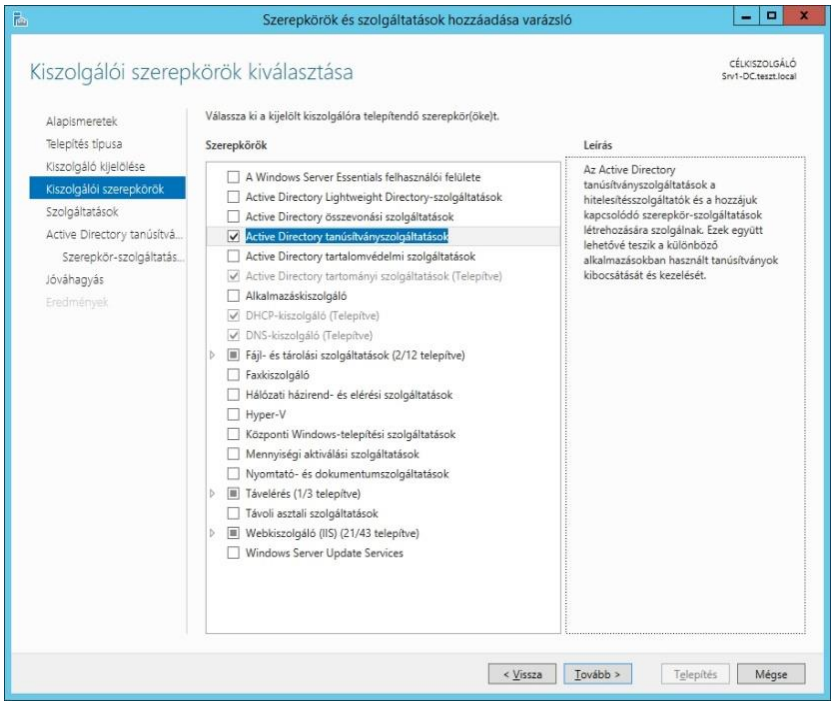
SSL tanúsítvány kérése AD-ban

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 bemelegítésképpen van most benne a leírásban.

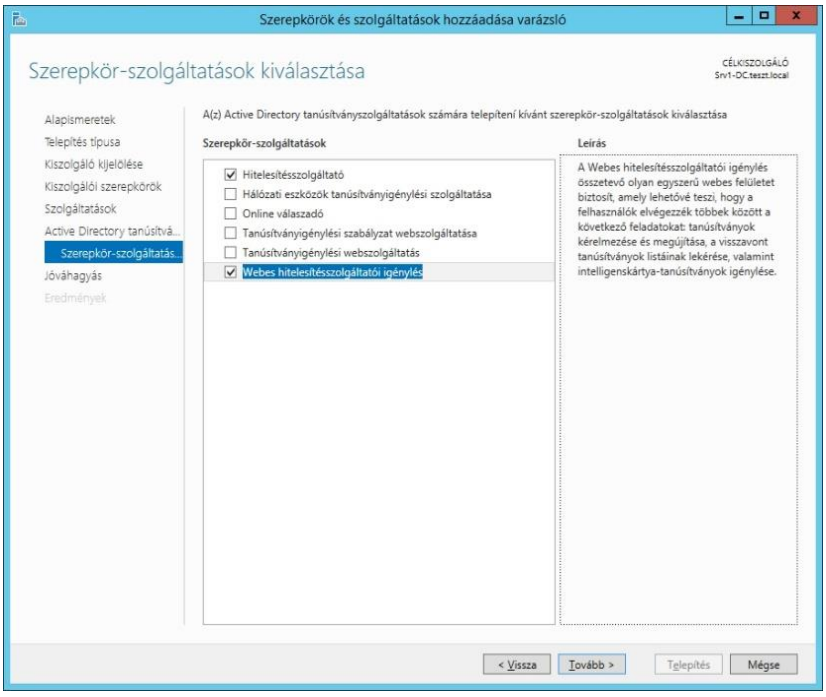
Weblapok biztonságos eléréséhez szükség van SSL tanúsítványra (HTTPS elérés). Ebben a feladatban Active Directory használatával valósítjuk meg a tanúsítvány kérését. Ehhez szükségünk van a megfelelő szerepkörökre.

Tanúsítvány szolgáltatás telepítése

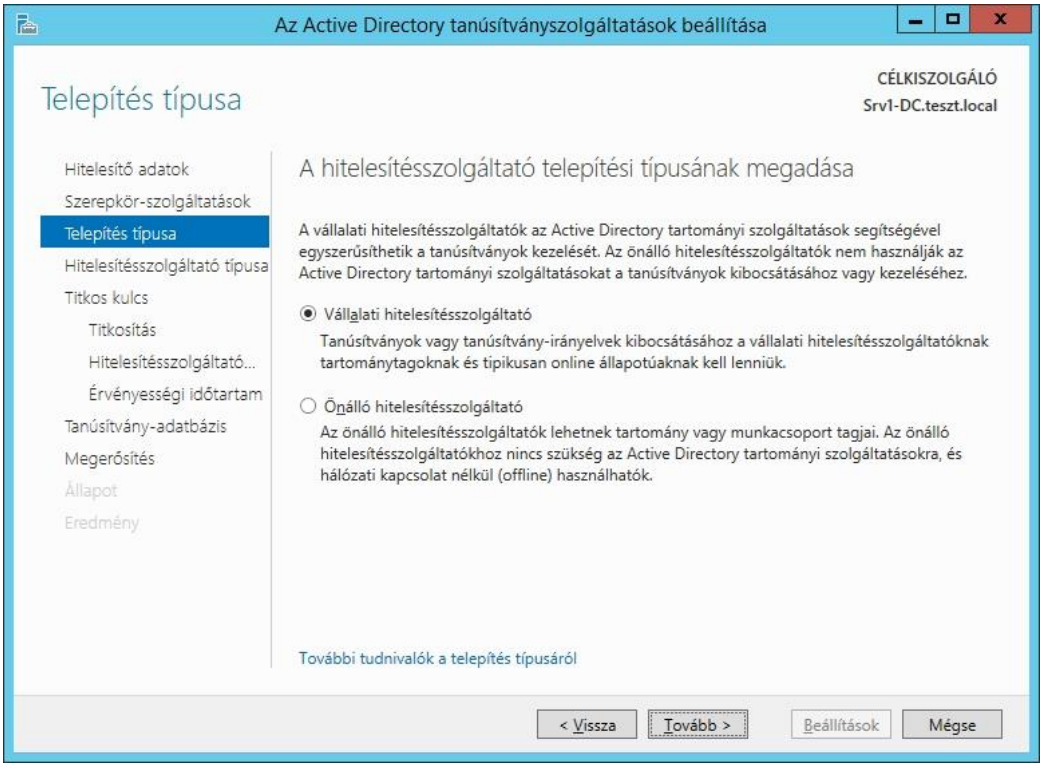
A kiszolgálókezelőben az Active Directory tanúsítványszolgáltatások szerepkört telepítjük.



