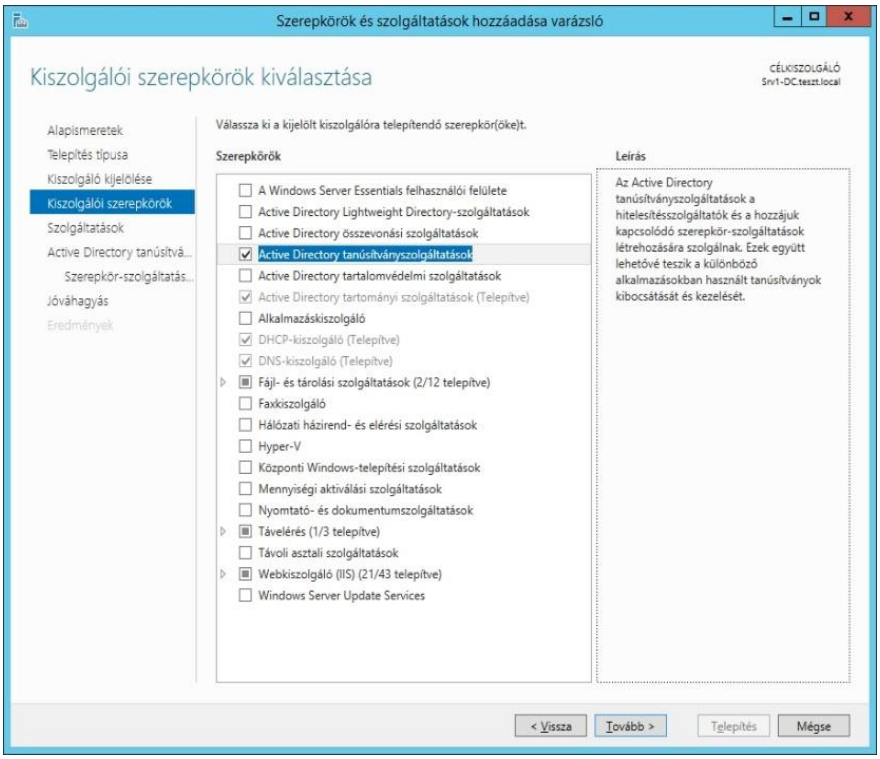
SSL tanúsítvány kérése AD-ban

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.

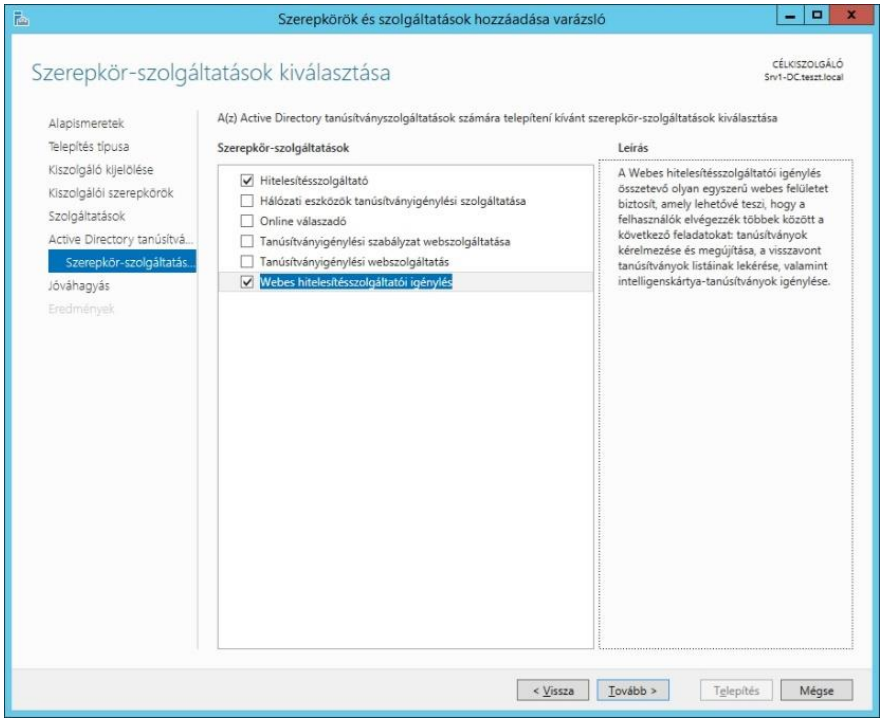
Először is szükségünk van a megfelelő szerepkörökre.

Tanúsítvány szolgáltatás telepítése

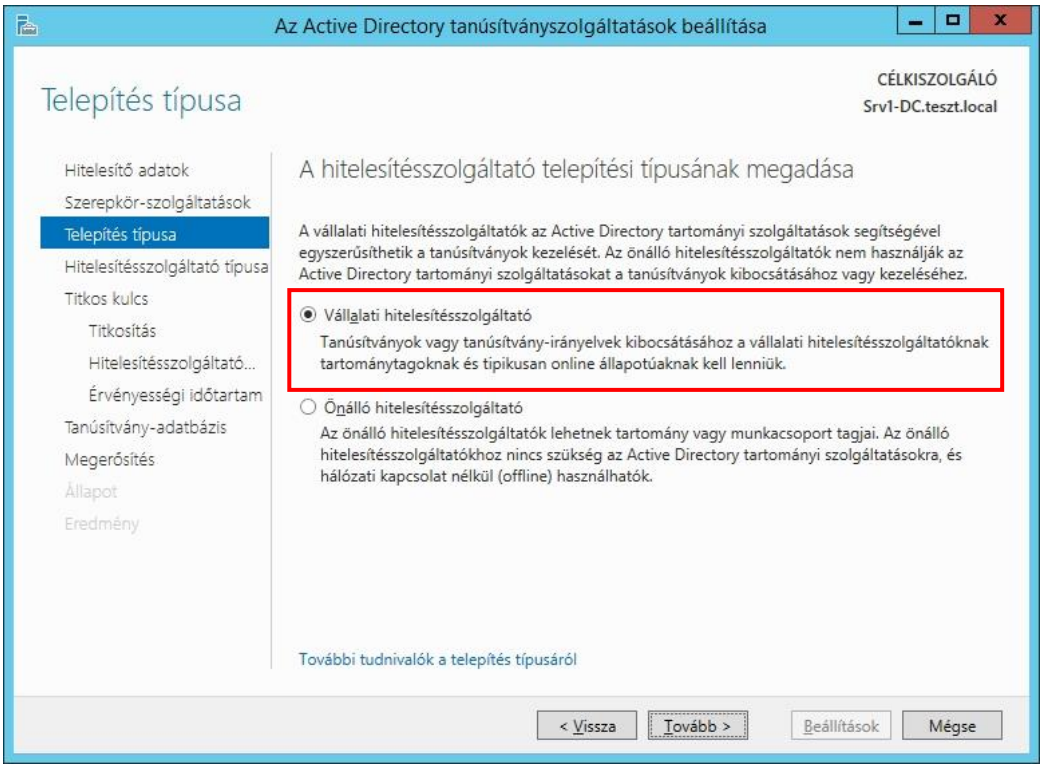
A kiszolgálókezelőben az ***Active Directory tanúsítványszolgáltatások*** szerepkört telepítjük.



