

Külső elektronikus „MALE” aláíró eszközök használatának beállítása az eFOKI rendszerben

eFOKI 4.1.49.0 verziótól

Tartalomjegyzék

1. A munkaállomás (laptop) felkészítése a külső eszközzel történő elektronikus aláírásra	3
1.1. Az elektronikus aláíró eszközök telepítése.....	3
1.2. eFOKI aláírás kezelő program üzembe helyezése.....	3
1.2.1. eFOKI aláírás kezelő program beállítása	3
1.3. Az eFOKI rendszer elektronikus aláírás adatainak beállításához szükséges nyilvános kulcs előállítása6	
1.3.1. E-Személyi igazolvány nyilvános kulcs előállítása	6
1.3.2. Microsec Telefonos távoli eszköz nyilvános kulcs előállítása	7
2. Az eFOKI felkészítése a külső eszközzel történő elektronikus aláírásra	10
2.1. Jogosultság beállítás az „Elektronikus aláírás adatok” rögzítésére.....	10
2.2. „Elektronikus aláírás adatok” rögzítése.....	11
3. Elektronikus aláírás használata.....	14
3.1. E-személyi igazolvány.....	14
3.1.1. E-személyi igazolvánnyal történő aláírás előtti ellenőrzés.....	14
3.1.2. Aláírás eFOKI-ban fizikai MALE eszközökkel (token, kártyaolvasó, e-személyi).....	15
3.2. Aláírás eFOKI-ban Microsec telefonos távazonosítással.....	17
3.2.1. Aláírás előtti ellenőrzés:	17

1. A munkaállomás (laptop) felkészítése a külső eszközzel történő elektronikus aláírásra

FONTOS!

Az eFOKI rendszeren belüli MALE eszközökkel történő elektronikus aláírás csak Windows operációs rendszerek esetében támogatott!

1.1. Az elektronikus aláíró eszközök telepítése

Kártyás vagy token-es tanúsítvány esetén a hitelesítés szolgáltató előírásainak megfelelően végezzük el a telepítést a munkaállomásra, vagy laptopra.

- Kártyaolvasó vagy token driver telepítése
- Kártya driver telepítése
- A hitelesítés szolgáltató aláíró software telepítése

Ellenőrizzük, hogy az aláíró kártya az előírásoknak megfelelően működik-e az eredeti környezetben.

Telefonos applikációra alapozott aláíró tanúsítvány esetében a telepítést szintén a szolgáltató előírásainak megfelelően végezzük el és próbáljuk ki.

A „Tanúsítványkezelő” -ben ellenőrizzük, hogy megfelelően látható-e telefonos applikáció esetében a távoli kulcsmenedzsment szolgáltatások között az aláíró tanúsítvány. A kártyás vagy token-es megoldás esetén a „Tanúsítványkezelő” -ben látható-e a kártya és a kártyán elhelyezett tanúsítványok. Amennyiben a munkaállomáson vagy laptopon már tudunk aláírni, akkor célszerű az eFOKI beállításokat elkezdeni.

1.2. eFOKI aláírás kezelő program üzembe helyezése

eFOKI aláírás kezelő program letöltése, telepítése (MALE eszközkészlet letöltése és telepítése). (MALE = Minősített elektronikus aláírás és minősített elektronikus bélyegző létrehozó eszközök)

A <https://efoki.hu> weboldalon válasszuk ki a „**Motorháztető alatt**” menüpontot és itt kattintsunk a „**Letölthető anyagok**” almenüre. Ezen az oldalon keressük meg az „**eFOKI aláírás kezelő program**” -ot.

Ebből a menüpontból töltsük le a „SAS.RemoteSign” zip-et. Ez a tömörített állomány kerüljön kitömörítésre és a kapott „SAS.RemoteSign” könyvtárat helyezzük el az általunk kiválasztott helyre. Célszerű például abba a könyvtárba rakni, amelyikben az eFOKI Scanner könyvtár is helyet kapott, ha az adott eszközön használnak vonalkódos rendszert. Természetesen ez a könyvtár a számítógépen bárhol lehet – csak legyen megtalálható később is. A „SAS.RemoteSign” könyvtárban található egy futtatható állomány „SAS.RemoteSign.exe” néven. Ez a program kapcsolja össze a MALE eszközöket az eFOKI-val. A „SAS.RemoteSign.exe” nem igényel telepítést csak futtatást, ezért érdemes a rendszerrel együtt indítandó feladatot erre létrehozni, hogy a gép bekapcsoláskor automatikusan induljon el, és ha nem muszáj, ne kelljen kézzel indítgatni.

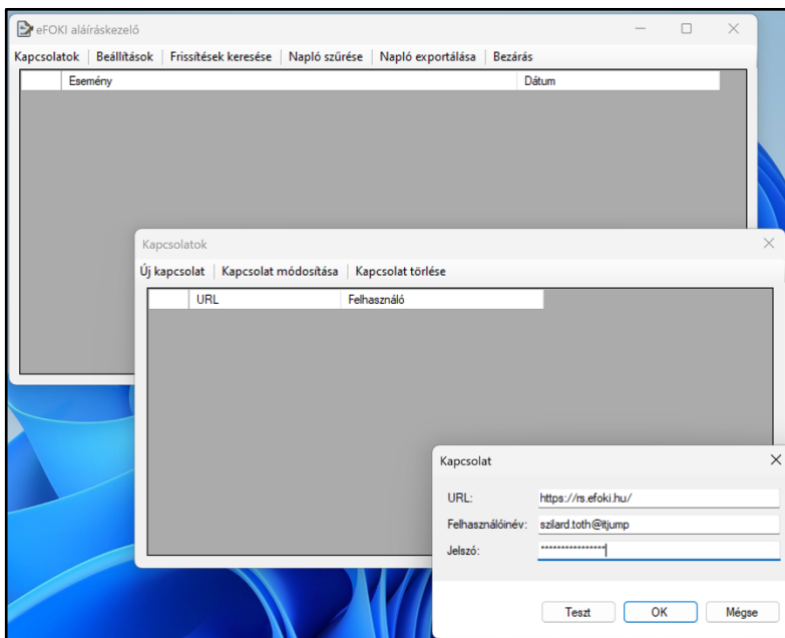
1.2.1. eFOKI aláírás kezelő program beállítása

A „SAS.RemoteSign.exe” indításával elindul az **eFOKI aláírás kezelő** program, amelyet az első alkalommal szükséges beállítani.



Kattintsunk a Kapcsolatok fülre, ezt követően a megjelenő ablak nyújt lehetőséget arra, hogy az eFOKI felhasználó számára engedélyezzük a külső aláíróeszközzel történő kapcsolatfelvételt.

