Építőipari Monitoring-és Adatszolgáltató Rendszer

Üvegkapu AMS tanúsítvány igénylés

v1.0

Tartalom

1. Bevezető

A dokumentum célja, hogy segítséget nyújtson a sikeres fizikai AMS fizikai teszt elvégzése után az éles tanúsítvány igényléshez szükséges .csr fájl létrehozásához. A dokumentációban található leírás feltétele a tanúsítvány megfelelő kezeléséhez és aláírásához, tartalmi előírásait kérjük betartani.

2. Tanúsítvány igénylése

2.1.Szabványok és ajánlások

Jelen dokumentumban hivatkozott szabványok és ajánlások listáját az alábbi táblázat foglalja össze:

Kulcsszó	
RFC 5280 **X.509** **CRL**	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile https://www.ietf.org/rfc/rfc5280.txt
RFC 6818 **X.509** **CRL**	Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile https://tools.ietf.org/html/rfc6818
RFC 6960 **OCSP**	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol (OCSP) https://tools.ietf.org/html/rfc6960
RFC 2986 **PKCS#10**	PKCS #10: Certification Request Syntax Specification Version 1.7 https://tools.ietf.org/html/rfc2986

Ezekhez az alábbi OID-ok használatát írjuk elő:

- **O (Organization, OID 2.5.4.10*)*:** *"A gyártó cég neve"* (max 64 karakter)
- **OU (Organization Unit, OID 2.5.4.11):** Uvegkapu AMS tanusitvany
- **L (Location):** *"Budapest"*
- **S(State):** *"Budapest"*
- **C(Country, OID 2.5.4.6):** HU
- **E(Email):** a gyártó központi e-mail címe *"gyartoceg@ceg.hu"*
- **CN (Common Name, OID 2.5.4.3):** a gyártó szoftverének megnevezése és a tesztelés során használt verzió száma

Az Üvegkapu AMS CA által kiállított tanúsítványok **érvényességi időtartama egységesen 2 év**.

2.2.Tanúsítványkérelem létrehozására Windows környezetben

Tesztelési céllal, Windows operációs rendszer környezetben, parancssorból a certreq segédprogram használatával hozhatunk létre tanúsítványkérelmet:

https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/certreq_1

Teszt tanúsítványkérelem létrehozása

A tanúsítványkérelem példához az alábbi konfigurációs állományhoz hasonlót kell összeállítani:

```
;
; amscert.ini
;
[NewRequest]
; A CN mezoben az AMS szoftver nevet es verzioszamat szukseges megadni maxium 64 karakter hosszusagban
; Az O mezoben az AMS gyarto cegnevet szukseges megadni maximumx 64 karakter hosszusagban
; Az emailAddress mezoben az AMS gyarto e-mail cimet szukseges megadni
; Az L mezoben az AMS gyarto szekhelyenek varosat kell megadni
; Az ST mezoben az AMS gyarto szekhelyenek megyejet
Subject = "CN=szoftver neve és verziószáma,O=cegnev kft.,E=info@aaa.kom,L=Budapest,ST=Budapest"
KeyLength = 4096
KeyUsage = "CERT_DIGITAL_SIGNATURE_KEY_USAGE | CERT_NON_REPUDIATION_KEY_USAGE | CERT_KEY_ENCIPHERMENT_KEY_USAGE"
HashAlgorithm = SHA256
KeyAlgorithm = RSA
Exportable = TRUE
MachineKeySet = TRUE
SMIME = FALSE
PrivateKeyArchive = FALSE
UserProtected = FALSE
UseExistingKeySet = FALSE
ProviderName = "Microsoft Enhanced RSA and AES Cryptographic Provider"
ProviderType = 24
RequestType = PKCS10

[EnhancedKeyUsageExtension]
OID=1.3.6.1.5.5.7.3.2
```

A .ini fájl neve tetszőleges, fontos, hogy a parancs futtatásához azt használjuk a példa szerint.

