TIOP 2.3.1 - 2.3.2

Tanúsítványigénylés

Minősített szolgáltató által kiállított tanúsítvány igénylése intézményi felhasználók azonosítására (Útmutató)

Tartalomjegyzék

1 Dokumentumtörténet

Verzió	Készítette	Dátum	Változás
1.0	Seres László	2016.08.17.	Első kiadott változat

2 Dokumentum célja

Jelen dokumentum tartalmazza az EESZT rendszer intézményi felhasználók általi használatához szükséges tanúsítványok igénylésének, EESZT részére történő átadásának részleteit.

3 Intézményi felhasználó azonosítás

Amennyiben a csatlakozó rendszer intézményi felhasználót is használ (intézményi technikai felhasználó), abban az esetben azt tanúsítvánnyal kell azonosítani. Az EESZT-hez csatlakozó rendszereknek minősített szolgáltató által elektronikus authentikációra kiadott szervezeti tanúsítványt kell használniuk az azonosításhoz.

Az EESZT intézményi felhasználó létrehozása során „Fokozott biztonságú szervezeti authentikációs tanúsítvány” használatát követeli meg, mely tanúsítvánnyal a felhasználó aktiválása előtt az intézményi felhasználónak rendelkeznie kell, valamint annak publikus részét az aktiválás során az EESZT részére át kell, adja.

A tanúsítványokról, valamint a tanúsítvány igényléséről részletesebben a 4. pontban talál ismertetőt, míg a publikus tanúsítvány EESZT részére történő átadásáról a 5. pontban olvashat.

3.1 Tanúsítványok

Tanúsítványt megbízható, bevizsgált szervezet, ún. hitelesítés szolgáltató állít ki emberek vagy számítógépek részére. A tanúsítvány egyrészt annak a megnevezését tartalmazza, akinek a számra a tanúsítványt kiállították, és emellett olyan információkat tartalmaz, amely segítségével mások biztonságosan - titkosan vagy hitelesen - kommunikálhatnak a tanúsítvány birtokosával.

Minden tanúsítványhoz kapcsolódik valamilyen titkos információ, amelyet kizárólag a tanúsítvány alanya, birtokosa (vagyis aki számára a tanúsítványt kiállították) ismer. Ezen információt nevezik magánkulcsnak, elektronikus aláírásra használható tanúsítvány esetén pedig aláírás-létrehozó adatnak is nevezik.

Ezen információ lehet egy fájl egy számítógépen (ekkor beszélünk szoftveres tanúsítványról), de lehet intelligens kártyán, vagy más hardver eszközön is.

Különböző fajta tanúsítványok léteznek:

- Titkosításra szolgáló tanúsítványok esetén a tanúsítvány arra vonatkozó információt tartalmaz, hogy hogyan lehet egy fájlt vagy egy elektronikus levelet úgy titkosítani, hogy azt kizárólag a címzett, a tanúsítvány birtokosa tudja (ezen titkos információ, tehát az ő magánkulcsa) segítségével visszafejteni.
- Az aláírásra szolgáló tanúsítvány arra vonatkozó információt tartalmaz, hogy ha valaki elektronikus aláírással látott el egy dokumentumot (tehát a saját magánkulcsa segítségével kódolta azt), akkor hogyan lehet megbizonyosodni arról, hogy ezt a kódolást (aláírást) valóban ő készítette. Ezt a műveletet nevezzük az elektronikus aláírás ellenőrzésének.
- A biztonságos azonosításra (más néven hitelesítésre vagy authentikációra) szolgáló tanúsítványokból az állapítható meg, hogy a tanúsítvány birtokosát hogyan lehet elektronikus úton (például Interneten keresztül) azonosítani, és ezt követően hogyan lehet vele biztonságos (titkosított és hitelesített) csatornát kialakítani.

