Authentication based on certificates on Apache server,
Redhat distribution

After installing the server certificate the following steps are followed:

Download the DIGISIGN root certificate from the address : http://www.digisign.ro/certs/DIGISIGNTRUSTEDSERVICESCA.cer and rename it with the extension .crt. (ex. digisigntrustca.crt).

Copy into the folder /etc/httpd/conf/ssl.crt

In the file httpd.conf (or in ssl.conf depending on Apache version) set the following sections and the name must correspond:
SSLCACertificatePath /etc/httpd/conf/ssl.crt
SSLCACertificateFile /etc/httpd/conf/ssl.crt/digisigntrustca.crt

In the section of authentication module the following variants can be selected:
None – no authentication is wanted;
Optional – authentication made also based on certificate, if any;
Require – authentication made based on certificate only;
SSLVerifyClient require;
SSLVerifyDepth 2;

The last section to be present refers to the list of revoked certificates. Download the file LatestCRL.crl from the address :
http://crl.adacom.com/DIGISIGNSASecurityServices/LatestCRL.crl
This file must be transformed into PEM (character) variant in order to be accepted by the module Apache mod_ssl with the following command:
"openssh crl -inform DER -in LatestCRL.crl -out fisier.crl" and then it is copied into the folder /etc/httpd/conf/ssl.crl.

The path is set to the .crl file:
SSLCARevocationPath /etc/httpd/conf/ssl.crl
SSLCARevocationFile /etc/httpd/conf/ssl.crl/fisier.crl

Finally, restart the service httpd. with apachectl stop, apachectl start or other command.

The rights of the files above must be 644 and held by root.

Recommendation: crl file must be renewed as often as possible (on daily basis if possible with a script with wget and openssl: the command of transforming the crl must be executed each time) in order to reflect as accurate as possible the certificates status.