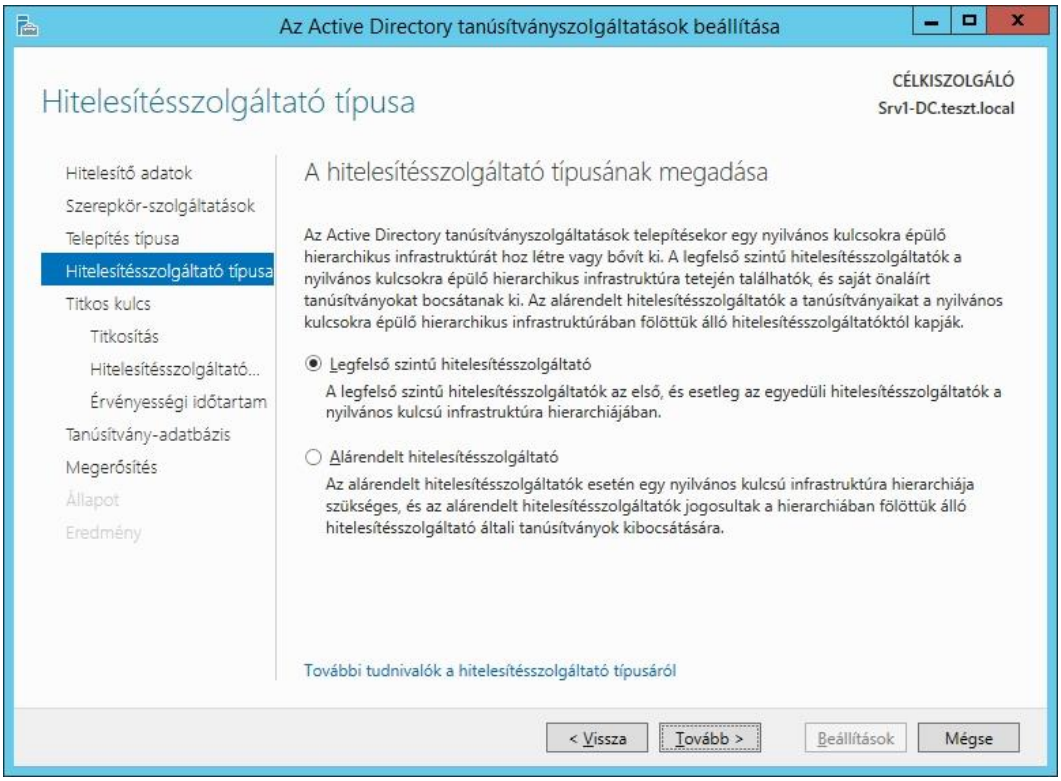
A következő ablakban, kiválasztjuk a telepíteni kívánt szolgáltatásokat itt az első kettőt jelöljük be. A második pont bejelölése után a felugró ablakban az IIS telepítését fogadjuk el és kattintsuk a tovább gombra.



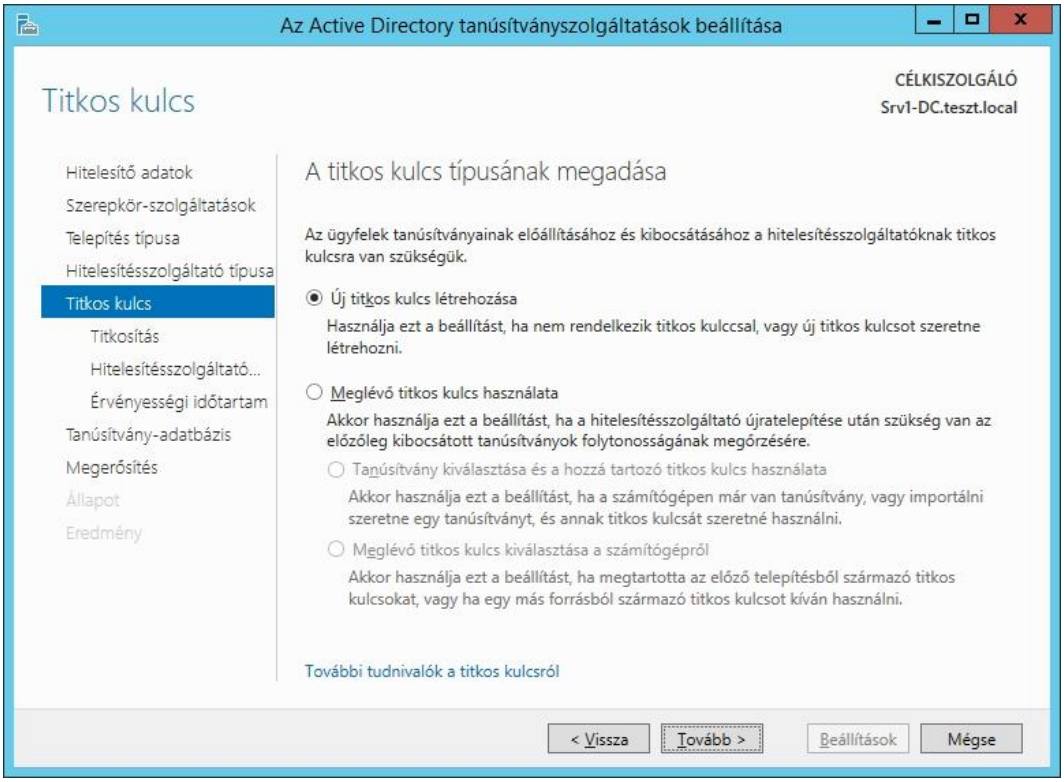
A telepítés típusánál a Vállalat szintű beállítást választjuk, ezt csak tartományi tagként tehetjük meg, és mivel a feladat az AD-ban való tanúsítványszolgáltatásról szól, ezt választjuk.



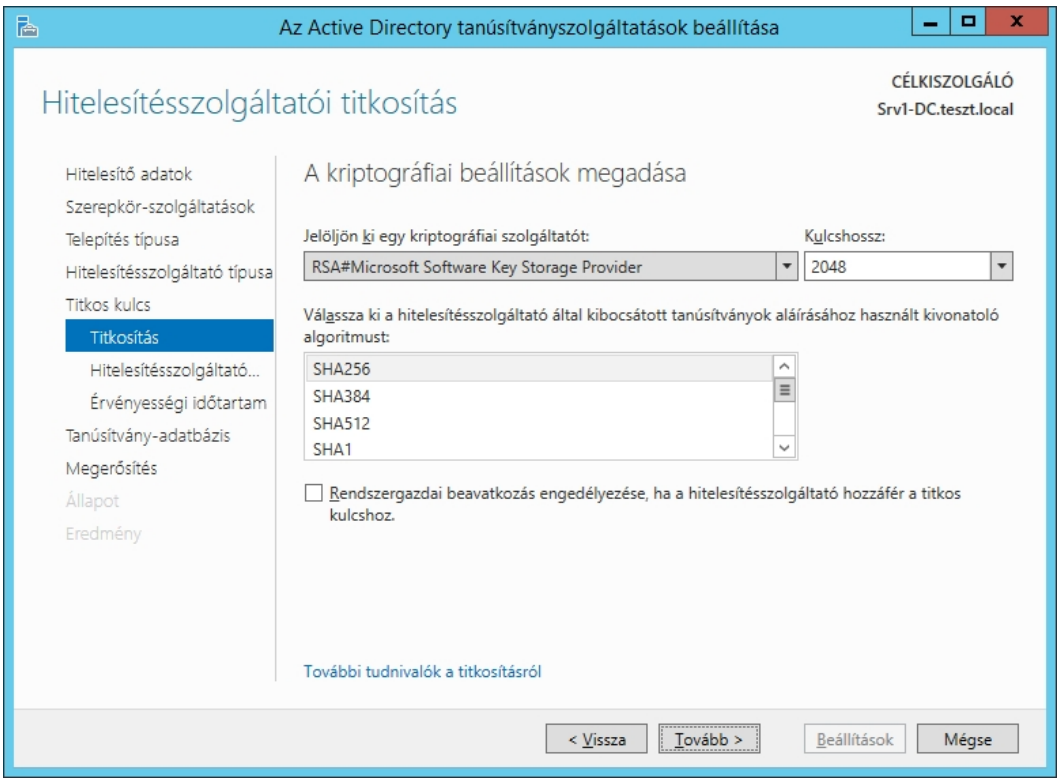
A következő pontban a legfelső szintű szolgáltatást választjuk.

