

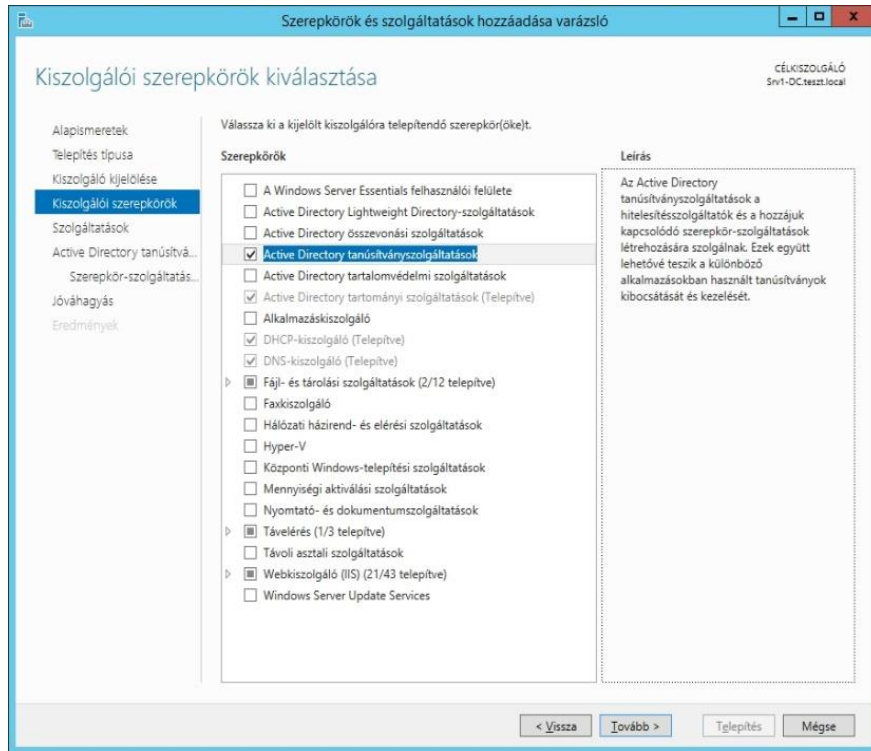
SSL tanúsítvány kérése AD-ban

Weblapok biztonságos eléréséhez szükség van SSL tanúsítványra (HTTPS elérés). Ebben a feladatban Active Directory használata mellett valósítjuk meg a tanúsítvány kérését. A kliens gépet léptessük be az Active Directory-ba.

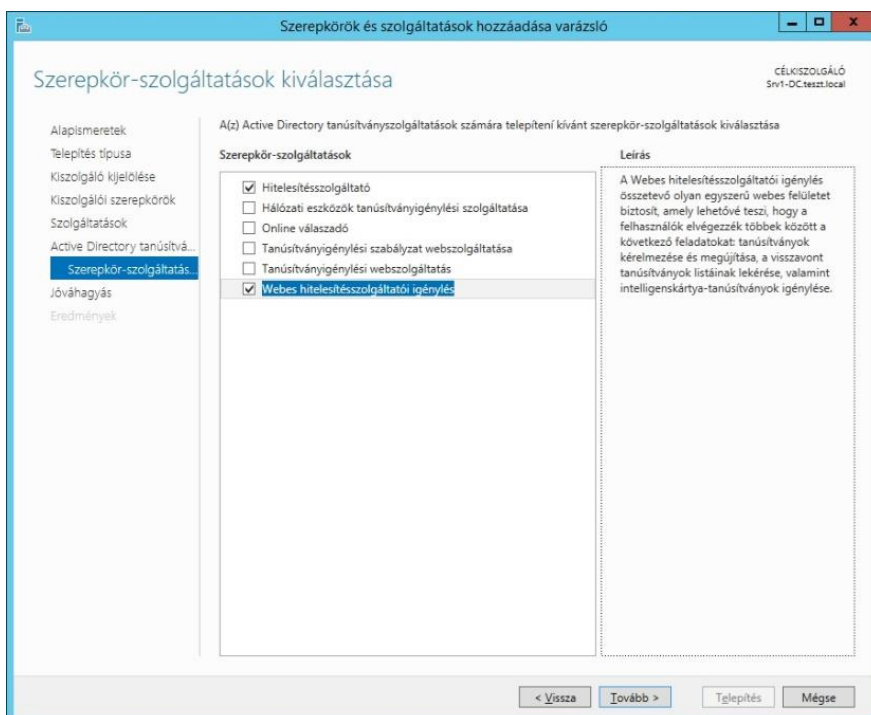
Először is szükségünk van a megfelelő szerepkörökre.

