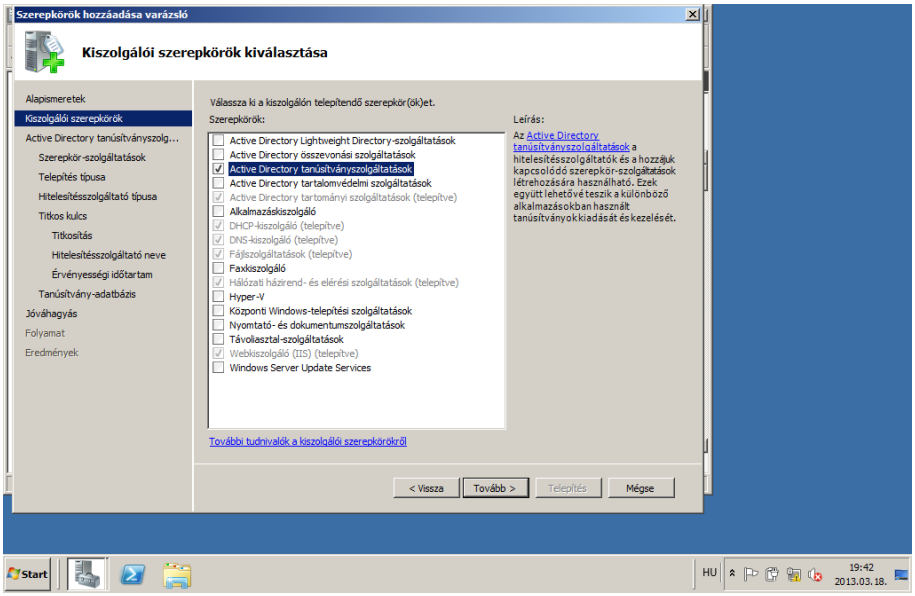
SSL tanúsítvány kérése AD-ban

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

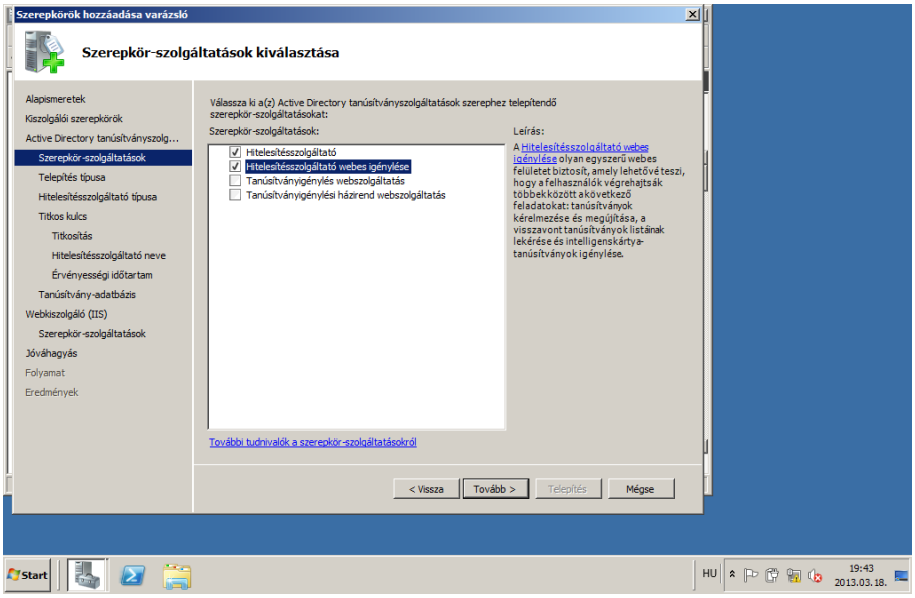
A kliens gépet léptessük be az Active Directory-ba, a szerveren és a kliensen is kapcsoljuk be a tűzfalat a bejövő forgalomnál. A webhely működéséhez a 80-as és a 4400-as portokat engedélyeznünk kell a bejövő forgalom esetén.

Tanúsítvány szolgáltatás telepítése

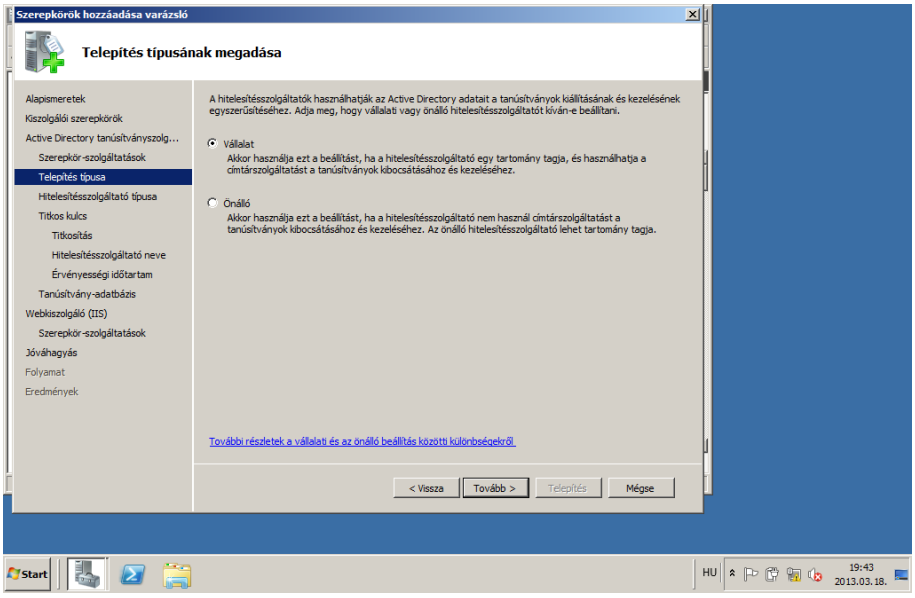
A kiszolgálókezelőben az Active Directory tanúsítványszolgáltatások szerepkört telepítjük.