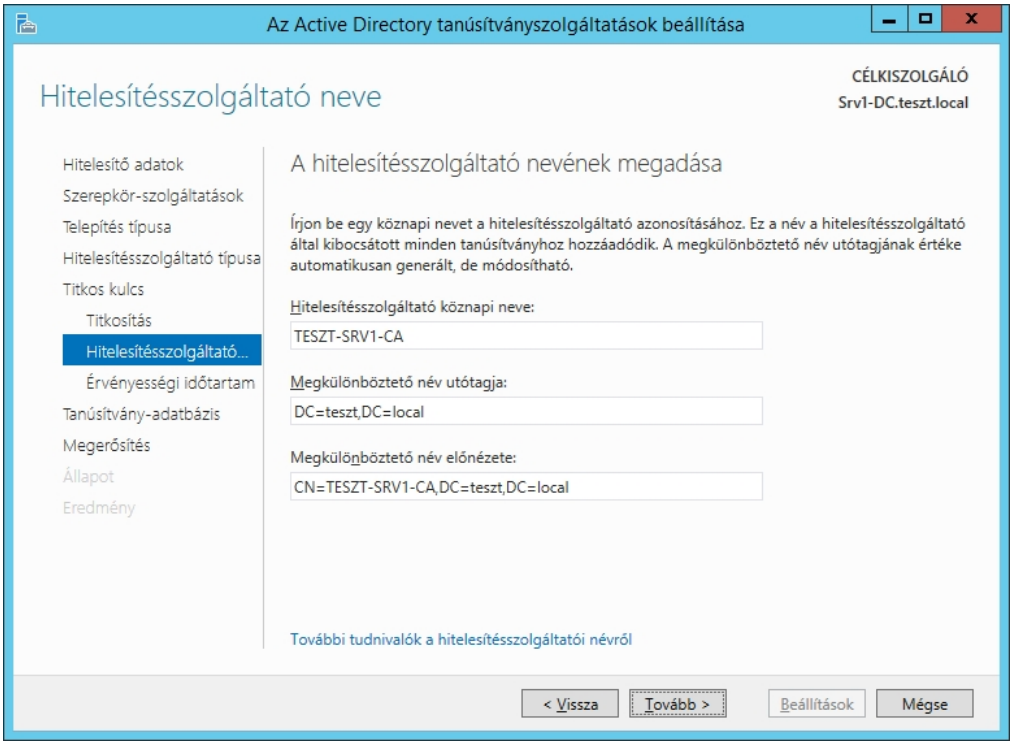


A tanúsítványokhoz szükség van egy kulcs létrehozására és mivel most telepítünk elsőnek tanúsítványszolgáltatást, nincs létező kulcsunk, újat kell létrehoznunk

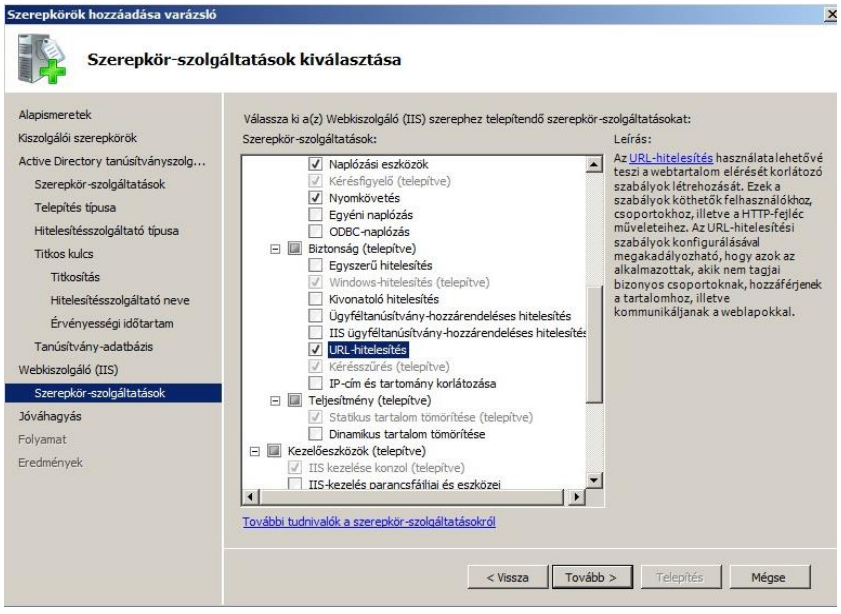


A következő pontban a titkosítást választjuk, rengeteg féle közül lehet válogatni. Mi az RSA kriptográfiát választjuk, SHA256-os hash algoritmussal és 2048-es kulcshosszal. A következő pár pontban nem kell semmit se változtatni azokat az alapbeállításokon hagyjuk.





