

# **Kormányzati Elektronikus Aláíró és Aláírás-ellenőrző Szoftver**

## **Felhasználói leírás**

verzió: 1.33

2017.10.12.

---

# TARTALOMJEGYZÉK

|         |   |    |
|---------|---|----|
| 1.      | BEVEZETÉS .....                                     | 4  |
| 2.      | A PROGRAM INDÍTÁSA.....                             | 4  |
| 3.      | EGYSZERŰ / HALADÓ ÜZEMMÓD KIVÁLASZTÁSA.....         | 5  |
| 4.      | EGYSZERŰ ÜZEMMÓD .....                              | 6  |
| 4.1     | Menüszerkezet.....                                  | 6  |
| 4.2     | Beállítások.....                                    | 7  |
| 4.2.1   | Tanúsítvány profil .....                            | 9  |
| 4.2.1.1 | MSCAPI - Windows Tanúsítványtár.....                | 9  |
| 4.2.1.2 | PKCS11 Hardveres Tanúsítványtár .....               | 9  |
| 4.2.1.3 | PKCS12 Szoftveres Tanúsítványtár.....               | 10 |
| 4.2.1.4 | JKS Szoftveres (Java) Tanúsítványtár.....           | 11 |
| 4.2.2   | Internet beállítások .....                          | 12 |
| 4.2.2.1 | Proxy megadása.....                                 | 13 |
| 4.2.3   | Vizuális aláírás beállításai .....                  | 14 |
| 4.2.3.1 | Általános beállítások.....                          | 15 |
| 4.2.3.2 | Szöveg beállítása .....                             | 17 |
| 4.2.3.3 | Kép beállítása .....                                | 18 |
| 4.3     | Dokumentum aláírása .....                           | 21 |
| 4.3.1   | Aláírás egyenként.....                              | 21 |
| 4.3.2   | Aláírás kötegben.....                               | 25 |
| 4.4     | Aláírás kiterjesztése .....                         | 29 |
| 5.      | HALADÓ ÜZEMMÓD .....                                | 33 |
| 5.1     | Menüszerkezet.....                                  | 33 |
| 5.2     | Beállítások.....                                    | 34 |
| 5.2.1   | Profilok .....                                      | 35 |
| 5.2.2   | Tanúsítvány profilok .....                          | 37 |
| 5.2.2.1 | Új tanúsítvány profil létrehozása .....             | 38 |
| 5.2.2.2 | Tanúsítványtár és Aláíró tanúsítvány megadása ..... | 39 |
| 5.2.3   | Időbélyeg profilok .....                            | 40 |
| 5.2.3.1 | Új időbélyeg profil létrehozása .....               | 41 |
| 5.2.4   | Internet beállítások .....                          | 44 |
| 5.2.5   | Általános beállítások.....                          | 44 |
| 5.2.5.1 | Kimeneti mappa .....                                | 45 |
| 5.2.5.2 | Kimeneti fájlok utótagjai (postfix-ek) .....        | 45 |
| 5.2.5.3 | Automatikus frissítések keresése .....              | 45 |
| 5.2.5.4 | Figyelmeztetés Időbélyeg kérés előtt.....           | 46 |
| 5.2.6   | Csoportos ellenőrzés fájl típusai.....              | 46 |
| 5.2.6.1 | Fájl típus hozzáadása a listához.....               | 46 |
| 5.2.6.2 | Fájl típus törlése a listából .....                 | 47 |
| 5.2.7   | Vizuális aláírás beállítások .....                  | 48 |
| 5.3     | Dokumentum aláírása .....                           | 52 |
| 5.3.1   | Aláírás egyenként.....                              | 52 |
| 5.3.2   | Aláírás kötegben.....                               | 55 |
| 5.4     | Aláírás kiterjesztése .....                         | 60 |
| 6.      | ALÁÍRÁS ELLENŐRZÉSE .....                           | 63 |

---

|     |                           |    |
|-----|---------------------------|----|
| 7.  | ASIC FÁJLOK KEZELÉSE..... | 69 |
| 7.1 | ASIC FÁJLKEZELŐ.....      | 70 |

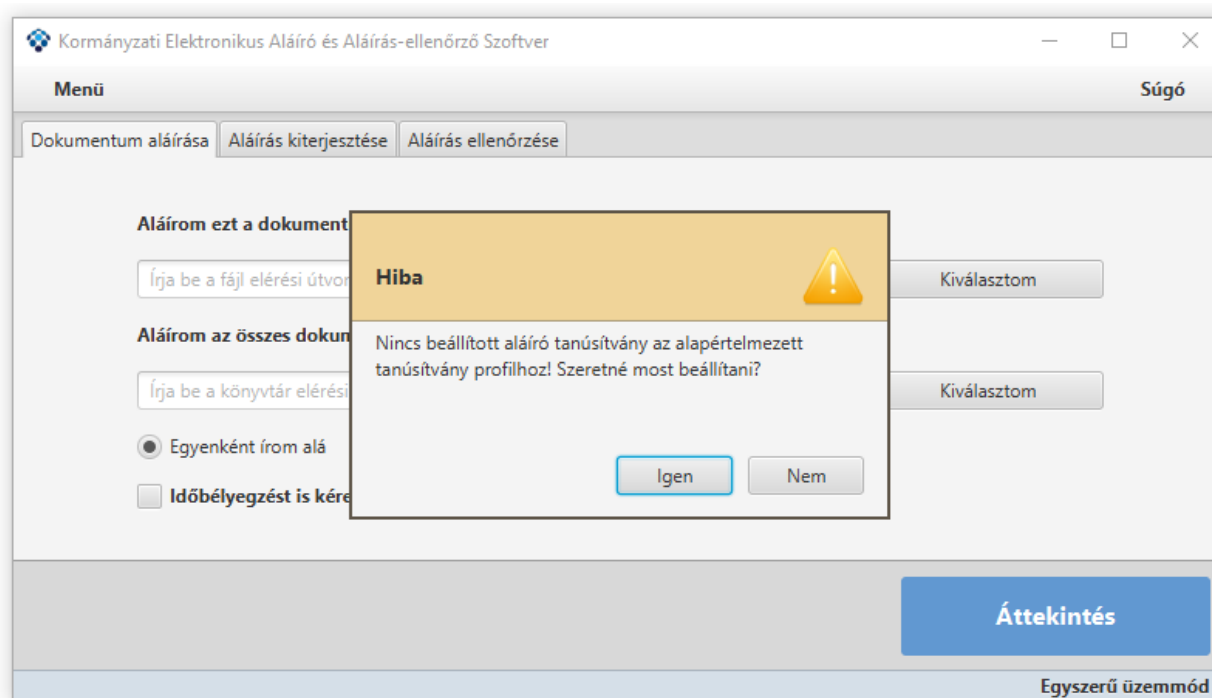
# 1. BEVEZETÉS

A Kormányzati Elektronikus Aláíró és Aláírás-ellenőrző Szoftver (**KEAASZ**), egy önállóan telepíthető szoftver, amely elektronikus aláírás és időbélyegzés, valamint aláírás ellenőrzés funkciót szolgáltat a felhasználók számára.

A KEAASZ szoftver lehetőséget nyújt arra, hogy (meghatározott informatikai feltételek biztosítása mellett) alá tudjunk írni dokumentumot, egy dokumentumon lévő aláírást ki tudjunk terjeszteni, illetve segítségével ellenőrizhetjük korábban aláírt dokumentumok érvényességét is.

# 2. A PROGRAM INDÍTÁSA

Indítsa el a programot a KEAASZ ikonra kattintva. A KEAASZ alkalmazás indításakor a program ellenőrzést végez, hogy van-e beállítva az alapértelmezett tanúsítvány profilhoz aláíró tanúsítvány, amennyiben nincs az alábbi figyelmeztető üzenetet jeleníti meg.



Amennyiben nem kíván aláíró tanúsítványt beállítani, nyomja meg a „Nem” gombot ekkor a figyelmeztető üzenet képernyője bezárul és az alapképernyő jelenik meg.

Amennyiben aláíró tanúsítványt kíván hozzárendelni az alapértelmezett tanúsítvány profilhoz, nyomja meg az „Igen” gombot, ekkor a program megnyitja a **”Tanúsítvány beállítások”** képernyőt, ahol be tudja állítani az aláíró tanúsítványt jelen dokumentum Tanúsítvány profil (4.2.1 és 5.2.2) fejezetekben leírtak szerint.

---

### 3. EGYSZERŰ / HALADÓ ÜZEMMÓD KIVÁLASZTÁSA

A „Menü” menüpont alatt lehet váltani az egyszerű és a haladó üzemmód között.



A haladó üzemmódban a **Beállítások** menüpont alatt érhetőek el azok a funkciók, amelyek a program használatához magasabb szintű informatikai ismeretet igényelnek.

Az aktuális üzemmód az alkalmazás jobb alsó sarkában mindig megjelenik.

---

## 4. EGYSZERŰ ÜZEMMÓD

Az alkalmazás első indítását követően, vagy az alkalmazás egy korábbi használata után amennyiben egyszerű módban voltunk, vagy a menüben az „**Egyszerű üzemmód**” kerül kiválasztásra, akkor az egyszerű üzemmód alapképernyő jelenik meg.

