Raport pentru lucrarea 6: Infrastructura de chei publice (PKI)

Autor: Birlutiu Claudiu-Andrei

Sarcina 1: Deveniți o autoritate de certificat (CA)

- În prima faza am creat containerul și am pornit acest serviciu

```
 ---> 2c046310435d
Step 3/7 : COPY ./index.html ./index_red.html $WWWDIR/
 ---> Using cache
 ---> 0a307bbf2797
Step 4/7 : COPY ./bank32_apache_ssl.conf /etc/apache2/sites-available
 ---> Using cache
 ---> fdc2b914bf37
Step 5/7 : COPY ./certs/bank32.crt ./certs/bank32.key  /certs/
 ---> Using cache
 ---> eafa76b546fe
Step 6/7 : RUN  chmod 400 /certs/bank32.key      && chmod 644 $WWWDIR/index.html      &&
chmod 644 $WWWDIR/index_red.html      && a2ensite bank32_apache_ssl
 ---> Using cache
 ---> ead4e1d3c001
Step 7/7 : CMD  tail -f /dev/null
 ---> Using cache
 ---> dc3190c196bb

Successfully built dc3190c196bb
Successfully tagged seed-image-www-pki:latest
[04/21/23]seed@VM:~/.../BirlutiuClaudiu_Cod$ dcup
Starting www-10.9.0.80 ... done
Attaching to www-10.9.0.80
```

- Am adaugat în /etc/hosts cele 2 intrari

```
# For XSS Lab
10.9.0.5        www.xsslabelgg.com
10.9.0.5        www.example32a.com
10.9.0.5        www.example32b.com
10.9.0.5        www.example32c.com
10.9.0.5        www.example60.com
10.9.0.5        www.example70.com

# For CSRF Lab
10.9.0.5        www.csrflabelgg.com
10.9.0.5        www.csrflab-defense.com
10.9.0.105      www.csrflab-attacker.com

# For Shellshock Lab
10.9.0.80       www.seedlab-shellshock.com
#For L06 lab
10.9.0.80 www.bank32.com
10.9.0.80 www.birlutiu2023.com

~
"/etc/hosts" 35L, 848C                                    34,30         All
```

- am creat cele 2 fisiere mentionate

```
[04/21/23]seed@VM:~/.../certificates$ touch index.txt
[04/21/23]seed@VM:~/.../certificates$ echo 1000 > serial
[04/21/23]seed@VM:~/.../certificates$
```

- am generat certificatul X.509 auto-semnat astfel:

```
[04/21/23]seed@VM:~/.../certificates$ openssl req -x509 -newkey rsa:4096 -sha256 -days 365
0 \-keyout ca.key -out ca.crt
Generating a RSA private key
.....................................................................................
...............................++++
.....................................................................................
.....................................................................................
.....................................................................................
.....................................................................................
.....................................................................++++
writing new private key to 'ca.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:RO
State or Province Name (full name) [Some-State]:CJ
Locality Name (eg, city) []:Cluj-Napoca
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UTCN
Organizational Unit Name (eg, section) []:UTCN
Common Name (e.g. server FQDN or YOUR name) []:Birlutiu Claudiu
Email Address []:birlutiuclaudiuc@gmail.com
[04/21/23]seed@VM:~/.../certificates$
```

- generăm o pereche de chei RSA cu o lungime de 4096 biți prin optiunea -newkey rsa:4096
- -sha256: specifică faptul că dorim să folosim algoritmul de hash SHA-256 pentru semnarea certificatului.
- Certificatul va fi valid 3650 de zile (10 ani aprox)

- am vizualizat continutul decodat al fisierelor

```
[04/21/23]seed@VM:~/.../certificates$ openssl x509 -in ca.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            0e:af:a9:19:18:01:71:18:90:c1:91:49:09:c2:95:95:57:69:fb:ed
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = RO, ST = CJ, L = Cluj-Napoca, O = UTCN, OU = UTCN, CN = Birlutiu Claudiu, emailAddress = birlutiuclaudiuc@gmail.com
        Validity
            Not Before: Apr 21 22:58:11 2023 GMT
            Not After : Apr 18 22:58:11 2033 GMT
        Subject: C = RO, ST = CJ, L = Cluj-Napoca, O = UTCN, OU = UTCN, CN = Birlutiu Claudiu, emailAddress = birlutiuclaudiuc@gmail.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (4096 bit)
                Modulus:
                    00:aa:fb:bd:87:96:b8:34:6e:fa:d5:9a:19:58:2d:
                    df:63:bb:33:82:93:46:2e:29:e0:c2:19:f5:13:cf:
                    ae:81:59:fd:0a:ef:8b:55:f7:32:0a:93:7b:29:de:
                    44:54:b1:b6:ea:c6:42:59:b8:b0:8b:3c:f3:18:94:
                    09:92:9f:71:ae:53:a5:91:35:e6:68:66:02:09:43:
                    a9:0b:36:9f:89:7f:d6:78:03:bb:54:af:56:e7:9e:
                    fa:91:25:4f:25:fc:96:11:71:96:0b:55:44:66:08:
                    4c:17:7d:be:f7:bc:5f:1b:67:24:d9:f0:1d:2c:5a:
                    0a:b8:26:76:75:4e:13:fb:76:92:77:d3:48:ab:a1:
                    bf:22:45:d2:0f:32:b1:0a:5c:75:2e:05:5a:4a:98:
                    25:fc:3b:7c:0a:e4:f6:28:fa:db:67:96:c0:18:54:
                    5a:30:9a:7d:66:31:8c:20:df:85:13:4b:a0:3b:73:
                    f1:20:fd:c0:e5:40:75:6e:25:0c:41:b5:37:bf:e8:
                    37:ad:99:a8:85:db:c1:77:d7:f9:92:34:22:cc:62:
                    54:b0:5f:f8:9f:c8:0b:26:78:eb:79:fb:f2:9f:5e:
                    7c:d1:46:1a:76:9f:b4:de:a3:7d:25:89:8b:9c:30:
                    05:53:4a:2f:3b:7c:2f:ee:a8:76:52:e3:24:50:ca:
                    56:fe:d2:2a:a4:ef:cc:a5:d7:85:8b:c0:79:0b:46:
```

```
[04/21/23]seed@VM:~/.../certificates$ openssl rsa -in ca.key -text -noout
Enter pass phrase for ca.key:
RSA Private-Key: (4096 bit, 2 primes)
modulus:
    00:aa:fb:bd:87:96:b8:34:6e:fa:d5:9a:19:58:2d:
    df:63:bb:33:82:93:46:2e:29:e0:c2:19:f5:13:cf:
    ae:81:59:fd:0a:ef:8b:55:f7:32:0a:93:7b:29:de:
    44:54:b1:b6:ea:c6:42:59:b8:b0:8b:3c:f3:18:94:
    09:92:9f:71:ae:53:a5:91:35:e6:68:66:02:09:43:
    a9:0b:36:9f:89:7f:d6:78:03:bb:54:af:56:e7:9e:
    fa:91:25:4f:25:fc:96:11:71:96:0b:55:44:66:08:
    4c:17:7d:be:f7:bc:5f:1b:67:24:d9:f0:1d:2c:5a:
    0a:b8:26:76:75:4e:13:fb:76:92:77:d3:48:ab:a1:
    bf:22:45:d2:0f:32:b1:0a:5c:75:2e:05:5a:4a:98:
    25:fc:3b:7c:0a:e4:f6:28:fa:db:67:96:c0:18:54:
    5a:30:9a:7d:66:31:8c:20:df:85:13:4b:a0:3b:73:
    f1:20:fd:c0:e5:40:75:6e:25:0c:41:b5:37:bf:e8:
    37:ad:99:a8:85:db:c1:77:d7:f9:92:34:22:cc:62:
    54:b0:5f:f8:9f:c8:0b:26:78:eb:79:fb:f2:9f:5e:
    7c:d1:46:1a:76:9f:b4:de:a3:7d:25:89:8b:9c:30:
    05:53:4a:2f:3b:7c:2f:ee:a8:76:52:e3:24:50:ca:
    56:fe:d2:2a:a4:ef:cc:a5:d7:85:8b:c0:79:0b:46:
    1d:5b:41:11:cc:d9:e3:5d:fd:84:c6:f0:6b:db:63:
    e2:12:3d:38:cf:e3:c9:9c:fb:36:06:fd:73:d4:8d:
    90:00:5e:60:22:8f:8d:47:9f:cc:51:cc:1a:2c:c7:
    14:8f:25:e8:dc:62:1f:85:e6:20:d4:3d:72:c4:0d:
    71:c6:8a:d5:7b:d2:18:82:7d:fa:59:2b:88:16:86:
    79:e8:4b:97:7d:79:cd:b8:03:e9:c5:cb:2a:2a:3d:
    3a:cb:a8:06:c8:99:a5:55:c2:f5:0f:e7:2e:f6:5c:
    53:d7:f6:b3:51:fd:6f:78:5e:c8:60:ab:fa:60:ff:
    d3:a8:4d:1b:3e:af:4a:12:7d:4f:b3:41:09:93:89:
    8d:54:47:a5:f9:b1:0b:04:db:15:1f:9a:2c:d8:c4:
```