Azaz, ha egy gépen több aláírókártyát használ egy személy, akkor az ő aláírási jogához egy kapcsolat elegendő, de ha egy a gépen lévő telepített külső aláíró eszközt azon a gépen több felhasználó is kezel, abban az esetben mindkettő vagy több felhasználónak önálló kapcsolatfelvételre lesz szüksége. Ez abban az esetben fordulhat elő például, ha az adott irodában van egy, az elektronikus aláírásra dedikált gép, és akinek hitelesítenie kell, az ezt a dedikált számítógép használatával teheti meg.

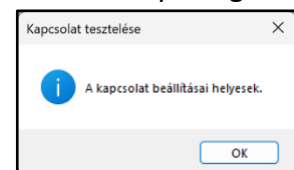


Ha egy személy több egymástól független és más felhasználónévvel rendelkező adatbázisba való belépési joggal rendelkezik, akkor mindegyik adatbázishoz szükséges önálló kapcsolatot felvennie.

A kapcsolat adatok kitöltése során a központi URL megadását követően meg kell adnunk az eFOKI felhasználónevünket, és az eFOKI felhasználónevünkhöz tartozó jelszót.

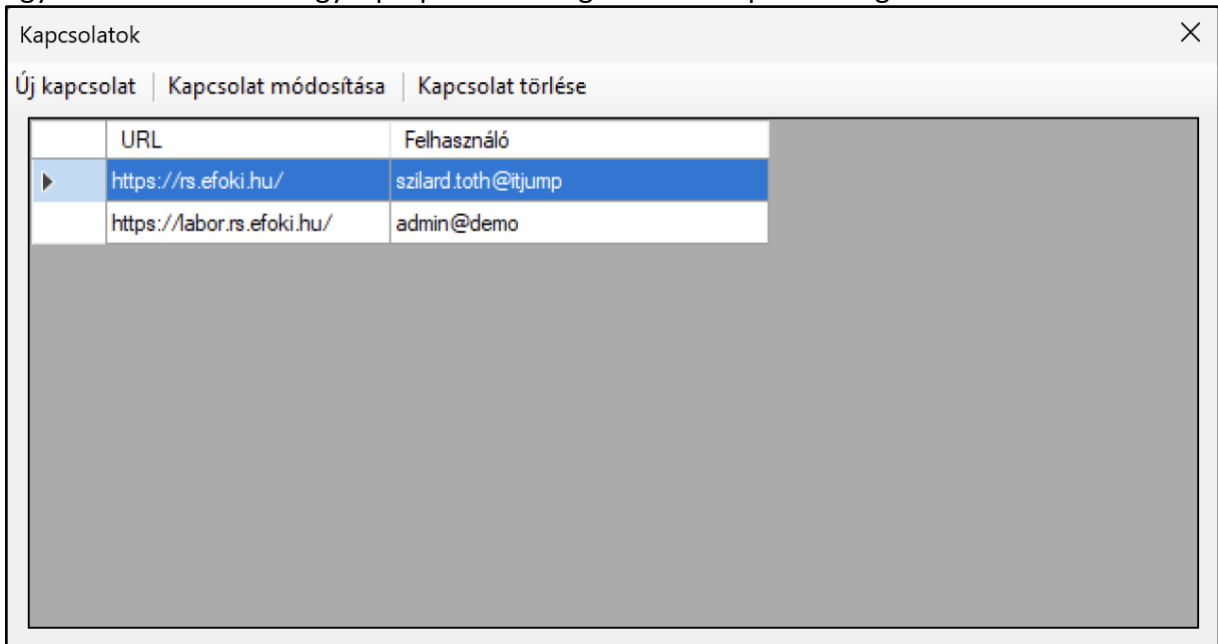
A **Teszt** nyomógomb

megnyomása során az **eFOKI aláírás kezelő** program ellenőrzi az URL helyességét és a felhasználónév és jelszó páros megfelelőségét. Amennyiben minden adat helyes, a felhasználó egy erre utaló pozitív üzenetet kap egy felugró ablakban. Amennyiben a beállított adatok bármelyike hibás, a felugró ablak tartalma a következő tájékoztatást



adja: „A szerverkapcsolat beállításai hibásak.” A felugró ablakon az OK nyomógombra kattintva javíthatjuk az adatokat.

Egy munkaállomáson vagy laptopon tetszőleges számú kapcsolat rögzíthető.

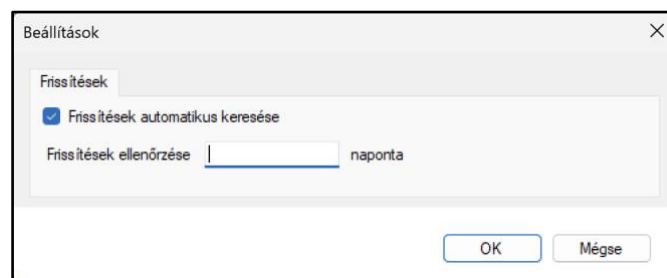
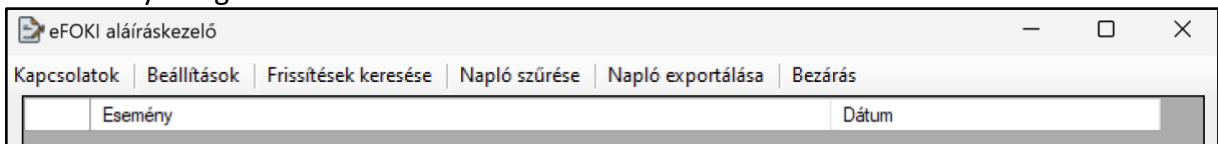


FONTOS!

Fontos figyelemmel lenni arra, ha valaki, akinek már rögzített kapcsolata van az **eFOKI aláírás kezelő** programban és az eFOKI belépéskor elfelejtett jelszót kér, az új jelszó beállítását követően az **eFOKI aláírás kezelő** programban a Kapcsolatok fülön is helyesbítenie kell a jelszavát.

Fontos figyelembe venni, hogy egy felhasználó szervezettől való távozás esetén célszerű és szükséges az eFOKI rendszerben a felhasználó jogainak megszüntetése. A felhasználó törlése során javasolt a beállított kapcsolatok törlése is az általa használt eszközön.

Az **eFOKI aláírás kezelő** programban a Beállítások fülön megadható a program automatikus frissítésének ütemezése, de a program frissítése manuálisan is elvégezhető a Frissítések keresése nyomógomb használatával.