Fontos megjegyeznünk, hogy a fenti példa konfigurációs állományban az Exportable=TRUE paraméter lehetővé teszi a létrehozott kulcspár átmozgatását másik számítógépre, illetve a MachineKeySet=TRUE paraméter alapján a számítógép tanúsítványtárában jön létre a kulcspár, és ide kell betölteni a kiadott tanúsítványt is. Utóbbi esetén rendszergazdaként szükséges indítani a CertReq parancsot.

A kiállított tanúsítványkérelemben kötelező adat a sikeres fizikai teszten alkalmazott a gyártó által fejlesztett szoftver nevének és verziószámának megadása, aminek a részére a tanúsítványkérelem kiállításra kerül. Ezt az adatot a fent látható módon a Subject CN mezőjében kell rögzíteni, a példában szereplő szoftver megnevezése és verziószáma tehát „szoftvernev v1.2.3”.

A tanúsítvány kérelem előállítása parancssorból az alábbi paranccsal végezhető el:

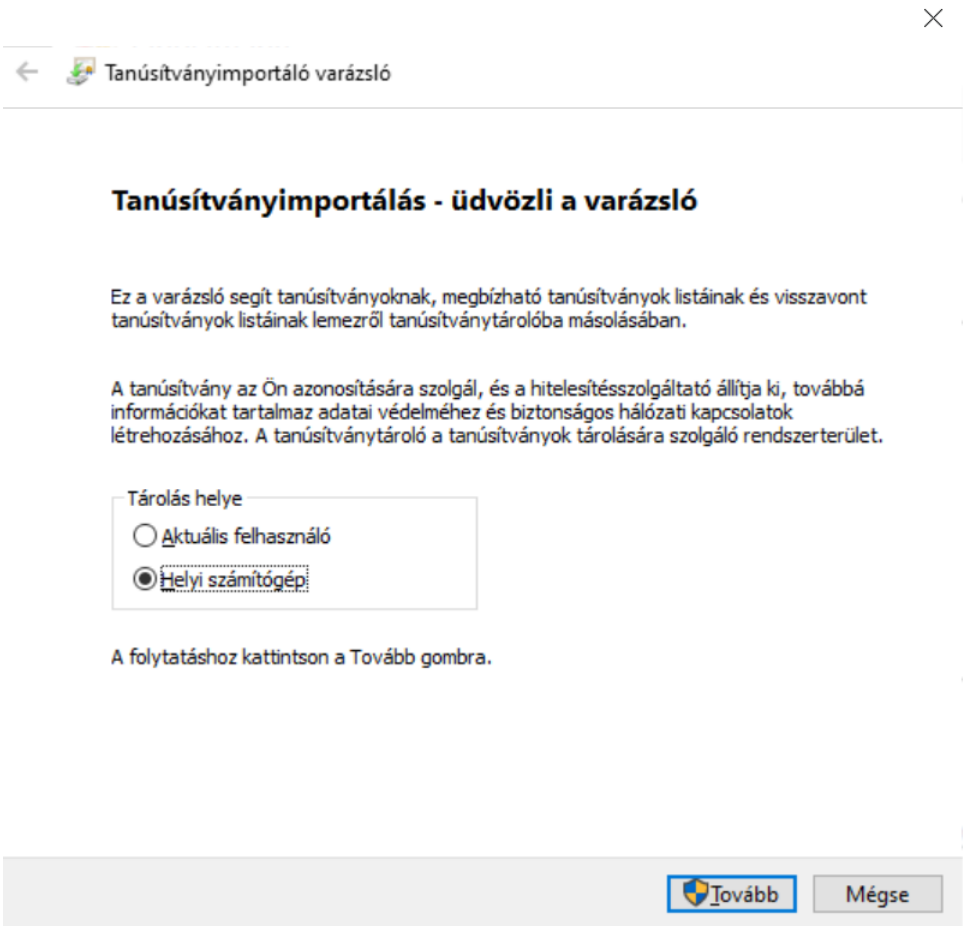
```
CertReq –New amscert.ini amsfajlneve.csr
```

A parancs futtatása után létrejövő .csr fájlt kell Datrak számára elküldeni aláírásra.

