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

Apache SSL certifikat administration

Følgende vejledning beskriver hvordan SSL administrationsopgaver for Apache med udføres med OpenSSL.

Denne vejledning kan anvendes til at bestille og installere certifikater, med og uden AutoCSR og eksportere og importere SSL certifikat backup filer.

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 eller kontakt os på info@fairssl.dk.

Indholdsfortegnelse

Version 1.1 – Februar 2012

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 Apache, uden brug af AutoCSR, kræves en generering af en CSR kode samtidigt med at den private nøgle oprettes på serveren.

Bemærk at oprettelse af CSR til et SAN SSL certifikat, kræver flere ændringer i openssl.cnf og manuel tilføjelse af SAN navnene heri. Vi anbefaler at oprette SAN SSL certifikater til Apache med AutoCSR for at undgå problemer, alternativt kontakt os for yderligere information på support@fairssl.dk.

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 kan anvendes: > < ! @ # $ % ^ * ( ) ~ ? \. &

Common Name (CN): *Det primære fulde internet domæne navn på din Apache server. (eks. mail.fairssl.dk)*	
Organization Name (O): *Det fulde gyldige navn på virksomheden inkl. evt. endelse, eller personen der bestiller certifikatet. (eks. Not Yours ApS)*	
Department (OU): *Afdelingen, eller lignende beskrivende del af virksomheden. (eks. FairSSL eller IT)*	
Stat/region (S): *Stat eller region, i Danmark kan DK anvendes. (eks. DK)*	
Country (C): *ISO standard to bogstavs landekode. (eks.for Danmark, vælg DK)*	
Locality (L): *By.* *(eks. Oerum Djurs)*	

Der er tre trin i oprettelsen og installationen af et certifikat:

1. Oprettelse af privat nøgle
2. Oprettelse af CSR (Certifikat Signing Request)
3. Installation af Certifikatet

For generel information om certifikater og SSL, se
http://www.fairssl.dk/vejledninger/hvad-er-ssl-certifikater/

For både oprettelse af den private nøgle og CSR forespørgslen, beskriver vi her anvendelsen af OpenSSL værktøjet. OpenSSL værktøjet er som standard installeret under /usr/local/ssl/bin, hvis du har en standard installation.

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

Oprettelse af privat nøgle

1. Log ind på serveren med root adgang og opret en mappe, hvor SSL certifikat filerne for serveren skal placeres, dette sted skal være tilgængeligt for Apache serveren. Gå herefter til denne mappe.

2. For at oprette en privat nøgle anvendes følgende kommando:
   ```
   openssl genrsa –out www.mitdomain.dk.key 2048
   ```
   Denne kommando vil lave en 2048bit RSA privat nøgle, uden beskyttelse af en kode. Ønskes en kode på den private nøgle anvend i stedet følgende kommando og indtast efterfølgende den ønskede kode, når forespurgt på denne.
   ```
   openssl genrsa –des3 –out www.mitdomain.dk.key 2048
   ```

3. Sørg for at gemme den private nøgle et sikkert sted, den er krævet for at webserveren senere skal kunne anvende SSL certifikatet som du får udstedt.

Oprettelse af CSR

4. Indtast følgende kommando for at oprette en CSR til ovenstående private nøgle:
   ```
   openssl req –new –key www.mitdomain.dk.key –out
   www.mitdomain.dk.csr
   ```

   Hvis du udfører denne kommando på en Windows Server og får en fejl, anvend i stedet følgende kommando:
   ```
   openssl req –new –key www.mitdomain.dk.key –out
   www.mitdomain.dk.csr –config openssl.cnf
   ```

5. Hvis du valgte at sikre nøglen med en kode, vil du blive promptet for denne nu og skal indtaste den valgte kode.

6. Indtast de informationerne du tidligere indsamlede for certifikatet, husk at du ikke må anvende ÆØÅ eller special tegn. Derudover skal du ikke indtaste noget for de sidste 3 felter, se følgende eksempel.:
   ```
   Country Name: DK
   State or Province Name: DK
   Locality Name: Copenhagen
   Organization Name: Mit Firma A/S
   Organizational Unit Name: IT
   Common Name: www.mitdomain.dk
   Email Address:
   A challenge password:
   An optional company name:
   ```

7. Du kan nu bekræfte at din CSR er oprettet korrekt med følgende commando:
   ```
   openssl req –noout –text –in www.mitdomain.dk.csr
   ```

