

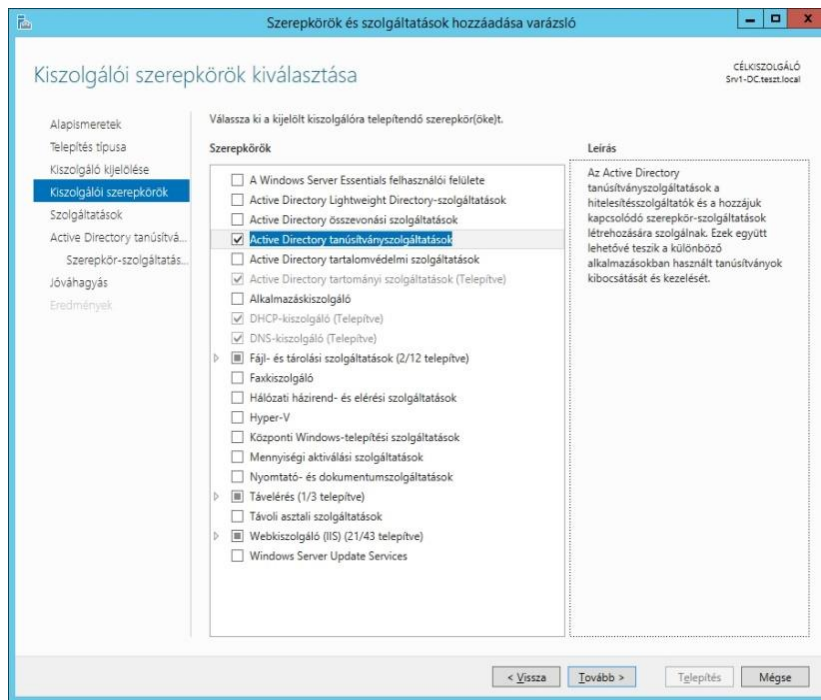
## SSL tanúsítvány kérése AD-ban

A kliens gépet léptessük be az Active Directory-ba, a szerveren és a kliensen is kapcsoljuk be a tűzfalat a bejövő forgalomnál. A webhely működéséhez a 80-as és a 443-as portokat engedélyeznünk kell a bejövő forgalom esetén. A tűzfalról és annak beállításairól még nem volt szó, ez csak kis bemelegítésként van most benne a leírásban.

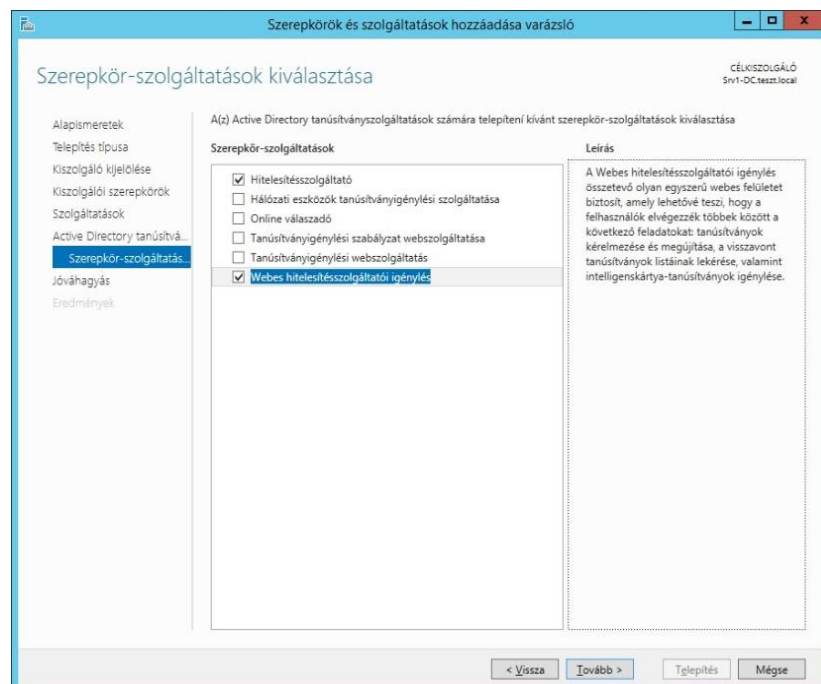
Weblapok biztonságos eléréséhez szükség van SSL tanúsítványra (HTTPS elérés). Ebben a feladatban Active Directory használatával valósítjuk meg a tanúsítvány kérését. Ehhez szükségünk van a megfelelő szerepkörökre.

### Tanúsítvány szolgáltatás telepítése

A kiszolgálókezelőben az Active Directory tanúsítványszolgáltatások szerepkört telepítjük.