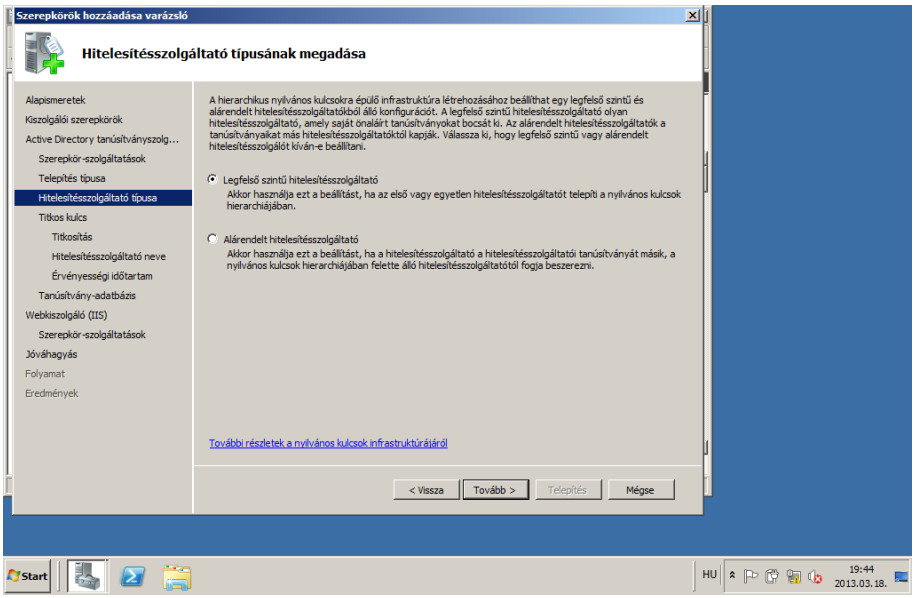
A következő ablakban, kiválasztjuk a telepíteni kívánt szolgáltatásokat itt az első kettőt jelöljük be. A második pont bejelölése után a felugró ablakban az IIS telepítését fogadjuk el és kattintsuk a tovább gombra.



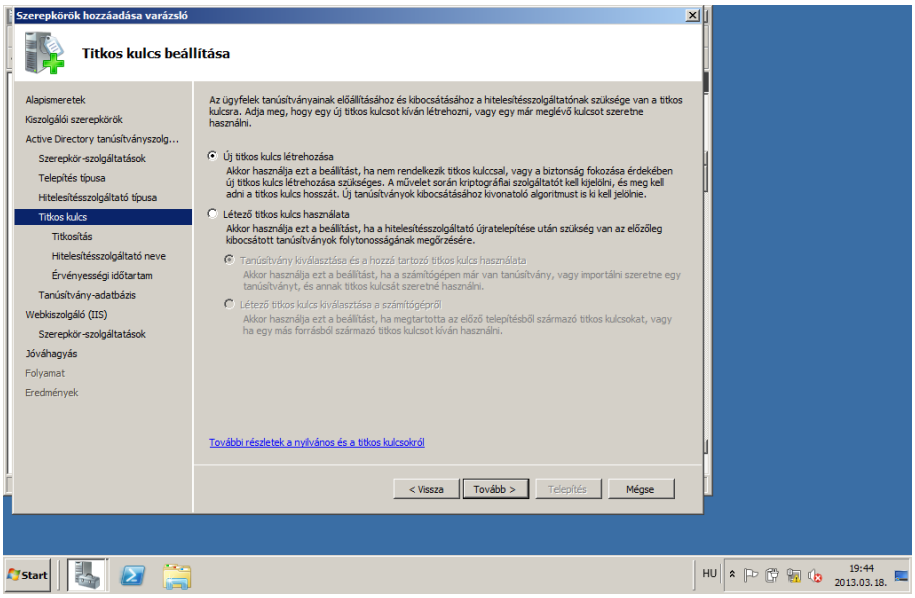
A telepítés típusánál a Vállalat szintű beállítást választjuk, ezt csak tartományi tagként tehetjük meg, és mivel a feladat az AD-ban való tanúsítványszolgáltatásról szól, ezt választjuk.



