Tanúsítványszolgáltatás

A Pro-M tanúsítványszolgáltatás leírása

- Pro-M tanúsítványszolgáltatás
- TCSCertTypes (Archív)
- TCS ServerCert (archív)

Pro-M tanúsítványszolgáltatás

Értesítések:

- *Elindult a szolgáltatás, ezen az emailcímen lehet érdeklődni a részletekről!*

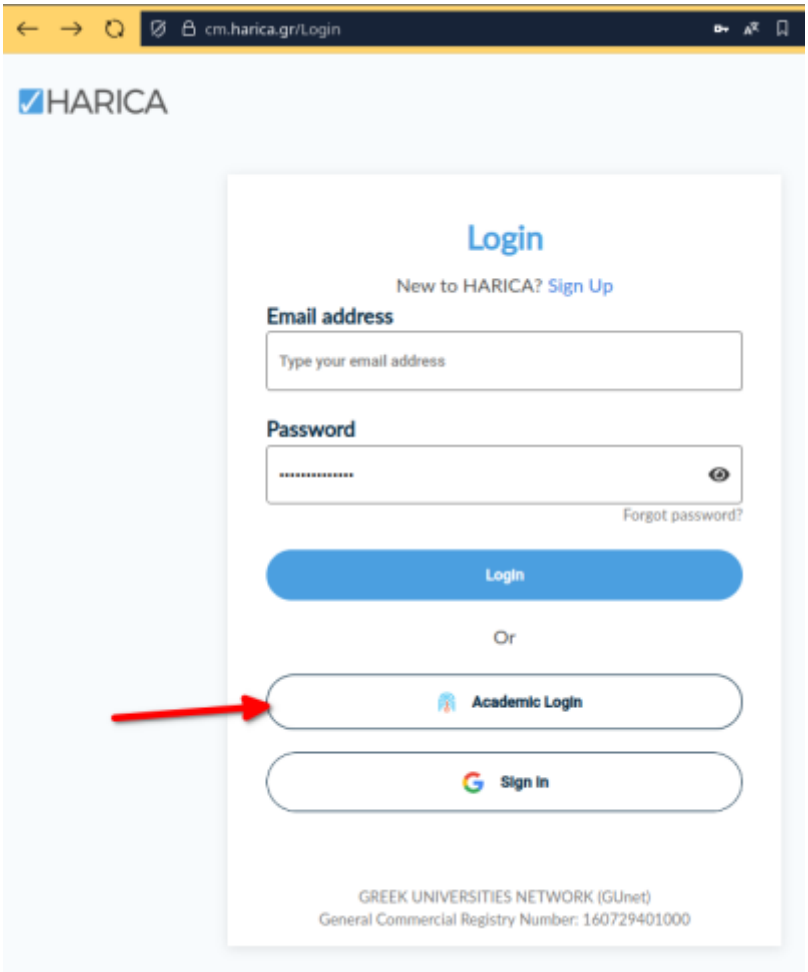
A *Megbízható Tanúsítványszolgáltatás* (Trusted Certificate Service, **TCS**) olyan tanúsítványok kiállítását biztosítja, amelyet az elterjedt böngészők és kliensprogramok megbízhatónak tartanak, valamint bizonyos típusaik Grid hálózatokban is elfogadhatóak.

HARICA tanúsítványszolgáltatás

A görög egyetemek szövetségének fejlesztésére épül az új TCS tanúsítványszolgáltató. Gyorsan haladnak a fejlesztéssel, de jelenleg még pár funkció – több szintű jogosultságkezelés, intézmények kezelése, ACME, stb. – fejlesztés alatt áll, és nem érhető el teljes funkcionalitásában. A HARICA rendszere az alábbi **linken** érhető el.

Regisztráció/belépés

1. Működik az eduID-s belépés, nincs szükség külön regisztrációra; az **Academic login** gombra kattintva érhető el. Előfeltételek leírása itt



2. Lehetséges egyéb e-mail címmel is regisztrálni a HARICA felületére, azonban ajánljuk a hivatali email cím használatát, mivel ez alapján az adott intézményhez is rendelődik a felhasználó, amennyiben az intézmény már benne van a rendszerben, és felvette magához a domaint, valamint a tanúsítványkérelem engedélyezésénél is ez alapján döntik el a kérelem jogosságát.
3. Belépés után, ha a tanúsítványigénylésen felül egyéb jogokat szeretnénk, akkor kötelező beállítani a kéttényezős hitelesítést. Ezt a jobb felső sarokban a saját nevünkre kattintva, a **Profile** menüpontnál lehet elérni. Jelenleg nem veszik figyelembe, hogy az eduID folyamatában is kéttényezős hitelesítés szerepel; ezt a problémát a GÉANT és az NREN-ek is jelezték a HARICA-nak. Valószínűleg engedélyezni fogják, hogy az intézmény kétlépcsős azonosítása esetén ne kelljen TOTP-t használni HARICA-nál.
4. Az e-mail cím domainje alapján automatikusan a PRO-M-hez vagy az intézményhez rendeli a felhasználót.
5. Csak ezután tudunk bárkinek bármiféle jogosultságot beállítani. Ilyen igényeket erre az emailcímre lehet küldeni.