A következő ablakban, kiválasztjuk a telepíteni kívánt szolgáltatásokat itt az első kettőt jelöljük be. A második pont bejelölése után a felugró ablakban az IIS telepítését fogadjuk el és kattintsuk a tovább gombra.



A telepítés típusánál a Vállalat szintű beállítást választjuk, ezt csak tartományi tagként tehetjük meg, és mivel a feladat az AD-ban való tanúsítványkezelésről szól, ezt választjuk.

The screenshot shows the 'Telepítés típusa' (Installation Type) window in the 'Az Active Directory tanúsítványkezelési szolgáltatások beállítása' (Configure Active Directory Certificate Services) console. The window title is 'Az Active Directory tanúsítványkezelési szolgáltatások beállítása'. The top right corner shows 'CÉLKISZOLGÁLÓ' and 'Srv1-DC.teszt.local'. The left sidebar contains a list of configuration steps: 'Hitelesítő adatok', 'Szerepkör-szolgáltatások', 'Telepítés típusa' (selected), 'Hitelesítésszolgáltatató típusa', 'Titkos kulcs', 'Titkosítás', 'Hitelesítésszolgáltatató...', 'Érvényességi időtartam', 'Tanúsítvány-adatbázis', 'Megerősítés', 'Állapot', and 'Eredmény'. The main content area is titled 'A hitelesítésszolgáltatató telepítési típusának megadása' (Specify the installation type for the certificate service). It contains a paragraph explaining that enterprise certificate services use Active Directory for simplified management, while standalone services do not. Below this, there are two radio button options: 'Vállalati hitelesítésszolgáltatató' (selected) and 'Önálló hitelesítésszolgáltatató'. The 'Vállalati' option is described as being used for issuing certificates to domain members and requiring online status. The 'Önálló' option is described as being used for standalone services without Active Directory dependencies. At the bottom, there are buttons for '< Vissza', 'Tovább >', 'Beállítások', and 'Mégse'.

A következő pontban a legfelső szintű szolgáltatást választjuk.

The screenshot shows the 'Hitelesítésszolgáltatató típusa' (Certificate Service Type) window in the 'Az Active Directory tanúsítványkezelési szolgáltatások beállítása' (Configure Active Directory Certificate Services) console. The window title is 'Az Active Directory tanúsítványkezelési szolgáltatások beállítása'. The top right corner shows 'CÉLKISZOLGÁLÓ' and 'Srv1-DC.teszt.local'. The left sidebar contains a list of configuration steps: 'Hitelesítő adatok', 'Szerepkör-szolgáltatások', 'Telepítés típusa', 'Hitelesítésszolgáltatató típusa' (selected), 'Titkos kulcs', 'Titkosítás', 'Hitelesítésszolgáltatató...', 'Érvényességi időtartam', 'Tanúsítvány-adatbázis', 'Megerősítés', 'Állapot', and 'Eredmény'. The main content area is titled 'A hitelesítésszolgáltatató típusának megadása' (Specify the certificate service type). It contains a paragraph explaining that Active Directory certificate services are built on a hierarchy of public keys, with the top-level service being the root of the hierarchy. Below this, there are two radio button options: 'Legfelső szintű hitelesítésszolgáltatató' (selected) and 'Alárendelt hitelesítésszolgáltatató'. The 'Legfelső' option is described as the first and only service in the hierarchy. The 'Alárendelt' option is described as being part of a hierarchy where the service is subordinate to a higher-level service. At the bottom, there are buttons for '< Vissza', 'Tovább >', 'Beállítások', and 'Mégse'.

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

**Az Active Directory tanúsítványszolgáltatások beállítása**

CÉLKISZOLGÁLÓ  
Srv1-DC.teszt.local

### Titkos kulcs

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

#### A titkos kulcs típusának megadása

Az ügyfelek tanúsítványainak előállításához és kibocsátásához a hitelesítésszolgáltatóknak titkos kulcsra van szükségük.

☒ **Új titkos kulcs létrehozása**  
Használja ezt a beállítást, ha nem rendelkezik titkos kulccsal, vagy új titkos kulcsot szeretne létrehozni.

☐ **Meglévő titkos kulcs használata**  
Akkor használja ezt a beállítást, ha a hitelesítésszolgáltató újratelepítése után szükség van az előzőleg kibocsátott tanúsítványok folytonosságának megőrzésére.

☐ **Tanúsítvány kiválasztása és a hozzá tartozó titkos kulcs használata**  
Akkor használja ezt a beállítást, ha a számítógépen már van tanúsítvány, vagy importálni szeretne egy tanúsítványt, és annak titkos kulcsát szeretné használni.

☐ **Meglévő titkos kulcs kiválasztása a számítógépről**  
Akkor használja ezt a beállítást, ha megtartotta az előző telepítésből származó titkos kulcsokat, vagy ha egy más forrásból származó titkos kulcsot kíván használni.