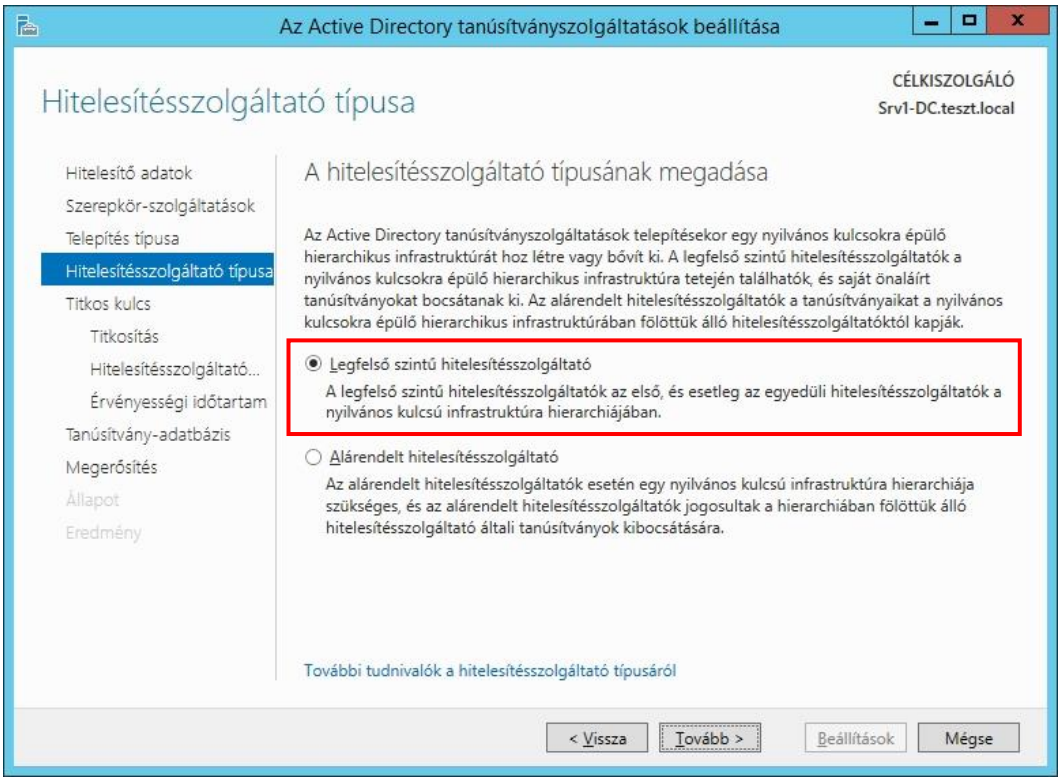
A következő ablakban kiválasztjuk a telepíteni kívánt szolgáltatások közül a ***Hitelesítésszolgáltató*** és a ***Webes hitelesítésszolgáltatói igénylés*** nevű szerepkör-szolgáltatásokat. Kattintsuk a ***Tovább*** gombra.



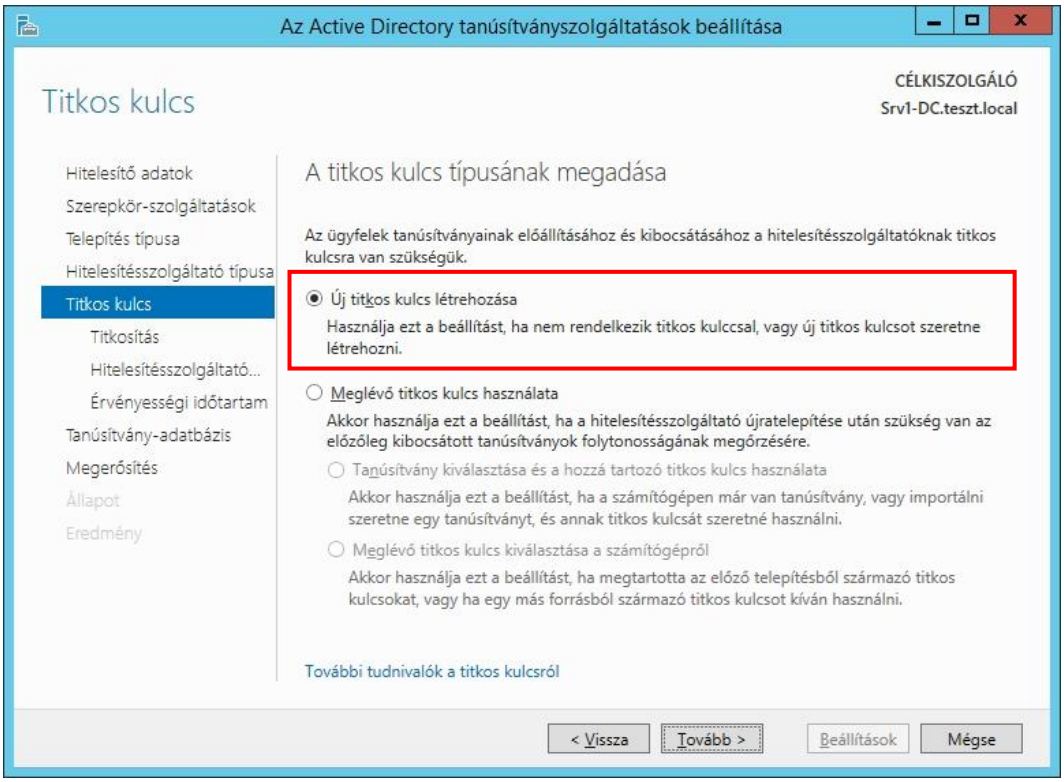
Az Active Directory tanúsítványszolgáltatások konfigurálásakor, a telepítés típusánál a ***Vállalati hitelesítésszolgáltatót*** választjuk, ezt csak tartományi tagként tehetjük meg és mivel a feladat az AD-ban való tanúsítványszolgáltatásról szól, ezt választjuk.



