha. en internet browser.
2. Accepter vilkår og tryk Næste
3. Angiv et navn (gerne så beskrivende som muligt) samt et kodeord – vær sikker på at PKCS#12 feltet er markeret og tryk Hent Digital Signatur.

Man bliver bedt om at gemme certifikatet. Virksomheden skal gemme certifikatet et sted hvor der er rettighedsmæssig beskyttelse – tilknyttede kodeord skal ligeledes beskyttes.

Genbestille certifikat

Hos DanID kan I genbestille jeres certifikat. Følg venligst DanID's vejledning.

Fremsendelse af certifikat og kode

Certifikat og kode skal tilføjes til SikkerMail serveren hos Comendo. Således skal både certifikat og kode sendes til Comendo.

Certifikatet kan sendes pr. e-mail til cert@comendo.com.

Koden sendes i separat e-mail til certpass@comendo.com.

BRUGERVEJLEDNING

Det er nu muligt for alle medarbejdere i virksomheden at kommunikere sikkert med klienter, borgere, virksomheder og offentlige myndigheder ved brug af sikker e-mail. Dette betyder, at det vil være muligt fremover at sende materiale indeholdende fortrolige oplysninger (f.eks. virksomheds- eller personoplysninger) med e-mail, hvor det tidligere har været nødvendigt at sende dette på papir.

Den sikre kommunikation sker ved brug af virksomhedens digitale certifikater, der er tilknyttet specielle sikre postkasser (funktionspostkasser).

For at sende signerede, respektivt krypterede e-mails med SikkerMail skal man angive hvilken handling man ønsker SikkerMail skal benytte på den pågældende e-mail.

NB: Sendes e-mails krypterede, er de altid signerede.

Hierarkiet i SikkerMail er som følger:

1. Explicit sikkerhed (Syntaks eller Outlook add-in)
   Således vil SikkerMail først undersøge om der er anvendt syntaks eller angivet noget ved brug af Outlook add-in. Er dette tilfældet, vil SikkerMail udføre den ønskede handling, eksempelvis vil "#K…" i emnefeltet medføre at e-mail sendes krypteret og signeret.

2. Implicit sikkerhed (funktionspostkasse->funktionspostkasse)
   Dernæst vil SikkerMail undersøge om e-mailen er sendt fra en funktionspostskasse til en anden ditto. Er det tilfældet vil SikkerMail sende e-mailen krypteret og signeret.

3. Tunnelmails
   Dernæst vil SikkerMail undersøge om modtager af e-mail understøtter tunnelmails. Er dette tilfældet, vil e-mailen blive afsendt som tunnelmail.

4. Evt. Secure-IT
   Dernæst vil SikkerMail undersøge om afsender understøtter og har tilkøbt Secure-IT modulet, samt om modtager gør ditto. Er dette tilfældet, vil e-mailen blive afsendt jævnfør regler og funktioner i Secure-IT.

	BRUGER INTERAKTION / OUTLOOK ADDIN	OPPORTUNISTISK LEVERING
EXPLICIT	Ja	Nej*
IMPLICIT	Nej	Ja
TUNNELMAILS	Nej	Ja

* Explicit vil sikre at e-mails kun leveres såfremt de kan leveres krypteret, i modsat fald vil de ikke blive leveret og afsenderen vil blive notificeret om den manglende fremsendelse.

Digital underskrift og kryptering

Når man anvender certifikater til sikker e-mail, er det muligt at vælge, om der kun skal sendes med signatur eller med både digital underskrift og kryptering.
Kun digital underskrift: Giver modtageren af en meddelelse garanti for, at den kommer fra den person, som påstår at have sendt den (= autenticitet) og sikkerhed for, at en modtaget meddelelse er identisk med den meddelelse, som afsenderen sendte (= integritet).

Digital underskrift + kryptering: Som ovenfor + sikkerhed for, at ingen uvedkommende kan få kendskab til meddelelsens indhold (fortrolighed).

Afsendelse af almindelig e-mail foregår fuldstændig på samme måde, som man plejer. Det er kun, hvis man ønsker at signere/kryptere e-mailen, at der skal foretages noget ekstra.

Det er en forudsætning for afsendelse med både signatur og kryptering, at SikkerMail løsningen 'kender' modtagerens certifikat. Er modtagerens certifikat registreret i DanID's certifikatoversigt, hvilket kan undersøges på https://selvbetjening.certifikat.tdc.dk/ldapsearch/searchemail, eller har virksomheden modtaget en sikker e-mail fra modtageren, vil denne betingelse altid være opfyldt, idet certifikatet automatisk bliver gemt i systemet.

Afsendelse af sikker e-mail

Kryptering kan lade sig gøre til modtagere, der har en kendt digital signatur dvs. enten en offentlig signatur (OCES) eller har sendt myndigheden eller medarbejderen en e-mail med digital signatur.

Forudsætninger for afsendelse af signeret og krypteret e-mail:

- Der skal afsendes fra en e-mail adresse, der har tilknyttet et virksomhedscertifikat.
- Der skal sendes Signeret mails til alle modtagere, uanset mail adresse, land, virksomhed eller privat.
- Der skal sendes Krypteret og Signeret mails til de mailadresser der har et certifikat tilknyttet deres mail adresse.
- Såfremt det ikke er muligt at aflevere mailen krypteret og signeret, bliver mailen returneret til afsender, med besked om manglende levering, da mailen ikke kunne leveres sikkert.

Opslagsregister for mailadresser med tilknyttet certifikat fra DanID se:

https://www.nets-danid.dk/produkter/nemid_medarbejdersignatur/information_om_nemid/sikker_e-mail/soeg_certifikat/

Anvendelse af SikkerMail Outlook Add-in (se senere i denne guide) eller syntakskode (se bilag 2) kan tilsikre at den afsendte e-mail bliver krypteret og signeret. Såfremt det ikke er muligt at aflevere mailen krypteret og signeret, bliver mailen returneret til afsender, med besked om manglende levering, da mailen ikke kunne leveres sikkert.

Send altid krypteret til specifikke modtagere

I kan konfigurere en liste af modtagere, som understøtter modtagelse af krypterede e-mails – eksempelvis funktionspostkasser – som I vil sikre altid bliver sendt som krypterede e-mails fra jeres system.

I definerer listen af modtagere, minimum en e-mail adresse, og sender den til Comendo Support.
Derefter vil e-mails til disse bestemte/definerede e-mailadresser, "skrives om" og afsendes fra virksomhedens funktionspostkasse, signeret og krypteret, til modtager. Bemærk at e-mailen får en ny/anden afsender adresse og dette medfører at svar fra modtager vil blive sendt til jeres funktionspostkasse. Ligeledes vil eventuelle fejlmeddelelser og lignende også blive sendt til funktionspostkassen.

Således kan kryptering enforces til bestemte modtagere, bestemt af jeres administrator.

Alt e-mail til bestemte adresser, krypteres automatisk, uden brugerinteraktion, Outlook Add-in, syntaxkode eller andet.

Modtagelse af sikker e-mail

Sikker e-mail modtages altid i virksomhedens sikre postkasser (funktionspostkasser). Sikker e-mail vil altid automatisk være blevet kontrolleret inden den når frem til funktionspostkassen. Kontrollen omfatter dels om der er anvendt korrekt digitalt certifikat (OCES), og dels om certifikatet er gyldigt, dvs. ikke spærret eller udløbet.

Signatur-bevis.txt

Er den modtagne e-mail signeret med en gyldig digital nøgle, er der vedhæftet en fil der hedder signaturbevis.txt. Dette signaturbevis angiver at der har været udført en behandling/kontrol af e-mailen ved modtagelse. Resultatet af denne kontrol fremgår af et såkaldt signaturbevis, som vil være vedhæftet den modtagne e-mail. Signaturbeviset skal gemmes sammen med den e-mail den vedrører, idet signaturbeviset er medarbejderens dokumentation for den foretagne kontrol af certifikatet.

Den videre håndtering af den modtagne sikre e-mail, eksempelvis videresendelse til medarbejder, afhænger af myndighedens e-mailpolitik.

Advarsel.txt

Hvis posten modtages med et vedhæftet dokument der hedder "Advarsel.txt" er der et sikkerhedsmæssigt problem med modtagelse af posten f.eks. ugyldig signatur. Virksomhedens e-mail ansvarlige bør kontaktes/orienteres i disse tilfælde. Den konkrete håndtering af den modtagne meddelelse med et sikkerhedsproblem må vurderes ud fra indholdet.

Vedhæftningen Sikkerhed.txt kan bl.a. indeholde følgende beskeder:

- Meddelelsen var signeret men signaturen kan ikke verificeres. Meddelelsen kan være ændret!
- Certifikatet på den modtagne e-mail er ikke gyldigt eller er ikke et OCES certifikat
- Kryptering af e-mail til følgende modtager kunne ikke foretages, certifikat er ikke kendt
- Udstederen af certifikatet

Lidt viden omkring anvendelse af centrale certifikater

Der bliver altid automatisk foretaget et opslag i et centralt register for alle modtagere af en sikker post hos DANID (/OCES). Opslaget sker for eventuelt at kunne knytte et digital certifikat til modtageren, hvilket f.eks. er nødvendigt for at kunne sende krypteret e-mail. Derudover kan systemet håndtere certifikater fra modtagere der ikke har et offentligt certifikat.

Når en sikker post modtages foretager systemet en læsning af afsenderens certifikat. Hvis certifikatet ikke er et DANID/OCES certifikat gemmes dette centralt og anvendes ved krypteret besvarelse.

Hvis man prøver at sende til et modtager der ikke har et offentligt DanID/OCES certifikat og ikke har modtaget sikker e-mail fra personen man ønsker at sende til, vil afsendelse fejle. Man bør i de situationer bede den, som man vil sende til, om at fremsende en sikker e-mail hvorved certifikatet automatisk bliver registreret.

Bemærk: Det er pt. Ikke muligt at sende sikker post mellem myndigheder/virksomheder som er tilknyttet samme interne mailsystem. Intern post anses for at være sikker.

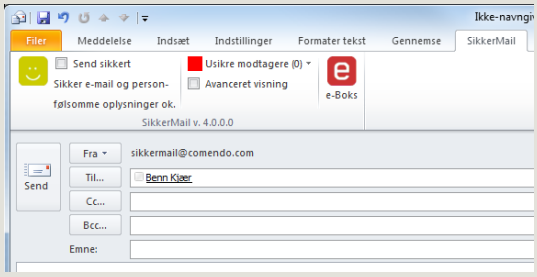
OUTLOOK ADD-IN

Comendo SikkerMail Outlook add-in kan hjælpe brugere med korrekt afsendelse af sikre e-mail med kryptering samt at kontrollere hvorvidt modtagere kan modtage krypterede e-mails, inden e-mailen afsendes.

Integreret mod kundens Active Directory (AD) bistår Comendo SikkerMail Outlook add-in brugere med at vælge funktionspostkasse, måtte dette ønskes.

Markeres en e-mail til at skulle fremsendes krypteret, vil Comendo udelukkende levere den såfremt dette er muligt – i modsat fald hindres levering og afsender adviseres.

Comendo's Outlook add-in vers. 4.0 gør brugen af SikkerMail endnu nemmere og hjælper brugeren med automatisk at vælge den mest sikre og direkte forsendelsestype som muligt.



Add-in'et installeres som en fane i Outlook klienten og benyttes nemt ved at vælge fanen. Det vises øjeblikkeligt om e-mailen kan sendes sikkert eller ej, ligesom der er yderligere info vedr. eventuelle usikre modtagere.

Funktioner

Inden afsendelse af en e-mail er det muligt at se hvorvidt den pågældende e-mail kan sendes sikkert. Det visualiseres med ikoner samt tekst, der indikerer om modtager er i stand til at modtage sikkert.

Sikker e-mail og personfølsomme oplysninger ok.

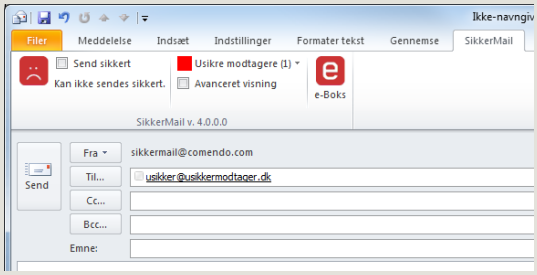
Kan ikke sendes sikkert.

Således skal den enkelte medarbejder kun tage stilling til om ikonet er grønt eller rødt.

Såfremt virksomheden betragter TLS som sikkert (kan konfigureres på centralt hold) vil TLS også give en grøn smiley.

Indeholder e-mailen fortrolige eller personfølsommme oplysninger kan afsenderen markere at e-mailen ønskes sendt sikkert og Comendo's plugin vælger automatisk imellem TunnelMail, krypteret e-mail eller TLS.

Ved at benytte Comendo's sikrede cloud tjenester, kan add-in'et med det samme afgøre hvilken sikker e-mail metode en modtagers e-mailsystemer understøtter. Brugeren advares med det samme, hvis nogle modtagere ikke kan modtage sikkert og skal derfor ikke vente på at få en fejlbesked via e-mail senere.



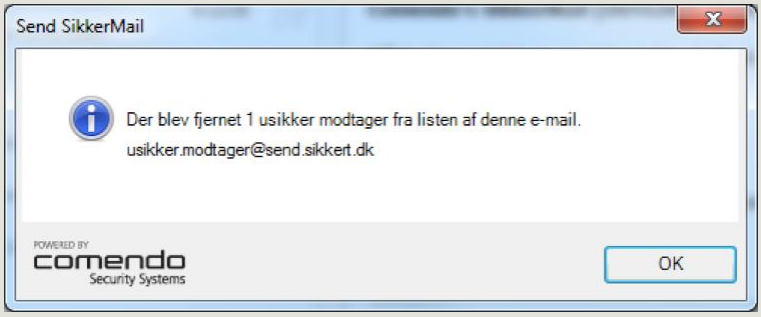
Add-in'et har her detekteret tre usikre modtagere ud af fire mulige og således kan e-mailen ikke sendes sikkert og er markeret rød.

Er den eneste sikre mulighed for at sende krypteret via afsendelse fra en fælles postkasse/funktions-postkasse, beder add-in'et brugeren om at vælge hvilken postkasse, der skal sendes fra. Information om mulige funktionspostkasser for den enkelte bruger defineres som rettigheder i AD og synkroniseres automatisk med add-in.