További tudnivalók a titkos kulcsról

< Vissza   **Tovább >**   Beállítások   Mégse

A következő pontban a titkosítást választjuk, rengeteg féle közül lehet válogatni. Mi az RSA kriptográfiát választjuk, SHA256-os hash algoritmussal és 2048-es kulchosszal. A következő pár pontban nem kell semmit se változtatni azokat az alapbeállításokon hagyjuk.

**Az Active Directory tanúsítványszolgáltatások beállítása**

CÉLKISZOLGÁLÓ  
Srv1-DC.teszt.local

### Hitelesítésszolgáltatói titkosítás

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

#### A kriptográfiai beállítások megadása

Jelöljön ki egy kriptográfiai szolgáltatót:   Kulchossz:

RSA#Microsoft Software Key Storage Provider   2048

Válassza ki a hitelesítésszolgáltató által kibocsátott tanúsítványok aláírásához használt kivonatoló algoritmust:

SHA256  
SHA384  
SHA512  
SHA1

☐ Rendszergazdai beavatkozás engedélyezése, ha a hitelesítésszolgáltató hozzáfér a titkos kulcshoz.

További tudnivalók a titkosításról

< Vissza   **Tovább >**   Beállítások   Mégse

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 köznapit a hitelesítésszolgáltató azonosításához. Ez a név a hitelesítésszolgáltató által kibocsátott minden tanúsítványhoz hozzáadódik. A megkülönböztető név utótagjának értéke automatikusan generált, de módosítható.

Hitelesítésszolgáltató köznapit 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

Alapmeretek

Kiszolgálói szerepkörök

Active Directory tanúsítvány-szolg...

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
  - ☒ Kérésfigyelő (telepítve)
  - ☒ Nyomkövetés
  - ☐ Egyéni naplózás
  - ☐ ODBC-naplózás
- ☒ Biztonság (telepítve)
  - ☐ Egyszerű hitelesítés
  - ☒ Windows-hitelesítés (telepítve)
  - ☐ Kivonatoló hitelesítés
  - ☐ Ügyfél-tanúsítvány-hozzárendeléses hitelesítés
  - ☒ IIS ügyfél-tanúsítvány-hozzárendeléses hitelesítés
  - ☒ URL-hitelesítés
- ☒ Kérésűrés (telepítve)
- ☐ IP-cím és tartomány korlátozása
- ☒ Teljesítmény (telepítve)
  - ☒ Statisztika tartalom tömörítése (telepítve)
  - ☐ Dinamikus tartalom tömörítése
- ☒ Kezelőeszközök (telepítve)
  - ☒ IIS kezelése konzol (telepítve)
  - ☐ IIS-kezelés parancsfájlai és eszközei

[További tudnivalók a szerepkör-szolgáltatásokról](#)

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.