SAML konfiguráció

Azoknak a TCS tagoknak, akik egyben identitásszolgáltatók is az eduGAIN-ben, a következő attribútumokat kell közzétenniük:

- givenName (oid:2.5.4.42)
- surname (oid:2.5.4.4)

- mail (oid:0.9.2342.19200300.100.1.3)
- edupersonTargetedID (oid:1.3.6.1.4.1.5923.1.1.1.10)

Közzétehető további attribútumok:

- eduPersonPrimaryAffiliation (oid:1.3.6.1.4.1.5923.1.1.1.5)
- eduPersonPrincipalName (kötelező az IGTF személyes tanúsítványokhoz) (oid:1.3.6.1.4.1.5923.1.1.1.6)
- eduPersonEntitlement (szükséges az IGTF személyes tanúsítványokhoz) (oid:1.3.6.1.4.1.5923.1.1.1.7)

Ügyeljen arra, hogy csak a TCS-hez társított értékeket küldje el a HARICA SP-knek. Használja az „urn:mace:terena.org:tcs:personal-user” azonosítót az IGTF személyes tanúsítványok kiadásának engedélyezéséhez.

- schacHomeOrganization (oid:1.3.6.1.4.1.25178.1.2.9)

A következő HARICA EntityID-knek kell attribútumot kiadni:

- **PRODUCTION:**
  - https://www.harica.gr/simplesamlphp/module.php/saml/sp/metadata.php/pki-grnet-sp
  - Attribútum kiadás teszt: https://cm.harica.gr/loginsaml/test.php

Alternatív letöltési / megtekintési link az XML fájlhoz: https://met.refeds.org/met/entity/https%253A%252F%252Fwww.harica.gr%252Fsimplesamlphp%252Fmodule.php%252Fsaml%252Fsp%252Fmetadata.php%252Fpki-grnet-sp/?federation=grnet-federation

Az attribútum kiadás teszt elérhető a felületen a „View login information” gombbal is a felhasználói profil alatt.

Ismert problémák: A mail attribútumban több érték megadása jelenleg nem támogatott.

Jogosultsági szintek

- **Admin:** Csak a saját intézményén belül tevékenykedik; más intézményekre nem lát rá. Az adott intézmény validálását (OV), akárcsak a domainjeiét (DV) intézheti. Jogosultságokat adhat az intézmény felhasználóinak (Admin és alatta lévő jogok). Tanúsítványt igényelhet. Az Admin mellé Approver jogosultság is beállítható.
- **Approver:** El tudja fogadni a beküldött tanúsítványokat (kivéve a saját maga által beküldötteket). Tanúsítványt igényelhet.
- **User:** Tanúsítványt igényelhet. Felhasználóként bárki beregisztrálhat a HARICA felületére – eduID mellett felhasználó/jelszó regisztráció is működik. Ha a regisztrációhoz használt e-

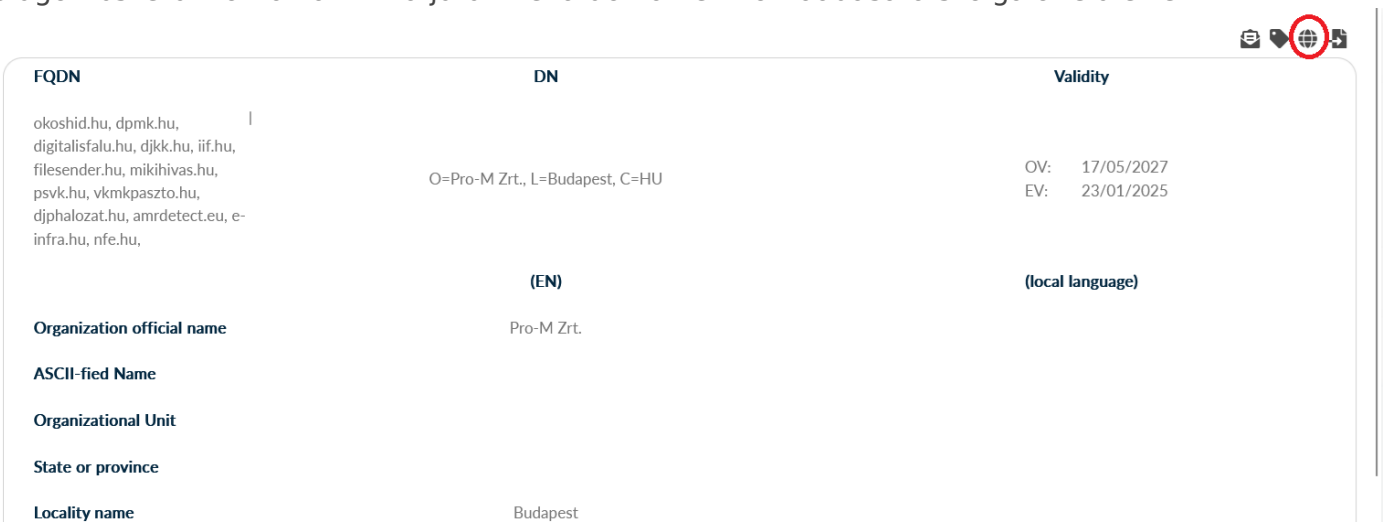
mail cím domainje valamely intézmény felrögzített domainjei közé tartozik, akkor a felhasználót automatikusan hozzárendeli, és az intézmény Adminjai tudják kezelni. Jogosultságot csak Admin vagy Manager adhat, ha a User beállította a 2FA-t.

