

## Tanúsítványok beszerzése

Ha intézményünk hálózatán a rendszergazda megtette a szükséges előkészületeket a titkosítás és digitális aláírás használatához, akkor igen egyszerű a kulcsok beszerzése. Lehet, hogy semmit sem kell tennünk, mert automatikusan kapjuk kulcsainkat, de az is lehetséges, hogy a cégünk hálózatán kell felkeresnünk a megfelelő weboldalt. Ha a megfelelő weblapot felkeressük (például: ca.demovpc.hu/certsrv), néhány adat megadása után már levelezhetünk is. Most ezt az utóbbi esetet tekintjük át, de a tanúsítvány beszerzésének lehetnek cégünkre jellemző egyedi lépései.

- A weblap eléréséhez meg kell adni nevünket és jelszavunkat.
- A megjelenő oldalon válasszuk a *Request a certificate (Bizonyítvány kérése)* pontot, és haladjunk tovább.
- A *Select the certificate type (Kérelmetípus kiválasztása)* oldalon a *User Certificate (Felhasználói bizonyítványkérelem)* lehetőséget válasszuk ki, és lépünk tovább.
- A megjelenő oldalon a gyakorlottabbak finomíthatják a kérelem beállításait a *More Options (További beállítások)* gombra kattintva, de azonnal el is küldhetjük kérelmünket a *Submit (Küldés)* gomb segítségével.
- Ha minden rendben, akkor rövid várakozás után (*waiting for server response...*) a 8.1. ábra szerint megkapjuk bizonyítványunkat.



8.1. ábra: Megkaptuk a tanúsítványunkat



A 8.1. ábra szerint még telepíteni kell a megkapott bizonyítványt, de ehhez csak a megfelelő felírra kell kattintanunk (*Install this certificate*). Ha megkaptuk a *Your new certificate has been successfully installed. (Bizonyítvány telepítése sikeresen befejeződött)* üzenetet, akkor használhatjuk a digitális aláírás és a titkosítás lehetőségeket. A példában igényelt tanúsítvány aláírásra és titkosításra is használható, de előfordulhat, hogy a különböző feladatokra különböző tanúsítványokat kell igényelni.

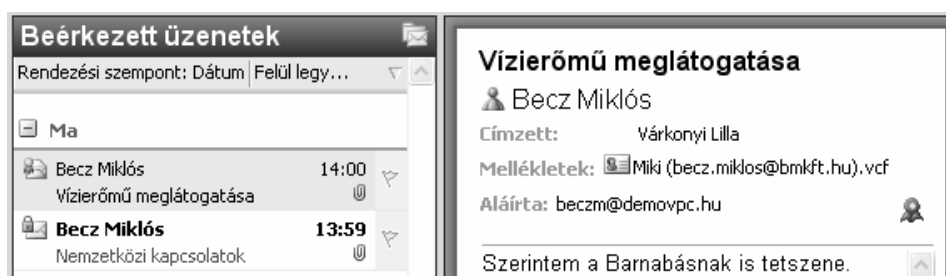
## 8. Digitális aláírás, titkosítás

Ha külső szolgáltatótól szeretnénk kulcsainkat beszerezni, akkor keressük fel a kiválasztott szolgáltató honlapját. Példaként röviden a NetLocktól való igénylés folyamatát tekintjük át. Elsőként a weblapon kezdjük meg a kulcsigénylést. Ehhez szükséges, hogy legyen e-mail címünk. Az igénylésünk összefoglalásáról egy e-mailt fogunk kapni. Fontos, hogy amíg kulcsainkat nem kapjuk meg, addig az igényléshez használt gépnek léteznie kell. Nem szabad újratelepíteni sem! Utána természetesen szabadon rendelkezhetünk kulcsaink felett. A következő lépésben a választott kulcs erősségének megfelelő adatainkat kell hitelesen bizonyítanunk (például igazolványok postai vagy személyes bemutatása). A cég honlapján figyelemmel kísérhetjük, hogyan áll az igénylési folyamat. Végül kapni fogunk egy e-mailt, hogy kulcsunk elkészült. Töltsük le és telepítsük. A telepítésnél célszerű azt a lehetőséget választani, hogy engedélyünk szükséges, ha valamelyik program használni szeretné személyes kulcsainkat.

Jó tudni, hogy a NetLocktól díjmentesen igényelhetünk egy hónapig érvényes teszt tanúsítványokat. Ezekkel a teszt tanúsítványokkal mindent, teljes értékűen kipróbálhatunk.

## Levél titkosítása és aláírása

Írjuk meg levelünket a szokásos módon, majd kattintsunk az eszköztár megfelelő gombjára (  aláírás és  titkosítás). Ha az említett ikonok nem láthatók az eszköztáron, akkor olvassuk el a fejezet 8.3. ábra utáni részét. Természetesen lehetséges egy levelet aláírni és titkosítani egyszerre. Fontos, hogy a titkosítás választásánál már rendelkezniünk kell a címzett nyilvános kulcsával, hiszen ennek a kulcsnak már a titkosítás folyamatában részt kell vennie. Ha a címzettnek nem érhető el a nyilvános kulcsa, akkor a küldéskor figyelmeztetni fog erre az Outlook.



8.2. ábra: Aláírt, titkosított üzenetet kaptunk

Ebben az esetben választhatjuk a titkosítás nélküli küldést is. Ha mégis titkosítva küldenénk el üzenetünk, akkor a címzett nem tudná megnyitni, hiszen a titkosításhoz használt nyilvános kulcs privát párja nem áll rendelkezésére. A beérkezett üzenetek között a 8.2. ábra szerinti jelzések mutatják a titkosítást és az aláírást.