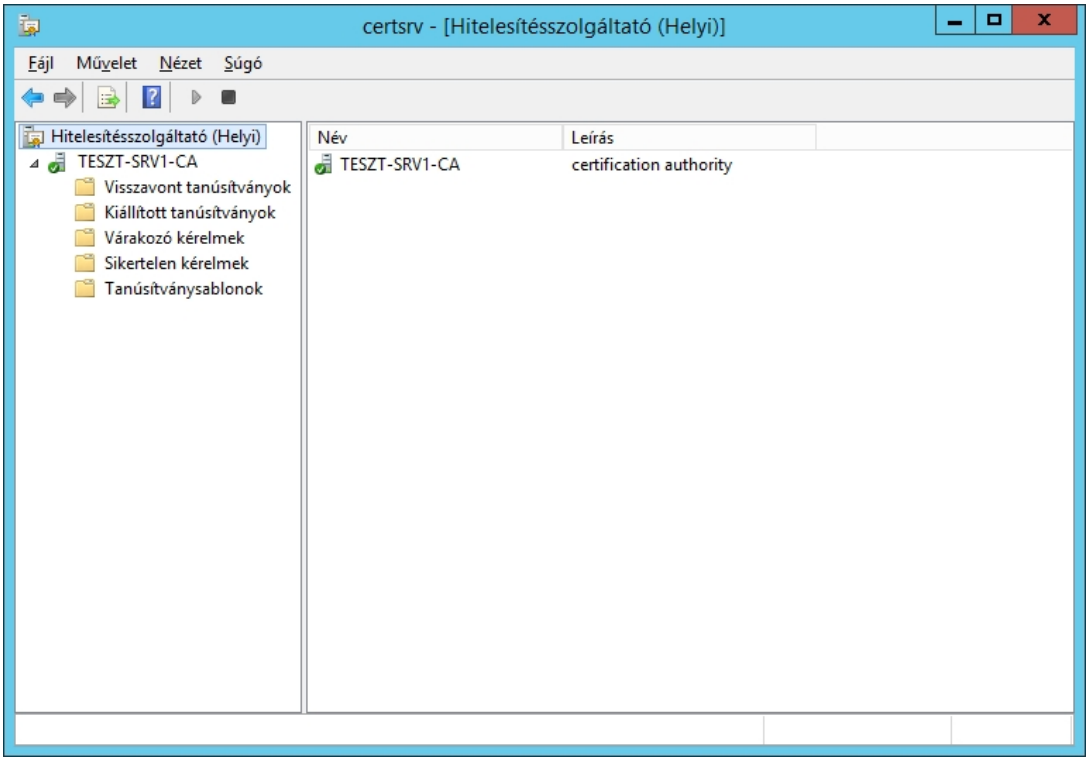
A következő beállítást az IIS-nél végezzük, ha nem volt telepítve, az URL-hitelesítést adjuk hozzá. Ezzel a szerepkör-szolgáltatással korlátozhatjuk, hogy ki érje el a honlapot és ki nem a megfelelő felhasználónév/jelszó párossal.



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

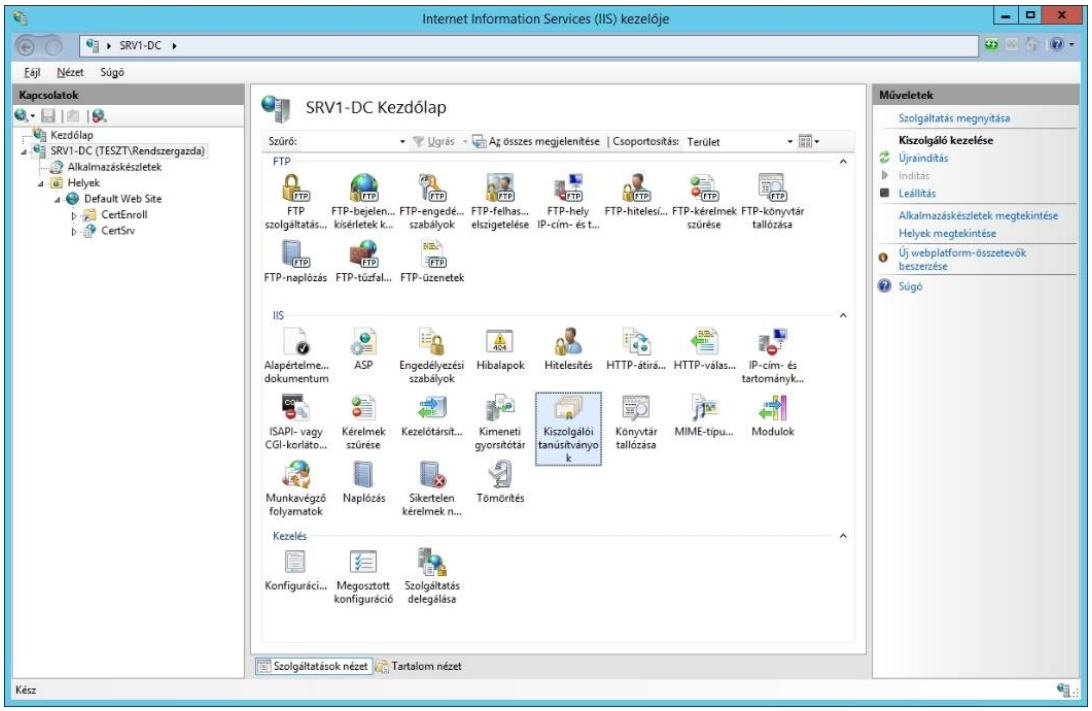
A felügyeleti eszközökben megtalálhatjuk a tanúsítványszolgáltatót, valamilyen oknál fogva ezt a nevet nem fordították le magyarra.