Jogosultságok beállítása

Egy adott intézmény (Enterprise) admin jogosultságú felhasználója képes az intézmény usereinek jogokat beállítani (amennyiben az adott felhasználó beállította a kétfaktoros hitelesítést). Ehhez a fejlécen található **Enterprise → Admin** menüpontra kell elnavigálni, ott a **Users** fülön a felhasználók listájából kiválasztani a megfelelőt. A felugró ablakban az **Account info** fülön lehet beállítani a megfelelő jogokat. Figyelni kell arra is, hogy a **Validator groups** résznél a *Manage groups* gomb segítségével a megfelelő intézményt is adjuk hozzá.

Domain menedzsment

Admin felhasználóként a felső menüsoron az **Enterprise → Admin** gombra kattintva az intézményválasztó oldalra kerülünk, ahol a saját intézményünk nevére kattintva annak alapadatait tartalmazó ablakra irányít. Itt újfent az intézménynévre kattintva felugrik egy nagyobb ablak az intézmény részletesebb információival, valamint a jobb felső saroknál egy ikonsorral. Itt a földgömbszerű ikonra kattintva jutunk el a domainek hozzáadására szolgáló felületre.



Egy .csv mintafájlt letöltve, abban az adatokat értelemszerűen kitöltve is visszaimportálva tudunk új domaineket hozzáadni az intézményünkhöz. Nem fognak azonnal megjelenni a domainlistában, kell egy átfutási idő, ami akár pár órát is jelenthet.

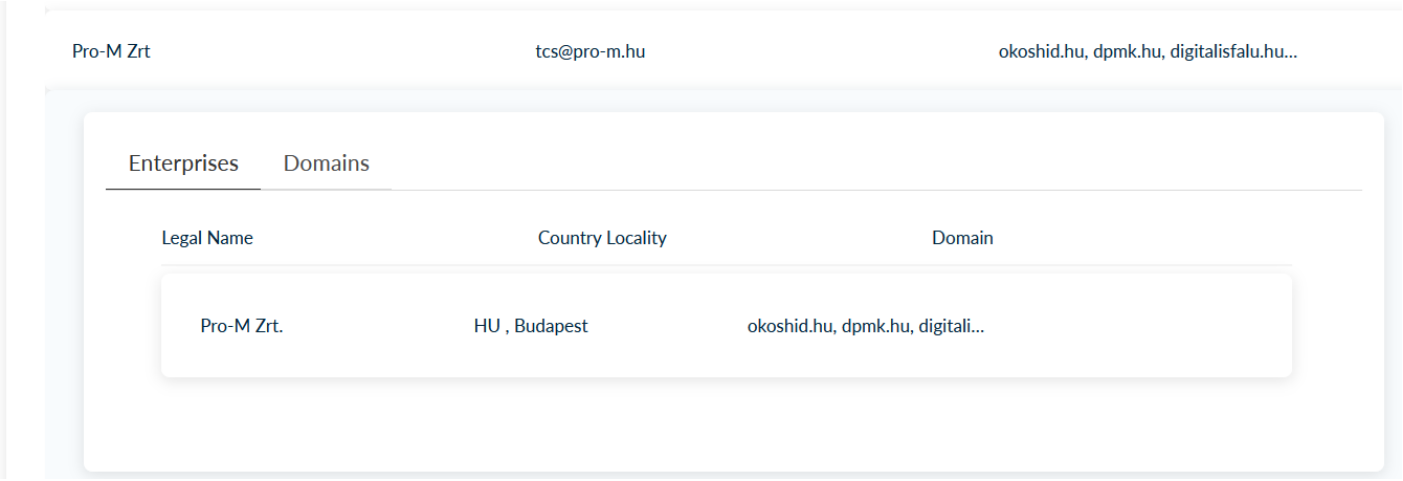
Visszatérve az intézményválasztó felületre a **Domains** fülön az intézményhez felvitt domainek listája található, itt lehet levalidáltatni a domaineket, illetve meghosszabbítani a lejárt domainek validációját. A **Validate Domain** gombra kattintva:

- DNS-record módszer: itt a felugró ablaknál megadott emailcímre küldik majd a kódot, amit be kell illeszteni a DNS recordba.
- E-mail: a választott domain alap technikai e-mail címeire küldött ellenőrző levél alapján validálunk. Új domain hozzáadásához vissza kell navigálni az **Enterprises** fülre, majd ott

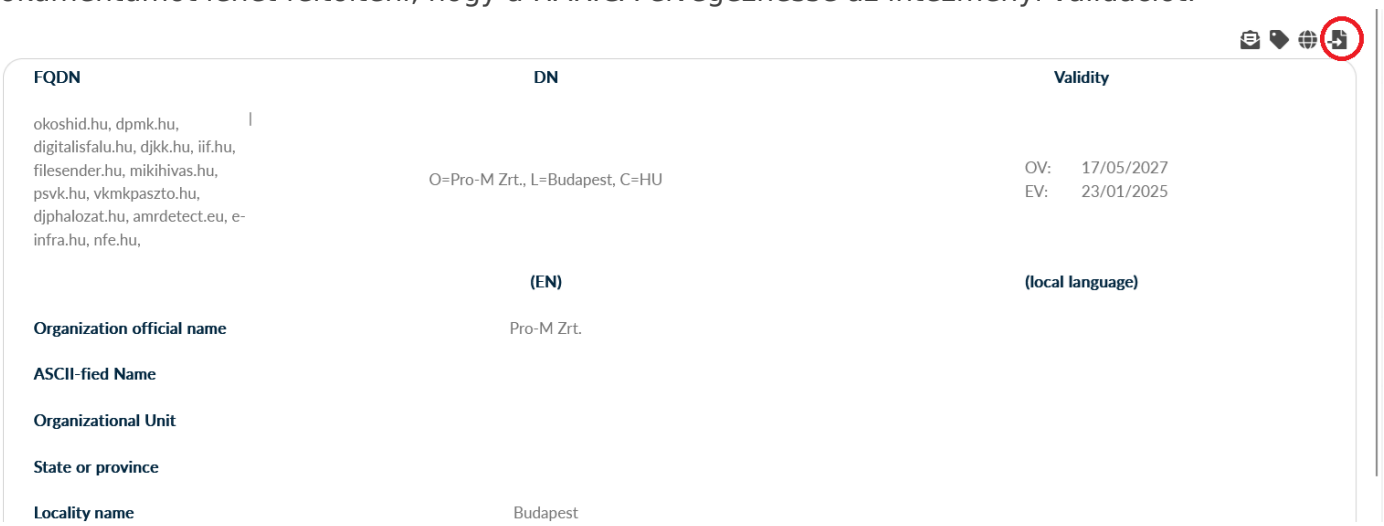
az intézményt kiválasztva, a megjelenő ablak jobb felső sarkában található földgömb ikonra kattintani. A letöltött CSV fájlt értelemszerűen kitöltve kell megadni az új domaineket. A felkínált minta fájlt kell használni, mert más formátum esetén hibát kapunk. Az admin saját emailcímére kap egy visszajelzést, hogy beküldött x db domaint a szervezetéhez. (HARICA Notification, *Your request for x new Domain(s) in yourenterprise has been submitted.*) A domainek elfogadásáról azonban nincs visszajelzés, kb 1 napon belül megjelennek a listában.

Szervezet validációja

Admin felhasználóként a felső menüsoron az **Enterprise → Admin** gombra kattintva az intézmény adatait tartalmazó ablakra kerülünk. Itt az intézmény nevére kattintva megnyílik az adatablaka, ahol szintén az intézménynévre kell kattintani.



Ezek után megjelenik az az ablak, ahol az intézménnyel kapcsolatos beállításokat lehet megtenni. A jobb felső ikonsornál az utolsó ikon vezet oda, ahol az intézmény alapadatait tanúsító hiteles dokumentumot lehet feltölteni, hogy a HARICA elvégezhesse az intézményi validációt.



Javasoljuk az Alapító okirat használatát, de más hiteles dokumentum is megflelhet erre a célra. Beküldést követően jellemzően pár órától 1-2 napig terjedő időintervallumban szokott megtörténni a hitelesítés. Amennyiben nem érkezik visszaigazolás 48 órán belül, érdemes a support címére írni.

Tanúsítvány típusok

> Az alábbi tanúsítványtípusok érhetőek el a PRO-m keretszerződés keretében:

Server Certificates (szerver tanúsítványok)

Mire jó?
Ez gondoskodik arról, hogy egy weboldal „biztonságos” legyen – vagyis titkosított kapcsolaton keresztül kommunikáljon (*https://*). A böngésző kis lakat ikonja is ezt jelzi.
Kinek van rá szüksége?
Weboldalak üzemeltetőinek, akik adatokat kezelnek (belépés, regisztráció, űrlapok, webshop). Cégek, iskolák, kutatóintézetek szerverei számára kötelező lehet.