- Ce parte a certificatului indica ca acesta este un certificat CA?
  - există o extensie numită "Basic Constraints" care indică dacă certificatul este un certificat de autoritate de certificare (CA) sau nu.

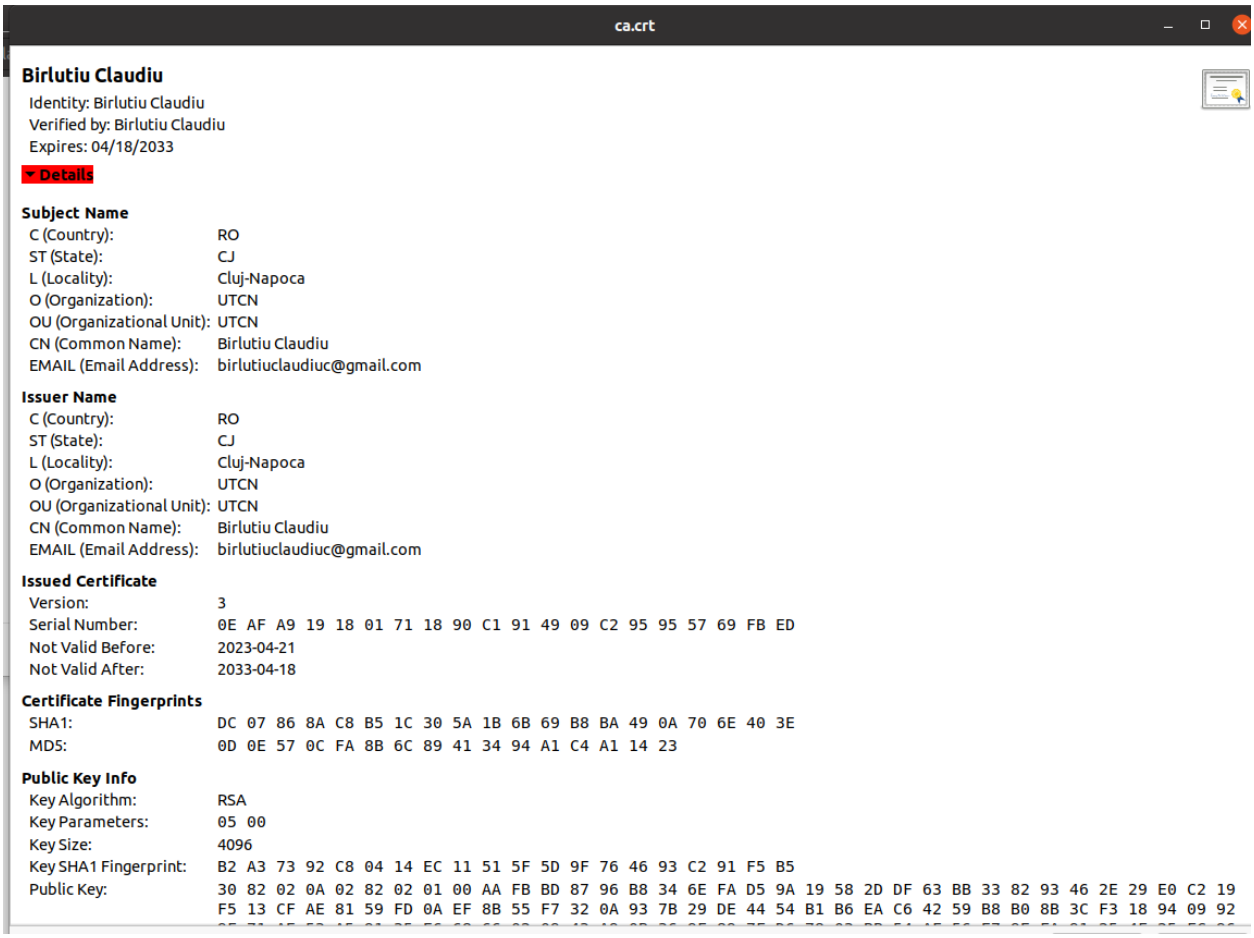
```
X509v3 Basic Constraints: critical
    CA:TRUE
gnature Algorithm: sha256WithRSAEncryption
```

- Ce parte a certificatului indica ca acesta este un certificat semnat de sine?
  - există un câmp numit "Issuer" care indică entitatea care a emis certificatul.

```
Version: 3 (0x2)
Serial Number:
    0e:af:a9:19:18:01:71:18:90:c1:91:49:09:c2:95:95:57:69:fb:ed
Signature Algorithm: sha256WithRSAEncryption
Issuer: C = RO, ST = CJ, L = Cluj-Napoca, O = UTCN, OU = UTCN, CN = Birlutiu Claudiu, emailAddress = birlutiuclaudiuc@gmail.com
Validity
    Not Before: Apr 21 22:58:11 2023 GMT
    Not After : Apr 18 22:58:11 2033 GMT
```