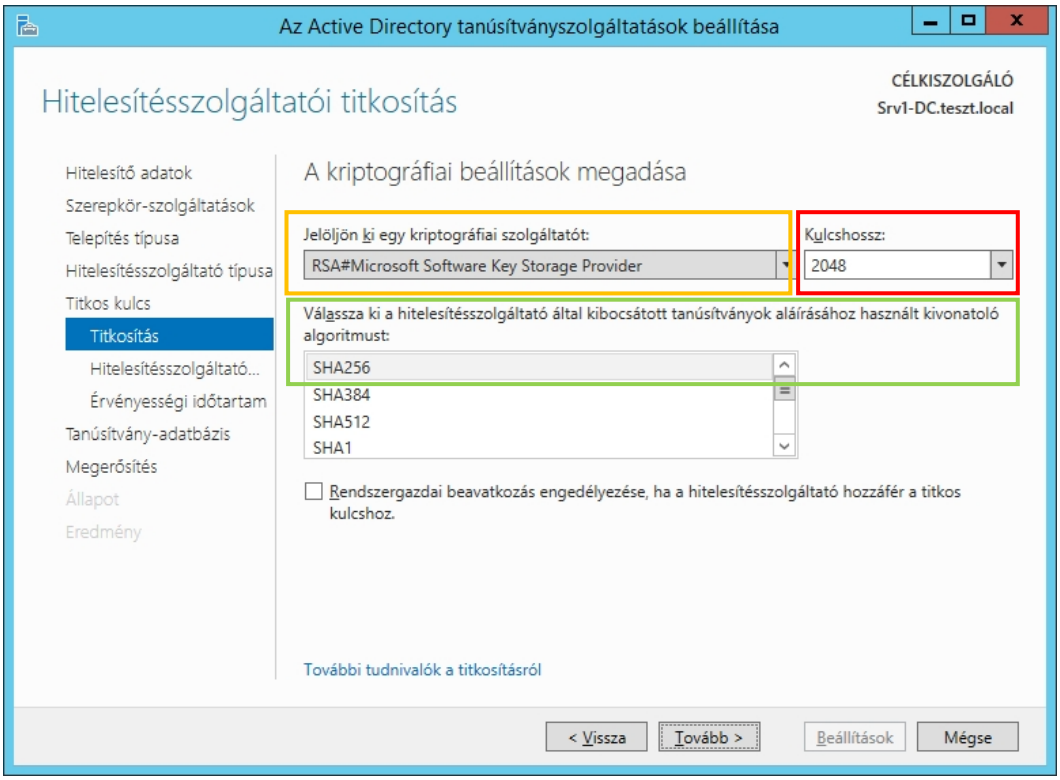
A következő pontban a ***Legfelső szintű hitelesítésszolgáltató***-t választjuk.



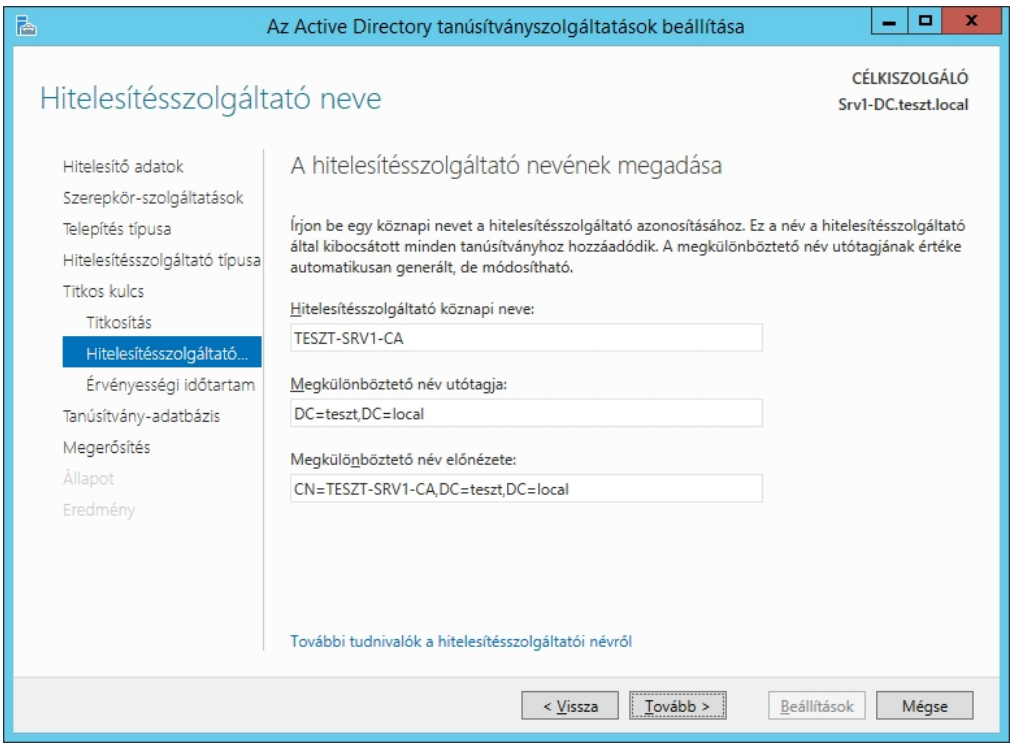
A tanúsítványokhoz szükség van egy kulcs létrehozására és mivel most telepítünk elsőnek tanúsítványszolgáltatást, nincs létező kulcsunk, ***új kulcsot kell létrehoznunk***



