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

Exchange 2007 SSL certifikat administration

Følgende vejledning beskriver hvordan man vælger hvilke adresser der skal være i ens Exchange 2007 SAN SSL certifikat. Derudover er der tekniske guides til at importere, eksportere, liste og aktivere certifikater i Microsoft Exchange 2007.

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, 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 1.3 – August 2010

GlobalSign. Gold 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 2007

Exchange 2007 (og Exchange 2010) 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.

Her vil vi kort gennemgå de mest typisk anvendte adresser der inkluderes i et Exchange 2007 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 en konfiguration 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.

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

Hvis der ikke er økonomi til at købe et SAN certifikat, kan en Exchange 2007 server sættes op til at fungere med kun en adresse som serveren tilgås fra internettet og lokalt. Det vil dog give følgende ulemper.

- Langt større og sværere konfiguration af miljøet
- Kræver en split DNS der gør det muligt at anvende samme servernavn internt og eksternt
- Autodiscover vil ikke virke eller give advarselsbeskeder til brugerne
- Vil kræve manuel konfiguration af eksterne klienter og mobile enheder

Det domæne navn som vælges til at tilgå serveren fra internettet og internt på det lokale netværk, skal være det navn som beskyttes i certifikatet. F.eks. ”**mail.fairssl.dk**”.

Det anbefales kraftigt at købe et SSL certifikat som understøtter mobile enheder, hvis der på et senere tidspunkt ønskes understøttelse af disse. F.eks. et AlphaSSL eller GeoTrust Premium SSL certifikat.

Vi anbefaler ikke denne løsning og har erfaring med at kunder der vælger løsningen, bruger uforholdsmæssigt mange timer på at få løsningen til at fungere korrekt.
Bemærk at Wildcard SSL certifikater ikke understøttes korrekt af Exchange 2007 og absolut ikke anbefales som certifikat til Exchange 2007/2010.

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.

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

Følgende adresser skal beskyttes i SSL certifikatet:

- **Mail.fairssl.dk**
- 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.

Small Business – Exchange 2007 på en Small Business Server 2008, med et aktivt e-mail domæne

Dette eksempel er for firmaer der kører Exchange 2007 på en Small Business Server 2008, med et aktivt e-mail domæne. Serveren i dette eksempel anvender følgende e-mail domæne "@fairssl.dk", den tilgås fra internettet på følgende adresser "remote.fairssl.dk/owa". Fra det lokale netværk tilgås serveren med adressen "exchsrv01.notyours.local" og/eller "sites". SBS2008 vil som standard være konfigureret til både det fulde interne servernavn og som en kort udgave med "sites". Hvis flere adresser anvendes til at tilgå serveren skal disse også tilføjes.

De fleste SBS2008 servere anvender sig af adressen remote.domæne.dk til at tilgå dens andre services fra internettet, derfor bør dette navn tilføjes, hvis disse services ønskes anvendt.

Følgende adresser skal beskyttes i SSL certifikatet:

- **Remote.fairssl.dk**
- Autodiscover.fairssl.dk
- Exchsrv01.notyours.local
- Sites

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:

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

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

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.

Generering af CSR til certifikat bestilling

Ved bestilling af et SSL certifikat til beskyttelse af en enkelt server adresse (FQDN) i Exchange 2007, 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.

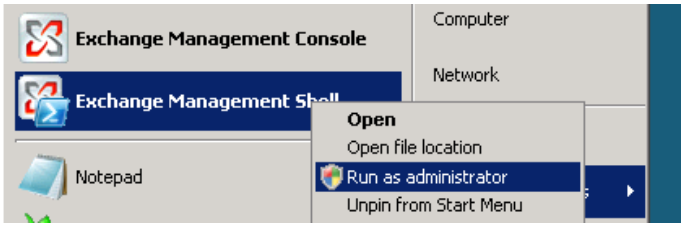
Bemærk at danske bogstaver og følgende tegn ikke normalt kan anvendes: > < ! @ # $ % ^ * ( ) ~ ? / \. &

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. Ææå skal udskiftes med tilsvarende AE/OE/AA eller A/O. (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 2007 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
   Er det en Windows Server 2008, højreklik da på genvejen og vælg "Run as Administrator".

