

# TCS

Auto-generated book for TCS

- TCSCertTypes
- TCS ServerCert
- TCS

# TCSCertTypes

Régi (Digicertes) típus név	Sectigo tanúsítványtípus	Leírás
SSL Plus	GÉANT OV SSL	Egy szerver névre érvényes tanúsítvány. A www.valami.hu-formájú nevek esetében tartalmazza a valami.hu nevet is.
Multi-Domain SSL	GÉANT OV Multi-Domain	Több szerver nevet tartalmazó tanúsítvány
EV SSL Plus	GÉANT EV SSL	Egy szerver névre érvényes Extended Validation tanúsítvány
EV Multi-Domain	GÉANT EV Multi-Domain	Több szerver névre érvényes Extended Validation tanúsítvány
Grid Robot Email	GÉANT IGTF-Classic-Robot Email	Grid e-mail szolgáltatásra és kliens azonosításra érvényes robot tanúsítvány, amelyet az IGTF Grid rendszerei elfogadnak
Grid Robot Name	GÉANT IGTF-MICS-Robot Personal	Általános Grid robot tanúsítvány, amelyet az IGTF Grid rendszerei elfogadnak
Digital Signature Plus	GÉANT Personal Certificate	Személyes tanúsítvány azonosításra, dokumentum és e-mail aláírásra.
Wildcard Plus	GÉANT Wildcard SSL	Egy teljes tartományra érvényes szerver tanúsítvány (pl. *.domain.hu). Wildcard tanúsítványoknál nem lehetséges további neveket tenni a tanúsítványba, így egy wildcard tanúsítvány csak egyetlen domain alá érvényes.
Code Signing	Code Signing	Számítógépes programkódok aláírására szolgáló tanúsítvány
Document Signing	Document Signing Certificate	Hivatalos dokumentumok aláírására szolgáló tanúsítvány, amely tartalmazza az aláíró intézmény nevét is.
Grid Premium	GÉANT IGTF-MICS Personal	Biztonságos e-mail, dokumentum aláírás és kliens azonosítás céljaira érvényes olyan tanúsítvánnyal, amelyet az IGTF Grid rendszerei elfogadnak
Grid Host Multi-domain SSL	GÉANT IGTF Multi-Domain	Grid e-Science szerver tanúsítvány, amelyet az IGTF Grid rendszerei elfogadnak

Régi (Digicertes) típus név	Sectigo tanúsítványtípus	Leírás
.	GÉANT Unified Communications Certificate	.

# TCS\_ServerCert

## Usage

With this script, you can generate a certificate request that you can submit manually to Terena TCS service. It's possible to include multiple SubjectAltName -s in the request, such as `aai.niif.hu` and `www.aai.niif.hu`.

This script creates the following files in your current working directory:

- `hostname.you.provided.first.org.key` (private key)
- `hostname.you.provided.first.org.csr` (certificate request)

## Program code

```
#!/usr/bin/perl -w

print "Please enter the fqdn's of the hosts one at a line\n";
print "Press Ctrl-D when done or Ctrl-C to cancel\n";

my $h;
my @hosts;

while ($h=<STDIN>) {
    chomp ($h);
    #XXX sanity check
    push @hosts,$h;
}

my $tmpfile=`mktemp`;
chomp $tmpfile;

my $defaulthost=$hosts[0];
my @opensslReqCmd=("openssl","req","-new","-nodes","-config","$tmpfile","-out","$defaulthost.csr");
```

```

#for re-key, you'd use:
#if (-r "$defaulthost.key") {
    #push @opensslReqCmd,("-key","$defaulthost.key");
#}

my @opensslVerifyCmd=("openssl","req","-text","-in","$defaulthost.csr");

&mkConfig($tmpfile,@hosts);

umask 0077;
system @opensslReqCmd;
system @opensslVerifyCmd;

unlink $tmpfile;

sub mkConfig(@) {
    my $out=shift;
    my @hosts=@_;
    my $defaulthost=$hosts[0];

    open (CONF,">$out") or die "$!";

    print CONF <<EOS;

[ req ]
default_bits      = 2048
default_keyfile    = $defaulthost.key
default_days      = 1095 # 3x365 days
default_md        = sha256
distinguished_name = req_distinguished_name
req_extensions     = v3_req
prompt            = no

[ req_distinguished_name ]
CN                = $defaulthost

[ v3_req ]
subjectAltName     = \@alt_names

```

```
[alt_names]
```

```
EOS
```

```
for (my $i=1; $i<=$#hosts+1; $i++) {  
    print CONF "DNS." . $i . "          = " . $hosts[$i-1] . "\n";  
}  
close CONF;  
}
```

# Apache config

This is how you can instruct Apache to use the new cert

```
SSLCertificateFile /path/to/your/pki/hostname.you.provided.first.crt  
SSLCertificateKeyFile /path/to/your/pki/hostname.you.provided.first.key  
SSLCertificateChainFile /path/to/your/pki/hostname.you.provided.first-chain.crt
```

# Self-signed

It's not recommended to use CA-signed certificates with your IdPs or SPs. It has no benefits and has some drawbacks (ie. some older versions of mod\_ssl refuse to work with expired SP certs).

Instead, you should generate a self-signed certificate with the following commands (please adjust the subject):

```
export host=your.host.name  
openssl req -new -newkey rsa:2048 -subj "/C=HU/O=NIIF/OU=AAI/CN=$host" -days 10000 -nodes \  
-keyout $host-fed.key -out $host-fed.csr  
openssl x509 -in $host-fed.csr -out $host-fed.crt -req -signkey $host-fed.key
```

# TCS

## A KIFÜ

# tanúsítványszolgáltatás

### Értesítések:

- *2020.08.19-től nem lehet 2 éves TLS tanúsítványokat igényelni a Sectigo rendszerében!*  
--->[LINK](#)
- *2021.03.01-től a Sectigo kiveszi a tanúsítványokból az utca megnevezésére és az irányítószámra vonatkozó információkat. Ez a már kiadott tanúsítványokat nem érinti, és nem is szükséges lecserélni azokat!* --->[LINK](#)

---

A Megbízható Tanúsítványszolgáltatás (Trusted Certificate Service, **TCS**) olyan tanúsítványok kiállítását biztosítja, amelyet az elterjedt böngészők és kliensprogramok megbízhatónak tartanak, valamint bizonyos típusaik Grid hálózatokban is elfogadhatóak. A felület az alábbi linken érhető el: <https://cert-manager.com/customer/KIFU> Az eléréséhez szükséges, hogy az intézmény létre legyen már hozva a felületen, és legalább egy adminisztrátor be legyen állítva. Lásd a “Belépés” részt.

