

Autentificarea pe baza de certificate pe serverul Apache, distribuție Redhat.

După instalarea certificatului de server se efectuează pașii următori:

Se face download la certificatului de root DIGISIGN de la adresa

<http://www.digisign.ro/certs/DIGISIGNTRUSTEDSERVICESCA.cer>, si se redenumeste cu extensia crt. (ex. digisigntrustca.crt).

Se copiază in directorul `/etc/httpd/conf/ssl.crt`.

In fișierul `httpd.conf` (sau in `ssl.conf` in funcție de versiunea de Apache) se setează secțiunile următoare iar numele trebuie sa corespunda:

`SSLCACertificatePath /etc/httpd/conf/ssl.crt`

`SSLCACertificateFile /etc/httpd/conf/ssl.crt/digisigntrustca.crt`

La secțiunea modului de autentificare se pot alege variantele:

None - când nu se dorește autentificare.

Optional – autentificarea se face si pe baza de certificat daca exista.

Require – autentificarea se face numai pe baza de certificat.

`SSLVerifyClient require`

`SSLVerifyDepth 2`

Ultima secțiune care trebuie sa fie prezenta se refera la lista certificatelor revocate.

Se face download la fișierul `LatestCRL.crl` de la adresa

<http://crl.adacom.com/DIGISIGNSA SecurityServices/LatestCRL.crl>

Acest fișier trebuie transformat in varianta PEM (character) pentru a fi acceptat de modulul Apache `mod_ssl` cu următoarea comanda:

`“openssl crl -inform DER -in LatestCRL.crl -out fisier.crl”` si apoi si se copiază in directorul `/etc/httpd/conf/ssl.crl`.

Se setează calea către fișierul `crl`:

`SSLCARevocationPath /etc/httpd/conf/ssl.crl`

`SSLCARevocationFile /etc/httpd/conf/ssl.crl/fisier.crl`

In final se restarteaza serviciul `httpd`. cu `apachectl stop`, `apachectl start` sau alta comanda.

Drepturile fișierelor de mai sus trebuie sa fie 644 si deținute de root.

Recomandare: fișierul `crl` trebuie reînnoit cat mai des cu puțința (recomandam zilnic cu un script cu `wget` si `openssl` : comanda de transformare a `crl`-ului trebuie executata de fiecare data) pentru a reflecta cat mai bine situația certificatelor.