

Mérési jegyzőkönyv  
**Publikus Kulcsú Infrastruktúra**  
**2022/2023/2 félév**

A mérőhely (VM) száma:	<b>10</b>
A mérés időpontja:	<b>2023. 04. 17.</b>
A mérést végezték:	<b>Wágner Réka (CGUOR8), Rittgasszer Ákos (Z8WK8D)</b>
Ennek a fájlnak a neve:	<b>PKI_0417_10_Z8WK8D_CGUOR8.doc</b> (<mérés rövidítése>_<hónap nap>_<mérőhely>_<Neptun1>_<Neptun2>. doc)

## 1. Webszerver tanúsítványok igénylése és kibocsátása

### 1. Önálírt CA tanúsítvány kibocsátása

#### 1.1.1. Kulcs generálása a CA számára

Az alábbi paranccsal generáltuk le a megfelelő kulcsot, amit a ca.key file-ba mentettünk:

```
meres@pki-meres ~/pkilabor/certificate_authority  
$ openssl ecparam -out ca.key -name prime256v1
```

Ez a parancs szolgált az önálírt tanúsítvány generálásához:

```
meres@pki-meres ~/pkilabor/certificate_authority  
$ openssl ecparam -out ca.key -name prime256v1 -genkey  
  
meres@pki-meres ~/pkilabor/certificate_authority  
$ openssl req -x509 -new -sha256 -days 365 -key ca.key -out ca.crt  
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]:|
```

Megadtuk a kért adatokat:

```
meres@pki-meres ~/pkilabor/certificate_authority  
$ openssl req -x509 -new -sha256 -days 365 -key ca.key -out ca.crt  
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]:HU  
State or Province Name (full name) [Some-State]:Budapest  
Locality Name (eg, city) []:Budapest  
Organization Name (eg, company) [Internet Widgits Pty Ltd]:CrySyS Lab  
Organizational Unit Name (eg, section) []:PKI Labor  
Common Name (e.g. server FQDN or YOUR name) []:PKI Labor CA  
Email Address []:  
  
meres@pki-meres ~/pkilabor/certificate_authority  
$
```

#### 1.1.2. Önálírt CA tanúsítvány vizsgálata

Kiírtuk az önálírt tanúsítvány adatait. Itt szépen látszódnak az általunk megadott adatok:

```
meres@pki-meres ~/pkilabor/certificate_authority
$ openssl x509 -noout -in ca.crt -text
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      93:c7:e5:a9:9f:c2:bc:dd
    Signature Algorithm: ecDSA-with-SHA256
    Issuer: C=HU, ST=Budapest, L=Budapest, O=CrySyS Lab, OU=PKI Labor, CN=PK
I Labor CA
    Validity
      Not Before: Apr 17 12:56:33 2023 GMT
      Not After : Apr 16 12:56:33 2024 GMT
    Subject: C=HU, ST=Budapest, L=Budapest, O=CrySyS Lab, OU=PKI Labor, CN=P
KI Labor CA
    Subject Public Key Info:
      Public Key Algorithm: id-ecPublicKey
      Public-Key: (256 bit)
      pub:
        04:31:0d:58:c2:53:3a:cd:fb:fd:0a:5e:30:0f:d4:
        6a:f8:fa:a8:84:6e:52:81:56:33:0a:3d:1f:72:64:
        3a:d8:0b:72:0d:4f:f5:48:29:6c:4e:4f:b5:06:ee:
        1e:2a:ac:c0:f7:67:ad:79:14:8f:aa:32:97:dc:a7:
        4a:e2:59:65:20
      ASN1 OID: prime256v1
      NIST CURVE: P-256
    X509v3 extensions:
      X509v3 Subject Key Identifier:
        7D:59:B8:74:BD:67:E7:EA:DD:C0:C5:4B:5C:0A:5A:A8:5B:86:64:40
      X509v3 Authority Key Identifier:
        keyid:7D:59:B8:74:BD:67:E7:EA:DD:C0:C5:4B:5C:0A:5A:A8:5B:86:64:4
0
      X509v3 Basic Constraints:
        CA:TRUE
    Signature Algorithm: ecDSA-with-SHA256
      30:45:02:20:1a:cd:86:b9:2a:ba:5b:b6:a6:e1:88:64:18:fd:
      a1:51:27:ab:6e:ab:a8:07:bd:c8:be:67:b5:9a:d8:50:a1:a7:
      02:21:00:9d:7f:60:e6:2e:12:a9:e5:4f:52:0e:80:76:92:49:
      0f:96:6f:6b:dd:ed:5b:36:42:fc:a8:68:c9:b7:ce:80:60
```

## 2. Webszerver tanúsítvány kibocsátása

### 1.2.1. Az OpenSSL Subject Alternate Name konfigurációja a CSR generálásához

Az openssl.cnf file lemásoltuk és hozzáadtuk a kívánt szekciót subjectAltName néven.