Ha biztonságosan (titkosan vagy hitelesen) szeretnénk kommunikálni valakivel, először be kell szereznünk a tanúsítványát. Ha mi szeretnénk neki titkos üzenetet küldeni, akkor egy hitelesítés szolgáltató honlapján (tanúsítványtárában) kereshetjük meg az ő tanúsítványát. Ha ő már üzent nekünk, akkor üzenete vagy aláírása általában tartalmazza a tanúsítványát. Ha megszereztük a tanúsítványt, ellenőriznünk kell, hogy valóban érvényes-e, és célszerű megnéznünk, hogy valóban annak a neve szerepel-e benne, akivel mi kommunikálni szeretnénk.

3.1.1 Authentikáció (biztonságos azonosítás)

Az authentikáció, más néven partnerhitelesítés vagy biztonságos azonosítás azt jelenti, valamilyen biztonságos módon, jellemzően kódolási, kriptográfiai módszerek segítségével megbizonyosodunk róla, hogy azzal kommunikálunk-e, akivel szeretnénk.

Ez általában a következő elvek szerint történik:

1) Megszerezzük másik fél tanúsítványát, és meggyőződünk a tanúsítvány érvényességéről. Így hitelesen hozzájutottunk a tanúsítványba foglalt nyilvános kulcsához, biztosak lehetünk benne, hogy az valóban az ő nyilvános kulcsa.
2) Generálunk egy friss véletlen számot, ezt nevezzük kihívásnak. E véletlen kihívást küldjük el a másik félnek.
3) A másik fél - akit biztonságosan azonosítani szeretnénk - megválaszolja a kihívást: a kihívásban szereplő véletlen számot a saját tanúsítványához tartozó magánkulcsával kódolja. (E kódolást csak ő tudja elvégezni, mert az ő tanúsítványához tartozó magánkulcs kizárólag az ő birtokában van.) A kódolás eredményét visszaküldi nekünk.
4) Ellenőrizzük, hogy a másik fél helyesen válaszolt-e a kihívásunkra: a tanúsítványa - pontosabban a tanúsítványában lévő nyilvános kulcsa segítségével ellenőrizhetjük, hogy a kódolást a tanúsítványhoz tartozó magánkulccsal végezték-e el.

Az ilyen módon történő biztonságos azonosítást kihívás és válaszalapú azonosításnak is nevezik.

4 Authentikációs tanúsítvány igénylése

Szoftveres fokozott biztonságú szervezeti authentikációs tanúsítványt állami intézmények esetén a NISZ GovCA adja ki, míg piaci szereplőknek a Netlock Kft.-től vagy a Microsec Zrt.-től kell beszerezni.

A tanúsítványok igénylése jellemzően interneten keresztül online felületen történik a szolgáltatók honlapján található ismertetőknek megfelelően. A szolgáltatók online felületei az alábbi URL-eken érhetőek el:

- Netlock Kft.
  https://www.netlock.hu
- Microsec Zrt.
  https://www.e-szigno.hu

Mindként szolgáltató esetében fontos, hogy az igénylés végén kapott tanúsítványt arra a számítógépre kell elsőként telepíteni, ahonnan az igénylét kezdeményezték. Amennyiben a számítógép, amelyen a tanúsítványt használni fogják, eltér az igénylő gépétől, úgy mindenképpen szoftveres tanúsítványt kell igényelni, és így a tanúsítvány a későbbiekben az igénylő gépéről ki-exportálható és bármely más számítógépre átvihető.

4.1 Fontos információ az igényléshez

Az igénylés során a tanúsítványban feltüntetendő adatok megadásánál kerülni kell a „(” és a „)” karaktereket!

4.2 Netlock szoftveres authentikációs tanúsítvány igénylése

A Netlock Kft. választása esetén az igénylendő típus pontos megnevezése:

„C osztályú szervezeti authentikációs tanúsítvány”