Tanúsítvány szolgáltatás telepítése

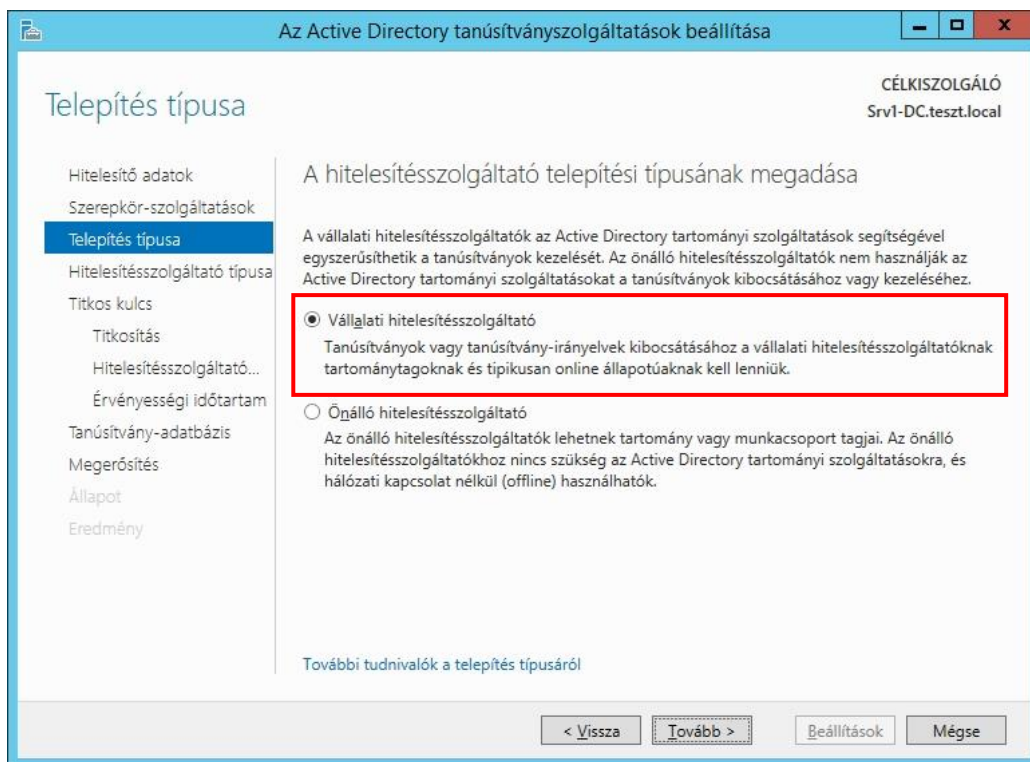
A kiszolgálókezelőben az **Active Directory tanúsítványszolgáltatások** szerepkört telepítjük.



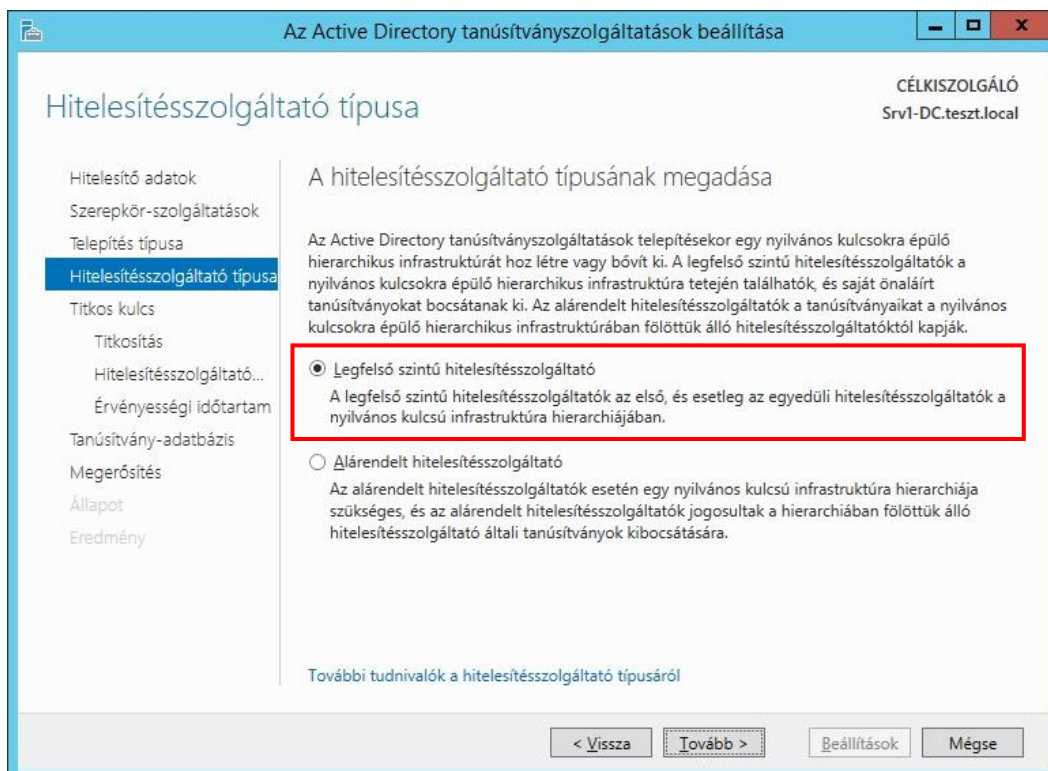
A következő ablakban kiválasztjuk a telepíteni kívánt szolgáltatások közül a **Hitelesítésszolgáltató** és a **Webes hitelesítésszolgáltatói igénylés** nevű szerepkör-szolgáltatásokat. Kattintsuk a **Tovább** gombra.



Az Active Directory tanúsítványszolgáltatások konfigurálásakor, a telepítés típusánál a **Vállalati hitelesítésszolgáltatót** választjuk, ezt csak tartományi tagként tehetjük meg és mivel a feladat az AD-ban való tanúsítványszolgáltatásról szól, ezt választjuk.



A következő pontban a **Legfelső szintű hitelesítésszolgáltatató**-t választjuk.



A tanúsítványokhoz szükség van egy kulcs létrehozására és mivel most telepítünk elsőnek tanúsítványszolgáltatást, nincs létező kulcsunk, **új kulcsot kell létrehoznunk**

The screenshot shows the 'Az Active Directory tanúsítványszolgáltatások beállítása' (Active Directory Certificate Services Configuration) window. The title bar indicates the target server is 'CÉLKISZOLGÁLÓ Srv1-DC.teszt.local'. The left sidebar lists various configuration tasks, with 'Titkos kulcs' (Private Key) selected. The main pane is titled 'A titkos kulcs típusának megadása' (Specify the private key type). It contains a text box explaining that a private key is needed for issuing and exporting certificates. Below this, three radio button options are presented: 'Új titkos kulcs létrehozása' (Create new private key), 'Meglévő titkos kulcs használata' (Use existing private key), and 'Tanúsítvány kiválasztása és a hozzá tartozó titkos kulcs használata' (Select certificate and use its private key). The first option is selected and highlighted with a red rectangle. The other two options are also highlighted with green rectangles. At the bottom, there are navigation buttons: '< Vissza', 'Tovább >', 'Beállítások', and 'Mégse'.