- *Domain Validated (DV)*
  - Egyszerű domain-vizsgálaton alapuló SSL/TLS
  - Gyors kiállítás, olcsóbb
- *Multi-domain (SAN)*
  - Több FQDN (Subject Alternative Name) egy tanúsítványban
  - Költséghatékony több szolgáltatás védelmére
- *Wildcard*
  - Egy domain és összes aldomain (pl. *.példa.hu) védelme
  - Praktikus dinamikusan létrejövő aldomain-ek esetén
- *Organization Validated (OV)*
  - Szervezeti validáció, tartalmazza a cég hivatalos adatait
  - Erősebb bizalom a látogatók felé
- *IGTF*
  - Tudományos és kutatási infrastruktúrák számára interoperábilis tanúsítvány
  - Követi az Interoperable Global Trust Federation szabványait

IGTF kliens tanúsítvány

Mire jó? Speciálisan tudományos számítástechnikai hálózatokban (GRID-ek) használják, ahol nagy számítási kapacitást igénylő kutatások zajlanak.
Kinek van rá szüksége? Tudósoknak, kutatóknak, akik nemzetközi számítási hálózatokhoz csatlakoznak (pl. CERN, bioinformatikai hálózatok, stb.).

Az itt leírtak teljesülése esetén válik elérhetővé.

Email (S/MIME tanúsítványok)

Mire jó?
Segít annak igazolásában, hogy az e-mailek valóban a megjelölt feladótól illetve szervezettől származnak (digitális aláírás), valamint hogy titkosítható legyen a tartalmuk, hogy illetéktelen ne

olvashassa el.
Kinek van rá szüksége?
Olyan magánszemélyeknek vagy szervezeti dolgozóknak, akik bizalmas adatokat küldenek emailben – pl. jogászok, orvosok, informatikusok, közigazgatási dolgozók.

- *Email-only*
  S/MIME tanúsítvány csak e-mail aláírásra és titkosításra
  - Tartalmazza az e-mail cím(eke)t
- *IV+OV – Hybrid*
  - Egyéni és szervezeti adatok egy tanúsítványban
  - Hasznos nagyvállalati környezetben

> Az alábbi típusok az oldalon helyben megjelölt díjazásért cserében igényelhetők, bankkártyával fizetve az igénylési folyamat végén:

eSignatures (elektronikus aláírások)

Mire jó?
Ezzel a tanúsítvánnyal hiteles elektronikus aláírást lehet létrehozni – például hivatalos dokumentumok, szerződések aláírására, ugyanúgy, mintha kézzel lenne aláírva, papíron.
Kinek van rá szüksége?
Magánszemélyeknek, cégek munkatársainak vagy hivatalos ügyintézőknek, akik dokumentumokat írnak alá elektronikusan.

- *Remote Qualified eSignature*
  Jogilag hitelesített, eszközfüggetlen minősített aláírás. Használható:
  - Szerződések (értékesítés, munka, bérlet, biztosítás stb.)
  - Tranzakciók (e-kereskedelem, online bankolás stb.)
  - Közigazgatási ügyintézés (adóbevallás, anyakönyvi kivonat kérése stb.)
- *Qualified eSignature in cryptographic device (token)*
  Minősített aláírás USB-tokenen vagy smartcardon
  - Ugyanazok a felhasználási területek, mint a Remote Qualified eSignature-nél
- *Advanced eSignature (legacy Class B)*
  Haladó elektronikus aláírási tanúsítvány korábbi (Class B) szabvány szerint
  - Dokumentumok digitális aláírására, jogi elismeréssel

eSeals (elektronikus pecsétek)

Mire jó?
Ez nem egy személyhez, hanem egy **szervezethez** kapcsolódik. Olyan, mint egy pecsét, amit automatikusan rá lehet tenni digitális dokumentumokra – például számlákra, igazolásokra.
Kinek van rá szüksége?
Cégeknek, intézményeknek, akik automatizált módon „hitelesítenék” dokumentumaikat (pl. e-számlák, gép által generált igazolások).

- *Remote Qualified eSeal*
  Hagyományos pecséttel jogilag egyenértékű, eszközfüggetlen
  - CertManager vagy API felületen keresztül, bármilyen eszközről használható
  - Tartalmazza a szervezet hivatalos adatait
  - Havi 500 ingyenes aláírás; többlet aláírás díjköteles (support@harica.gr)
- *Advanced eSeal*
  Haladó pecsét tanúsítvány jogilag kötelező dokumentumokhoz
  - Tartalmazza a szervezeti adatokat és aláírási logokat

Code Signing (kódaláírás)

Mire jó?
Ezzel tanúsítható, hogy egy program vagy alkalmazás **valóban attól származik, aki kiadta**, és nem módosították utólag.
Kinek van rá szüksége?
Szoftverfejlesztőknek és cégeknek, akik alkalmazásokat, programokat készítenek és szeretnék, hogy azt biztonságosnak ismerje fel a rendszer (Windows, macOS, stb.).

