Minősített szolgáltató által kiállított Authentikációs tanúsítvány igénylése intézményi felhasználók azonosítására

ESZFK
Egészséginformatikai
Szolgáltató és Fejlesztési Központ

Tartalom

1. Dokumentum célja

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

2. Intézményi felhasználó azonosítása

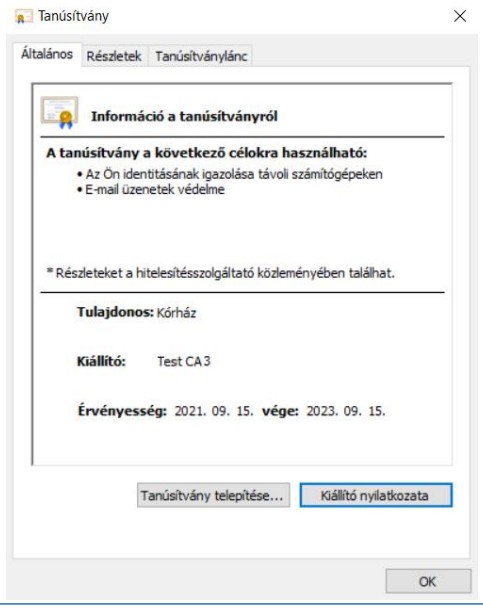
Amennyiben a csatlakozó rendszer Intézményi felhasználót is használ (Intézményi technikai felhasználó), abban az esetben tanúsítvánnyal kell azonosítani azt. Az EESZT-hez csatlakozó rendszereknek minősített szolgáltató által elektronikus authentikációra kiadott szervezeti tanúsítványt kell használniuk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

Az EESZT az Intézményi felhasználó létrehozása során „Fokozott biztonságú szervezeti Authentikációs Tanúsítvány" használatát követeli meg, mely tanúsítvánnyal az Intézményi felhasználó létrehozása előtt az egészségügyi intézménynek rendelkeznie kell, valamint annak publikus részét a felhasználó igénylése 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.

2.1. Tanúsítványok

Authentikációs Tanúsítványt megbízható, bevizsgált szervezet, úgynevezett hitelesítésszolgáltató állít ki természetes személyek vagy informatikai rendszerek részére. A tanúsítvány egyrészt annak a megnevezését tartalmazza, amely részre kiállították azt, másrészt olyan információkat tárol, amely segítségével mások biztonságosan - titkosítottan 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. Az említett 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 (titkosítottan vagy hitelesen) szeretnénk kommunikálni valakivel, be kell szereznünk a tanúsítványát. Ha mi szeretnénk neki titkos üzenetet küldeni, akkor egy hitelesítésszolgáltató honlapján (tanúsítványtárában) kereshetjük meg az ő tanúsítványát. Ha ő már üzent nekünk, akkor üzenete vagy aláírása általában tartalmazza a tanúsítványt. Ha megszereztük a tanúsítványt, ellenőriznünk kell, hogy valóban érvényes-e, illetve célszerű megnézni, hogy valóban annak a neve szerepel-e benne, akivel kommunikálni szeretnénk.

2.2. Authentikáció – avagy biztonságos azonosítás

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

Ez általában az alábbi elvek szerint történik:

1. Megszerezzük a másik fél tanúsítványát, és meggyőződünk a tanúsítvány érvényességéről. Így hitelesen hozzájutottunk a tanúsítványba foglalt nyilvános kulcshoz, és 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 le, hogy a másik fél helyesen válaszolt-e kihívásunkra: 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.

3. Authentikációs tanúsítvány igénylése

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

A tanúsítványok igénylése jellemzően interneten keresztül, online felületen történik a szolgáltatók honlapján található ismertetőknek megfelelően. A szolgáltatók online felületei, illetve az igénylés menetéről egyéb információk az alábbi linkeken érhetők el:

- **Netlock Kft.**

  https://www.netlock.hu

- **Microsec Zrt.**

  https://www.e-szigno.hu

- **NISZ Zrt.**

  https//www.hiteles.gov.hu

A NetLock Kft., illetve a Microsec Zrt. szolgáltatók 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 exportálható és bármely más számítógépre átvihető.