< Vissza

Tovább >

Telepítés

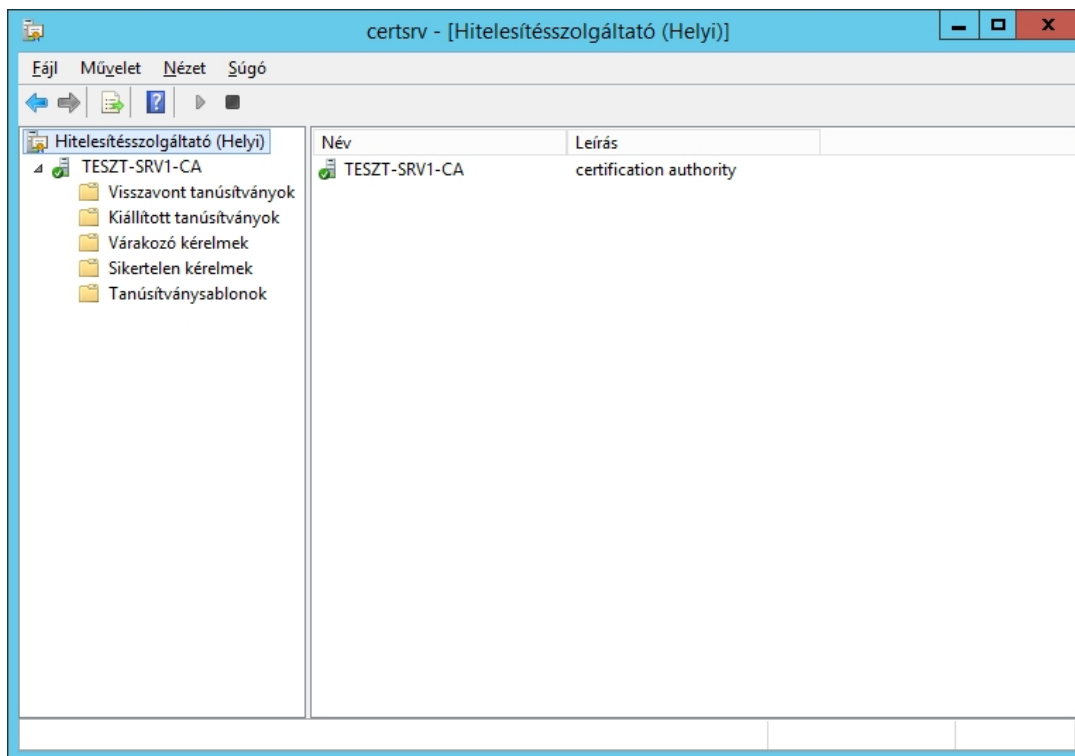
Mégse

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

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

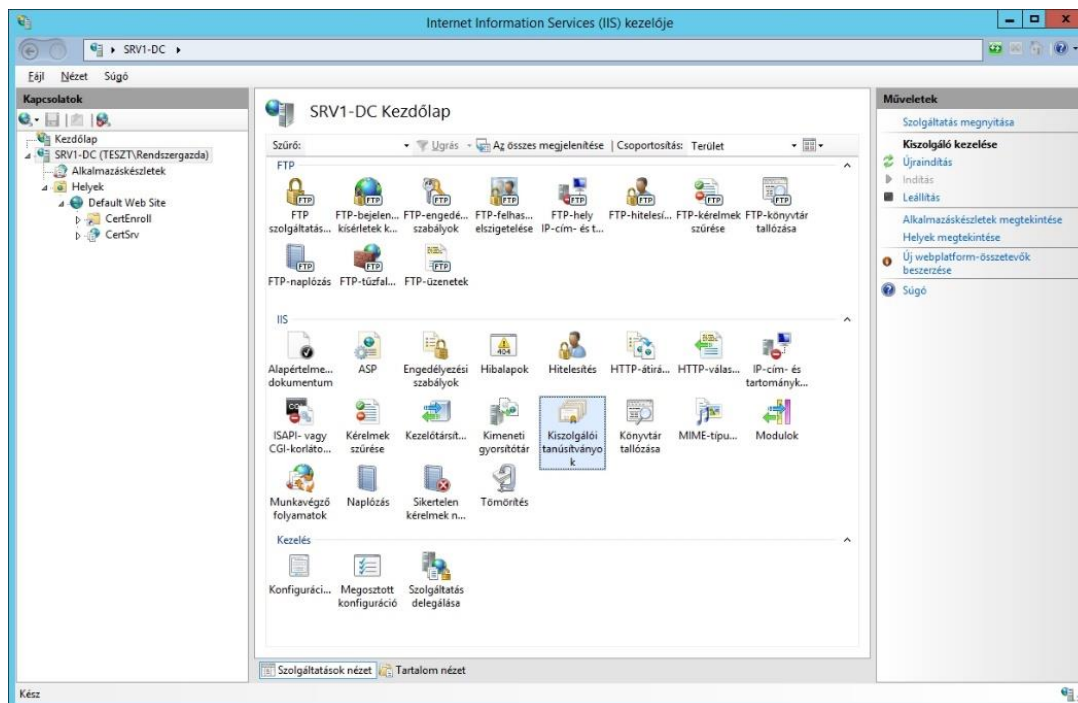


Megnyitás után lényegi beállítást nem kell végeznünk. A zöld pipával jelzett név a Hitelesítő szerver, benne 5 mappa található, a nevük alapján tudjuk mire szolgálnak. Ha **AD nélkül** telepítjük akkor a Tanúsítványsablonok mappa nem található meg.