- In algoritmul RSA, avem un exponent public **e,** un exponent privat **d** , un modul **n** si doua secrete, numerele **p** și **q,** astfel ıncat **n=pq.** Va rugam sa identificati valorile pentru aceste elemente in certificatul dvs. si fisierele cheie
  - Exponent: 65537 (0x10001)
  - publicExponent: 65537 (0x10001)
  - celelalte valori se pot observa din : **openssl rsa -in ca.key -text -noout**

- certificatul



ca.crt

Birlutiu Claudiu

Identity: Birlutiu Claudiu
Verified by: Birlutiu Claudiu
Expires: 04/18/2033

Details

Subject Name

C (Country):	RO
ST (State):	CJ
L (Locality):	Cluj-Napoca
O (Organization):	UTCN
OU (Organizational Unit):	UTCN
CN (Common Name):	Birlutiu Claudiu
EMAIL (Email Address):	birlutiuclaudiuc@gmail.com

Issuer Name

C (Country):	RO
ST (State):	CJ
L (Locality):	Cluj-Napoca
O (Organization):	UTCN
OU (Organizational Unit):	UTCN
CN (Common Name):	Birlutiu Claudiu
EMAIL (Email Address):	birlutiuclaudiuc@gmail.com

Issued Certificate

Version:	3
Serial Number:	0E AF A9 19 18 01 71 18 90 C1 91 49 09 C2 95 95 57 69 FB ED
Not Valid Before:	2023-04-21
Not Valid After:	2033-04-18

Certificate Fingerprints

SHA1:	DC 07 86 8A C8 B5 1C 30 5A 1B 6B 69 B8 BA 49 0A 70 6E 40 3E
MD5:	0D 0E 57 0C FA 8B 6C 89 41 34 94 A1 C4 A1 14 23

Public Key Info

Key Algorithm:	RSA
Key Parameters:	05 00
Key Size:	4096
Key SHA1 Fingerprint:	B2 A3 73 92 C8 04 14 EC 11 51 5F 5D 9F 76 46 93 C2 91 F5 B5
Public Key:	30 82 02 0A 02 82 02 01 00 AA FB BD 87 96 B8 34 6E FA D5 9A 19 58 2D DF 63 BB 33 82 93 46 2E 29 E0 C2 19 F5 13 CF AE 81 59 FD 0A EF 8B 55 F7 32 0A 93 7B 29 DE 44 54 B1 B6 EA C6 42 59 B8 B0 8B 3C F3 18 94 09 92

Sarcina 2: Generarea unei cereri de certificat pentru serverul dvs.

- Am generat o cerere de certificat pentru serverul nostru folsoind comanda:
  - openssl req -newkey rsa:2048 -sha256 \-keyout server.key -out server.csr \-subj "/CN=www.birlutiu2023.com/O=Birlutiu2023 Inc./C=RO" \-passout pass:claudiu -addext "subjectAltName = DNS:www.bank32.com, DNS:www.bank32A.com, DNS:www.bank32B.com, DNS: www.birlutiu2023.com, DNS: wwww.birlutiu2023A.com, DNS: www.birlutiu2023B.com"

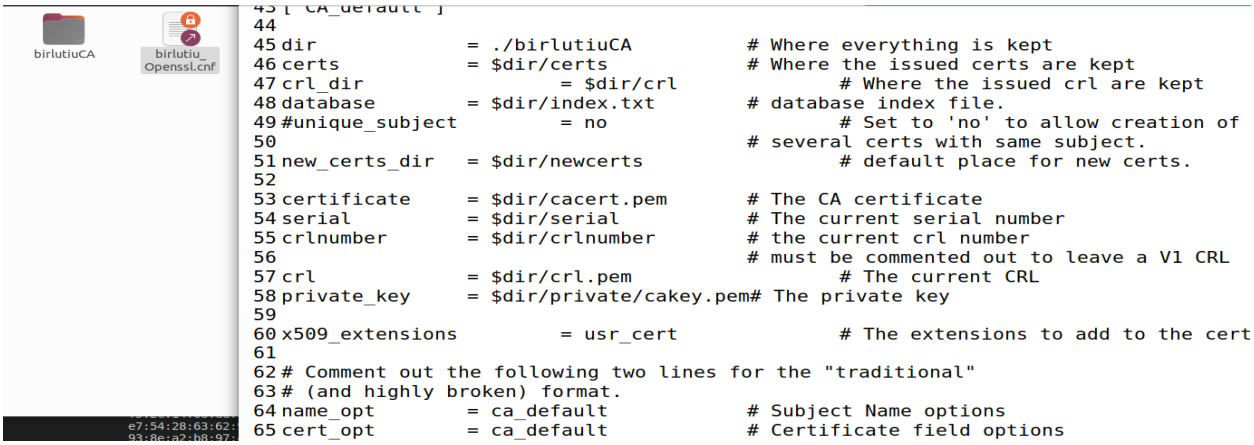
```
[04/21/23]seed@VM:~/.../certificates$ openssl req -newkey rsa:2048 -sha256 \-keyout server.key -out server.csr \-subj "/CN=www.birlutiu2023.com/O=Birlutiu2023 Inc./C=
RO" \-passout pass:claudiu -addext "subjectAltName = DNS:www.bank32.com, DNS:www.bank32A.com, DNS:www.bank32B.com, DNS: www.birlutiu2023.com, DNS: wwww.birlutiu2023A.
com, DNS: www.birlutiu2023B.com"
Generating a RSA private key
.........+++++
...........................+++++
writing new private key to 'server.key'
-----
[04/21/23]seed@VM:~/.../certificates$
```