A következő pontban a titkosítást választjuk, rengeteg féle közül lehet válogatni. Mi az **RSA** kriptográfiát választjuk, **SHA256**-os HASH algoritmussal és **2048-es kulcshosszal**.

The screenshot shows the 'Az Active Directory tanúsítványszolgáltatások beállítása' (Active Directory Certificate Services Configuration) window, specifically the 'Hitelesítésszolgáltatói titkosítás' (Certificate Authority Key Protection) tab. The title bar shows the target server is 'CÉLKISZOLGÁLÓ Srv1-DC.teszt.local'. The left sidebar has 'Titkosítás' (Encryption) selected. The main pane is titled 'A kriptográfiai beállítások megadása' (Specify cryptographic settings). It contains two dropdown menus: 'Jelöljön ki egy kriptográfiai szolgáltatót:' (Select a cryptographic provider) and 'Kulcshossz:' (Key length). The first dropdown is set to 'RSA#Microsoft Software Key Storage Provider' and the second to '2048'. Below these, a list of hash algorithms is shown: SHA256, SHA384, SHA512, and SHA1. The 'SHA256' option is selected and highlighted with a green rectangle. At the bottom, there is a checkbox for 'Rendszergazdai beavatkozás engedélyezése, ha a hitelesítésszolgáltató hozzáfér a titkos kulcshoz.' (Allow administrator intervention if the certificate authority can access the private key). Navigation buttons at the bottom include '< Vissza', 'Tovább >', 'Beállítások', and 'Mégse'.

A következő pár pontban nem kell semmit se változtatni azokat az alapbeállításokon hagyjuk.

Az Active Directory tanúsítványszolgáltatások beállítása

CÉLKISZOLGÁLÓ
Srv1-DC.teszt.local

Hitelesítésszolgáltató neve

Hitelesítő adatok
Szerepkör-szolgáltatások
Telepítés típusa
Hitelesítésszolgáltató típusa
Titkos kulcs
Titkosítás
Hitelesítésszolgáltató...
Érvényességi időtartam
Tanúsítvány-adatbázis
Megerősítés
Állapot
Eredmény

A hitelesítésszolgáltató nevének megadása

Írjon be egy köznevi nevet a hitelesítésszolgáltató azonosításához. Ez a név a hitelesítésszolgáltató által kibocsátott minden tanúsítványhoz hozzáadódik. A megkülönböztető név utótagjának értéke automatikusan generált, de módosítható.

Hitelesítésszolgáltató köznevi neve:
TESZT-SRV1-CA

Megkülönböztető név utótagja:
DC=teszt,DC=local

Megkülönböztető név előnézete:
CN=TESZT-SRV1-CA,DC=teszt,DC=local

További tudnivalók a hitelesítésszolgáltatói névről

< Vissza Tovább > Beállítások Mégse

A következő beállítást az IIS-nél végezzük, ha nem volt telepítve, az **URL-hitelesítést** adjuk hozzá. Ezzel a szerepkör-szolgáltatással korlátozhatjuk, hogy ki érje el a honlapot (és *ki nem*) a megfelelő felhasználónév/jelszó párossal.

Szerepkörök hozzáadása varázsló

Szerepkör-szolgáltatások kiválasztása

Alapismertek
Kiszolgálói szerepkörök
Active Directory tanúsítványszolg...
Szerepkör-szolgáltatások
Telepítés típusa
Hitelesítésszolgáltató típusa
Titkos kulcs
Titkosítás
Hitelesítésszolgáltató neve
Érvényességi időtartam
Tanúsítvány-adatbázis
Webkiszolgáló (IIS)
Szerepkör-szolgáltatások
Jóváhagyás
Folyamat
Eredmények

Válassza ki a(z) Webkiszolgáló (IIS) szerephez telepítendő szerepkör-szolgáltatásokat:

Szerepkör-szolgáltatások:

- ☒ Naplózási eszközök
- ☒ Kérésnyelvény (telepítve)
- ☒ Nyomkövetés
- ☐ Egyéni naplózás
- ☐ ODBC-naplózás
- ☐ Biztonság (telepítve)
- ☐ Egyszerű hitelesítés
- ☒ Windows-hitelesítés (telepítve)
- ☐ Kivonatoló hitelesítés
- ☐ Ügyféltanúsítvány-hozzárendeléses hitelesítés
- ☐ IIS ügyféltanúsítvány-hozzárendeléses hitelesítés
- ☒ URL-hitelesítés
- ☒ Kérésűrés (telepítve)
- ☐ IP-cím és tartomány korlátozása
- ☐ Teljesítmény (telepítve)
- ☒ Statikus tartalom tömörítése (telepítve)
- ☐ Dinamikus tartalom tömörítése
- ☐ Kezelőeszközök (telepítve)
- ☒ IIS Kezelése konzol (telepítve)
- ☐ IIS-kezelés parancsfájljai és eszközei

Leírás:
Az URL-hitelesítés használata lehetővé teszi a webtartalom elérését korlátozó szabályok létrehozását. Ezek a szabályok köthetők felhasználókhoz, csoportokhoz, illetve a HTTP-fejlec műveleteihez. Az URL-hitelesítési szabályok konfigurálásával megakadályozható, hogy azok az alkalmazottak, akik nem tagjai bizonyos csoportoknak, hozzáférjenek a tartalomhoz, illetve kommunikáljanak a weblapokkal.

