FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

Exchange 2010 SSL certifikat administration

Følgende vejledning beskriver hvordan man vælger hvilke adresser der skal være i ens Exchange 2010 SAN SSL certifikat. Derudover er der tekniske guides til at importere, eksportere, liste og aktivere certifikater i Microsoft Exchange 2010.

For at Exchange kan benytte et certifikat skal det først importeres og derefter aktiveres til de services der skal bruge certifikatet.

Husk at anvendes en ISA server foran Exchange serveren, skal certifikatet også installeres på denne.

For support og hjælp til anvendelsen af denne vejledning kan du kontakte FairSSL på e-mail support@fairssl.dk eller telefon +45 77 345 678. For certifikat bestilling, certifikat sammenligninger og flere vejledninger se websitet på www.fairssl.dk.

Husk at teste din installation når du er færdig gratis på www.fairssl.dk/ssltest/

Indholdsfortegnelse

Version 1.1a – December 2010

GlobalSign Platinum Partner
GeoTrust PARTNER
RapidSSL AUTHORIZED PARTNER

FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

Valg af domæner der skal inkluderes i et SAN SSL til Exchange 2010

Exchange 2010 (og Exchange 2007) anvender sig af flere domæne adresser der bør beskyttes af et SSL certifikat. Derfor anbefaler Microsoft at anvende et Subject Alternative Name (SAN) / Unified Communication (UC) kompatibelt SSL certifikat. Disse certifikater kan beskytte flere adresser på et SSL certifikat og derved spare offentlige IP adresser og gøre konfigurationen af serveren lettere.

Exchange 2010 kan som standard kun installere UC kompatible certifikater! Wildcard SSL certifikater kan absolut ikke anbefales og kan tilmed være umulige at installere. Enkelt adresse SSL certifikater kan som standard ikke installeres.

Her vil vi kort gennemgå de mest typisk anvendte adresser der inkluderes i et Exchange 2010 SAN SSL certifikat og hvilke certifikater som understøtter disse.

Generelt

- Der bør inkluderes alle de navne (FQDN) som Exchange serveren tilgås på fra internettet
- Der bør inkluderes alle de navne (FQDN) som Exchange serveren tilgås fra på det interne net
- Der bør være inkluderet autodiscover.domæne.dk for hvert af de e-mail domæner der anvendes af brugerne som deres primære e-mail adresse.

Autodiscover adressen tillader klienten at automatisk hente konfigurationen til Exchange og derved gøre opsætningen af klienter både internt og eksternt lettere. Der skal være en autodiscover adresse for hvert e-mail domæne som brugeren anvender som ”brugernavn”, dvs. som deres primære e-mail adresse.

Standard - 1 e-mail domæne som anvendes af brugerne i deres opsætning af klienten

Dette eksempel er ved anvendelse af et enkelt e-mail domæne ”@fairssl.dk”, som tilgås fra internettet på adressen ”mail.fairssl.dk” og internt på det lokale netværk med adressen ”exchsrv01.notyours.local”. Hvis flere adresser anvendes til at tilgå serveren skal disse også tilføjes.

Følgende adresser skal beskyttes i SSL certifikatet:

- Mail.fairssl.dk (owa. og webmail. er også typisk anvendt)
- Autodiscover.fairssl.dk
- Exchsrv01.notyours.local

Fordi der kun anvendes adresser på et offentligt domæne kan et domæne valideret SSL certifikat anvendes, f.eks. GlobalSign Domain SAN.

Udvidet - Flere e-mail domæner anvendes af brugerne i deres opsætning af klienten

Dette eksempel er for virksomheder der har brugere med flere e-mail domæner i deres primære e-mail adresse. Serveren i dette eksempel anvender følgende e-mail domæner ”@fairssl.dk” og ”@notyours.dk”, den tilgås kun fra internettet på adressen ”mail.fairssl.dk” og internt på det lokale netværk med adressen ”exchsrv01.notyours.local”. Hvis flere adresser anvendes til at tilgå serveren skal disse også tilføjes.

Følgende adresser skal beskyttes i SSL certifikatet:

FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

- **Mail.fairssl.dk**
- Autodiscover.fairssl.dk
- Autodiscover.notyours.dk
- Exchsrv01.notyours.local

Fordi der anvendes adresser på flere offentlige domæner skal et firma valideret SSL certifikat anvendes, f.eks. GlobalSign Organisation SAN eller GeoTrust True BusinessID MultiDomain, derudover skal firmaet have ejerskab over alle domænerne.

FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

Generering af CSR til certifikat bestilling

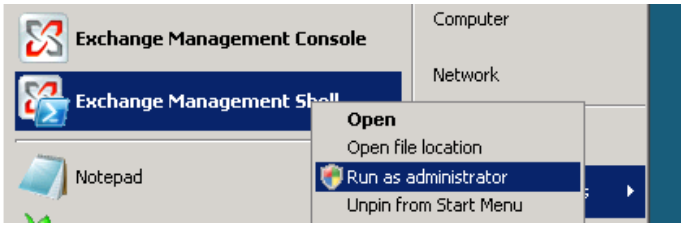
Ved bestilling af et SSL certifikat til beskyttelse af en enkelt server adresse (FQDN) i Exchange 2010, uden brug af AutoCSR, kræves en generering af en CSR kode samtidigt med at den private nøgle oprettes på serveren. For at gennemføre en bestilling og genereringen af CSR koden, har du brug for at samle følgende oplysninger til certifikatet.

Bemærk at danske bogstaver og følgende tegn ikke normalt kan anvendes: > < ! @ # $ % ^ * ( ) ~ ? / \. & Hvis de alligevel tilføjes, kan det forsinke og/eller kræve en rettelse af navnet inden ordren kan gennemføres. Dog vil udstedere typisk tillade at firmanavnet skrives identisk med offentlig registrering.

Common Name (CN): *Det primære fulde internet domæne navn på din Exchange server. (eks. mail.fairssl.dk)*	
Alternative Domænenavne (DomainName): *Navne udover det primære common name, der skal inkluderes i certifikatet, denne parameter virker kun på SAN/UC certifikater. (eks. Autodiscover.fairssl.dk)*	**Husk: Autodiscover._____**
Organization Name (O): *Det fulde gyldige firmanavn som det står i offentlige databaser som CVR. Typisk vil / være tilladt ved A/S og v/Navn. (eks.NOT yours A/S)*	
Department (OU): *Afdelingen, eller lignende beskrivende del af virksomheden. (eks. FairSSL)*	
Stat/region (S): *Stat eller region, i Danmark anvendes bynavnet. (eks.Oerum Djurs)*	
Country (C): *ISO standard to bogstavs landekode. (eks. DK)*	
Locality (L): *By/PostNavn.(eks. Oerum Djurs)*	

1. Log ind på den Exchange 2010 server som har CAS rollen. Benyt en konto som er medlem af "Exchange Administrators" gruppen samt "Administrators" gruppen på den lokale server.

2. Start Exchange Management Shell, højreklik på genvejen og vælg "Run as Administrator".



3. I Exchange Management Shell, skriv følgende kommando efterfulgt af [ENTER], hvor følgende parametre angiver ovenstående informationer du har indsamlet:
   -SubjectName Firma oplysninger

FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

-KeySize 1024/2048 antallet af bits der anvendes til kryptering **(anvend 2048 bit)**
-Path Sti til hvor CSR filen skal gemmes
-DomainName Subject Alternative Names, alternative navne der også skal beskyttes
-**PrivateKeyExportable** hvorvidt certifikatet efterfølgende skal kunne eksporteres til en backup

```
New-ExchangeCertificate -GenerateRequest -SubjectName "C=DK, O=Not Yours, OU=FairSSL, S=DK, L=Oerum Djurs, CN=mail.fairssl.dk" -KeySize 2048 –DomainName autodiscover.fairssl.dk, owa.fairssl.dk, exchsrv01.notyours.local, exchsrv01 -privatekeyexportable $true
```