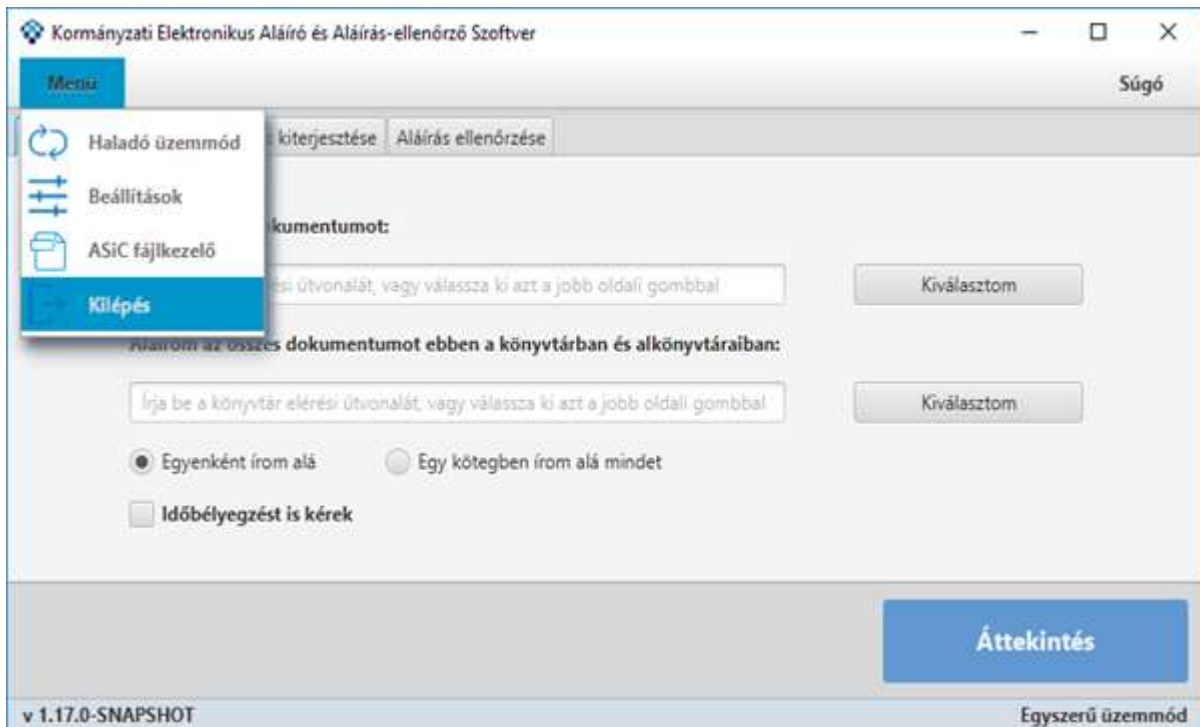
### 4.1 Menüszerkezet

Válasszon a következő fülek közül a program alkalmazásának célja szerint.

- A **Dokumentum aláírása** funkcióval aláírhatunk egy vagy több dokumentumot, ezáltal garantálva az aláírt dokumentum(ok) sértetlenségét.
- Az **Aláírás kiterjesztése** funkcióval az aláírt dokumentum(ok) hosszabb távú érvényességgel látható(ak) el.
- Az **Aláírás ellenőrzése** funkcióval megbizonyosodhatunk a dokumentumon lévő aláírás érvényességéről.

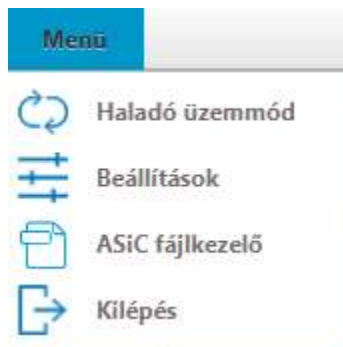
Az alapképernyőn kattintson a Menü ikonra az alábbi funkciók eléréséhez:

- A **Haladó üzemmód** menüpontra kattintva lehetőség van az egyszerű üzemmódból haladóra váltani.
- A **Beállítások** menüpontban lehetőség van a tanúsítványtípusok, valamint az Internet proxy beállítások megadására, illetve a Vizuális aláírás beállítására.
- A program bezárásához válassza a **Kilépés** gombot.



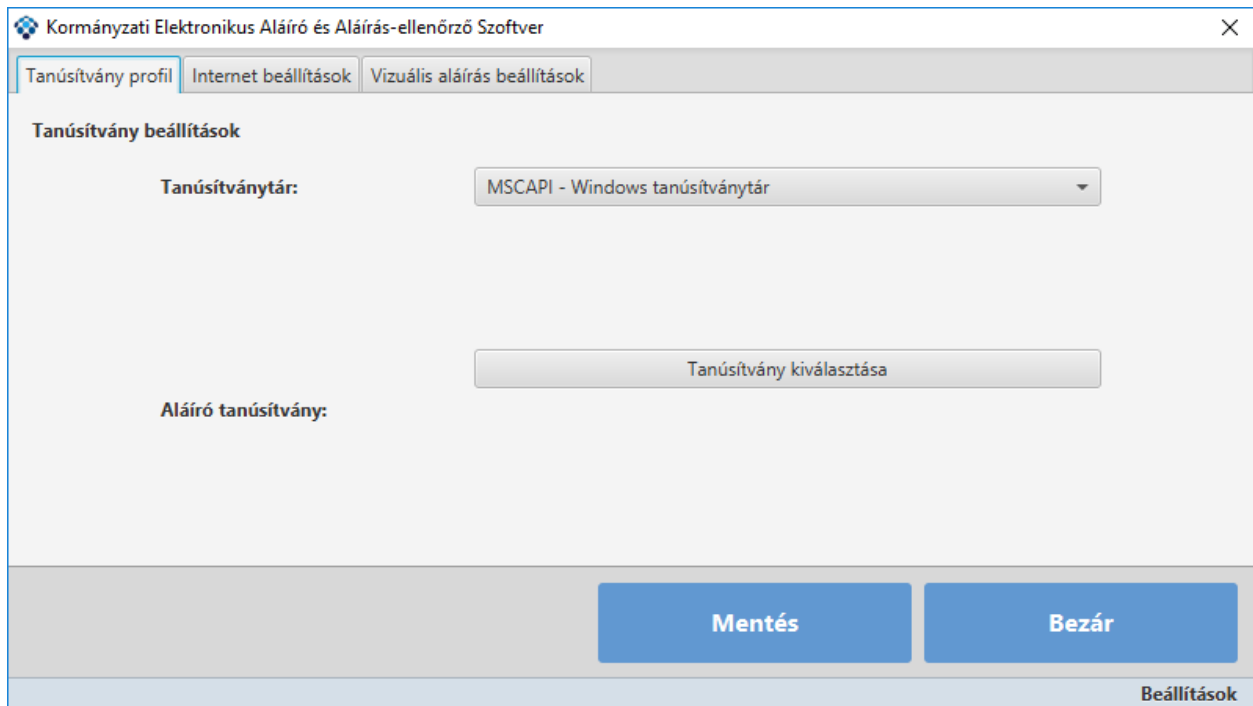
## 4.2 Beállítások

Amikor a program egyszerű üzemmódban fut a Menü ikon alatt a Beállítások pontra kattintva lehet elindítani az alkalmazás beállításainak funkcióit.

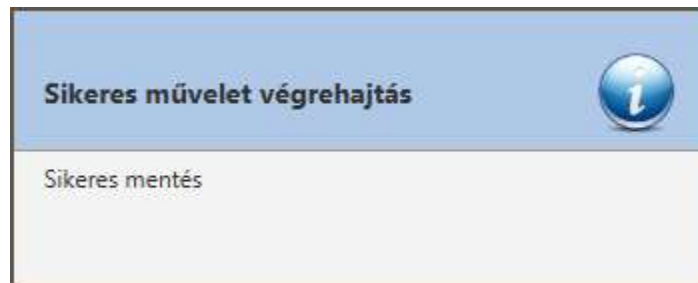


Az egyszerű üzemmódban a Beállítások képernyőn az alábbi funkciófülek szerepelnek:

- Tanúsítvány profil
- Internet beállítások
- Vizuális aláírás beállítások



Az adatok mentéséhez kattintson a „**Mentés**” gombra. A mentésről a program az alábbi üzenetet küldi, majd visszatér a Beállítások képernyőre.



Az indulóképernyőre való visszatéréshez kattintson a "**Bezár**" gombra.

## 4.2.1 Tanúsítvány profil

A „**Tanúsítvány profil**” fülön lehetősége van a tanúsítvány beállítások elvégzésére a tanúsítványtár típusának kiválasztása, majd a szükséges adatmezők kitöltése által.

- **Tanúsítványtár:** Válassza ki az értéklistában beállított Tanúsítványtárak közül a használni kívánt tanúsítványtárat.

### 4.2.1.1 MSCAPI - Windows Tanúsítványtár

Amennyiben az aláírói tanúsítványa a Windows tanúsítványtárban található, akkor kérjük, használja ezt a tanúsítványtár típust. Amennyiben az **eSzemélyi** igazolványához az **eSzemélyi Kliens** alkalmazást használja, abban az esetben az **eSzemélyi** igazolványán lévő tanúsítványt a Windows tanúsítványtárban találhatja meg.

MSCAPI - Windows Tanúsítványtár kiválasztása esetén az alábbi adatokat kell rögzíteni.

- A Tanúsítványtár lekérdezéséhez kattintson a „**Tanúsítvány kiválasztása**” gombra.
- **Aláíró tanúsítvány:** értéklistából választható.

Kormányzati Elektronikus Aláíró és Aláírás-ellenőrző Szoftver

Tanúsítvány profil | Internet beállítások | Vizuális aláírás beállítások

**Tanúsítvány beállítások**

Tanúsítványtár: MSCAPI - Windows tanúsítványtár

Tanúsítvány kiválasztása


Aláíró tanúsítvány:

Mentés Bezár

Beállítások


### 4.2.1.2 PKCS11 Hardveres Tanúsítványtár

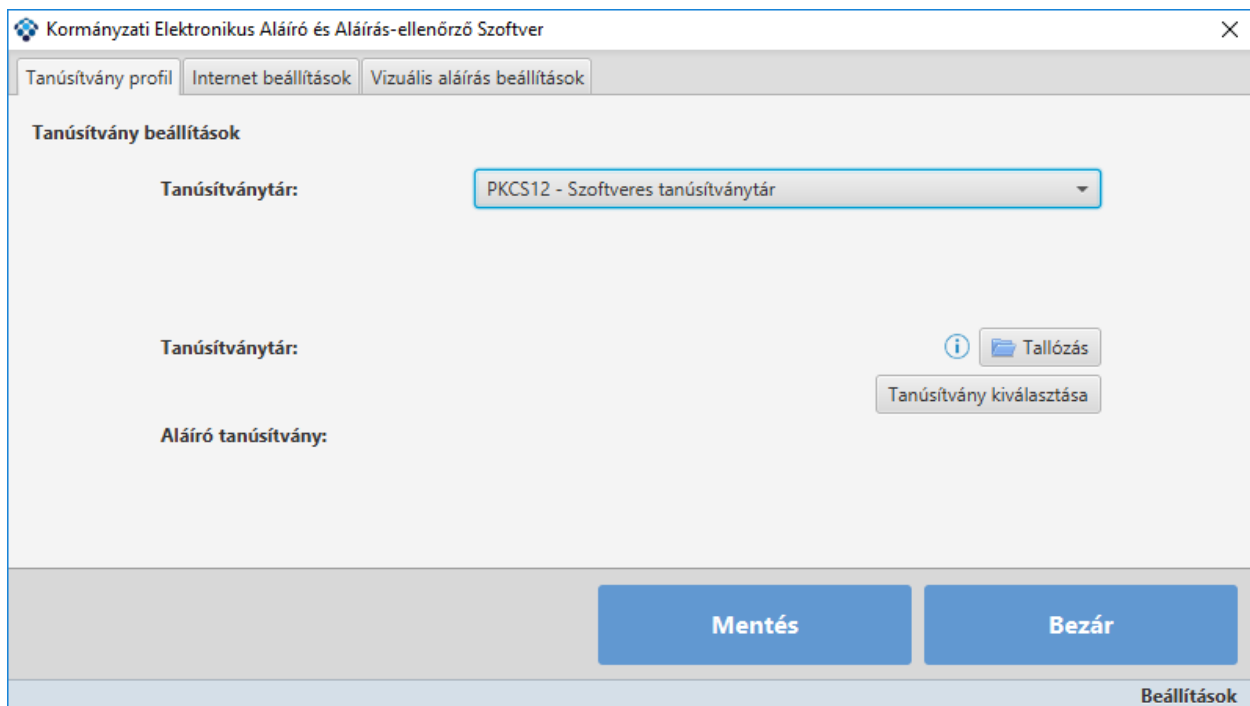
PKCS11 Hardveres Tanúsítványtár kiválasztása esetén az alábbi adatokat kell rögzíteni.

- **Eszközmeghajtó fájl:** a hardveres tanúsítványtár beállításánál ki kell választani a fájlkezelőben azt az eszközmeghajtó fájlt (MS Windows operációs rendszer esetén, általában DLL kiterjesztésű fájl), amely szükséges a tanúsítványtár eléréséhez.
  - a „**Tallózás**” gombra kattintva a Fájlkezelőben kiválasztható az adott fájl.
  - Az  ikonra kattintva megjelenik a Súgó.
  - A „**Tanúsítvány kiválasztása**” gombra kattintva a fájl lekérdezésre kerül.
- **Slot index:** Tanúsítványok helyének index száma az eszközön. (Általában a 0-s slot indexen találhatóak meg a tanúsítványok.)
- **Aláíró tanúsítvány:** értéklistából választható.

#### 4.2.1.3 PKCS12 Szoftveres Tanúsítványtár


PKCS12 Szoftveres Tanúsítványtár kiválasztása esetén az alábbi adatokat kell rögzíteni.

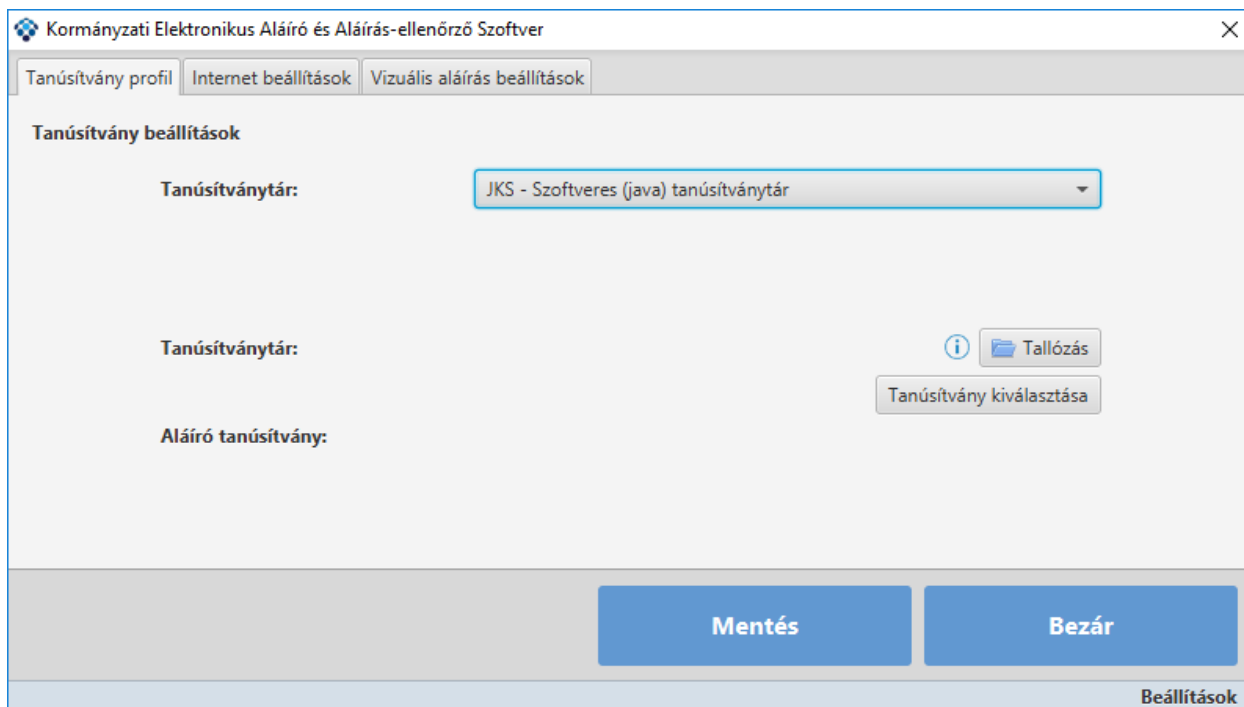
- **Tanúsítványtár fájl:**
  - a „**Tallózás**” gombra kattintva a Fájlkezelőben kiválasztható az adott fájl.
  - Az  ikonra kattintva megjelenik a Súgó.
  - A „**Tanúsítvány kiválasztása**” gombra kattintva a fájl lekérdezésre kerül.
- **Aláíró tanúsítvány:** értéklistából választható.



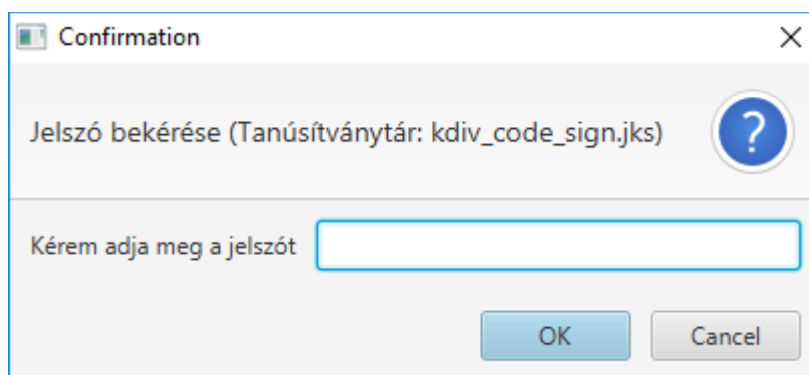
#### 4.2.1.4 JKS Szoftveres (Java) Tanúsítványtár

JKS Szoftveres (Java) Tanúsítványtár kiválasztása esetén az alábbi adatokat kell rögzíteni.

- **Tanúsítványtár fájl:**
  - a „**Tallózás**” gombra kattintva a Fájlközelítőben kiválasztható az adott fájl.
  - Az  ikonra kattintva megjelenik a Súgó.
  - A „**Tanúsítvány kiválasztása**” gombra kattintva a fájl lekérdezésre kerül.
- **Aláíró tanúsítvány:** értéklisztából választható.



Tanúsítvány kiválasztása után a jelszó bekérése ablak hiányzik.

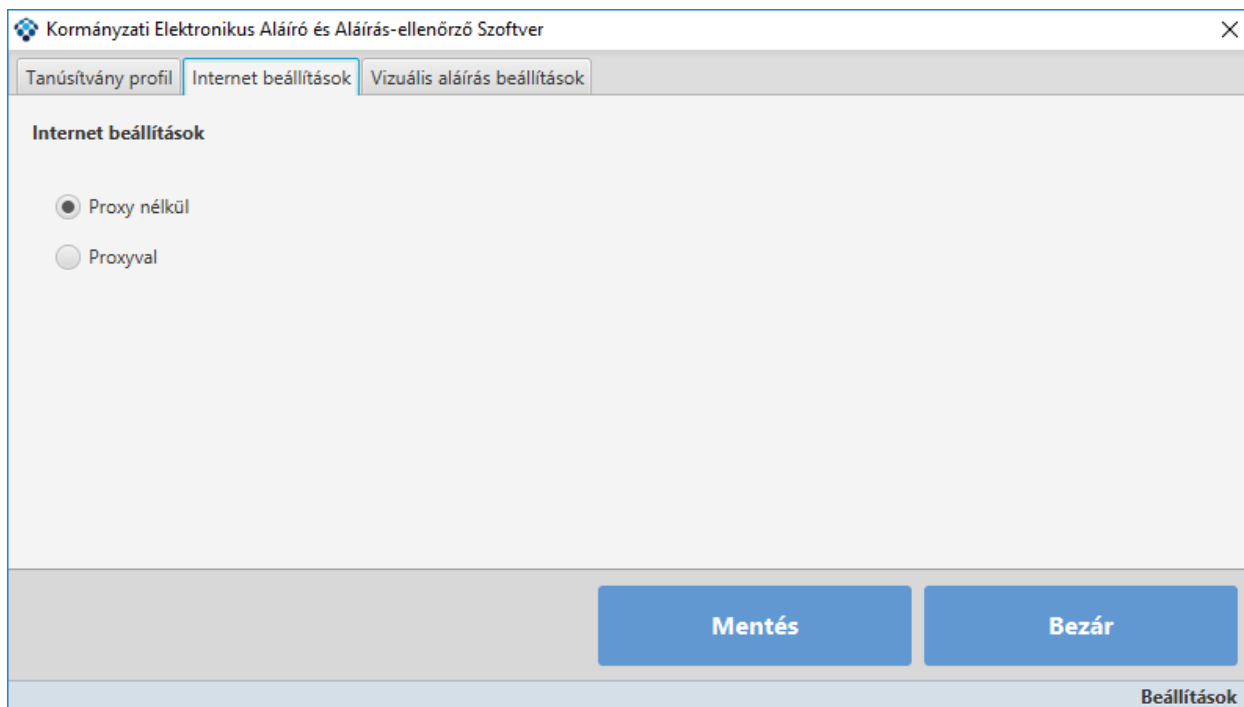


#### 4.2.2 Internet beállítások

Az aláírt dokumentumok ellenőrzéséhez és az időbélyegzés szolgáltatás igénybe vételéhez internetkapcsolatra van szükség. Amennyiben egy proxyn keresztül éri el az internetet, akkor ebben a menüpontban adja meg a beállításait.

Az Internet beállítások elvégzéséhez kattintson az **Internet beállítások** fülre egyszerű üzemmódban a Menü/Beállítások ikon kiválasztását követően. Itt az alábbi adatok megadása lehetséges:

- **Proxy nélkül/Proxyval:** a két lehetőség közül az egyiket lehet csak kiválasztani.



#### 4.2.2.1 Proxy megadása

Amennyiben a Proxyval radiogomb kerül bejelölésre a megjelenő képernyőn az alábbi adatokat kell rögzíteni:

- **Cím:** a proxy szerver URL címét kell megadni.
- **Port:** a proxy szerveren elérhető port számát kell megadni.
- **Felhasználó:** a felhasználó azonosítóját kell megadni.
- **Jelszó:** a felhasználó azonosítójához tartozó jelszót kell megadni.
- A „**Megbízható tanúsítványok tára**” ikonra kattintva a Fájlközvetítőből ki lehet választani egy megbízható tanúsítványtárat (angol neve: TrustStore), ezt a beállítást csak HTTPS protokollt használó proxy szerver esetén szükséges kitölteni. A kiválasztott tanúsítványtárnak a proxy szerver tanúsítványát kell tartalmaznia.

Kormányzati Elektronikus Aláíró és Aláírás-ellenőrző Szoftver

Tanúsítvány profil Internet beállítások Vizuális aláírás beállítások

**Internet beállítások**

Proxy nélkül

Proxyval

Cím:

Port:

Felhasználó:

Jelszó:

**Nincs kiválasztott fájl**

Beállítások

### 4.2.3 Vizuális aláírás beállításai

A vizuális aláírás beállítások felület az Egyszerű vagy Haladó üzemmódban a „Menü” ikon alatt a **Beállítások** menüpontra kattintva jelenik meg. Ezen a felületen lehetőség van beállítani az elektronikus aláírással ellátott dokumentum felületén az aláírás elhelyezkedését illetve a vizuális megjelenését.

A Vizuális aláírás beállítások fülre kattintva az alábbi képernyő jelenik meg:

Kormányzati Elektronikus Aláíró és Aláírás-ellenőrző Szoftver

Tanúsítvány profil | Internet beállítások | Vizuális aláírás beállítások

Általános | Szöveg | Kép

látható a szöveg az aláíráson  látható a kép az aláíráson Előnézet

**Margó/Pozíció**

X koordináta (pixel) Y koordináta (pixel)

10 10

**Igazítás**

Vízszintes Függőleges Oldal

Nincs igazítás Nincs igazítás Első oldal

**Aláírás**

Háttérszín

Mentés Bezár

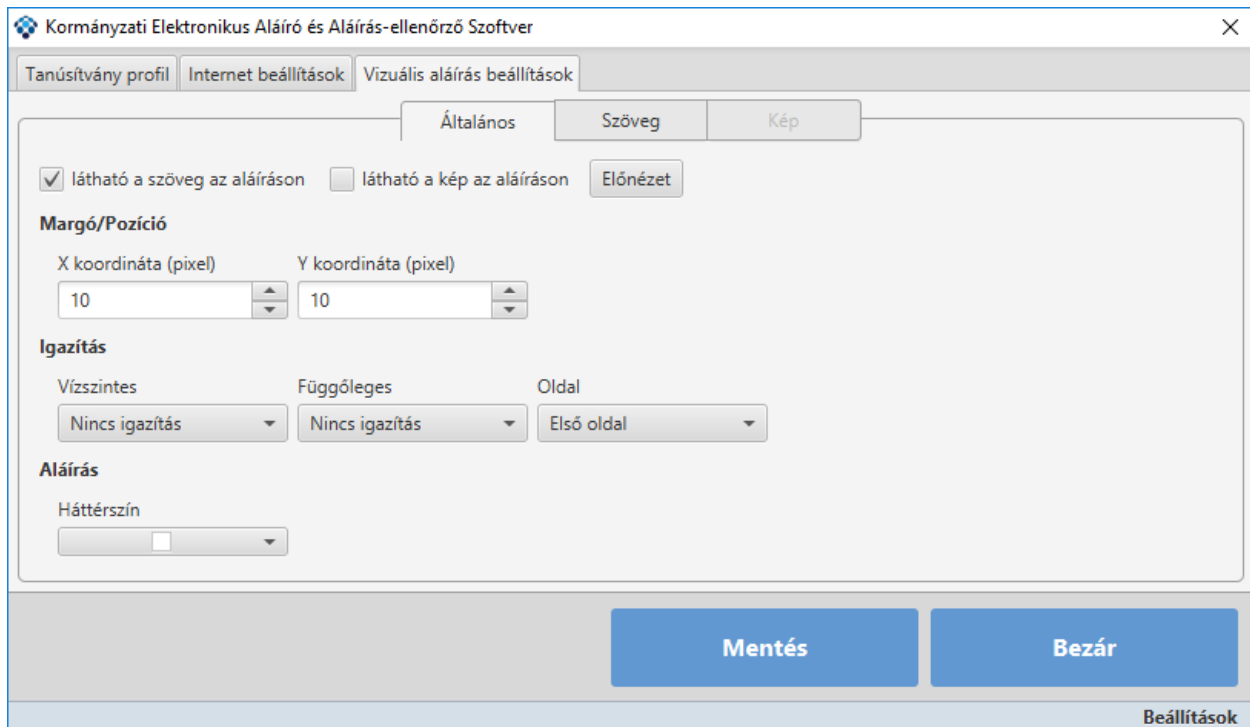
Beállítások

A vizuális aláírás beállítások képernyő három része van osztva.

- Általános, ahol az általános vizuális aláírás beállítások állíthatók be (pl. akarunk-e vizuális aláírás szöveget vagy képet beállítani és azt hova, stb...)
- Szöveg (amennyiben egy szöveget adnánk meg, mi legyen az és milyen színű legyen, stb...)
- Kép (kép estén melyik kép legyen az, milyen mérettel, stb...)

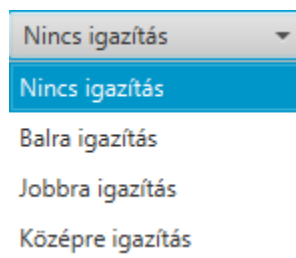
#### 4.2.3.1 Általános beállítások

A vizuális aláírás képernyő **Általános** részén lehet az alábbi tulajdonságokat beállítani:

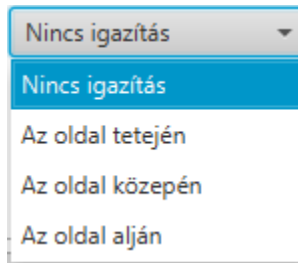


Általános képernyő beállításai:

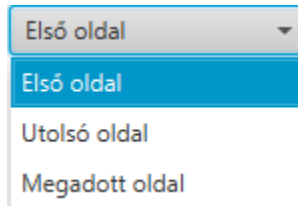
- **Látható a szöveg az aláíráson** – jelölőnégyzettel kiválasztható, hogy a vizuális aláírásnál látható legyen-e a megadott szöveg, melyet a szöveg fülön lehet beállítani, amennyiben ez a jelölőnégyzet be van állítva.
- **Látható a kép az aláíráson** – jelölőnégyzettel kiválasztható, hogy a vizuális aláírásnál látható legyen-e a megadott kép, melyet a kép fülön lehet beállítani, amennyiben ez a jelölőnégyzet be van állítva.
- **Előnézet** – gomb kiválasztásával megtekinthető a beállítások alapján az előnézet
- Margó/Pozíció:
  - o **X koordináta:** maximális érték 595 pixel (A4-es papírméret)
  - o **Y koordináta:** maximális érték 842 pixel (A4-es papírméret)
- Igazítás
  - o **Vízszintes:** értéklisztából választható



- o **Függőleges:** értéklisztából választható



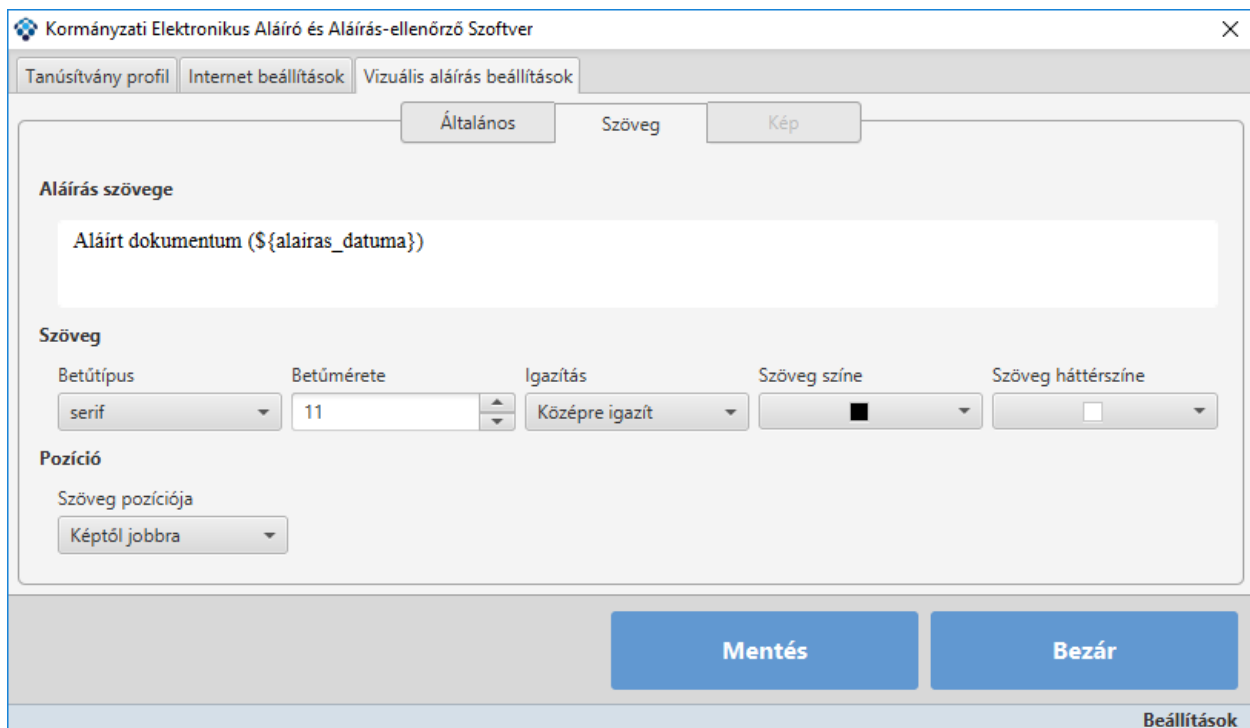
- **Oldal:** értéklisából választható



- Aláírás
  - **Háttérszín:** értéklisából választható



#### 4.2.3.2 Szöveg beállítása

A vizuális aláírás képernyő **Szöveg** részén lehet az alábbi tulajdonságokat beállítani:



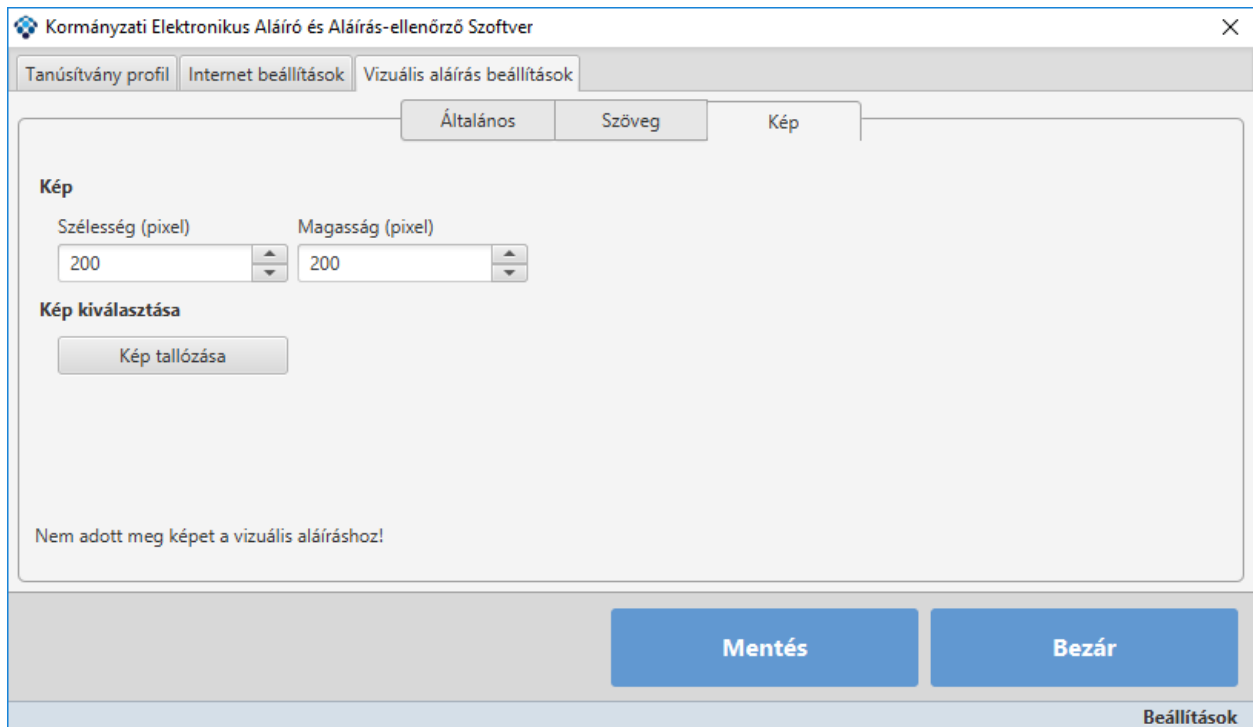
A megjelenő felületen az alábbi paramétereket lehet beállítani:

- **Aláírás szövege:** szabad szöveges mező, amelyben meg kell adni az aláírás szövegét. A szövegben paraméterek használhatók. Alapértelmezett szöveggként a „**Aláírt dokumentum (\${alairas\_datuma})**” jelenik meg.

- Lehetőség van a szövegbe paramétereket is elhelyezni. A paraméterek az alábbi formában adhatóak meg:  $\{\text{paraméternév}\}$ , ahol a paraméternév az alábbiak egyike lehet:
  - **certificate\_serial** – aláírói tanúsítvány széria száma
  - **certificate\_cn** – aláírói tanúsítvány common neve
  - **certificate\_ou** – aláírói tanúsítvány szervezeti egysége
  - **certificate\_o** – aláírói tanúsítvány szervezete
  - **certificate\_c** – aláírói tanúsítvány országkód
  - **certificate\_exp\_date** – aláírói tanúsítvány lejáratának dátuma
  - **now** – aláírás dátuma (yyyy.MM.dd HH:mm:ss)
  - **ip** – a gép IP címe
  - **logged\_in\_user** – bejelentkezett felhasználó neve
  - **host\_name** – a gép host neve
- Szöveg
  - **beütípus:** a mezőben a rendszer által biztosított betűtípusokból választhatunk, alapértelmezett a serif betűtípus
  - **betűméret:** a mezőben megjelenő alapértelmezett értéket a nyilakra kattintva vagy a mezőbe történő rögzítéssel lehet módosítani.
  - **Igazítás:** listából választható
  - **Szöveg színe:** a színválasztó  ikonra kattintva lehet kiválasztani a szöveg színét.
  - **Szöveg háttérszíne:** a színválasztó  ikonra kattintva lehet kiválasztani a szöveg háttér színét.
- Pozíció
  - **Szöveg pozíciója:** értéklistánból választható

### 4.2.3.3 Kép beállítása

A vizuális aláírás képernyő **Kép** részén lehet az alábbi tulajdonságokat beállítani:



A megjelenő felületen az alábbi paramétereket lehet beállítani:

- Kép
  - o **Szélesség** (pixel-ben)
  - o **Magasság** (pixel-ben)
- Kép kiválasztása
  - o **Kép tallózása** – kép kiválasztása a fájlrendszerből. Az elfogadható képformátumok a **gif, tiff, pcx, bmp, wbmp, png, jpg**. A kiválasztott kép a képernyő jobb oldalán megjelenítésre kerül.



---

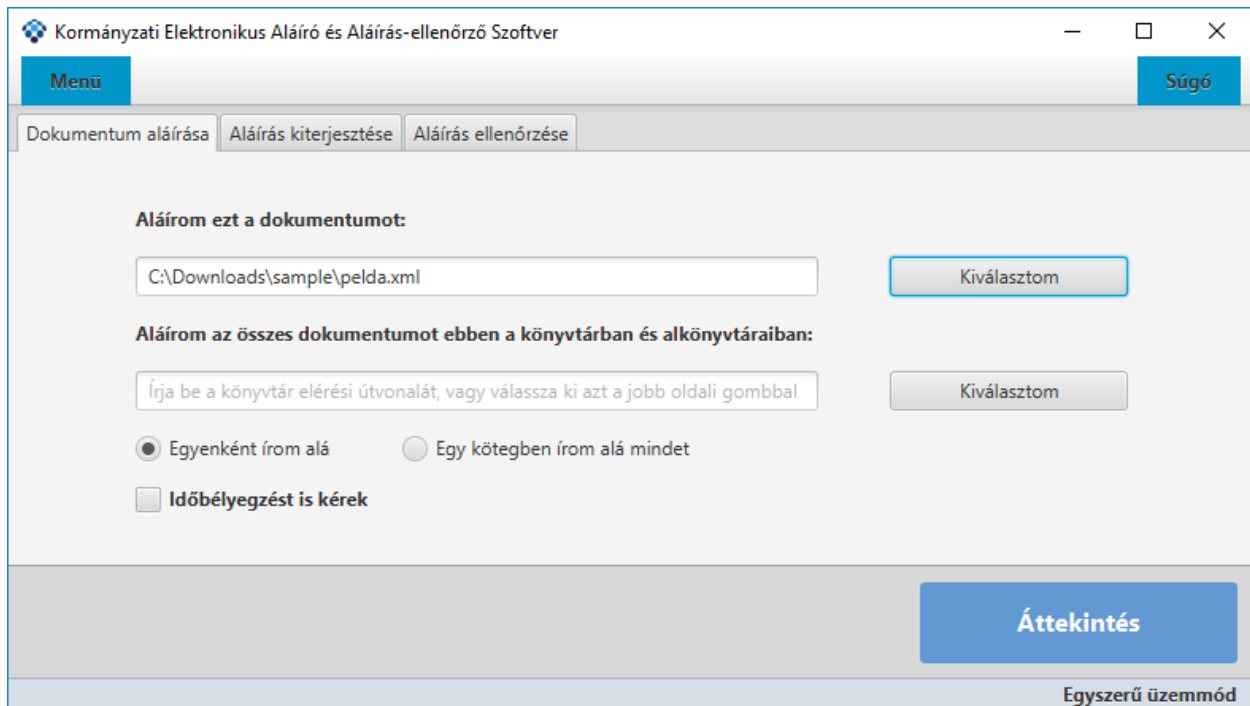
## 4.3 Dokumentum aláírása

Az egyszerű üzemmódban a Dokumentum/dokumentumok aláírásához válasszon az alábbi lehetőségek közül:

- **Aláírom ezt a dokumentumot** (ebben a mezőben csak egy dokumentum választható ki): a „**Kiválasztom**” gombra kattintva a megjelenő Fájlkezelőben válassza ki az aláírandó dokumentumot.
- **Aláírom az összes dokumentumot ebben a könyvtárban és alkönyvtárban** (a választott könyvtárban az összes dokumentum aláírásra kerül): a „**Kiválasztom**” gombra kattintva a Fájlkezelőben válassza ki az aláírandó dokumentumokat tartalmazó könyvtárat vagy alkönyvtárat.
- **Egyenként írom alá**: az „**Egyenként írom alá**” kijelölő radio gombra kattintva a kiválasztott dokumentumokat egyenként lehet aláírni. Ezzel a beállítással a dokumentumok egyenként, külön-külön lesznek aláírva.
- **Egy kötegben írom alá mindet**: az „**Egy kötegben írom alá mindet**” kijelölő radio gombra kattintva a kiválasztott dokumentumokat egyszerre tudjuk aláírni. Ezzel a beállítással az összes fájl együtt lesz aláírva egy közös konténerben.
- **Időbélyegzést is kérek**: dokumentum aláírásakor az „**Időbélyegzést is kérek**” jelölő négyzetet bepipálva a program időbélyeg kérését fog indítani a dokumentum aláírása után az állampolgári időbélyegzés szolgáltató felé alapértelmezett esetben, amelyet az **eSzemélyi** igazolvánnyal lehet igénybe venni.

### 4.3.1 Aláírás egyenként

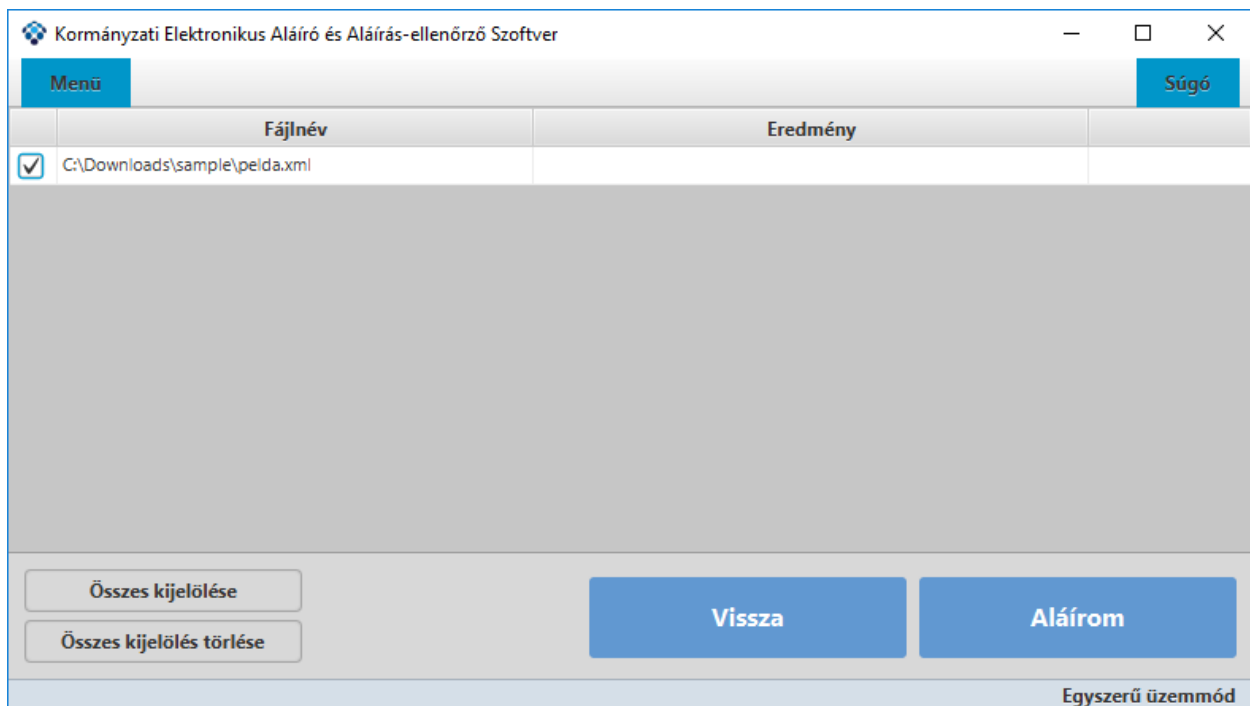
A Dokumentum aláírás felületen rá kell kattintani az „**Egyenként írom alá**” gombra majd a „**Kiválasztom**” gombra. A fájlkezelőben ki kell választani azt a fájlt, amely aláírásra kerül.



Miután a dokumentum(ok) kiválasztásra került(ek) kattintson az **Áttekintés** ikonra. Ezt követően megjelenik az alábbi felület a következő adatokkal:

- Fájlnév
- Eredmény

Kattintson a táblázatban a sorok elején megjelenő kijelölő négyzetbe az aláírandó dokumentum/dokumentumok kiválasztásához.



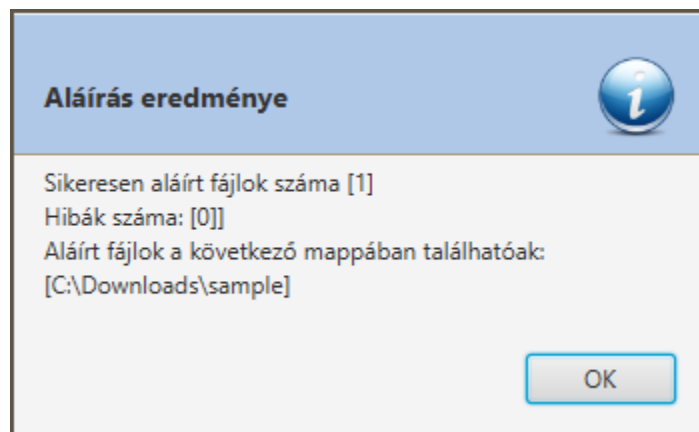
Lehetőség van több fájlt egyidejűleg kijelölni illetve a kijelöléseket megszüntetni is a bal alsó sarokban lévő gombok segítségével.

A képernyő bezárásához és a Dokumentum aláírása képernyőre való visszatéréshez kattintson a **Vissza** ikonra.

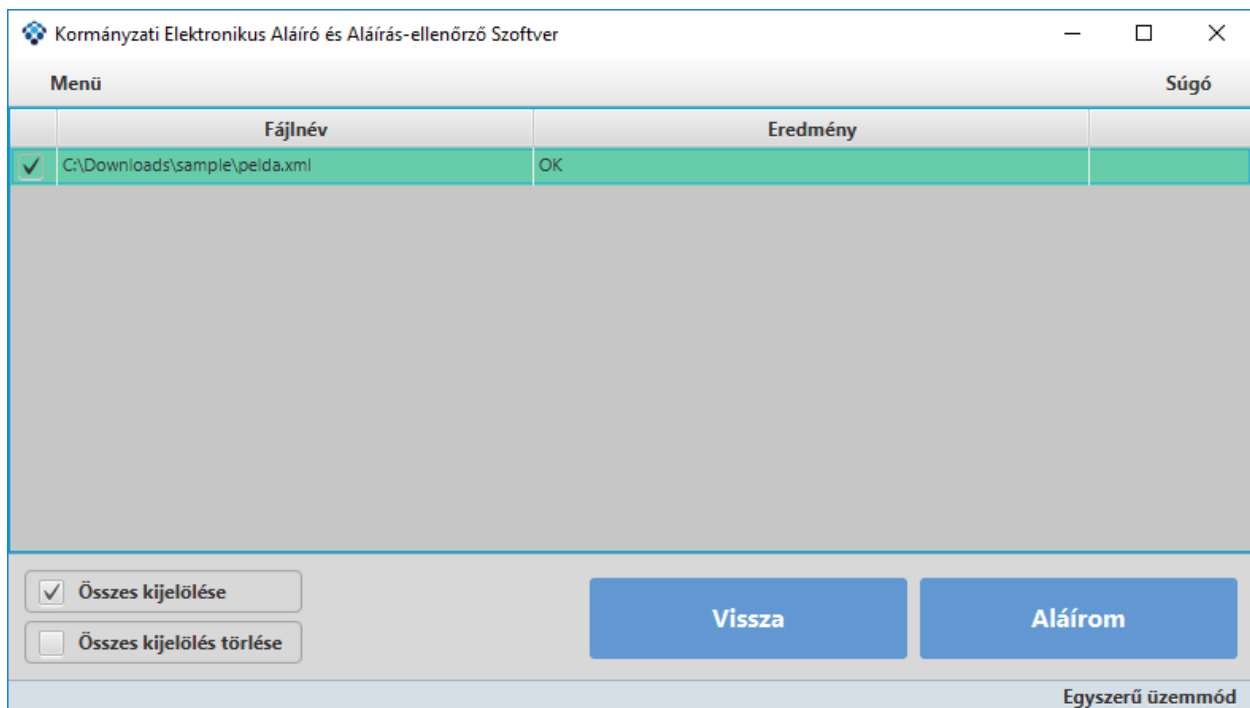
A listában kijelölt Dokumentumok aláírásához kattintson az **Aláírom** ikonra.

Az aláírás eredményéről a program üzenetet küld, amennyiben sikeres, illetve akkor is, ha hibát talál.

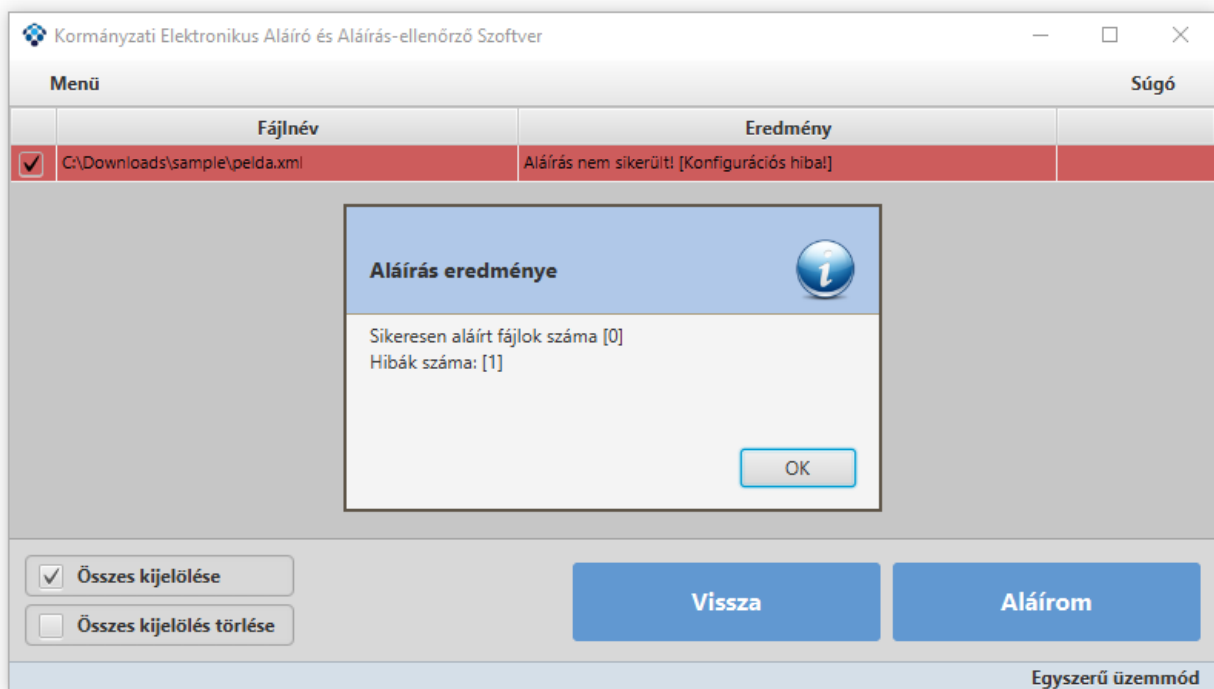
Amennyiben az aláírás eredménye sikeres az alábbi ablak jelenik meg.



Az **OK** gombra kattintva az üzenetablak bezárul és a képernyőn a listában zöld színnel kerül kiemelésre a sikeresen aláírt fájl sora, majd az Eredmény oszlopban az **OK** információ jelenik meg.



Amennyiben az aláírás eredménye sikertelen az alábbi képernyő jelenik meg.

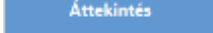


Az **OK** gombra kattintva az üzenetablak bezárul és a képernyőn a listában piros színnel kerül kiemelésre a hibás sor, majd az Eredmény oszlopban a hibára vonatkozó információ jelenik meg.

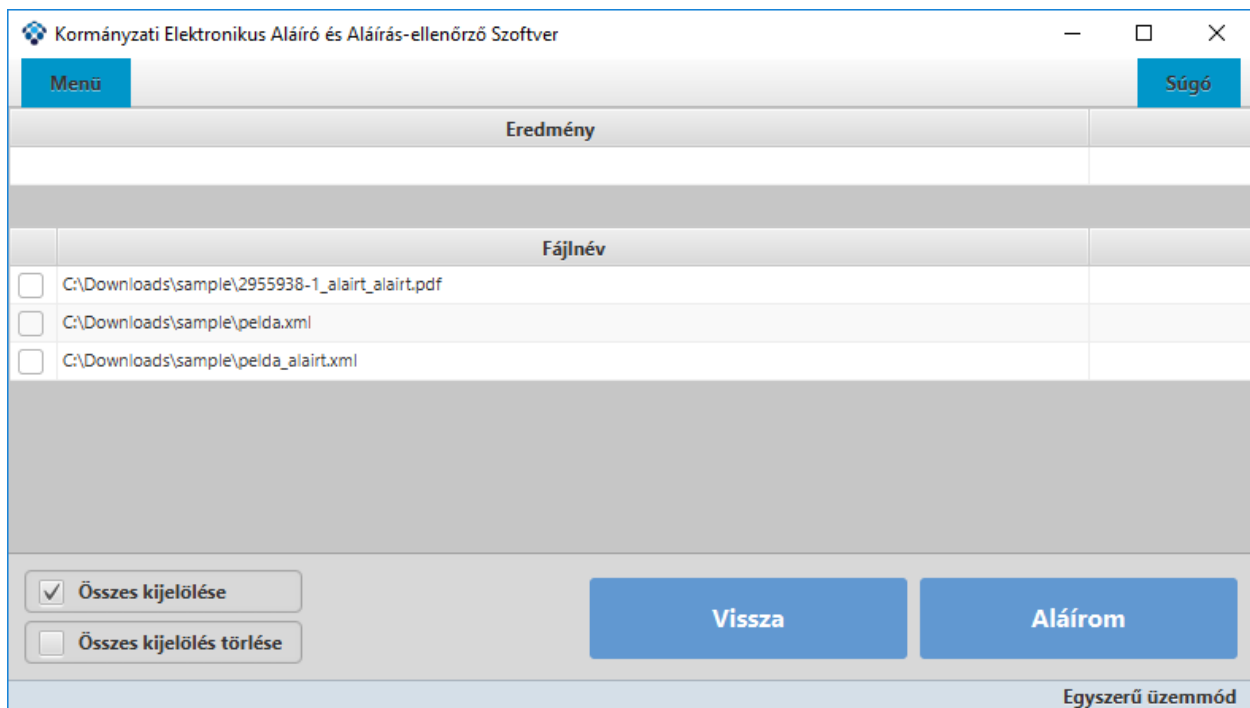
### 4.3.2 Aláírás kötegben


A dokumentumok egy kötegben történő aláírása egyszerű üzemmódban az alábbi felületen történik.

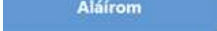
A **Dokumentum aláírás** felületen rá kell kattintani az „**Egy kötegben írom alá mindet**” gombra majd a „**Kiválasztom**” gombra. A fájlkezelőben ki kell választani az a könyvtárt, amelynek fájljai egy kötegben aláírásra kerülnek. Amennyiben a kiválasztott könyvtár alkönyvtárt tartalmaz, annak fájl tartalma is az aláírandó kötegbe kerül.

A könyvtár kiválasztását követően az  gombra kell kattintani ekkor megjelenik az alábbi képernyő, ahol a kijelölt fájlok felsorolásra kerülnek.

Az aláírandó fájlokat ki kell jelölni a fájlnev előtt lévő kijelölő négyzetbe kattintva. Amennyiben az összes fájl aláírásra kerül az „**Összes kijelölése**” négyzetbe kell kattintani, ekkor az összes fájl kijelölésre kerül. Az összes kijelölés törléséhez a „**Összes kijelölés törlése**” négyzetbe kell kattintani.



A  gombra kattintva a képernyő bezárul és visszatérünk a Dokumentum aláírása felületre.

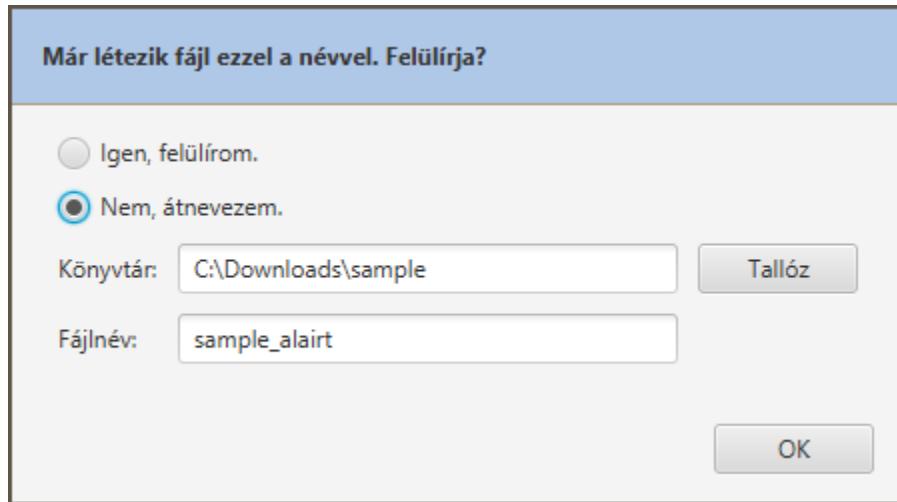
Amikor az aláírandó fájlok megjelölésre kerültek az aláírás elvégzéséhez az  gombra kell kattintani.

Amennyiben már létezik a kijelölt könyvtár nevével ellátott aláírt fájl, a program az alábbi üzenetet küldi. Amennyiben a fájlnév felülírásra kerül az „Igen, felülírom” opciót kell választani.