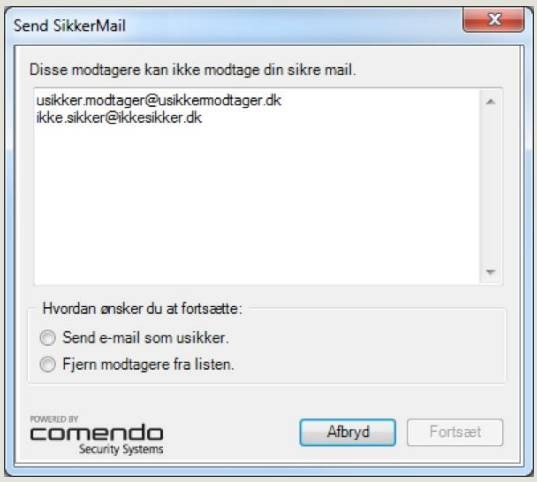
Advarsler / dialogbokse

Under installeringen kan man vælge om man ønsker at programmet automatisk skal fjerne e-mail adresser som er placeret under "Usikre modtagere" eller ej.

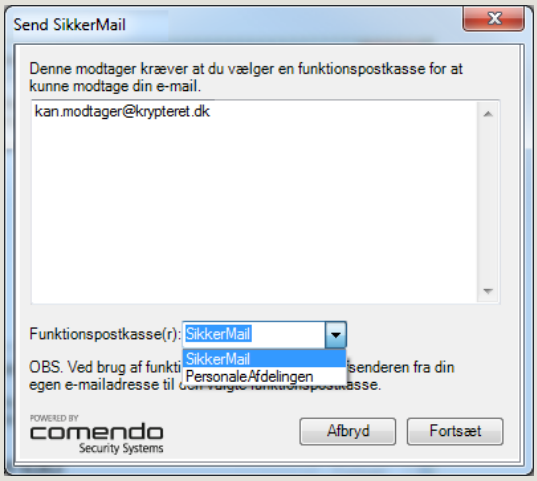
Hvis fjern e-mail adresser automatisk er valgt, vil denne dialog blive vist efter afsendelsen af e-mail'en.

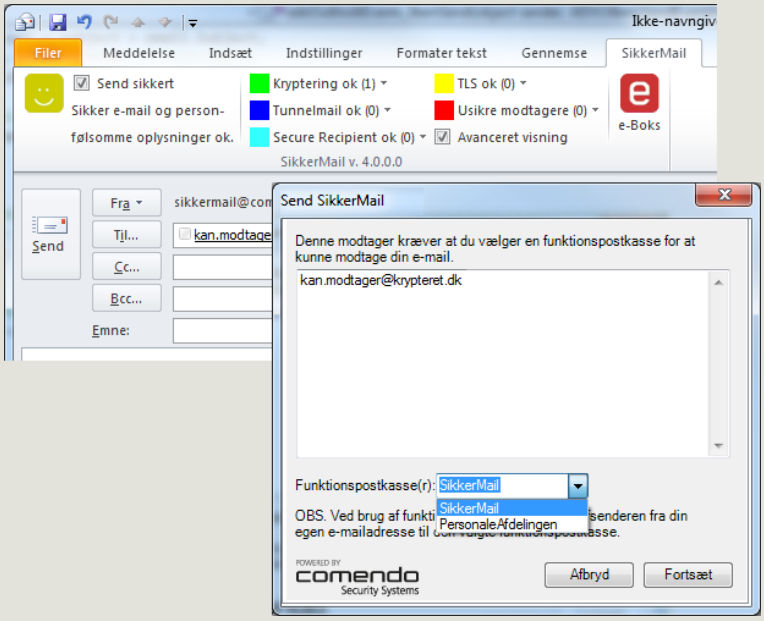


Hvis programmet ikke må fjerne "Usikre modtagere" automatisk, vil denne dialog blive vist i forbindelse med afsendelse til de "usikre modtagere". Man skal så selv foretage et valg.



Hvis sender til en modtager som kræver at afsenderen er en funktionspostkasse vil et af nedenstående skærmbilleder blive vist. Hvis man har mere end én (1) funktionspostkasse angivet.





Denne e-mail kan kun sendes sikkert, såfremt den sendes fra en funktionspostkasse. Baseret på brugerens rettigheder i Exchange AD, vises mulige funktionspostkasser og der vælges nemt den rigtige postkasse, så e-mailen kan sendes sikkert.

Add-in'et deler naturligvis automatisk den originale e-mail op i det nødvendige antal forskellige e-mails, der passer til de sikre metoder netop denne e-mails modtagere benytter sig af (TunnelMail, krypteret, SecureIT, TLS).

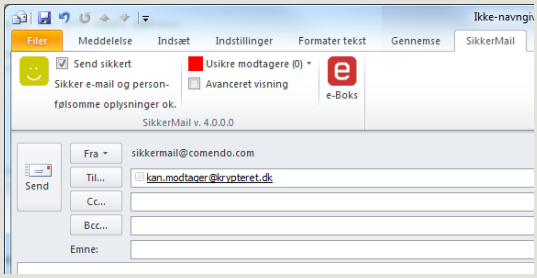
Brugeren ser et simpelt interface, med små ikoner og gode danske forklaringer på eventuelle problemer.

Avanceret visning

Det er i add-in'et muligt at vælge "Avanceret visning" og dermed få adgang til yderligere informationer om krypteringsmulighederne til de valgte modtagere.

Kundernes IT medarbejdere kan fortsat få fuldt overblik til at fejlsøge eventuelle problemer, men denne information er gemt lidt væk, så den enkelte sagsbehandler/medarbejder ikke forstyrres i sit daglige arbejde.

Med denne valgmulighed kan man få et overblik over hvordan den enkelte e-mail modtagere er placeret sikkerhedsmæssigt. Det er den system administrator der afgør om denne valgmulighed bliver vist eller ej.



Add-in med mulighed for at vælge "Avanceret visning" – den avancerede visning er foldet ind.

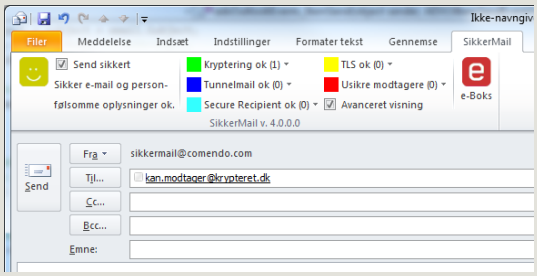
Kryptering ok:
E-mail modtagere der kan modtage krypterede e-mails. Typisk en funktionspostkasse hos modtager. (Grøn)

TunnelMail ok:
E-mail modtagere der kan modtage tunnelmails. Typisk en medarbejder, hvor domænet understøtter tunnelmail funktionalitet. Disse modtagere inkluderer også funktionspostkasser, som ydermere vil optræde under Kryptering OK. (Blå)

Secure Recipient ok:
E-mail modtagere der altid sendes krypteret til. Listen vedligeholdes af jeres IT administrator. Disse modtagere inkluderer også funktionspostkasser, som ydermere vil optræde under Kryptering OK. (Cyan)

TLS ok:
E-mail adresser der kan modtage via TLS. (Gul)

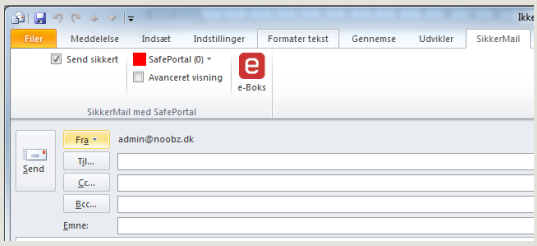
Usikre modtagere:
E-mail adresser der ikke er sikre. (Rød)



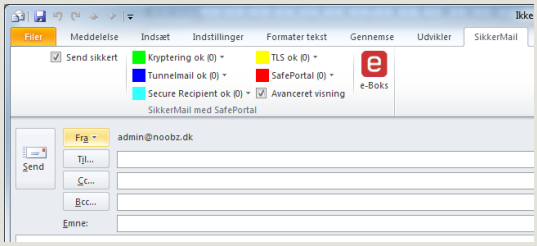
Add-in med mulighed for at vælge "Avanceret visning" - den avancerede visning er foldet ud og der vises krypteringsmuligheder for hver enkelt modtager af e-mailen.

Aflevering til safePortal

Såfremt Comendo safePortal er tilkøbt som produkt og gjort teknisk tilgængelig via eget AD eller konfigurationsfilen til Outlook Add-in'et, vil det fremstå som nedenstående.



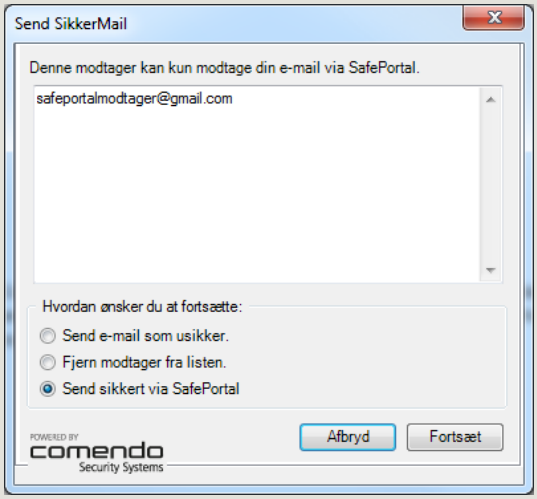
Add-in med mulighed for at vælge "Avanceret visning" – den avancerede visning er foldet ind. Bemærk at "SafePortal" fremgår.



Add-in med mulighed for at vælge "Avanceret visning" - den avancerede visning er foldet ud og der vises krypteringsmuligheder for hver enkelt modtager af e-mailen. Bemærk at "SafePortal" fremgår.

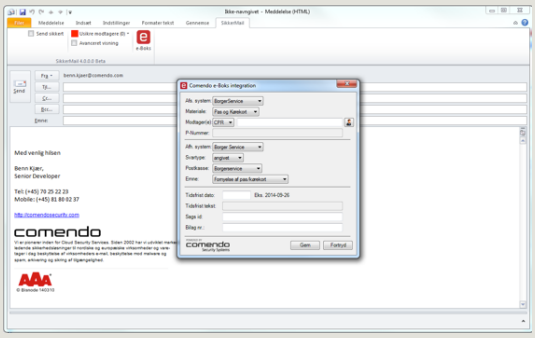
Under installeringen kan man vælge om man ønsker at programmet automatisk skal aflevere via safePortal, til de e-mail adresser som der ikke kan sendes "sikkert til", eller ej.

Såfremt det *ikke* er valgt at sende automatisk til safePortal, vil brugeren før afsendelse blive spurgt hvorvidt der ønskes at blive sendt som en usikker og almindelig e-mail eller sikkert og krypteret via safePortal.



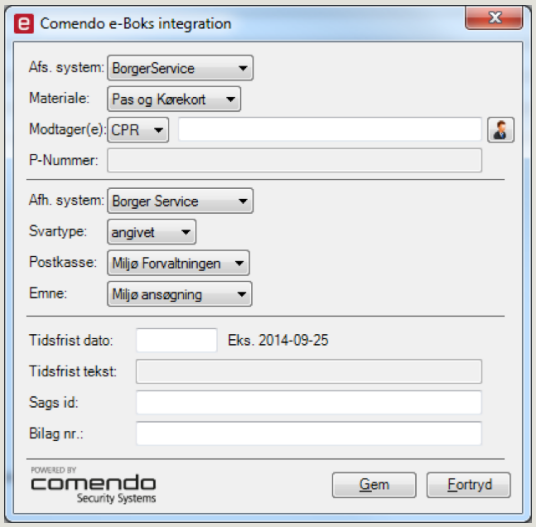
Aflevering til e-Boks

E-boks integration er en integreret og gratis del af Comendo SikkerMail og dermed også Outlook add-in.



Dialogboks til fremsendelse af meddelelser til e-Boks. De forskellige valg er relateret til virksomhedens e-Boks opsætning og afleveringsaftale.

Kunder med en e-Boks afleveringsaftale og Comendo SikkerMail kan benytte Comendo's Outlook add-in til at skrive e-mails, lave vedhæftninger og afsende disse til CVR / CPR nummer modtagere via e-Boks.

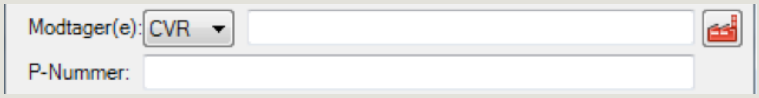


Afs. system:
Afsendersystem som skal anvendes til afsendelse af e-boks meddelelse.

Materiale:
Materiale (Emneteksten) der skal anvendes i e-boks meddelelsen.

Modtager(e):
CVR / CPR nummer som e-boks meddelelsen skal sendes til.

P-Nummer:
Undernummer på til en virksomhed.



 Importer fil med flere CVR numre. CVR numrene skal være adskilt med semikolon (;)

 Importer fil med flere CPR numre. CPR numrene skal være adskilt med semikolon (;)

Afh. System:
Afhentningsystem der skal anvendes hvis virksomheden / borgeren kan besvare e-boks beskeden.

Svartype:
Standard: Svarmulighed som angivet under e-boks.
Angivet: Mulighed for selv at angive Postkasse og Emne som svar skal placeres i.
Ikke muligt: Det er ikke muligt at besvare meddelelsen.

Postkasse:
Postkasse som besvarelse skal placeres i.

Emne:
Emne i postkasse som besvarelse skal placeres i.

Tidsfrist dato:
Her kan angives en dato hvis virksomheden / borgeren skal svare på meddelelsen inden en given dato.

Tidsfrist tekst:
Tekst der angives sammen med tidsfrist dato.

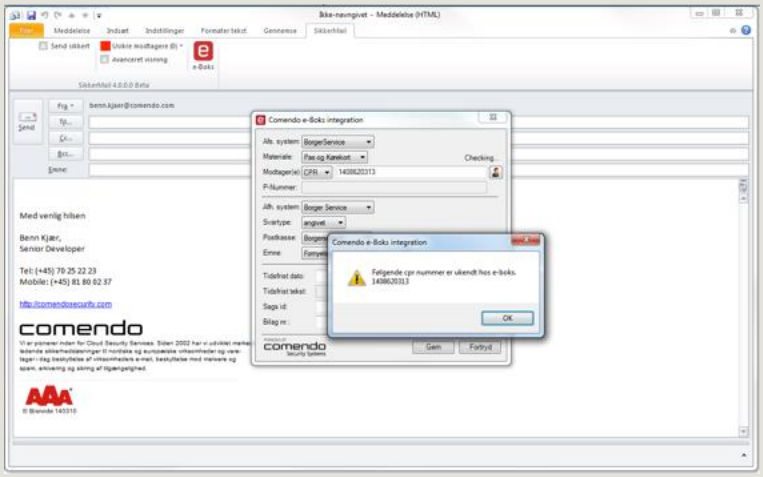
Sags id.:
Sagsnummer der evt. refereres til.