A frissítés keresés ütemezése

1.3. Az eFOKI rendszer elektronikus aláírás adatainak beállításához szükséges nyilvános kulcs előállítása

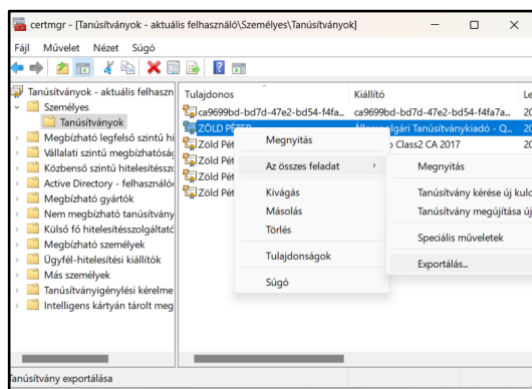
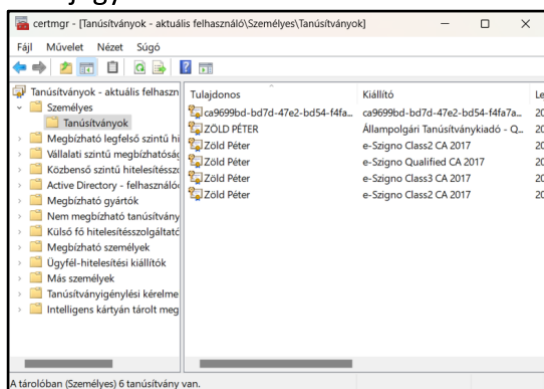
A használni kívánt aláíró kártya nyilvános kulcsának exportálása során egy cer kiterjesztésű file létrehozását végezzük el.

pl:

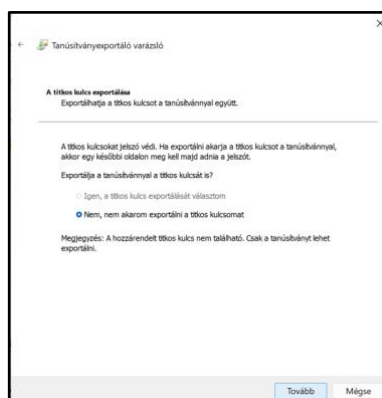
- Toth_Szilard_MSEC_Token.cer, - Microsec token-es aláíró tanúsítvány nyilvános kulcsa
- Toth_Szilard_eSZEM_Card.cer – E-személyi igazolvány aláíró tanúsítvány nyilvános kulcsa

1.3.1. E-Személyi igazolvány nyilvános kulcs előállítása

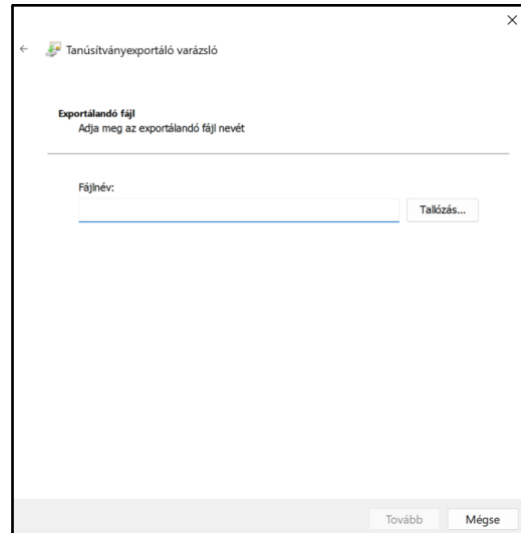
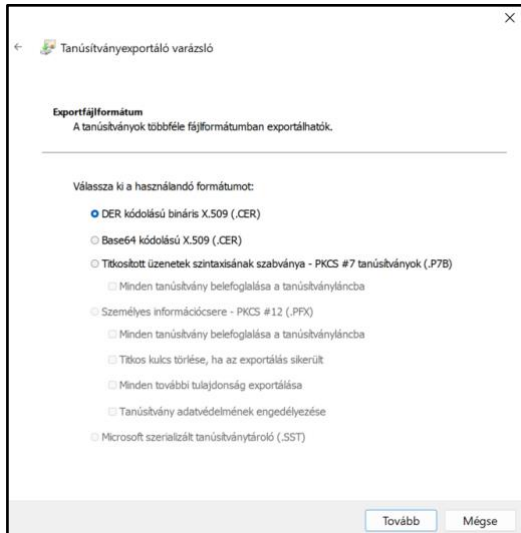
1. Windows kereséssel keressük a „Felhasználói Tanúsítványok kezelése” folyamatot (vezérlőpult elem) és indítsuk el.
2. A személyes tanúsítványok között a listában szerepelni fog egy olyan tanúsítvány, ahol a személyi igazolvány tulajdonosának neve és az „Állampolgári Tanúsítványkiadó...” kifejezés szerepel. Ez az e-személyiben található tanúsítvány tanúsítványtárban megjelenő bejegyzése.



Készítsünk egy exportot erről a tanúsítványról

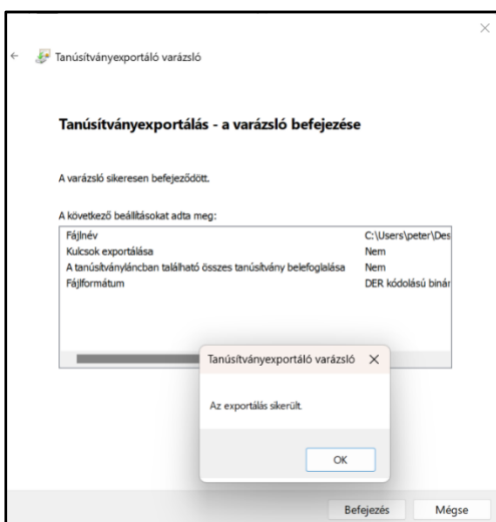
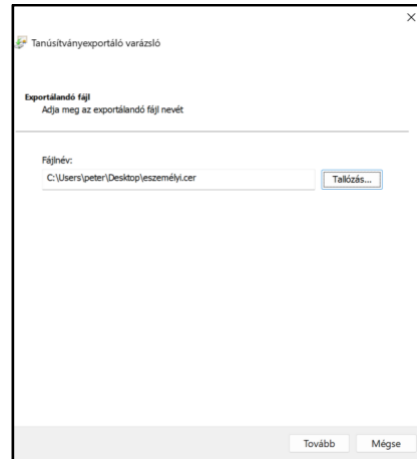
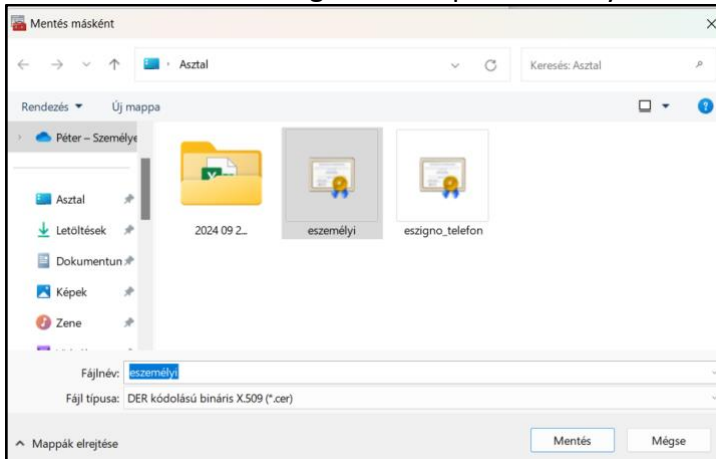


Mivel a titkos kulcs az e-személyiben található, a tanúsítványtárból csak titkos kulcs nélküli tanúsítvány exportálható.