- am urmărit continutul decoda al fisierului .csr

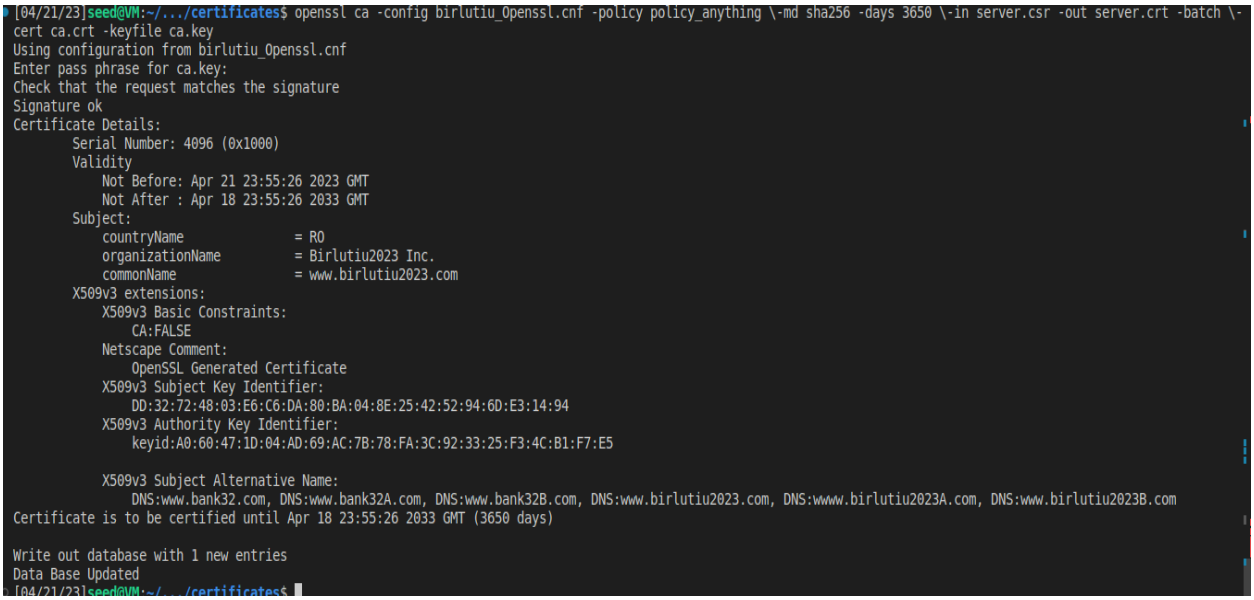
```
[04/21/23]seed@VM:~/.../certificates$ openssl req -in server.csr -text -noout
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: CN = www.birlutiu2023.com, O = Birlutiu2023 Inc., C = RO
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:9f:87:a1:0c:f9:f1:a6:5b:83:c0:1c:a3:69:3d:
                    15:ed:a9:4c:42:d2:0c:c3:a8:df:55:e4:98:c8:9d:
                    f5:2c:14:68:de:d9:41:62:65:bd:d2:57:2c:9a:2f:
                    e7:54:28:63:62:9a:54:0a:dc:69:59:63:d6:af:2d:
                    93:8e:a2:b8:97:43:81:95:63:ea:09:a3:a8:90:7c:
                    9f:ed:56:3d:51:2a:4e:16:4f:76:b5:2e:0e:d1:99:
                    97:94:ce:5f:be:9a:f9:34:a3:89:9f:c2:e3:7b:cc:
                    8c:a8:6c:98:47:49:d5:5f:c0:e4:f7:87:e2:90:f1:
                    3a:6a:e2:4a:b3:14:39:f1:35:cb:19:1c:f2:f6:13:
                    20:6a:cc:d0:81:9a:2d:0c:a6:e1:35:5f:2a:43:17:
                    d3:7f:89:1b:76:57:5c:a1:95:0f:b9:d9:1b:75:07:
                    ae:5a:77:8e:43:33:54:e7:e9:dc:36:e1:3e:9b:28:
```

Sarcina 3: Generarea unui certificat pentru serverul dvs.

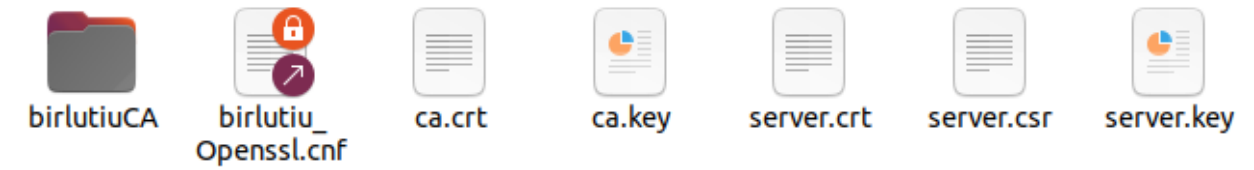
- Fişierul **server.csr** trebuie sa aibă **semnatura CA** pentru a forma un certificat.
- Am copiat fişierul openssl.cnf într-un folder din BirlutiuClaudiu_Cod lângă directorul **birlutiuCA** unde se afla toate certificatele pe care le-am generat



- Astfel, pentru sermnarea certificatului **server.csr** într-un certificat x509 (**server.crt**), folosind **CA.crt** şi **ca.key** vom rula următoarea comanda:
  - openssl ca -config **birlutiu_Openssl.cnf** -policy **policy_anything** \-md sha256 -days 3650 \-in **server.csr** -out **server.crt** -batch \-cert **ca.crt** -keyfile **ca.key**



- rezultatul obținut




```
● [04/21/23]seed@VM:~/.../certificates$ openssl x509 -in server.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4096 (0x1000)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = RO, ST = CJ, L = Cluj-Napoca, O = UTCN, OU = UTCN, CN = Birlutiu Claudiu, emailAddress = birlutiuclaudiuc@gmail.com
        Validity
            Not Before: Apr 21 23:55:26 2023 GMT
            Not After : Apr 18 23:55:26 2033 GMT
        Subject: C = RO, O = Birlutiu2023 Inc., CN = www.birlutiu2023.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:9f:87:a1:0c:f9:f1:a6:5b:83:c0:1c:a3:69:3d:
                    15:ed:a9:4c:42:d2:0c:c3:a8:df:55:e4:98:c8:9d:
                    f5:2c:14:68:de:d9:41:62:65:bd:d2:57:2c:9a:2f:
                    e7:54:28:63:62:9a:54:0a:dc:69:59:63:d6:af:2d:
                    93:8e:a2:b8:97:43:81:95:63:ea:09:a3:a8:90:7c:
                    9f:ed:56:3d:51:2a:4e:16:4f:76:b5:2e:0e:d1:99:
                    97:94:ce:5f:be:9a:f9:34:a3:89:9f:c2:e3:7b:cc:
                    8c:a8:6c:98:47:49:d5:5f:c0:e4:f7:87:e2:90:f1:
                    3a:6a:e2:4a:b3:14:39:f1:35:cb:19:1c:f2:f6:13:
                    20:6a:cc:d0:81:9a:2d:0c:a6:e1:35:5f:2a:43:17:
                    d3:7f:89:1b:76:57:5c:a1:95:0f:b9:d9:1b:75:07:
                    ae:5a:77:8e:43:33:54:e7:e9:dc:36:e1:3e:9b:28:
                    bb:94:5d:33:b0:fe:63:75:54:47:fb:3f:b5:2c:33:
                    8e:d3:1a:a2:9f:1f:b6:3c:74:dc:10:78:dc:53:ec:
                    5e:8a:18:35:39:09:f4:6c:2c:c8:a9:b7:11:41:f8:
                    a1:e5:7a:c3:17:63:fd:c6:17:e6:29:e6:ec:d3:25:
                    34:13:00:c3:74:ef:cc:97:ad:4b:83:eb:0d:0b:7c:
```