4. Du kan nu vælge at markere og kopiere teksten som generes som en CSR fil og sende den i certifikat ansøgningen, eller skrive følgende kommando for at gemme til en fil.

```
Set-Content -Path ”c:\mail.fairssl.dk.csr” –Value $Data
```

5. Du har nu lavet en certifikatansøgning som er blevet gemt i en tekst fil.

6. Åben certifikatansøgningen I notepad. I Exchange Management Shell, skriv følgende commando efterfulgt af [ENTER]:

```
notepad c:\mail.fairssl.dk.csr
```

7. Marker og kopier hele teksten fra CSR filen, inklusive start og slut taggen. Under certifikat bestillingen skal du indsætte denne tekst i CSR feltet. Følgende er et eksempel på en fuld CSR tekst.

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDVDCCAr0CAQAweTEeMBwGA1UEAxMVd3d3Lmpvc2VwaGNoYXBtYW4uY29tMQ8w
DQYDVQQLEwZEZXNpZ24xFjAUBgNVBAoTDUpvc2VwaENoYXBtYW4xEjAQBgNVBAcT
CU1haWRzdG9uZTENMAsGA1UECBMES2VudDELMAkGA1UEBhMCR0IwgZ8wDQYJKoZI
hvcNAQEBBQADgY0AMIGJAoGBAOEFDpnOKRabQhDa5asDxYPnG0c/neW18e8apjOk
1yuGRk+3GD7YQvuhBVS1x6wkw1D2RnmnZgN1nNUK0cRK7sIvOyCh1+jgD7u46mLk
81j+b4YSEmYZGPLIuclyocPDm0hXayjCUqWt7z6LMIKpLym8gayEZzz9Gn97PsbP
kVFBAgMBAAGgggGZMBoGCisGAQQBgjcNAgMxDBYKNS4xLjI2MDAuMjB7BgorBgEE
AYI3AgEOMW0wazAOBgNVHQ8BAf8EBAMCBPAwRAYJKoZIhvcNAQkPBDcwNTAOBggq
hkiG9w0DAgICAIAwDgYIKoZIhvcNAwQCAgCAMAcGBSsOAwIHMAoGCCqGSIb3DQMH
MBMGA1UdJQQMMAoGCCsGAQUFBwMBMIH9BgorBgEEAYI3DQICMYHuMIHrAgEBHloA
TQBpAGMAcgBvAHMAbwBmAHQAIABSAFMAQQAgAFMAQwBoAGEAbgBuAGUAbAAgAEMA
cgB5AHAAdABvAGcAcgBhAHAAaABpAGMAIABQAHIAbwB2AGkAZABlAHIDgYkAk0kf
HSkr4jsEVya3mgUoyaYMO456ECNZr4Cb+whPgexfjOO5qwOG1oDOTaKycrkc5pG+
IPBQnq+4cotT8hWJQwpc+qGb8xUETpxCokhrhN5079vFXq/5dsHkmtOTwkSqSnz9
yruVoxYeDQ8jI3KG3HTgxwFto8oZnm+E+Y4oshUAAAAAAAAAADANBgkqhkiG9w0B
AQUFAAOBgQAuAxetLzgfjBdWpjpixeVYZXuPZ+6jvZNL/9hOw7Fk5pVVXWdr8csJ
6JUW8QdH9KB6ZlM4yg8Df+vat1/DG6GuD2hiIR7fQONtPFBQmbrSm+TTBo95lwP+
ZSZTusPFTLKaqValdnS9Uw+6Vq7/I4ouDA8QBIuaTFtPOp+8wEGBHQ==
-----END NEW CERTIFICATE REQUEST-----
```

GlobalSign Platinum Partner
GeoTrust PARTNER
RapidSSL AUTHORIZED PARTNER

FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

Import af mellemudsteder certifikat ("Intermediate Certificate Authority")

Følgende beskriver hvordan mellemudsteder certifikater installeres på en Microsoft Windows baseret server og derved også en Exchange 2010 server. For at sikre at klienter kan godkende mellemudstedere i certifikatet, skal certifikatets mellemudstederes offentlige certifikat installeres på Exchange 2010 serveren. Bemærk at GlobalSign kræver at du henter et specielt intermediate certifikat til Exchange 2007/2010 (kan hentes på https://www.fairssl.dk/vejledninger/exchange-ocs-2007/).

1. Log ind på serveren med en konto der er medlem af gruppen "Administrators" på den lokale server.

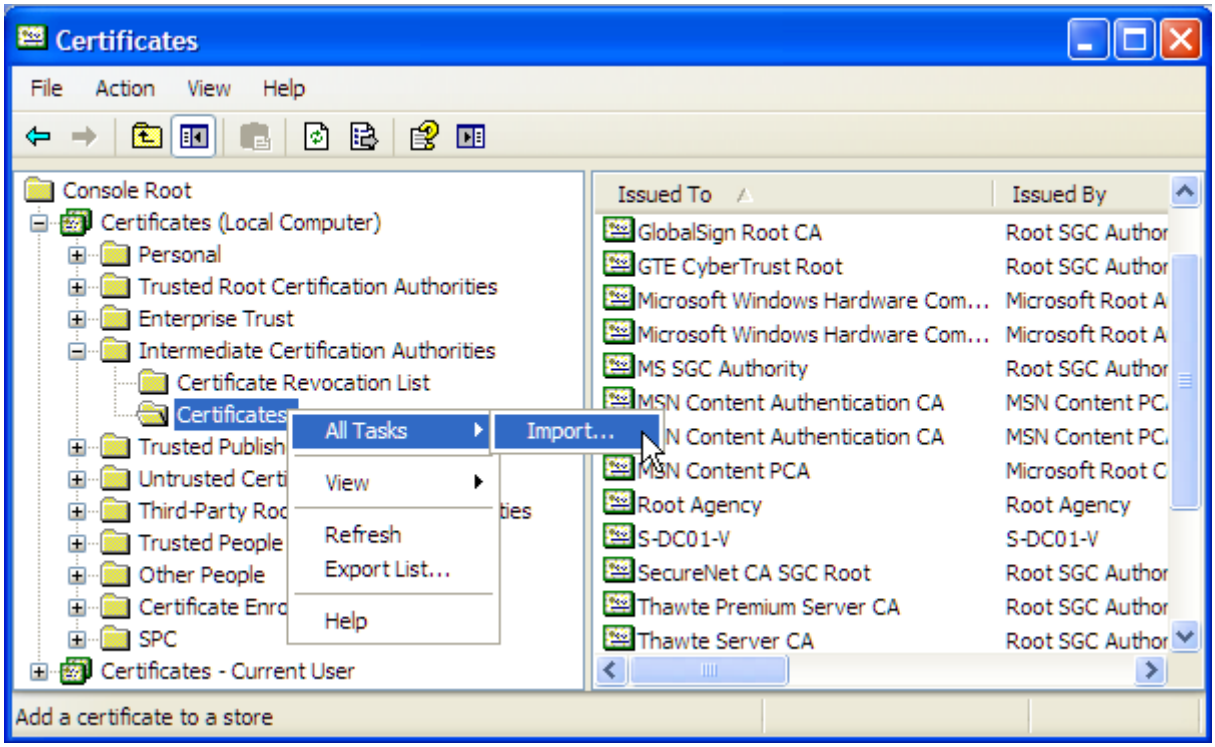
2. Kopier teksten med mellemudsteder certifikatet ("Intermediate certificate"), fra e-mailen med dit nye certifikat, til en simpel tekst editor (som Notepad). Gem filen på skrivebordet, med filnavnet "mellemudsteder.cer".

3. Vælg Start – Kør og skriv følgende kommando "certmgr.msc".
   (Alternativt start mmc.exe og vælg "Add/Remove Snap In" og tilføj "Certificates", vælg følgende svar muligheder, "Computer Account" og "Local Computer".)

4. Under "Certificates (Local Computer)" udvid "Intermediate Certification Authorities" og "Certificates".

5. Højre klik på "Certificates" og vælg "All-Tasks" og "Import".