További tudnivalók a szerepkör-szolgáltatásokról

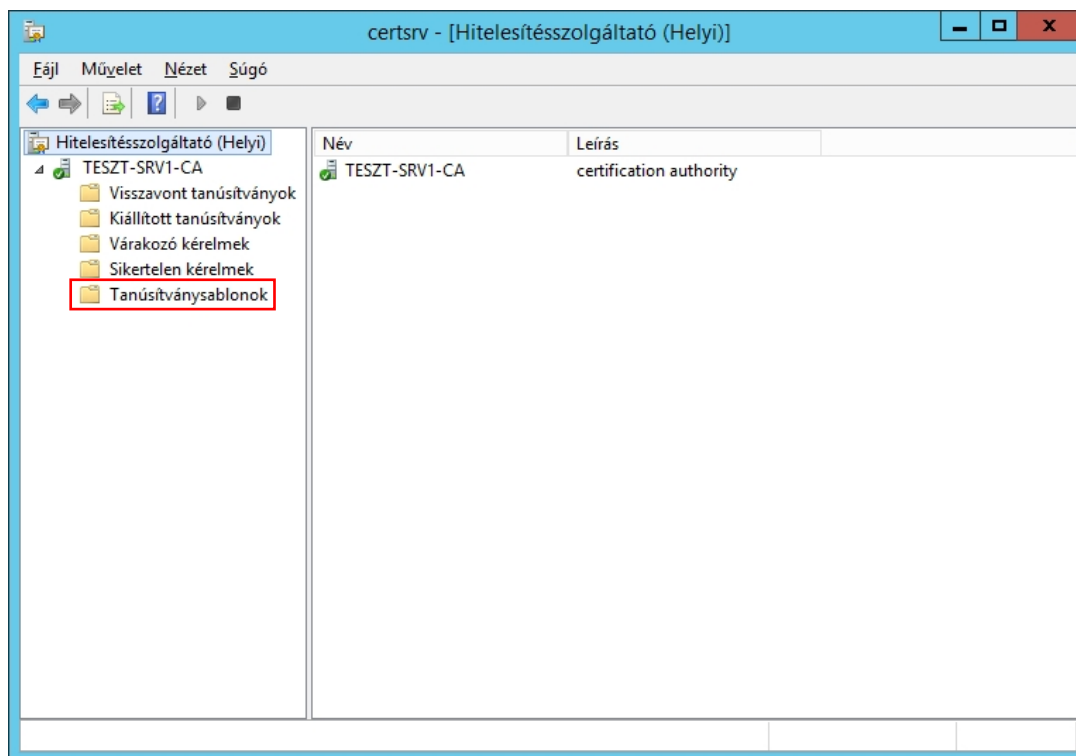
< Vissza Tovább > Telepítés Mégse

A jóváhagyásnál ellenőrizzük a beállításokat majd telepítsük a szerepköröket. Újraindítás nem szükséges.

A felügyeleti eszközökben megtalálhatjuk a Tanúsítványszolgáltatót, valamilyen oknál fogva ezt a nevet nem fordították le magyarra.

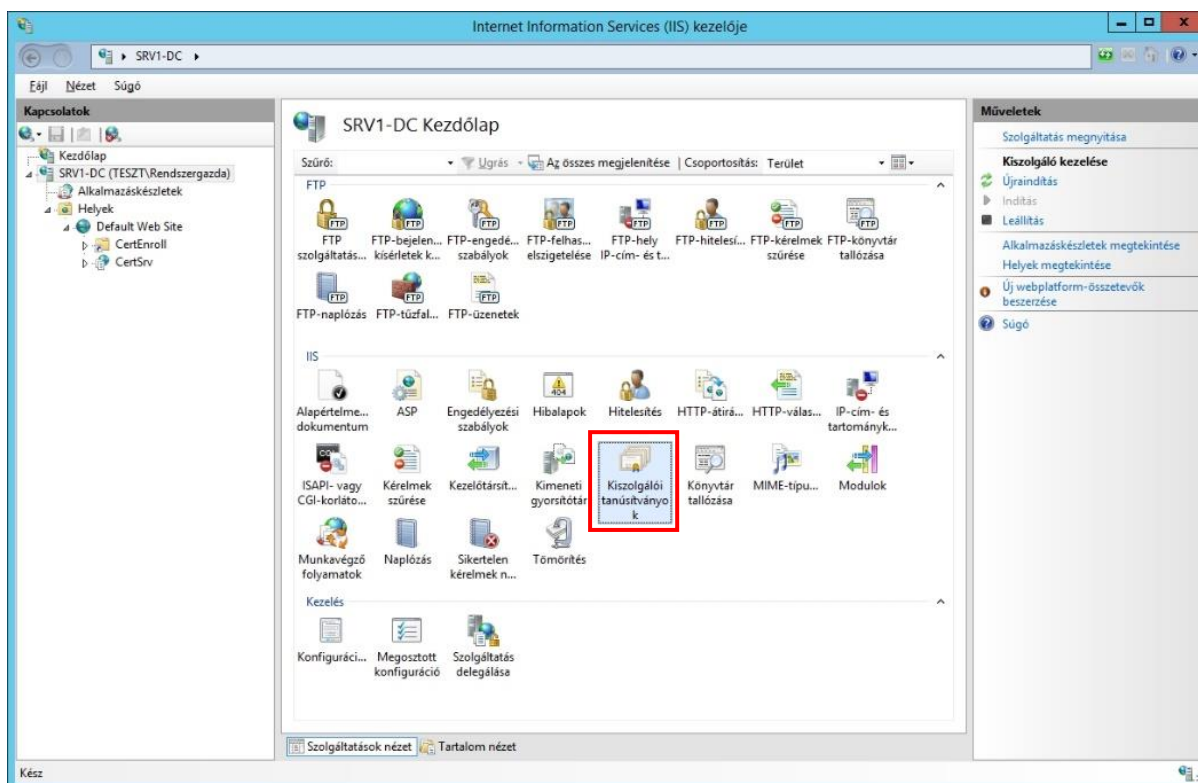


Megnyitás után lényegi beállítást nem kell végeznünk. A zöld pipával jelzett név a Hitelesítő szervert, benne 5 db mappa található, a nevük alapján tudjuk mire szolgálnak. Ha **AD nélkül** telepítjük akkor a Tanúsítványsablonok mappa nem található meg.