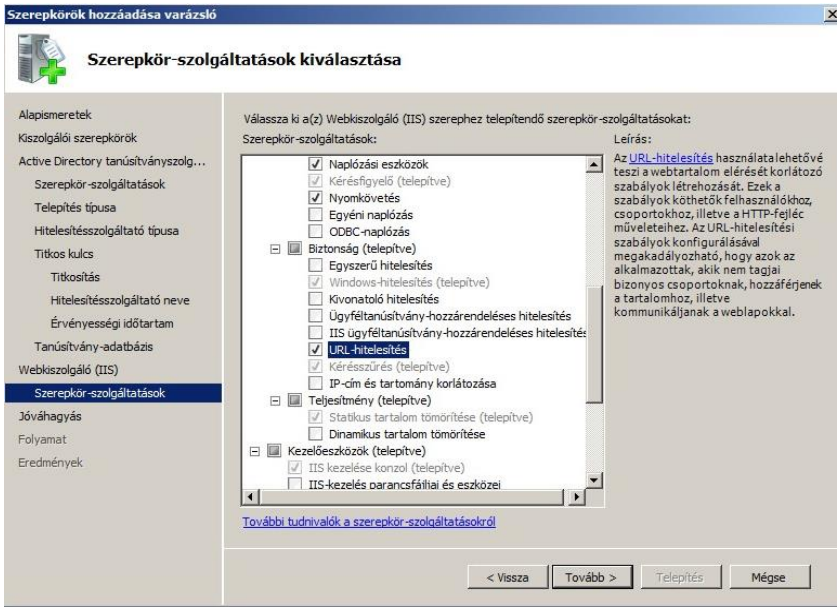
A következő pontban a titkosítást választjuk, rengeteg féle közül lehet válogatni. Mi az ***RSA*** kriptográfiát választjuk, ***SHA256***-os HASH algoritmussal és ***2048-es kulcshosszal***.



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

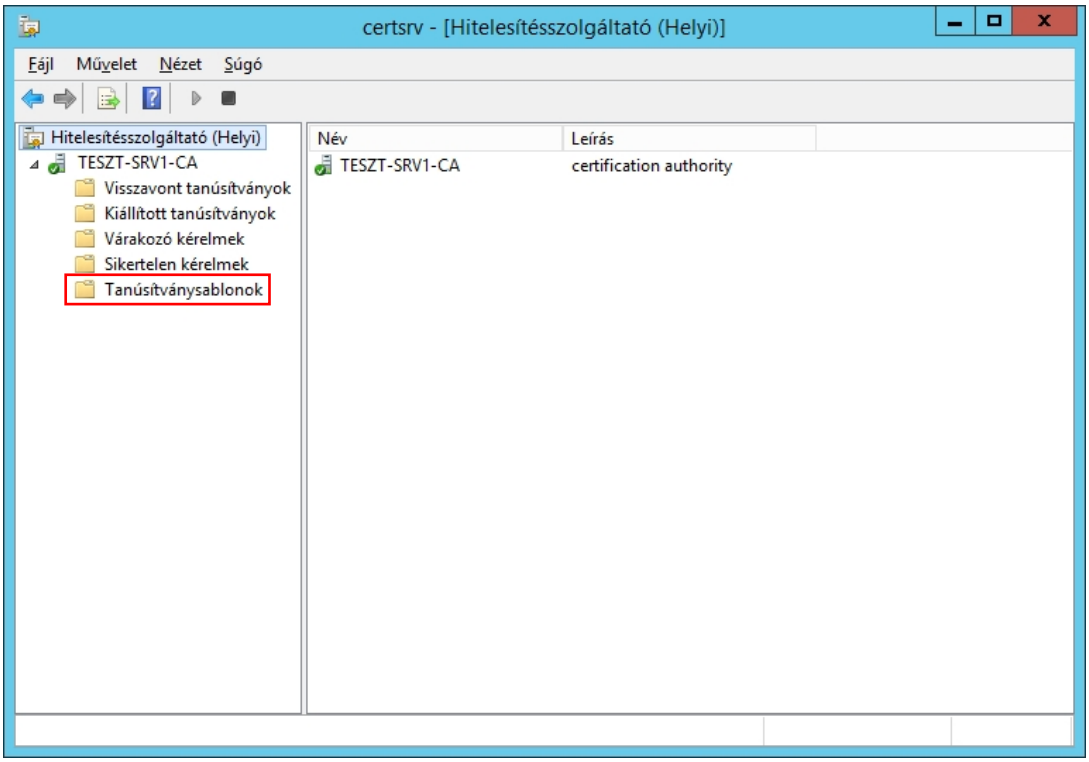


A következő beállítást az IIS-nél végezzük, ha nem volt telepítve, az ***URL-hitelesítést*** adjuk hozzá. Ezzel a szerepkör-szolgáltatással korlátozhatjuk, hogy ki érje el a honlapot (*és ki nem*) a megfelelő felhasználónév/jelszó párossal.



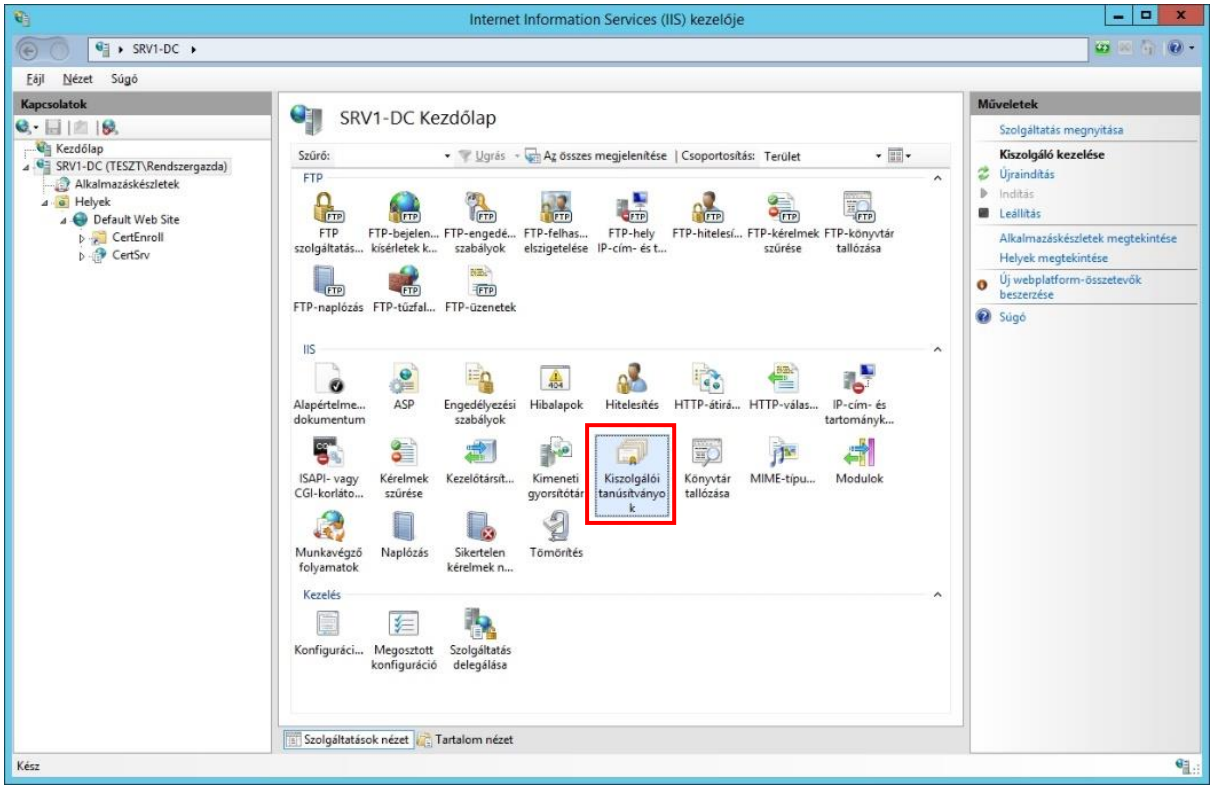
A jóváhagyásnál ellenőrizzük a beállításokat majd telepítsük a szerepköröket. Újraindítás nem szükséges.
A felügyeleti eszközökben megtalálhatjuk a Tanúsítványszolgáltatót, valamilyen oknál fogva ezt a nevet nem fordították le magyarra.