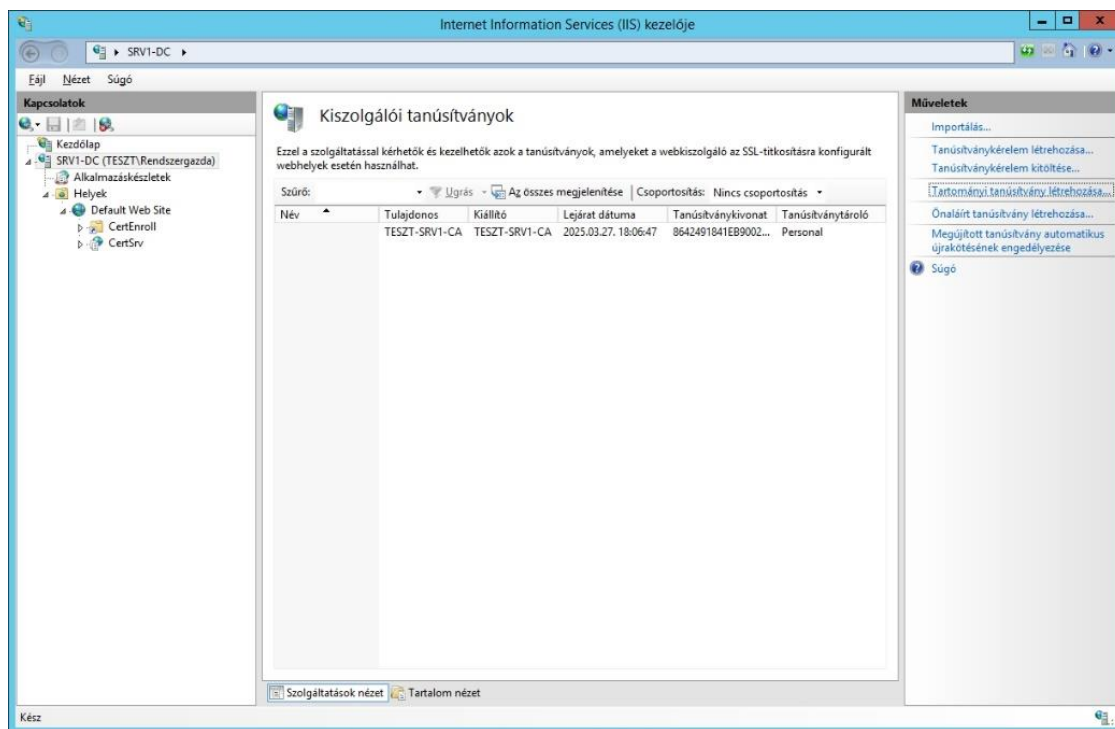
### Biztonságos webhely kialakítása

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 megkell adnunk az adatainkat. Az első helyre adjuk meg a tanúsítvány **Köznapi nevét** (ahogyan a kötésben is szerepel), a többi helyre írunk adatokat „tetszőlegesen”, kivétel az utolsó pont, oda a „**HU**”-t írunk.

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:

Szervezet:

Szervezeti egység:

Település/helység:

Állam/megye:

Ország/terület:

Vissza Tovább Befejezés Mégse

A tovább gombra kattintva ki kell választanunk a 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:

VisszaTovábbBefejezésMégse

Hitelesítésszolgáltató kiválasztása

Válassza ki a használni kívánt hitelesítésszolgáltatót:

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

OKMégse

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:

TESZT-SRV1-CA\Srv1-DC.teszt.local

Kijelölés...

Példa: HitelesítésszolgáltatóNeve\Kiszolgálónév

Rövid név:

www

VisszaTovábbBefejezésMégse

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

Internet Information Services (IIS) kezelője

SRV1-DC

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
www	www.teszt.local	TESZT-SRV1-CA	2025.03.27. 18:06:47	8642491841EB9002...	Personal