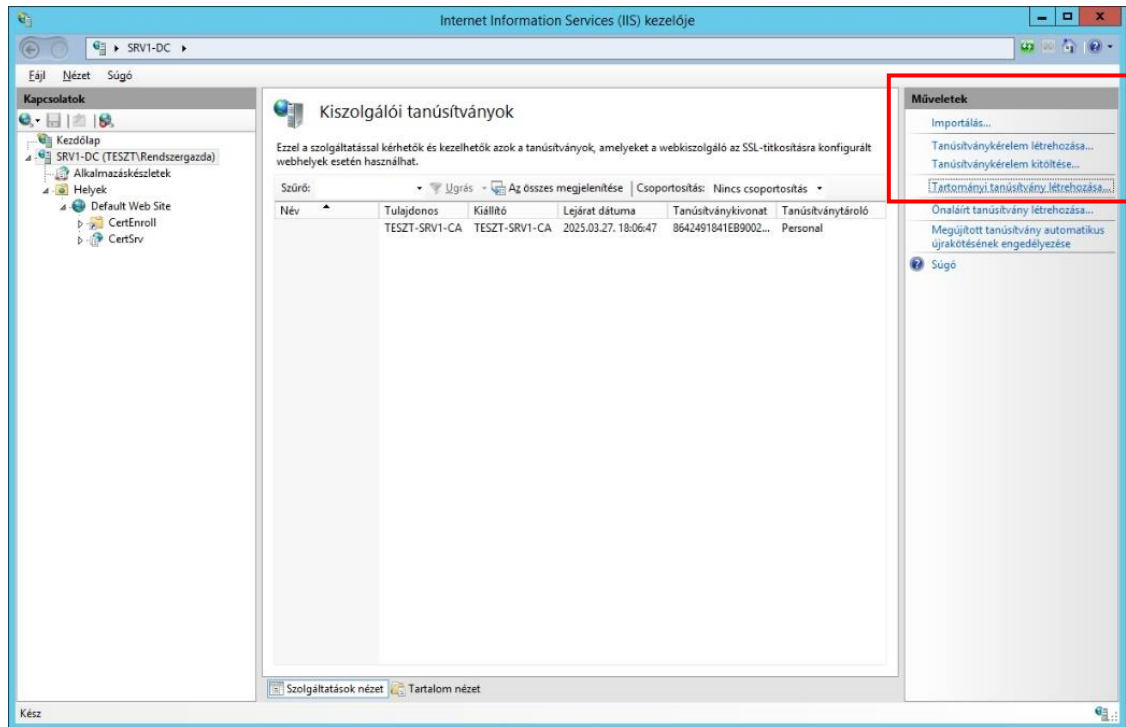


Biztonságos webhely kialakítása

Az alapértelmezett webhelyet fogjuk használni (Default Web Site). Előtte a webkiszolgálónak egy tanúsítványt kell igényelnünk. Első lépésként a legfelső (szerver) szinten a kiszolgálói tanúsítványok beállítás menüjébe lépünk.



Itt jobb oldalt a műveleteknél kiválasztjuk a **Tartományi tanúsítvány létrehozását**.



A felugró ablakban meg kell adnunk az adatainkat.

Az első helyre adjuk meg a tanúsítvány **Köznapi nevét** (ahogyan a kötésben is szerepel „a webkiszolgálónk neve”), a többi helyre írhatunk adatokat tetszőlegesen, kivétel az utolsó pont, oda a **HU**-t írjuk.

Tanúsítvány létrehozása

Megkülönböztető név tulajdonságai

Adja meg a tanúsítványhoz szükséges adatokat. Az Állam/megye és a Település/helység mezőben a hivatalos elnevezést kell megadni, és nem használható rövidítés.

Köznapi név:	www.teszt.local
Szervezet:	home
Szervezeti egység:	home
Település/helység:	DB
Állam/megye:	HB
Ország/terület:	HU

Vissza Tovább Befejezés Mégse

A tovább gombra kattintva ki kell választanunk az **online hitelesítési szolgáltatót**: ez a mi szerverünk, a **Kijelölés gombra** kattintva kiválasztjuk a szolgáltatót.

Tanúsítvány létrehozása

Online hitelesítésszolgáltató

Adja meg a tartományán belüli hitelesítésszolgáltatót, amely alá fogja írni a tanúsítványt. Meg kell adni egy rövid nevet, amelyet célszerű úgy megválasztani, hogy könnyen megjegyezhető legyen.

Adja meg az online hitelesítésszolgáltatót:

Kijelölés...

Példa: HitelesítésszolgáltatóNeve\Kiszolgálónév

Rövid név:

Vissza

Tovább

Befejezés

Mégse

Hitelesítésszolgáltató kiválasztása

Válassza ki a használni kívánt hitelesítésszolgáltatót:

Hitelesítésszolgáltató	Számítógép
TESZT-SRV1-CA	Srv1-DC.teszt.local

OK

Mégse

A rövid névhez „www” kifejezést írjuk. Majd a **Befejezés** gombra kattintunk.

Tanúsítvány létrehozása

Online hitelesítésszolgáltató

Adja meg a tartományán belüli hitelesítésszolgáltatót, amely alá fogja írni a tanúsítványt. Meg kell adni egy rövid nevet, amelyet célszerű úgy megválasztani, hogy könnyen megjegyezhető legyen.

Adja meg az online hitelesítésszolgáltatót:

Kijelölés...