- *IV – Individuals/Sole Proprietorships*
  Alkalmazások, driverek, futtatható állományok digitális aláírása
  - Tartalmazza a természetes személy Publisher adatait
- *OV – Organizations*
  Szoftver- és kódaláírás szervezetek részére
  - Tartalmazza a jogi személy adatait
- *EV – Extended Validation*
  - Azonnali reputáció Microsoft Windows rendszeren
  - Részvétel a Windows Hardware Compatibility programban
  - Hivatalos cégnyilvántartási adatok feltüntetésével

Email (S/MIME tanúsítványok)

- *IV – Individuals/Sole Proprietorships*
  Magánszemélyi tanúsítvány e-mail aláírásra/titkosításra
  - E-mail cím és természetes személy adatok
- *OV – Organizations*
  Szervezeti e-mail tanúsítvány
  - E-mail cím és céginformációk

Client Authentication (ügyfél hitelesítés)

Mire jó?
Ez egyfajta **digitális igazolvány**, amivel egy rendszer azonosítani tudja a felhasználót. Például belépéshez használható egy webes portálra.
Kinek van rá szüksége?
Egyetemek, intézmények dolgozói vagy diákjai, ha olyan belépési rendszert használnak, ami tanúsítványalapú azonosítást vár el.

- *IV (User)*
  Felhasználói hitelesítés tanúsítvány. Tartalmazhatja:
  - Természetes személy adatait
  - Kapcsolódó szervezet adatait
  - E-mail cím(eke)t
  - Egy vagy több domaint
- *OV (Machine)*
  Gép- vagy szolgáltatáshitelesítő tanúsítvány
  - Tartalmazza a szervezet adatait, e-mailt és doméneket

További információ A részletes leírások és megrendelési lehetőségek elérhetők a HARICA hivatalos weboldalán: .

Tanúsítvány igénylés

Minden tanúsítvány igénylés a rendszer bal oldali menüjében található menüpontokkal történik. A tanúsítványkérelmek létrehozásához rendelkeznie kell egy felhasználóval a rendszerben (lásd fent), de a felhasználónak nem kell szerepkörrel rendelkeznie. Felhasználó saját kérését nem hagyhatja jóvá, még akkor sem ha adminisztrátor. Ezt egy másik Szervezeti jóváhagyó (Approver) szerepkörrel rendelkező felhasználónak kell megtennie. Ezzel szemben, ha administrátor fogja jóváhagyni a tanúsítványt, akkor egy másik felhasználónak kell igényelnie.

Figyelem Approver-eknek: Tanúsítványigénylést bárki be tud küldeni, akár másik intézménytől is, ezért érdemes alaposan ellenőrizni az igénylést, beleértve az igénylő személyét is, hogy valóban jogosult a cert kiadására!

Szerver tanúsítványok

Használja a Certificate **Requests → Server** útvonalat.

Az első oldalon adjon meg egy opcionális becenevet a tanúsítványnak, majd adjon hozzá egy vagy több domain nevet, amely szerepelni fog a tanúsítványban. Az első hozzáadott név a tanúsítvány CN-je lesz, és az összes hozzáadott név SAN DNS-bejegyzésként jelenik meg a tanúsítványban. Ha nem törli a jelölést a név alatti jelölőnégyzetből, akkor a rendszer hozzáad egy további nevet a www előtaggal SAN DNS-ként.

A becenév csak a kérelmező számára jelenik meg a tanúsítvány listákon. A jóváhagyók/adminisztrátorok nem fogják látni. Javasoljuk, hogy hagyja üresen, mivel ebben az esetben a CN (az első beírt domainnév) jelenik meg.

CAA rekord megléte a domain zónájában nem kötelező, csak ha már létezik más CA-hoz tartozó CAA. Ez esetben megjeleníti milyen CAA-kat szeretne látni:

```
CAA 0 issue "harica.gr"
CAA 0 issuewild "harica.gr"
```

A később feltöltött CSR-ből nem veszik fel a tanúsítványhoz tartozó neveket. Ebben a szakaszban hozzá kell adnia őket. Ez a jövőben változhat.

Jelenleg legfeljebb 100 domain név adható meg (és feltételezzük, hogy ez összesen 200-t jelent, ha elfogadja az összes www-előtt nevet is).

Wildcard tanúsítvány a szokásos eljárással igényelhető. Például a domainnév mezőben a * *.example.com* formában adjuk meg. Ilyenkor az *example.com*-t nem kell a kérésbe belefoglalni.

A következő oldalon válassza ki a tanúsítvány típusát:

1. DV – mindig elérhető, amint a domain validálása megtörtént, és csak a domain információkat tartalmazza. Ez a típusú tanúsítvány hasonlít leginkább arra tanusítványra, amelyet a Let's Encrypt-től lehet kapni.
2. OV – a Szervezet érvényesítése után érhető el. Ez ugyanaz a típusú tanúsítvány, amelyet korábban a Sectigo-tól lehetett kapni.
3. EV – Ne válassza a **„Vállalkozásoknak vagy szervezeteknek (EV)”** lehetőséget, mert ez a fajta tanusítvány NEM része a HARICA TCS ajánlatának, mivel már nem látjuk értékét ennek a tanúsítványtípusnak az alapértelmezett opcióként való támogatásában. Ezeket (EV TLS) és más típusú tanúsítványokat (kódaláírás, minősített elektronikus aláírások/bélyegzők, QWAC-ok) és távoli aláírási szolgáltatásokat egyedileg is meg lehet vásárolni a HARICA-tól, ha speciális felhasználási eseteknél szükség van rá.