Bilag nr.:
Bilags nr. der evt. refereres til.

Ved tryk på knappen Gem og alle data er udfyldt korrekt bliver der dannet en fil som skal sendes til e-boks. Det er ud fra indholdet af denne fil som e-boks sender en meddelelse til virksomheden / borgeren.

Ved tryk på knappen Fortryd slettes alle indtastede e-boks data og der returneres til en blank e-mail.

CPR / CVR validering



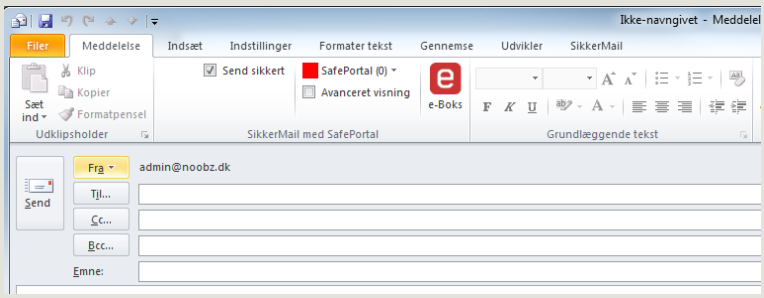
Når en meddelelse sendes til e-Boks, kan den sendes til CPR eller CVR numre. Disse numre valideres for både validitet og om den pågældende modtager er oprette hos e-Boks og accepterer meddelelser fra den konkret afsender.

Alle CPR samt CVR numre valideres for korrekt format samt valideres online mod e-Boks. Således vil det allerede inden afsendelse være muligt at vide om et eller flere CPR eller CVR er valide, oprettede hos e-Boks samt om de accepterer henvendelse fra den pågældende afsender.

Ændre placering af SikkerMail Outlook add-in

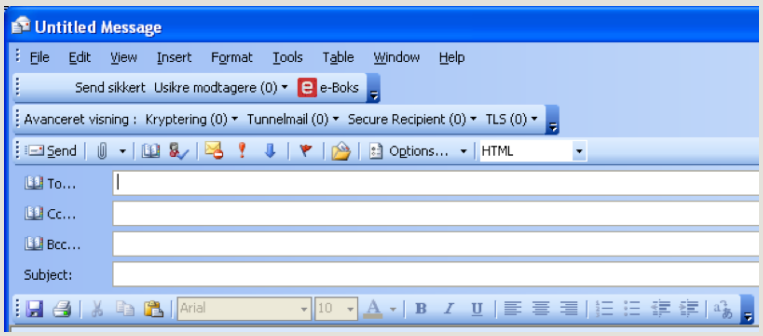
For de brugere der ønsker SikkerMail add-in'et placeret i "Meddelelse" fanen, som vist nedenfor, kan det tilpasses på følgende måde:

"Ny e-mail > Filer > Indstillinger > Tilpas båndet."



Office 2003

Ved klik på Ny vises værktøjslinjen til SikkerMail.



Værktøjslinjer

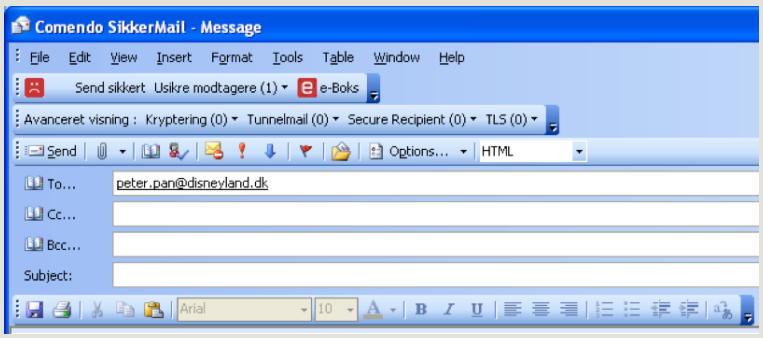
Send Sikkert:
Ved denne markering sendes e-mailen med højest mulige sikkerhedsniveau. Krypteret og signeret.

Usikre modtagere:
Viser antallet og hvilke e-mailadresser som betragtes som usikre.

E-Boks:
Se afsnit om e-boks længeden ide i dokumentet.

Avanceret visning:
Viser antallet af de enkelte mailtyper samt hvilke e-mailadresser som er kategoriseret hvor.

Når der indtastes en e-mail adresse bliver den valideret og der vises en overordnet status for hvordan aktuelle e-mail kan afsendes.



Sikker e-mail og personfølsomme oplysninger ok.

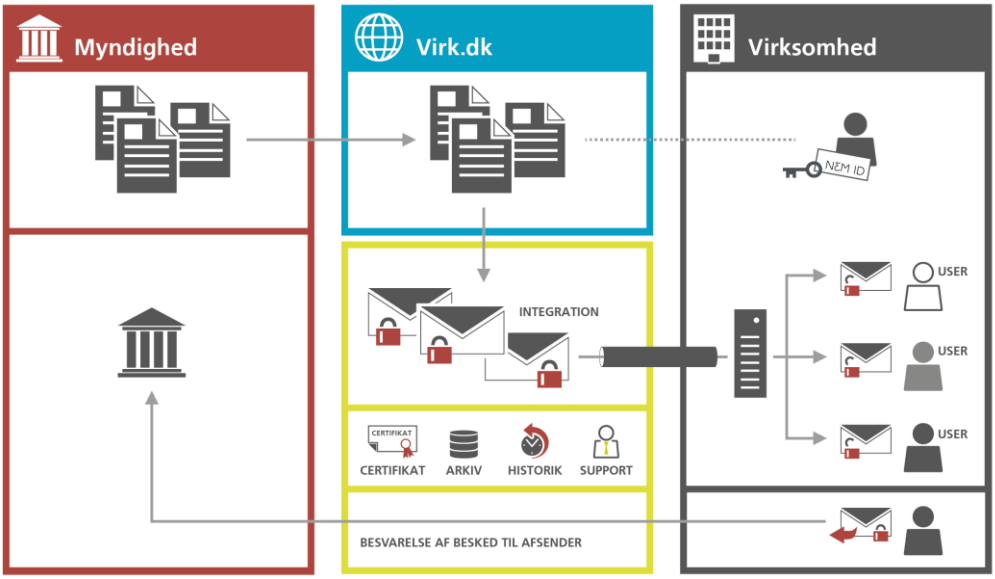
Kan ikke sendes sikkert.

For flere detaljer om add-in, se venligst afsnittet "Outlook Add-in".

INTEGRATION TIL VIRK.DK MED SIKKERMAIL

SikkerMail kan også integreres til Virk.dk. Det betyder at, SikkerMail automatisk krypterer og videresender meddelelser fra det offentlige til jeres virksomhed - uden at I skal bekymre jer om certifikater og koder.

Med SikkerMail får I en løsning, der automatisk fordeler meddelelserne fra de forskellige offentlige instanser til en eller flere medarbejdere. Derudover kan I opsætte ferieregler og videresendelsesregler, så de vigtige henvendelser fra det offentlige altid bliver håndteret korrekt.



Er I klar til Digital Post?

Hvis din virksomhed har e-Boks og er tilmeldt Digital Post fra det offentlige eller har oprettet en digital postkasse på Virk.dk, så opfylder I kravene for at modtage digital post fra det offentlige.

Er I i tvivl, kan I gå ind i virksomhedens digitale postkasse på Virk.dk under 'Tilmeldinger' og tjek, om I er tilmeldt "alle offentlige myndigheder".

Hvis din virksomhed ikke er tilmeldt "alle offentlige myndigheder" som afsendere, skal I gøre følgende:

1. Gå ind på Virk.dk
2. Tilmeld virksomheden "Digital Post".

Når I har tilmeldt jer Digital Post fra det offentlige, kan I både skrive til og modtage svar fra det offentlige via virksomhedens digitale postkasse på Virk.dk.

Gå direkte videre til Opsætning til Virk.dk på side 24.

Er I ikke klar til Digital Post?

For at blive klar til Digital Post, skal I være i besiddelse af en NemID medarbejdersignatur. Derefter skal I logge ind på Virk.dk og aktivere jeres digitale postkasse.

NemID - login til virk.dk

For at logge ind på virksomhedens side på Virk.dk skal I bruge en NemID medarbejdersignatur.
Det er Nets DanID, der udsteder en NemID medarbejdersignatur.

Opret NemID medarbejdersignatur

Har din virksomhed endnu ikke NemID medarbejdersignatur, skal den bestilles via Nets DanID på www.nets-danid.dk

1. Gå til www.nets-danid.dk for at bestille den første NemID medarbejdersignatur.
   Den person, som bestiller den første signatur, bliver automatisk NemID administrator i virksomheden.
   Det er administratoren, som bestiller de efterfølgende medarbejdersignaturer, hvis virksomheden har behov for det.

2. Følg trin-for-trin bestillingen på www.nets-danid.dk.

3. Udskriv aftalen, når bestillingen er gennemført.
   Underskriv aftalen, hvis du er ejer, eller få den underskrevet af en tegningsberettiget.
   Indsend aftalen til Nets DanID via e-mail, fax eller brev.

4. Vælg om NemID medarbejdersignatur skal sendes som nøglefil eller nøglekort

   Nøglefil: Signaturen kommer som et stykke software, som I installerer på én bestemt computer. De fleste virksomheder bruger nøglefil, som er den billigste løsning.

   Nøglekort: Et lamineret papkort med nøgler (engangskoder), som anvendes ved hvert log-in. Du modtager nøglekortet med posten og kan opbevare det i din pung. Du kender det måske fra NemID til private.

Priser

De første 3 medarbejdersignaturer er gratis. Ved behov for flere certifikater kan du læse mere på www.nets-danid.dk.

Login og aktivering af digital postkasse

Med NemID medarbejdersignaturen kan I logge ind på Virk.dk og aktivere jeres digitale postkasse.

1. Klik på "Opret digital postkasse"
2. Log ind med din medarbejdersignatur.
3. Klik på "Start oprettelse".
4. Vælg hvilken funktionalitet I vil bruge, enten "Standard" eller "Udvidet". SikkerMail fungerer med begge valg.
5. Angiv om du er med i ledelsen eller om et medlem af ledelsen skal acceptere oprettelse af den digitale postkasse.
5. Accepter vilkårene for oprettelse af en digital postkasse.
6. Bekræft virksomhedens navn.
7. Bekræft dine oplysninger og klik på "Godkend". Du har nu oprettet en digital postkasse.

Opsætning til virk.dk

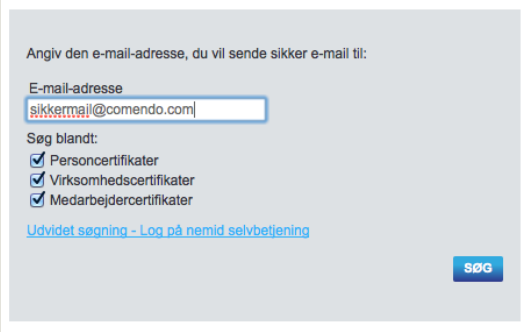
For at få videresendt jeres meddelelser fra det offentlige, skal I logge på Virk.dk og etablere denne videresendelse. I skal benytte den offentlige del af jeres virksomhedscertifikat for at, videresendelsen kan ske krypteret og i overensstemmelse med gældende lovgivning.

Hent den offentlige del af jeres virksomhedscertifikat

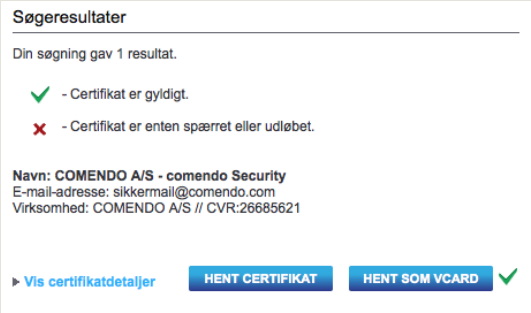
Hent den offentlige del af jeres certifikat på:

https://www.nets-danid.dk/produkter/nemid_medarbejdersignatur/information_om_nemid/sikker_e-mail/soeg_certifikat/

Skriv jeres e-mailadresse, der er tilknyttet jeres virksomhedscertifikat i dette felt, markér Virksomhedscertifikater og tryk søg.



Tryk på Hent certifikat.



Aktivering af videresendelse

Angiv e-mailadresse

I den digitale postkasse på Virk.dk under Indstillinger -> Videresendelse vælges Opret videresendelse.

I feltet "Certifikatets e-mailadresse" opgives den SikkerMail-adresse som er tilknyttet certifikatet.

Angiv medarbejder- eller virksomhedscertifikat

I feltet "Medarbejder- eller virksomhedscertifikat (base-64)" skal I vælge jeres virksomhedscertifikat, som I tidligere har hentet på www.nets-danid.dk/...

Bekræft jeres e-mailadresse

I modtager herefter en e-mail fra e-Boks A/S (som er leverandør til Digital Post), hvor e-mailadressen skal bekræftes for at forhindre misbrug. E-mailen indeholder et link, der skal anvendes.

Modtag posten i jeres e-mailsystem

Når I fremover modtager Digital Post på Virk.dk, sørger SikkerMail automatisk for at videresende posten, som en krypteret e-mail. Når disse e-mails modtages af jeres mailserver dekrypteres de automatisk og kan nu håndteres som helt almindelige e-mails.

Fordeling af Digital Post

Meddelelser fra Virk.dk videresendt til jeres mailsystem indeholder metadata, som kan benyttes til automatisk at fordele meddelelserne til relevante modtagere.

Denne fordeling sker gennem regler og kan opsættes som I ønsker det. I kan videresende en kopi eller en original til en eller flere modtagere, flytte meddelelsen til bestemte foldere, sende den til print eller andet.