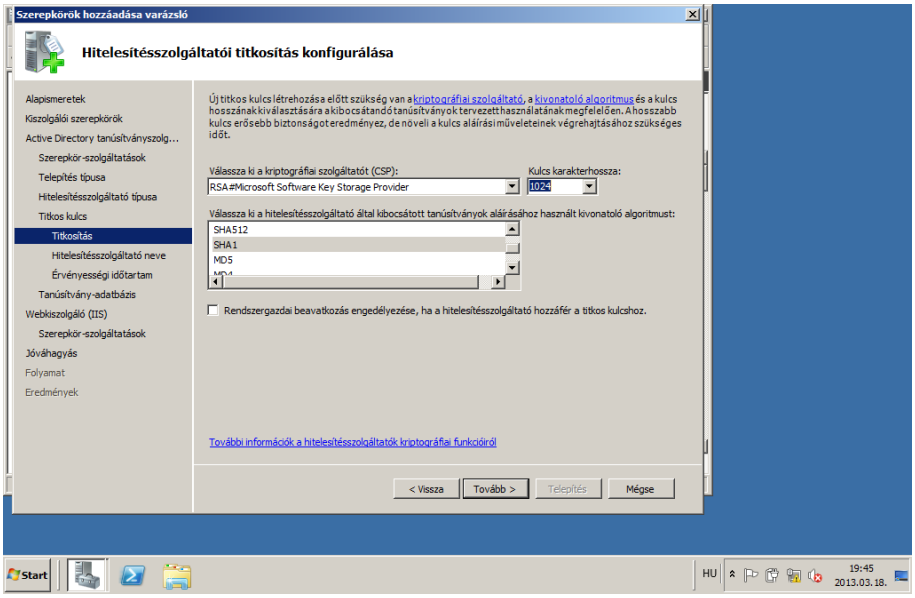
A következő pontban a legfelső szintű szolgáltatást választjuk.

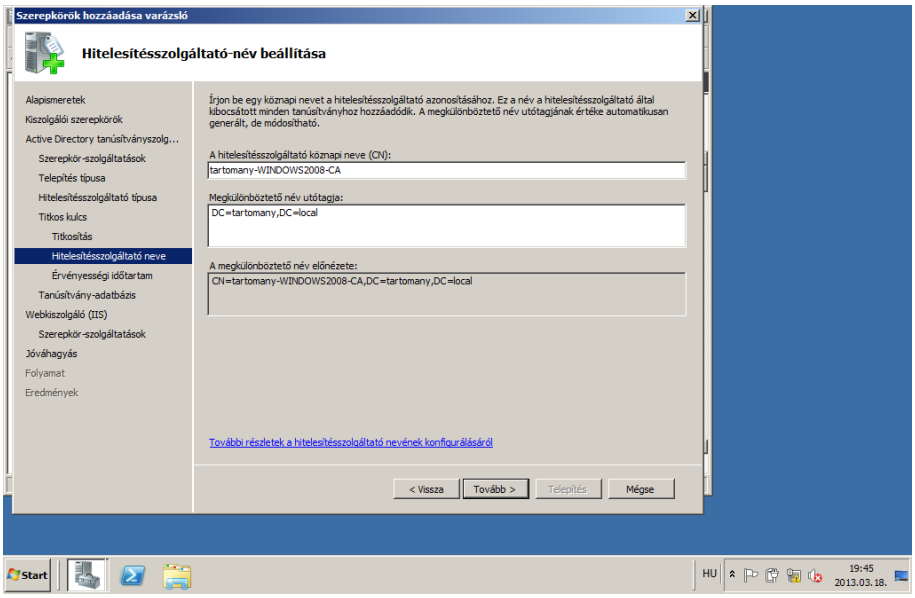


A tanúsítványokhoz szükség van egy kulcs létrehozására és mivel most telepítünk elsőnek tanúsítványszolgáltatást, nincs létező kulcsunk, újat kell létrehoznunk

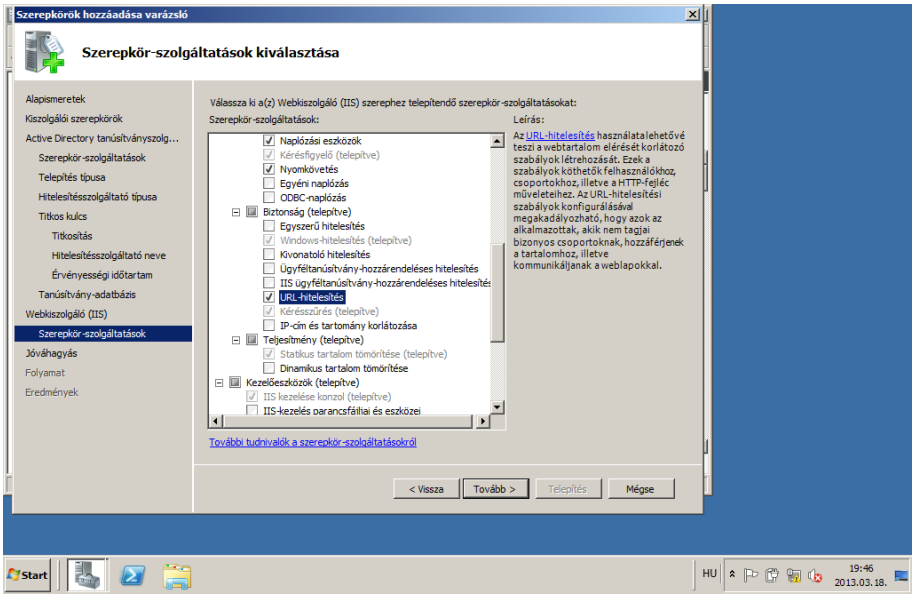


A következő pontban a titkosítást választjuk, rengeteg féle közül lehet válogatni. Mi az RSA kriptográfiát választjuk, SHA1-es hash algoritmussal és 1024-es kulcshosszal. A következő pár pontban nem kell semmit se változtatni azokat az alapbeállításokon hagyjuk.