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



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

   -SubjectName Firma oplysninger
   -KeySize 1024/2048 antallet af bits der anvendes til kryptering
   -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=www.fairssl.dk" -KeySize 2048 -DomainName autodiscover.fairssl.dk, mail.fairssl.dk, exchsrv01.notyours.local -Path c:\certificates\mail.fairssl.dk.req -privatekeyexportable $true
```

4. Du har nu lavet en certifikatansøgning som er blevet gemt i den tekstfil som du specificerede med ”-Path” værdien.

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

```
notepad c:\certificates\mail.fairssl.dk.req
```

6. 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/DG6GuD2hiIR7fQ0NtPFBQmbrSm+TTBo95lwP+
ZSZTusPFTLKaqValdnS9Uw+6Vq7/I4ouDA8QBIuaTFtPOp+8wEGBHQ==
-----END NEW CERTIFICATE REQUEST-----
```

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 2007 server. For at sikre at klienter kan godkende mellemudstedere i certifikatet, skal certifikatets mellemudstederes offentlige certifikat installeres på Exchange 2007 serveren. Ved modtagelse af et GlobalSign certifikat, vil du også modtage de offentlige certifikater for mellemudstederne.

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

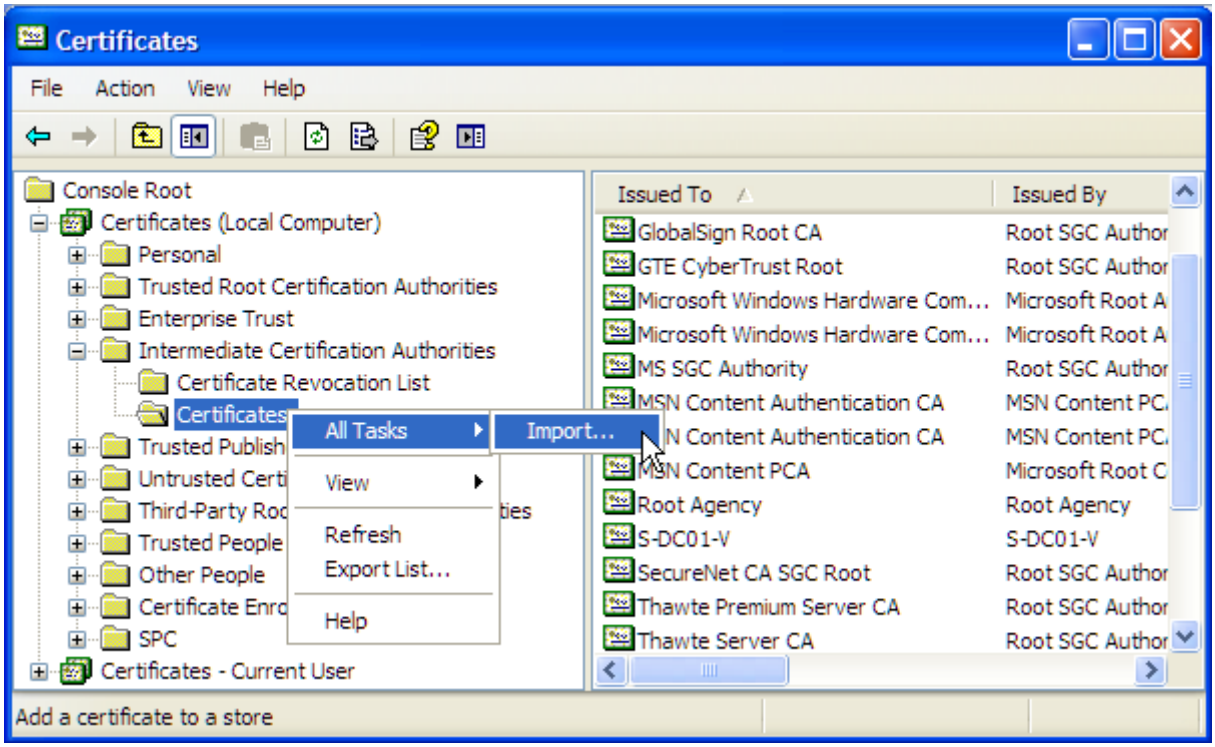
2. Kopier teksten med mellemudsteder certifikatet ("Intermediate certificate"), fra e-mailen med dit nye certifikat, til en simpel tekst editor (som Notepad). Gem filen på skrivebordet, med filnavnet "mellemudsteder.cer".