### 1.2.2. Kulcs és CSR generálás

Generáltunk egy új kulcsot:

```
meres@pki-meres ~/pkilabor/webserver_admin
$ openssl ecparam -out pkilabor.crysys.hu.key -name prime256v1 -genkey

meres@pki-meres ~/pkilabor/webserver_admin
$ openssl req -x509 -new -sha256 -days 365 -key pkilabor.crysys.hu.key -out pkilabor.crysys.hu.csr
-config openssl.cnf -reqexts subjectAltName
Error opening Private Key pkilabor.crysys.hu.key
4294956672:error:02001002:system library:fopen:No such file or directory:bss_file.c:406:fopen('pki
labor.crysys.hu.key','rb')
4294956672:error:20074002:BIIO routines:FILE_CTRL:system lib:bss_file.c:408:
unable to load Private Key

meres@pki-meres ~/pkilabor/webserver_admin
$ openssl req -x509 -new -sha256 -days 365 -key pkilabor.crysys.hu.key -out pkilabor.crysys.hu.csr
-config openssl.cnf -reqexts subjectAltName
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]:
```

Az új kulccsal generáltunk CSR-t:

```
meres@pki-meres ~/pkilabor/webserver_admin
$ openssl req -new -sha256 -days 365 -key pkilabor.crysys.hu.key -out pkilabor.crysys.hu.csr -conf
ig ./openssl.cnf -reqexts subjectAltName
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]:HU
State or Province Name (full name) [Some-State]:Budapest
Locality Name (eg, city) []:Budapest
Organization Name (eg, company) [Internet Widgits Pty Ltd]:CrySyS Lab
Organizational Unit Name (eg, section) []:PKI Labor
Common Name (e.g. server FQDN or YOUR name) []:pkilabor.crysys.hu
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:pkilabor_challenge
An optional company name []:CrySyS Lab
```

### 1.2.3. CSR vizsgálat

A CSR vizsgálatánál látható, hogy az aláírás helyes és látjuk az megadott alternatív nevet:

```
meres@pki-meres ~/pkilabor/certificate_authority
$ openssl req -in pkilabor.crysys.hu.csr -verify -text -noout
verify OK
Certificate Request:
Data:
  Version: 0 (0x0)
  Subject: C=HU, ST=Budapest, L=Budapest, O=CrySyS Lab, OU=PKI Labor, CN=pkilabor.crysys.hu
  Subject Public Key Info:
    Public Key Algorithm: id-ecPublicKey
    Public-Key: (256 bit)
      pub:
        04:b3:52:c1:aa:55:d2:6d:b8:56:ce:5d:7a:9e:0e:
        fd:25:09:56:cc:77:31:23:61:7b:c5:21:59:70:fe:
        e6:82:05:84:13:b4:48:c0:fc:2c:4b:74:10:84:19:
        37:3e:2c:7c:a0:1b:c2:85:d8:21:c9:b9:db:7e:51:
        44:45:22:98:04
      ASN1 OID: prime256v1
      NIST CURVE: P-256
  Attributes:
    unstructuredName          :CrySyS Lab
    challengePassword         :pkilabor_challenge
  Requested Extensions:
    X509v3 Subject Alternative Name:
      DNS:pkilabor.crysys.hu
  Signature Algorithm: ecdsa-with-SHA256
    30:45:02:20:2c:a1:51:a4:9f:85:a5:57:1b:55:2e:d1:38:39:
    08:02:0f:d5:2f:57:25:32:5c:f0:d5:13:53:b9:f0:bd:43:4e:
    02:21:00:cb:24:54:cc:0d:a1:46:bd:b4:57:e7:eb:04:d1:47:
    a0:8f:3f:32:7e:cd:ce:33:4b:4a:d4:e6:f1:8d:4d:0c:08
```

### 1.2.4. Az OpenSSL Subject Alternate Name konfigurációja a webszerver tanúsítvány kibocsátásához

Az 1.2.1. lépés megismétlése.

### 1.2.5. Webszerver tanúsítvány kibocsátása

Sikeres tanúsítvány kibocsátás a webszerverhez:

```
meres@pki-meres ~/pkilabor/certificate_authority
$ openssl x509 -req -in pkilabor.crysys.hu.csr -days 20 -CA ca.crt -CAkey ca.key -set_serial 00001
-out pkilabor.crysys.hu.crt -extfile ./openssl.cnf -extensions subjectAltName
Signature ok
subject=/C=HU/ST=Budapest/L=Budapest/O=CrySyS Lab/OU=PKI Labor/CN=pkilabor.crysys.hu
Getting CA Private Key
```

### 1.2.6. Webszerver tanúsítvány vizsgálata

A tanúsítvány vizsgálata során látható az összes általunk megadott adat:

A mérést végezték:  
CGUOR8, Z8WK8D

IT biztonság laboratórium (VIHIMB01)  
PKI mérés

```
meres@pki-meres ~/pkilabor/certificate_authority
$ openssl x509 -noout -in pkilabor.crysys.hu.crt -text
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 1 (0x1)
    Signature Algorithm: ecdsa-with-SHA256
    Issuer: C=HU, ST=Budapest, L=Budapest, O=CrySyS Lab, OU=PKI Labor, CN=PKI Labor CA
    Validity
      Not Before: Apr 17 14:15:50 2023 GMT
      Not After : May  7 14:15:50 2023 GMT
    Subject: C=HU, ST=Budapest, L=Budapest, O=CrySyS Lab, OU=PKI Labor, CN=pkilabor.crysys.hu
    Subject Public Key Info:
      Public Key Algorithm: id-ecPublicKey
      Public-Key: (256 bit)
      pub:
        04:b3:52:c1:aa:55:d2:6d:b8:56:ce:5d:7a:9e:0e:
        fd:25:09:56:cc:77:31:23:61:7b:c5:21:59:70:fe:
        e6:82:05:84:13:b4:48:c0:fc:2c:4b:74:10:84:19:
        37:3e:2c:7c:a0:1b:c2:85:d8:21:c9:b9:db:7e:51:
        44:45:22:98:04
      ASN1 OID: prime256v1
      NIST CURVE: P-256
    X509v3 extensions:
      X509v3 Subject Alternative Name:
        DNS:pkilabor.crysys.hu
    Signature Algorithm: ecdsa-with-SHA256
      30:46:02:21:00:da:b6:13:fb:ec:dc:c9:56:24:d0:7b:ea:80:
      8c:38:30:e0:20:87:a6:8d:e5:15:ad:97:a7:20:5f:08:db:7a:
      4a:02:21:00:e7:6b:90:66:a8:52:91:e0:a4:93:eb:0a:e9:29:
      af:83:19:a7:16:c9:a8:53:7d:6a:5c:15:54:1f:e7:18:bb:ed

meres@pki-meres ~/pkilabor/certificate_authority
```