Sarcina 4: Plasarea unui certificat într-un sit de web HTTPS bazat pe Apache

- Vizualizare în cobatianrul nousru a fisierului **bank32_apache_ssl.conf**

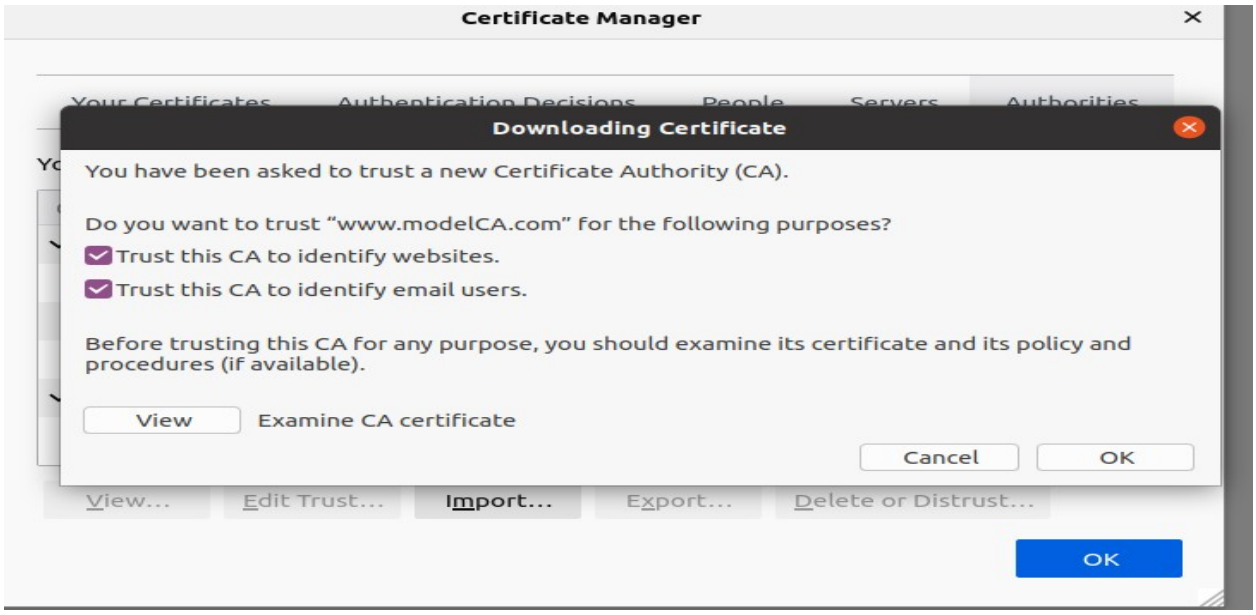
```
root@2f51a8af7e11:/# cd /etc/apache2/sites-available/
root@2f51a8af7e11:/etc/apache2/sites-available# ls
000-default.conf  bank32_apache_ssl.conf  default-ssl.conf
root@2f51a8af7e11:/etc/apache2/sites-available# cat bank32_apache_ssl.conf
<VirtualHost *:443>
    DocumentRoot /var/www/bank32
    ServerName www.bank32.com
    ServerAlias www.bank32A.com
    ServerAlias www.bank32B.com
    ServerAlias www.bank32W.com
    DirectoryIndex index.html
    SSLEngine On
    SSLCertificateFile /certs/bank32.crt
    SSLCertificateKeyFile /certs/bank32.key
</VirtualHost>

<VirtualHost *:80>
    DocumentRoot /var/www/bank32
    ServerName www.bank32.com
    DirectoryIndex index_red.html
</VirtualHost>

# Set the following gloal entry to suppress an annoying warning message
ServerName localhost
root@2f51a8af7e11:/etc/apache2/sites-available#
```

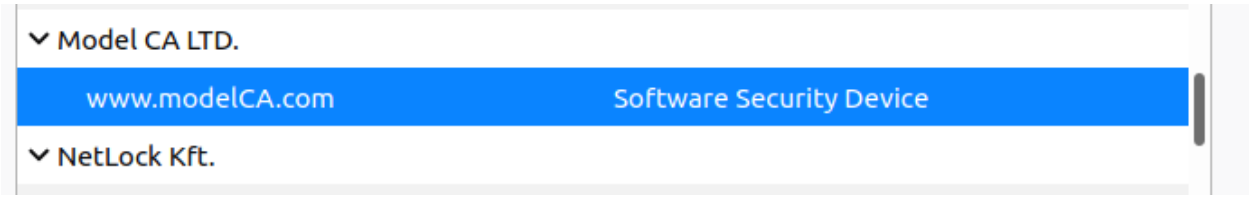
- DocumentRoot – unde sunt stocate fisierele pentru site-ul web
- **activam apache2** din container:

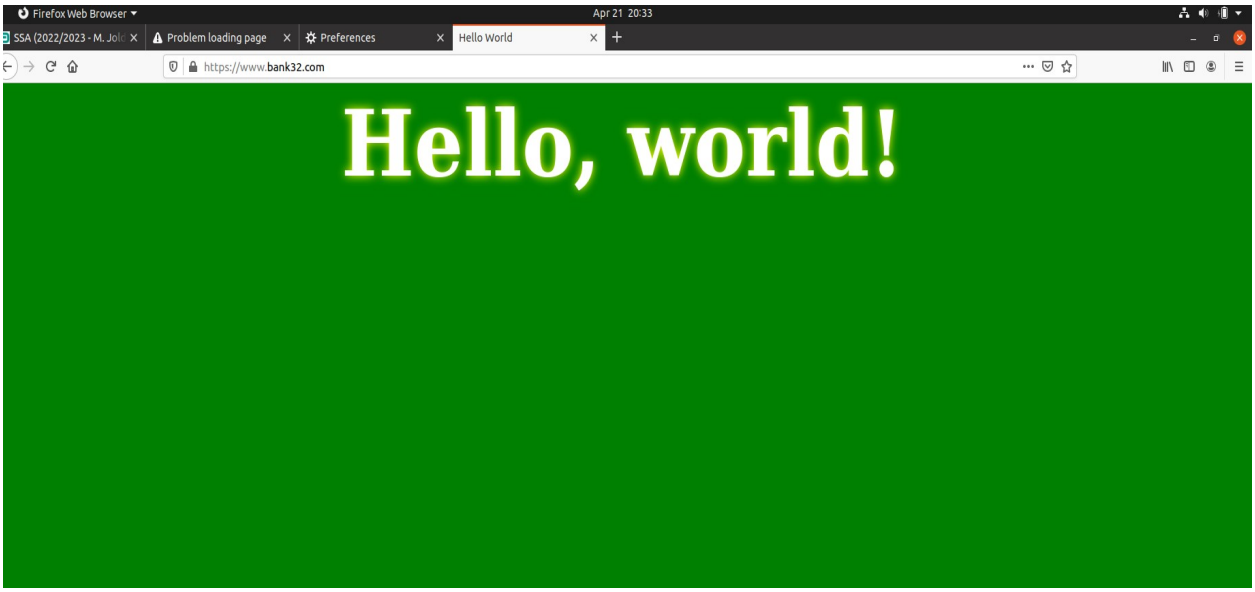
```
root@2f51a8af7e11:/etc/apache2/sites-available# service apache2 start
 * Starting Apache httpd web server apache2
Enter passphrase for SSL/TLS keys for www.bank32.com:443 (RSA):
 *
root@2f51a8af7e11:/etc/apache2/sites-available# service apache2 start
 * Starting Apache httpd web server apache2
 *
root@2f51a8af7e11:/etc/apache2/sites-available#
```