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

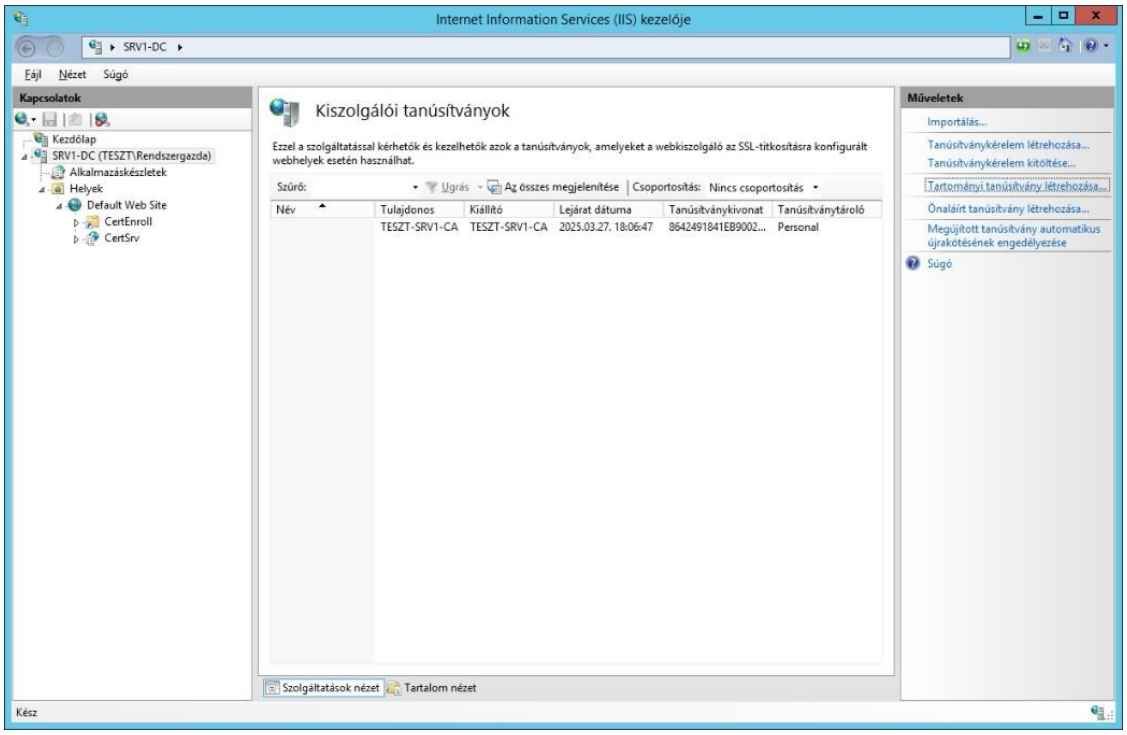


Biztonságos webhely kialakítása

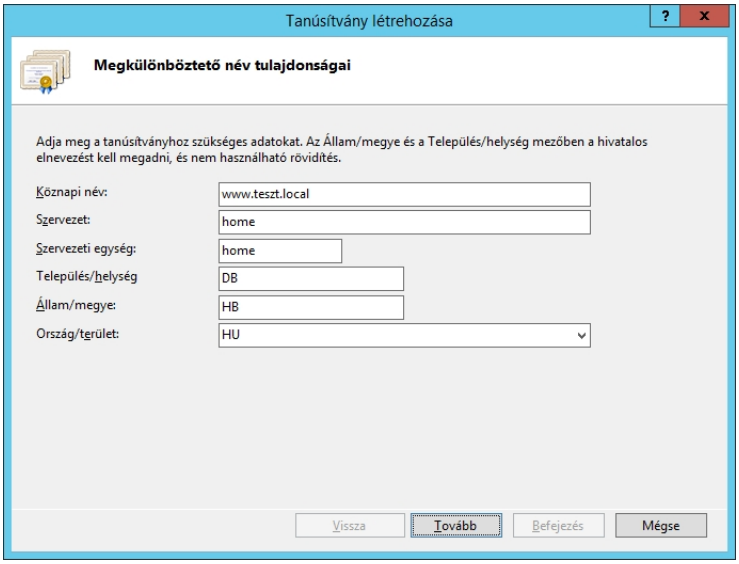
Az alapértelmezett webhelyet fogjuk használni (Default Web Site). Előtte a webkiszolgálónak egy tanúsítványt kell igényelnünk. Első lépésként a legfelső (szerver) szinten a kiszolgálói tanúsítványok beállítás menüjébe lépünk.



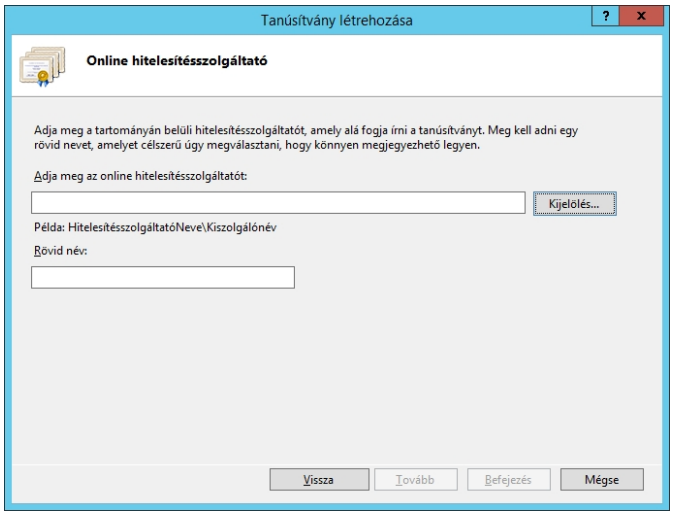
Itt jobb oldalt a műveleteknél kiválasztjuk a **Tartományi tanúsítvány létrehozását**.

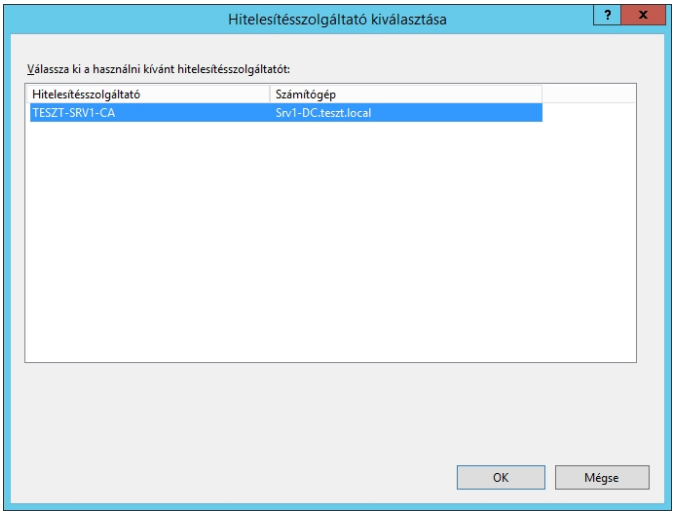


A felugró ablakban megkell adnunk az adatainkat. Az első helyre adjuk meg a tanúsítvány **Köznapi nevét** *(ahogyan a kötésben is szerepel)*, a többi helyre írunk adatokat „tetszőlegesen”, kivétel az utolsó pont, oda a „**HU**”-t írjunk.

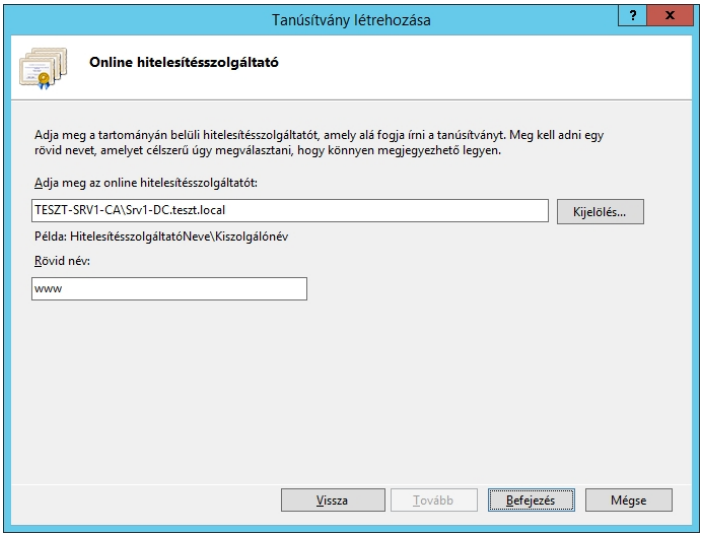


A tovább gombra kattintva ki kell választanunk a hitelesítési szolgáltatót: ez a mi szerverünk, a kijelölés gombra kattintva kiválasztjuk a szolgáltatót.