A TCS rendszerben a tanúsítványokat kiállító CA (a **Sectigo**) az igénylők azonosításának és a tanúsítványigénylések elbírálásának jogát és felelősségét átruházza a TCS rendszert használó intézmények erre felhatalmazott adminisztrátorai számára. Az igényléseket a Sectigo [validálja](#).

## Igényelhető tanúsítványok

- [Igényelhető tanúsítvány típusok](#)

## Szolgáltatás feltételei

A szolgáltatás kizárólag a Kormányzati Informatikai Fejlesztési Ügynökség azon intézményei számára vehető igénybe, amelyek erre szerződést kötöttek a KIFÜ-vel. Amennyiben szeretné igénybevenni a KIFÜ tanúsítványszolgáltatását, kérjük írjon az Ügyfélszolgálat emailcímére vagy hívja a +3614503070 telefonszámot.

# Különbségek az előző (DigiCertes) szolgáltatóhoz képest

## Új szolgáltató, új webes felület

A Sectigo a GÉANT Trusted Certificate Service (TCS) szolgáltatás új szállítója a DigiCert helyett. A Sectigo Certificate Manager-t (SCM) használjuk a DigiCert CertCentral helyett. A további részben bemutatjuk a legfontosabb változásokat.

“ Figyelem! A Sectigo SCM platformról törölni nem lehet. Ezt azt jelenti, hogy ha tévedésből igényelt egy tanúsítványt vagy rossz DNS TLD-t küldött be DCV-re vagy elírta a ACME account nevet, akkor ezeket csak a Sectigo Support tudja törölni az SCM platformról.

## Nincs "Divízió" objektum az új rendszerben

Az SCM-ben nem működik a divízió koncepciója, úgy ahogyan az a DigiCert CertCentralban volt.

- A KIFÜ-nek van egy SCM felülete, amelyet az összes KIFÜ adminisztrátor használ (az intézmények szintjén és a KIFÜ „superuser” szintjén), de a többi GEANT TCS tagország nem fér hozzá.
- Mivel nincs az a Divízió-rendszer, mint ami a DigiCertnél volt, így arra sincs lehetőség, hogy a velünk szerződött intézmények szabadon alkossanak Szervezet-objektumokat, amiket a Divízió fog össze. Ehelyett a KIFÜ intézményi szintjén hozunk létre egy szervezet objektumot a KIFÜ intézményei számára, és ehhez adunk meg egy intézményi adminisztrátort.
- Az Organization alatt lehetőség van kisebb szervezeti egységeket, Departmenteket létrehozni, és akár saját adminisztrátorokat rendelni hozzá.



# Nincs User-szintű felhasználó

A DigiCert CertCentral-ban két alapvető felhasználófajta létezik: "*Rendszergazdák*", akik tanúsítványokat igényelhetnek/jóváhagyhatnak, validációs folyamatokat indíthatnak, megváltoztathatják a beállításokat és más adminisztrátori szintű dolgokat végezhetnek; valamint a "*Felhasználók*", akik csak tanúsítványokat kérhetnek (de mégis hitelesített felhasználói voltak a CertCentalnak, csakúgy, mint az adminisztrátorok). Az SCM-ben alapvetően csak adminisztrátori felhasználók vannak. Ez azt jelenti, hogy elvileg nem lehetnek olyan felhasználók, akik bejelentkezhetnek az SCM-be, és csak tanúsítványokat kérhetnek. De az SSL tanúsítványok részben kínálunk erre is megoldást.

## Department (szervezeti egység)

Az SCM lehetővé teszi a szervezetek alatt kisebb szervezeti egységek - departmentek - létrehozását. Csakúgy, mint a szervezet neve, ami belekerül a tanúsítvány "O =" objektumba, az egység neve is belekerül a tanúsítvány "OU =" objektumába. A departmentek kétféle módon használhatók:

- Egyszerű eszközként a tanúsítványok rendezéséhez és a helyes "OU =" objektum beállításához, de a jóváhagyást továbbra is a szervezet adminisztrátorai fogják végrehajtani.
- A tanúsítványok jóváhagyásának átruházásával a Department adminisztrátorainak. A legtöbb esetben ez összekapcsolódik egy aldomain (vagy egy teljesen más domain) regisztrálásával, és annak használatára korlátozza a szervezeti egységet.

## MRAO, RAO, DRAO!

Az adminisztrátoroknak három szintje létezik az SCM-ben, és mindegyiket RAO-val (Registration Authority Officer) jelölik:

- **MRAO:** a "superuser szint", a KIFÜ munkatársai látják el ezt a szerepet, amely képes kezelni minden szervezetet, osztályt, domaint, tanúsítványt, rendszergazdát stb.
- **RAO:** szervezeti adminisztrációs szint, egy szervezet működtetéséhez, valamint a szervezethez tartozó osztályok, tartományok, tanúsítványok, adminok stb. kezeléséhez
- **DRAO:** a szervezet alatt lévő Department rész működtetésének adminisztrátori szintje, az ehhez tartozó tartományok, tanúsítványok, adminok stb. kezelése

Ennél kicsit összetettebben is szabályozható a rendszer: a RAO tartozhat egy vagy több szervezethez, a DRAO egy vagy több részleghez. Lehetőség van azt is beállítani, hogy csak SSL tanúsítványok, ügyfél tanúsítványok és/vagy kód aláírásokhoz szükséges tanúsítványokat legyen joga intézni. Így lehet egy adminisztrátor "RAO - SSL tanúsítványok" és "RAO - kliens tanúsítványok" jogkörökkel is egy-egy szervezet számára, miközben "DRAO - SSL tanúsítványok"

szerepkört is kaphat egy másik szervezethez tartozó szervezeti egységnél. Az első rendszergazda, akit a KIFÜ ad meg az intézményhez, RAO jogosultsággal rendelkezik, és teljes hozzáférése van az Organization területén mindenhez, így a további adminisztrátorok (RAO-k és DRAO-k) beállítása is az ő feladata.