## 2. Apache http szerver konfigurálása https kapcsolatokhoz

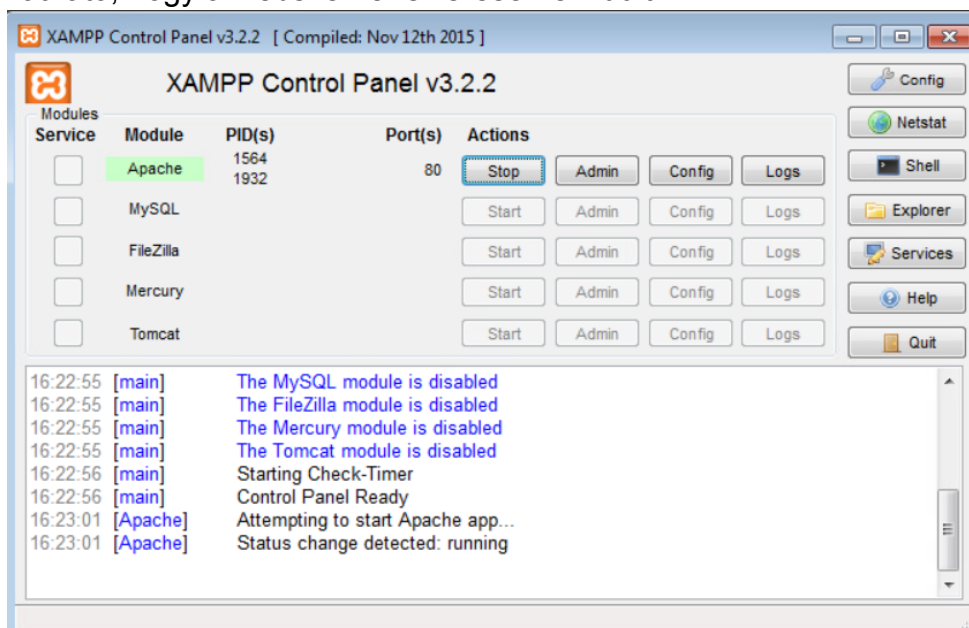
### 1. Hosts file módosítás

Az alábbi képen látható, hogy felvettük a megadott sort a hosts fileba:

```
# localhost name resolution is handled within DNS itself.
# 127.0.0.1      localhost
# ::1           localhost
# 127.0.0.1      pkilabor.crysys.hu          # CrySyS PKI labor re-route
```

### 2. Webszerver indítás

Látható, hogy a webszerver sikeresen elindult.



Látható, hogy működik a szerver és megjelenik a köszöntő oldal.



Valamint az átirányítás is működik:



### 3. SSL engedélyezés és konfiguráció

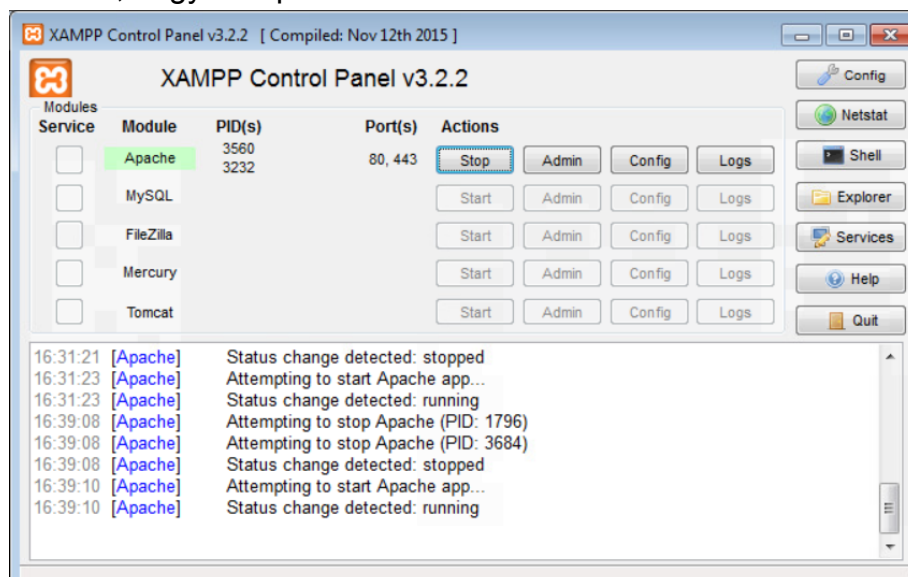
Az SSL konfigurációhoz a megadott módon módosítottuk a httpd.conf és httpd-ssl.conf file-okat.

```
66 #LoadModule socache_memcache_module modules/mod_socache_memcache.so
67 LoadModule socache_shmcb_module modules/mod_socache_shmcb.so
68 #LoadModule spelling_module modules/mod_spelling.so
69 LoadModule ssl_module modules/mod_ssl.so
70 LoadModule status_module modules/mod_status.so
71 #LoadModule substitute_module modules/mod_substitute.so
72 #LoadModule unique_id_module modules/mod_unique_id.so
73 #LoadModule userdir_module modules/mod_userdir.so
74 #LoadModule usertrack_module modules/mod_usertrack.so
75 LoadModule version_module modules/mod_version.so
76 #LoadModule vhost_alias_module modules/mod_vhost_alias.so
77 #LoadModule watchdog_module modules/mod_watchdog.so
78 #LoadModule xml2enc module modules/mod_xml2enc.so
```



```
523 <IfModule proxy_html_module>
524 Include conf/extra/proxy-html.conf
525 </IfModule>
526
527 # Secure (SSL/TLS) connections
528 Include conf/extra/httpd-ssl.conf
529 #
530 # Note: The following must must be present to support
531 #       starting without SSL on platforms with no /dev/random equivalent
532 #       but a statically compiled-in mod_ssl.
533 #
534 <IfModule ssl_module>
535 SSLRandomSeed startup builtin
536 SSLRandomSeed connect builtin
537 </IfModule>
538 #
539 # uncomment out the below to deal with user agents that deliberately
540 # violate open standards by misusing DNT (DNT *must* be a specific
541 # end-user choice)
542
543 # General setup for the virtual host
544 DocumentRoot "C:/xampp/htdocs"
545 ServerName pkilabor.crysys.hu:443
546 ServerAdmin admin@example.com
547 ErrorLog "C:/xampp/apache/logs/error.log"
548 TransferLog "C:/xampp/apache/logs/access.log"
549
550 #
551 # SSL Engine Switch:
552 # Enable/Disable SSL for this virtual host.
553 SSLEngine on
554
555 #
556 # Server Certificate:
557 # Point SSLCertificateFile "conf/ssl.crt/server.crt"
558 # the certificate is encrypted, then you will be prompted for a
559 # pass phrase. Note that a kill -HUP will prompt again. Keep
560 # in mind that if you have both an RSA and a DSA certificate you
561 # can configure both in parallel (to also allow the use of DSA
562 # ciphers, etc.)
563 # Some ECC cipher suites (http://www.ietf.org/rfc/rfc4492.txt)
564 # require an ECC certificate which can also be configured in
565 # parallel.
566 SSLCertificateFile "C:/cygwin64/home/meres/pkilabor/webserver_admin/pkilabor.crysys.hu.crt"
567 #SSLCertificateFile "conf/ssl.crt/server.crt"
568
569 #
570 # Server Private Key:
571 # If the key is not combined with the certificate, use this
572 # directive to point at the key file. Keep in mind that if
573 # you've both a RSA and a DSA private key you can configure
574 # both in parallel (to also allow the use of DSA ciphers, etc.)
575 # ECC keys, when in use, can also be configured in parallel
576 SSLCertificateKeyFile "C:/cygwin64/home/meres/pkilabor/webserver_admin/pkilabor.crysys.hu.key"
577 #SSLCertificateKeyFile "conf/ssl.key/server.key"
578
579 #
580 # Server Certificate Chain:
581 # Point SSLCertificateChainFile at a file containing the
582 # concatenation of PEM encoded CA certificates which form the
583 # certificate chain for the server certificate. Alternatively
584 # the referenced file can be the same as SSLCertificateFile "conf/ssl.crt/server.crt"
585 # certificate for convenience.
586 SSLCertificateChainFile "C:/cygwin64/home/meres/pkilabor/certificate_authority/ca.crt"
```

Látható, hogy az Apache szerver sikeresen elindult:

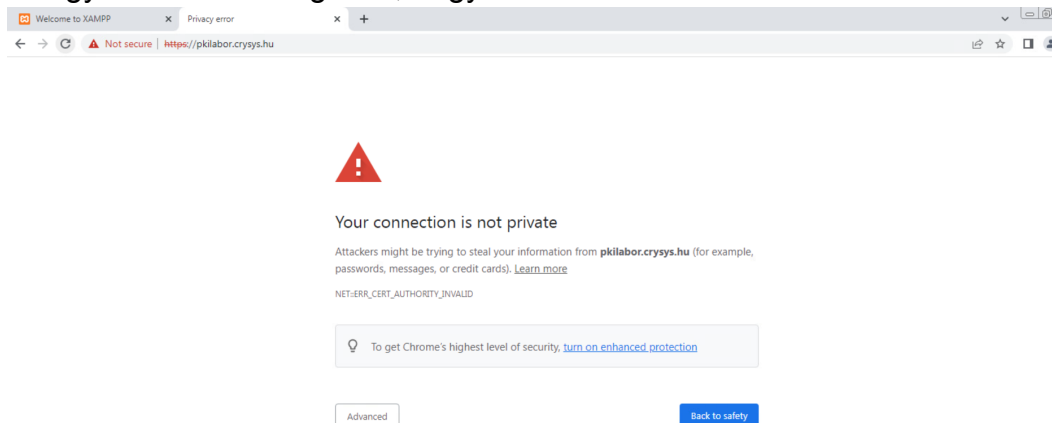




A mérést végezték:  
CGUOR8, Z8WK8D

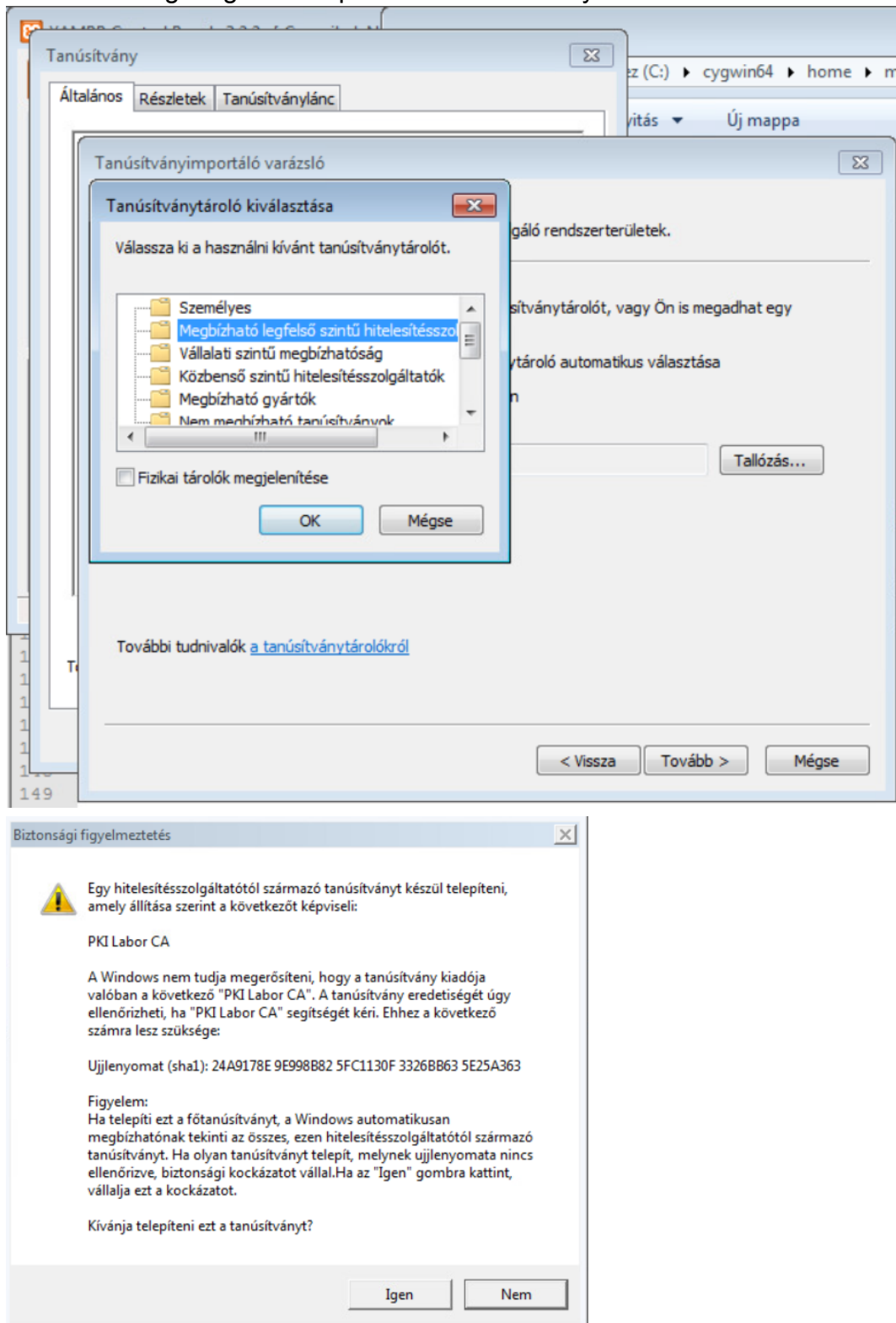
IT biztonság laboratórium (VIHIMB01)  
PKI mérés

És figyelmeztet a böngésző, hogy ismeretlen a kibocsátó CA:

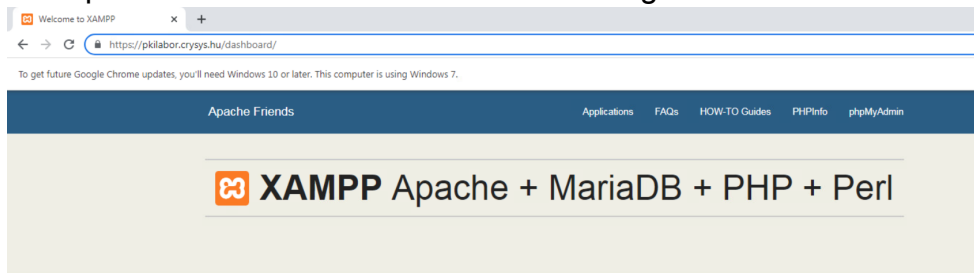


#### 4. Tanúsítvány telepítése a böngésző tanúsítványtárába

A varázsló segítségével telepítettük a tanúsítványt:



## A telepítést követően már az üdvözlő oldal fogad minket:



### Welcome to XAMPP for Windows 5.5.30

You have successfully installed XAMPP on this system! Now you can start using Apache, MariaDB, PHP and other components. You can find more info in the FAQs section or check the HOW-TO Guides for getting started with PHP applications.

Start the XAMPP Control Panel to check the server status.