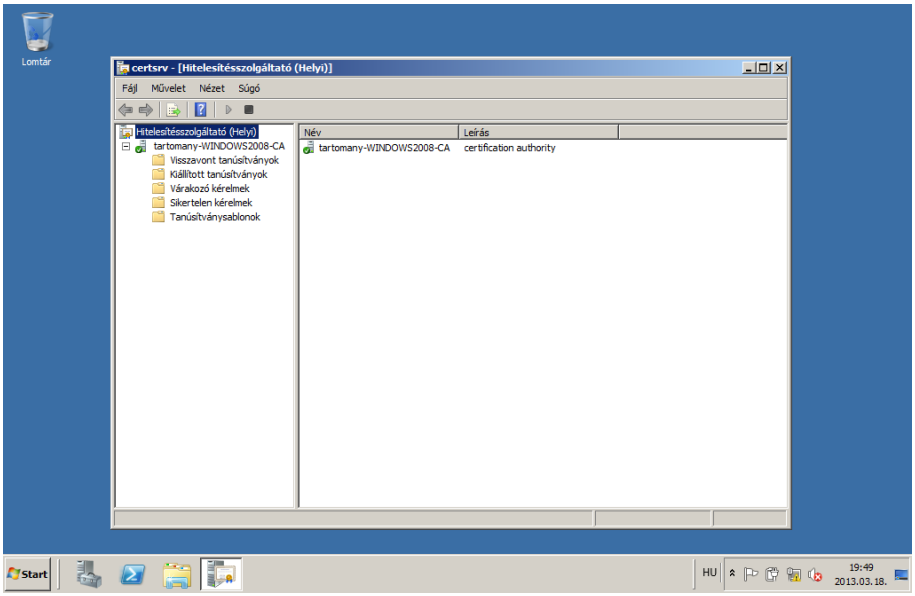
A következő beállítást az IIS-nél végezzük, itt egyedül már csak az URL-hitelesítést állítsuk be. Ezzel a ponttal korlátozhatjuk, hogy ki érje el a honlapot és ki nem a megfelelő felhasználónév/jelszó párossal.



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

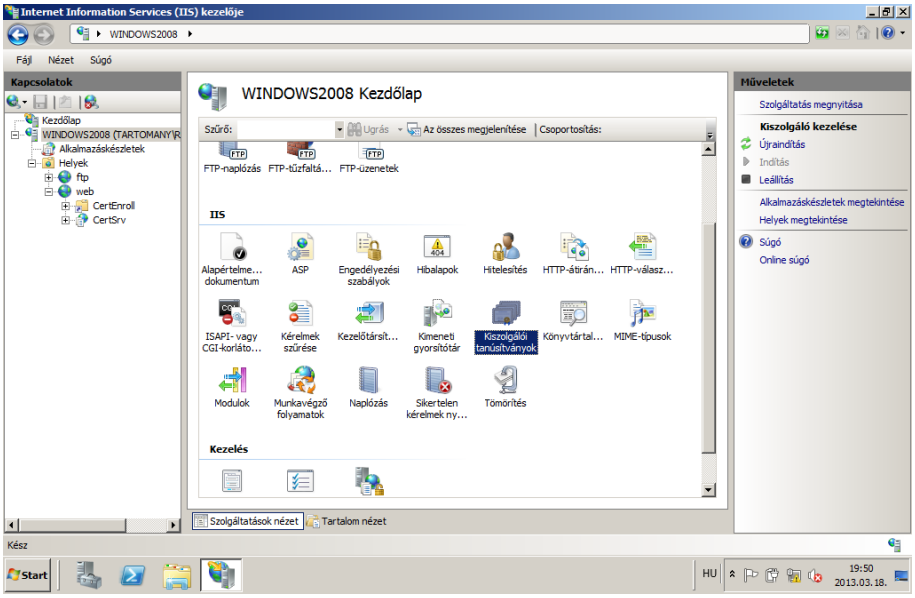
A felügyeleti eszközökben megtalálhatjuk a tanúsítványszolgáltatót, valamilyen oknál fogva ezt a nevet nem fordították le magyarra.

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.