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.



Certifikatet 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 et certifikat installeres og aktiveres for services, efter at være udstedt fra en CSR du tidligere har lavet på samme server.

1. Log ind på den Exchange 2007 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
   Er det en Windows Server 2008, højreklik da 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 -Path c:\certificates\mycert.cer
   | Enable-ExchangeCertificate -Services "IIS, IMAP, SMTP, POP, UM,
   None"
   ```

   (bemærk UM servicen kan give fejl hvis ikke installeret, fjern UM fra listen efter behov)

4. Gå til Eksporter certifikat til backup fil, for at lave en backup af certifikatet og hvis nødvendigt installere på andre Exchange servere efterfølgende med backup filen.

*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 et certifikat installeres, efter at være udstedt fra en CSR du tidligere har lavet på samme server.

1. Log ind på den Exchange 2007 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
   Er det en Windows Server 2008, højreklik da 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 -Path c:\certificates\mycert.cer
   ```

4. Gå til Eksporter certifikat til backup fil, for at lave en backup af certifikatet og hvis nødvendigt installere på andre Exchange servere efterfølgende med backup filen.

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 2007. Ved bestilling af domæner med AutoCSR modtages certifikatet som en backup fil, beskyttet med en unik kode.

1. Log ind på den Exchange 2007 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
   Er det en Windows Server 2008, højreklik da 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 -Path c:\certificates\mycert.pfx
-Password (read-host "Password" -AsSecureString) | Enable-
ExchangeCertificate -Services IIS, IMAP, SMTP, POP, UM, None
```

4. Der vises nu en "Password:" prompt.
   Skriv det password som filen er beskyttet med, efterfulgt af [ENTER]

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 2007. Ved bestilling af domæner med AutoCSR modtages certifikatet som en backup fil, beskyttet med en unik kode.

1. Log ind på den Exchange 2007 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
   Er det en Windows Server 2008, højreklik da 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 -Path c:\certificates\mycert.pfx
   -Password (read-host "Password" -AsSecureString)
   ```

4. Der vises nu en "Password:" prompt.
   Skriv det password som filen er beskyttet med, efterfulgt af [ENTER]

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

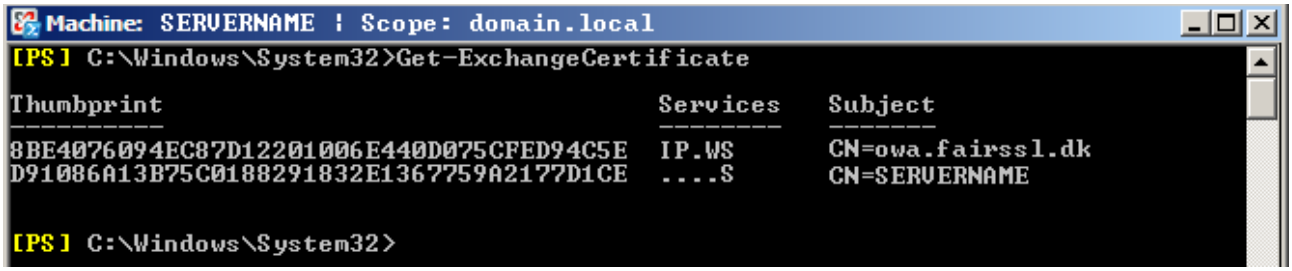
List alle certifikater installeret i Exchange 2007

Følgende viser alle installerede certifikater på Exchange 2007 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 2007.

1. Log ind på den Exchange 2007 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
   Er det en Windows Server 2008, højreklik da 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 funktioner:

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

Eksporter certifikat til backup fil (PKCS12)

Følgende beskriver hvordan man kan eksportere et installeret certifikat fra en Exchange 2007, den resulterende certifikat backup fil kan anvendes til at installere det samme certifikat på en anden server.

1. Log ind på den Exchange 2007 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
   Er det en Windows Server 2008, højreklik da på genvejen og vælg "Run as Administrator".

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

```
Export-ExchangeCertificate –Thumbprint <number> -Path
c:\certificates\mycert.pfx
-Password (read-host "Password" -assecurestring)
```

4. Der vises nu en "Password:" prompt.
   Skriv det password som filen skal beskyttes med, efterfulgt af [ENTER]