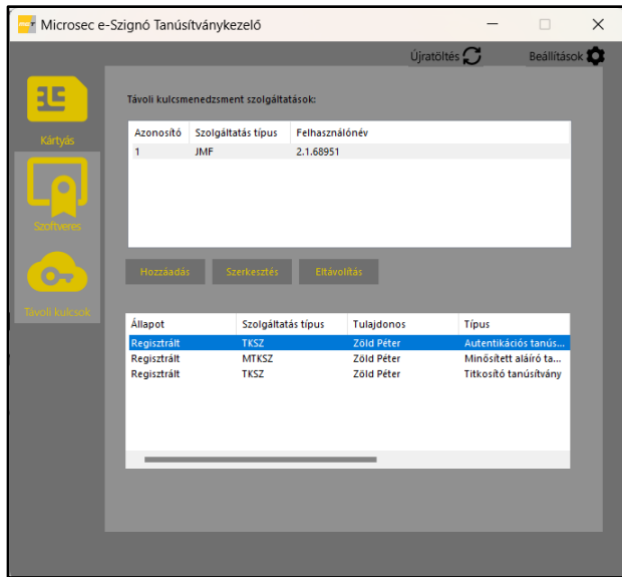
Kódolás tekintetében akár a DER, akár a BASE64 választható, az eFOKI mindkettőt képes kezelni.

Tallózással érdemes megadni az exportálás helyét.



1.3.2. Microsec Telefonos távoli eszköz nyilvános kulcs előállítás

A számítógépen telepíteni kell a Microsec által kiadott tanúsítvány kezelő szoftvert (MET).



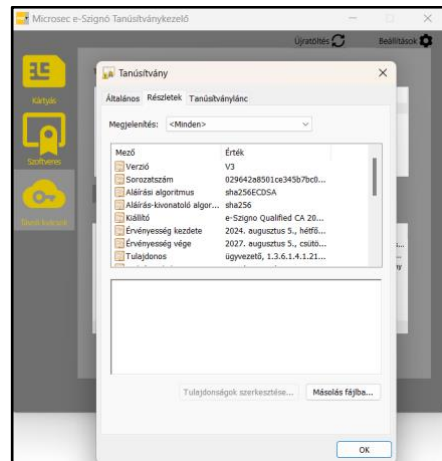
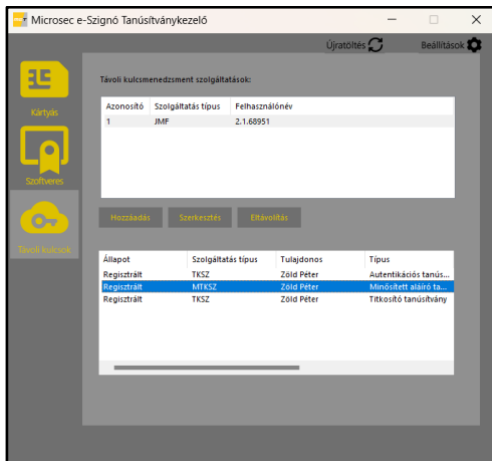
Minden a Microsec által kiadott tanúsítvány ebben a szoftverben kezelhető, legyen az akár szoftveres vagy MALE eszközös.

A mobiltelefonra le kell tölteni a Microsec aláíró alkalmazását.

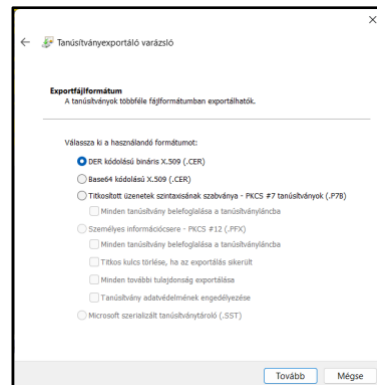
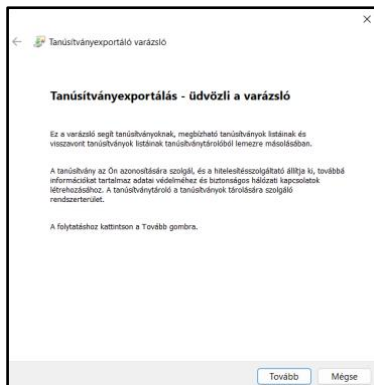


A Microsec pontos leírást ad, hogy melyik tanúsítványt hogyan kell üzembe helyezni, valamint hogyan kell a mobiltelefonos alkalmazást összekapcsolni a számítógépre telepített tanúsítvánnyal.

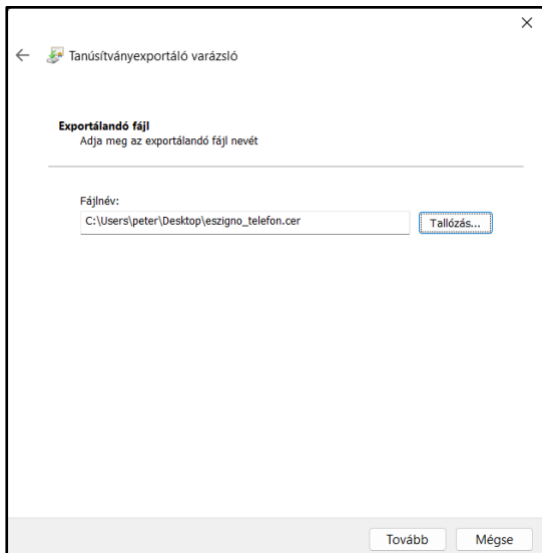
Exportálni kell a MET-ből a tanúsítványt.



A távoli kulcsok közül választjuk ki az aláíró tanúsítványt és nyissuk meg megtekintésre. A részletek fülön található Másolás fájlba... gomb segítségével indítsuk el az exportálást.