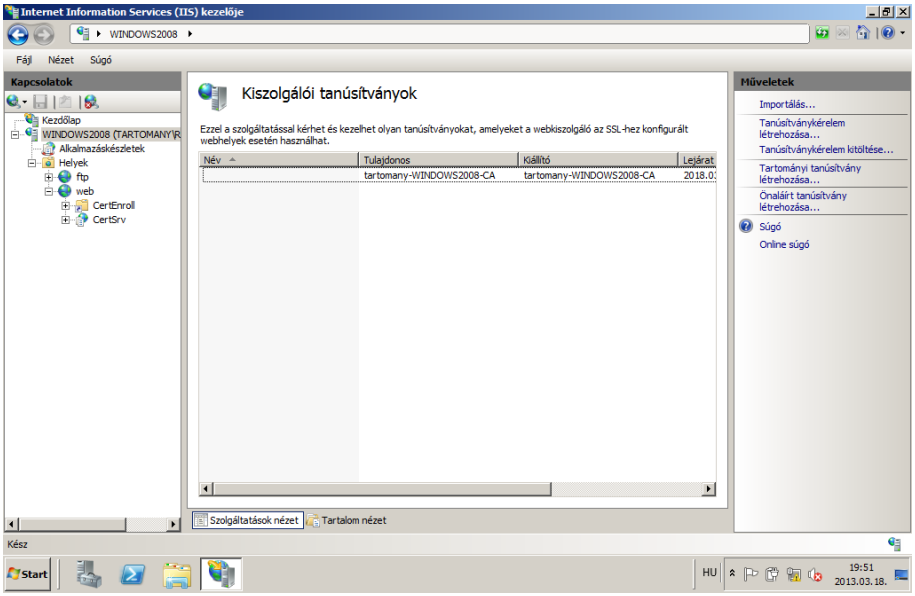


Biztonságos webhely kialakítása

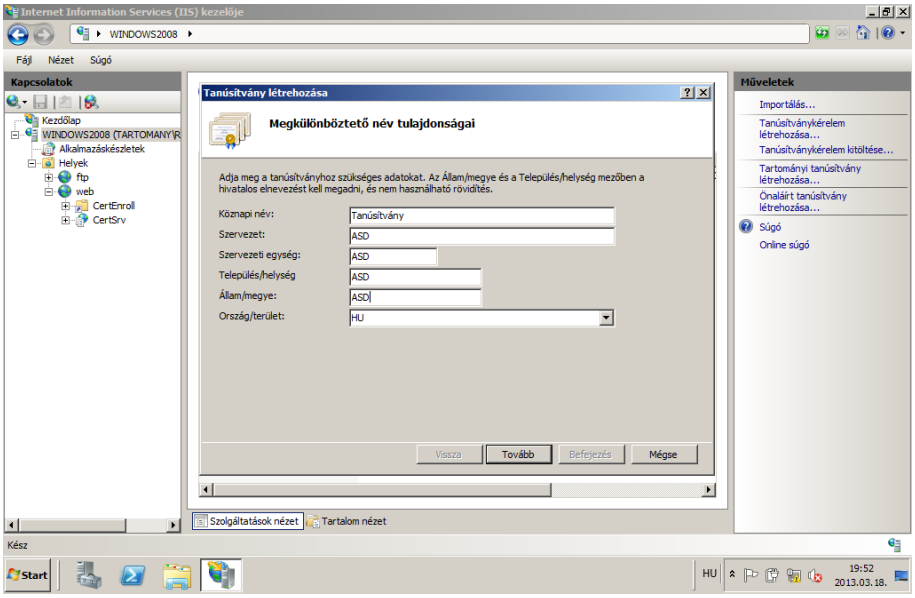
Az alapértelmezett webhelyet fogjuk használni (Default Web Site). Előtte a webkiszolgálónak egy tanúsítványt kell igényelnünk. Első lépésként a legfelső szinten a kiszolgálói tanúsítványok beállítás menüjébe lépünk.



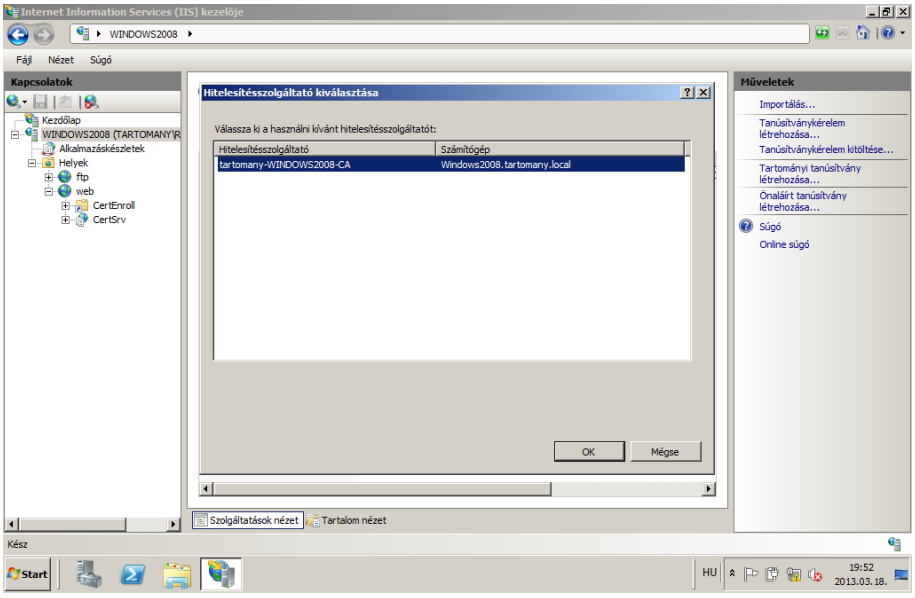
Itt jobb oldalt a műveleteknél kiválasztjuk a Tartományi tanúsítvány létrehozását.



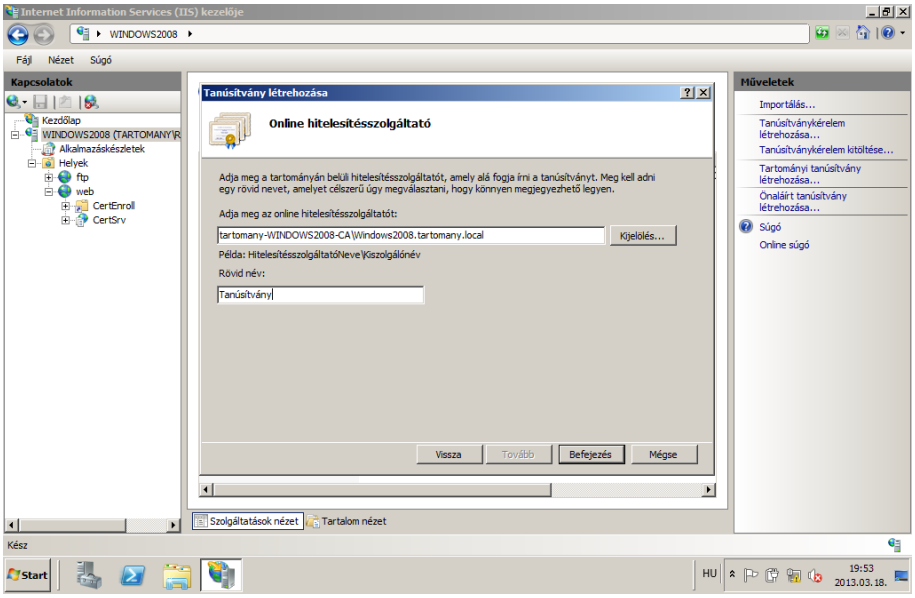
A felugró ablakban megkell adnunk az adatainkat. Az első helyre adjuk meg a „**Tanúsítvány**” nevet, az egyszerűség kedvéért a többi helyre „**ASD**”-t írunk be, kivétel az utolsó pont, oda a „**HU**”-t.



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

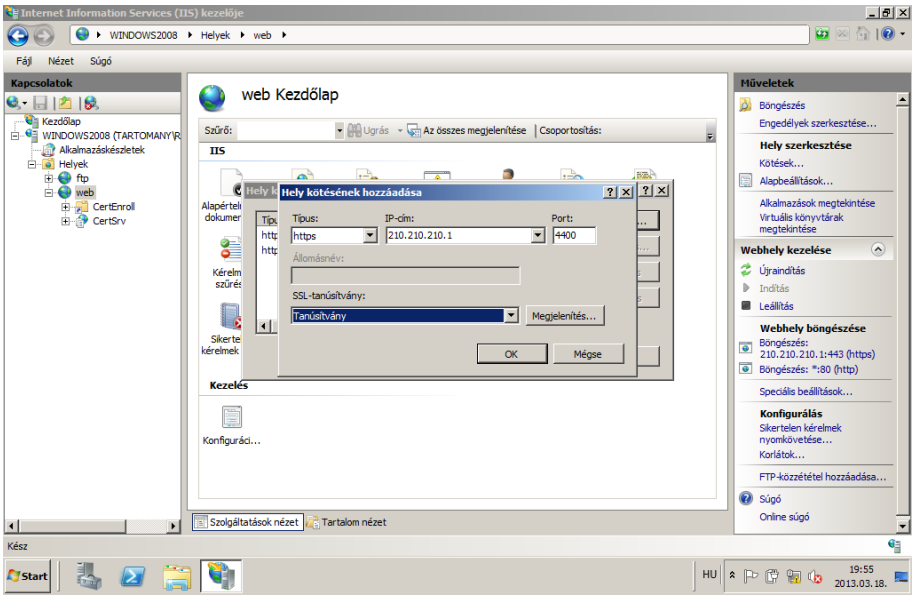


A rövid névhez a „**Tanúsítvány**” szót írjuk. Majd a befejezés gombra kattintunk.



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 4400-as porttal. A típus kiválasztása után az állomásnév beszürkül és az SSL-tanúsítvány-nál kijelölhetjük a tanúsítványt. Itt az általunk létrehozott „**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 protokol is működik a megfelelő portszámmal, de emellet 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.

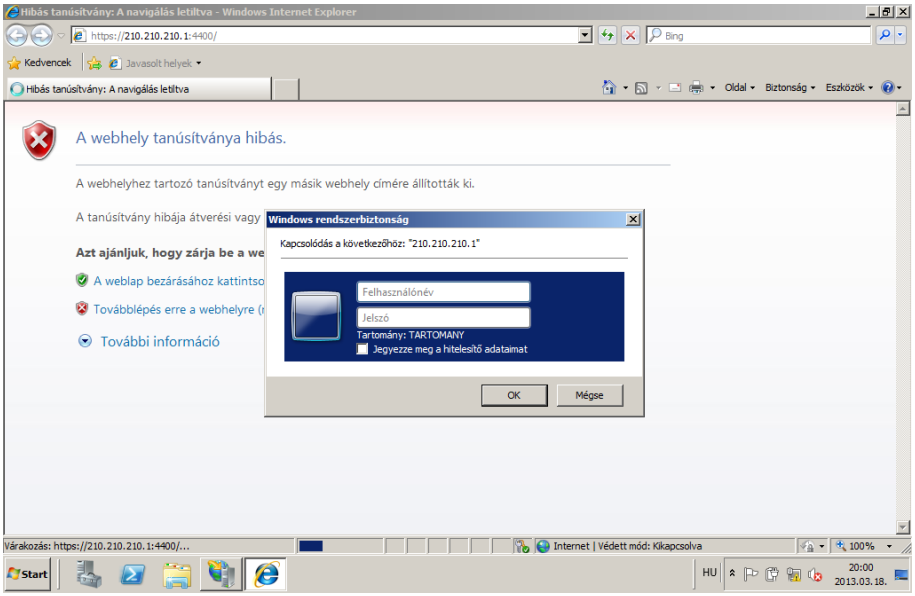
Az SSL beállításával a kliensek honlap elérését korlátozhatjuk és megakadályozhatjuk a 80-as port használatát. Állítsuk be az SSL-t: kattuntsunk az SSL-beállítás fülre, és pipáljuk be a SSL – megkövetelését, majd jobb oldali sávban az alkalmaz gombra kattinva érvényesítjuk a beállításunkat.

A probléma most következik, a 4400-as porton továbbra is elérjük a weblapunkat, de a 80-as portra hibalapot ad ki.

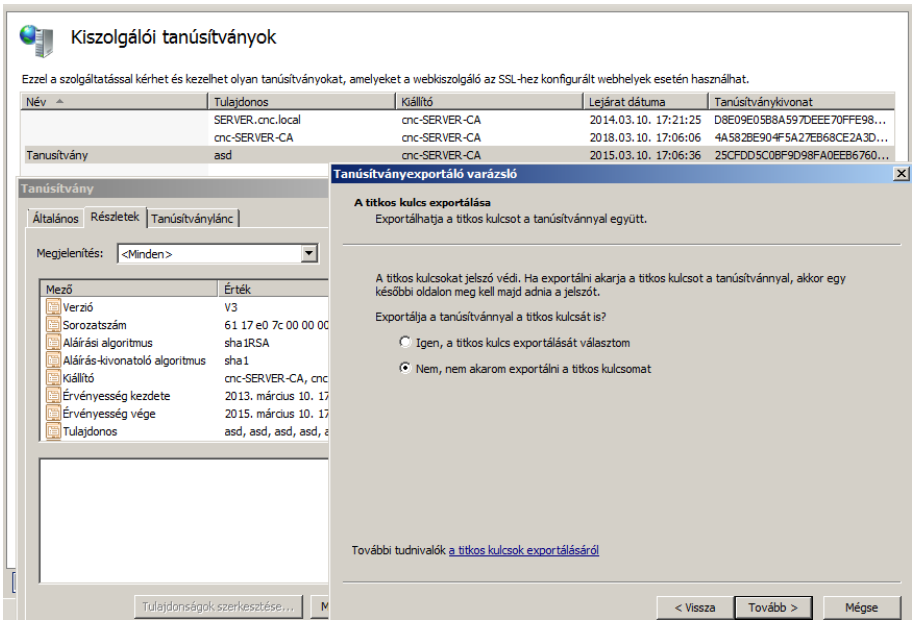
Megoldás: Hiba lapoknál vegyünk fel egyéni hibalapot.

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

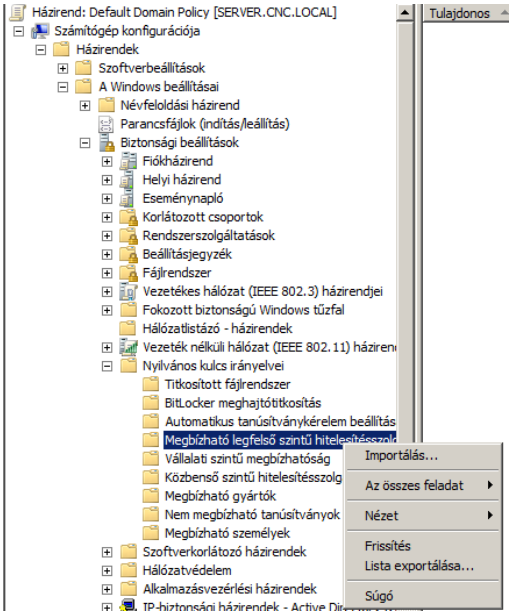
A beállítás után teszteljük a szerverről a belépést, a webhely indítása után írjuk be a megfelelő felhasználónév és jelszó párost, ha beenged akkor sikerült, ha nem akkor nézzük át a beállításokat. Teszteljük úgyis, hogy belépésre nem jogosult felhasználót adunk meg.

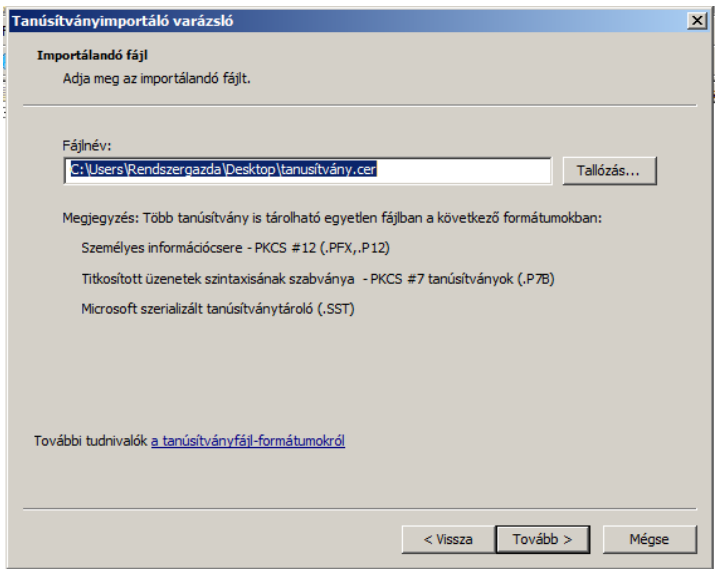


A végül érjük el, hogy a Windows7-ről ne kelljen külön letölteni a tanúsítványt, hanem azonnal megkapja. Ezt a csoportházirendben állíthatjuk be, és itt beállítjuk még a megfelelő portok engedélyezését is. Először az IIS-ben az általunk létrehozott tanúsítványt kiexportáljuk. Megjelenítés aztán a részletek 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 tanúsítványt.

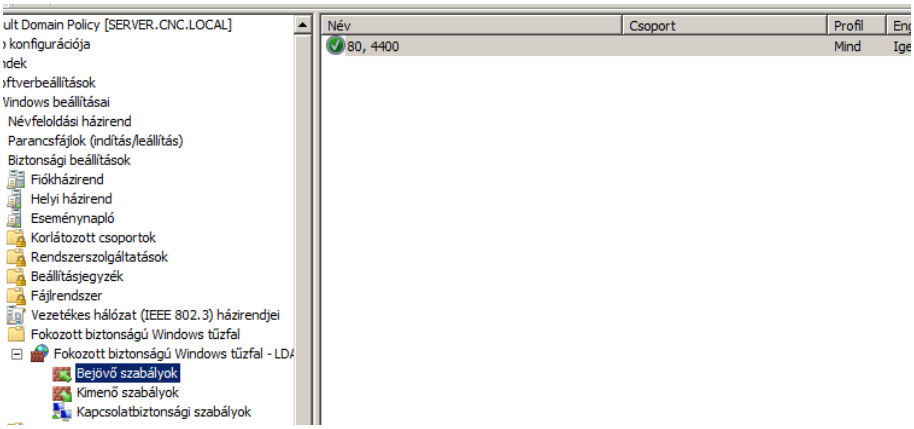


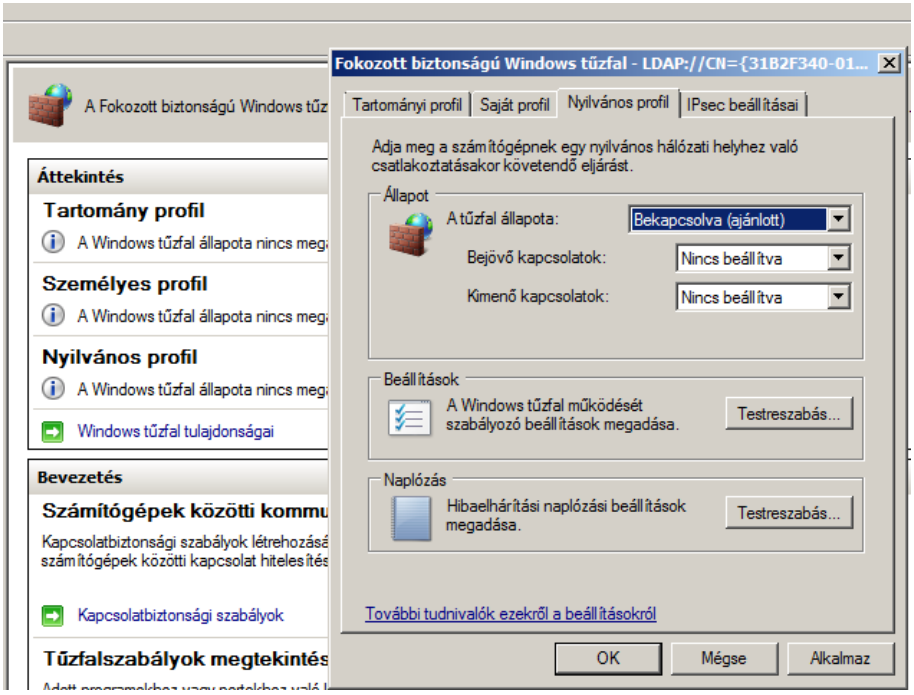


Ezzel elértük azt,hogy a tartományi számítógép minden beállítás nélkül letöltse a tanúsítványt. A következő beállítást is a csoportházirendben kell elvégeznünk.

Szintén a Windows beállításoknál vagyunk és válasszuk ki a Fokozott biztonságú Windows tűzfal beállítást. Nyissunk le minden menüpontot.

Az első menüpontnál kapcsoljuk be a tűzfalat, utána vegyük fel a 80-as és a 4400-as portokat.





A végső, tesztelési fázisba érkeztünk. Indítsuk el a windows 7 virtuális számítógépet. Léptessük be a tartományba (tartomany.local). Ezután lépjünk be valamelyik felhasználóval. A tűzfal indítása után ellenőrízhetjük, hogy megkapta-e a tűzfal a beállításokat (Figyeljünk arra, hogy rendszergazdaként indítsuk). A tanúsítványt is ellenőrizzük. Végül a webhely elérhetőségét mind a 4400-as mind a 80-as porttal is. (80-as portnál a webhely átirányítását teszteljük).