6. Følg instruktionerne og vælg filen du gemte på skrivebordet.



Certificatet vil blive vist på listen over "Intermediate Certification Authorities" og er nu installeret.

FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

Installation og aktivering af certifikat fil (.CER)

Følgende beskriver hvordan du installerer og aktiverer en certifikat fil, du har modtaget efter udstedelse af et certifikat med anvendelse af en CSR under bestillingen. Installationen skal foregå på samme server som CSR'en er oprettet på.

1. Log ind på de Exchange 2010 server som har CAS rollen. Benyt en konto som er medlem af "Exchange Administrators" gruppen samt "Administrators" gruppen på den lokale server.

2. Start Exchange Management Shell, højreklik på genvejen og vælg "Run as Administrator".

3. I Exchange Management Shell, skriv følgende kommando efterfulgt af [ENTER], hvor "-Path" angiver filens placering og "-Services" angiver de ønskede services der skal aktiveres:

   ```
   Import-ExchangeCertificate –FileData ([Byte[]]$(Get-Content –Path c:\mail.notyours.dk.cer –Encoding byte –ReadCount 0)) | Enable-ExchangeCertificate –Services "IIS,POP,IMAP,SMTP,None"
   ```

   (tilføj UM til services, **KUN** hvis Unified Messaging er installeret i Exchange miljøet.)

4. Gå til Eksporter certifikat til backup fil, for at gemme en kopi af certifikat og for at kunne installere certifikatet på andre Exchange og hvis anvendt ISA server.

*Den første del af kommandoen (venstre side af "|") vil nu importere certifikatfilen.
Herefter vil anden del af kommandoen (Højre for "|") tage det nyligt importerede certifikat og aktivere det for de angivne services.

Installation af certifikat fil (.CER)

Følgende beskriver hvordan du installerer en certifikat fil, du har modtaget efter udstedelse af et certifikat med anvendelse af en CSR under bestillingen. Installationen skal foregå på samme server som CSR'en er oprettet på.

1. Log ind på de Exchange 2010 server som har CAS rollen. Benyt en konto som er medlem af "Exchange Administrators" gruppen samt "Administrators" gruppen på den lokale server.

2. Start Exchange Management Shell, højreklik på genvejen og vælg "Run as Administrator".

3. I Exchange Management Shell, skriv følgende kommando efterfulgt af [ENTER], hvor "-Path" angiver filens placering og "-Services" angiver de ønskede services der skal aktiveres:

   ```
   Import-ExchangeCertificate –FileData ([Byte[]]$(Get-Content –Path c:\mail.notyours.dk.cer –Encoding byte –ReadCount 0))
   ```

4. Gå til Eksporter certifikat til backup fil, for at gemme en kopi af certifikat og for at kunne installere certifikatet på andre Exchange og hvis anvendt ISA server.

FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

Import og aktivering af certifikat backup fil (PKCS12)

Følgende beskriver hvordan en certifikat backup fil, importeres og aktiveres i Exchange 2010. Ved bestilling af domæner med AutoCSR modtages certifikatet som en backup fil, beskyttet med en unik kode.

1. Log ind på de Exchange 2010 server som har CAS rollen. Benyt en konto som er medlem af "Exchange Administrators" gruppen samt "Administrators" gruppen på den lokale server.

2. Start Exchange Management Shell, højreklik på genvejen og vælg "Run as Administrator".

3. I Exchange Management Shell, skriv følgende kommando efterfulgt af [ENTER], hvor "-Path" angiver filens placering og "-Services" angiver de ønskede services der skal aktiveres:


```
Import-ExchangeCertificate -FileData ([Byte[]]$(Get-Content -Path
c:\mail.notyours.dk.pfx -Encoding byte -ReadCount 0)) -
password:(Get-Credential).password | Enable-ExchangeCertificate -
Services "IIS,POP,IMAP,SMTP,None"
```

(tilføj UM til services, hvis Unified Messaging er installeret.)

4. Der vises nu en prompt for brugernavn og kode, bemærk brugernavnsfeltet anvendes ikke, men der skal stå noget.

Skriv "none" i brugernavn og det password som filen er beskyttet med i password.
Bemærk at vælges services som ikke er installeret, vil kommandoen fejle, vælg kun de services hvor certifikatet skal anvendes.

5. Gentag proceduren på eventuelle andre Exchange servere der skal benyttes som CAS servere.

*Den første del af kommandoen (venstre side af "|") vil nu importere certifikatfilen.
Herefter vil anden del af kommandoen (Højre for "|") tage det nyligt importerede certifikat og aktivere det for de angivne services.

FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

Import af certifikat backup fil (.PFX og .P12)

Følgende beskriver hvordan en certifikat backup fil, importeres uden aktivering i Exchange 2010. Ved bestilling af domæner med AutoCSR modtages certifikatet som en backup fil, beskyttet med en unik kode.

1. Log ind på de Exchange 2010 server som har CAS rollen. Benyt en konto som er medlem af "Exchange Administrators" gruppen samt "Administrators" gruppen på den lokale server.

2. Start Exchange Management Shell, højreklik på genvejen og vælg "Run as Administrator".

3. I Exchange Management Shell, skriv følgende kommando efterfulgt af [ENTER], hvor "-Path" angiver filens placering:

   ```
   Import-ExchangeCertificate –FileData ([Byte[]]$(Get-Content –Path c:\mail.notyours.dk.pfx –Encoding byte –ReadCount 0)) –password:(Get-Credential).password
   ```

4. Der vises nu en prompt for brugernavn og kode, bemærk brugernavnsfeltet anvendes ikke, men der skal stå noget.

   Skriv "none" i brugernavn og det password som filen er beskyttet med i password.
   Bemærk at vælges services som ikke er installeret, vil kommandoen fejle, vælg kun de services hvor certifikatet skal anvendes.

Gentag proceduren på eventuelle andre Exchange servere der skal benyttes som CAS servere.

FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

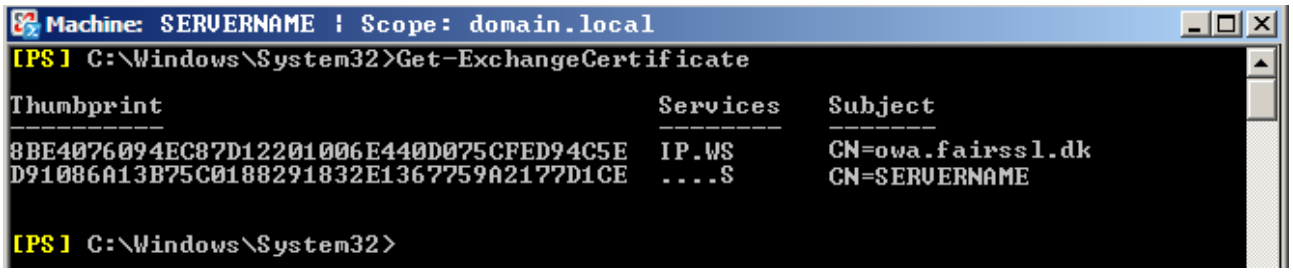
List alle certifikater installeret i Exchange 2010

Følgende viser alle installerede certifikater på Exchange 2010 serveren og hvilke som er aktive for de enkelte services.

I Exchange Management Shell, skriv følgende kommando efterfulgt af [ENTER]:

```
Get-ExchangeCertificate
```

Alle certifikater I Exchange vil nu blive listet med certifikatets Thumbprint, Services og Subject.



Tip: skriv `Get-ExchangeCertificate | fl` [ENTER] for at se flere informationer om de enkelte certifikater.

FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

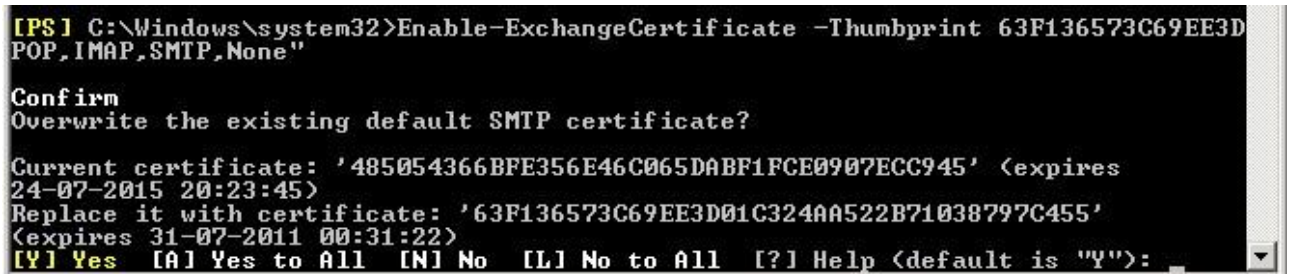
Aktiver certifikat for angivne services

Følgende beskriver hvordan et installeret certifikat aktiveres for en given service på Exchange 2010.

1. Log ind på den Exchange 2010 server som har certifikatet installeret. Benyt en konto som er medlem af "Exchange Administrators" gruppen samt "Administrators" gruppen på den lokale server.

2. Start Exchange Management Shell, højreklik på genvejen og vælg "Run as Administrator".

3. I Exchange Management Shell, skriv følgende kommando efterfulgt af [ENTER], hvor "-Thumbprint" angiver certifikatets ID og "-Services" angiver de ønskede services det skal aktiveres på:




```
Enable-ExchangeCertificate -Thumbprint <number> -Services IIS,
IMAP, SMTP, POP, UM, None
```

Bemærk kommandoen vil fejle, hvis der vælges services der ikke er installeret på serveren, vælg kun dem som skal anvendes. Typisk anvendes følgende på en normal Exchange installation:

```
Enable-ExchangeCertificate -Thumbprint <number> -Services IIS,
IMAP, SMTP, POP, None
```

4. Herefter skal der bekræftes at SMTP servicens certifikat skal erstattes, tryk [ENTER] for at acceptere.

FairSSL ApS
Kratbakken 6, 8586 Oerum Djurs
+45 77 345 678, info@fairssl.dk

Eksporter certifikat til backup fil (PKCS12)

Følgende beskriver hvordan man kan eksportere et installeret certifikat fra en Exchange 2010, den resulterende certifikat backup fil kan anvendes til at installere det samme certifikat på en anden server.

1. Log ind på den Exchange 2010 server som har certifikatet installeret. Benyt en konto som er medlem af "Exchange Administrators" gruppen samt "Administrators" gruppen på den lokale server.

2. Start Exchange Management Shell, højreklik på genvejen og vælg "Run as Administrator".

3. I Exchange Management Shell, skriv følgende kommando efterfulgt af [ENTER], hvor"-Thumbprint" angiver hvilket certifikat som skal exporteres:

   ```
   $file = Export-ExchangeCertificate –Thumbprint <number> -
   BinaryEncoded:$true -Password (Get-Credential).password
   ```

4. Der vises nu en prompt for brugernavn og password.
   Skriv "none" i brugerfeltet (anvendes ikke).
   Skriv det password som filen skal beskyttes med, efterfulgt af [ENTER]

   For at gemme certifikatet i en fil skriv følgende kommando, hvor "-Path" er stien til filen det skal gemmes i:

   ```
   Set-Content –Path "C:\mail.notyours.dk.pfx" –Value $file.FileData –
   Encoding Byte
   ```