Fordeling på baggrund af metadata

En regel opbygges af en "identifikator" og en – eller flere – "handling".

- Identifikator er den relevante tekst i mailheader og starter altid med "X-DPI" og derefter det relevante søgeparameter.
- Handlingen er typisk videresendelse til en eller flere modtagere, men kan også være andre mere avancerede handlinger, herunder print, køre et specifikt script eller andet.

I enhver videresendt meddelelse fra Virk.dk, er de relevante og brugbare metadata angivet i e-mailens header informationer. De starter alle med "X-DPI" og derefter dette relevante felt-navn og felt-værdi. Mailheader kan ses i de fleste mailklienter ved at vise mailens kildekode.

Dette kunne eksempelvis være p-nummer, der angives således:

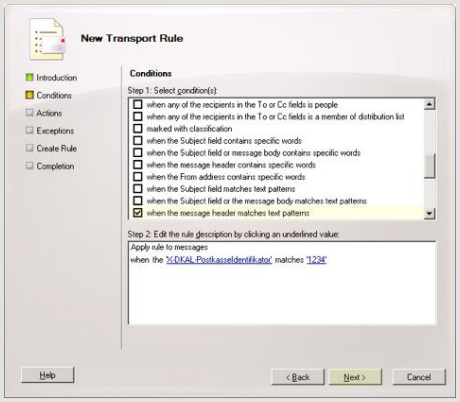
"X-DPI-PNUMMER-1003290274" – dette er betegnelsen for en bestemt skole i en kommune.

CVR nummeret angiver kommunen og det angivne p-nummer refererer til en bestemt skole i kommunen (som hører under dette CVR nummer).

Det er muligt at foretage opsætningen enten gennem Exchange eller direkte på Outlook klienten.

Exchange 2010 opsætning

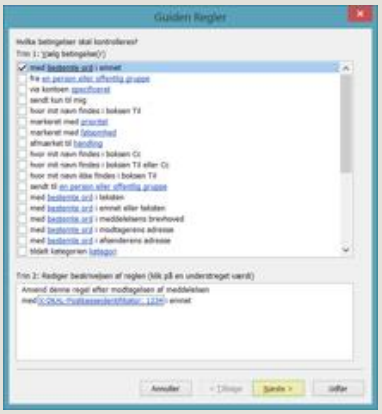
Hvis I opsætter regler på jeres Exchange server, bliver de indkomne e-mails fordelt ved ankomst til jeres mailserver. I skal oprette en "Transport Rule" i jeres Exchangeservers "Exchange Management Console".



1. Åbn "Exchange Management Console".
2. Udvid "Organization Configuration".
3. Kilk på "Hub Transport".
4. Kilk på "Transport Rules" tab.
5. Kilk på "New Transport Rule".

Outlook 2010 opsætning

Hvis I opsætter regler på en Outlook klient, bliver de indkomne e-mails i de fleste tilfælde først fordelt ved ankomst til klienten. Her vises opsætning i Outlook 2010, men opsætning i andre versioner af Outlook ligner dette. Opsætning i andre mailklienter er også muligt - men ikke beskrevet i denne manual.



1. I Outlooks vælges "Regler" fra topmenuen og "Opret regel".
2. Næste vindue vælges der "Avancerede Indstillinger".
3. Vælg "med Bestemte ord i emnet".
4. Udfyld headeren som skal identificere mailen og klik "Tilføj".
5. Klik "OK" når headeren er tilføjet.
6. Vælg "Videresend den til en person eller offentlig gruppe" og klik "Næste".
7. Navngiv reglen og aktivér den.

Oversigt over kendte metadata

Videresendte meddelelser fra den digitale postkasse på Virk.dk kan indeholde en række metadata bl.a. "Kanaldata", "Sagsdokumentdata" eller "Attentiondata".

Den afsendende myndighed kan medsende:

Kanaldata, der indeholder oplysninger om selve forsendelsen og hvordan den er fremsendt. Disse oplysninger fortæller om meddelelsens navn, hvor meddelelsen skal sendes hen, og typisk hvilken returpostkasse der kan besvares til.

Sagsdokumentdata, der indeholder oplysninger om den eller de sager, som meddelelsen vedrører samt metadata om de dokumenter (hoveddokument og bilag), der er med i meddelelsen.

Attentiondata, der indeholder de oplysninger, der erstatter att.-feltet fra fysisk post. Det kan fx. Være reference til virksomhedens produktionsenheder (p-nummer), organisatoriske enheder, personer m.v.

Bemærk, at det er op til den afsendende myndighed at vurdere, om og i hvilket omfang den vælger at benytte metadata.

Besvarelse af henvendelse videresendt fra Virk.dk

Med SikkerMail kan I også besvare og sende e-mails sikkert og krypteret til det offentlige. Det vil sige, at I kan besvare henvendelser videresendt fra Virk.dk direkte til den relevante offentlige afsender.

Bemærk, at I ikke skal vælge "besvar" i e-mailklienten, men "Videresend" og manuelt adressere den til myndighedens sikre postkasse. Adressen til myndighedens sikre postkasse findes i e-mailen og/eller på myndighedens hjemmeside.

OFTE STILLEDE SPØRGSMÅL

Hvad er kryptering og dekryptering?

Kryptering er en teknik, der anvendes for at hemmeligholde information, der kan opsnappes af uvedkommende.

Kryptering refererer til den proces, der omdanner den oprindelige information til information, der er ulæselig for uvedkommende. Dekryptering refererer til den modsatte proces. Begge processer gør brug af krypteringsalgoritmer og krypteringsnøgler.

Hvad er TLS, Transport Layer Security?

Transport Layer Security (TLS) er en protokol, der krypterer e-mailforbindelsen og dermed forhindrer aflytning mellem mailservere. Comendo sender og modtager beskeder til ind- og udgående mailservere ved hjælp af TLS.

Alle e-mails og vedhæftede filer sendes via en krypteret forbindelse for at sikre fuldstændig fortrolighed. TLS forudsætter kun installation af gyldigt SSL-certifikat. Der skal ikke bruges andet hardware eller software og brugernes adfærd behøver ikke ændres.

Hvad er en digital signatur?

Populært sagt er en digital signatur en elektronisk udgave af ens personlige underskrift. Teknisk set er der tale om en beregnet værdi, som fremkommer ved at kombinere data med ens private nøgle.

Måden den digitale signatur er konstrueret på gør, at den kan bruges til at sikre autenticitet og integritet – dvs. modtager af data, der er påhæftet en digital signatur, kan anvende den digitale signatur til at overbevise sig om afsenders og datas ægthed.

Hvad er en sikker mail?

Ved begrebet en sikker mail forstås en mail, hvis indhold er krypteret og/eller digitalt signeret, og som sendes til og fra sikre postkasser.

Hvad er en funktionspostkasse / sikker postkasse?

Ved begrebet en sikker postkasse forstås en mail-adresse med tilhørende certifikat og krypteringsnøgler. Et typisk eksempel på en sikker postkasse kunne være mailadressen SikkerMail@comendo.com – dvs. en fælles-postkasse hørende til en afdeling, hvortil der er blevet udstedt et certifikat.

Hvem kan man sende sikre e-mails til?

En mail der kun er digitalt signeret (dvs. ikke krypteret) kan læses af alle, så den kan sendes til alle. En mail der er krypteret kan kun læses af den modtager, hvis nøgle er blevet anvendt til at kryptere mailen med. Det er således kun muligt at sende krypterede mails til modtagere, der har en krypteringsnøgle. I Danmark kan man finde og hente modtagerens krypteringsnøgle på certifikat.dk.

Hvad er et virksomhedscertifikat / OCES?

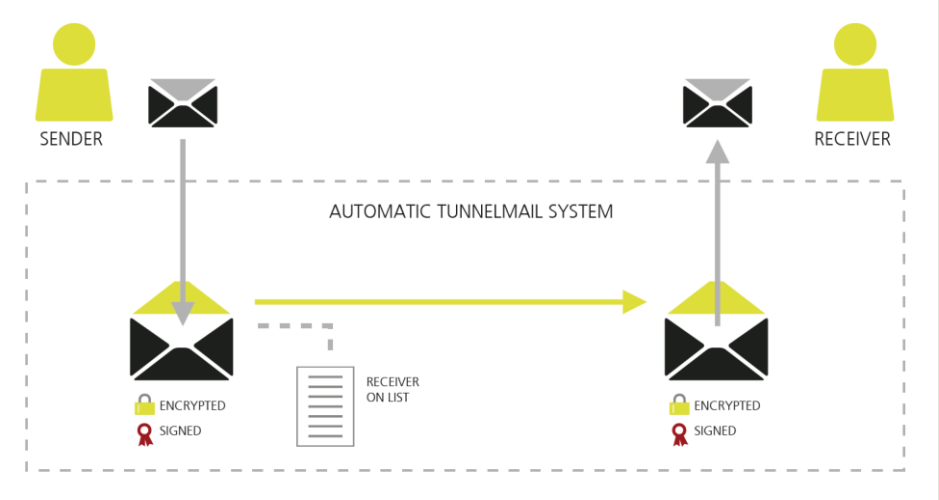
Ministeriet for Videnskab, Teknologi og Udvikling har udarbejdet en fælles offentlig standard for certifikater kaldet OCES, Offentlige Certifikater til Elektronisk Service. OCES er udarbejdet for at skabe en type certifikater, der er lettere og hurtigere at udbrede end de kvalificerede certifikater. Samtidig er hensigten at undgå, at mange konkurrerende standarder skaber samspilsproblemer for brugerne og for de offentlige systemer (kilde: digitalsignatur.dk).

Hvad er Tunnelmail?

Begrebet Tunnelmail beskriver det forhold, at alle mails mellem to eller flere domæner automatisk bliver sendt som sikre mails.

Tunnelmail kræver, at domænerne hver især har et certifikat og et nøglepar, der kan anvendes til formålet samt en sikker mail løsning der understøtter Tunnelmail (det gør Comendos SikkerMail løsninger). I Tunnelmail anvendes afsenders og modtagers sikre postkasser kun som mellemstationer, der henholdsvis krypterer og dekrypterer en mail inden mailen afleveres til den endelige modtager.

Comendo's SikkerMail løsninger understøtter Tunnelmail, og det gør visse andre leverandørers SikkerMail løsning også.



Kan vi stadig bruge de gamle styrekoder fra en tidligere krypteringsløsning?

Der er tilsvarende "styrekoder" i Comendo SikkerMail. Disse er logisk og nemme at anvende, eksempelvis er #K kryptering og #S signering. Det fremgår tydeligt af manualen hvilke styrekoder der skal anvendes hvornår og hvordan. Det er vigtigt at bruge de nye styrekoder, da Comendo SikkerMail ikke forstår de gamle styrekoder.

Kan vi stadigvæk bruge styrekoder for at fortælle hvilken funktionspostkasse som skal være afsender?

Ja, man kan anvende styrekoder til at fastslå hvilke handlinger og hvilket certifikat der skal anvendes. Eksempelvis vil '#S-xxx#' signere mails, '#K-xxx#' til at kryptere mails fra xx@xxx.dk. Bemærk at det ikke er nødvendigt at anvende styrekoder i forbindelse med brugen af funktionspostkasser. Dette sker automatisk med Comendo SikkerMail.

Hvordan sendes sikkert fra en funktionspostkasse?

Det er ikke er nødvendigt at anvende styrekoder i forbindelse med brugen af funktionspostkasser. Dette sker automatisk med Comendo SikkerMail.

Systemet genkender afsender som en postkasse med tilknyttet digitalt certifikat og krypterer automatisk. Dette sker automatisk og kræver ingen handling fra afsender.

Hvad sker der når man bruger 'Send sikkert' knappen?

SendSikker knappen i Outlook, giver brugeren mulighed for at sende en krypteret og signeret mail fra de funktionspostkasser brugeren har adgang til i AD'et. Dvs. at før brugeren trykker på 'Send Sikker' vælger de funktionspostkassen de vil afsende fra.

Er der support på SikkerMail fra Comendo?

Comendo Support er inkluderet for vores kunder og har telefonnummer (+45) 43 330 393.

Uden for almindelig åbningstid kan driftvagten kontaktes på telefonnummer (+45) 70 25 22 23.

Comendos Partnere kender også disse kontaktinformationer.

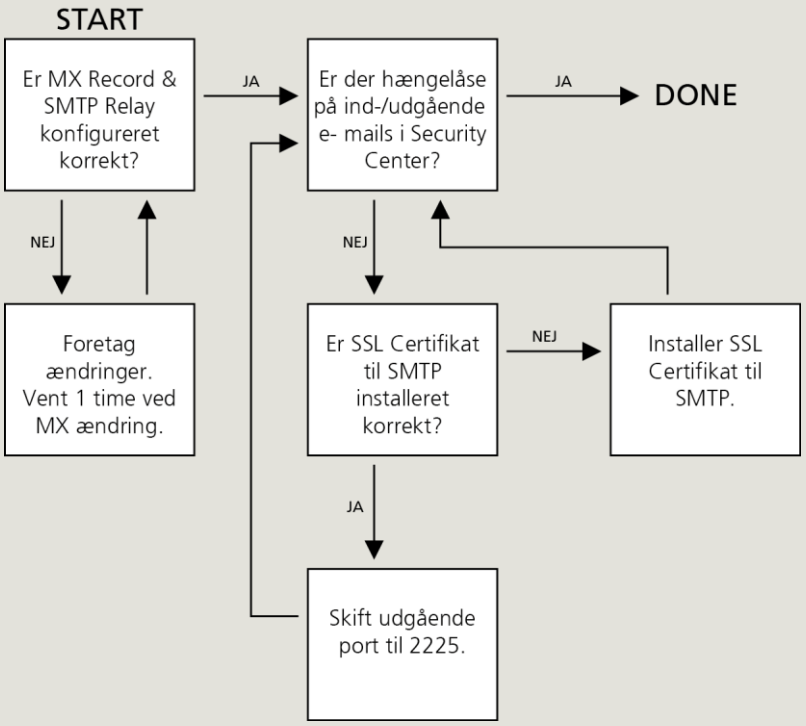
BILAG 1

MX Records, SMTP Relay og TLS

Det er en forudsætning for SikkerMail at der er konfigureret korrekte MX records og SMTP relay – samt opsat kryptering i form af Transport Layer Security (TLS). Nedenstående guide hjælper dig med at konfigurere MX records, SMTP relay, samt konfigurere og installere SSL certifikat til brug for TLS.