Ha a DV vagy OV opció a *“free”* helyett *“from AMOUNT€ year”* felirattal jelenik meg, ne folytassa. A valószínű okok a következők:

- Elírást vétett, és olyan domain nevet adott meg, amely nem tartozik az Ön Szervezetéhez. Kezdje elölről, és ellenőrizze, hogy a nevek helyesek-e.
- Olyan domaint próbált használni, amelyet még nem adott hozzá és nem validált a rendszerben. (Lásd fent: További domainek hozzáadása) Erősítse meg a típusválasztást, majd erősítse meg az információkat, és fogadja el a használati feltételeket stb.

A Submit Request lépésben használja a CSR beküldése manuálisan lehetőséget, hogy beillessze a CSR-t. Fogadja el újra a használati feltételeket stb., és küldje el a kérelmet.

CSR generálás a következő paranccsal lehetséges: (4096 bites RSA kulcs létrehozásához)

```
openssl req -new -newkey rsa:4096 -nodes \ -out peldadomain.hu.csr \ -keyout
peldadomain.hu.key \ -subj "/C=HU/L=Budapest/O=Pro-M Zrt/CN=peldadomain.hu"
```

Azonban a -subj utáni résznek nincs jelentősége, mert:

- DV esetén nem lesz értelme, mert csak a CN-t tartalmazza,

- OV esetében pedig a Szervezet - annak létrehozásakor megadott - **C=HU,L=Budapest,O=Pro-M Zrt.** értékeit fogja felvenni.

Ha az “Auto-generate CSR” módot választjuk, akkor a privát kulcs közvetlenül jön létre, és a rendszer automatikusan generálja a CSR-t. Ekkor a privát kulcsot védő, legalább 8 karakteres jelszó megadása szükséges, és a privát kulcs letöltésének megtörténtét is meg kell erősíteni. Annak pótlására nincs lehetőség a későbbiekben.

> 2025-01-16-án felfedezett BUG: A következő hibaüzenet jelenhet meg: **”You have already used this key before. If your private key gets compromised, we will have to revoke ALL CERTIFICATES associated with this key.“** ha van egy üres sor a CSR előtt a mezőben (és esetleg más szintaktikai hibák esetén is). Ne folytassa, hanem ellenőrizze, hogy a CSR formátuma megfelelő-e, és küldje be újra. Természetesen akkor is ezt az üzenetet fogja kapni, ha újra megpróbál egy kulcsot használni.

Tanúsítványkérelme mostantól a függőben lévő (Pending) tanúsítványok között lesz felsorolva, amíg az egyik Szervezetéhez tartozó jóváhagyó jóvá nem hagyja azt. A függőben lévő jóváhagyásról e-mailt küld a rendszer az intézményi értesítési aliasra.

Ha egy Szervezetéhez tartozó jóváhagyó jóváhagyta a tanúsítványt, a listában a tanúsítványtól jobbra található letöltési nyíl segítségével töltheti le.

IGTF (aka Grid, eScience) Server Certificates - IGTF szerver tanúsítványok

Előfeltételek

1. IGTF OV szerver tanúsítvány igényléséhez a szervezethez be kell kapcsolni az IGTF tanúsítványigénylés engedélyezését. Ezt a szervezet információi oldalon a jobb felső sarokban lévő *Tags* gombon megjelenő ablakban lehet megtenni. (Admin szintű jogosultság szükséges)
2. Megtörtént az Organization Validation eljárás.

Igénylés Szervertanúsítvány igénylésekor a második oldalon (a nevek megadása után) válassza az OV típust. Erősítse meg a következő oldalon. Ezután a „Szervezeti adatok” oldalon jelölje be az „IGTF eScience digitális tanúsítvány igénylése” jelölőnégyzetet. Ahogy ott is szerepel, az „L” és „O” névkomponensek szükség szerint ASCII karakterekké alakulnak.