Miután visszakapta a gyártó az aláírt tanúsítványt importálva a local computer tanúsítvány tárába, a teljes tanúsítvány és privát kulcsa exportálható PKCS#12 (PFX) formátumban.

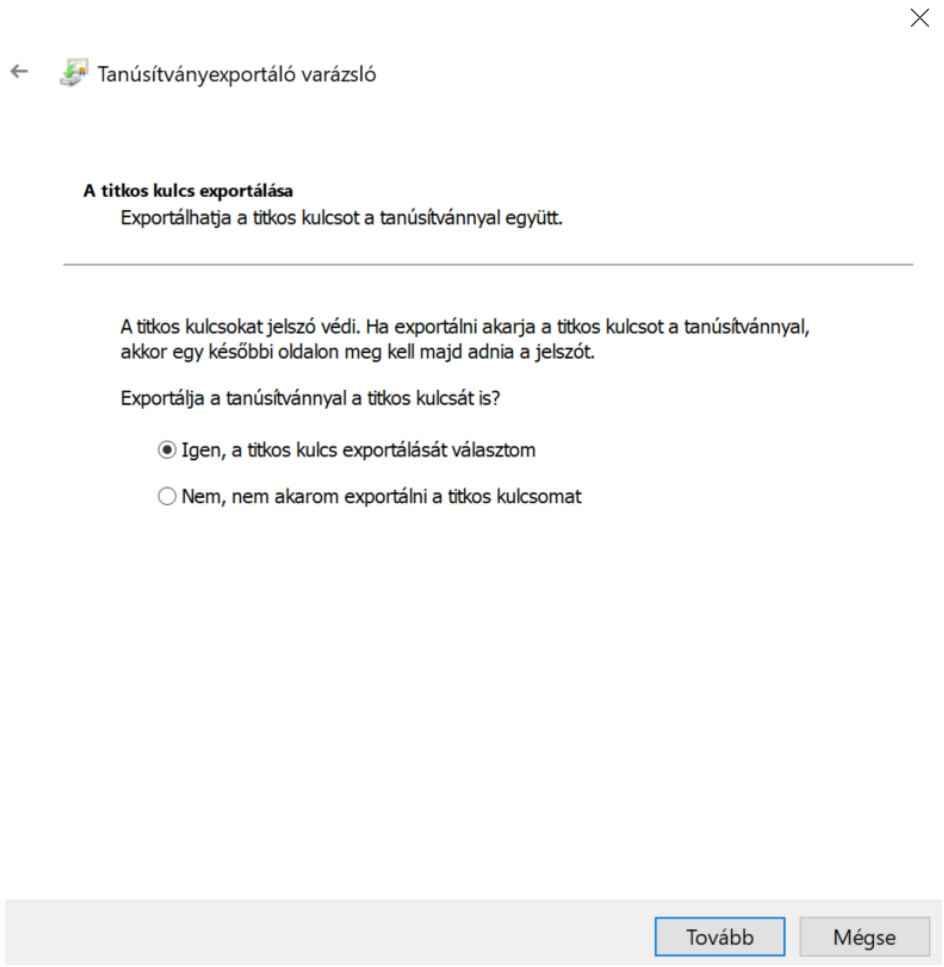
A csr fájl generálás során a privát kulcs letárolása megtörténik azon az operációs rendszeren, amelyen az igénylést futtatják.

A visszakapott aláírt tanúsítványt megnyitva telepíteni szükséges. **Fontos,** hogy a tanúsítvány importálása abba a környezetbe kerüljön, ahol az igény generálás is történt (helyi számítógép).



A következő lépésben a telepítésvarázsló automatikusan felkínálja a tanúsítványtípusnak megfelelő tanúsítványtárolót.