## Első lépések

Amikor létrejön egy szervezeti egység az SCM felületén, generálódik számára egy ún. *Master key*, ezzel lesznek titkosítva az igényelt tanúsítványok. Ezt a kulcsot egy megfelelően biztonságos helyre le kell menteni. Az alábbi helyen található meg: **Settings** → **Encryption** fülön kell az intézményt kiválasztani. Itt kezdetben a státusz *Not initialized*. Meg kell nyomni az **Initialize Encryption** gombot a fenti menüsoron. Ekkor feldobja a privát kulcsot, amit ki kell másolni és egy text fájlban gondosan, védetten eltárolni. A felugró ablakon ezek után **Done** billentyűt megnyomva rákérdez, hogy elmentettük-e a kulcsot, majd bezárja a felugró ablakot és az intézmény státuszát *Public key is loaded* állapotúra változtatja. Ezek után rendeltetésszerűen lehet használni a felületet.

## Validációs folyamatok

### Szervezet validációja

Az *Organization* létrehozásakor annak validációját a KIFÜ MRAO jogosultságú adminisztrátorai indítják el. Csak ha a validáció sikeresen lezárult, akkor tudják az intézmény adminisztrátorai érdemben használni a felületet. Az *Organization* adatait a RAO jogosultságú adminisztrátorok tudják szerkeszteni, viszont bizonyos mezők átírása a szervezet újbóli validációját teszi szükségessé. Ebben az esetben értesíteni kell az MRAO adminisztrátorokat, hogy indítsák el a folyamatot.

### Domain validáció

A tanúsítványok kiállítása előtt érvényesítenie kell egy vagy több domaint. Ennek a folyamatnak több lépése van:

1. Győződjön meg arról, hogy a DNS-zónájában nincs CAA-rekord, amely megtiltja a Sectigo számára, hogy tanúsítványokat állítson ki az adott domainra. Ebben az esetben a domain validálása kudarcot vallana. Ha hiányzik a CAA-rekord vagy ott van de tartalmazza a „sectigo.com” bejegyzést, akkor menni fog a validáció.
2. Válassza a bal oldali menüből a **Domains** menüpontot, és nyomja meg a zöld színű + (Add) jelet. Töltse ki a domain nevet (example.org) és az opcionális leírást. Válassza ki a domainhez engedélyezni kívánt tanúsítványok típusát (SSL, kliens, CS). A fő domainhez

általában érdemes mindet engedélyezni, de a többi kiegészítő domainhez elegendő csak az SSL tanúsítványokat. A Client Certificate és a Code Signing-ot csak akkor szabad kijelölni, ha valóban használni szeretné azokat. Ha Departmenteket hozott létre, és ezt a tartományt az adott egység DRAO-jainak kell átruházni, nyissa le a választási sort, és engedélyezze a domaint a megfelelő egységnél és állítsa be a megfelelő típusokat is.

3. Nyomja meg újra az Add gombot, és pontosan ugyanezeket a lépéseket kell megtenni a "\*" -al kiegészített domainnév esetében is (a példánkban \*.example.org). **Ezt**

**mindenképpen tegye meg, hogy ne okozzon gondot az aldomainekre is igényelni tanúsítványt!**

4. Amennyiben egy DRAO jogosultságú személy vagy egy szűkített jogosultsággal bíró RAO személy indította a domain validációt, szükség van egy megfelelő jogosultságokkal rendelkező RAO vagy egy MRAO engedélyezésére is a delegációkat illetően.
5. A **Delegations** fülről váltson a **DCV (Domain Control Validation)** fülre. Jelölje ki a megfelelő domaint, és a megjelenő DCV gomb segítségével indítsa el a DCV folyamatot. Válasszon metódust:

- Az "Email" opcióval a tartomány öt lehetséges címe közül választható ki az, ami majd fogadja és kezeli az oda küldött e-maileket. Példánk esetében ez lehet az „admin@example.org”, „administrator@example.org”, „hostmaster@example.org”, „postmaster@example.org” vagy „webmaster@example.org”.
- A "CNAME" opciót választva az SCM létrehoz egy DNS CNAME rekordot a választott domainhez, amit be kell tenni a DNS zónába. Javasolt egy külső névfeloldóval ellenőrizni, hogy a CNAME rekord a helyén van-e és kívülről valóban látható. **Ezt a metódust javasoljuk mindenki számára, stabilan, gyorsan működik a tapasztalataink alapján!**
- **FIGYELEM! Ez a metódus kivezetésre kerül 2021. 11.15-én!** A ""HTTP / HTTPS" opció esetében egy bizonyos tartalommal létre kell hozni egy fájlt egy megadott névvel a domain névhez tartozó webkiszolgálón.

6. Kövesse a kiválasztott módszerre vonatkozó utasításokat.
7. Ha az érvényesítési folyamat rendben lezajlott, akkor a DCV lapon a Validation Status állapota Validated-re változik. A Delegations lapon a domain állapotának is "Validated"-nek kell lennie. A plusz sor a "\*" előtaggal bizonyos esetekben továbbra is "Not validated" státuszban van, de ez általában csak egy bizonyos ideig (pár órától egy napig) tart mire frissül.
8. Most már minden készen áll arra, hogy ezt a domaint és az aldomainjeit tanúsítványkéresekhez használja. Nem kell megvárni, hogy a "\*" előtagú domain is érvényes állapotba kerüljön.

**2021. decemberétől kizárólag subdomainre is elvégezhető a validáció!**

## Metódus módosítása

Amennyiben nem megfelelő metódus lett kiválasztva, illetve valamiért nem működik a választottnál a validáció, van lehetőség változtatni. Ehhez a **Settings → Domains → DCV** fülön ki kell jelölni az érintett domaint, ekkor megjelenik a domainlista fölött a DCV gomb, és arra kattintva felugrik egy kis ablak. Itt lehet visszalépni illetve bizonyos fázisban resetelni a választott metódust.

## Domain lejárat

A domainvalidáció 1 évig érvényes. A lejárat előtt figyelmeztetést küld a rendszer. Az újra validálás lehetősége pár nappal a lejárat előtt lesz éles. A lépések teljesen megegyeznek az első alkalommal történő validációs folyamattal.

## Departments (Szervezeti egységek)

### Department létrehozása:

1. Lépjen a **Settings** → **Organizations** elemre, és kattintson a megfelelő szervezeti sorra, majd a **Departments** gombbal jelenítse meg a listázási ablakot, és nyomja meg az **Add** gombot.
2. Adja meg a kívánt "OU =" név összetevőt a *Department Name* mezőnél. A név többi része megegyezik a szervezettel.
3. Válassza ki a **Client Certificate** fület, és tiltsa le a MRAO és a DRAO számára a Key Recovery kulcs-helyreállítást ("Allow Key Recovery by Master Administrators" és "Allow Key Recovery by Department Administrators").
4. Az egyéb opciókkal nem kell most foglalkozni, mivel ezek később is beállíthatóak. A befejezéshez nyomja meg az **OK** gombot.

### Departmenthez tartozó adminok

Most már létrehozhat olyan adminisztrátorokat, akik DRAO jogosultsággal rendelkeznek és csak ehhez az egységhez kapcsolódnak, nem pedig az egész szervezethez.

### A Departmenthez kapcsolódó domainek

Ha olyan department adminisztrátorokat (DRAO) ad hozzá, akik jóváhagyhatják a részleg tanúsítványait, akkor érdemes korlátozni őket a szervezeti egység saját domainjeire (department-example.com) vagy a fő domain aldomainjére (department.example.org). Az első esetben, amennyiben egy teljesen új domain van a részleg számára, akkor kövesse a fenti szokásos domain validálási eljárást a department-example.com és a \*.department-example.com esetében, a szervezeti egység számára delegálva azt. A második esetben, amikor az aldomainhez tartozó fő domain már hitelesítve van, adja hozzá a department.example.org és a \*.department.example.org domaint a department számára delegálva, de ekkor már nem kell kezdeményezni a DCV folyamatot, mivel az SCM elég okos ahhoz, hogy tudja, az example.org már érvényesítve van. Amint a fő domain esetében, itt is meg kell várni a department.example.org státuszának "Validated"-re váltását, amit némi késéssel a \*.department.example.org-é követ.

## Adminisztrátorok

További rendszergazdákat hozhat létre (RAO-kat az egész szervezet számára, vagy DRAO-kat a szervezeti egységek számára) az Admins lapon az **Add** gombra. A meglévő adminisztrátorokat szerkesztheti is, ha kiválasztja, majd megnyomja az Edit gombot.

1. Töltse ki a bejelentkezési adatokat (megfelelő felhasználói névvel), az e-mailt, az utónévet és a vezetéknévet. Javasoljuk, hogy hagyja üresen a többi kapcsolattartási információt, mivel erre nincs szükség.
2. Válassza ki a "*Your Institution*" résznél az Identity Provider-ét (IdP), és töltse ki az admin ePPN-jét ("*SWAMID identity*") az "*IdP Person Id*"-ben, hogy az adminisztrátor be tudjon jelentkezni SWAMID-en keresztül, ha a SAML helyesen van beállítva.
3. Az új rendszergazda számára jelszót kell megadni. Az első bejelentkezéskor meg kell azt változtatnia.
4. Válassza ki a kívánt jogosultságokat a **Privileges** fül alatt. Ne jelölje be a "*WS API use only*" opciót!
5. Válassza ki a kívánt szerepeket a **Roles** alatt, azaz RAO-t az egész szervezet számára vagy DRAO-t a létrehozott szervezeti egység számára, valamint azon tanúsítványtípust (SSL, kliens vagy kód aláírás) amely igénylését lehetővé kívánjuk tenni a számára.
6. Ha kész, akkor a kiválasztott jelszót közölnie kell az új adminisztrátorral (a rendszer nem küld e-mailt).

Azt határozottan javasoljuk, hogy hozzon létre saját admin felhasználókat is, hogy képes legyen látni, ki mit csinált a rendszerben. Úgy tűnik, hogy bizonyos privilégiumokat (társ-adminisztrátorok kezelése, DCV engedélyezése) jelenleg egyik RAO nem rendelhet hozzá a másikhoz. Ha ez előfordulna, írjon e-mailt az Ügyfélszolgálat emailcímére, hogy beállítsuk azokat.

## Zárolt felhasználói fiók

Lezáródhat, ha többször rossz bejelentkezési információkat ad meg. Ezután egy "Helytelen bejelentkezési adatok, a fiók zárolva van, a jelszó lejárt vagy a forrás IP-je le van tiltva" üzenetet kap. üzenet, amikor megpróbál bejelentkezni, akkor is, ha immár a helyes jelszót használja. Ez akkor is így lesz, ha jelszavát megváltoztatta egy másik rendszergazda, aki erre egyébként jogosult. A lezárás feloldását csak egy MRAO jogosultságú adminisztrátor végezheti el, így jelezze az ilyen jellegű problémát az Ügyfélszolgálatnál.

## SSL (szerver) tanúsítványok

### Tanúsítványok kérelmezése és jóváhagyása az SCM-ben

# adminisztrátorként

Lépjen a **Certificates** → **SSL certificates** elemre, és a tanúsítvány igényléséhez nyomja meg az **Add** gombot.

1. Válassza ki a *"Manual creation of CSR"* opciót.
2. Adjon meg egy CSR-t a szövegmezőbe való beillesztéssel, vagy tölts fel fájlként az **Upload CSR** gomb segítségével.
3. Válassza ki és tölts ki a megfelelő információkat a *"Basic info"* lépésben. Győződjön meg arról, hogy egy több domaint tartalmazó tanúsítványhoz a megfelelő típust választotta, hogy egy szöveges mezőt kapjon, ahol szükség esetén megadhatja a *"Subject Alternative Names"* - alternatív domainneveket. Ha valaki más nevében kéri, felveheti az e-mail címét külső igénylőként.
4. További beállítási lehetőségekhez kattintson a *"Click here for advanced options"* feliratra, hogy hozzáférjen egy megjegyzés mezőhöz, ahol megadhatja azokat az információkat, amelyeket később a tanúsítványban szeretne látni. Ne távolítsa el a címmezőket a *"Remove"* jelölőnégyzetek használatával, mivel ez úgy tűnik, hogy a tanúsítvány elakad, mivel az információ nem egyezik az előzetesen validált szervezet adataival.
5. A következő képernyőn fogadja el vagy utasítsa el az automatikus megújítást, és fejezze be az **OK** gombbal.

Ha az igénylő rendelkezik az *"Allow SSL auto approve"* jogosultsággal, akkor a tanúsítvány automatikusan jóváhagyásra kerül, és megjelenik mellette az *"Applied"* felirat. Ha az adminisztrátor nem rendelkezik ezzel a jogosultsággal, akkor a tanúsítvány *"Requested"* állapotba kerül, és manuálisan kell elfogadni a tanúsítvány kiválasztásával és az **Approve** megnyomásával. Amikor a tanúsítvány kiadásra kerül, annak státusza *"Issued"* lesz, és e-mailt kap erről az igénylő. Ha szükséges, akkor is letöltheti a tanúsítványt, ha rákattint annak kijelöléséhez, és használja a **Details** gombot, majd a **Select** gombot a *"Certificate download"* jobb oldalán.

## CSR generálására példák

### Egy domain esetén

```
openssl req -new -newkey rsa:4096 -nodes \  
-out domain_kifu_hu.csr \  
-keyout domain_kifu_hu.key \  
-subj "/C=HU/ST=Budapest/L=Budapest/O=KIFÜ/OU=IKT/CN=domain.kifu.hu"
```

### Több domain esetén

```
openssl req -new -newkey rsa:4096 -nodes \  
-out domainX_kifu_hu.csr \  
-keyout domainX_kifu_hu.key
```

```
-keyout domainX_kifu_hu.key \  
-subj "/C=HU/ST=Budapest/L=Budapest/O=KIFÜ/OU=IKT/CN=domain1.kifu.hu/CN=domain2.kifu.hu"
```

## Wildcard

```
openssl req -new -newkey rsa:4096 -nodes \  
-out star_domain_kifu_hu.csr \  
-keyout star_domain_kifu_hu.key \  
-subj "/C=HU/ST=Budapest/L=Budapest/O=KIFÜ/OU=IKT/CN=*.domain1.kifu.hu/CN=*.domain2.kifu.hu"
```

Ha csak lehet, kerüljük az emailcím használatát a subjectben. Ha valamiért mégis szerepeltetni kell, akkor vigyázni kell arra, hogy az emailcím domainje szerepeljen az adott Organization/Department levalidált domainjei között.

"Figyelem: A Sectigo ellenőrzi, hogy a Subjectben megadott adatok egyeznek-e az SCM felületén szereplő szervezeti adatokkal! Azaz az ST tagot akkor fogadja el, ha a szervezeti adatoknál ki van töltve a megye; valamint az OU-t csak akkor, ha az Organization alatt van Department is létrehozva. Ez utóbbi esetben ráadásul a CSR-ben szereplő domain(ek) delegálva kell legyen(ek) az adott Departmenthez!

# Nem adminisztrátor jogosultságú igénylések engedélyezése

Lehetőség van nem adminisztrátori jogkörrel rendelkező személyeknek is engedélyezni, hogy tanúsítványkérelmet nyújtsanak be az SCM felületén. Ehhez válassza a **Settings → Organizations** menüpontot, válassza ki a szervezetet, majd kattintson az **Edit** gombra. (Vagy ha csak egy szervezeti egységhez szeretné rendelni, akkor a szervezet kiválasztása után kattintson a **Department** gombra, válassza ki az egységet, és itt használja az **Edit** lehetőséget).

- Az **SSL certificate** lapon engedélyezze a "Self enrollment" opciót, és írjon egy titkos értéket az "Access Code" mezőbe, majd másolja ki a mező alatt található URL-t. Most elküldheti ezt az URL-t azoknak, akiket szeretné, hogy beléphessenek a nem adminisztrátorok számára fenntartott tanúsítvány igénylő felületre. Mint teszteléskor láthatja, hozzávetőlegesen ugyanazokat a mezőket tartalmazza ez az oldal, mint maga az SCM **"Add certificate"** része. Ne felejtse ellenőrizni az emailcímet amire elküldi a hozzáférést, illetve alakítson ki egy saját metódust a kérelmezők autentikálására!
- Amennyiben működik a SAML attribútum átadása a Sectigo felé (lásd a [SAML konfiguráció](#) szekciót), akkor engedélyezheti a **"Self enrollment via SAML"** funkciót is, titkosítva tarthatja a hozzáférési kódot, és elküldheti a felhasználók számára a Token mező alatti URL-t. Ezután a SAML használatával hitelesíteniük kell magukat mielőtt a fentiekkel megegyező igénylő űrlapra belépnének. Mivel az e-mail cím most az IdP-től érkezik a SAML-en keresztül, biztos lehet abban, hogy helyes, de eldöntheti, hogy szükség lesz-e

további autentikációra az igénylést megelőzően.

- Nem javasoljuk az "Automatically Approve Self Enrollment Requests" opció bejelölését! Legalább manuálisan jóvá kell hagyatni az ezen a módon érkező tanúsítványkérdéseket!
- Érdemes lehet testreszabnia a választható SSL típusokat az igénylő űrlaphoz (**SSL types** → **Customize**, jobb oldali rész), hogy megakadályozza a felhasználót abban, hogy olyan tanúsítványtípusokat is igényeljen, melyeket nem kíván engedélyezni a számára. Az SCM felületén továbbra is megőrizheti a választási lehetőséget (a fenti felület bal oldali részén).

## EV tanúsítványok

Amennyiben nem feltétlenül szükséges, nem javasolt EV tanúsítványok használata. Ha mégis igényelnének, akkor első lépésben meg kell nyitni a **Settings** -> **Organizations** résznél a saját intézményt szerkesztésre, és ott az **'EV Details'** fülön ki kell tölteni a megadott mezőket:

Edit Organization: Kormányzati Informatikai Fejlesztési Ügynökség

General

EV Details

Client Certificate

SSL Certificate

Code Signing Certificate

Email Template

Incorporation or Registration Agency

Incorporating Agency

Kormányzati Informatikai Fejlesztési Ügynökség

Main Telephone Number

+3614503060

DUN and Bradstreet Number

Company Registration Number

598316

Jurisdiction of Incorporation City or Town

State or Province of Incorporation

Country of Incorporation

Hungary

Date of Incorporation

01/10/2006

Business Category

Government Entity

Contract Signer

Title

Mr.

OK

Cancel

Amennyiben nem szerkeszthetők ezek a mezők, kérjük küldje el az adatokat az Ügyfélszolgálat emailcímére, és a KIFÜ adminisztrátorai kitöltik azokat. Ezek után indítható az EV tanúsítvány igénylése.



# Személyes tanúsítványok

## Önkiszolgáló portál SAML használatával

### Az IdP és az SCM konfigurálása a portál engedélyezéséhez

Az önkiszolgáló portál a következő címen található: [https://cert-](https://cert-manager.com/customer/KIFU/idp/clientgeant)

[manager.com/customer/KIFU/idp/clientgeant](https://cert-manager.com/customer/KIFU/idp/clientgeant) Ahhoz, hogy működjön a felhasználók számára, a következőket kell tenni:

- Helyesen be kell konfigurálni az IdP-t a Sectigo-hoz. Lásd a [SAML konfiguráció](#) pontnál.
- Szerkessze a szervezeti objektumot, és állítsa az "Academic code (SCHAC Home Organization)" értéket ugyanarra az értékre, mint amit az IdP küld mint "schacHomeOrganization". Ez általában a fő domain, de ezt egyeztesse le az IdP rendszergazdáival.

Ahhoz, hogy a felhasználók használhassák az IGTF / grid tanúsítványokat, a következőkre is szükség van:

- Szerkessze az **Organization** objektumot, és állítsa be a "Secondary Organization Name" mezőben a grid tanúsítványokban használt nevet. Mivel a grid tanúsítvány objektumokat "felhasználónévként" használják a rendszerekben, elengedhetetlen, hogy a teljes tárgysorozatot úgy tárolják, ahogy korábban is történt a felhasználók számára.
- Küldjön a fentiekről az [ugyfelszolgalat@kifu.hu](mailto:ugyfelszolgalat@kifu.hu) -ra e-mailt, miszerint kéri a másodlagos név érvényesítését, mivel ezt a lépést nem tudja végrehajtani, és akkor elindítjuk ezt a folyamatot.

### Az érintett szerverek konfigurálása grid / IGTF használatához

A "sima" kliens tanúsítványokhoz nem kell semmilyen beállítást elvégeznie. A grid / IGTF tanúsítványoknál győződjön meg arról, hogy a szerverek rendelkeznek-e a legfrissebb IGTF Trust Anchor Distributionnel, amely magában foglalja ezt a sort: **"/CNL/O=GEANT Vereniging/CN=GEANT eScience Personal CA4"** (megtalálható a [ca\\_GEANTeSciencePersonalCA4-1.105-1.noarch.rpm](#) vagy újabb RPM csomagban)

### A portál használata

Az itt található utasítások a tanúsítványokat ismerő RAO-knak szólnak. Lehet, hogy ki kell bővítenie ezt, amikor utasításokat ad a végfelhasználóknak, például megmutatni nekik, hová importálják a tanúsítványokat a támogatott böngészőkben, stb. Így kaphat tanúsítványt:

1. Nyissa meg a <https://cert-manager.com/customer/KIFU/idp/clientgeant> oldalt, válassza ki a szervezet IdP-jét, és jelentkezzen be oda.
2. Válassza ki a megfelelő tanúsítási profilt:
  - "GÉANT Personal Certificate" - normál kliens tanúsítványhoz, e-mail aláírásra stb. a grid/IGTF felhasználási területen kívül.
  - "GÉANT IGTF-MICS Personal" - grid/IGTF személyes (kliens) tanúsítványhoz normál használathoz.
  - "GÉANT IGTF-MICS-Robot Personal" - grid/IGTF robot személyes tanúsítvány (ritkán használt).
3. Válassza ki, hogy a kulcsot a kiszolgáló oldalán vagy helyileg generálja. Noha az előbbi sokkal kényelmesebb, policy vagy technikai okokból kifolyólag kellhet esetenként az utóbbi:
  - Használja a "Generate RSA" elemet, ha szerver-oldalon generált kulccsal szeretne tanúsítványt igényelni.
  - Csak akkor használja a "Generate ECC" elemet, ha ECC tanúsítványokat tesztl. Ha nem biztos benne, használja inkább az RSA-t.
  - Ha nem szerver-oldalon generált kulccsal szeretne igényelni, használja az "Upload CSR" opciót.
4. Ha a CSR feltöltést választja, akkor először létre kell hoznia a kulcsot és a CSR-t helyileg, bármilyen szoftverrel, amelyet amúgy erre használ. OpenSSL esetén:

```
openssl req -new -newkey rsa:2048 -out usercert_request.pem -keyout userkey.pem -subj '/CN=Teszt'  
chmod go = userkey.pem  
cat usercert_request.pem
```

5. Ha úgy dönt, hogy a tanúsítványt a szerver oldalon generálja, meg kell adnia a létrehozandó PKCS#12 fájl titkosításához használt jelszót.
6. Kattintson a **Submit** gombra, és fogadja el a feltételeket.
7. Rövid idő elteltével letöltheti a tanúsítványt. A formátum az alábbi választástól függ:
  - A "Generate RSA/ECC" funkcióval kap egy PKCS#12 fájlt certs.p12 névvel, ami tartalmazza a kulcsot és a tanúsítványt. Ezt importálhatja böngészőjébe a "Tanúsítvány importálása" opcióval.
  - Az "Upload CSR" funkcióval kap egy PEM-formátumú certs.pem fájlt, amely csak a tanúsítványt tartalmazza. Ha szükség van a böngészőbe importálásra, akkor saját magának kell létrehoznia egy PKCS#12 fájlt. Az OpenSSL-lel így lehet:

```
openssl pkcs12 -export -inkey userkey.pem -in certs.pem -out certs.p12
```

8. Ha az alábbi hibaüzenetet kapja miután a Submit gombra kattintott, és elfogadta a feltételeket: "Sectigo Certificate Manager enrollment request failed. Please contact your security administrator." annak az lehet az oka, hogy meghaladta a két érvényes tanúsítvány korlátját személyenként és tanúsítványprofilonként. Az új tanúsítvány kiállítása előtt vissza kell vonnia a két tanúsítvány közül legalább egyet. Ez hibaként lett leadva a Sectigo felé, remélhetőleg mielőbb javítják.

# Kliens tanúsítványok visszavonása

A végfelhasználók nem tudják visszavonni a tanúsítványokat az önkiszolgáló portálon. Jelezni kell számukra, hogy az adminisztrátorokkal kell kapcsolatba lépniük ezen szándék esetén. Rao adminisztrátorok visszavonhatják a tanúsítványokat a **Certificates → Client certificates** menüben, kiválasztva a megfelelő személyt, rá kell kattintani a Certificates gombra, kiválasztani a megfelelő tanúsítványt, és a Revoke gombra kattintani.

## Kliens tanúsítványok kiállítása az SCM használatával

*Megjegyzés: ez egy tartalék megoldás. A személyes tanúsítványok kiadásának fő módja a fentebb tárgyalt önkiszolgáló portálon keresztül történik.*

1. RAO adminisztrátorként menjen a **Certificates → Client certificates** menübe és használja az **Add** gombot. Válassza ki a megfelelő szervezetet, szervezeti egységet és domaint. Töltse ki az e-mail címet és a nevet. Töltse ki a külön névmezőket. Hagyja üresen a *Secret ID* és a *Validation Type Standard* mezőket.
2. Most már hozzáadta a kívánt személyt. Kattintson rá, hogy bepipálja a sor elején a checkboxot, majd kattintson a **Certificates** gombra. Itt a **Send invitation** használatával kiküld egy meghívó emailt a felhasználónak, amely egy egyszeri hozzáférést biztosít a számára ügyféltanúsítvány létrehozására.
3. A felhasználónak meg kell adnia egy jelszót (amelyet a generált PKCS#12 fájl titkosításához használnak) és egy *Passphrase*-t (mely révén a felhasználható az Ön segítségét nélkül is vissza tudja vonni a tanúsítványt), valamint el kell fogadnia a feltételeket.
4. A felhasználó ezután kap egy PKCS#12 fájlt, amely tartalmazza a kulcsot, a tanúsítványt és a láncot, készen a webböngészőbe való importálásra.

*Érdemes megjegyezni:* Ennél a módszernél a kulcs mindig a szerver oldalán jön létre. Nincs lehetőség CSR feltöltésére az ügyféloldalon generált kulcs használatával. Ez valószínűleg a felhasználók számára nem elfogadható vagy policy (nem szabad a kulcsot a szerveroldalon generálni) vagy technikai okok (a kulcs nem exportálható hardver eszköztől) miatt. Az önkiszolgáló portál használatakor van lehetőség a CSR feltöltésére.

## Értesítések

A **Settings → Notifications** menüpont alatt létrehozhatja és szerkesztheti azokat az értesítéseket amiket kiküld a rendszer, ha bizonyos feltételek teljesülnek. Az **Add** gomb használatával választhat egyet a rendelkezésre álló értesítési típusokból:

- Legalább a tanúsítványok lejáratával kapcsolatban érdemes értesítést beállítani, ehhez az **SSL Expiration** opciót kell választani. A **DCV Expiration**-t ugyanezen okból szintén javasolt beállítani.
- Ha lehetővé tette a nem adminisztrátor felhasználók számára, hogy tanúsítványokat igényeljenek (lásd fent), akkor ajánlott az **SSL Awaiting Approval** használata, hogy figyelmeztetést kapjon a RAO arról, hogy jóvá kell hagyni egy igénylést.
- Kérjük, ne engedélyezze a "**Notify MRAO Admin(s)**" elemet, mivel ilyenkor ez e-mailt küld a KIFÜ "superusereinek" is.

Ha módosítania kell a rendszerből küldött e-mailek szövegét, akkor ezt megteheti a **Settings → Templates → Email template** menüpont alatt.

# SAML konfiguráció

## Állítsa be az IdP-t a Sectigo-val való együttműködéshez

A SAML bejelentkezés engedélyezve van a KIFÜ SCM példányához, de az attribútumot manuálisan kell beállítani az Identity Providernél, mivel a metaadatokban lévő SCM entitásnak nincs előre definiált kategóriája. A következő attribútumokat kell közzétenni az Entiyld-ben (<https://cert-manager.com/shibboleth>):

- eduPersonPrincipalName (urn:oid:1.3.6.1.4.1.5923.1.1.1.6)
- mail (urn:oid:0.9.2342.19200300.100.1.3)
- displayName (urn:oid:2.16.840.1.113730.3.1.241)
- giveName (urna:oid:2.5.4.42)
- sn (urn:oid:2.5.4.4)
- schacHomeOrganization (urn:oid:1.3.6.1.4.1.25178.1.2.9)
- eduPersonEntitlement (urn:oid:1.3.6.1.4.1.5923.1.1.1.7) az alábbi értékkel:  
urn:mace:terena.org:tcs:personal-user

## Ellenőrizze, hogy az IdP megfelelően van-e konfigurálva

Miután az IdP rendszergazdái bekonfigurálták a szükséges attribútum kiadását, ellenőrizze azt a <https://cert-manager.com/customer/KIFU/ssocheck> oldalon. Ehhez a teszthez csak az eduPersonPrincipalName és a mail szükséges, a személyes tanúsítványokhoz viszont a giveName,

sn, displayName, schachHomeOrganization és eduPersonEntitlement (amelyek jelenleg nem jelennek meg a tesztben) is szükségesek. A további vizsgálatokra és tesztelésre bejelentkezés után az alábbi oldalon van lehetőség: <https://cert-manager.com/Shibboleth.sso/Session> Itt megtudhatja, mely attribútumokat kapja meg a Sectigo az Ön IdP-jétől.

## Konfigurálja az SCM-et

Miután ellenőrizte, hogy az IdP helyesen van-e beállítva, folytathatja a SAML-hitelesítés használatának konfigurálását:

- Ahhoz, hogy használni lehessen a föderációs bejelentkezést az SCM portálon, be kell lépni az összes meglévő RAO és DRAO admin felhasználói fiókját tartalmazó oldalra (**Admins**) és módosítani az **Identity provider** mezőt a saját intézményre, valamint az **IdP person ID** mezőt az *admin ePPN (eduPersonPrincipalName)* értékére.
- Az SSL-tanúsítványokról a "Self Enrollment via SAML" leírásnál olvashat fentebb a Nem adminisztrátor jogosultságú igénylések engedélyezése részben.

## A REST API használata

A Sectigo REST API dokumentáció megtalálható a

[https://support.sectigo.com/Com\\_KnowledgeProductPage?c=Sectigo\\_Certificate\\_Manager\\_SCM](https://support.sectigo.com/Com_KnowledgeProductPage?c=Sectigo_Certificate_Manager_SCM) az "SCM - Sectigo Certificate Manager REST API" dokumentumban. Javasoljuk, hogy hozzon létre külön RAO vagy DRAO adminisztrátorokat az API-val történő műveletekhez, ne azokat a adminisztrátorokat használja, akiket a webes felhasználói felületen végzett tevékenységekhez. Csak API-hoz használni kívánt adminisztrátor létrehozása:

1. Használja a RAO adminisztrátort az új admin létrehozásához, ugyanúgy, mint egy "normál webfelület adminisztrátort", beleértve az ideiglenes jelszó beállítását. Nem fogja tudni használni az API-t ezzel az ideiglenes jelszóval.
2. Jelentkezzen be az új adminisztrátor felhasználóval az SCM felületén, és hajtsa végre a kötelező kezdeti jelszó megváltoztatását.
3. Visszatérve az eredeti RAO-hoz, szerkessze az új admint, és állítsa be rá a „WS API use only” opciót.
4. Ahhoz, hogy az API-hívásokat tanúsítványok kezelésére használhassuk, szerkeszteni kell a megfelelő *Organization* vagy *Department* objektumot, és az **SSL Certificate** lapon engedélyeznie kell a Web API jelölőnégyzetet. Meg kell adnia egy értéket a *Secret key* mezőhöz is.

## ACME Windows

A certbot egyelőre béta verziójú, ennek figyelembevételével használja mindenki!

1. Első lépésben létre kell hozni egy ACME (Automated Certificate Management Environment) felhasználót az SCM-ben. Ezt a **Settings → Organizations** részben tehető meg, a saját szervezet kiválasztása után fent megjelenik az **ACME Accounts** menüpont. A felugró menüben az **Add** gomb megnyomásával hozható létre új account. A szükséges adatok kitöltése után létrejön az account, és az utolsó kis képernyőn megjeleníti a felhasználáshoz szükséges adatokat. (4. lépés) Ezeket megfelelő helyre el kell menteni.

ACME Account successfully created: JoDi

ACME URL

https://acme.sectigo.com/v2/OV

EXTERNAL ACCOUNT BINDING

Account ID

3YR-KXZ9hI09FRd3coisFw

Key ID

3YR-KXZ9hI09FRd3coisFw

HMAC Key

DVJx8GBjZCdU3rRQ2ueVMXJgmxwfn7ePm2HEYoXNkNjhS1ajpQoiHUC  
JpVfPWTcyD2iDpmzu9Rnd3CuTgeXQw

Close

2. Le kell tölteni a Windowsra a certbot klienst: <https://dl.eff.org/certbot-beta-installer-win32.exe>
3. Fel kell installálni a klienst Windows 2016 vagy Windows 2019 szerverre. Az installálás során létrejön egy ütemezett feladat, ami naponta kétszer ellenőrzi, hogy szükséges-e a tanúsítvány megújítása, és ha igen, el is végzi.
4. Negyedik lépésben be kell állítani a certbot klienst. El kell indítani a parancssort adminisztrátori jogosultsággal. A következő parancsot kell kiadni: `certbot register --server https://acme.sectigo.com/v2/OV --eab-kid <your own KeY ID> --eab-hmac-key <your own HMAC Key> --email <an email address>`
5. A *Key ID* és a *HMAC key* a certbot account létrehozásakor elmentett adatokból származnak. A certbot most már be van konfigurálva.
6. Az ACME-n keresztüli tanúsítványigénylés: `certbot certonly --domain <domainname> --server https://acme.sectigo.com/v2/OV`
7. A cert a következő elérési úton lesz megtalálható: `C:\Certbot\live<domainname>`
8. Fel kell installálni a tanúsítványt a szerverre (sajnos itt még nem sikerült kitalálni, hogy lehet ezt is automatizálni). Egy órába is beletelhet, mire megjelenik a tanúsítvány az SCM felületén. A státusza *External* lesz, az igénylőnél pedig ez jelenik meg: *CN=Sectigo RSA Organization Validation Secure Server CA*

# Segítség

## KIFÜ ügyfélszolgálat

Amennyiben ez a dokumentum nem tartalmazza a kérdésre a választ vagy megoldást a problémájára, kérjük írjon az alábbi email címre: [Ügyfélszolgálat](#)

## Sectigo támogatás

Ha a probléma jellege megkívánja, vegye fel a kapcsolatot a Sectigo Ügyfélszolgálatával a <https://sectigo.com/support-ticket> webhelyen a kérdésével/problémájával kapcsolatban. Eltérő utasítás hiányában válassza az "SCM Support" pontot a jegy okának. A leírásban szerepeljen az alábbi sor: "We are a KIFÜ member of the GEANT TCS service, using the <https://cert-manager.com/customer/KIFU> SCM SCM instance."

Javasolt átnézni a Sectigo support oldalát is, illetve jól használható az ottani kereső is, a gyakori hibákra általában írnak egy külön cikket, mint pl. az [Anchor Certificate details are different](#)

## Sectigo dokumentáció

A Sectigo teljes dokumentációja megtalálható az [Admin Guides&k&lang=](#) alábbi webhelyen.

Néhány javaslat:

- "SCM - Sectigo® Certificate Manager Quick Start Guide" - az SCM rendszer rövid bemutatása
- "SCM - Sectigo Certificate Manager Administrator's Guide" - lényegesen hosszabb, és alaposabb leírás a szolgáltatásról
- "SCM - Sectigo Certificate Manager REST API" - a REST API leírása, automatizálási lehetőségek

## GÉANT Trusted Certificate Service (TCS)

Az alábbi oldalon található a GÉANT leírása a tanúsítványszolgáltatásról (angol):

[https://www.geant.org/Services/Trust\\_identity\\_and\\_security/Pages/TCS.aspx](https://www.geant.org/Services/Trust_identity_and_security/Pages/TCS.aspx) TCS repository:

<https://wiki.geant.org/display/TCSNT/TCS+Repository>