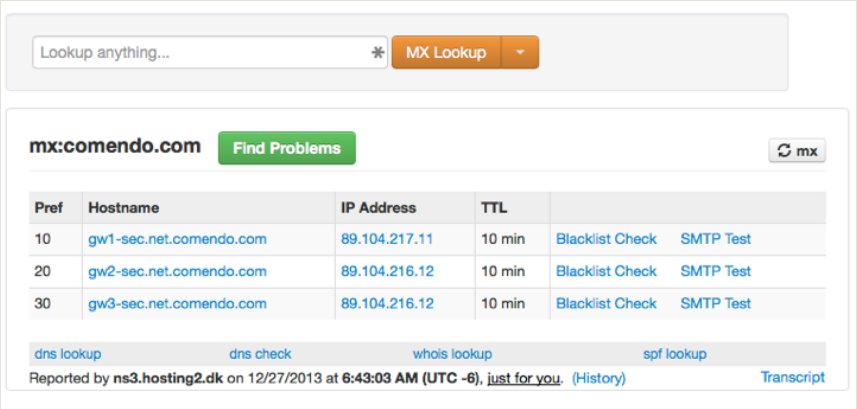
For at oprette en Transport Layer Security forbindelse til Comendo kræves et SSL-certifikat. Certifikatet skal være X509 og udstedt af en anerkendt Certificate Authority (Public CA). Certifikater kan købes direkte hos en anerkendt Certificate Authority (CA) eller fra en autoriseret certifikatforhandler.
TLS skal aktiveres i jeres mailserver og knyttes til et SSL certifikat.

Følg nedenstående diagram for at verificere korrekt opsætning. Der er yderligere forklaring til hvert enkelt punkt senere i teksten.



MX-Record

Benyt hjemmesiden http://www.mxtoolbox.com til at verificere din MX-record.



SMTP Relay

På din mailserver skal du konfigurere/verificere om du benytter vores server til at sende igennem. Du skal benytte:

- smtprelay-sec.net.comendo.com

På en Microsoft Exchange konfigureres dette i f.eks Exchange Management Console.

Hængelåse på ind/udgående mailflow i Security Center.

For at se om TLS virker skal det sådan ud i Security Center under "mailFence/spamFence > Gennemse e-mails":

Indgående mails

- Guldlås betyder, at mailen var TLS-krypteret ved aflevering til Comendo.
- Sølvlås betyder, at mailen blev leveret TLS-krypteret fra Comendo til den eksterne modtager.
- Er begge lås-ikoner på, betyder det, at mailen var krypteret fra afsenderen og frem til modtageren.

Udgående Mails

- Guldlås betyder, at mailen var TLS-krypteret ved aflevering til Comendo.
- Sølvlås betyder, at mailen blev leveret fra Comendo til den eksterne modtager TLS-krypteret.
- Er begge lås-ikoner på, betyder det, at mailen var krypteret fra afsenderen og frem til modtagere

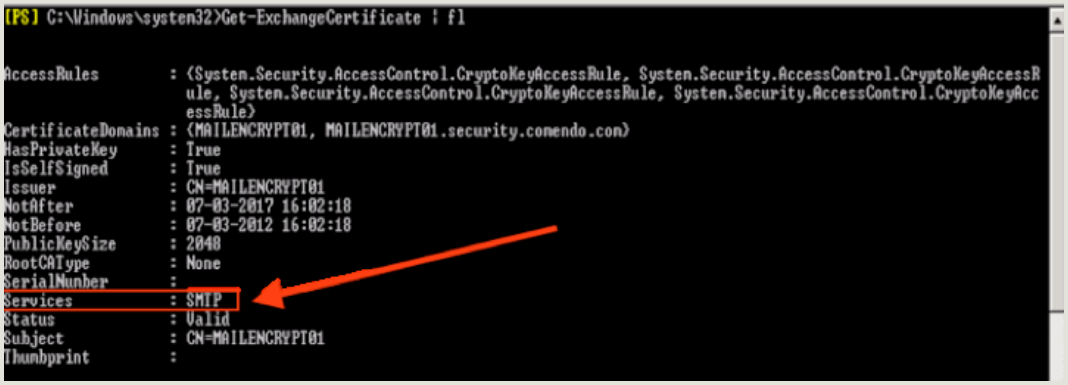
Er SSL Certifikat installeret?

Forudsætningen for at TLS virker er, at der er tilknyttet et SSL certifikat til SMTP servicen på Exchange serveren.

Sådan tjekkes der om et certifkat er installeret og på hvilke services.

1. Åben Exchange Management Shell (EMS)
2. Skriv følgende kommando:

   Get-exchangeCertificate | fl



Skift udgående port til 2225

5. Start Exchange Management Shell (EMS).
6. Skriv følgende kommando for at få navnet (Identity) på din SendConnector:

   Get-SendConnector

7. Skriv følgende kommando for at skifte til port 2225:

   Set-SendConnector –Id "Navnet på din SendConnector (Identity)" -Port 2225

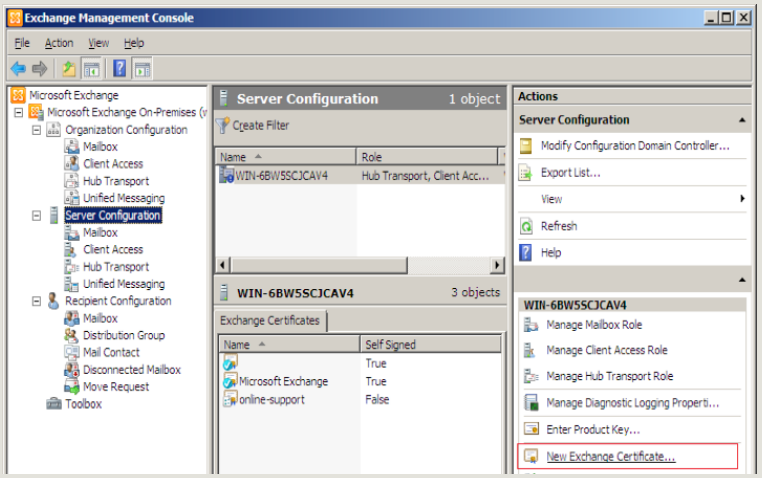
Anskaffelse og installation af certifikat

For at konfigurere TLS på din exchange server, skal du bruge et SSL certifikat. Du kan her læse hvorledes du anskaffer et certifikat fra en CA (Certificate Authority) og installerer dette på din Exchange server. Hvis du allerede har et certifikat til rådighed, kan du hoppe ned til punktet "Install certificate" og køre opsætningen derfra.

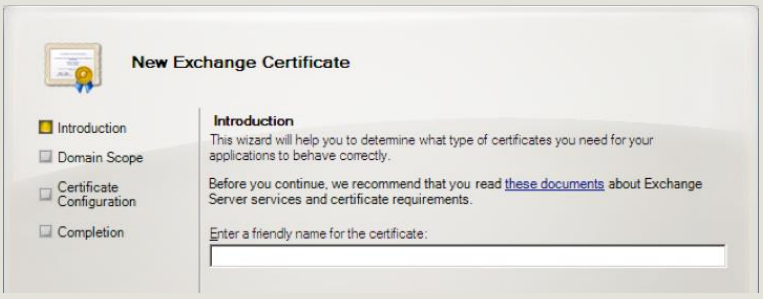
Bemærk at nedenstående guide er på engelsk og tager udgangspunkt i Exchange 2010.

Creating a certificate request with Exchange 2010

1. Start the Exchange Management Console by going to Start > Programs > Microsoft Exchange 2010 > Exchange Management Console.



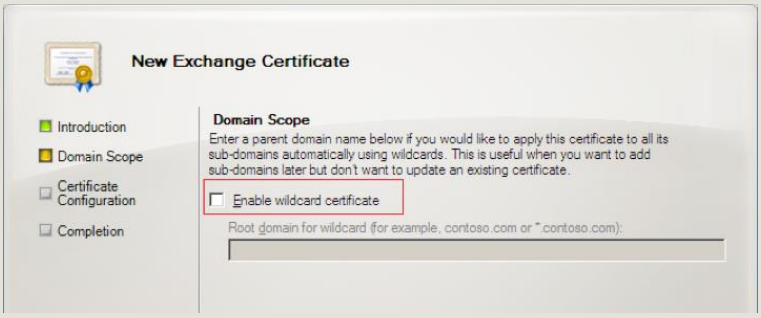
2. Select Server Configuration in the menu on the left and then New Exchange Certificate from the actions menu on the right.



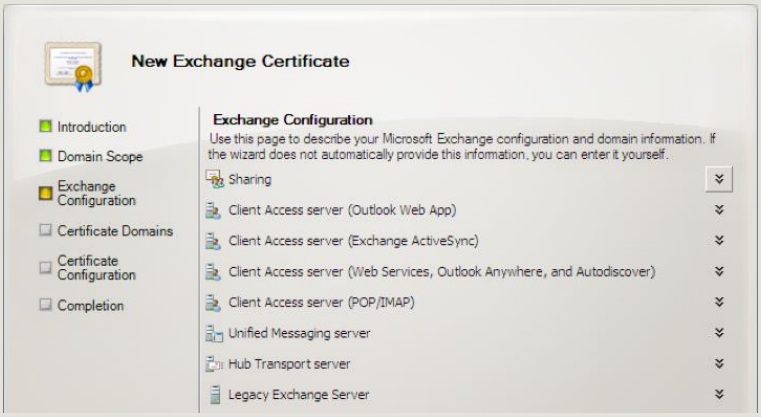
3. When prompted for a friendly name, use a name of your own choice. The name will not affect your request.

4. Under Domain Scope, you can check the box if you will be generating the CSR for a wildcard. Otherwise, just go to the next screen.

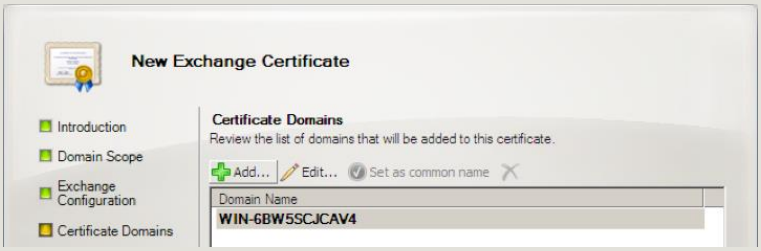
   Note: If you do select that box for a wildcard, skip to step 7.



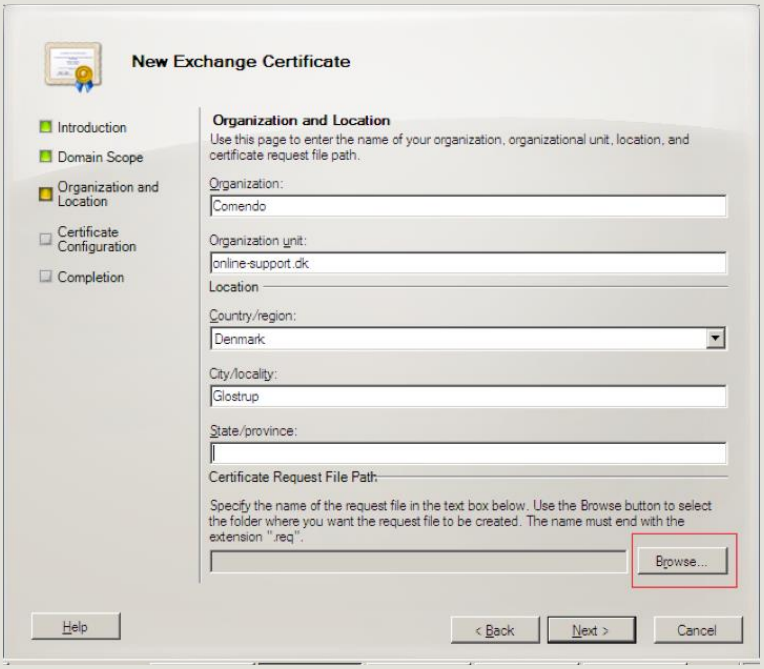
5. In the Exchange Configuration menu, select the services, which you plan to run securely. In this case Hub Transport server / SMTP.



6. You will be able to review a list of the domain names, which Exchange 2010 suggests you include in your certificate request. We recommend that your domain name should be one of them.

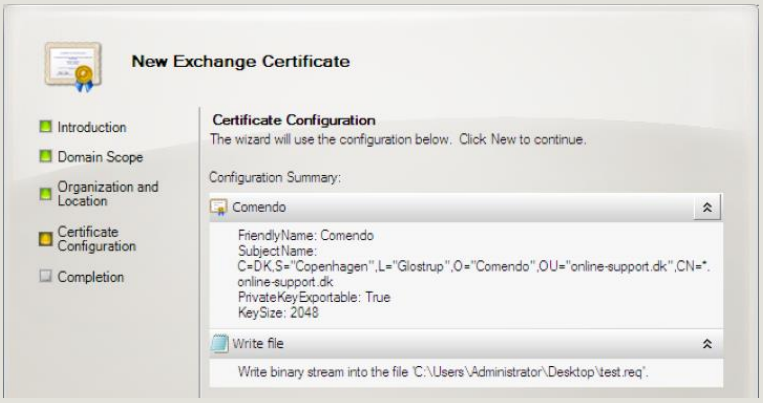


7. Your Organization should be the full legal name of your company. If you do not have a State/Province, enter the city information again.

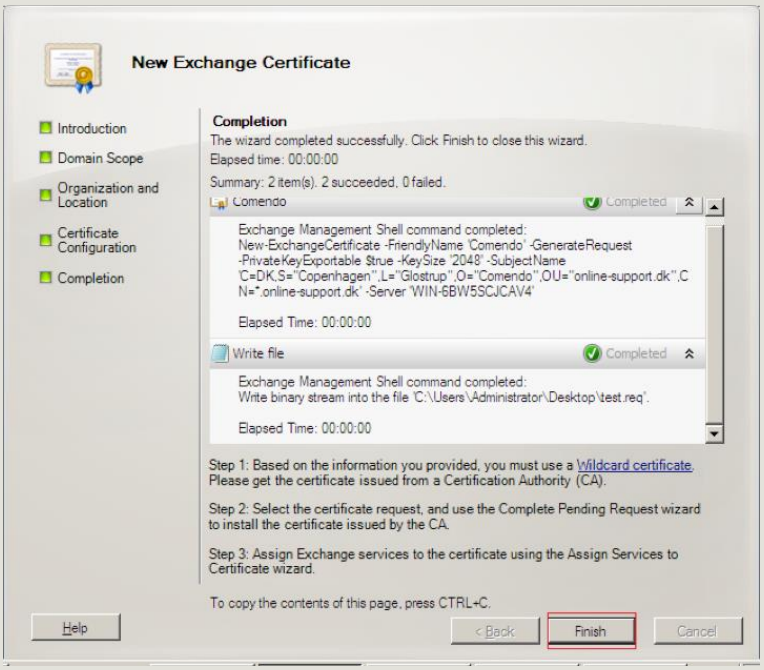


8. Click Browse to save the CSR to your computer as a .req file

9. Review the information, and continue by clicking 'New'.



10. Finally click Finish to create the CSR.



11. Your request is now finalized. To complete the request, and in order to get your certificate mailed, you need to send the .CSR (the request) file to your certificate supplier.

Install certificate

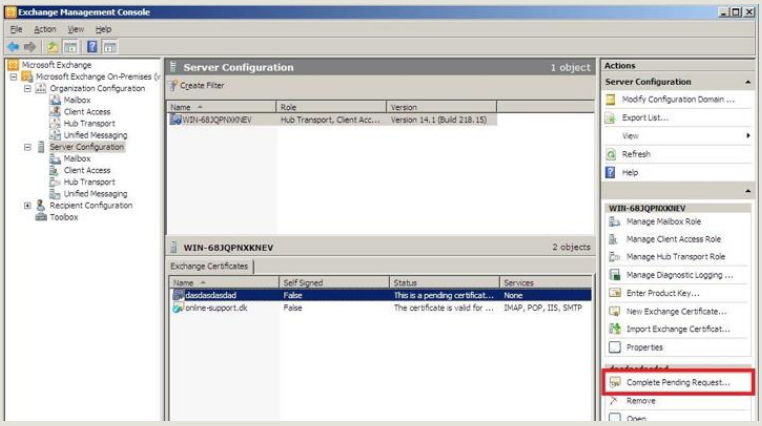
5. Download and open the ZIP file containing your certificate. Your certificate file will most likely be named "your_domain_name.cer"

6. Copy the "your_domain_name.cer" file to your Exchange server.

7. Start the Exchange Management Console by going to "Start > Programs > Microsoft Exchange 2010 > Exchange Management Console".

8. Click the link to "Manage Databases", and then go to "Server configuration".

9. Select your certificate from the menu in the center of the screen (listed by its Friendly Name), and then click the link in the Actions menu to "Complete Pending Request".

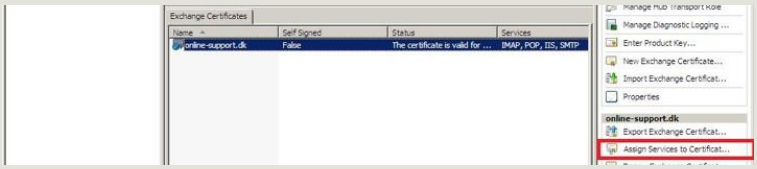


10. Browse to your certificate file, then click Open > Complete.

    Frequently Exchange 2010 will show an error message stating that "The source data is corrupted or not properly Base64 encoded." Ignore that error.

    Hit F5 to refresh the certificate and verify that it now says "False" under "Self Signed". If it still shows "True", you may have selected the wrong certificate or you may have generated the request on a different server.

11. Now, to enable your certificate for use, go back to the Exchange Management Console and click the link to "Assign Services to Certificate."



12. Select your server from the list provided, then click Next.

13. Select the services for which you would like to enable your new certificate, click "Next > Assign > Finish".

Your certificate should now be installed and enabled for use with Exchange.

To use TLS on incoming mails you have to change the authentication settings from the "Server Configuration - Hub Transport – Receive Connectors – ClientName – Right click and choose Properties - Authentication" menu.

For the use of TLS on outgoing mails you have to route your mails through our relay. This can be done by going in to:

"Organization Configuration – Hub Transport – Send Connectors". Right click on your domain and choose Properties and then Network – " Route mail through the following smart host: smtprelay-sec.net.comendo.com

As the final step you must execute the following line in your command shell to force TLS

- Set-SendConnector – Identity "SendConnectorName" –RequireTLS:$true

You should now be able to receive and send mails through Comendo MailTunnel.
If you have any trouble installing this or have other questions, feel free to contact us either on mail or by phone.

BILAG 2

Krypteret og signeret e-mail manuelt ved brug af syntaks

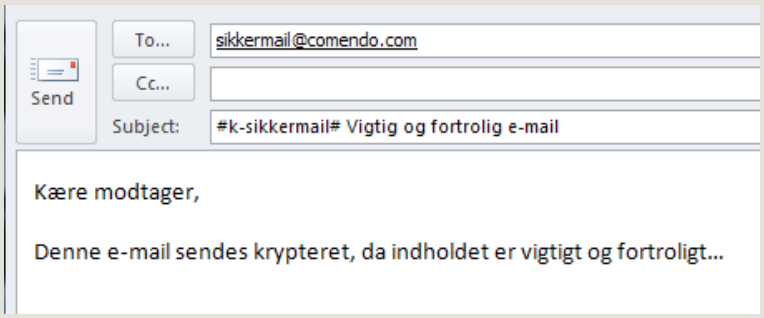
Bemærk at kryptering og signering ved brug af syntaks også kan gøres ved brug af Outlook add-in, se andetsteds i dette dokument.

Ved såvel en ny meddelelse som besvarelse af en modtaget meddelelse som ønskes fremsendt digital signeret og krypteret kan en af følgende 'koder' angives i meddelelsens emne-felt:

#k = signer og krypter
#s = signer

Syntax = #k-[ID]#"Vedr. henvendelse…."

[ID] = navn på funktionspostkasse, defineres i databasen.



Den normale tekst i emnefeltet anføres efter 'koden'. Når meddelelsen når frem til modtageren vil 'koden' være fjernet og kun den normale tekst fremgår af emnefeltet.

Anvendelse af 'koden' medfører, at meddelelsen bliver signeret og krypteret med det angivne certifikat. Det betyder også, at meddelelsen hos modtageren vil fremstå som afsendt fra den sikre postkasse og ikke medarbejderen, og at meddelelsen er sendt med signatur.

Det forhold, at meddelelsen fremstår som afsendt fra den sikre postkasse betyder også, at automatiske kvitteringer og besvarelser fra modtageren vil blive sendt til den sikre postkasse og ikke til medarbejderen.

SikkerMail kan dog sættes op således at medarbejderne får en kvittering ved afsendelse af sikker post. Anvendelse af Til, Cc og Bcc felter Man kan anvende SikkerMail systemet til at sende sikkerpost både ved anvendelse af "Til", "Cc" og "Bcc" felterne i dit e-mailsystem. Systemet virker på samme måde som ved afsendelse af almindelig e-mail, på tilsvarende måde som dit postsystem virker i dag.

Når man sender Cc, kan den egentlige modtager se, hvem der yderligere har modtaget e-mailen.
Cc bruges normalt til orientering. Ved anvendelse af Bcc kan den egentlige modtager ikke se, at e-mailen er sendt til andre.

Gældende regler for videregivelse af personoplysninger skal overholdes såvel ved fremsendelse Cc og Bcc som ved angivelse af flere e-mailadresser i til-feltet.

Afsendelse af krypteret og signeret e-mail

- #K-funktionspostkassenavn#

Eksempel:
Emne: #K-advokatkontoret# herefter indtastes det relevante emnefelt i den pågældende mail.

Afsendelse af signeret e-mail

- #S-funktionspostkassenavn#

Eksempel:
Emne: #S-advokatkontoret# herefter indtastes det relevante emnefelt i den pågældende e-mail.

I begge tilfælde vil syntaksen '#S-advokatkontoret#' ikke være synlig for modtageren.

BILAG 3

Outlook add-in for administrator

Afhængigheder

.Net Framework 4.0 (http://www.microsoft.com/en-us/download/details.aspx?id=17851)
Office 2003/2013 32 bit / 64 bit
Ovenstående skal forefindes på klienternes maskiner før Add-in'et virker. Ved en lokal installation klarer Setup.exe automatisk installation af disse, ved Group Policy Object (GPO) udrulling er det administratoren selv der må sikre sig at de eksisterer hos brugeren.

Lokal konfigurationsfil i stedet for AD indstillinger

Hvis man ikke laver en GPO udrulning har man under installationen mulighed for at skabe en lokal konfigurationsfil. Denne kræver at man importerer en kundespecifik funktionspostkasse-konfigurationsfil, som leveres af Comendo. Filen deles af samtlige brugere på maskinen og placeres i '<All users>/PROGRAMDATA' mappen i en undermappe kaldet SikkerMail. På eksempelvis Windows7 giver det følgende placering:

C:\ProgramData\SikkerMail\SikkerMail.config

OBS. Under Windows XP placeres filen under:

C:\Documents and Settings\All Users\Application Data\SikkerMail

Hvor er de enkelte config filer placeret

<All users>/programdata/SikkerMail:
SikkerMail.config. Config fil som bruges hvis denne enkelte bruger ikke har en lokal config fil.

<current user>/Appdata/Roaming/SikkerMail:
SikkerMail.config. Den aktuelle brugers lokale config fil.

Logfiler og fejlfinding

De fejl som brugeren kan reagere på vises på skærmen i form af en 'Pop up' besked. Alle andre fejl bliver i stedet logget per bruger. Logfilerne kan findes ved at indtaste følgende i Explorer:
%appdata%/SikkerMail/Logs

Konfigurationsfil format

Dette format gælder både for den kundespecifikke funktionspostkasse-konfigurationsfil og den lokale konfigurationsfil.

```
<?xml version="1.0" encoding="utf-8"?>
<SikkerMail>
	<AdvancedView>false</AdvancedView>
	<SendTlsAsSecure>false</SendTlsAsSecure>
	<DefaultSendAlwaysAsSecure>false</DefaultSendAlwaysAsSecure>
	<ForcedSendSecure>false</ForcedSendSecure>
	<UseSafePortal>false</ UseSafePortal >
	<SafePortalAskMe>false</SafePortalAskMe>
	<AlwaysRemoveUnsecureRecipients>false</AlwaysRemoveUnsecureRecipients>
	<CertificateMailBoxes>
		<postbox Name="Postkasse1_Navn" CertAlias="Postkasse1_Alias" />
		<postbox Name="Postkasse2_Navn" CertAlias="Postkasse2_Alias" />
		<postbox Name="Postkasse3_Navn" CertAlias="Postkasse3_Alias" />
	</CertificateMailBoxes>
	<ProxyServer>http://[proxyadresse]</ProxyServer>
	<EboksEmailAddress>indgaande@e-boks.dk</EboksEmailAddress>
</SikkerMail>
```

Nedenstående felter findes kun i den lokale konfigurationsfil. Den lokale konfigurationsfil fra én maskine kan bruges til installation på andre maskiner, skulle det blive nødvendig.

Lokale felter:

'AdvanedView' - Skal brugeren have mulighed for at aktivere Avanceret visning (Viser alle modtager typer)

'SendTlsAsSecure' - Skal modtagere der understøtter TLS betragtes som sikre modtagere.

'DefaultSendAlwaysAsSecure' - Marker "Send Sikkert" som standard. Bemærk at denne attribut har ændret navn fra 'SendAlwaysAsSecure' til 'DefaultSendAlwaysAsSecure'.

'ForcedSendSecure' - Lås indstilling for "Send Sikkert".

'AlwaysRemoveUnsecureRecipients' - Fjern automatisk usikre modtager fra e-mail der sendes.

'ProxyServer' - Proxy server adresse der skal anvendes til integration med e-Boks. (Angives af Comendo)

'EboksEmailAddress' - E-mail adresse der skal anvendes for at sende e-boks meddelser.

'UseSafePortal' - Anvend SafePortal hvis det er tilkøbt som produkt hos Comendo.

'SafePortalAskMe' - Skal brugeren spørges før afsendelse af e-mail via SafePortal.

'MultipleEboksAccounts' – Har brugeren adgang til mere end én e-boks konto (Afsendersystem).

<CertificateMailBoxes>
'Name' er den tekst der vises i Addin'et funktionskasse dropdown, mens 'CertAlias' er det ID som vores system identificerer funktionspostkassen på. Således kan 'Name' tilrettes af kunden uden det påvirker funktionaliteten.

Filen kan også indeholde e-boks konfigurationsdata. Disse data kan findes på e-Boks's Administrationsportal.

```
<EBoksData>
        <Kunde>
                <KundeNr>123456</KundeNr>
                <Register>
                        <ID>1337</ID>
                        <Navn>Comendo Register</Navn>
                </Register>
                <AfsenderSystem>
                        <ID>2034</ID>
                        <Navn>Digital post</Navn>
                        <Materiale>
                                <ID>162771</ID>
                                <Navn>Information</Navn>
                        </Materiale>
                </AfsenderSystem>
                <AfhentningsSystem>
                        <ID>2039</ID>
                        <Navn>Digital post</Navn>
                        <Postkasse>
                        <ID>4897</ID>
                        Navn>Digital postkasse</Navn>
                        <Emne>
                                <ID>11008</ID>
                                <Navn>Digital postkasse emne</Navn>
                        </Emne>
                </AfhentningsSystem>
        </Kunde>
```

Lokale felter:
'Kundenr' – Firmaets kundenr. hos e-Boks.
'Register' – ID og navn. Bruges til at hente informationer om indtastede CVR / CPR nr.
'Afsendersystem' – ID og navn. System der skal afsende meddelelsen i e-boks.
'Materiale' – ID og navn. Enmetekst som vises i e-boks meddelelsen til virksomheden / borgeren.
'AfhentningsSystem' – ID og navn. System der skal modtage et evt. svar fra virksomheden / borgeren.
'Postkasser' – ID og navn. Postkasse som svar placeres i.
'Emne' – ID og navn Emne som svar placeres i.

Såfremt filen skal editeres, anbefales det at anvende Notepad eller lign. og ikke et tekstbehandlings-program som Microsoft Word.

Active Directory indstillinger

I stedet for at anvende en lokal konfigurationsfil kan man i stedet placere de relevante indstillinger i virksomhedens Active Directory (AD). Det giver en række fordele:

- Add-in'et kan udrulles centralt fra i stedet for en lokal manuel installation.
- Indstillingerne kan specificeres per bruger i stedet for per maskine.
- Indstillingerne kan samles både på brugere og/eller grupper i AD'et.

Funktionspostkasse indstillingerne bliver lagt sammen således at postkasser defineret direkte på brugeren og postkasser defineret på en eller flere af de grupper som brugeren er tilknyttet, alle præsenteres for brugeren i Add-in'et.

Måden man tilføjer indstillingerne på brugeren eller gruppen er ved at indtaste en specielt formateret streng i en vilkårlig 'Attribute'.

Formatet på attributtens indhold er følgende:

En attribut streng SKAL altid starte med ##B2SPIRIT#:
Herefter tilføjes #KODE#VÆRDI

Postkasserne har Kode #187#,
##B2SPIRIT#:#187#Postkasse1_Alias;Postkasse1_ Navn,Postkasse2_ Alias;Postkasse2_Navn

Herefter kan der tilføjes flere koder med en TRUE/FALSE værdi.
F.eks ved aktivering af Avanceret visning som har Kode #208#,
##B2SPIRIT#:#187#Postkasse1_Alias;Postkasse1_ Navn,Postkasse2_ Alias;Postkasse2_Navn#208#TRUE

Værdier relateret til e-Boks opsætningen SKAL alle placeres på hver sin linje (#200#kundeNr; – #206#KundeNr).

Følgende attributter må IKKE undlades i AD opsætningen:

#187#, #208#, #209#, #211#, #212#, #213#, #214#, #215#

Eventuelle '#','' og ';' i data escapes med et \.

De relevante værdier af 'PostkasseX_Navn' og 'PostkasseX_Alias' tages fra den kundespecifikke funktionspostkasse-konfigurationsfil som Comendo har leveret.
Se vejledning for Opsætning af Active Directory (Group Policy) senere i dokumentet.

Eksempel på AD indstillinger

Beskrivelse af koder.

"187" SIKKERMAIL Mailboxes.
"200" E-BOKS Kundenr.
"201" E-BOKS Afsendersystem.
"202" E-BOKS Materiale.
"203" E-BOKS Afhentningssystem.
"204" E-BOKS Postkasse.
"205" E-BOKS Emne.
"206" E-BOKS Register.
"216" E-BOKS Har bruger adgang til flere e-boks afs. systemer

"207" SIKKERMAIL ProxyServer.
"208" SIKKERMAIL Advanced view
"209" SIKKERMAIL Send TLS as secure
"210" SIKKERMAIL E-Boks e-mail
"211" SIKKERMAIL Send always as secure
"212" SIKKERMAIL Always remove unsecure recipients when sending secure
"213" SIKKERMAIL Force 'Send always as secure'

"214" SAFEPORTAL Anvend SafePortal hvis tilgængelig
"215" SAFEPORTAL Spørg bruger før afsendelse via af SafePortal

OBS. **#187# skal angives i konfigurationen.**
#208# - #216# kan angives i én linje. ##B2SPIRIT#:#208#False#209#True#214#true
…

Eksempel:

##B2SPIRIT#:#187#OKONOMI;ADØkonomi,PERSONALE;ADPersonaleadminstration,LOEN;ADLønadmin
stration
##B2SPIRIT#:#200#KundeNr;15710
##B2SPIRIT#:#206#KundeNr;15710,RegisterID;2056,Navn;Comendo Register
##B2SPIRIT#:#201#KundeNr;15710,AfsenderSystemID;2034,Navn;Comendo Afsendersystem
##B2SPIRIT#:#202#KundeNr;15710,AfsenderSystemID;2034,MaterialeID;162771,Navn;Test materiale
##B2SPIRIT#:#203#KundeNr;15710,AfhentningsSystemID;2039,Navn;Comendo Afhentnings System
##B2SPIRIT#:#204#KundeNr;15710,AfhentningsSystemID;2039,PostkasseID;4897,Navn;Comendo
postkasse 1
##B2SPIRIT#:#205#KundeNr;15710,AfhentningsSystemID;2039,PostkasseID;4897,EmneID;11008,
EmneNavn;Standard
##B2SPIRIT#:#207#https://c723ced9a73628e8608205447420d22x.webapi01.comendosystems.com
##B2SPIRIT#:#208#False
##B2SPIRIT#:#209#True
##B2SPIRIT#:#210#indgaaende@prod.e-boks.dk
##B2SPIRIT#:#211#False
##B2SPIRIT#:#212#False
##B2SPIRIT#:#213#False
##B2SPIRIT#:#214#False
##B2SPIRIT#:#215#False

Group Policy (GPO) opsætning og udrulning

Skal SikkerMail installeres på et større antal maskiner i virksomheden anbefales det at anvende sig af Group Policy (GPO).

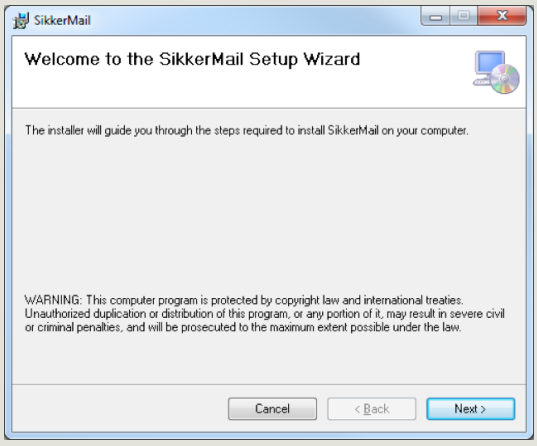
GPO installationsfilen af SikkerMail finder selv ud af om det er en 32 bit eller 64 bit version der skal installeres på den enkelte maskine.

Se vejledning for Generel opsætning af Group Policy senere i dokumentet.

Lokal installation af SikkerMail add-in

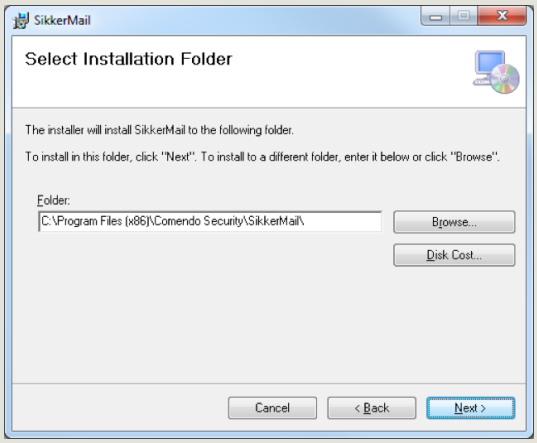
Uanset hvilket Outlook version man har 2003-2013 er det den samme installationsfil der skal anvendes.

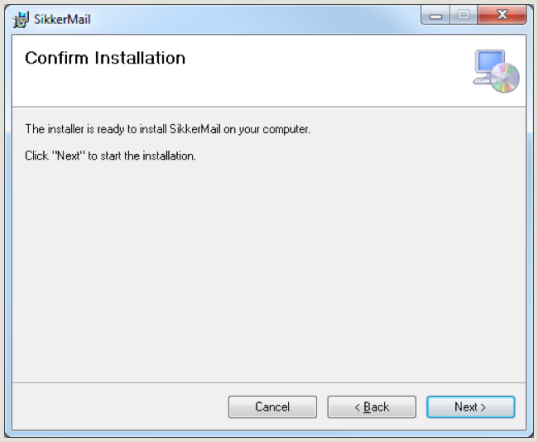
Det er filen Setup.exe der skal køres og *ikke* .msi filen.

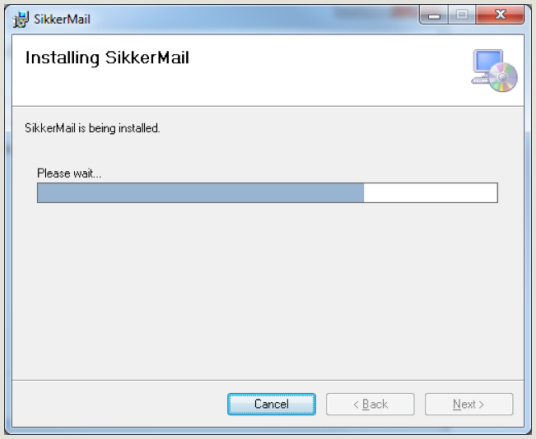


Følgende skal udføres på dette skærmbillede:

- Angiv hvor SikkerMail skal installeres. Det anbefales at vælge den foreslåede placering.





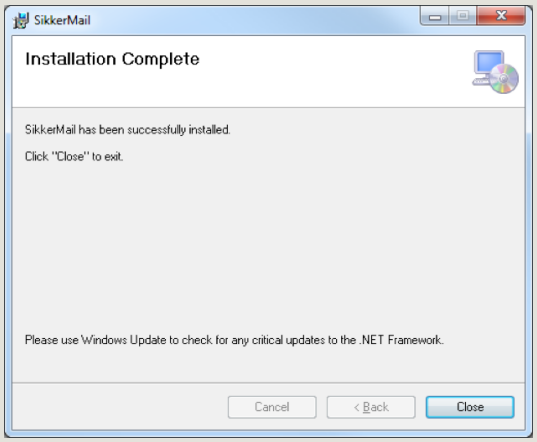


Skal indstillinger indlæses via Active Directory trykkes der på knappen Ingen lokal indstilling i nedenstående skærmbillede, men det kræver så at Active Directory sættes op ifølge vejledningen Opsætning af Active Directory senere i dokumentet.

Alternativt oprettes der en lokal konfigurations fil ved at gøre følgende:

- Klik på Åbn… for at vælge den kunde specifikke funktionspostkasse-konfigurationsfil.
- Vælg om der skal vises en advarsel ved afsendelse af e-mails til usikre e-mail modtagere.
- Tryk på knappen Anvend lokal indstilling.

Efter valg af indstillinger for funktionspostkasserne er installation færdig og SikkerMail er klar til brug næste gang Outlook genstartes.

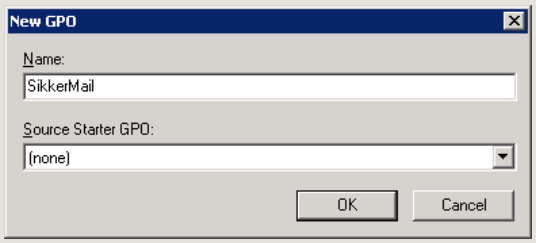


Generel opsætning af Group Policy

Start Group Policy Management ved at klikke på Start, vælg Administrative Tools og klik på Group Policy Management.

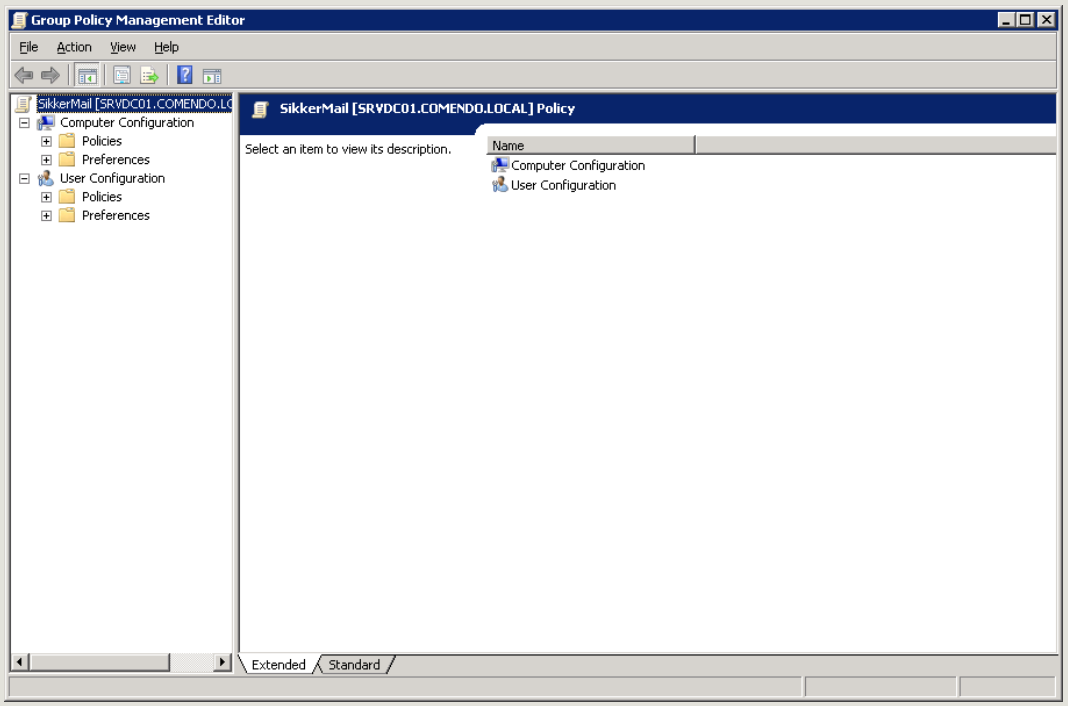
Vælg dernæst Group Policy Objects.

Højreklik på Group Policy Objects (GPO) og vælg New.



Indtast navnet på den nye GPO og tryk OK.

Når GPO'en er oprettet og vises i listen skal man højre klikke på GPO'en og vælge Edit.