Megnyitjuk a számítógép-tanúsítványok kezelése alkalmazást, ahol a személyes tanúsítványok alatt megtalálható a beimportált tanúsítvány, amit szükséges exportálni. Az exportáló varázsló lépései között **fontos** kiválasztani a titkos kulcs exportálása opciót. Ezzel kerül be a privát kulcs a kiexportált .pfx állományba.



2.3.Tanúsítványkérelem létrehozása Linux környezetben

Linux operációs rendszer környezetben, parancssorból az **openssl** segédprogram használatával hozhatunk létre tanúsítványkérelmet

https://www.openssl.org/docs/manmaster/man1/openssl.html

AMS tanúsítványkérelem létrehozása

A tanúsítvány kérelem példához az alábbi konfigurációs állományhoz hasonlót kell összeállítani:

```
#
# amscert.conf
#
[ req ]
default_bits       = 4096
default_md         = sha256
prompt             = no
encrypt_key        = no
distinguished_name = req_distinguished_name
req_extensions     = req_extensions

[ req_distinguished_name ]
# A CN mezoben az AMS szoftver nevet es verzioszamat szukseges megadni maxium 64 karakter hosszusagban
CN                 = "szoftver neve es verzioszama"
```

```
# Az O mezoben az AMS gyarto cegnevet szukseges megadni maximumx 64 karakter hosszusagban
O               = "cegnev kft."
# Az emailAddress mezoben az AMS gyarto e-mail cimet szukseges megadni
emailAddress      = "info@kac.ku"
# Az L mezoben az AMS gyarto szekhelyenek varosat kell megadni
L               = "Budapest"
# Az ST mezoben az AMS gyarto szekhelyenek megyejet
ST              = "Budapest"


[ req_extensions ]
keyUsage        = digitalSignature, keyEncipherment, nonRepudiation
extendedKeyUsage  = clientAuth
extendedKeyUsage  = clientAuth
```

A privát kulcs és a tanúsítványkérelem előállítása parancssorból az alábbi módon történik:

```
openssl req -outform PEM -config amscert.conf -new -newkey rsa:4096 -keyout privat_kulcs.key -out
gyarto_uvegkapu_certificate_csr_4096.csr
```

A „-keyout” paraméterben a privát RSA kulcsállomány nevét kell megadni (a fenti példában „privat_kulcs.key”). Az „-out” paraméterben a tanúsítványigény állománynevét szükséges megadni (a fenti példában „gyarto_uvegkapu_certificate_csr_4096.csr”.

A kiállított tanúsítványkérelemben kötelező adat a sikeres fizikai teszten alkalmazott a gyártó által fejlesztett szoftver nevének és verziószámának megadása, aminek a részére a tanúsítványkérelem kiállításra kerül. Ezt az adatot a fent látható módon a Subject CN mezőjében kell rögzíteni, a példában szereplő szoftver megnevezése és verziószáma tehát „szoftvernev v1.2.3”.

A parancs futtatása után létrejövő .csr fájlt kell Datrak számára elküldeni aláírásra.

A tanúsítványkérelem-állományban lévő adatok helyességét az alábbi parancs segítségével ellenőrizhetjük (a „-in” paraméterben az újonnan elkészített tanúsítvány kérés állománynevét szükséges megadni):

```
openssl req -in gyarto_uvegkapu_certificate_csr_4096.csr -noout –text
```

3. Tanúsítvány használata

A csr fájl elkészítése és Datrak felé továbbítása után az igénylő egy aláírt tanúsítványt kap vissza, amit a gyártó szoftverének megfelelő formátumba átalakítva (pl: pfx) használ az alkalmazásában annak érdekében, hogy az AMS szoftver kommunikálni tudjon a HFE eszközzel és így az Üvegkapu rendszerével.

Az előminősítés folyamatában a fizikai tesztek alkalmával ugyanez a kommunikáció lett kialakítva azzal a különbséggel, hogy a tanúsítvány Datrak oldalról lett biztosítva a gyártó részére.