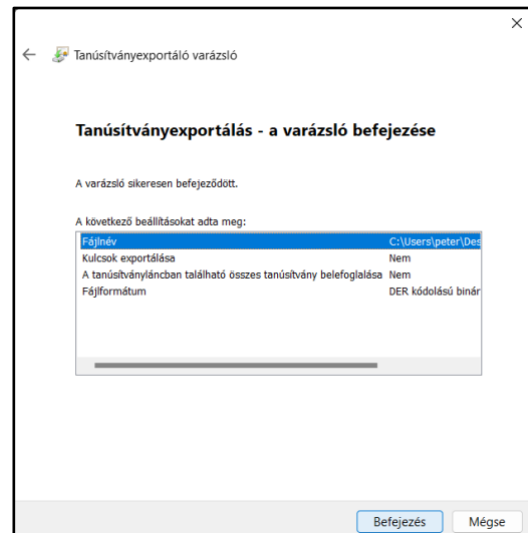


Akár a DER, akár a Base64 kódolás megfelelő lehet, az eFOKI mindkettőt fogadja.



Tallózással válasszuk ki a mentés helyét.

Az elmentett CER fájl beparaméterezése az eFOKI-ban ugyanúgy történik, mint az e-személyi tanúsítvány esetén.



Befejezés és kész.

2. Az eFOKI felkészítése a külső eszközzel történő elektronikus aláírásra

Az eFOKI rendszer esetében több lépést kell elvégezni ahhoz, hogy egy adott felhasználó a saját vagy adminisztrátorként a szervezet több munkavállalójának tudjon elektronikus aláírási jogot biztosítani.

2.1. Jogosultság beállítás az „Elektronikus aláírás adatok” rögzítésére

Ahhoz, hogy egy felhasználónak elektronikus aláírást tudjunk beállítani vagy közvetlenül a felhasználónak vagy az adminisztrációs beállításokkal megbízott személynek kell jogosultságot biztosítani arra, hogy elektronikus aláírás adatokat tudjon rögzíteni.

Ehhez válasszuk ki a „Rendszeradminisztráció” menüpontban azt a felhasználói csoportot, akinek ezt a jogot meg kívánjuk adni. A felhasználói csoport módosítás ikonjával belépve az engedélyek fülön válasszuk ki a „Rendszeradminisztráció” menüpontot. Ezen belül válasszuk ki az „Elektronikus aláírás adatok” sort és a szervezeten belül meghatározott jogosultságot adjuk meg a kiválasztott csoportnak.

Amennyiben egy kulcsfelhasználóhoz rendeljük az aláírások beállításának jogát, akkor célszerű neki teljes körű jogosultságot adni és figyelni rá, hogy rajta kívül senki ne férjen hozzá az „Elektronikus aláírás adatok” menüponthoz.

	Listázás	Megtekintés	Új felvétel	Módosítás	Törlés	Összes	
Adat szintű napló	●	●	●	●	●	○	⌵
Adatimportok lekérdezése	●	●	●	●	●	○	⌵
Automatikus email postafiók feldolgozások	●	●	●	●	●	○	⌵
Bejelentő űrlap beállítások	●	●	●	●	●	○	⌵
Cégek-Hivatali kapu gépi kapcsolat beállítások	●	●	●	●	●	○	⌵
Egyedi mezők	●	●	●	●	●	○	⌵
Elektronikus aláírás adatok	●	●	●	●	●	●	⌵

Például, ha van egy „Ügyvezetők” felhasználói csoportunk és számukra úgy szeretnénk engedélyt adni, hogy mindenki csak a saját elektronikus aláírását állíthatja be, akkor az engedély sorban a következő beállítást alkalmazzuk:

Elektronikus aláírás adatok	⚠	⚠	⚠	⚠	✖	✖	⌵
-----------------------------	---	---	---	---	---	---	---

Ebben az esetben minden felhasználó, aki ebbe a csoportba tartozik, csak és kizárólag a saját elektronikus aláírás adatait tudja beállítani.

A jogokon kívül (minden esetben) szükséges és célszerű engedélyezni a nem kötelező mezőket az engedélyezésre kerülő „Elektronikus aláírás adatok” menüponthoz. Ezt a sor végén látható négyzethálóra kattintva tehetjük meg.

⌵ Nem kötelező mezők engedélyezési ikonja

Mezők viselkedése ✕

- Összes
- Cím
- Helyszín
- Készítő
- Kulcsszavak
- Létrehozó
- Ok
- Szerző
- Tárgy

Tiltott
 Csak olvasás
 Módosítás

Az ikonra kattintva az elektronikus aláírásához kapcsolódó metaadatok megjelenése és azok használatának meghatározása állítható be az „Elektronikus aláírás adatok” menüponthoz.

2.2. „Elektronikus aláírás adatok” rögzítése

Az arra jogosultsággal rendelkező felhasználók az eFOKI rendszer főmenüjében, a „Rendszeradminisztráció” menüponthoz megtalálják az „Elektronikus aláírás adatok” almenüpontot. Erre kattintva a jogosultság típusának megfelelően láthatják a már rögzített elektronikus aláírás adatokat, amelyeket módosíthatnak vagy törölhetnek, továbbá új elektronikus aláírás adatokat rögzíthetnek.

A Kézikönyvben bemutatott minősített vagy minősített tanúsítványra alapuló, fokozott biztonságú szoftveres tanúsítvány telepítésénél bemutatott kitöltés tekintetében csak a különbségeket mutatjuk be.

Elektronikus aláírás adatok

Alapadatok
Dokumentumok 0

Alapadatok

Megnevezés *

Cég * Felhasználó * Jelleg *

Típus *

A **Megnevezés** mezőben célszerű a megnevezést úgy meghatározni, hogy a megfelelő aláírás gyorsan és egyszerűen kiválasztható legyen.

Például:

- „**Tóth Szilárd MSEC ügyvezető Itjump**” itt jeleztem a személyt, a tanúsítvány kiállítóját, továbbá azt, hogy ez egy céghez kötődő és a szervezeten belül betöltött pozícióhoz kapcsolódó elektronikus aláírás.
- „**Tóth Szilárd Netlock Itjump**” itt jeleztem a személyt, a tanúsítvány kiállítóját, továbbá azt is, hogy ez egy céghez kötődő, de pozíciót nem tartalmazó aláírás, tehát a cég nevében aláírhatok, akár ügyvezetőként, akár felszámolóbiztosként.
- „**Tóth Szilárd e_személyi**” itt jeleztem, hogy ez az aláírás sem szervezethez, sem pozícióhoz nem kötődik, a természetes személyt azonosítja.