Kiemelten fontos, hogy az igénylés során a tanúsítványban feltüntetendő adatok megadásánál kerülni kell a „(” és a „)” karaktereket!

3.1. NetLock szoftveres Authentikációs Tanúsítvány igénylése

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

„C osztályú szervezeti Authentikációs Tanúsítvány”

Tanúsítvány igénylésének lépései:

1. ***Indítsa el az Internet Explorer böngészőt!***
2. ***Látogasson el a http://www.netlock.hu oldalra!***
3. ***Bejelentkezést követően nyissa le a „Tanúsítványok igénylése” menüpontot, majd válassza a „Nem minősített tanúsítvány igénylése” almenüpontot!***
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 létrehozott 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 tanúsítvány igénylésével kapcsolatosan részletes ismertetőt a szolgáltató honlapján talál.

3.2. Microsec szoftveres Authentikációs Tanúsítvány igénylése

A Microsec Zrt. választása esetén az igénylendő tanúsítvány 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” mezőbe az igénylő szervezet nevét kell megadni!

Az igénylés menetéről részletesen a szolgáltató honlapján talál információkat.

4. Tanúsítvány átadása az EESZT-nek

Ahhoz, hogy az Intézményi felhasználó megfelelően működjön, az intézménynek rendelkeznie kell minősített szolgáltatótól származó szervezeti authentikációs tanúsítvánnyal, melynek publikus részét elektronikus úton meg kell küldeni az EESZT felé, a következő e-mail címre:

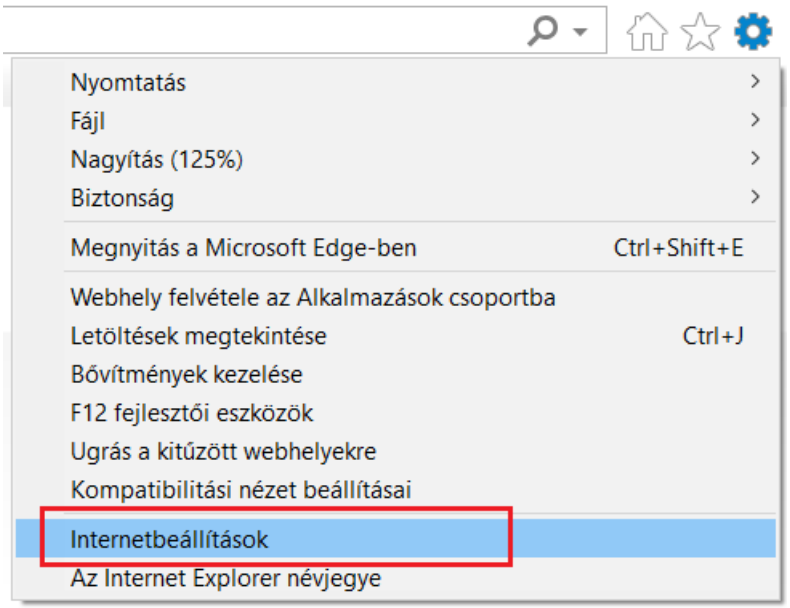
jogosultsag.eeszt@eszfk.hu

A küldést megelőzően a tanúsítványt titkosítás nélkül, ZIP formátumban szükséges tömöríteni, és a tömörített állományt kell a küldendő levél mellékletében elhelyezni. A publikus kulcs a szolgáltató honlapjáról letölthető, vagy az igénylő gépen a Windows tanúsítványtárból exportálható.