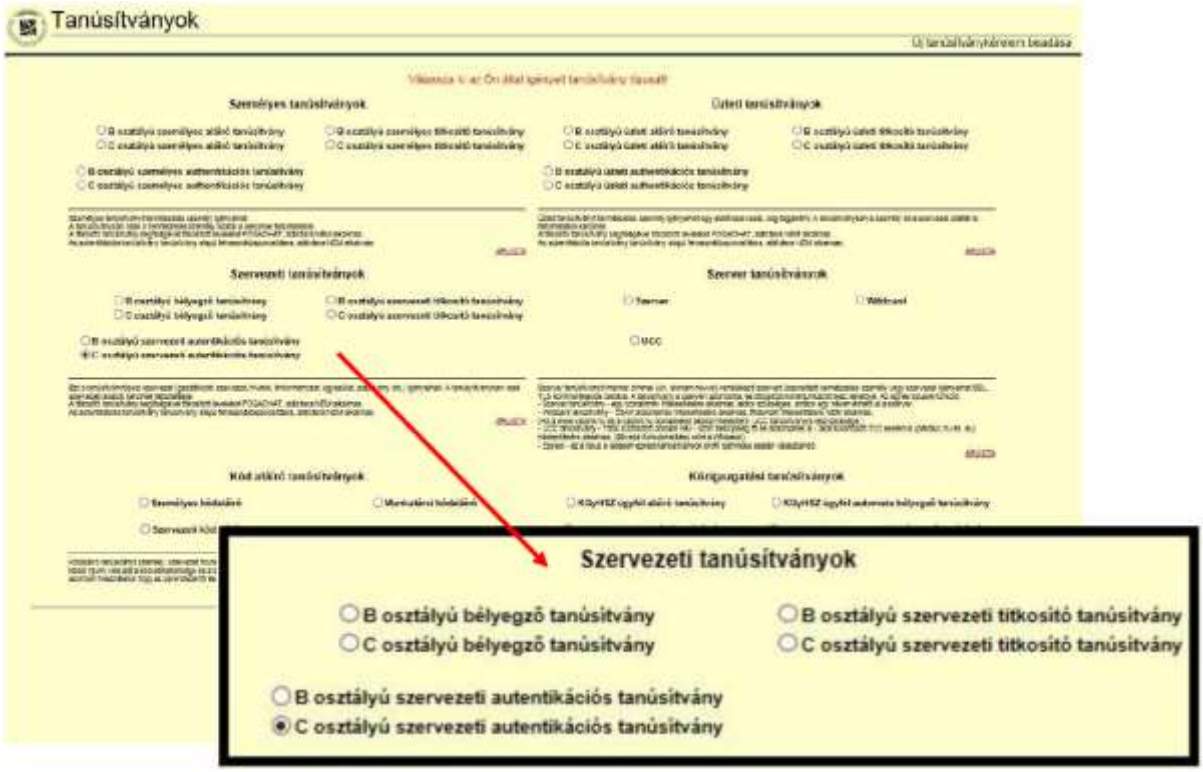
Tanúsítvány igénylés lépései:

1) Indítsa el az Internet Explorer böngészőt
2) Látogasson el a www.netlock.hu oldalra
3) Nyissa le a Tanúsítványok igénylése menüt, majd válassza a Nem minősített tanúsítvány igénylése menü pontot.

4) Itt tud regisztrációt készíteni, mellyel egy úgynevezett ügyfélmenüt hoz létre. Az ügyfélmenü segítségével tudja intézni a tanúsítvány kérelmeit, és innen tudja majd letölteni a kiadott tanúsítványát.

5) Jelentkezzen be a létre hozott ügyfélmenüjébe.
6) Az ügyfélmenüben válassza a Tanúsítványok menüt, majd az Új tanúsítványkérelem beadása menüpontot.

7) Válassza ki az igényelni kívánt tanúsítványt, a kulcsgenerálás módját, majd az oldal alján lévő Tanúsítvány kérelem gombra kattintva lépjen tovább.



A tanúsítványigényléssel kapcsolatosan részletes ismertetőt a mellékelt dokumentumban talál.

4.3 Microsec szoftveres authentikációs tanúsítvány igénylése

A Microsec Zrt. választása esetén az igénylendő típus pontos megnevezése:

„Nem minősített (fokozott) bélyegző, autentikációs és titkosító tanúsítványok szervezetek (automatizmusok, szerverek) számára”

Az online igénylőlap az alábbi URL-en érhető el:

https://srv.e-szigno.hu/index.php?lap=szoftveres_automata_igenyles

Az igénylés során az „Autentikációs tanúsítvány”-t kell bejelölni.

A „Tanúsítványban szereplő név” mezőben az igénylő szervezet nevét kell megadni.