A **Felhasználó mezőben** kiválaszthatom azt a felhasználót, akinek joga lesz az eFOKI-ban ezzel az aláírással aláírni. Ez természetesen alapértelmezetten az a személy, aki a tanúsítvány tulajdonosa. Speciális helyzetben ezt a jogot a tanúsítvány tulajdonosa minden jogalapot nélkülözve ruházhatja csak át más személyre.

A **Jelleg** aszerint választandó ki, hogy a beállítani kívánt tanúsítvány személyhez kötődik-e, vagy csak szervezethez – azaz szervezeti bélyegző vagy hitelesítésre alkalmas személyt azonosító elektronikus aláíró tanúsítvány.

Típus: legördülő menü, amely esetében a külső eszköz választandó:

SW aláíró tanúsítvány használata

✓ Külső eszköz (kártya, token, távoli tanúsítvány) használata

Az „Elektronikus aláírás adatok” következő rovata a tanúsítvány rovat, amely szintén kardinális különbséget mutat a külső eszköz beállítás és a szoftveres tanúsítvány beállítása között.

Tanúsítvány

Tanúsítvány

Tanúsítvány 🗑️

A külső eszköz esetében nincs mód a tanúsítvány jelszavak megadására és mentésére sem. Továbbá itt nem „**px**” típusú magánkulcsot, hanem „**cer**” típusú nyilvános kulcsot csatolunk, amelyet az előkészítés során tanúsítvány exportálással állítottunk elő.

A többi rovat kitöltése teljes mértékig megegyezik a szoftveres tanúsítvány esetében leírtakkal.

Időbélyegző szervert adatai

Alapértelmezett időbélyegző szervert használata *

Igen

Bélyegző kép adatai

Bélyegző kép

Bélyegző kép



Elhelyezkedés

Első oldal

Horizontális origó

Jobb oldal

Vertikális origó

Alsó rész

Horizontális eltolás

Vertikális eltolás

Metaadatok

Ok

Helyszín

Szerző

Cím

Tárgy

Kulcsszavak

Készítő

Létrehozó

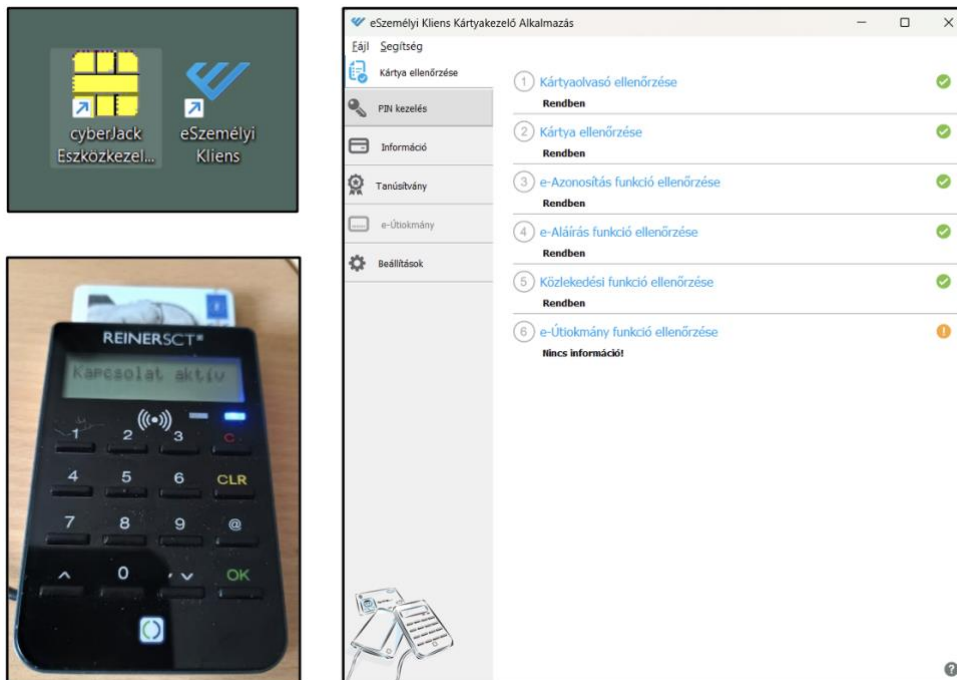
3. Elektronikus aláírás használata

3.1. E-személyi igazolvány

3.1.1. E-személyi igazolvánnyal történő aláírás előtti ellenőrzés

3.1.1.1. e-Személyi aláíró képességének ellenőrzése

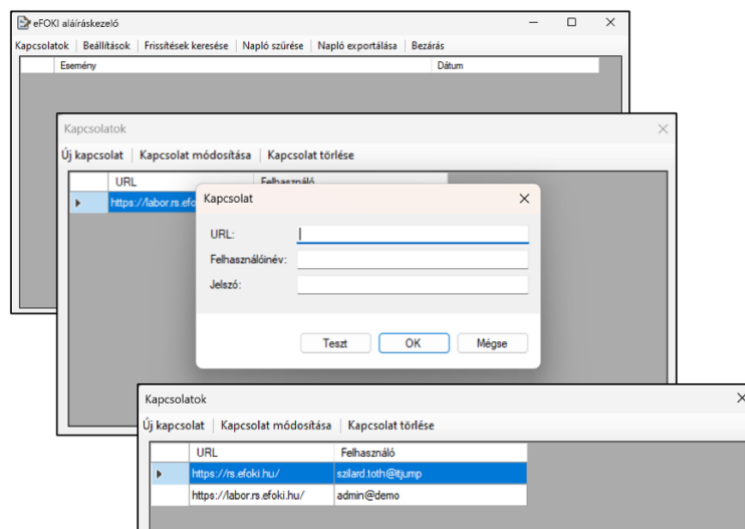
Első lépésként győződjünk meg róla, hogy az e-személyi használatához szükséges alkalmazások telepítve vannak és lehetséges az aláírás az e-személyivel a szolgáltató által előírt módon.



Győződjünk meg róla, hogy a személyi igazolvány aláírásra kész

3.1.1.2. eFOKI aláíráskezelő alkalmazás működésének ellenőrzése

Ellenőrizzük, hogy fut-e, azaz működik-e a gépünkön helyileg futtatott és az 1.2 fejezetben leírt módon letöltött és beállított eFOKI aláíráskezelő alkalmazás.



Ellenőrizzük, hogy létre lett-e hozva a megfelelő felhasználó részére a kapcsolat az eFOKI aláíráskezelő alkalmazásban (ha nem, akkor hozzuk létre).

3.1.1.3. Elektronikus aláírás adatok beállítása az eFOKI rendszeradminisztráció menüpontban

Feltételezzük, hogy az Aláírás létrehozása eFOKI-ban megtörtént az „Elektronikus aláírás adatok” rögzítése 2.2 fejezetben leírtak szerint.