Példa: HitelesítésszolgáltatóNeve\Kiszolgálónév

Rövid név:

Vissza

Tovább

Befejezés

Mégse

Ezzel a **webkiszolgálónk kapott egy tanúsítványt**, ami már megfelelő a biztonságos webhely létrehozásához.

Internet Information Services (IIS) kezelője

Kapcsolatok

Kiszolgálói tanúsítványok

Ezzel a szolgáltatással kérhetők és kezelhetők azok a tanúsítványok, amelyeket a webkiszolgáló az SSL-titkosításra konfigurált webhelyek esetén használhat.

Szűrő: Ugrás: Az összes megjelenítése | Csoportosítás: Nincs csoportosítás

Név	Tulajdonos	Kiállító	Lejárat dátuma	Tanúsítványkivonat	Tanúsítványtároló
TESZT-SRV1-CA	TESZT-SRV1-CA	TESZT-SRV1-CA	2025.03.27. 18:06:47	8642491841EB9002...	Personal
www	www.teszt.local	TESZT-SRV1-CA	2022.03.27. 19:01:00	2A93F7054626B9B...	Personal

Műveletek

Importálás...

Tanúsítványkérelem létrehozása...

Tanúsítványkérelem kitöltése...

Tartományi tanúsítvány létrehozása...

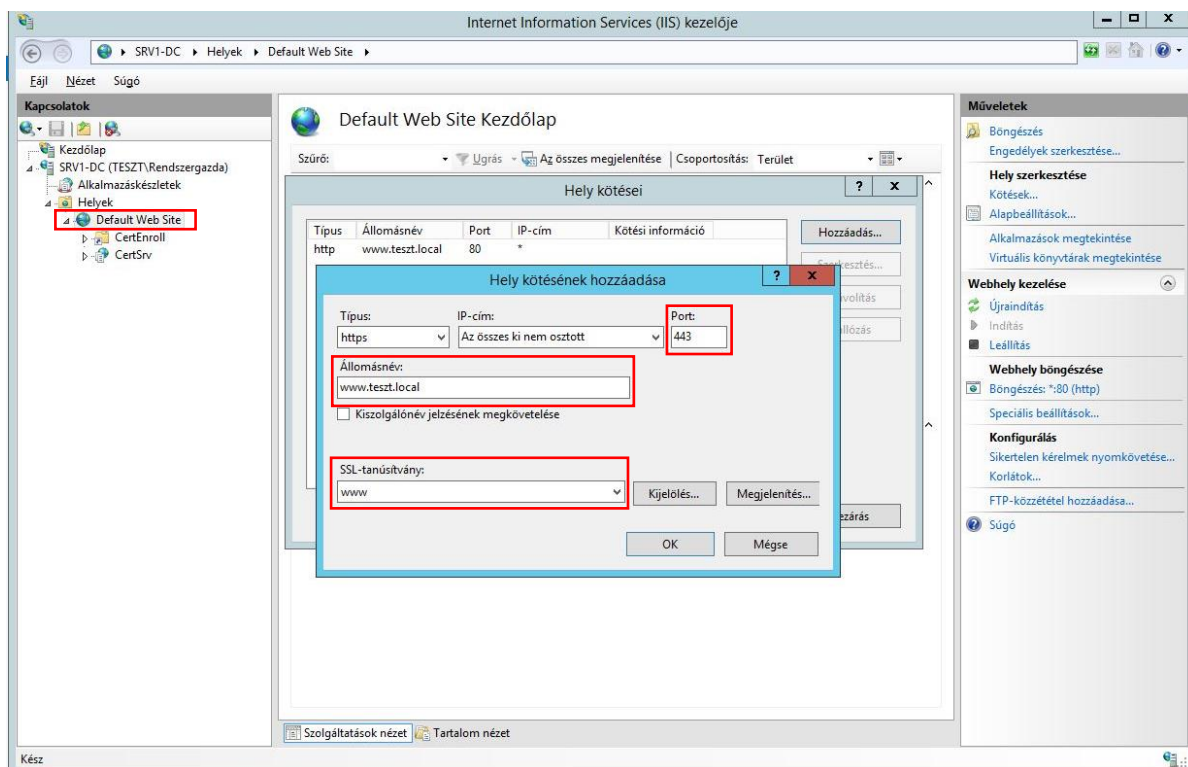
Önaláírt tanúsítvány létrehozása...

Megújított tanúsítvány automatikus újrakötésének engedélyezése

Súgó

Az **alapértelmezett webhelynél** vegyünk fel egy új kötést, **HTTPS** kapcsolattal és a **443 porttal**. A típus kiválasztása után az állomásnév beszűrkül és az **SSL-tanúsítvány-nál** kijelölhetjük a tanúsítványt. Itt az általunk létrehozott **www** nevű tanúsítványt válasszuk.

A **Megjelenítés gomb-ra** kattintva megnézhetjük a tanúsítványunkat, a megjelenő adatlap harmadik fülén pedig a Tanúsítvány-láncot, hogy milyen hierarchiában épülnek fel. Végül az **OK** gombra kattintunk.



Kitérésként:

Megoldottuk, hogy a **HTTPS** protokoll is működik a megadott portszámon, de emellett még a **80-as** alapértelmezett port is működik, ez így nem mindig a legbiztonságosabb és a legelőnyösebb, ezért a **80-as** portot vagy letiltják vagy átirányítják.

Az SSL megfelelő beállításával a kliensek honlap elérését korlátozhatjuk és megakadályozhatjuk a **80-as** port használatát. Állítsuk be az SSL-t:

Kattintsunk az SSL-beállítás fülre, és pipáljuk be a **SSL – megkövetelését**, a jobb oldali sávban az **alkalmaz** gombra kattintva érvényesítsük a beállításunkat.

