

Instructions for obtaining APACHE server certificates (Secure Server IDs or Global Server IDs)

1. Generating the CSR (Certificate Signing Request) file

In order to generate the private key and create the CSR file, you need the *openssl* exe. It is available for download at:

- <http://www.openssl.org/source/> (OpenSSL) for *nix or linux systems
- <http://www.modssl.org/contrib/> (OpenSSL + ModSSL) for Windows systems

Please read the documentations on these sites in order to install OpenSSL.

To generate the public/private keys pair (and implicitly the certificate signing request - CSR) you need to open the `/etc/httpd/conf` directory. Then, enter: *make numecertificat.csr*

The script will generate the private key of the certificate, which will be password-protected.

Warning: Remember this password because you will not be able to use the key otherwise. This password has to be used if the server, respectively the httpd service are restarted!

The script will then generate the CSR (certificate signing request) file, which will be sent to Verisign to be signed and will return under the form of a certificate that you can use together with the generated private key.

WARNING ! *The data requested upon the generation of the CSR must be an exact match of the ones in the registration.*

The exit file is *numecertificat.csr* where CSR is generated. The following data will be requested:

- country code: enter abbreviation only (ex: MX for Mexico, RO for Romania);
- full name of the state or province: enter full name, not abbreviation;
- name of the town or locality;
- company's name: the company must be the holder of the domain entered in the 1st step of the registration process and must hold the right to use it according to step 2 in the registration process;
- department name: (e.g.: Marketing, Sales, etc.);
- qualified domain name: e.g.: www.story.com – needs to be identical with the URL https you will use;

The format of the *numecertificat.csr* will be:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBETCBvAIBADBXMqswCQYDVQQGEwJBVTETMBEGA1UECBMKU29tZ
S1TdGF0ZTEhMB8GA1UEChMYSW50ZXJlZXRuZXQgV2lkZ2l0cyBQdHkgTHRkMR
AwDgYJKoZIhvcNAQkGMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAL6nPT
y3avNgubx+ESmD4LV1LQGfcSh8nehEOIxGwmCPlrhTP87PaA0XvGpvRQUj
```

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

2. Registration process

To obtain a server certificate please [contact us](#).

3. Installing a server certificate

You will then receive an e-mail message confirming the server certificate approval, a message including a few links and a code under the following form:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBYDCCATECAQAwwYgx CzAJBgNVBAYTAIVTMREwDwYDVQQIEwhWaXJna
W5pYTEQMA4GA1UEBxMHUum9hbm9rZTEuMCQGA1UEChMdTmV3IENlbnR1cn
kgVGVjaG5vbG9zIEluYy4xDzANBgNVBAsTBk5DVGlueEYzEjMBkGA1UEAx
QSd3d3Lm5ld2NlbnRlY2guY29tMIGeMA0GCSqGSIb3DQEBAQUAA4GMADCBi
AKBgFHdQ2up+9Z06F8pVfC9R0oj0A8fX6mLdc66JhUv6QGleJ37lLciLpgv
Dwvvg+Tyi5uThrua+B2zmgMnpr0AkpN2nqIe0inHTR29vcbjUNiMSkaxZHN
/NQISSKwQbCB9d6TJBUErzGGfULpSF8dhlTfcI4krbEE9TY/r1/kCGmnSB
AgMBAAGgADANBgkqhkiG9w0BAQQFAAOBgQAgOn0at410ohHnKEzVgElu0a
1w10AL37qXgJIBflnLD+7C0h8UKOUFPyrC2DBwP3kKzGRFDLJiwshV3y
PuGMOaqYcTLB8/DK553TyuLR2Fiftr4oxKZ6wT8D8v38a1s1D+1owU20Cb
zA7Ur0YBqrnQdD2PnTv/XpHtAAr+M4oez==MIIBYDCCATECAQAwwYgx Cz
AJBgNVBAYTAIVTMREwDwYDVQQIEwhWaXJnaW5pYTEQMA4GA1UEBxMHUum9
hbm9rZTEuMCQGA1UEChMdTmV3IENlbnR1cnkgVGVjaG5vbG9zIEluYy4xDz
ANBgNVBAsTBk5DVGlueEYzEjMBkGA1UEAxQSd3d3Lm5ld2NlbnRlY2guY2
9tMIGeMA0GCSqGSIb3DQEBAQUAA4GMADCBiAKBgFHdQ2up+9Z06F8pVfC9R
0oj0A8fX6mLdc66JhUv6QGleJ37lLciLpgvDwvvg+Tyi5uThrua+B2zmgMn
pr0AkpN2nqIe0inHTR29vcbjUNiMSkaxZHN/NQISSKwQbCB9d6TJBUErzGG
fULpSF8dhlTfcI4krbEE9TY/r1/kCGmnSBAgMBAAGgADANBgkqhkiG9w0BA
QQFAAOBgQAgOn0at410ohHnKEzVgElu0a1w10AL37qXgJIBflnLD+7C0h8
UKOUFPyrC2DBwP3kKzGRFDLJiwshV3yPuGMOaqYcTLB8/DK553TyuLR2Fi
ftr4oxKZ6wT8D8v38a1s1D+1owU20CbzA7Ur0YBqrnQdD2PnTv/XpHtAAr
+M4oez==
-----END NEW CERTIFICATE REQUEST-----
```

You will copy this text (including the first line “-----BEGIN NEW CERTIFICATE REQUEST-----” and the last one “-----END NEW CERTIFICATE REQUEST-----”) in a *crt* file, e.g. *numecertificat.crt*

The following lines of the *httpd.conf* (or *ssl.conf*, depending on the Apache version) setup file need to include no comments, and the paths have to match:

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

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

Restart the Apache server using “*apachectl stop*” and then “*apachectl start*”.

When restarting the *httpd* server, insert the private key password (generated upon the creation of the private key and of the *csr*).

Warning: Upon each httpd restart, the password is requested.

Warning: You need to carefully set the *numecertificat.key* file rights as the server identity security depends on the file's security level.(chown root:root, chmod 600).