3.1.2. Aláírás eFOKI-ban fizikai MALE eszközökkel (token, kártyaolvasó, e-személyi)

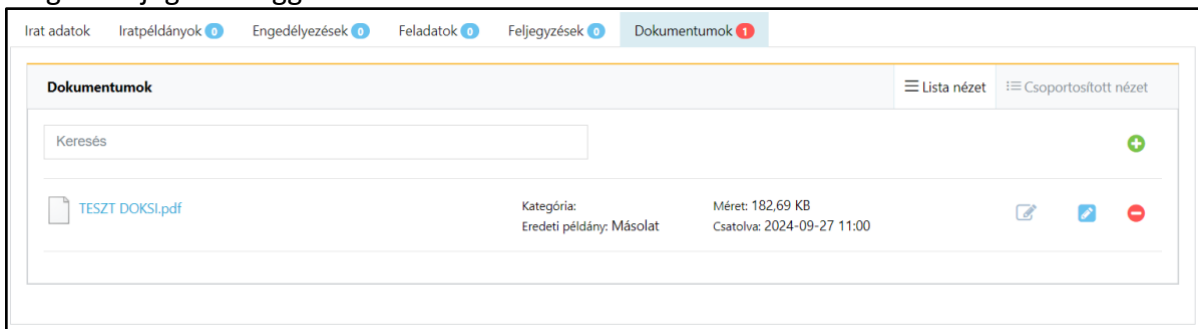
Előfeltételek: (előző fejezetekben részletesen leírva)

- MALE (minősített aláíró eszközök működőképességének ellenőrzése a munkahelyen)
- eFOKI aláíráskezelő fut-e a háttérben
- a számítógép tanúsítványtárában az e-személyi tanúsítvány regisztrálva van-e
- eFOKI rendszerben a felhasználó részére létrehozásra került az elektronikus aláírás beállítása

3.1.2.1. Iktató felület használata az aláírásra

Hozunk létre iktatást, vagy bármely képernyőn, ahol dokumentum csatolásra van lehetőség, csatoljuk be az aláírandó PDF állományt, illetve, ha már csatolásra került, akkor keressük meg.

Az iktatás dokumentumok képernyőn található a hitelesítésre szolgáló  ikon, amely lehetővé teszi a PDF dokumentumok hitelesítését, amennyiben a bejelentkezett felhasználó rendelkezik megfelelő jogosultsággal.



PDF aláírása gombra kattintva megjelennek az elérhető aláírások.

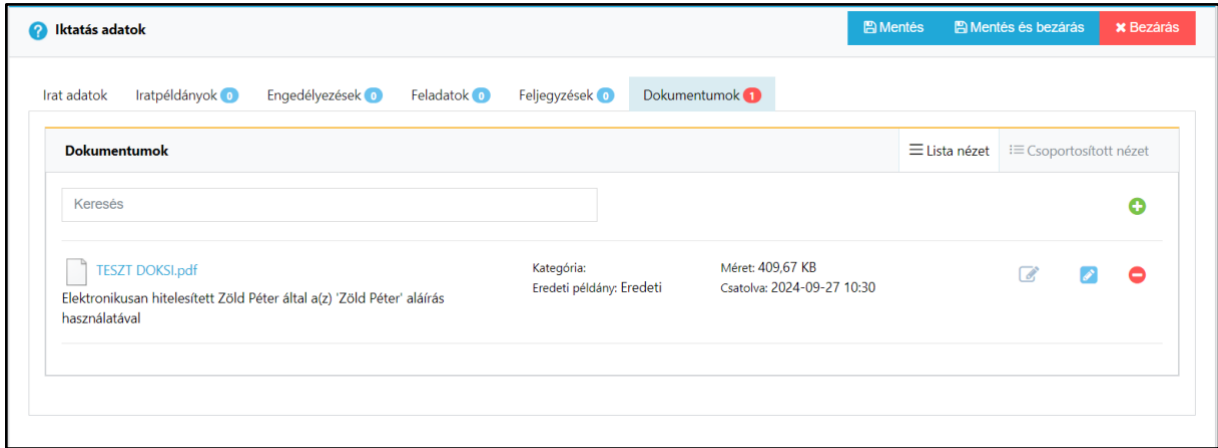


Válasszuk ki az e-személyihez kapcsolódó aláírást.

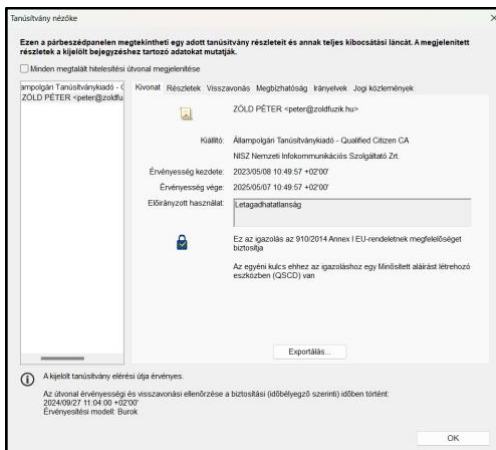
Megjelenik a képernyőn a felhívás, hogy a kártyaolvasó billentyűzetén adja meg a PIN kódot.

Adjuk meg a PIN kódot a kártyaolvasón.

A számítógép képernyőjén eltűnik a felhívó felirat és létrejön az aláírás. A hitelesítés során a dokumentum metaadatai megváltoznak a rendszerben és „másolat” helyett „eredeti” státuszt vesz fel. A metaadatok közé bekerül, hogy melyik felhasználó hitelesítette és milyen hitelesítési eszközt használt, szervezeti bélyegzőt vagy személyhez kötött elektronikus aláírást.