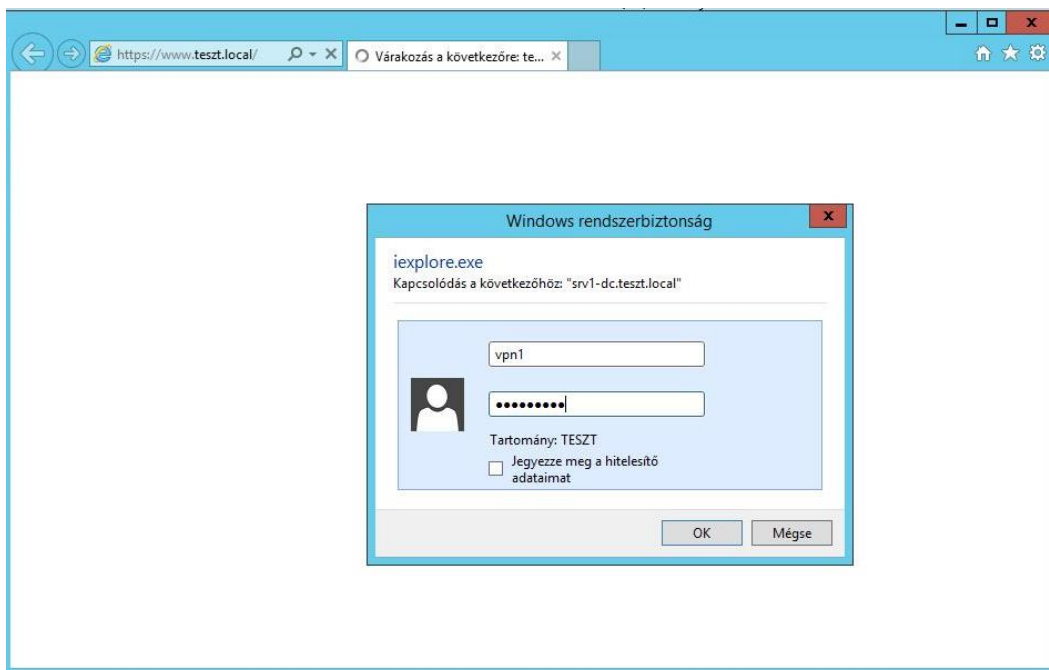
Felmerül egy probléma, a **443-as** porton továbbra is elérjük a weblapunkat, de a **80-as** portra hibalapot ad ki.

Megoldás: Hibalapoknál vegyünk fel egyéni hibalapot. (*hibakód száma: 403.4*)

A korlátozzuk le, hogy ki érhesse el a weblapunkat:

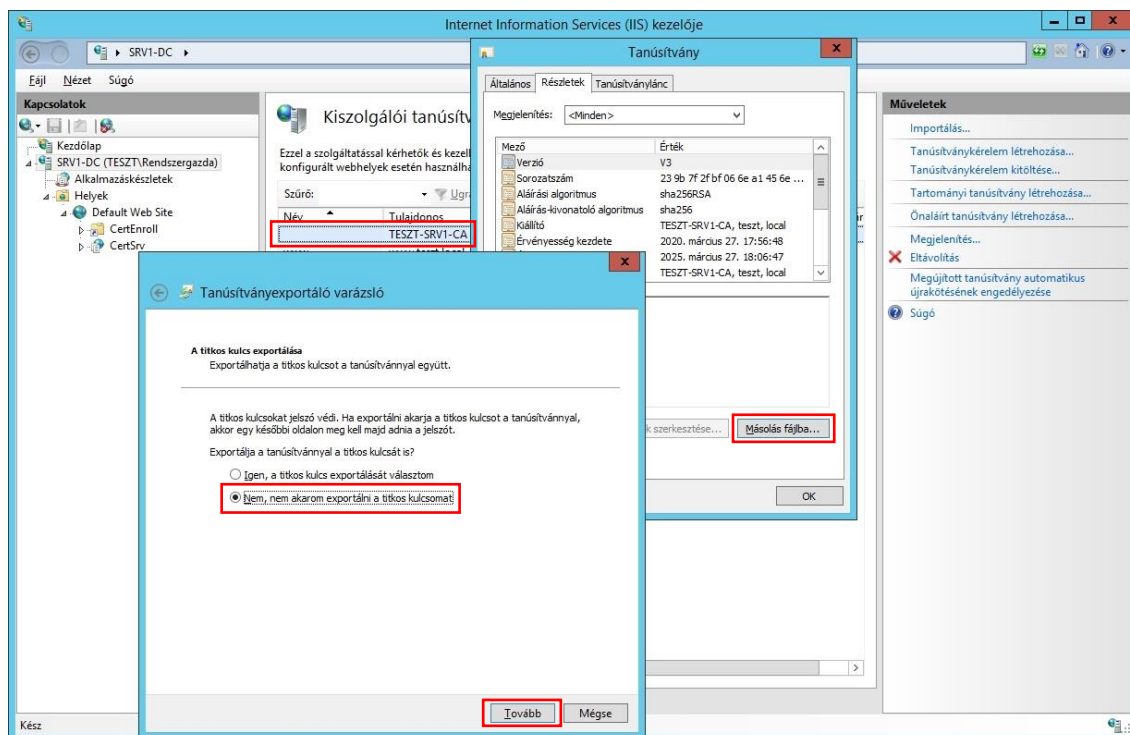
Ezt az IIS szerepkörében *-tartományi felhasználók esetén-* a **Windows-hitelesítés** nevű szerepkör-szolgáltatás használatával végezzük el.

A beállítás után **teszteljük a szerverről a belépést**, a webhely indítása után írjuk be a megfelelő felhasználónév és jelszó párost, ha beenged akkor sikerült, ha nem akkor nézzük át a beállításokat.
Teszteljük úgyis, hogy belépésre nem jogosult felhasználót adunk meg.