Az igénylés menetéről részletesen a szolgáltató honlapján talál információkat.

5 Tanúsítvány EESZT részére történő átadása

Az intézményi felhasználó aktiválása előtt az intézményi felhasználónak rendelkeznie kell minősített szolgáltatótól származó szervezeti authentikációs tanúsítvánnyal, valamint annak publikus részét az aktiválás során az EESZT részére át kell, adnia.

Az átadás a publikus tanúsítvány .....@eeszt.gov.hu címre történő elküldésével lehetséges. A küldést megelőzően a tanúsítványt titkosítás nélkül **ZIP formátumban szükséges tömöríteni**, és a tömörített állományt kell a küldendő levél mellékletében elhelyezni.

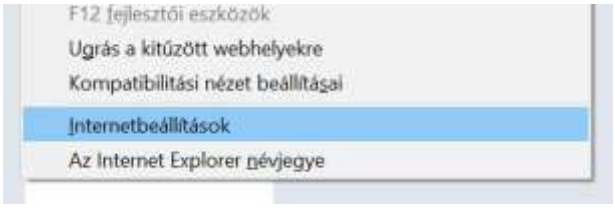
A publikus tanúsítvány a szolgáltató honlapjáról letölthető, vagy az igénylő gépen a Windows tanúsítványtárból ki-exportálható.

5.1 Publikus tanúsítvány exportálása

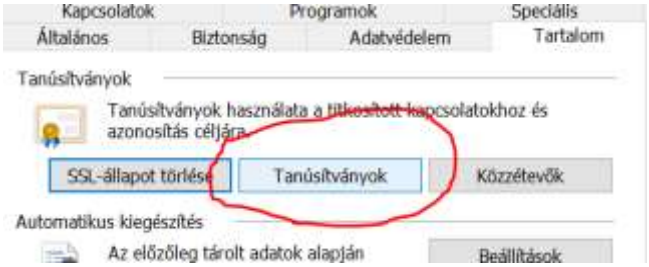
A publikus tanúsítvány exportjához az igénylő felhasználójával kell belépni az igénylés során használt számítógépre.

A Windows tanúsítványtár legegyszerűbben az Internet Explorerből jeleníthető meg:

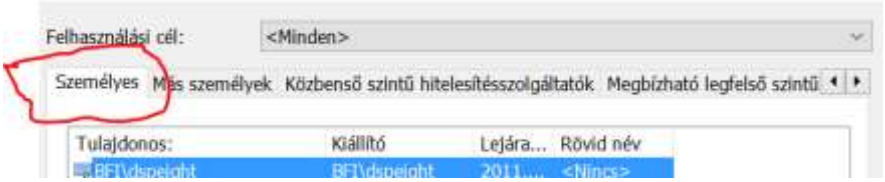
➔ Internet beállítások



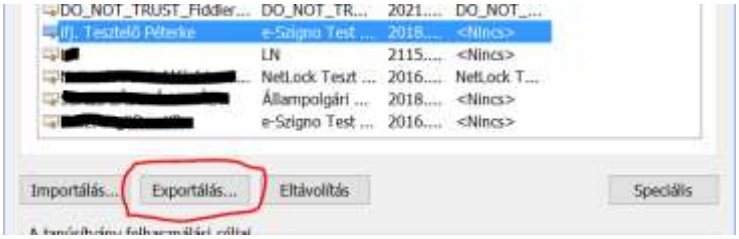
➔ Tartalom -> Tanúsítványok



Sikeres igénylést követően a tanúsítvány a megjelenített tanúsítványtár „Személyes” tanúsítványai között található meg:

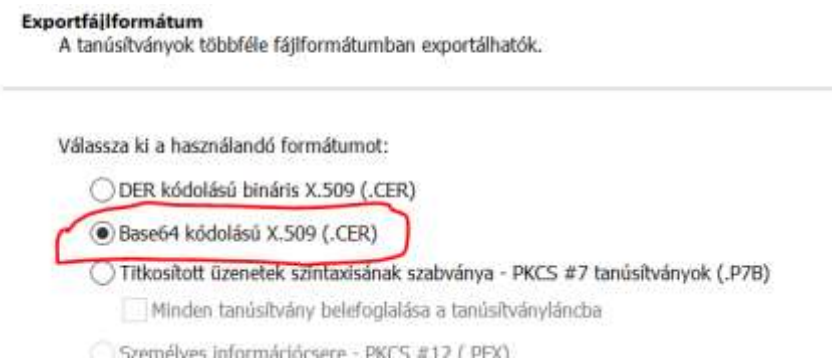


A tanúsítvány exportálása a tanúsítvány kiválasztásával az Exportálás gombra kattintással kezdhető meg:

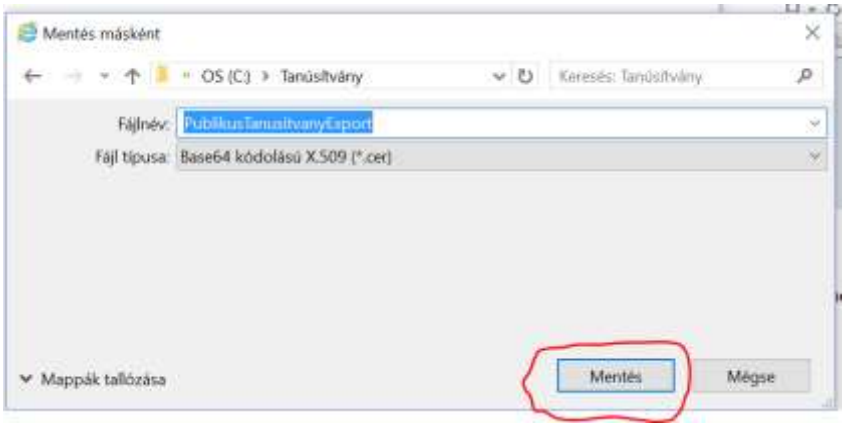


Fontos! Az exportálás során titkos kulcs NE kerüljön exportálásra

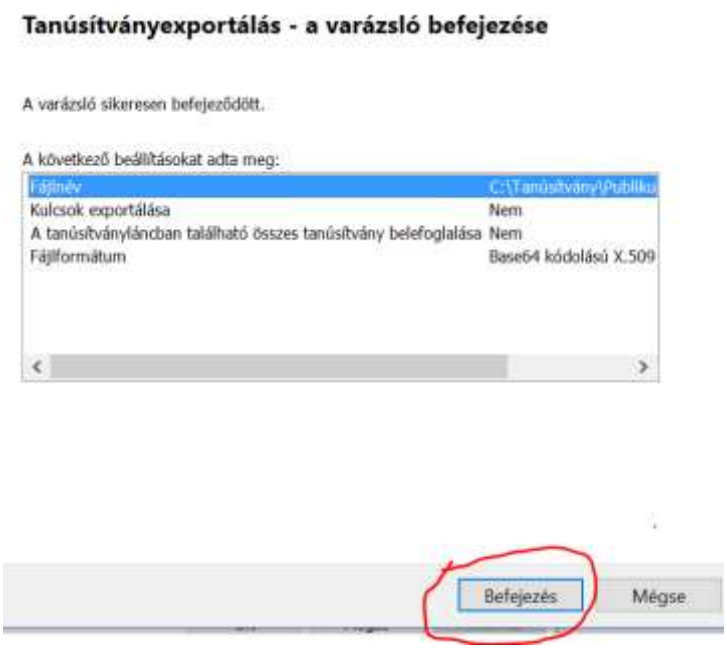
Az Exportfájl formátum kiválasztásánál válasszuk a Base64 kódolású X.509 formátumot.



Végül mentsük el az Exportált publikus tanúsítványt számítógépünkre.



A Varázslót a „Befejezés” gombra kattintva zárhatjuk be.



Következő lépésként tömörítsük az Exportált tanúsítványunkat titkosítás nélküli ZIP formátumba a küldéshez, ellenkező esetben a vírusirtók eltávolíthatják levelünk mellékletét. A tömörített publikus tanúsítványt levél mellékleteként továbbítsuk az ismertetett email címre.