A dokumentumban a hitelesítés letöltés után az Acrobat Readerrel ellenőrizhető:




3.2. Aláírás eFOKI-ban Microsec telefonos távazonosítással

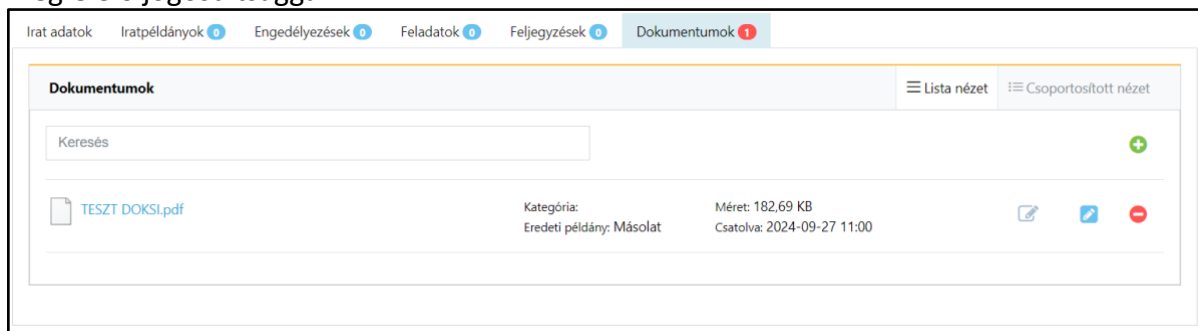
3.2.1. Aláírás előtti ellenőrzés:

- eFOKI aláíráskezelő fut a háttérben
- a MET alkalmazás fut a számítógépen
- a számítógép tanúsítványtárában az e-személyi tanúsítvány regisztrálva van-e
- eFOKI rendszerben a felhasználó részére létrehozásra került az aláírás
- a mobiltelefonon az e-Szignó aláíró alkalmazás telepítve van

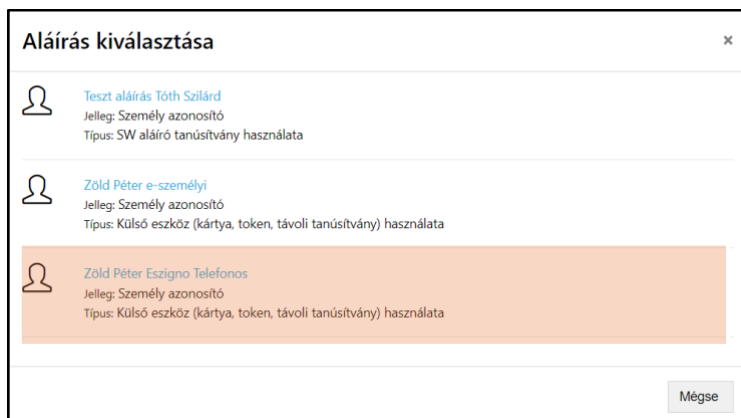
3.2.1.1. Iktató felület használata aláírásra Microsec telefonos tanúsítvány esetén

Hozunk létre iktatást, vagy bármely képernyőn, ahol dokumentum csatolásra van lehetőség, csatoljuk be az aláírandó PDF állományt, illetve, ha már csatolásra került, akkor keressük meg.

Az iktatás dokumentumok képernyőn található a hitelesítésre szolgáló  ikon, amely lehetővé teszi a PDF dokumentumok hitelesítését, amennyiben a bejelentkezett felhasználó rendelkezik megfelelő jogosultsággal.



PDF aláírása gombra kattintva megjelennek az elérhető aláírások.



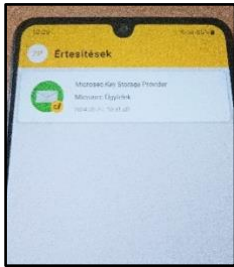
Válasszuk ki az e-Szignó telefonos aláírást

A képernyőn megjelenik egy felugró ablak, amely arra utal, hogy a rendszer várakozik a telefonos hitelesítésre.

A mobiltelefonon megjelenik egy push üzenet, illetve az aláíró applikációban is láthatóvá válik az üzenet, miszerint egy dokumentum vár aláírásra.

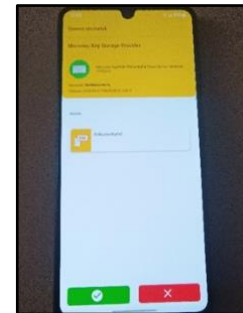


Az e-Szignó aláíró alkalmazás indításakor be kell írni a tanúsítványhoz tartozó PIN kódot.



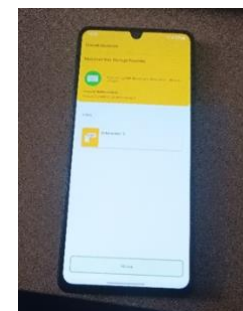
Az értesítések között ott az üzenet arról, hogy egy dokumentum vár aláírásra.

Az üzenetre kattintva megjelenik az aláírandó dokumentum. A zöld pipára kattintva kezdeményezhető az aláírás.

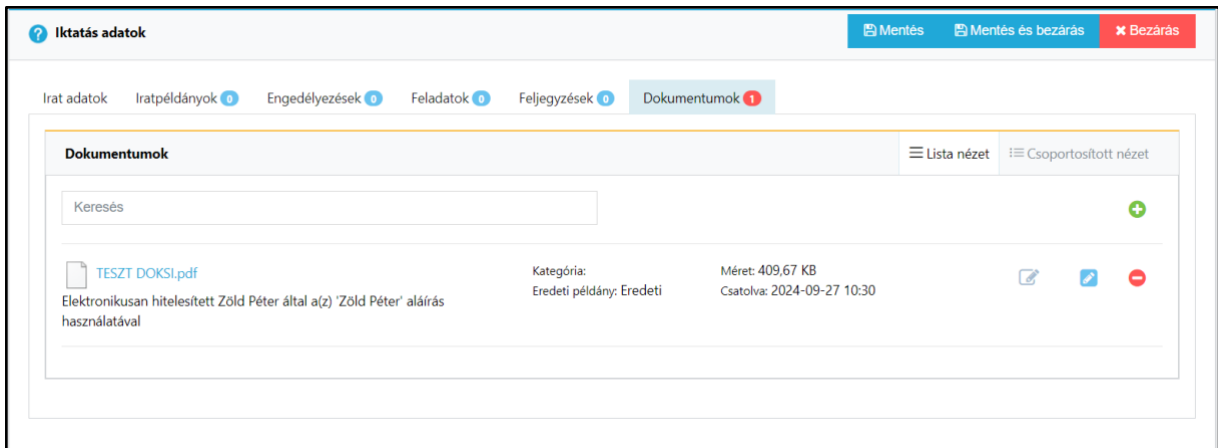


Aláírás során ismét be kell írni a tanúsítványhoz tartozó PIN kódot.

Sikeres aláírás esetén a telefon kijelzőjének alján megjelenik a halvány zöld üzenet, hogy kész az aláírás, valamint a számítógép képernyőjén eltűnik a korábban megjelent felugró ablak.



A számítógép képernyőjén eltűnik a felhívó felirat és létrejön az aláírás. A hitelesítés során a dokumentum metaadatai megváltoznak a rendszerben és „másolat” helyett „eredeti” státuszt vesz fel. A metaadatok közé bekerül, hogy melyik felhasználó hitelesítette és milyen hitelesítési eszközt használt, szervezeti bélyegzőt vagy személyhez kötött elektronikus aláírást.



A dokumentumban a hitelesítés letöltés után az Acrobat Readerrel ellenőrizhető:

