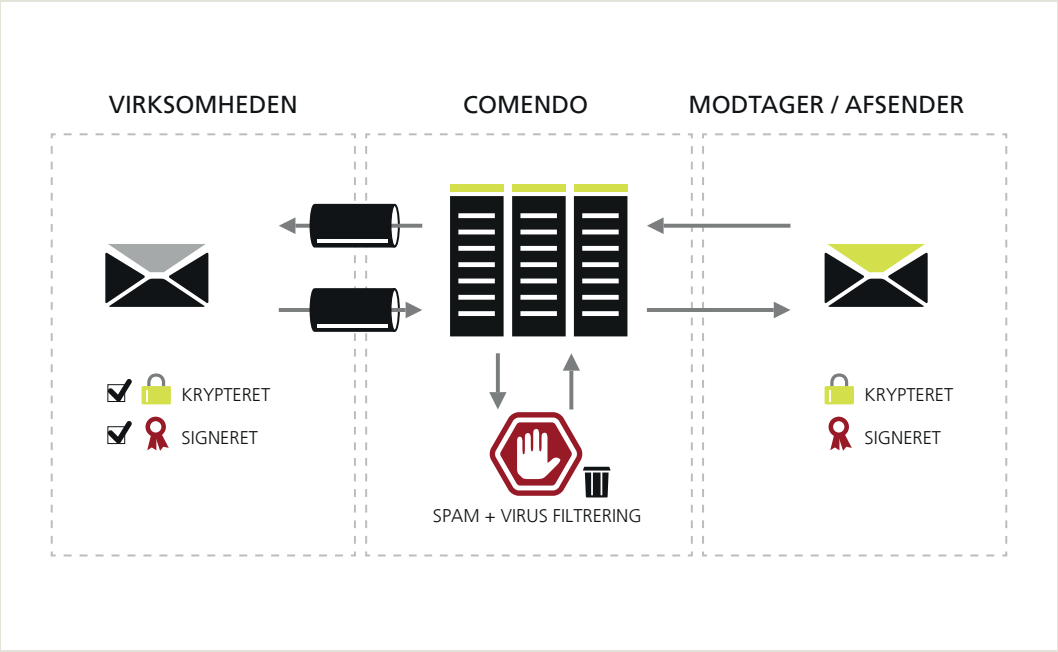
comendo

Manual

Comendo SikkerMail

VERSION 10-01-2014



© 2014 Comendo

comendo

INDHOLDSFORTEGNELSE

© 2014 Comendo

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:

- 89.104.214.192/29
- 89.104.216.0/24
- 89.104.217.0/24

Virksomhedscertifikat

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.

Læs mere i afsnittet "Anskaffelse og installation af virksomhedscertifikater"

Genbestille certifikat

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

© 2014 Comendo

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 sikkermail@sikkermail.comendo.com.

Koden anbefaler vi oplyses på en alternativ kommunikationsvej, eksempelvis fysisk post eller SMS.

Anskaffelse og installation af certifikater

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 funktionspost-kassen 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.

© 2014 Comendo

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- elle person-oplysninger) 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.

© 2014 Comendo

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.

Krypteret og signeret e-mail manuelt ved brug af syntaks

Ved såvel en ny meddelelse som besvarelse af en modtaget meddelelse som ønskes fremsendt digital signeret og krypteret skal 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.

Hvis man skriver flere e-mailadresser i til-feltet eller hvis man sender Cc, videregiver man oplysninger om

© 2014 Comendo

andre modtagere. Der skal være et lovligt grundlag for at videregive både de oplysninger, der er indeholdt i meddelelsen og oplysning om, hvem de andre modtagere er og disses e-mailadresser. En uhensigtsmæssig brug af Cc-funktionen eller flere adresser i til-feltet kan føre til overtrædelse af persondataloven.

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.

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/

Afsendelse af sikker e-mail i Microsoft Outlook

Der findes flere forskellige måder at anvende SikkerMail på. Hvis der anvendes Outlook 2000 til 2010 som mailklient, kan der installeres et Outlook Add-in.

Hvis man ønsker e-mail digitalt underskrevet trykkes på "Digital Signatur", hvis man ønsker e-mailen digitalt krypteret dvs. beskyttet så kun modtageren kan læse e-mailen så trykkes på "Kryptering".

Kryptering kan kun lade sig gøre til modtagere der har en kendt digital signatur dvs. enten en offentlig

© 2014 Comendo

signatur (OCES) eller har sendt myndigheden eller medarbejderen en e-mail med digital signatur.

Anvendelse af Sikkermail Outlook Add-in, fungerer som en alternativ send knap, der tilsikrer at den afsendte 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.

Tilsvarende funktion kan anvendes og opnås ved manuel indtastning af en syntaks i emnefeltet inden mailen afsendes med den almindelige send knap, i en hvilken som helst mailklient.

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 plugin, 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.

© 2014 Comendo

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.

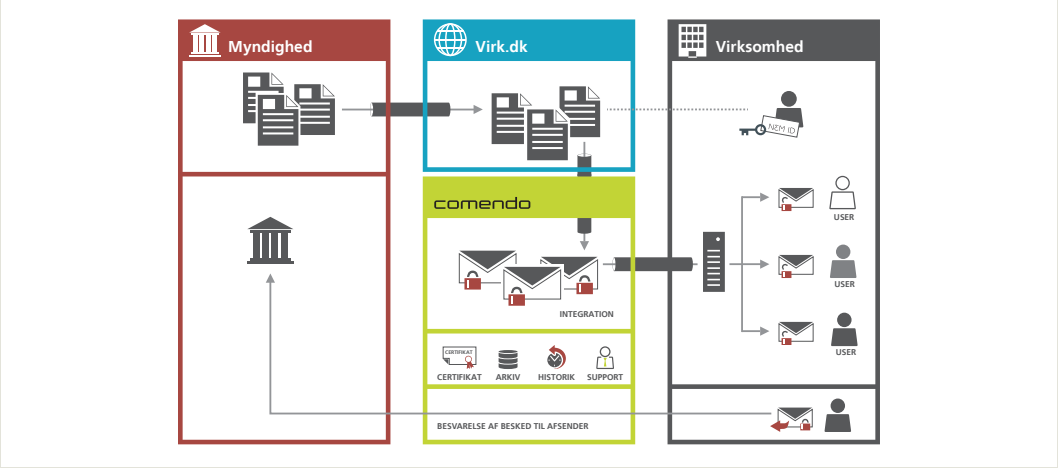
Bemærk: Det er pt. Ikke muligt at sende sikker post mellem myndigheder/virksomheder som er tilknyttet samme interne mailsystem. Intern post anses for at være sikker.

© 2014 Comendo

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 13.

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.

© 2014 Comendo

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.

© 2014 Comendo

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.
6. Accepter vilkårene for oprettelse af en digital postkasse.
7. Bekræft virksomhedens navn.
8. Bekræft dine oplysninger og klik på "Godkend". Du har nu oprettet en digital postkasse.

© 2014 Comendo

Opsætning til virk.dk

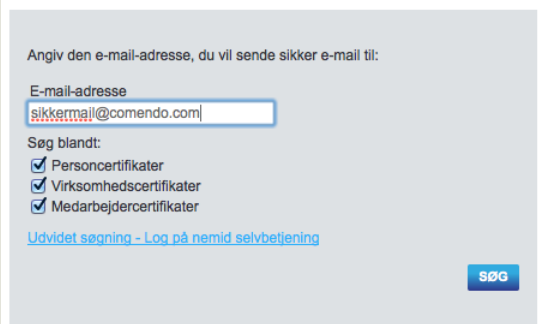
For at få videresendt jeres meddelelser fra det offentlige, skal I logge på Virk.dk og etablere denne videresendelse. I skal benytte den offentlige del af jeres virksomhedscertifikat for at, videresendelsen kan ske krypteret og i overensstemmelse med gældende lovgivning.

Hent den offentlige del af jeres virksomhedscertifikat

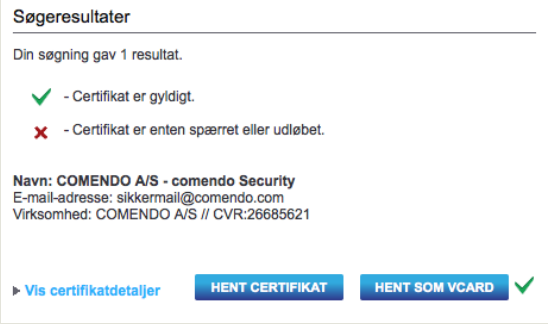
Hent den offenlige del af jeres certifikat på

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.



© 2014 Comendo

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.

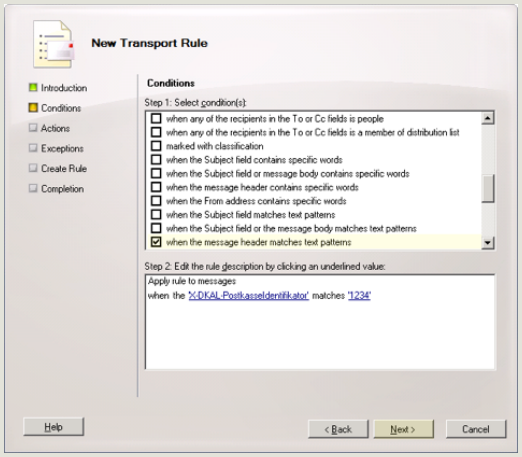
© 2014 Comendo

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

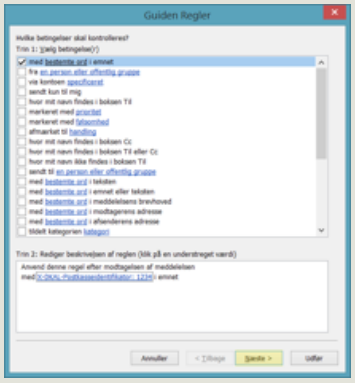
Hvis I opsætter regler på jeres Exchange server, bliver de indkomne e-mails fordelt ved ankomst til jeres mailserver. I skal oprette en "Transport Rule" i jeres Exchangeservers "Exchange Management Console".



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.

© 2014 Comendo

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.

© 2014 Comendo

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 of-

© 2014 Comendo

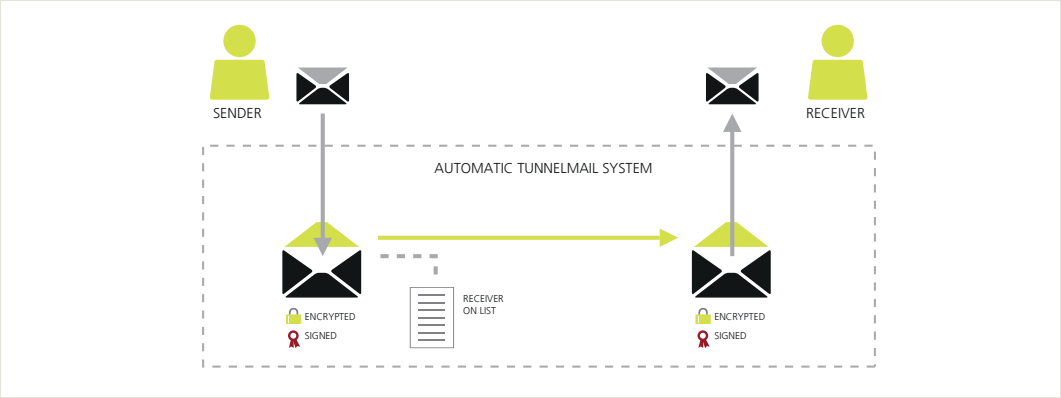
fentlige systemer (kilde: digitalsignatur.dk).

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.

© 2014 Comendo

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.

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

Comendos Partnere kender også disse kontaktinformationer.

© 2014 Comendo

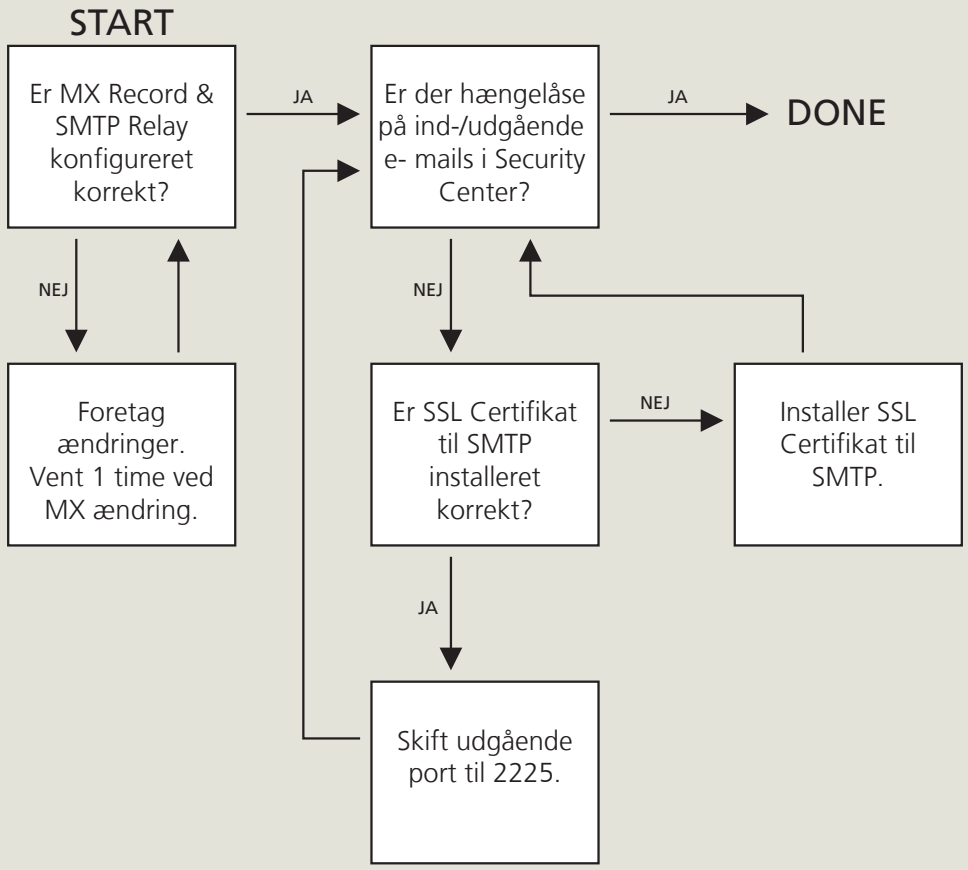
BILAG 1

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.

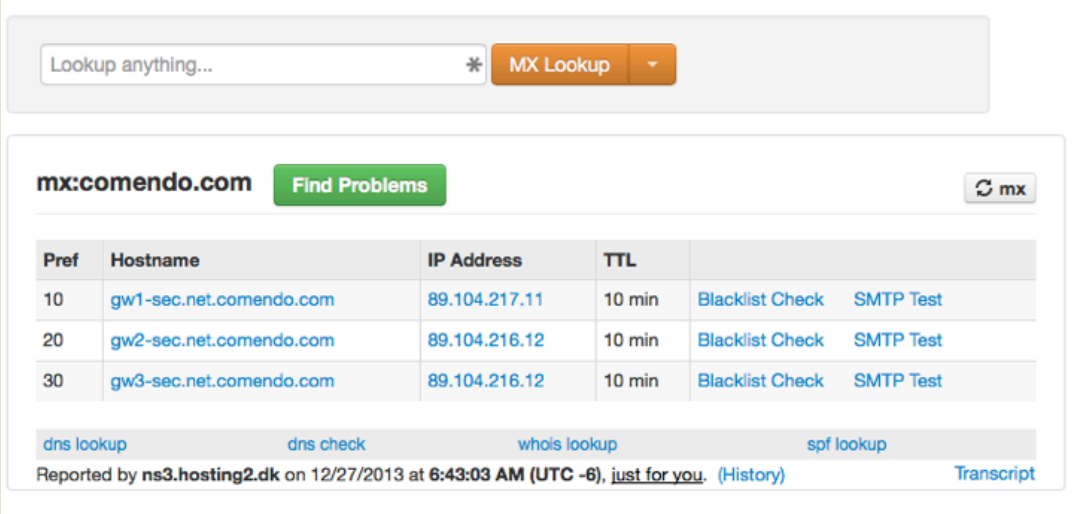
Følg nedenstående diagram for at verificere korrekt opsætning. Der er yderligere forklaring til hvert enkelt punkt senere i teksten.



© 2014 Comendo

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 modtageren.

© 2014 Comendo

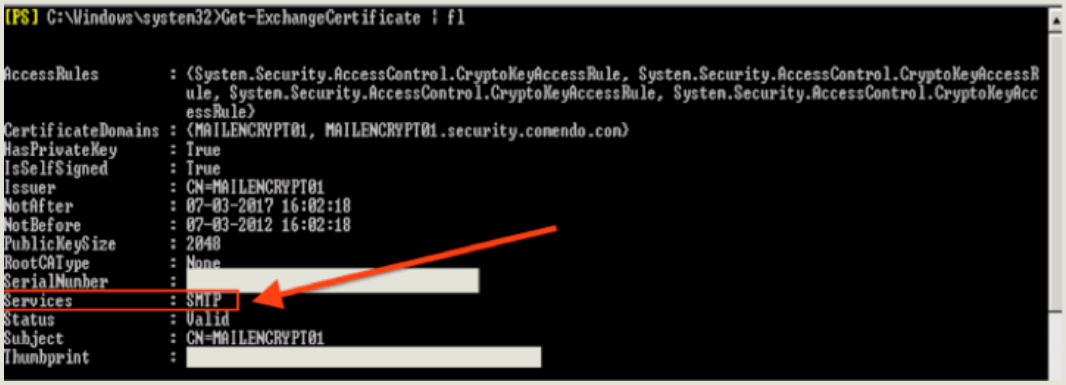
Er SSL Certifikat installeret?

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

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

   Get-SendConnector

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

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

© 2014 Comendo

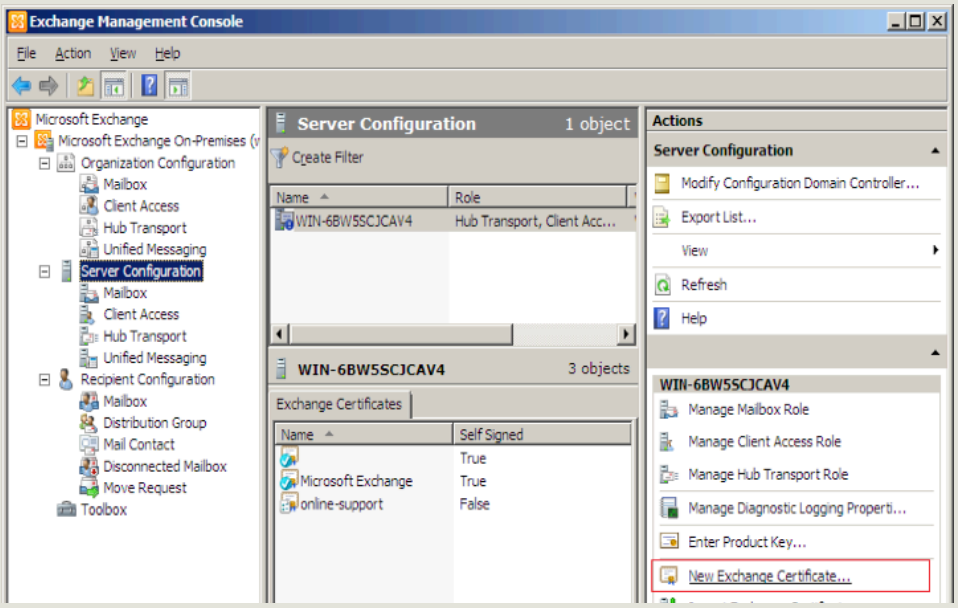
Anskaffelse og installation af certifikat

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.

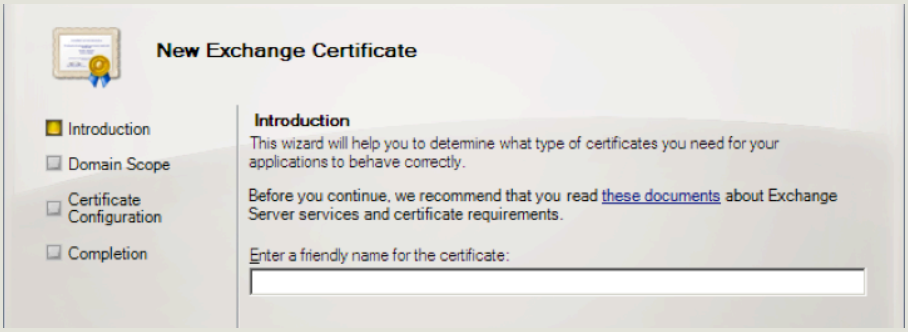
Bemærk at nedenstående guide er på engelsk og tager udgangspunkt i Exchange 2010.