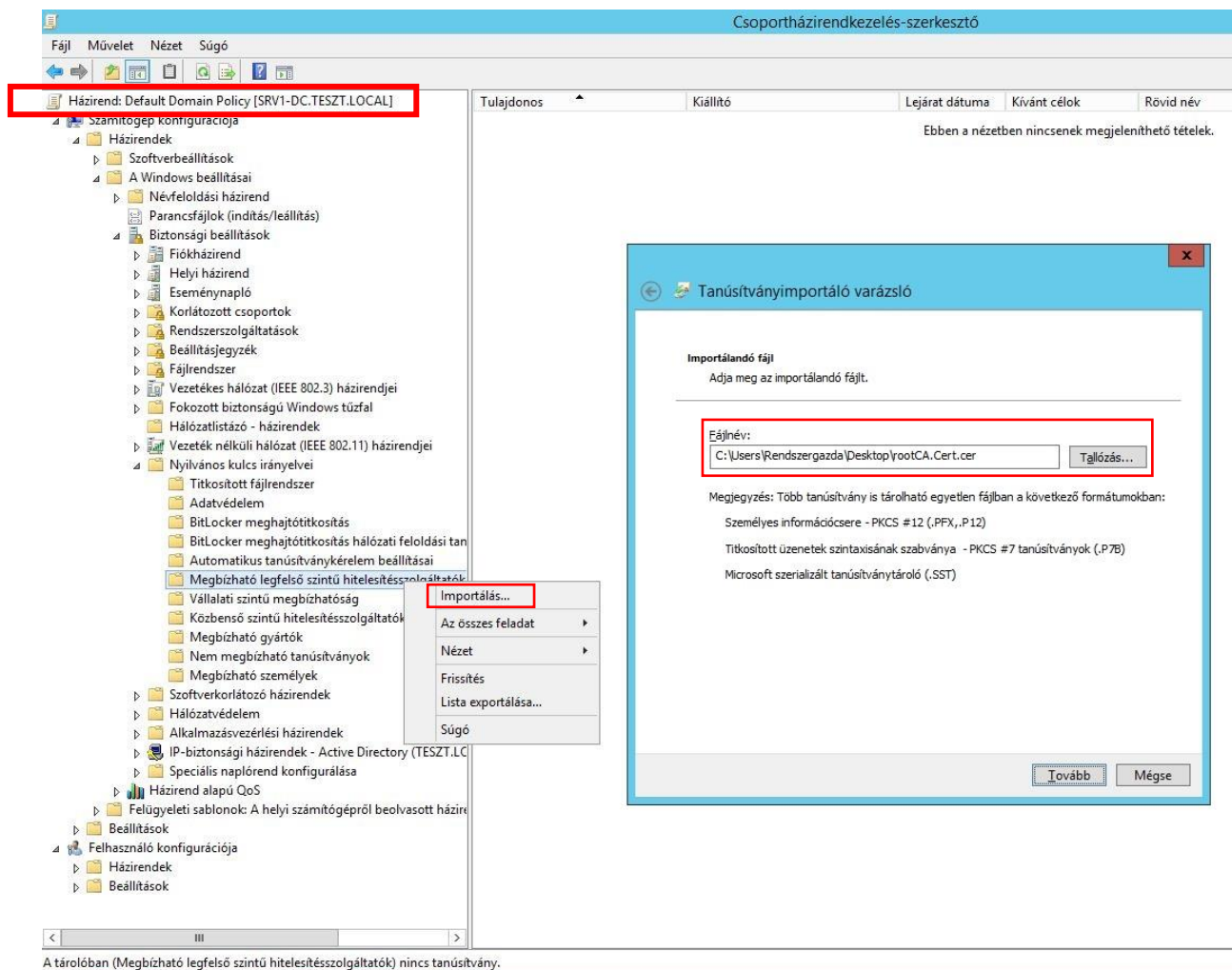


A végül érjük el, hogy a Window10 kliensen ne kelljen külön letölteni a CA kiszolgálói tanúsítványt, hanem azonnal megkapja. Ezt csoportházirendben állíthatjuk be.

Először az IIS-ben az általunk használt **CA kiszolgáló tanúsítványát** kiexportáljuk. Megjelenítés dupla kattintással a tanúsítvány nevéen, aztán a részletek fülénél az alsó sarokban kiválasztjuk a „Másolás fájlba...” menüpontot, nem állítjuk át az alapértelmezéseket. (Mentsük az asztalra!)



Ezután a csoportházi rendben kiválasztjuk a megfelelő menüpontot a **Default Domain Policy**-ban.
Számítógép konfigurációja / Windows beállítások / Biztonsági beállítások / Nyilvános kulcs irányelvei majd a **Megbízható legfelső szintű hitelesítésszolgáltatók**-nál **Importálás**-t választunk.
Kiválasztjuk az előzőleg letöltött (exportált) tanúsítványt.



Ezzel elértük, hogy a tartományi számítógépeken minden további beállítás nélkül letöltse a tanúsítványt.

Ne felejtsünk el gondoskodni a csoportházi rend frissítéséről. (*gpupdate /force*)

Szükség esetén a kliensünket újra is kell indítani, hiszen Számítógépek konfigurációjára ható csoportházi rend szabályt módosítottunk!

A végső, tesztelési fázisba érkezünk.

Indítsuk el a **Windows 10** virtuális számítógépet!

Léptessük be a kliens gépünket a tartományba! (esetünkben ez a tartomány a **teszt.local**).

Ezután lépünk be valamelyik általunk létrehozott felhasználóval (pl. **vpn1**)!

Ellenőrizzük a szerver tanúsítványát. (*kis lakat zárva?*)

Végül a webhely elérhetőségét mind a **443**-as mind a **80**-as porton át is. (**80-as portot használva a webhely átirányítását teszteljük**).