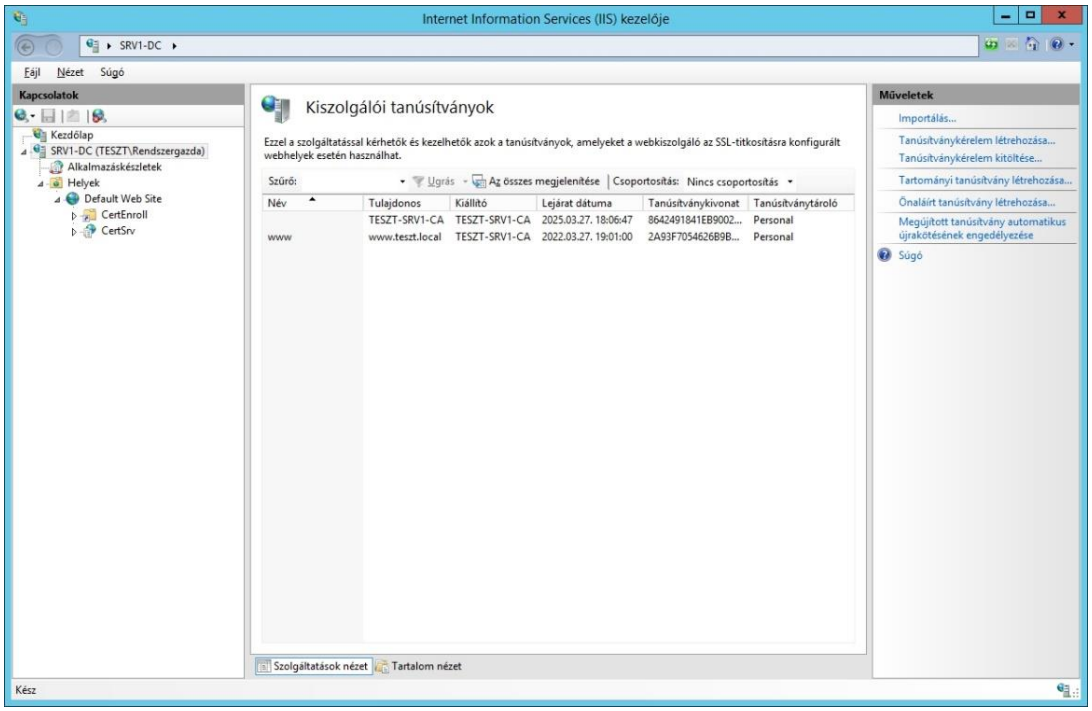




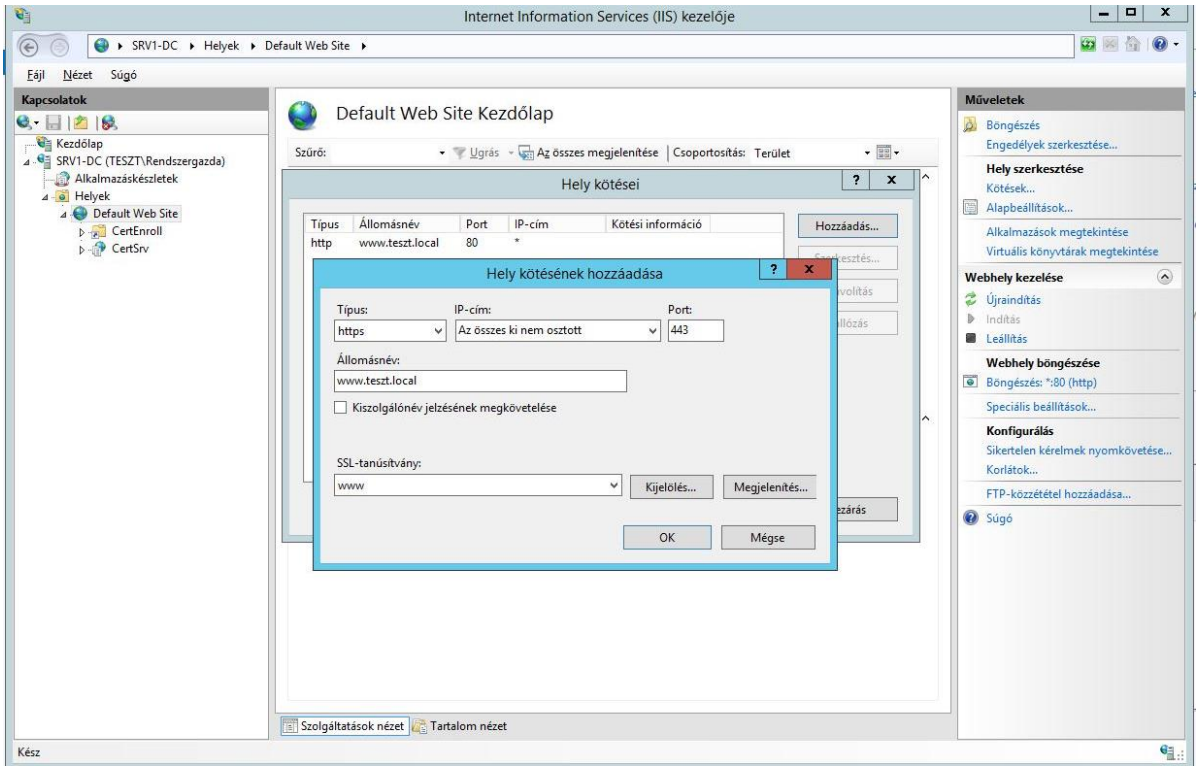
A rövid névhez „**www**” kifejezést írjuk. Majd a **Befejezés** gombra kattintunk.



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



Az alapértelmezett webhelynél vegyünk fel egy új kötést, HTTPS kapcsolattal és a **443** porttal. A típus kiválasztása után az állomásnév beszürkül 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.



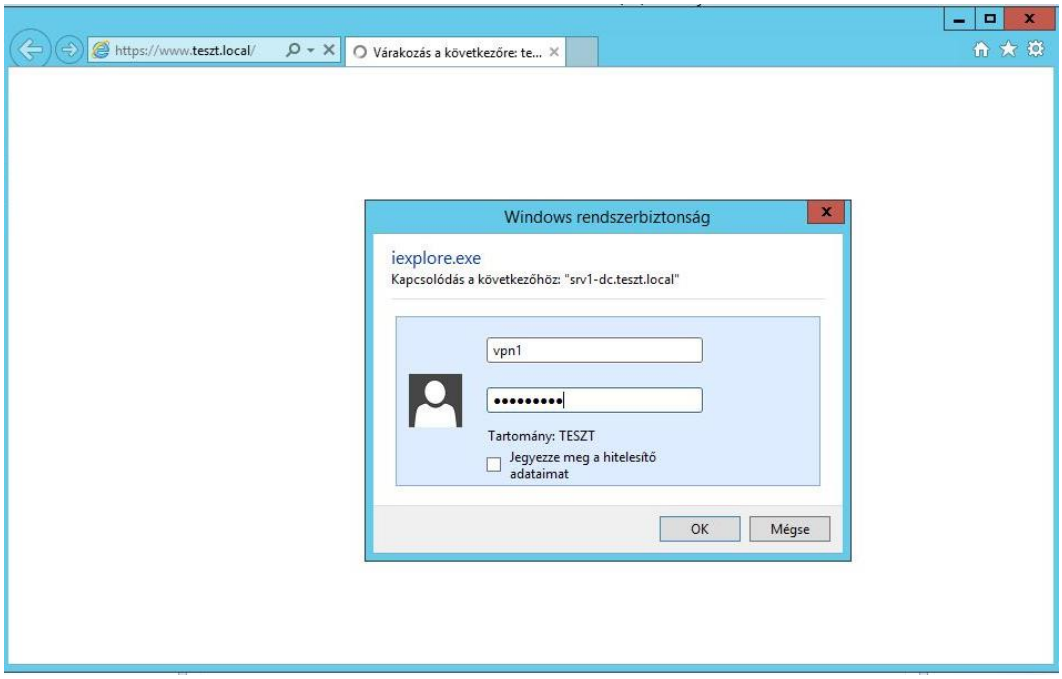
Kitérésként:
Ameddig most elérkeztünk, megoldható, hogy a **HTTPS** protokoll is működik a megfelelő portszámmal, de emellett a **80**-as alapértelmezett port is működik, ez így nem mindig a legbiztonságosabb és a legelőnyösebb, ezért a **80**-as portot vagy letiltják vagy átirányítják.

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 kattinva érvényesítsük a beállításunkat.

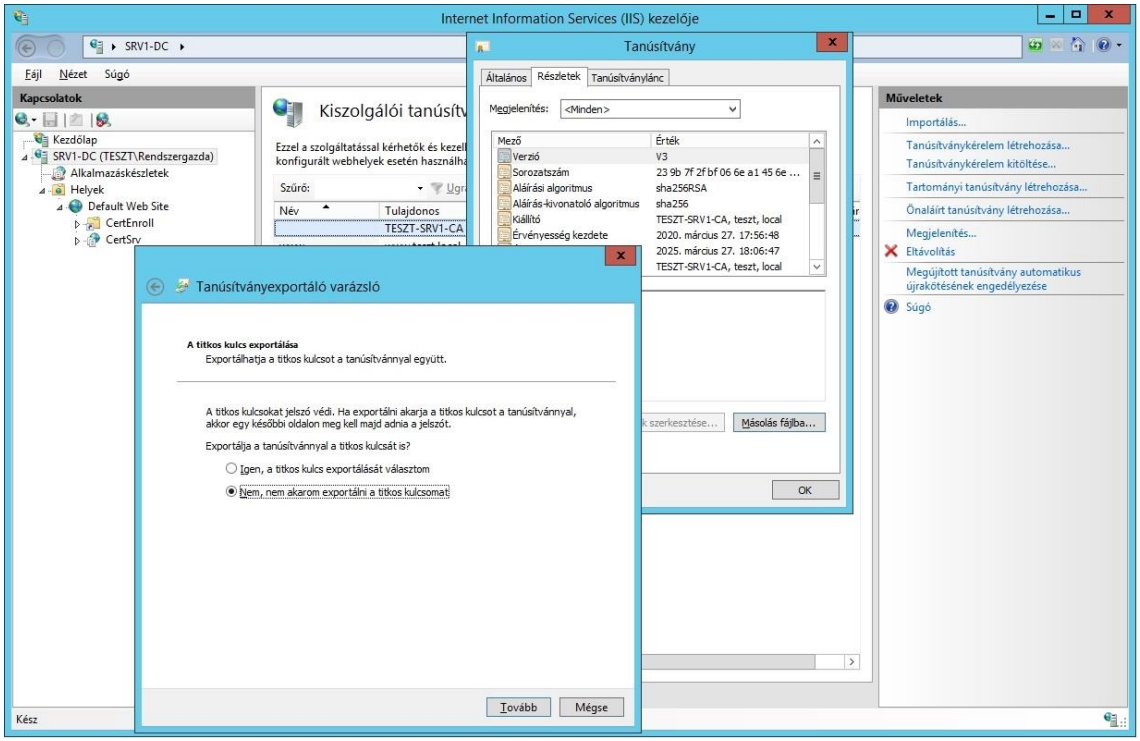
A probléma most következik, a **443**-as porton továbbra is elérjük a weblapunkat, de a 80-as portra hibalapot ad ki. Megoldás: Hiba lapoknál vegyünk fel egyéni hibalapot. (hibakód száma: 403.4)

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.

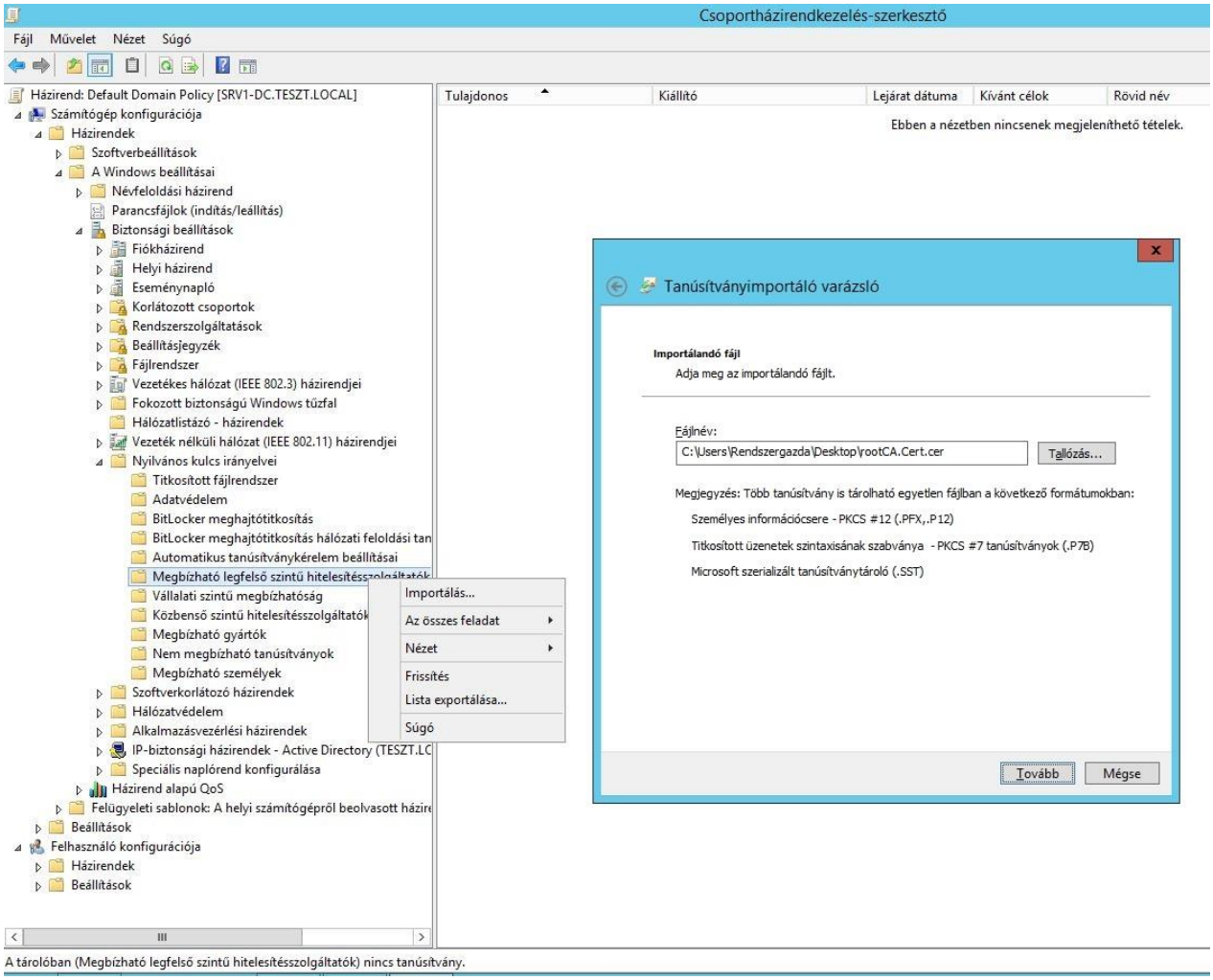
A beállítás után teszteljük a szerverről a belépést, a webhely indítása után írjuk be a megfelelő felhasználónév és jelszó párost, ha beenged akkor sikerült, ha nem akkor nézzük át a beállításokat. Teszteljük úgyis, hogy belépésre nem jogosult felhasználót adunk meg.



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 aztán a részletek fülnél az alsó sarokban kiválasztjuk a „**Másolás fájlba…**” menüpontot, nem állítjuk át az alapértelmezéseket. (Az asztalra mentjük!)

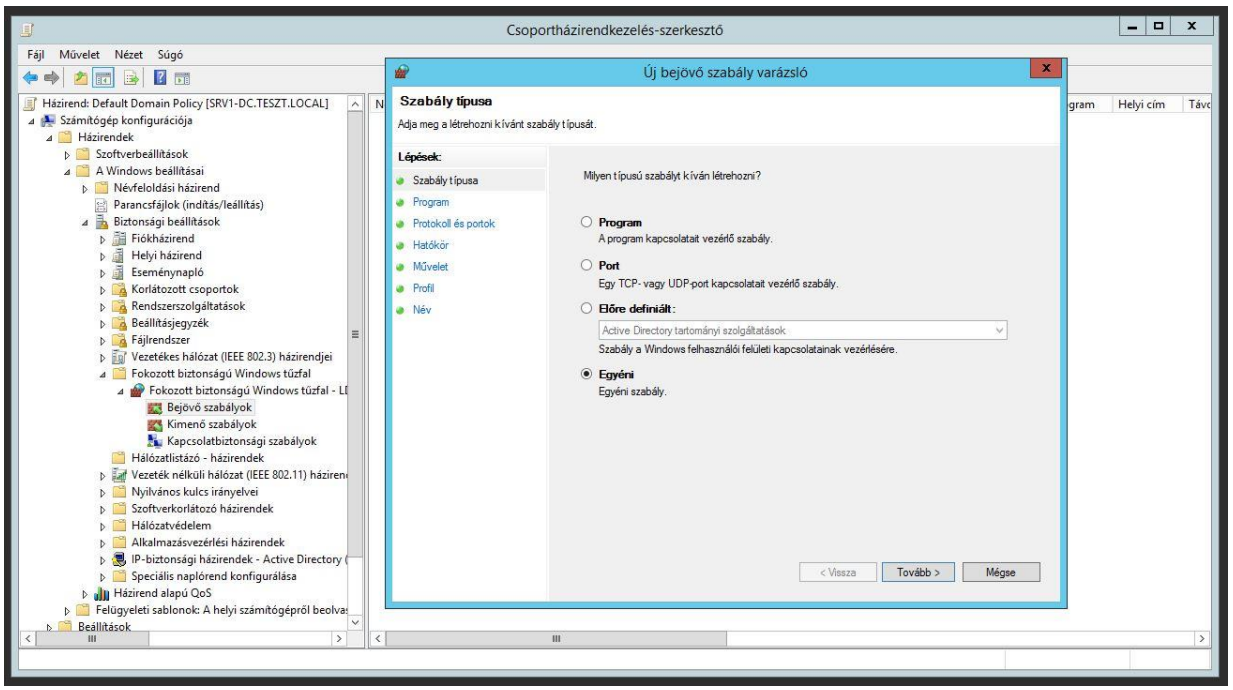


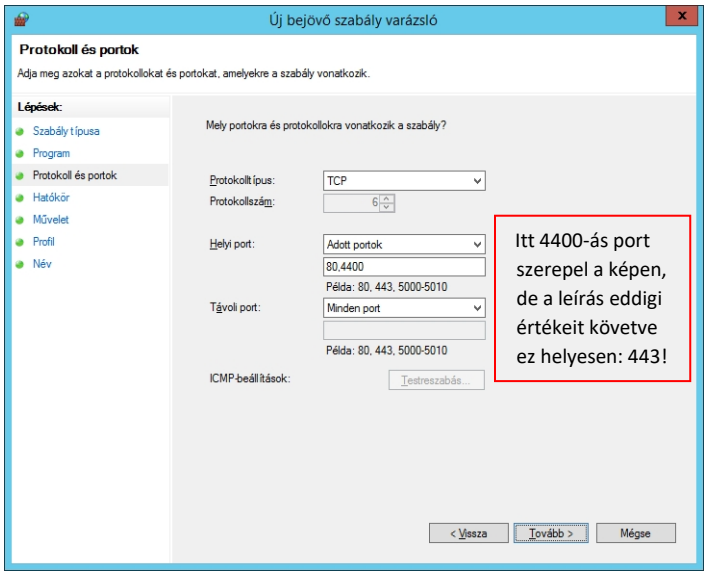
Ezután a csoportházirendben kiválasztjuk a megfelelő menüpontot. A *számítógép konfigurációjában*, *Windows beállítások*, *Biztonsági beállítások*, *Nyilvános kulcs irányelvei* majd a *Megbízható legfelső szintű hitelesítésszolgáltatónál* importálást választunk. Kiválasztjuk az előzőleg letöltött (exportált)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



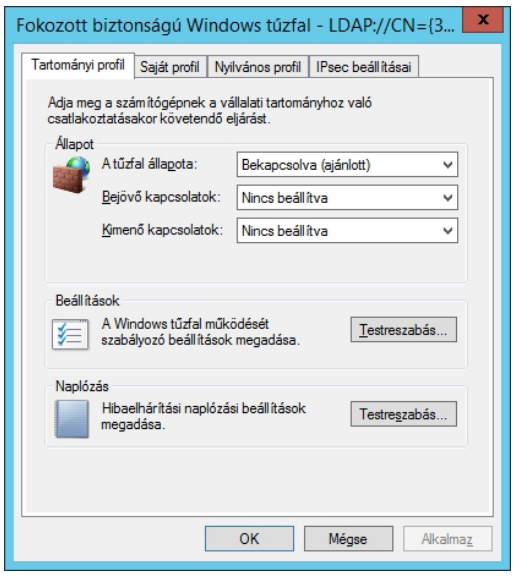
Ezzel elértük, hogy a tartományi számítógép minden beállítás nélkül letöltse a tanúsítványt.

A következő beállítást is a csoportházirendben kell elvégeznünk. Szintén a Windows beállításoknál vagyunk és válasszuk ki a Fokozott biztonságú Windows tűzfal beállítást. Nyissunk le minden menüpontot vegyük fel a **80**-as és a **443-**as portokat, és kapcsoljuk be a tűzfalat!





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



A végső, tesztelési fázisba érkeztünk.

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

Ezután lépjünk be valamelyik felhasználóval (*pl.* ***vpn1***).

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

A tanúsítványt is ellenőrizzük. (kis lakat zárva)

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