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

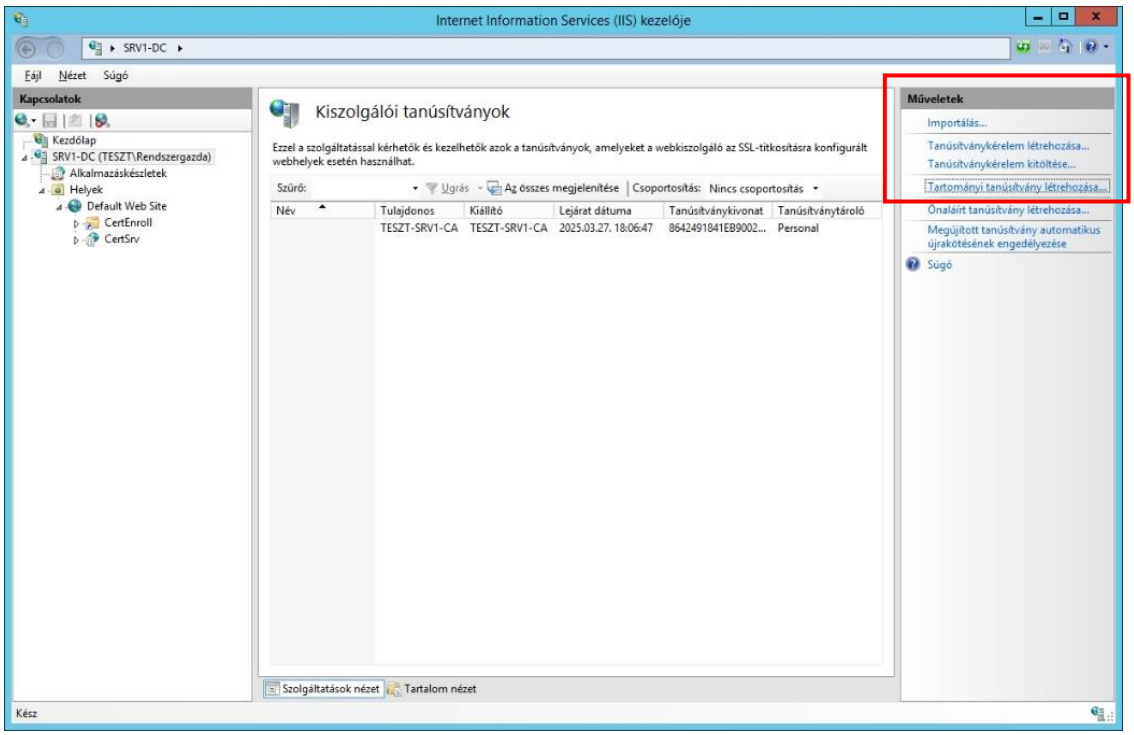


Biztonságos webhely kialakítása

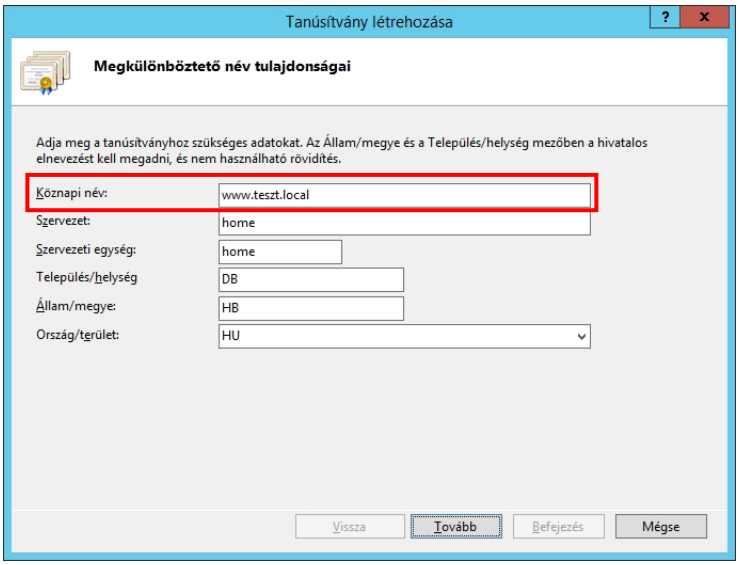
Az alapértelmezett webhelyet fogjuk használni (Default Web Site). Előtte a webkiszolgálónak egy tanúsítványt kell igényelnünk. Első lépésként a legfelső (szerver) szinten a kiszolgálói tanúsítványok beállítás menüjébe lépünk.



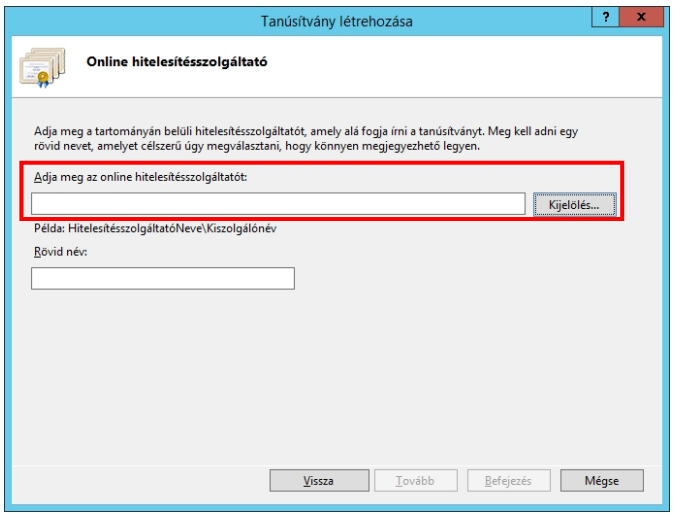
Itt jobb oldalt a műveleteknél kiválasztjuk a **Tartományi tanúsítvány létrehozását**.