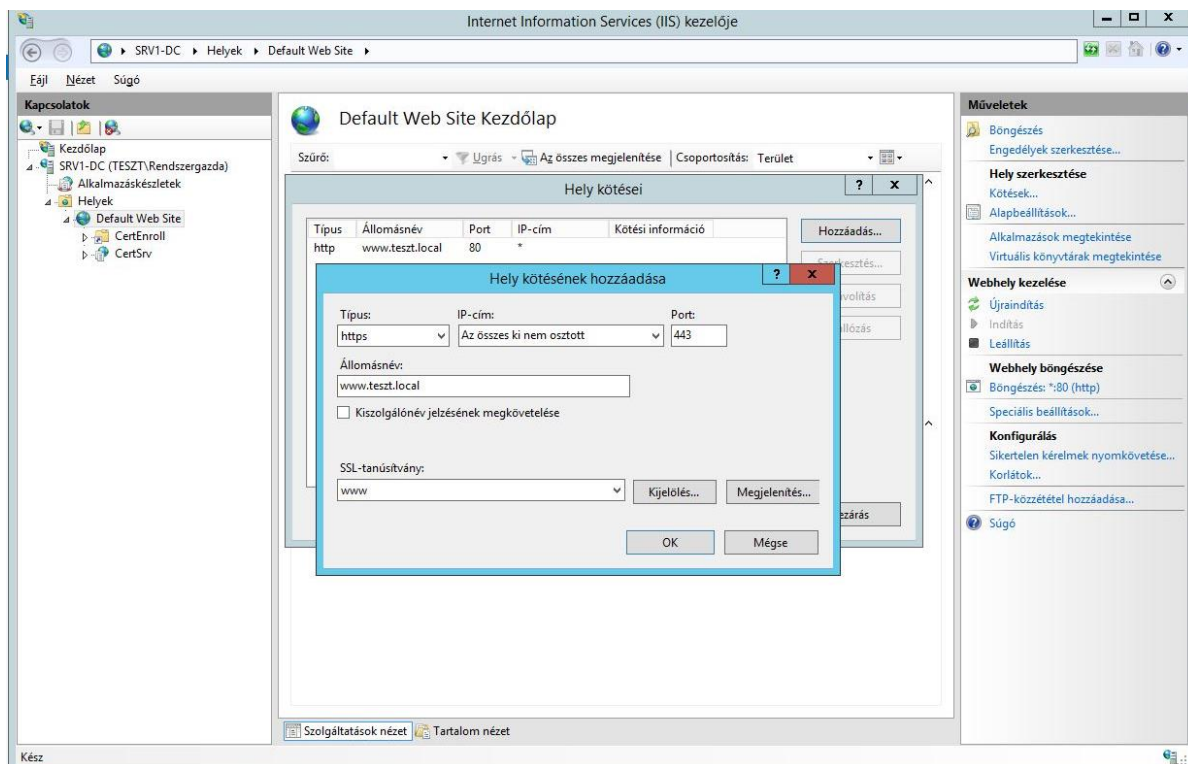
Műveletek

Importálás...  
Tanúsítványkérelem létrehozása...  
Tanúsítványkérelem kitöltése...  
Tartományi tanúsítvány létrehozása...  
Ónaláírt tanúsítvány létrehozása...  
Megújított tanúsítvány automatikus újrakötésének engedélyezése

Súgó

Kész

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 gombra kattintva megnézhetjük a tanúsítványunkat, a harmadik fülön pedig a Tanúsítvány-láncot, hogy milyen hierarchiába épülnek fel. Végül az **OK** gombra kattintunk.



Kitérőként:

Ameddig most elérkeztünk, megoldható, hogy a **HTTPS** protokoll is működik a megfelelő portszámmal, de emellett 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.

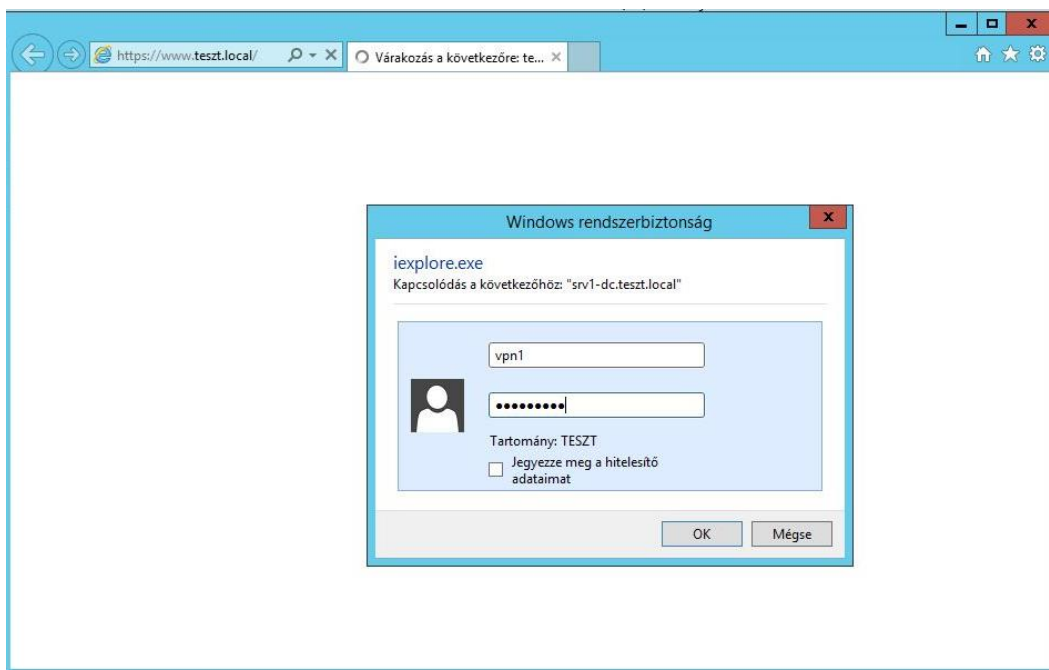
Az SSL beállításával a kliensek honlap elérését korlátozhatjuk és megakadályozhatjuk a **80**-as port használatát. Állítsuk be az SSL-t: kattintsunk az SSL-beállítás fülre, és pipáljuk be a SSL – megkövetelését, majd jobb oldali sávban az alkalmaz gombra kattintva érvényesítsük a beállításunkat.