#### Community

XAMPP has been around for more than 10 years – there is a huge community behind it. You can get involved by joining our Forums, adding yourself to the Mailing List, and liking us on Facebook, following our exploits on Twitter, or adding us to your Google+ circles.

#### Contribute to XAMPP translation at [translate.apachefriends.org](https://translate.apachefriends.org).

Can you help translate XAMPP for other community members? We need your help to translate XAMPP into different languages. We have set up a site, [translate.apachefriends.org](https://translate.apachefriends.org), where users can contribute translations.

### 3. Tanúsítvány alapú autentikáció bekapcsolása

#### 1. Elfogadott tanúsítványok tárának építése

Miután letöltöttük a megadott tanúsítványokat az <https://srv.e-szigno.hu> oldalról az alábbi módon konvertáltuk át PEM formátumra:

```
meres@pki-meres ~/pkilabor/webserver_admin
$ openssl x509 -inform DER -outform PEM -in TRootCA2008.crt -out TRootCA2008_pem.crt

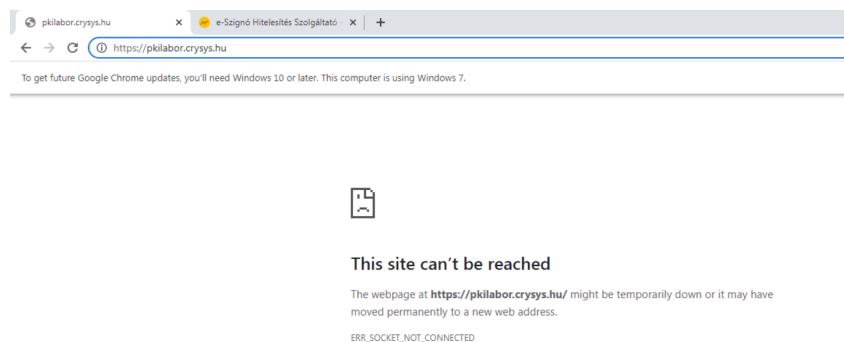
meres@pki-meres ~/pkilabor/webserver_admin
$ openssl x509 -inform DER -outform PEM -in testeca2017.crt -out testeca2017_pem.crt
```

#### 2. SSL konfiguráció

A `httpd-ssl.conf` fileban beállítottuk az előbb beszerezett tanúsítvány elérési útvonalát.

```
155 # Server Certificate Chain:
156 # Point SSLCertificateChainFile at a file containing the
157 # concatenation of PEM encoded CA certificates which form the
158 # certificate chain for the server certificate. Alternatively
159 # the referenced file can be the same as SSLCertificateFile "conf/ssl.crt/server.crt"
160 # certificate for convenience.
161 SSLCertificateChainFile "C:/cygwin64/home/meres/pkilabor/certificate_authority/ca.crt"
162
163 # Certificate Authority (CA):
164 # Set the CA certificate verification path where to find CA
165 # certificates for client authentication or alternatively one
166 # huge file containing all of them (file must be PEM encoded)
167 # Note: Inside SSLCACertificatePath you need hash symlinks
168 # to point to the certificate files. Use the provided
169 # Makefile to update the hash symlinks after changes.
170 SSLCACertificateFile "C:/cygwin64/home/meres/pkilabor/webserver_admin/auth_ca.pem.crt"
171
172 # Certificate Revocation Lists (CRL):
173 # Set the CA revocation path where to find CA CRLs for client
174 # authentication or alternatively one huge file containing all
175 # of them (file must be PEM encoded).
176 # The CRL checking mode needs to be configured explicitly
177 # through SSLCAREvocationCheck (defaults to "none" otherwise).
178 # Note: Inside SSLCAREvocationPath you need hash symlinks
179 # to point to the certificate files. Use the provided
180 # Makefile to update the hash symlinks after changes.
181 SSLCAREvocationPath "C:/Apache24/conf/ssl.crl"
182 SSLCAREvocationFile "C:/Apache24/conf/ssl.crl/ca-bundle.crl"
183 SSLCAREvocationCheck chain
184
185 # Client Authentication (Type):
186 # Client certificate verification type and depth. Types are
187 # none, optional, require and optional_no_ca. Depth is a
188 # number which specifies how deeply to verify the certificate
189 # issuer chain before deciding the certificate is not valid.
190 SSLVerifyClient require
191 SSLVerifyDepth 10
192
```

Ezután valamilyen ismeretlen hiba (mindenkinél jelentkezett) nem töltött be az oldal, annak ellenére, hogy itt is az üdvözlő képernyőt kellett volna látnunk.