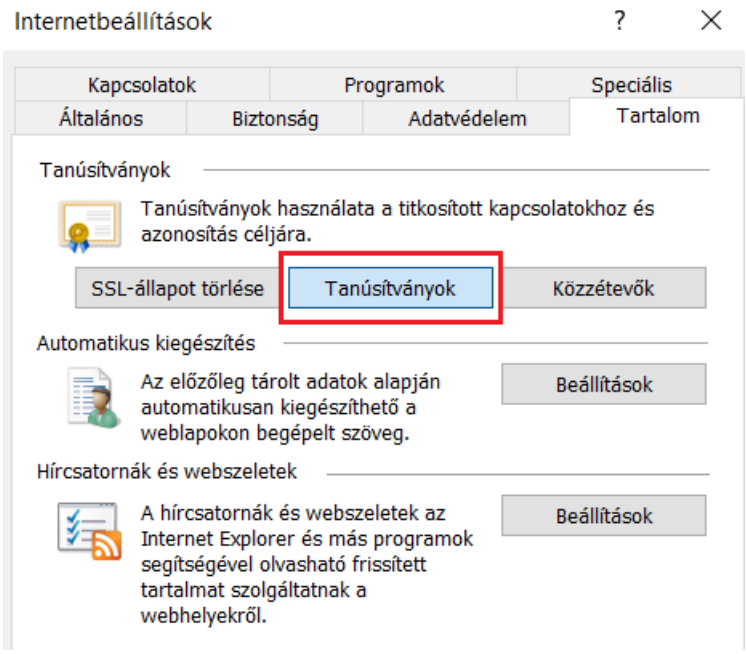
4.1. Publikus tanúsítvány exportálása

A publikus tanúsítvány exportjához az igénylő felhasználójával kell belépni az igénylés során használt számítógépre. A Windows tanúsítványtár legegyszerűbben az Internet Explorerből jeleníthető meg.

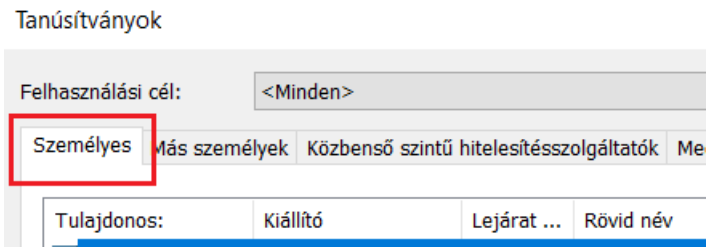
1. ***Az Internet Explorer jobb felső sarkában található fogaskerék ikonra kattintva válasszuk ki az „Internetbeállítások”-at!***



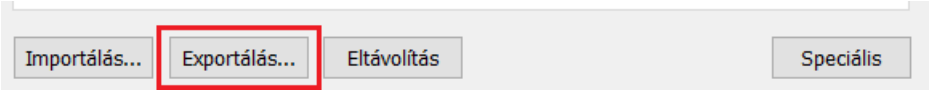
2. ***A megnyíló ablakban a „Tartalom” fül alatt található „Tanúsítványok” gombra kell kattintani.***



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

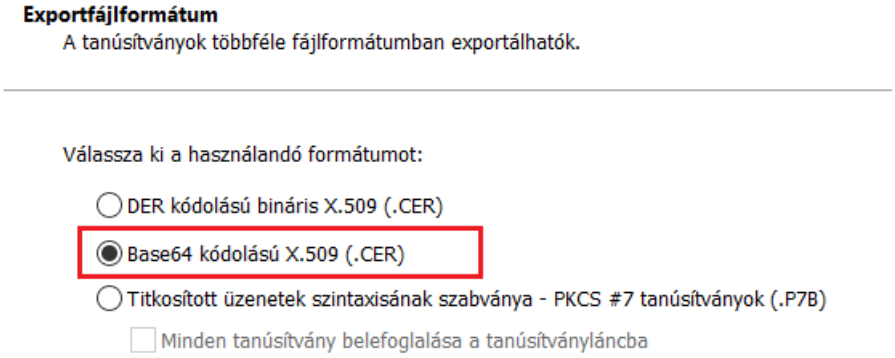


3. ***A tanúsítvány exportálása a tanúsítvány kiválasztásával az „Exportálás” gombra kattintáva kezdhető meg.***



4. ***FONTOS: Az exportálás során titkos kulcs NE kerüljön exportálásra!***

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



6. ***Végül mentsük el az Exportált publikus tanúsítványt számítógépünkre!***

7. ***A Varázslót a „Befejezés” gombra kattintva zárhatjuk be.***

Ezek után tömörítsük az exportált tanúsítványunkat titkosítás nélküli ZIP formátumba a küldéshez, ellenkező esetben a vírusirtók eltávolíthatják levelünk mellékletét!

A tömörített publikus tanúsítványt elektronikus levél (e-mail) mellékleteként kell továbbítani az Intézményi felhasználói fiók igénylőlappal együtt, az alábbi címre:

jogosultsag.eeszt@eszfk.hu