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

8. Åben www.mitdomain.dk.csr filen, med din foretrukne tekst editor, kopier hele teksten fra CSR filen, inklusive start og slut tags. 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-----
```

Installer dit SSL certifikat på en Apache 1.x server

Følgende beskriver hvordan du på en Apache webserver, installerer dit SSL certifikat og mellemudsteder "intermediate certificate" når du modtager dette.

1. Log ind på serveren med en konto der har root adgang til serveren.

2. Opret en tekst fil med navnet "www.mitdomain.dk.crt" og indsæt teksten fra e-mailen med dit SSL certifikat, inkl. start og slut tags.

3. Opret en tekst fil med navnet "intermediate.pem" og indsæt teksten fra certifikats mellemudsteder certifikat (intermediate certificate).

4. Åben din webservers konfigurations fil, f.eks. httpd.conf, ssl.conf, eller lignende fil der indeholder dit websites konfiguration. Find og rediger virtual host sektionen og tilføj følgende parametre for at pege på SSL certifikat filerne:

```
SSLEngine On
SSLCertificateChainFile /fulde/sti/ssl-filer/intermediate.pem
SSLCertificateFile /fulde/sti/ssl-filer/www.mitdomain.dk.crt
SSLCertificateKeyFile /fulde/sti/ssl-filer/www.mitdomain.dk.key
```

5. Det kan også være nødvendigt at tilføje andre parametre for at aktivere SSL på serveren, bl.a. skal serveren lytte på port 443. Følgende er et eksempel fra en Ubuntu server med Apache2 SSL

```
SSLEngine On

<IfModule mod_ssl.c>
```

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

```
    # SSL name based virtual hosts are not yet supported, therefore
no NameVirtualHost statement here
    Listen 443
</IfModule>
```

6. Gem ændringerne og genstart Apache.

Installer dit SSL certifikat på en Apache 2.x server

Følgende beskriver hvordan du på en Apache webserver, installerer dit SSL certifikat og mellemudsteder "intermediate certificate" når du modtager dette.

1. Log ind på serveren med en konto der har root adgang til serveren.

2. Opret en tekst fil med navnet "www.mitdomain.dk.crt" og indsæt teksten fra e-mailen med dit SSL certifikat, inkl. start og slut tags.

3. Opret en tekst fil med navnet "intermediate.pem" og indsæt teksten fra certifikats mellemudsteder certifikat (intermediate certificate).

4. Opret en tekst fil med navnet "ca_root.pem" og indsæt teksten fra certifikats rodudsteder certifikat (root certificate).

5. Åben din webservers konfigurations fil, f.eks. httpd.conf, ssl.conf, eller lignende fil der indeholder dit websites konfiguration. Find og rediger virtual host sektionen og tilføj følgende parametre for at pege på SSL certifikat filerne:

```
SSLCACertificateFile /fulde/sti/ssl-filer/ca_root.pem
SSLCertificateChainFile /fulde/sti/ssl-filer/intermediate.pem
SSLCertificateFile /fulde/sti/ssl-filer/www.mitdomain.dk.crt
SSLCertificateKeyFile /fulde/sti/ssl-filer/www.mitdomain.dk.key
```

6. Det kan også være nødvendigt at tilføje andre parametre for at aktivere SSL på serveren, bl.a. skal serveren lytte på port 443. Følgende er et eksempel fra en Ubuntu server med Apache2 SSL

```
SSLEngine On
<IfModule mod_ssl.c>
    # SSL name based virtual hosts are not yet supported, therefore
    no NameVirtualHost statement here
    Listen 443
</IfModule>
```

7. Gem ændringerne og genstart Apache.

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

Hent mellemudsteder og rodcertifikater for dit certifikat

Her er links til at hente mellemudsteder og rodcertifikater til nogle af vores certifikater.

GlobalSign:

Domain validated
Rod certifikat:
http://www.globalsign.com/support/root-certificate/root-globalsign.php

Mellemudsteder certifikat:
http://www.globalsign.com/support/intermediate/domainssl_intermediate.php

Organization validated
Rod certifikat:
http://www.globalsign.com/support/root-certificate/root-globalsign.php

Mellemudsteder certifikat:
http://www.globalsign.com/support/intermediate/organizationssl_intermediate.php

Extended validated
Rod certifikat:
http://www.globalsign.com/support/root-certificate/root-globalsign-rc2.php

Mellemudsteder certifikat:
http://www.globalsign.com/support/intermediate/extended_bundle.php

AlphaSSL rod og mellemudsteder certifikat
Rod og mellemudsteder certifikater:
http://www.alphassl.com/support/install-root-certificate.html

GeoTrust
Rod og mellemudsteder certifikater:
https://www.geotrust.com/resources/root-certificates/

Verisign & Thawte
Rod og mellemudsteder certifikater:
http://www.verisign.com/support/roots.html

RapidSSL
Rod og mellemudsteder certifikater:
http://www.rapidssl.com/legal/