A probléma most következik, a **443**-as porton továbbra is elérjük a weblapunkat, de a 80-as portra hibalapot ad ki. Megoldás: Hiba lapoknál vegyünk fel egyéni hibalapot. (hibakód száma: 403.4)

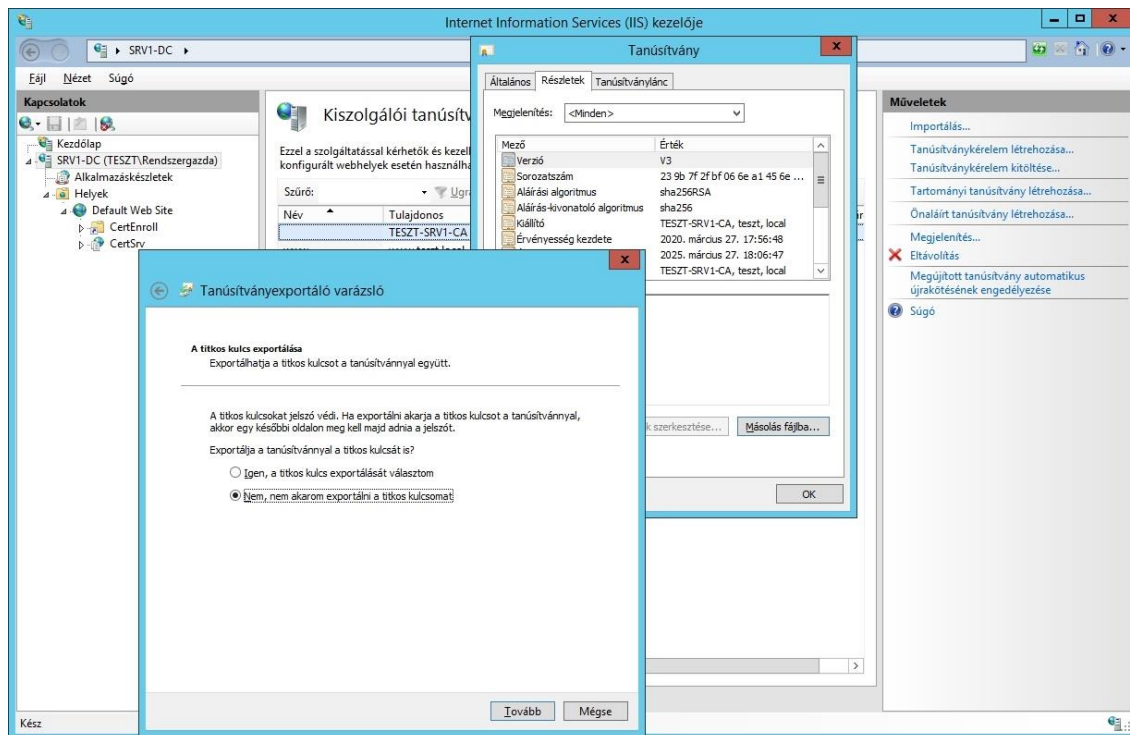
A következőkben korlátozzuk le, hogy ki érhesse el a weblapunkat. Ezt az IIS szerepkörében -tartományi felhasználók esetén- a **Windows-hitelesítés** nevű szerepkör-szolgáltatás használatával végezzük el.