## 4. Tanúsítványadatok kinyerése

1. Apache konfigurálás
2. Adatok feldolgozása PHP szkriptből

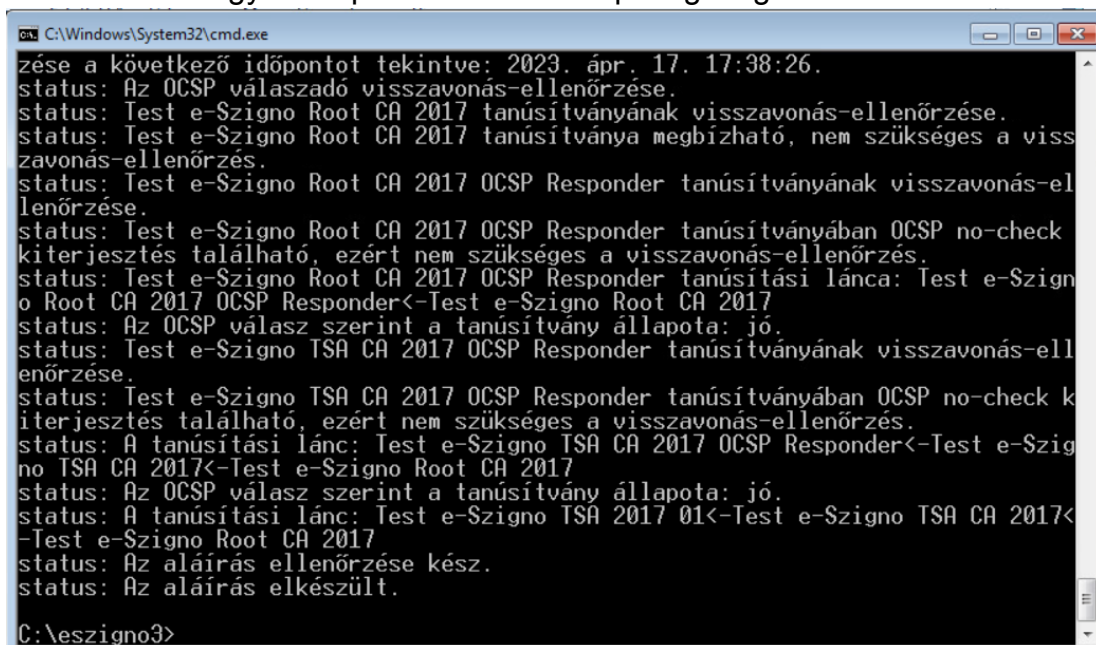
## 5. SSL tanúsítványok vizsgálata

1. A pkilabor.crysys.hu tanúsítvány vizsgálata
2. Az e-szigno.hu szervertanúsítvány vizsgálata

## 6. Digitális aláírások vizsgálata

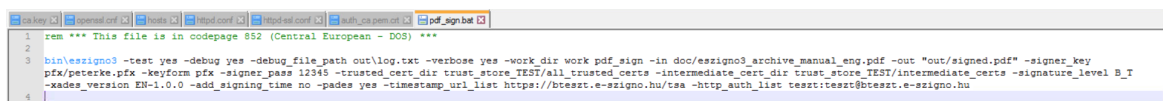
1. Aláírt PDF készítése parancssorból

Elkészítettünk egy aláírt pdf-et a mint a script segítségével:



```
C:\Windows\System32\cmd.exe
zése a következő időpontot tekintve: 2023. ápr. 17. 17:38:26.
status: Az OCSP válaszadó visszavonás-ellenőrzése.
status: Test e-Szigno Root CA 2017 tanúsítványának visszavonás-ellenőrzése.
status: Test e-Szigno Root CA 2017 tanúsítványa megbízható, nem szükséges a visszavonás-ellenőrzés.
status: Test e-Szigno Root CA 2017 OCSP Responder tanúsítványának visszavonás-ellenőrzése.
status: Test e-Szigno Root CA 2017 OCSP Responder tanúsítványában OCSP no-check kiterjesztés található, ezért nem szükséges a visszavonás-ellenőrzés.
status: Test e-Szigno Root CA 2017 OCSP Responder tanúsítási lánc: Test e-Szigno Root CA 2017 OCSP Responder<-Test e-Szigno Root CA 2017
status: Az OCSP válasz szerint a tanúsítvány állapota: jó.
status: Test e-Szigno TSA CA 2017 OCSP Responder tanúsítványának visszavonás-ellenőrzése.
status: Test e-Szigno TSA CA 2017 OCSP Responder tanúsítványában OCSP no-check kiterjesztés található, ezért nem szükséges a visszavonás-ellenőrzés.
status: A tanúsítási lánc: Test e-Szigno TSA CA 2017 OCSP Responder<-Test e-Szigno TSA CA 2017<-Test e-Szigno Root CA 2017
status: Az OCSP válasz szerint a tanúsítvány állapota: jó.
status: A tanúsítási lánc: Test e-Szigno TSA 2017 01<-Test e-Szigno TSA CA 2017<-Test e-Szigno Root CA 2017
status: Az aláírás ellenőrzése kész.
status: Az aláírás elkészült.
C:\esigno3>
```