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.

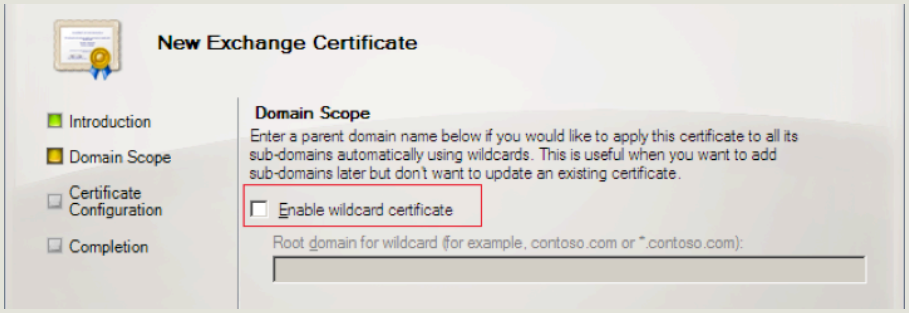


3. When prompted for a friendly name, use a name of your own choice. The name will not affect your request

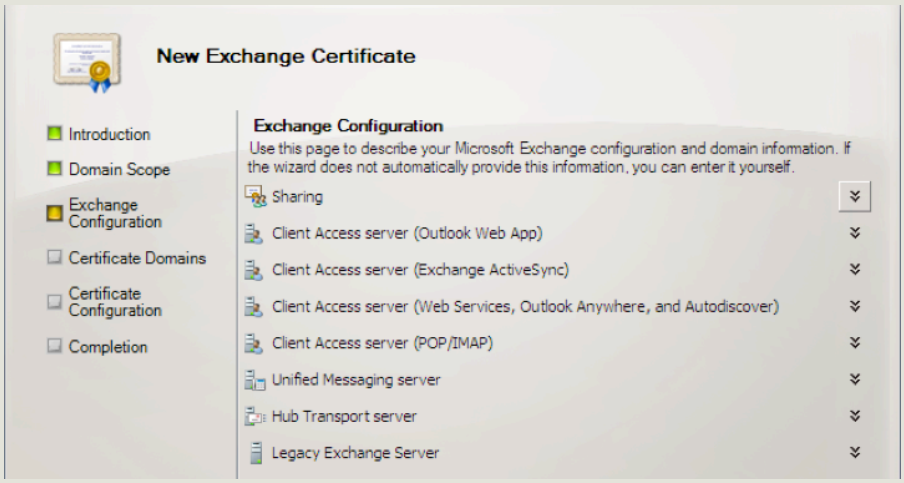
© 2014 Comendo

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.

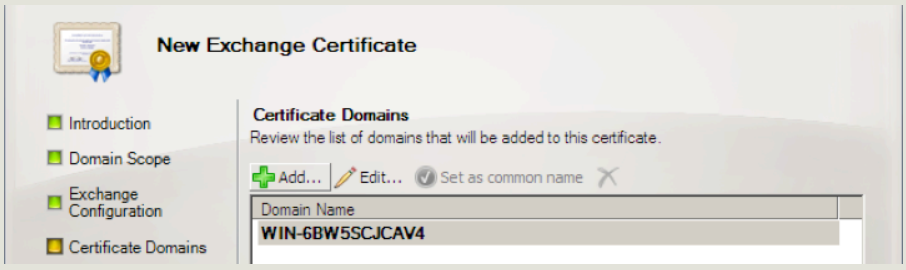
   Note: If you do select that box for a wildcard, skip to step 7.



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

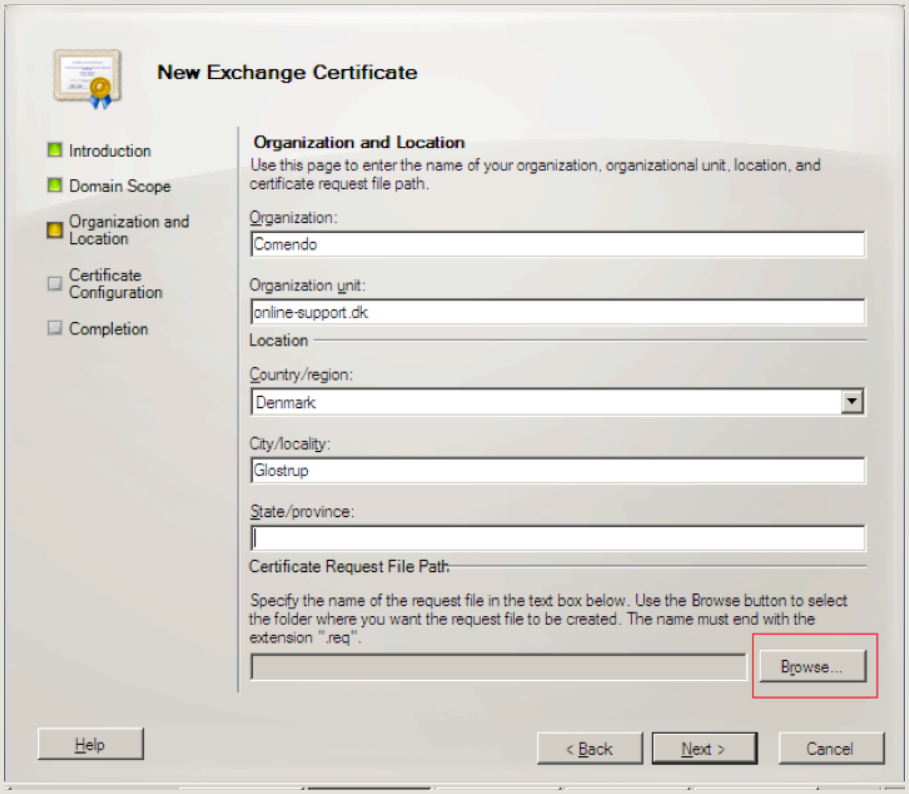


6. You will be able to review a list of the domain names which Exchange 2010 suggests you include in your certificate request. We recommend that your domain name should be one of them.

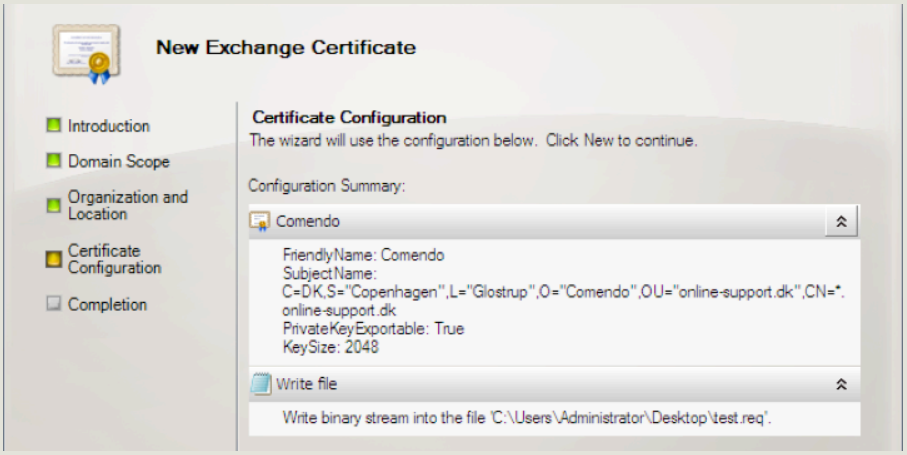


© 2014 Comendo

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.

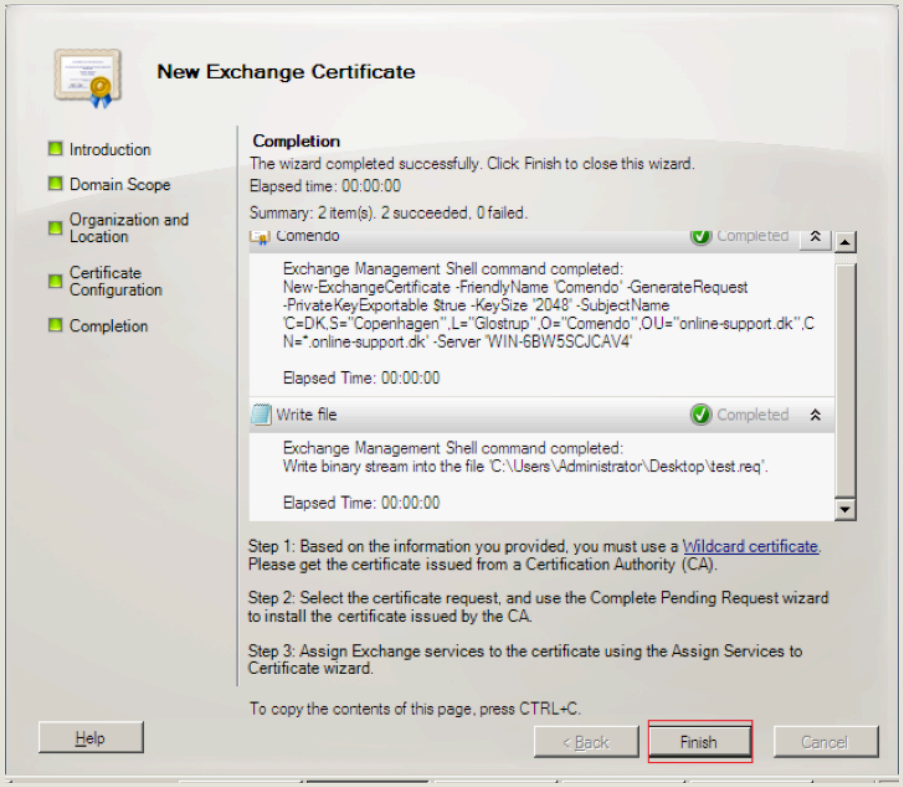


8. Click Browse to save the CSR to your computer as a .req file
9. Review the information, and continue by clicking 'New'.



© 2014 Comendo

10. Finally click Finish to create the CSR.



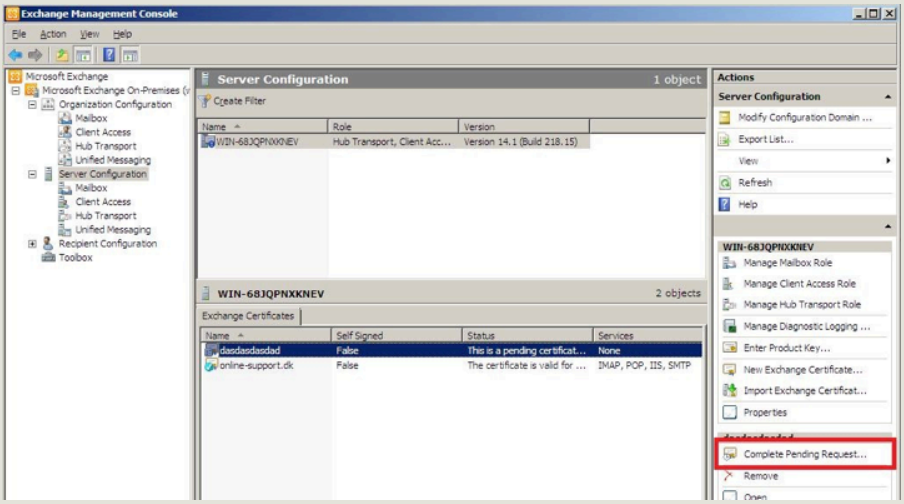
11. Your request is now finalized. To complete the request, and in order to get your certificate mailed, you need to send the .CSR (the request) file to your certificate supplier.

© 2014 Comendo

Install certificate

Once you have received your certificate, you must complete the following, in order to setup your certificate and prepare your server for MailTunnel.

1. Download and open the ZIP file containing your certificate. Your certificate file will most likely be named "your_domain_name.cer"
2. Copy the "your_domain_name.cer" file to your Exchange server.
3. Start the Exchange Management Console by going to Start > Programs > Microsoft Exchange 2010 > Exchange Management Console.
4. Click the link to "Manage Databases", and then go to "Server configuration".
5. 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".



6. 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.
7. Now, to enable your certificate for use, go back to the Exchange Management Console and click the link to "Assign Services to Certificate."

© 2014 Comendo

8. Select your server from the list provided, then click Next.
9. 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.

© 2014 Comendo