SSL Certifikat med Apache webserver

Krypter dine formdata med et unikt SSL certifikat - her er guiden. Apache 1.3+ - med Linux (kan bruges på Windows).

Skrevet den **03. Feb 2009** af **blaz** I kategorien **Webservere / Apache** | ★★☆☆☆

Denne SSL opsætnings artikel lærer dig hvordan man generer og opsætter et SSL certifikat.
Jeg regner med at du har en kørende Apache webserver før du går igang med denne artikel, ellers bliver det jo ikke til meget :)
Denne artikel kræver også at du har en del kendskab til Apache da artiklen ikke er tilegnet nybegyndere.
Bemærk: de forskellige links til dine destinationer kan variere, dette afhænger af om du har ændret i dine mappenavne. Et SSL certifikat er platformsuafhængigt, det vil sige at det kan køre på alle platforme.
Denne artikel er skrevet til Linux, men kører udemærket på Windows platformen.

Hvad er SSL?

SSL er en perfekt måde at kryptere sine form data på. Som du måske har erfaret, kan man kryptere eller "dekode" sine data ved hjælp af PHP.
Dvs., hvis nogen kigger med; vil de ikke have egenskaber til at forstå koden. Hvis jeg skriver "Blaz" i en form, vil den returnere noget i stil med "50923a@". Dette kan sammenlignes med PHP's base_64, bare i sådan et format at den krypterer alt formdata.

Generering af RSA & CSR (Underskrivelses forespørgsel)

```
[root@blaz root]#
[root@blaz root]# cd /etc/httpd/conf/ssl.key
```

VALG 1: Generering af RSA private key uden et passphrase

```
[root@blaz /etc/httpd/conf/ssl.key]# openssl genrsa -out mitdomæne.dk.key 1024
```

VALG 2: Generering af RSA private key MED passphrase. (Du vil blive mindet om at indtaste lige efter du trykker enter =)

```
[root@blaz /etc/httpd/conf/ssl.key]# openssl genrsa -des3 -out mitdomæne.dk.key
1024
```

Bemærk: *Det er dumt IKKE at generere RSA private key'en med et passphrase hvis du har scripts som genstarter Apache automatisk.*
Hvis du har, vil Apache vente på scriptet til at inputte passphraset som i den sidste ender laver meget rod Der er en metode så du kan undlade passphraset til at påminde dig når du genstarter Apache (det vil jeg vise senere).

Næste: *Vi genererer CSR'en med RSA private key'en*

```
[root@blaz /etc/httpd/conf/ssl.csr]# openssl req -new -key mitdomæne.dk.key -out
```

```
mitdomæne.dk.csr
[root@blaz /etc/httpd/conf/ssl.csr]# mv mitdomæne.dk.csr ../ssl.csr
```

Herefter vil du blive bedt om at indtaste dit navn, by, E-mail og blablabla.
Disse tegn vil ikke blive accepteret, så indtast dem ikke!
Tegn: < > ~ *! @ # $ % ^ * / ( ) ?.,&.*

Dette er det som du vil blive bedt om at udfylde, så jeg hjælper dig på vej:

Common Name: domænet for serveren (mitdomæne.dk)
Organization: navnet på din "organisation" (fx. Blaz)
Organization Unit: beskæftigelse af "organisationen" / firmaet (fx. salg)
Resten skulle vel ikke være noget problem.

Du vil nu blive spurgt om "emeow" adressen og et password, jeg plejer at trykke enter når jeg generer csr'en.

Nu skulle du gerne have:

```
/etc/httpd/conf/ssl.key/mitdomæne.dk.key
/etc/httpd/conf/ssl.csr/mitdomæne.dk.csr
```

Husk at tage backup af din private key! Hvis du mister den skal du igennem en længere procedure for at genvinde den.
Du skal du sende forespørgslen og de vil maile dig certifikatet.
Bemærk: *E-Mail adressen er den som du indtastede ved din renerering af din private key.*

Installeringen af certifikatet til Apache.

```
[root@blaz root]# cd /etc/httpd/conf/ssl.crt
```

Kopier certifikatet som de mailede til dig, åben din httpd.conf fil og placer dette i din virtualhost.

```
<VirtualHost 123.456.789.123:443>
SSLEngine  on
SSLCertificateFile /etc/httpd/conf/ssl.crt/mitdomæne.dk.crt
SSLCertificateKeyFile /etc/httpd/conf/ssl.key/mitdomæne.dk.key
</VirtualHost>
```

Genstart Apache

```
Valg 1: [root@blaz /etc/httpd/conf/ssl.crt]# apachectl restart
Valg 1: (hvis vi bruger sh scriptet) [root@blaz /etc/httpd/conf/ssl.crt]#
/etc/rc.d/init.d/httpd restart
```

Du vil måske blive spurgt om at indtaste passphraset hvis du har genereret RSA'en med et passphrase.Hvis ikke du vil spørges om dette, når du genstarter apache skal du re-generere din RSA key fil.

```
[root@blaz /etc/httpd/conf/ssl.crt]# cd ../ssl.key
[root@blaz /etc/httpd/conf/ssl.key]# mv mitdomæne.dk.key mitdomæne.dk.key.has-
passphrase
[root@blaz /etc/httpd/conf/ssl.key]# openssl rsa -in mitdomæne.dk.key.has-
passphrase -out mitdomæne.dk.key
```

Genstart nu Apache igen

```
[root@blaz /etc/httpd/conf/ssl.crt]# /etc/rc.d/init.d/httpd restart
```

Nu skulle du gerne have mulighed for at gå ind på https://mitdomæne.dk for at sikre dig at mapperne og filerne kun er write og readable af root.

Tillykke - du har nu opsat dit eget SSL certifikat =) Jeg håber du fik udbytte af denne artikel og du fik det hele til at virke.

Læs mere om SSL på http://httpd.apache.org/docs-2.1/ssl/.

Blaz - blaz.users.whitehat.dk

Kommentar af the_email d. 30. Jan 2005 | 1

Citat start Kopier certifikatet som de mailede til dig, åben din httpd.conf fil og placer dette i din virtualhost. Citat slut Hvem er det som mailer et certifikat til mig? Ellers interesseant artikel som kommer yderst belejligt for mit vedkommende

Kommentar af per-olof d. 12. Aug 2006 | 2

Gratis https://www.cacert.org/ De andre som "mailer et certifikat til mig" tar $$ før det. God og letbegribelig artikel

Kommentar af alister_crowley d. 29. Jan 2005 | 3

god, men synes ikke at kunne se hvor du requester certifikatet henne. (er windåse bruger)