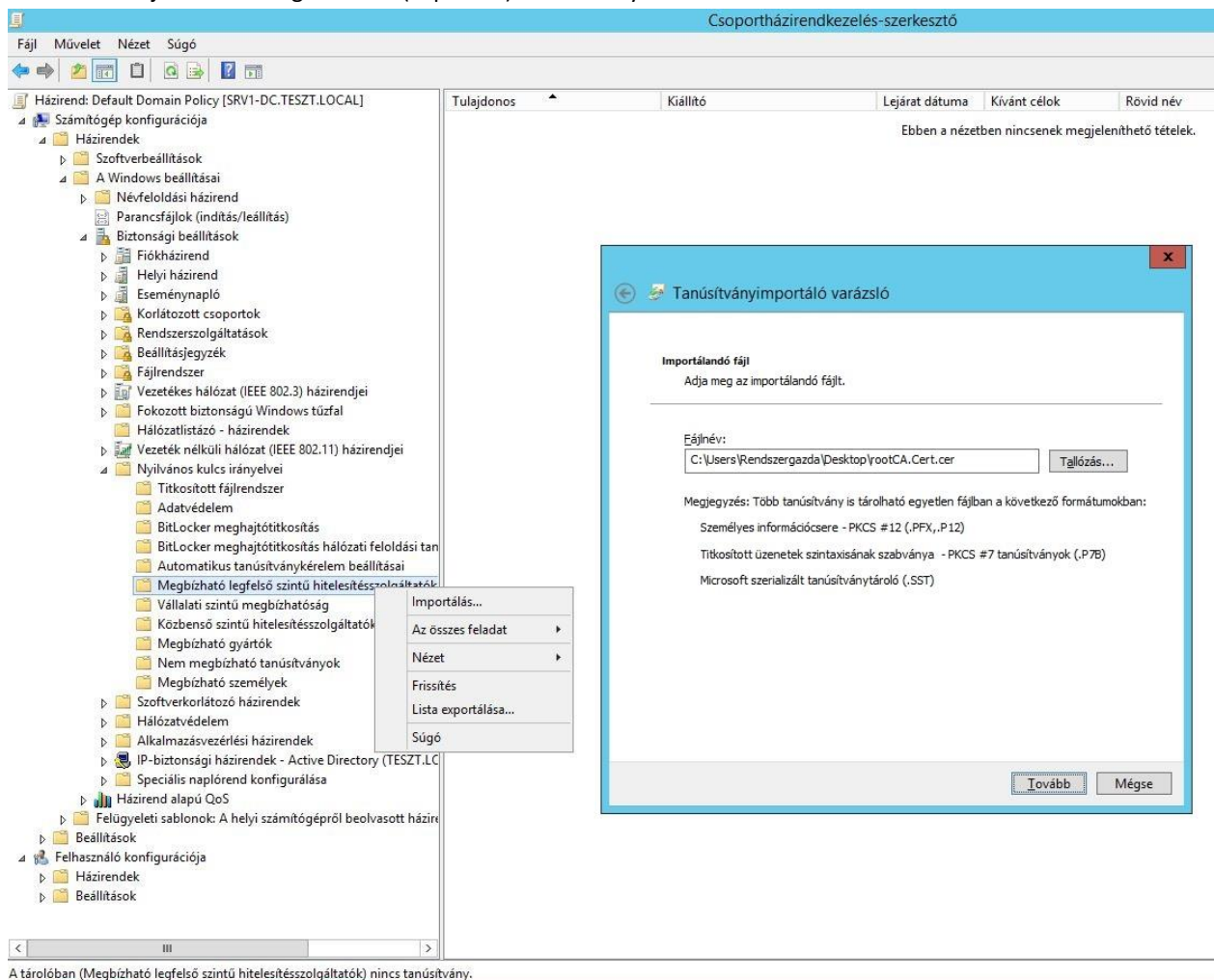
A beállítás után teszteljük a szerverről a belépést, a webhely indítása után írjuk be a megfelelő felhasználónév és jelszó párost, ha beenged akkor sikerült, ha nem akkor nézzük át a beállításokat. Teszteljük úgyis, hogy belépésre nem jogosult felhasználót adunk meg.



A végül érjük el, hogy a Window10 kliensen ne kelljen külön letölteni a tanúsítványt, hanem azonnal megkapja. Ezt csoportházirendben állíthatjuk be, és itt beállítjuk még a megfelelő portok engedélyezését is. Először az IIS-ben az általunk létrehozott tanúsítványt kiexportáljuk. Megjelenítés után a részletek fülnél az alsó sarokban kiválasztjuk a „**Másolás fájlba...**” menüpontot, nem állítjuk át az alapértelmezéseket. (Az asztalra mentjük!)



Ezután a csoportházirendben kiválasztjuk a megfelelő menüpontot. A *számítógép konfigurációjában, Windows beállítások, Biztonsági beállítások, Nyilvános kulcs irányelvei* majd a *Megbízható legfelső szintű hitelesítésszolgáltatónál* importálást választunk. Kiválasztjuk az előzőleg letöltött (exportált) tanúsítványt.



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

Új bejövő szabály varázsló

X

Protokoll és portok

Adja meg azokat a protokollokat és portokat, amelyekre a szabály vonatkozik.

Lépések:

Szabály típusa

Program

Protokoll és portok

Hatókör

Művelet

Profil

Név

Mely portokra és protokollokra vonatkozik a szabály?

Protokolltípus:

TCP

Protokollszám:

6

Helyi port:

Adott portok

80,4400

Példa: 80, 443, 5000-5010

Távoli port:

Minden port

Példa: 80, 443, 5000-5010

ICMP-beállítások:

Testreszabás...

Itt 4400-as port szerepel a képen, de a leírás eddigi értékeit követve ez helyesen: 443!

< Vissza

Tovább >

Mégse

Indítsuk el a **Windows 10** virtuális számítógépet. Léptessük be a tartományba (**teszt.local**).

A tűzfal indítása után ellenőrizhetjük, hogy megkapta-e a tűzfal a beállításokat. (Figyeljünk arra, hogy rendszergazdaként indítsuk).

Végül a webhely elérhetőségét mind a **443**-as mind a **80**-as porttal is. (**80**-as portnál a webhely átirányítását teszteljük).