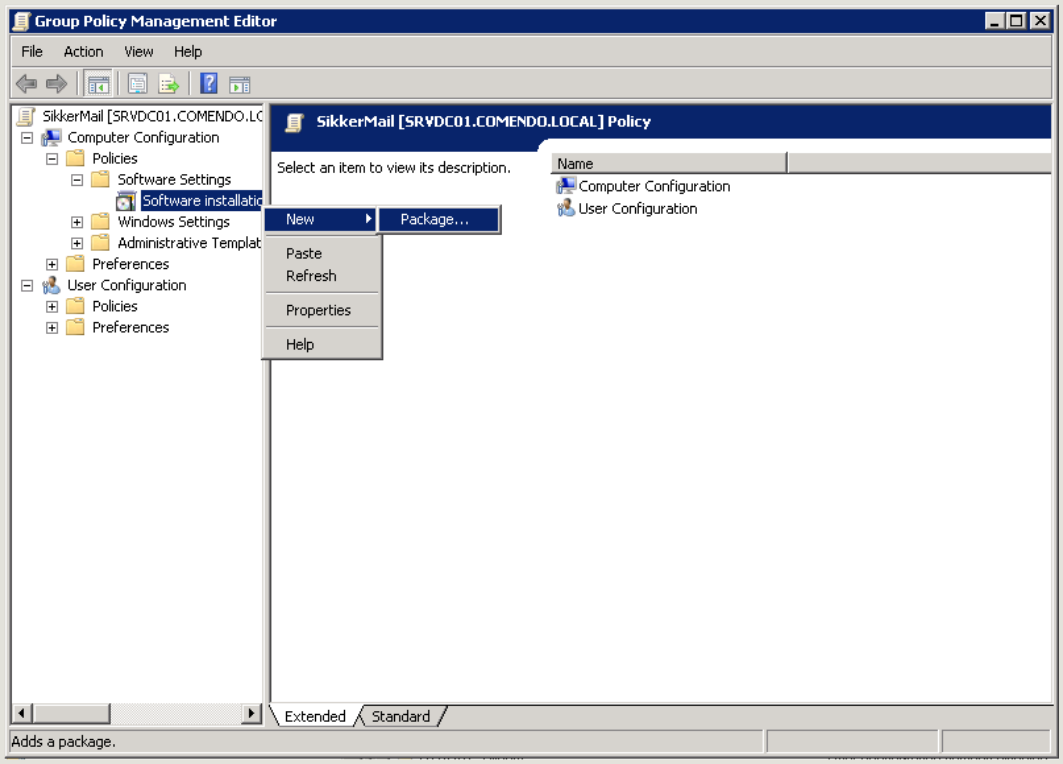


Under Computer Configuration klik på plus'et (+) ud for Policies.

Derefter på plus'et (+) udfor Software Settings.

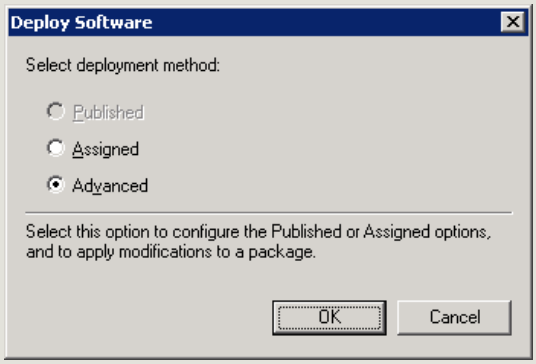
* Genstartspunkt ved oprettelse af flere pakker (Package…).

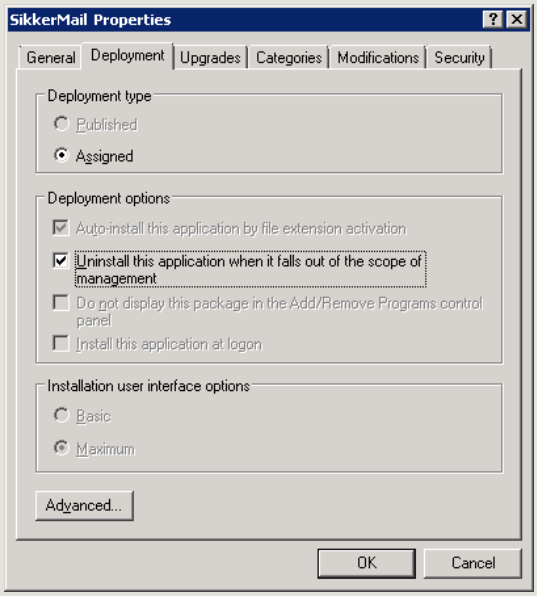
Højreklik på Software installation og vælg New -> Package...



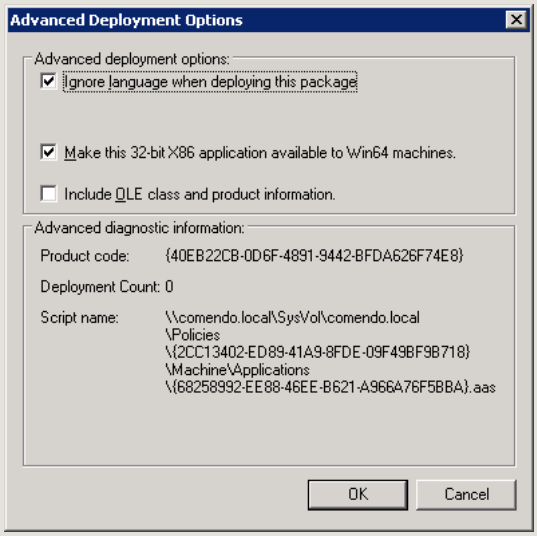
Find den .msi pakke/fil der skal tilføjes, 32 bit eller 64 bit, og vælg den.

I skærmbilledet Deploy Software skal der vælges Advanced og klikkes på OK.



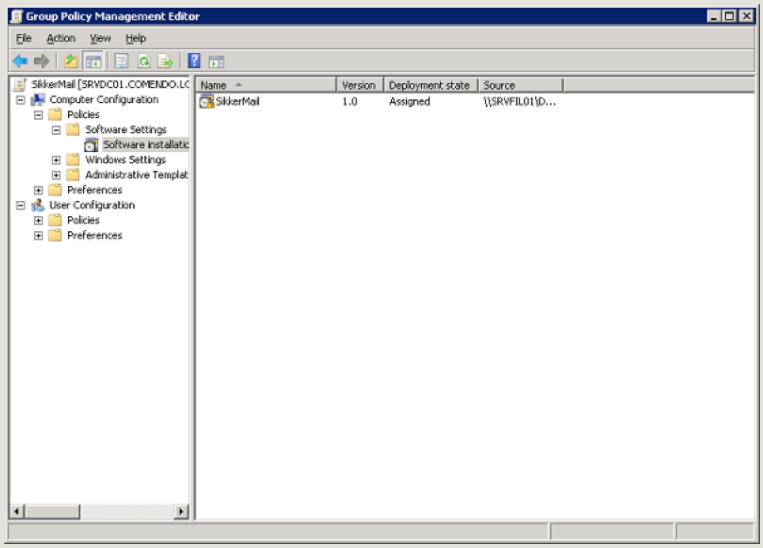


Vælg fanebladet Deployment og marker Uninstall this application when it fall out of the scope of management og tryk på Advanced…



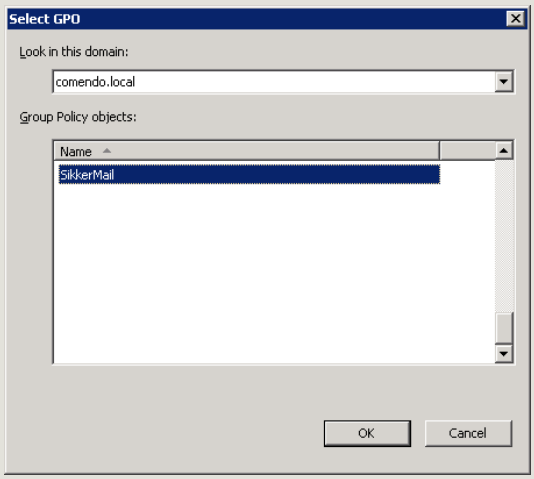
Marker Ignore language when deploying this package og tryk på OK.

I det næste skærmbillede trykkes også OK. Nu vil den nyoprettede pakke blive vist i listen under Software installation.

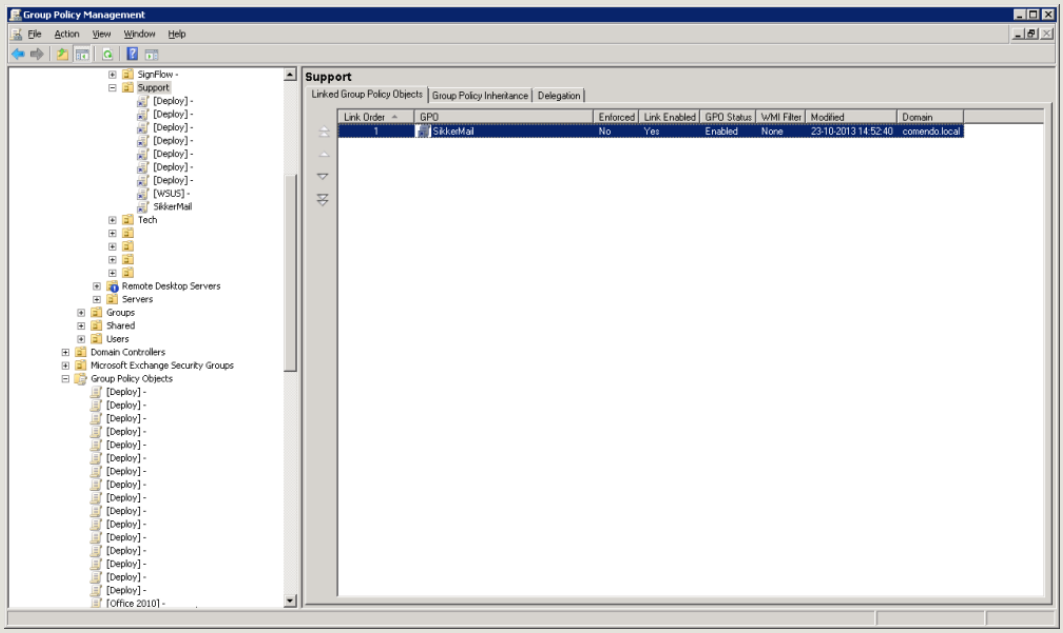


Luk dette skærmbillede for at vende tilbage til Group Policy Management skærmbilledet.

Højreklik på den Organizational Unit (OU) hvor du ønsker at linke GPO til og vælg Link an existing GPO…
(Skal være der hvor computer accounts er placeret)



Vælg den nyoprettede GPO og klik på OK.



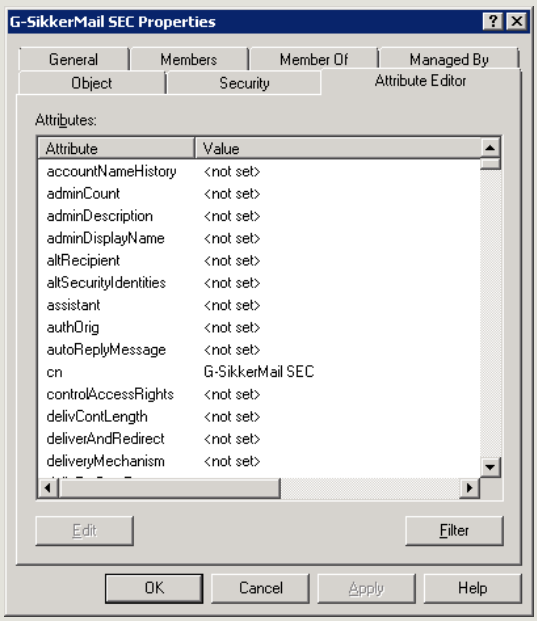
Opsætning af Active Directory

Start Active Directory Users and Computers ved at klikke på Start, vælg Administrative Tools og klik på Active Directory Users and Computers.

Find den bruger/gruppe der skal have tilknyttet SikkerMail opsætningen.

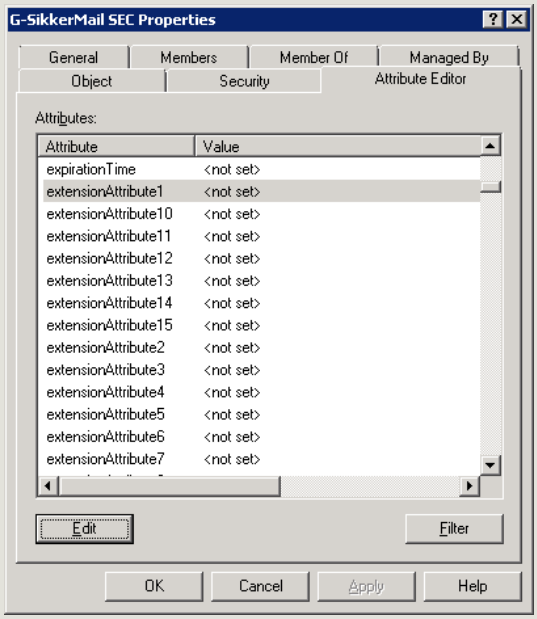
Højreklik på bruger/gruppe og vælg Properties. Vælg fanebladet Attribute Editor.

OBS. Attribute Editor findes kun i Windows Server 2008 og frem. For Servere før 2008 skal der anvendes ADSI Edit. Læs mere via dette link http://technet.microsoft.com/en-us/library/cc773354(v=ws.10).aspx

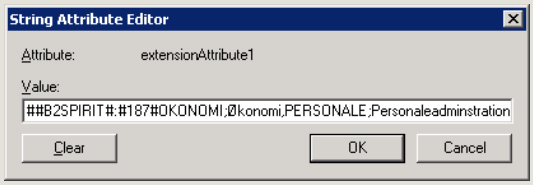


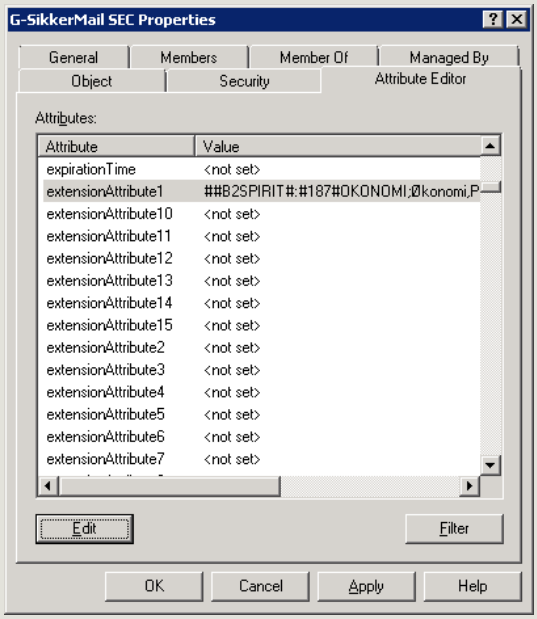
Vælg den 'Attribute' du vil ligge SikkerMail indstillingerne ind under og klik på Edit.

Det anbefales at anvende extentionAttributeXX.



Indtast nu indstillingerne for funktionspostkasser og visning der opfylder kravene for dette. (Se vejledning for Active Directory indstillinger tidligere i dokumentet). Tryk derefter på OK.





Efter endt indtastning trykkes på OK.

Indstillingerne indlæses automatisk næste gang brugeren starter Outlook og såfremt at Add-in'et er installeret.