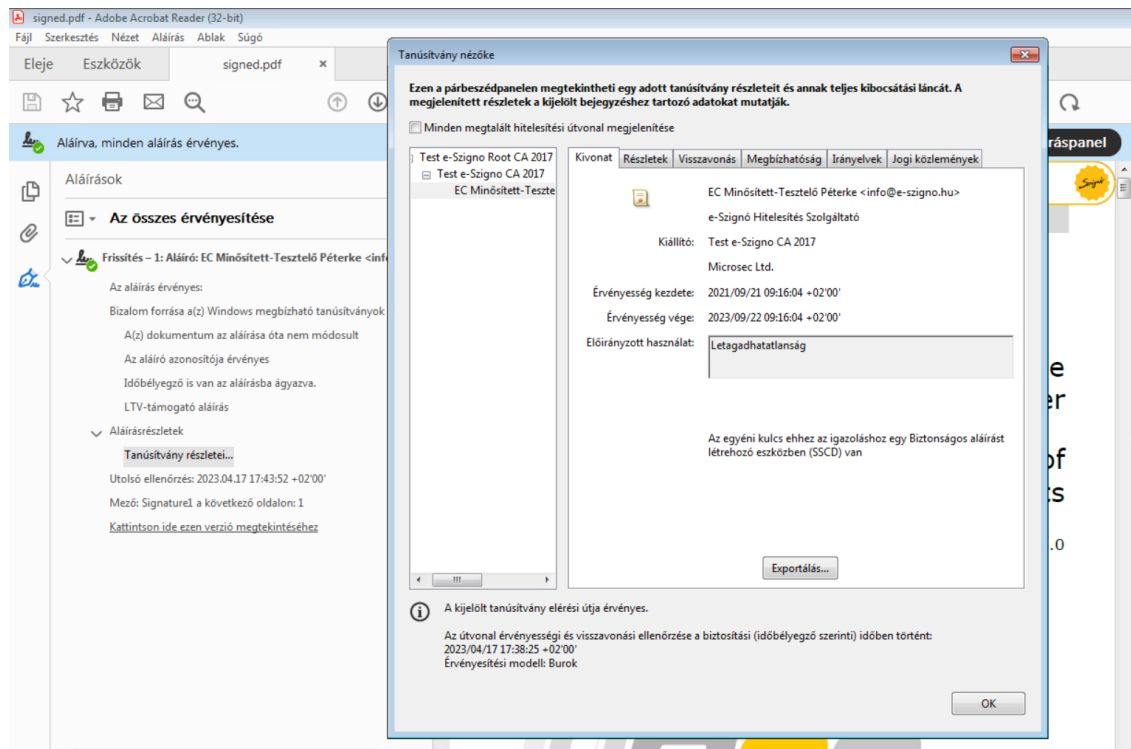
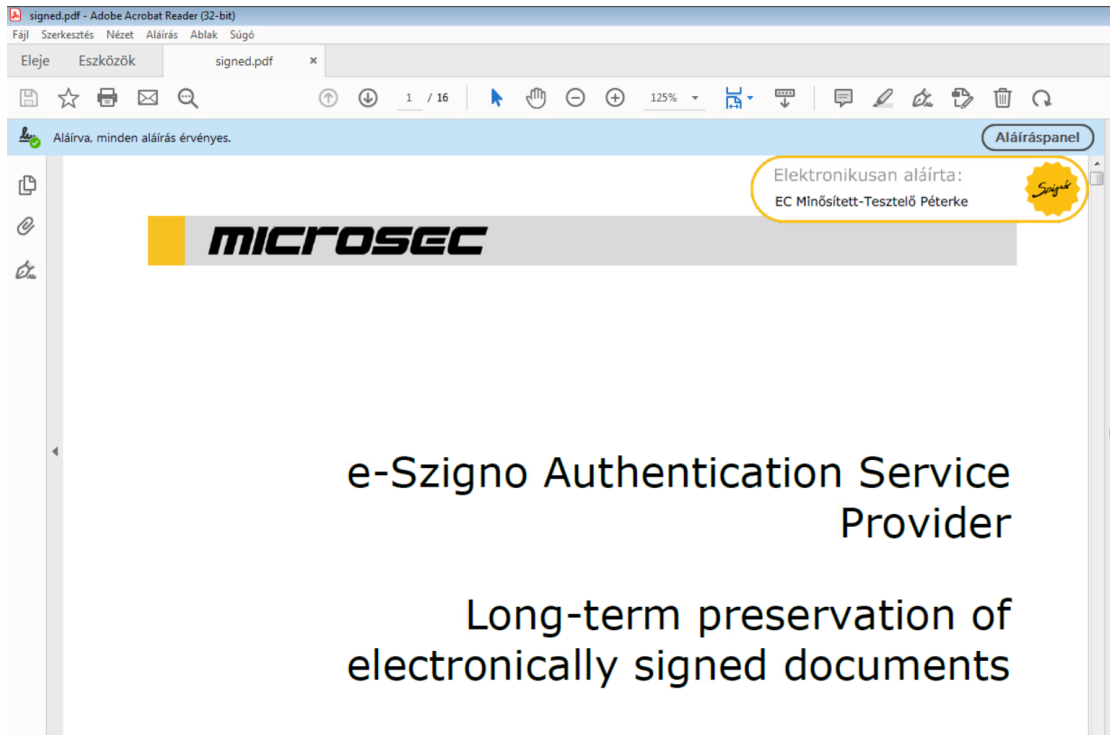
A script futtatásához egy kis módosításra volt szükség. Az aláírni kívánt pdf nem létezett:



```
1 rem *** This file is in codepage 852 (Central European - DOS) ***
2
3 bin\esigno3 -test yes -debug yes -debug_file_path out\log.txt -verbose yes -work_dir work_pdf_sign -in doc/esigno3_archive_manual_eng.pdf -out "out/signed.pdf" -signer_key
4 pfx/peterke.pfx -keyform pfx -signer_pass 12345 -trusted_cert_dir trust_store_TEST/all_trusted_certs -intermediate_cert_dir trust_store_TEST/intermediate_certs -signature_level B_T
-xades_version EN-1.0.0 -add_signing_time no -pades yes -timestamp_uri_list https://btest.e-szigno.hu/tsa -http_auth_list test:test@btest.e-szigno.hu
```

2. Adobe Reader konfiguráció Windows tanúsítványtár használatához

Az Adobe Reader segítségével megnyitottuk az aláírt pdf-et. Itt meg tudtuk nézni az elektronikus aláírás adatait:



### 3. Az e-Szignóval aláírt PDF-ek vizsgálata

### 4. Aláírás Adobe Readerrel