

Instrucțiuni pentru obținerea unui certificat de server pentru APACHE (Secure Server ID's sau Global Server ID's)

1. Generarea fișierului CSR (Certificate Signing Request)

Pentru a genera cheia privată și crearea fișierului CSR trebuie să aveți executabilul *openssl*. Acesta poate fi instalat de la adresa:

- <http://www.openssl.org/source/> (OpenSSL) in cazul in care sistemul dumneavoastră este *nix sau linux
- <http://www.modssl.org/contrib/> (OpenSSL + ModSSL) in cazul in care sistemul dumneavoastră este Windows

Va rugam sa citiți documentația de pe aceste site-uri in vederea instalării OpenSSL.

Pentru generarea perechii de chei publica/privata (si implicit a cererii de semnare a certificatului - CSR) va localizați in directorul `/etc/httpd/conf`. Tastați apoi comanda: *make numecertificat.csr*

Scriptul va genera cheia privata a certificatului care va fi protejata de o parola.

Atenție: Nu uitați această parolă deoarece cheia nu va putea fi folosită. Aceasta parola trebuie folosita in cazul repornirii serverului respective a serviciului httpd !

Scriptul va genera in continuare fișierul CSR (certificate signing request) , care va fi trimis la Verisign pentru a fi semnat și se va întoarce sub forma unui certificat pe care-l veți putea utiliza împreună cu cheia privată pe care ați generat-o.

ATENȚIE ! *Datele solicitate la generarea CSR trebuie sa corespunda exact cu cele din formularul de înregistrare.*

Fișierul de ieșire este *numecertificat.csr* unde se generează CSR. Vă vor fi solicitate următoarele informații:

- codul de țară: veți introduce doar abrevierea (ex: MX pentru Mexic, RO pentru România);
- numele întreg al statului sau provinciei: veți introduce numele complet și nu abrevierea;
- numele orașului sau localității;
- numele companiei: compania trebuie să fie deținătoarea domeniului înscris în pasul 1 al procesului de înregistrare și trebuie să aibă dreptul de utilizare a acestuia conform pasului 2 din procesul de înregistrare;
- numele departamentului: (ex: Marketing, Vânzări, etc.);
- numele calificat al domeniului: ex: www.story.com – trebuie să fie identic cu URL https pe care îl veți utiliza;

Fișierul *numecertificat.csr* va arăta sub forma:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBETCBvAIBADBXMqSwCQYDVQQGEwJBVTETMBEGA1UECBMKU29tZ
S1TdGF0ZTEhMB8GA1UEChMYSW50ZXJuzXQgV2lkZ210cyBQdHkgTHRkMR
AwDgYJKoZIhvcNAQkgMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAL6nPT
y3avNgbubx+ESmD4LV1LQGfcSh8nehEOIxGwmCPlrhTP87PaA0XvGpvRQUj
```

CGStrlQsd8lcYVVkOaytNUCAwEAAaAAMA0GCSqGSIb3DQEBAUAA0EAXc
Msa8eXgbG2ZhVyFkRvrI4vhaN39/QJc9BrRh2nOTKgfMcT9h+1Xx0wNRQ9/SIG
V1y3+3abNiJmJBWnJ8Bg==
-----END CERTIFICATE REQUEST-----

2. Procesul de înregistrare

Pentru obținerea unui certificate de server va rugam sa ne [contactati](#).

3. Instalarea certificatului de server

Veți primi ulterior un mesaj de e-mail în care vi se confirmă aprobarea certificatului de server, mesaj ce conține câteva link-uri și un cod de forma:

-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBYDCCATECAQAwwYgxCzAJBgNVBAYTAIVTMREwDwYDVQQIEwhWaXJnaW5pYTEQMA4GA1UEBxMHUUm9hbm9rZTEemMCQGA1UEChMdTmV3IENlbnR1cnkgVGVjaG5vbG9zIEluYy4xDzANBgNVBAsTBk5DVGlueZEBMBkGA1UEAxQSd3d3Lm5ld2NlbnRlY2guY29tMIGeMA0GCSqGSIb3DQEBAQUAA4GMADCBiAKBgFHDQ2up+9Z06F8pVfC9R0oj0A8fX6mLdc66JhUv6QGleJ37lLciLpgvDwvg+Tyi5uThrua+B2zmgMnpr0AkpN2nqIe0inHTR29vcbjUNiMSkaxZHN/NQISSKwQbCB9d6TJBURzGGfULpSF8dhlTfcI4krbEE9TY/r1/kCGmnSBAGMBAAGgADANBgkqhkiG9w0BAQQFAAOBgQAgOn0at410ohHnKEzVgElu0a1w10AL37qXgJIBflnLD+7C0h8UKOUFPyrC2DBwP3kKzGRFDLJiwshV3yPuGMOaqYcTLB8/DK553TyuLR2Fiftr4oxKZ6wT8D8v38a1s1D+1owU20CbzA7Ur0YBqrmQdD2PnTv/XpHtAAr+M4oez==MIIBYDCCATECAQAwwYgxCzAJBgNVBAYTAIVTMREwDwYDVQQIEwhWaXJnaW5pYTEQMA4GA1UEBxMHUUm9hbm9rZTEemMCQGA1UEChMdTmV3IENlbnR1cnkgVGVjaG5vbG9zIEluYy4xDzANBgNVBAsTBk5DVGlueZEBMBkGA1UEAxQSd3d3Lm5ld2NlbnRlY2guY29tMIGeMA0GCSqGSIb3DQEBAQUAA4GMADCBiAKBgFHDQ2up+9Z06F8pVfC9R0oj0A8fX6mLdc66JhUv6QGleJ37lLciLpgvDwvg+Tyi5uThrua+B2zmgMnpr0AkpN2nqIe0inHTR29vcbjUNiMSkaxZHN/NQISSKwQbCB9d6TJBURzGGfULpSF8dhlTfcI4krbEE9TY/r1/kCGmnSBAGMBAAGgADANBgkqhkiG9w0BAQQFAAOBgQAgOn0at410ohHnKEzVgElu0a1w10AL37qXgJIBflnLD+7C0h8UKOUFPyrC2DBwP3kKzGRFDLJiwshV3yPuGMOaqYcTLB8/DK553TyuLR2Fiftr4oxKZ6wT8D8v38a1s1D+1owU20CbzA7Ur0YBqrmQdD2PnTv/XpHtAAr+M4oez==
-----END NEW CERTIFICATE REQUEST-----

Veți copia acest text (inclusiv prima linie “-----BEGIN NEW CERTIFICATE REQUEST-----” și ultima linie “-----END NEW CERTIFICATE REQUEST-----”) într-un fișier cu extensia *crt*, de exemplu *numecertificat.crt*

Următoarele linii din fișierul de configurare *httpd.conf* (sau *ssl.conf* în funcție de versiunea de Apache) trebuie să fie necomentate iar căile să corespundă:

SSLCertificateFile /etc/httpd/conf/ssl.crt/*numecertificat.crt*

SSLCertificateKeyFile /etc/httpd/conf/ssl.key/*numecertificat.key*

Se repornește serverul Apache cu “*apachectl stop*” și apoi “*apachectl start*”.

In momentul pornirii serverului httpd se introduce parola cheii private (pe care ați generat-o în momentul generării cheii private și a cererii de semnare csr).

Atenție: La fiecare repornire a demonului httpd se furnizează această parolă.

Atenție: Trebuie setate cu atenție drepturile fișierului *numecertificat.key* deoarece de siguranța acestuia depinde siguranța identității serverului. (chown root:root, chmod 600).