IGTF (aka Grid, eScience) Client Auth Certificates – IGTF kliens auth tanúsítványok

Előfeltételek

- Be kell kapcsolni az IGTF tanúsítványigénylés engedélyezését. Ezt a szervezet információi oldalon a jobb felső sarokban lévő Tags gombon megjelenő ablakban lehet megtenni. (admin role szükséges)
- Konfigurálja az IdP-t, hogy a szükséges attribútumokat kiadja a HARICA-nak. Lásd az alábbi „SAML konfiguráció” részt. :?:

Igénylés

1. Jelentkezzen be a https://cm.harica.gr/ címen az Academic Login és az IdP-nél használt felhasználónevével. Ehhez a működéshez Academic Login szükséges.
2. A bal szélen található menüben válassza az IGTF klienshitelesítés lehetőséget. Ne válassza a Klienshitelesítés lehetőséget (ami a szerződésünkben nem szereplő, nem IGTF hitelesítési tanúsítványokhoz tartozik).
3. Válassza a GÉANT személyes hitelesítést tanúsítványtípusként, és erősítse meg ezt újra a következő oldalon.
4. Fogadja el a feltételeket, és folytassa a Kérés elküldése gombbal.
5. Használja a Tanúsítvány regisztrálása gombot a Kész tanúsítványok listában.
6. Használja a Tanúsítvány generálása lehetőséget a következő oldalon, és győződjön meg arról, hogy olyan jelszót választ, amelyre később emlékezni fog. Jelölje be a „Megértettem…” jelölőnégyzetet, és folytassa a Tanúsítvány regisztrálása gombbal.
7. Használja a Letöltés gombot a Tanúsítvány beszerzése oldalon a kulcsot és a tanúsítványt tartalmazó PKCS#12 fájl mentéséhez.
8. Importálja a PKCS#12 fájlt oda, ahol szüksége van rá.

- A kiemelt felhasználók dönthetnek úgy is, hogy manuálisan küldik el a CSR-t (miután korábban generáltak egy kulcsot, és szükség szerint kombinálják a kulcsot és a letöltött tanúsítványt).

ACME / Certbot használata

Ez a funkció jelenleg még általunk is tesztelés alatt áll, utána feltöltjük magyar nyelvű leírással ezt a részt is. Addig is angol nyelven az alábbi leírások érhetőek el:

- HARICA ACME funkció használata (EduID belépés)
- HARICA saját leírása az ACME beállításáról

Tanúsítvány igénylés elfogadása

Mivel a saját igényét senki nem fogadhatja el, ezért szükség van az intézmény részéről egy másik felhasználóra, aki rendelkezik ***Approver*** jogosultsággal. Az igénylés az **Enterprise -> SSL request / S/MIME Certificate request** menüpontban található, itt kell rákattintani a megfelelőre. DV tanúsítvány esetén fontos, hogy a tanúsítványban megadott domain le legyen előtte validálva (lásd ITT); illetve OV tanúsítványnál pedig a szervezet validációját el kell előtte intézni (lásd ITT). A

felugró ablakban piros "*X*" jelzi, hogy melyik fülön van probléma. Amennyiben a validációk rendben vannak, a "***Consent***" fület jelzi csak pirosnak. Az igényt elfogadni akkor lehet, ha a ***Consent*** fülön található Message ablakba beírunk valamit - elegendő annyi is, hogy *OK*. Ekkor aktív lesz az *Accept* gomb, és el lehet fogadni az igénylést.

Értesítések e-mailben

Értesítések lejáró S/MIME tanúsítványok esetében

Terv alatt álló funkció:

Egyedi tanúsítványigénylések esetén a rendszer automatikusan lejárati értesítést küld a CertManager portálról, a tanúsítványban szereplő e-mail címre, a lejárat előtt 30, 15, 5 és 1 nappal.

Tömeges (bulk) igénylések esetén a felhasználók egyetlen értesítést kapnak 30 nappal a lejárat előtt, közvetlenül a tanúsítványkiadótól (CA).

A tanúsítvány lejáratáról szóló e-mail az alábbihoz hasonló:

> A xxxxxxxxxxxx sorszámú tanúsítvány, amely az alábbi entitás részére került kiadásra:
> E=xxxxx@auth.gr, CN=Aristotle University of Thessaloniki, O=Aristotle University of Thessaloniki, L=Thessaloniki, C=GR,
> és amelyet az alábbi tanúsítványkiadó bocsátott ki:
> CN=HARICA S/MIME RSA SubCA R3, O=Hellenic Academic and Research Institutions Cert. Authority, L=Athens, C=GR,
> lejár: 2025-05-14 10:14:45+03:00.

Amint a tömeges kérésekkel kiadott S/MIME tanúsítványok is megjelennek a "S/MIME Certificates" fülön, az értesítési rendszer ezekre is alkalmazni fogja a fenti figyelmeztetési időpontokat.

Szervezeti események

Az Organization felvételekor megadott emailcím értesítést kap:

- tanúsítvány igénylés érkezése
- tanúsítványigénylés elfogadása
- tanúsítvány visszavonása
- domain validálása

Leírások angol nyelven

- Enterprise Admin Guide
- Enterprise Approver Guide
- Hivatalos útmutatók

Segítség

PRO-M ügyfélszolgálat

Amennyiben ez a dokumentum nem tartalmazza a kérdésre a választ vagy megoldást a problémájára, az alábbi oldalon keresztül jelezhet nekünk: https://www.pro-m.hu/ugyfelszolgalat PRO-M Ügyfélszolgálat

TCSCertTypes (Archív)

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 (archív)

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
```