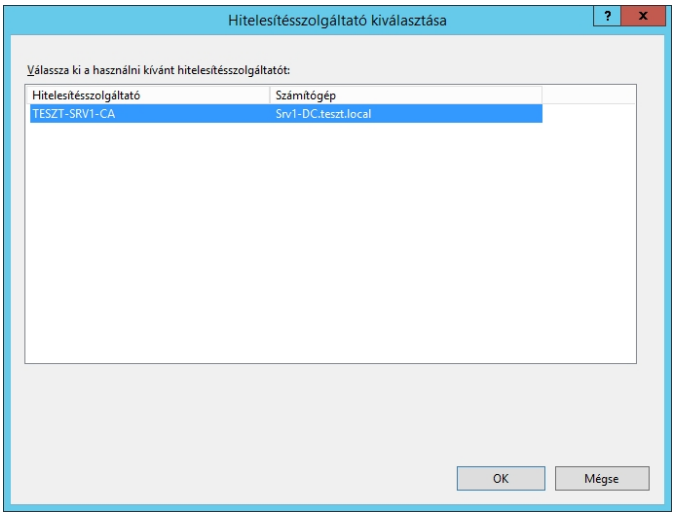


A felugró ablakban megkell adnunk az adatainkat.
Az első helyre adjuk meg a tanúsítvány ***Köznapi nevét*** *(ahogyan a kötésben is szerepel „a webkiszolgálónk neve”)*,
a többi helyre írhatunk adatokat tetszőlegesen, kivétel az utolsó pont, oda a **HU**-t írjunk.

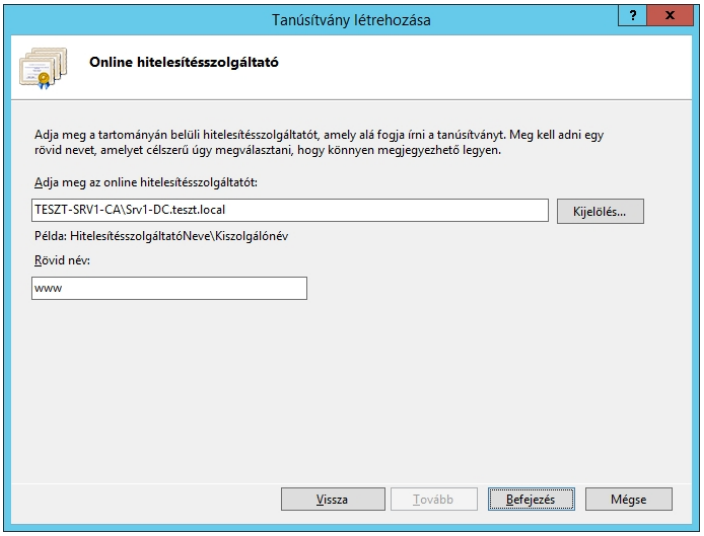


A tovább gombra kattintva ki kell választanunk az ***online hitelesítési szolgáltatót***: ez a mi szerverünk, a ***Kijelölés gombra*** kattintva kiválasztjuk a szolgáltatót.

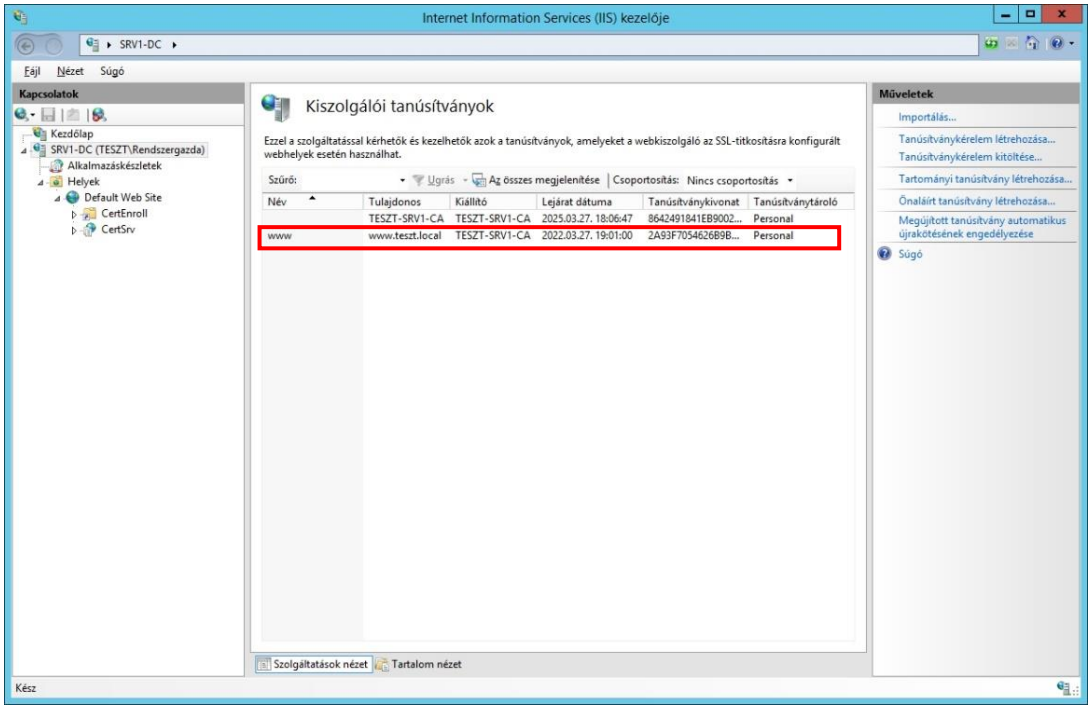




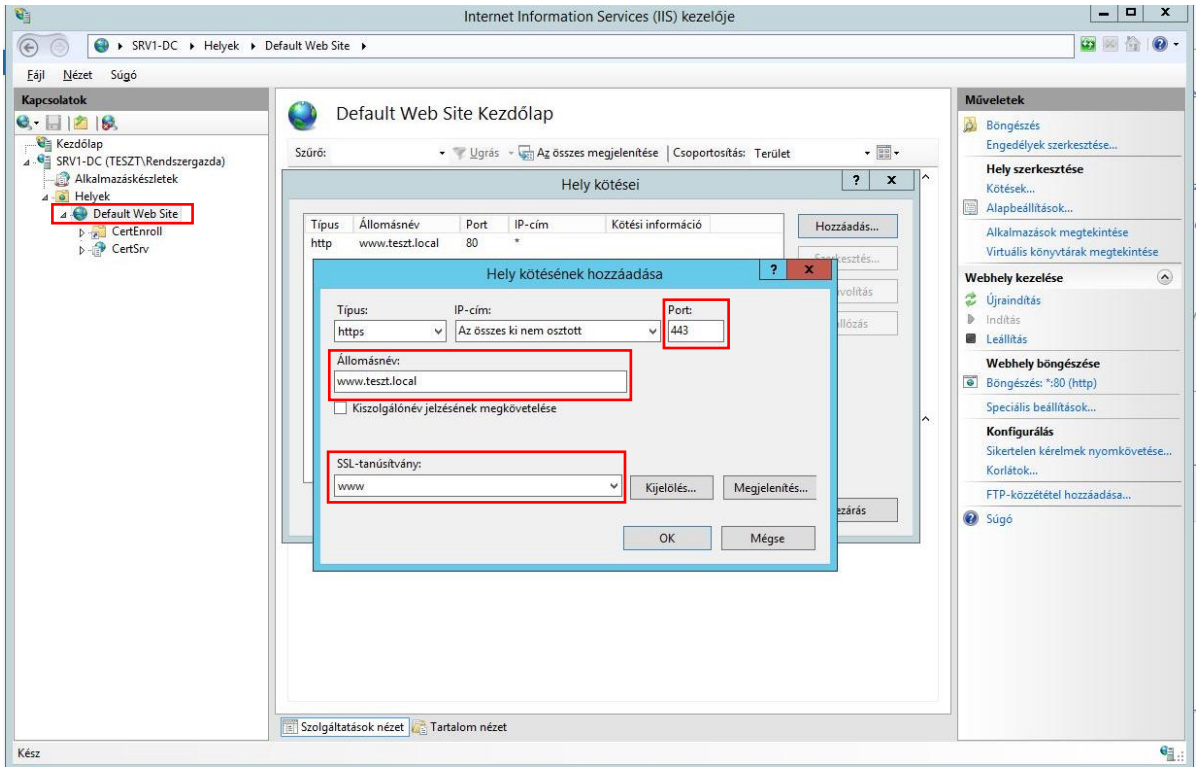
A rövid névhez „**www**” kifejezést írjuk. Majd a **Befejezés** gombra kattintunk.



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 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.

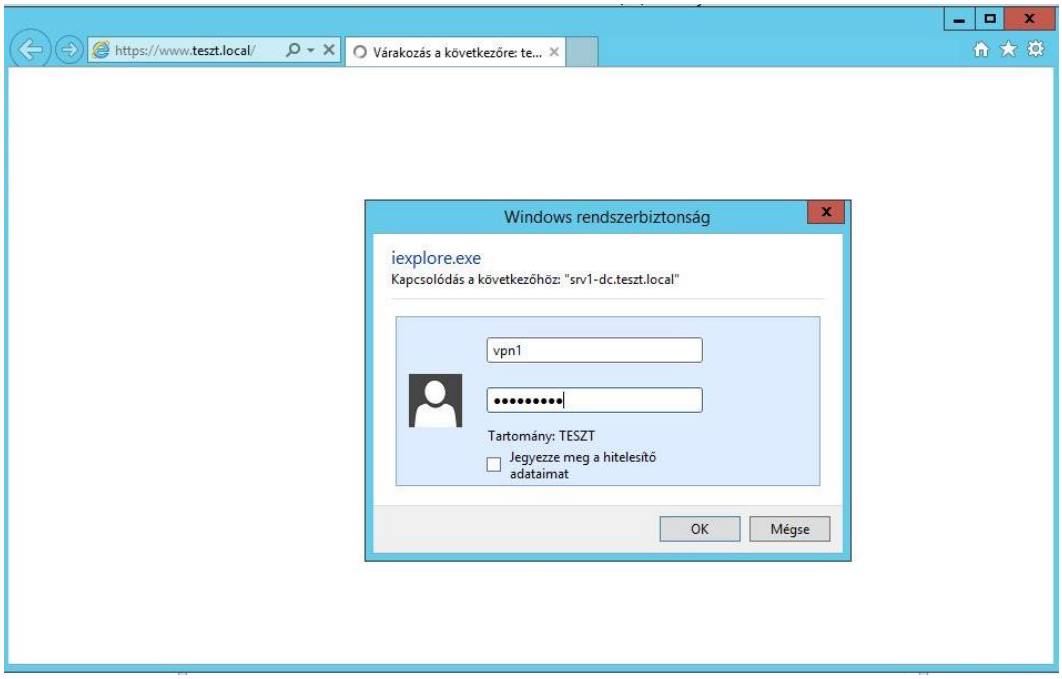
Felmerül egy probléma, a ***443***-as porton továbbra is elérjük a weblapunkat, de a ***80***-as portra hibalapot ad ki.

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

A korlátozzuk le, hogy ki érhesse el a weblapunkat:

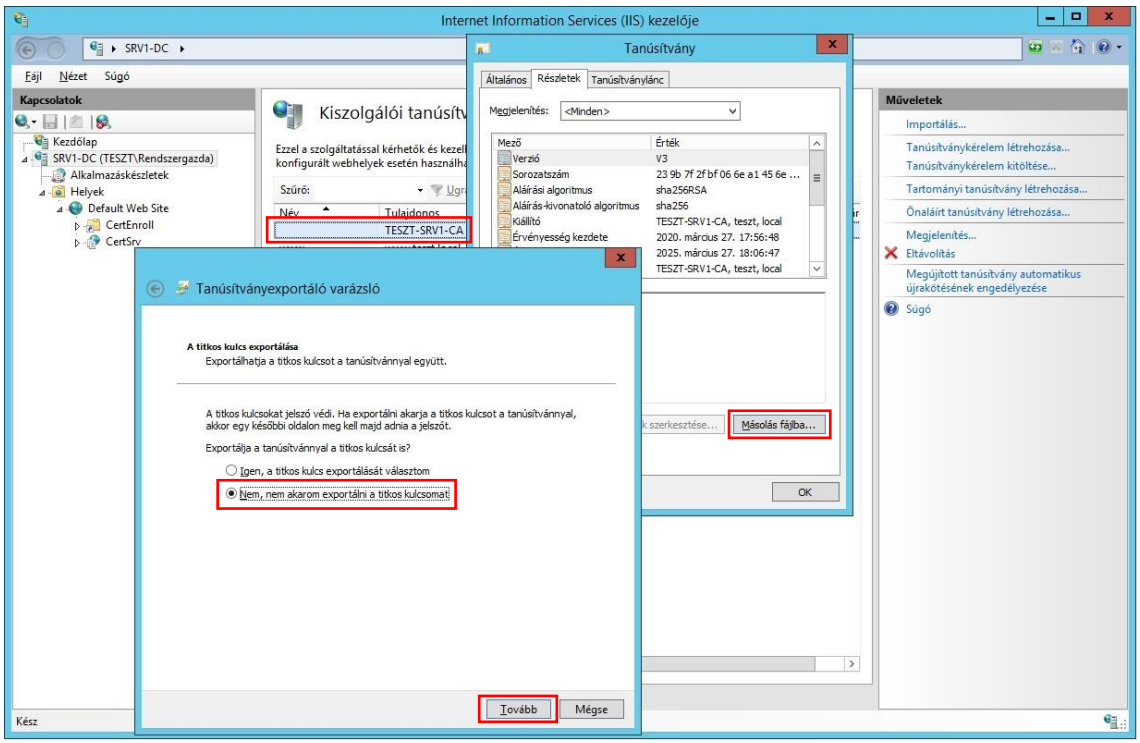
Ezt az IIS szerepkörében -*tartományi felhasználók esetén*- a **Windows-hitelesítés** nevű szerepkör-szolgáltatás használatával végezzük el.

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.

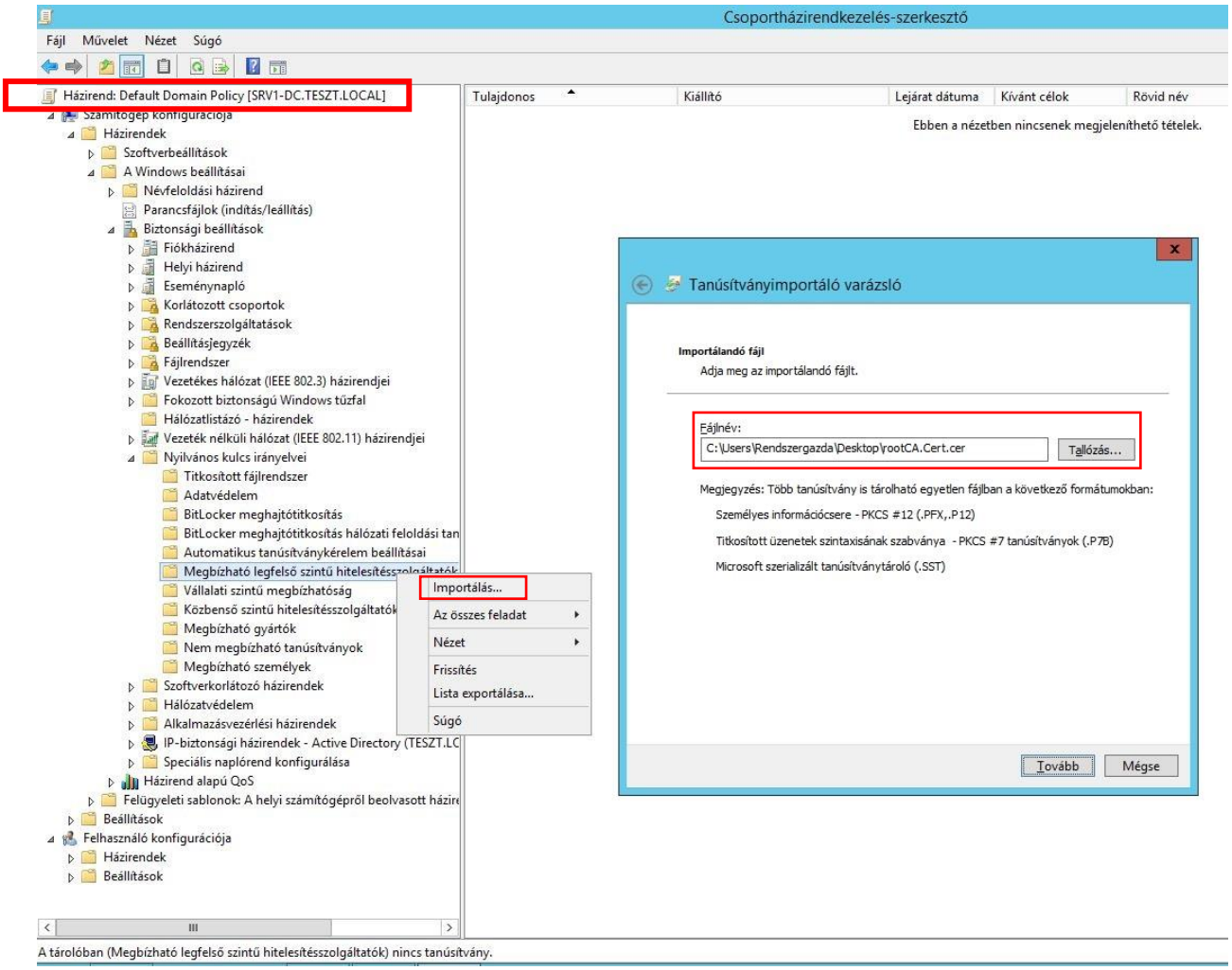


A végül érjük el, hogy a Window10 kliensen ne kelljen külön letölteni a CA kiszolgálói tanúsítványt, hanem azonnal megkapja. Ezt csoportházirendben állíthatjuk be.

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



Ezután a csoportházirendben 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 csoportházirend frissítéséről. (*gpupdate /force*)
Szükség esetén a kliensünket újra is kell indítani, hiszen Számítógépek konfigurációjára ható csoportházirend szabályt módosítottunk!

A végső, tesztelési fázisba érkeztünk.

Indítsuk el a ***Windows 10*** virtuális számítógépet!
Léptessük be a kliens gépünket a tartományba! (esetünkben ez a tartomány a ***teszt.local***).
Ezután lépjünk 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*).