- la o prima încercare a accesarii din browser a site-ului www.bank.com observam ca nu se randeaza niciun site deaorece nu avem încărcata autoritatea pentru validarea certif pentru acest site; vom încarca în FireFox

certificatul **modelCA.crt** din folderul **certs;** aceasta e autoritatea care va certifica site-ul bank32 cu certificatul bank32.crt

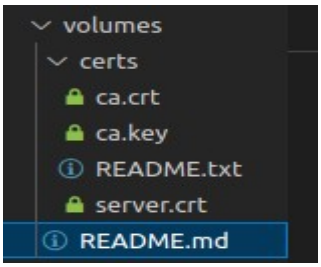






În continuare ne vom ocupa de configurarea propriului nostru site pentru care am obținut certificatul.

- pentru început vom crea în volumes un fisier denumiit certs unde se vor afla fiserele **ca.crt, ca.key, server.crt si server key** fisiere pe care le-am obținut anterior în



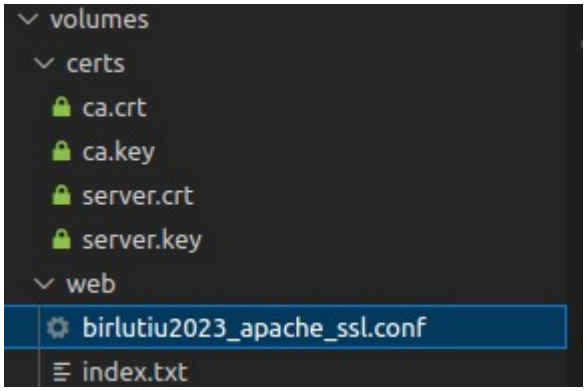
- cream un folder nou în volumes numit web și adaugam fișierul **index.txt**
- cream fișierul de configurare pentru apache2

birlutiu2023_apache_ssl.conf M × bank32_apache_ssl.conf index.txt

L06 > Birlutiu_Claudiu_L06 > BirlutiuClaudiu_Cod > volumes > web > birlutiu2023_apache_ssl.conf

```
<VirtualHost *:443>
    DocumentRoot /var/www/birlutiu2023
    ServerName www.birlutiu2023.com
    ServerAlias www.birlutiu2023A.com
    ServerAlias www.birlutiu2023B.com
    DirectoryIndex index.txt
    SSLEngine On
    SSLCertificateFile /certs/server.crt
    SSLCertificateKeyFile /certs/server.key
</VirtualHost>

<VirtualHost *:80>
    DocumentRoot /var/www/birlutiu2023
    ServerName www.birlutiu2023.com
    DirectoryIndex index.txt
</VirtualHost>

# Set the following gloal entry to suppress an annoying warning message
ServerName localhost
```

- structura fisierului Volumes este aceasta:



- repornim containerul și observam ca s-au copiat cele 2 foldere

```
PROBLEMS    OUTPUT    DEBUG CONSOLE    TERMINAL

[04/21/23]seed@VM:~/.../certificates$ docksh 2f51a8af7e11
root@2f51a8af7e11:/# cd volumes/
root@2f51a8af7e11:/volumes# ls
README.md  certs  web
root@2f51a8af7e11:/volumes#
```

- în continuare vom copia în **certs** *server.crt* și *server.key* din /volumes/certs

```
[04/21/23]seed@VM:~/.../certificates$ docksh 2f51a8af7e11
root@2f51a8af7e11:/# cd volumes/certs/
root@2f51a8af7e11:/volumes/certs# ls
ca.crt  ca.key  server.crt  server.key
root@2f51a8af7e11:/volumes/certs# cp /volumes/certs/server.crt /certs/
root@2f51a8af7e11:/volumes/certs# cp /volumes/certs/server.key /certs/
root@2f51a8af7e11:/volumes/certs#
```

- vom copia și **birlutiu2023_apache_ssl.conf** în /etc/apache2/sites-available

```
root@2f51a8af7e11:/volumes/web# ls
birlutiu2023_apache_ssl.conf  index.html  index_red.html
root@2f51a8af7e11:/volumes/web# cp birlutiu2023_apache_ssl.conf /etc/apache2/sites-available/
root@2f51a8af7e11:/volumes/web#
```

- activam acest site

```
root@2f51a8af7e11:/etc/apache2/sites-available# service apache2 reload
 * Reloading Apache httpd web server apache2
 *
root@2f51a8af7e11:/etc/apache2/sites-available# a2ensite birlutiu2023_apache_ssl.conf
Site birlutiu2023_apache_ssl already enabled
root@2f51a8af7e11:/etc/apache2/sites-available#
```

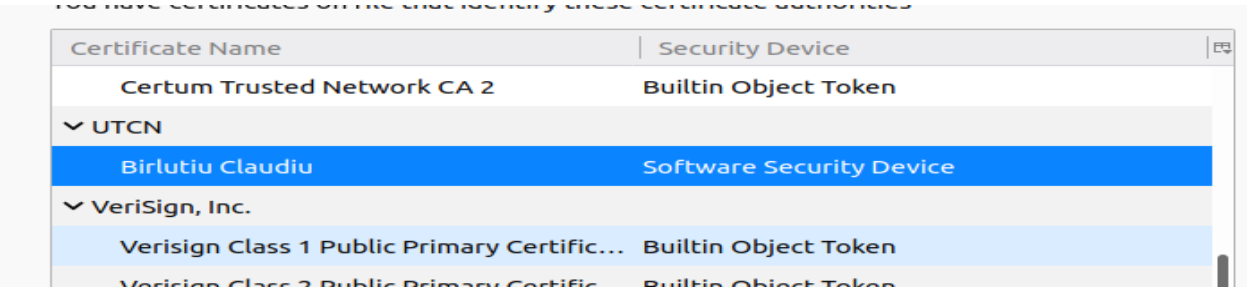
- schimbam tipurile de acces pentru fiesiere în felul următor:

```
root@2f51a8af7e11:/etc/apache2/sites-available# cd /certs/
root@2f51a8af7e11:/certs# ls
bank32.crt  bank32.key  server.crt  server.key
root@2f51a8af7e11:/certs# chmod 400 server.key
root@2f51a8af7e11:/certs# cd /volumes/web/
root@2f51a8af7e11:/volumes/web# ls
birlutiu2023_apache_ssl.conf  index.html  index_red.html
root@2f51a8af7e11:/volumes/web# chmod 644 index.html
root@2f51a8af7e11:/volumes/web# chmode 644 index_red.html
bash: chmode: command not found
root@2f51a8af7e11:/volumes/web# chmod 644 index_red.html
root@2f51a8af7e11:/volumes/web#
```

- copiere index.txt în ***var/*www/birlutiu2023** și adaugare chmod **644**

```
root@2f51a8af7e11:/var/www# cp /volumes/web/index.txt /var/www/birlutiu2023/
root@2f51a8af7e11:/var/www# cd birlutiu2023/
root@2f51a8af7e11:/var/www/birlutiu2023# chmod 644 index.txt
root@2f51a8af7e11:/var/www/birlutiu2023#
```

- încarcam certificatul **ca.crt** în Firefox



- pornim serviciul apache2

```
root@2f51a8af7e11:/volumes/web# service apache2 restart
 * Restarting Apache httpd web server apache2
Enter passphrase for SSL/TLS keys for www.birlutiu2023.com:443 (RSA):
                                                                      [ OK ]
root@2f51a8af7e11:/volumes/web#
```

REZULATUL OBTINUT!!!! - ceea ce avem în fișierul nostru index.txt

Sarcina 5: Lansarea unui atac de tipul om-la-mijloc

- În continure vom lansa un atac de tipul MITM având ca site luat ca studiu fiind https://www.emag.ro/ , un site de cumpărături cunoscut
- m-am cobectat la container și am modificat server name de la bank32 conf apache i www.emag.ro

```
root@b71f009b71f2:/etc/apache2/sites-available# nano bank32_apache_ssl.conf
root@b71f009b71f2:/etc/apache2/sites-available# cat bank32_apache_ssl.conf
<VirtualHost *:443>
    DocumentRoot /var/www/bank32
    ServerName www.emag.ro
    ServerAlias www.bank32A.com
    ServerAlias www.bank32B.com
    ServerAlias www.bank32W.com
    DirectoryIndex index.html
    SSLEngine On
    SSLCertificateFile /certs/bank32.crt
    SSLCertificateKeyFile /certs/bank32.key
</VirtualHost>

<VirtualHost *:80>
    DocumentRoot /var/www/bank32
    ServerName www.emag.ro
    DirectoryIndex index_red.html
</VirtualHost>

# Set the following gloal entry to suppress an annoying warning message
ServerName localhost
root@b71f009b71f2:/etc/apache2/sites-available#
```

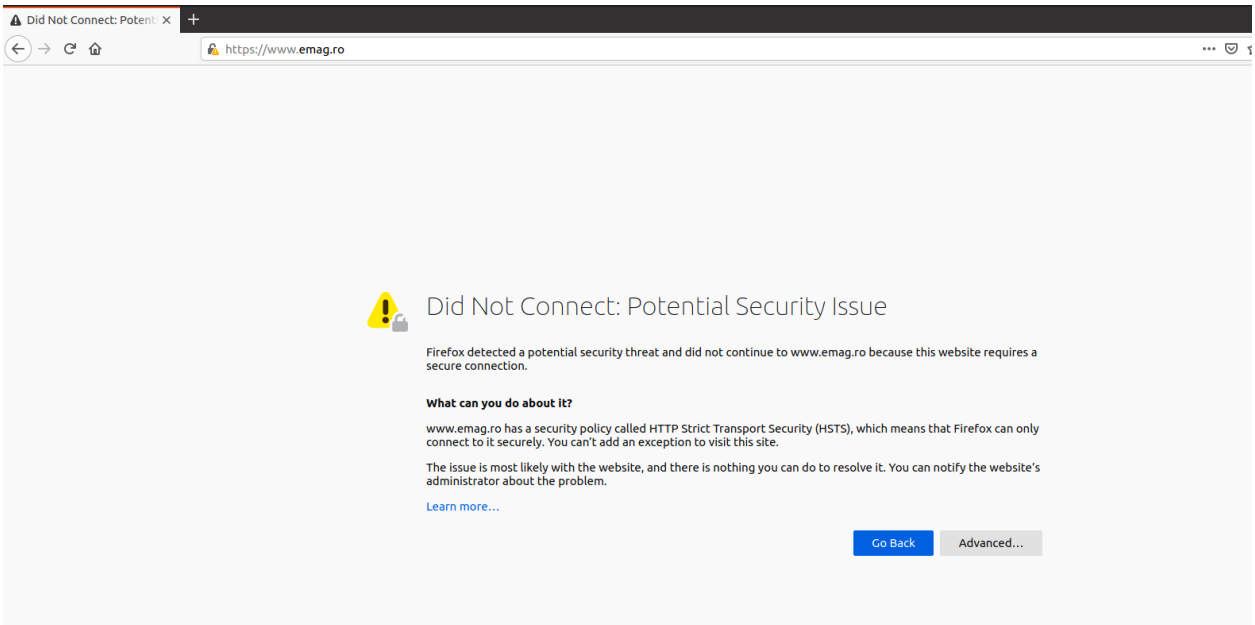
- dam un restart serverul de apache2

```
root@b71f009b71f2:/etc/apache2/sites-available# service apache2 restart
 * Restarting Apache httpd web server apache2
Enter passphrase for SSL/TLS keys for www.emag.ro:443 (RSA):
```

- adaugam în etc/hosts al mașinii virtuale intrearea 10.9.0.80 www.emag.ro pentru a simula atacarea DNS a site-ului emag.ro

```
#For L06 lab
10.9.0.80 www.bank32.com
10.9.0.80 www.birlutiu2023.com
10.9.0.80 www.emag.ro
```

- obținem următoarea eroare când accesam site-ul www.emag.ro



- site-ul **emag.ro ut**ilizeaza polita de securitate HTTP Strict Transport Security (HSTS) ce impune ca browserul să se conecteze doar în mod securizat la site-ul web, utilizând protocolul HTTPS.
- chiar dacă am adăuga o intrare în fișierul "etc/hosts" pentru a redirecționa traficul către site-ul web, browserul continua să aplice politica HSTS și blocheaza accesul la site prin HTTP.
- atunci când un site web utilizează HSTS, browserul, în cazul nostru Firefox, va fi instruit să se conecteze numai prin HTTPS la acel site pentru o anumita perioada de timp

Sarcina 7: Lansarea unui atac de tipul om-la-mijloc cu o CA compromisă

- Am creat un certificat nou cu domeniul **emag.ro**:
  - openssl req -x509 -newkey rsa:4096 -sha256 -days 3650 \-keyout emag.key -out emag.crt \-subj "/CN=www.emag.ro/O=Emag CA LTD./C=US" \-passout pass:emag
  - openssl req -newkey rsa:2048 -sha256 \-keyout emag_server.key -out emag_server.csr \-subj "/CN=www.emag.ro/O=Emag Inc./C=US" \-passout pass:emag -addext "subjectAltName = DNS:www.emag.ro "
  - openssl ca -config birlutiu_Openssl.cnf -policy policy_anything \-md sha256 -days 3650 \-in emag_server.csr -out emag_server.crt -batch \-cert emag.crt -keyfile emag.key
  - Am creat un certificat nou cu common name www.emag.ro
  - Punem aceste fisier noi create in volumes pentru a le avea in container la pornirea acestuia

```
[04/25/23]seed@VM:~/.../emag_certificates$ openssl ca -config birlutiu_Openssl.cnf -policy policy_anything \-md sha256 -days 3650 \-in emag_server.csr -out
emag_server.crt -batch \-cert emag.crt -keyfile emag.key
Using configuration from birlutiu_Openssl.cnf
Enter pass phrase for emag.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4096 (0x1000)
        Validity
            Not Before: Apr 25 22:39:29 2023 GMT
            Not After : Apr 22 22:39:29 2033 GMT
        Subject:
            countryName               = US
            organizationName          = Emag Inc.
            commonName                = www.emag.ro
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                8C:A4:7A:8A:FC:86:A9:20:3F:05:AB:FD:FD:80:0F:DF:5A:DC:54:2D
            X509v3 Authority Key Identifier:
                keyid:91:C0:85:BB:5E:F3:10:07:A2:D3:24:94:9A:77:AA:D4:BB:5C:DC:4E

            X509v3 Subject Alternative Name:
                DNS:www.emag.ro
Certificate is to be certified until Apr 22 22:39:29 2033 GMT (3650 days)

Write out database with 1 new entries
Data Base Updated
[04/25/23]seed@VM:~/.../emag_certificates$
```

- Am modificat fisierul de configurare bank32 cu server name-ul emag.ro

```
  GNU nano 4.8                    bank32_apache_ssl.conf                    Modified
<VirtualHost *:443>
    DocumentRoot /var/www/emag
    ServerName www.emag.ro
    ServerAlias www.emagA.com
    ServerAlias www.emagB.com
    ServerAlias www.emagW.com
    DirectoryIndex index.txt
    SSLEngine On
    SSLCertificateFile /certs/emag_server.crt
    SSLCertificateKeyFile /certs/emag_server.key
</VirtualHost>

<VirtualHost *:80>
    DocumentRoot /var/www/emag
    ServerName www.emag.ro
    DirectoryIndex index.txt
</VirtualHost>

# Set the following gloal entry to suppress an annoying warning message
ServerName localhost
```

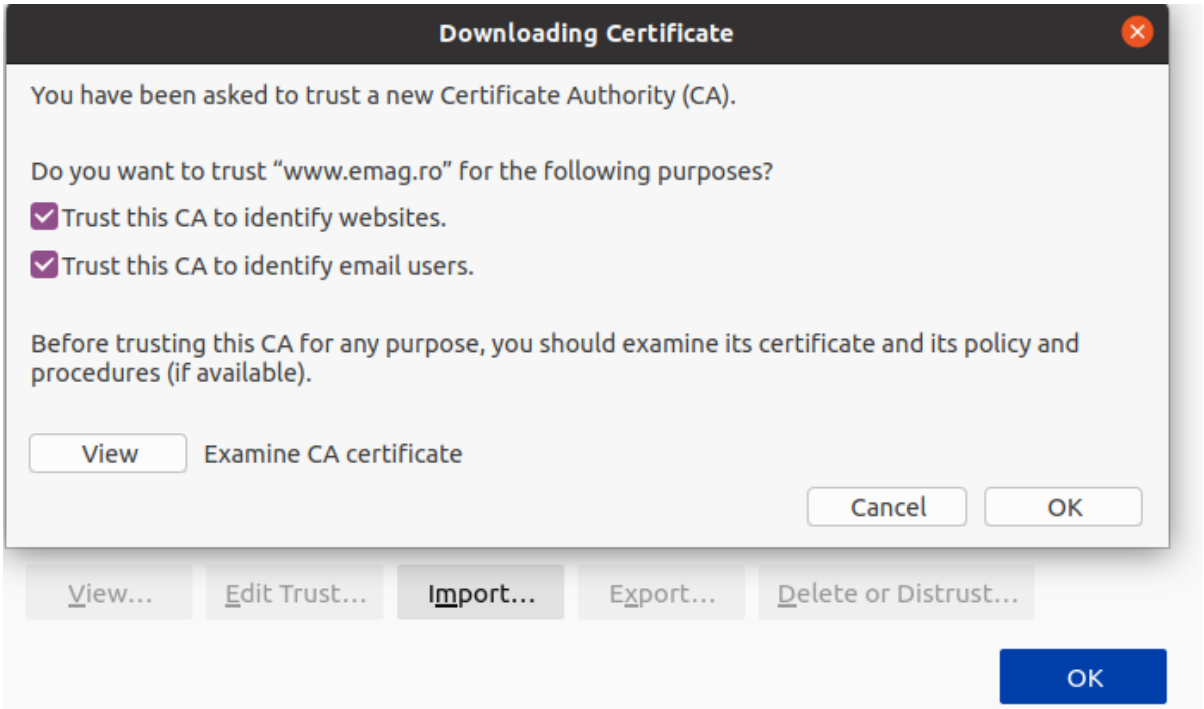
- Am facut modificareile corespunzatoare in container

```
bank32.crt  bank32.key
root@b71f009b71f2:/certs# cp /volumes/emag/emag_server.crt .
root@b71f009b71f2:/certs# cp /volumes/emag/emag_server.key .
root@b71f009b71f2:/certs# chmod 400 emag_server.key
root@b71f009b71f2:/certs# cd /var/www/
root@b71f009b71f2:/var/www# mkdir emag
root@b71f009b71f2:/var/www# cp /volumes/emag/index.txt
cp: missing destination file operand after '/volumes/emag/index.txt'
Try 'cp --help' for more information.
root@b71f009b71f2:/var/www# cp /volumes/emag/index.txt .
root@b71f009b71f2:/var/www# cp /volumes/emag/index.txt ./emag/
root@b71f009b71f2:/var/www# cd emag/
root@b71f009b71f2:/var/www/emag# chmod 644 index.txt
root@b71f009b71f2:/var/www/emag# nano /etc/apache2/sites-available/
root@b71f009b71f2:/var/www/emag# nano /etc/apache2/sites-available/bank32_apache_
ssl.conf
root@b71f009b71f2:/var/www/emag#
```

- Am dat restart la serviciul apache2

```
root@b71f009b71f2:/var/www/emag# service apache2 restart
 * Restarting Apache httpd web server apache2
Enter passphrase for SSL/TLS keys for www.emag.ro:443 (RSA):
                                                            [ OK ]
root@b71f009b71f2:/var/www/emag#
```

- Am incarcat certificatul in browser



- Am adaugat in etc hosts al masinii virtuale intarea 10.9.0.80 www.emag.ro pentru a simula dns

REZULTATUL OBTINUT IN MOMENTUL IN CARE SE ACCESEAZA **www.emag.ro**

- E ceea ce avem in fisierul index.txt al nostru