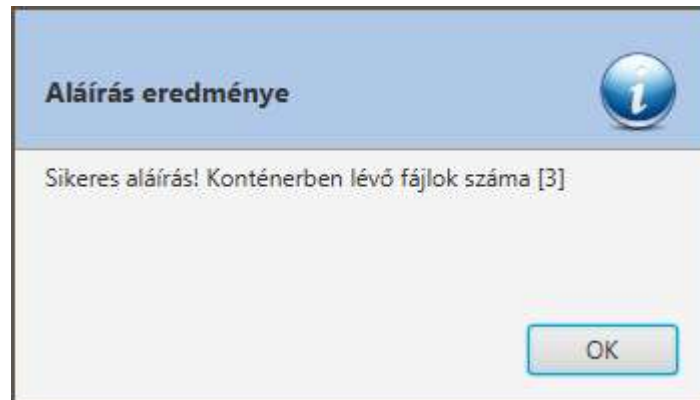


---

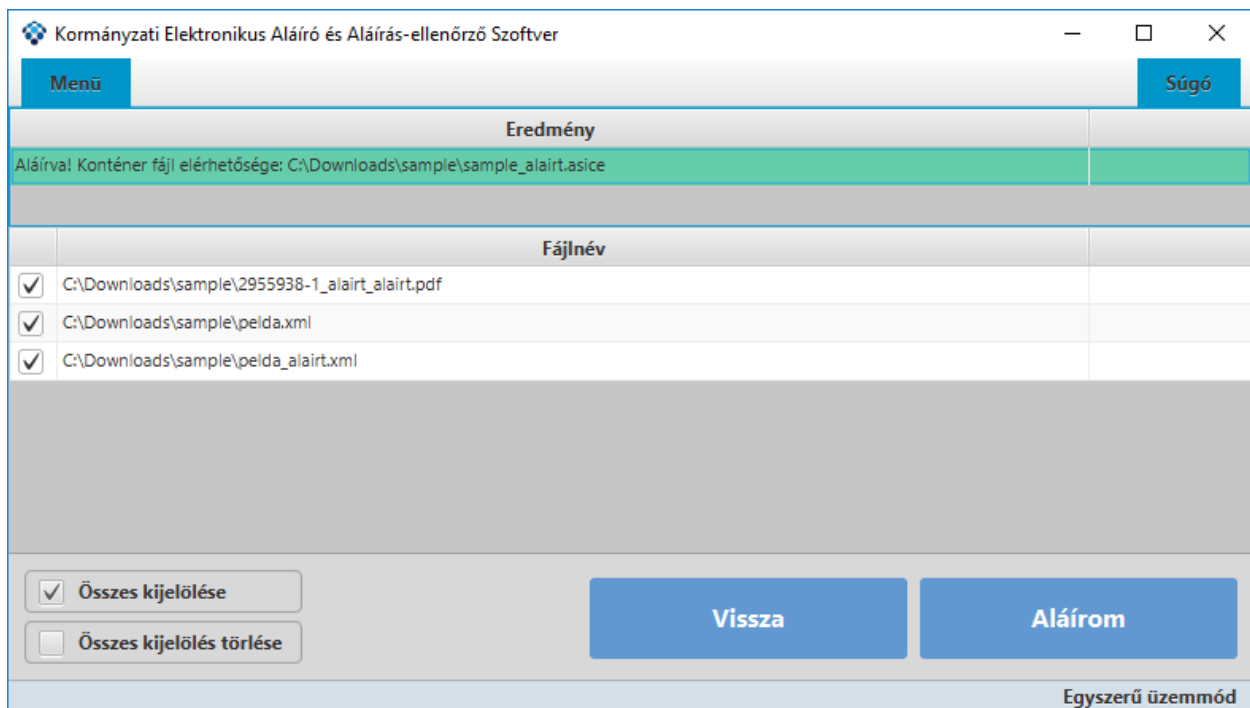
Amennyiben a fájlnev átnevezésre kerül a „**Nem, átnevezem**” gombra kell kattintani és a Fájlnev mezőben a név átírható, illetve a Könyvtár mezőben a „**Tallóz**” gombra kattintva a mentés helyét lehet megadni.



Az aláírás eredményéről a program az alábbi üzenetet küldi.



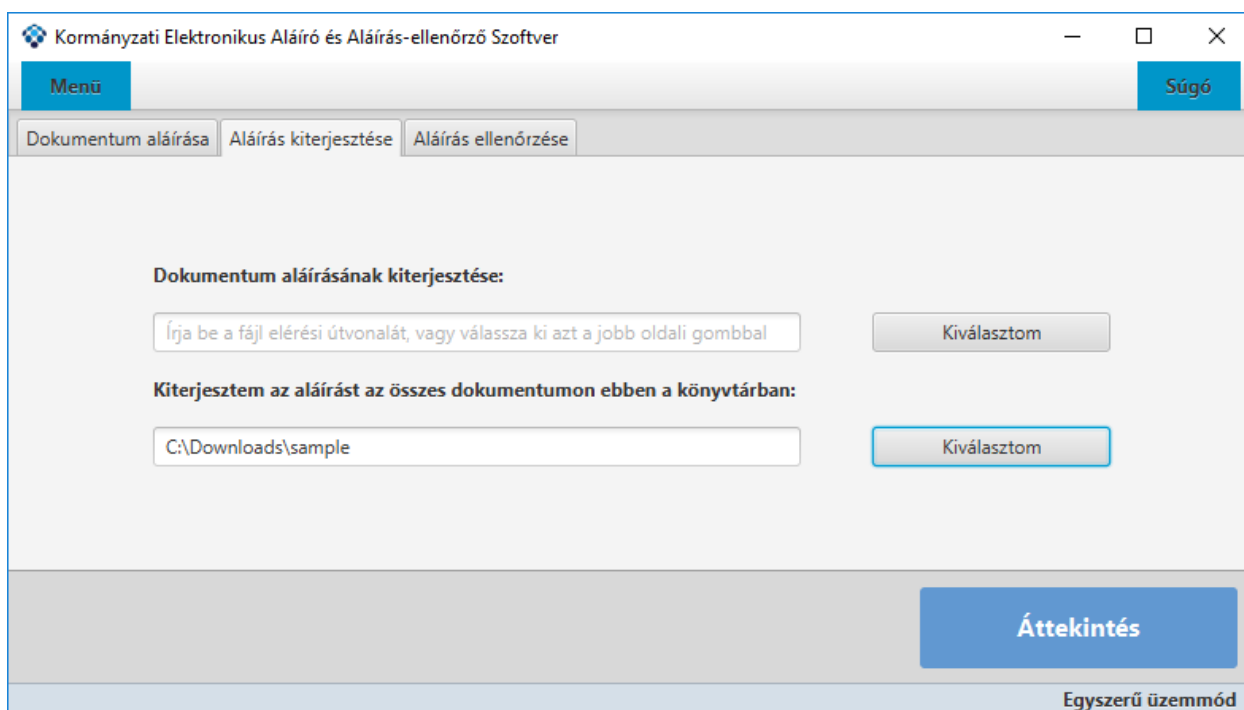
Az **OK** gombra kattintva az üzenet bezárul és az alábbi képernyő jelenik meg, ahol a képernyő felső részén látható, hogy az aláírt fájlokat tartalmazó „**Konténer fájl**” melyik könyvtárba került mentésre.

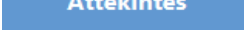


## 4.4 Aláírás kiterjesztése

Amennyiben az egyszerű üzemmódban a dokumentum(ok) aláírását szeretné kiterjeszteni, válasszon az alábbi két lehetőség közül:

- **Dokumentum aláírásának kiterjesztése** (ebben a mezőben csak egy dokumentum választható ki): a „**Kiválasztom**” gombra kattintva a megjelenő Fájlkezelőben válassza ki a kiterjesztendő dokumentumot.
- **Kiterjesztem az aláírást az összes dokumentumon ebben a könyvtárban** (a választott könyvtárban az összes dokumentum kiterjesztésre kerül): a „**Kiválasztom**” gombra kattintva a Fájlkezelőben válassza ki a kiterjesztendő dokumentumokat tartalmazó könyvtárat.



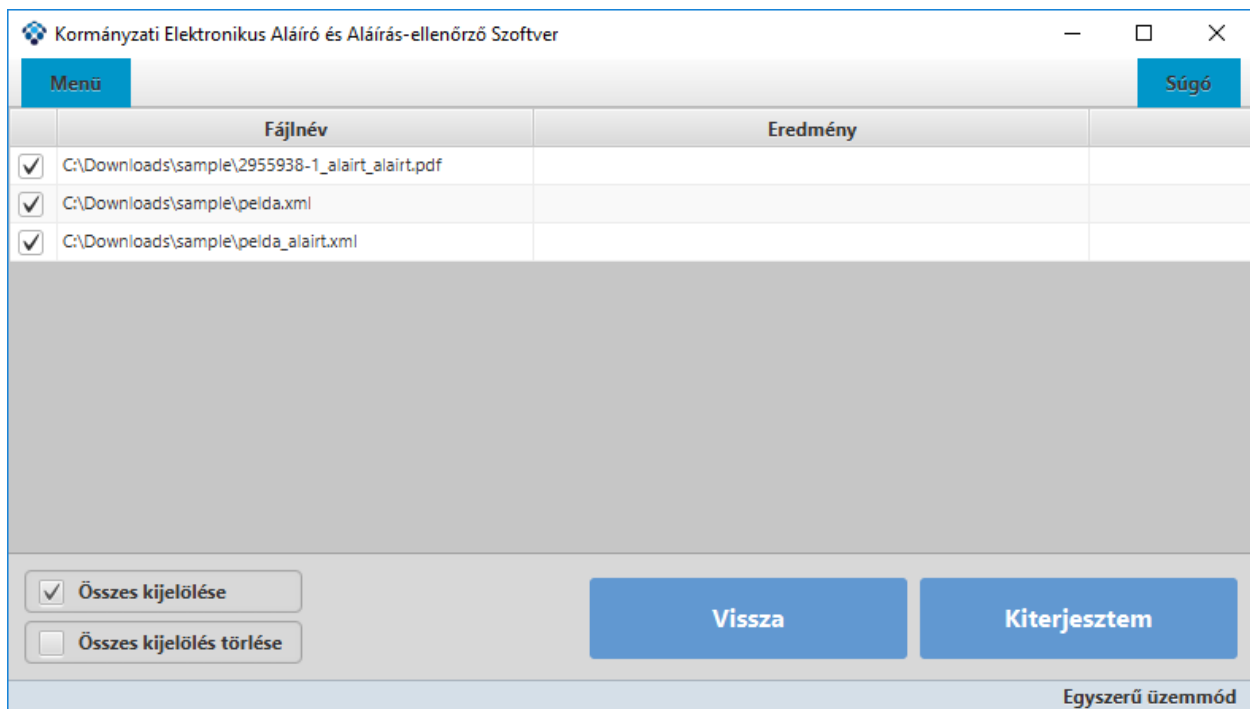
Miután a dokumentum(ok) kiválasztásra került(ek) kattintson az  ikonra. Ezt követően megjelenik az alábbi felület a következő adatokkal:


- Fájlnev
- Eredmény


Kattintson a táblázatban a sorok elején megjelenő kijelölő négyzetbe a kiterjesztendő dokumentum/dokumentumok kiválasztásához.

Az összes dokumentum kijelöléséhez kattintson az „**Összes kijelölése**” gombra.

Amennyiben az összes kijelölést törölni szeretné kattintson az „**Összes kijelölés törlése**” gombra.

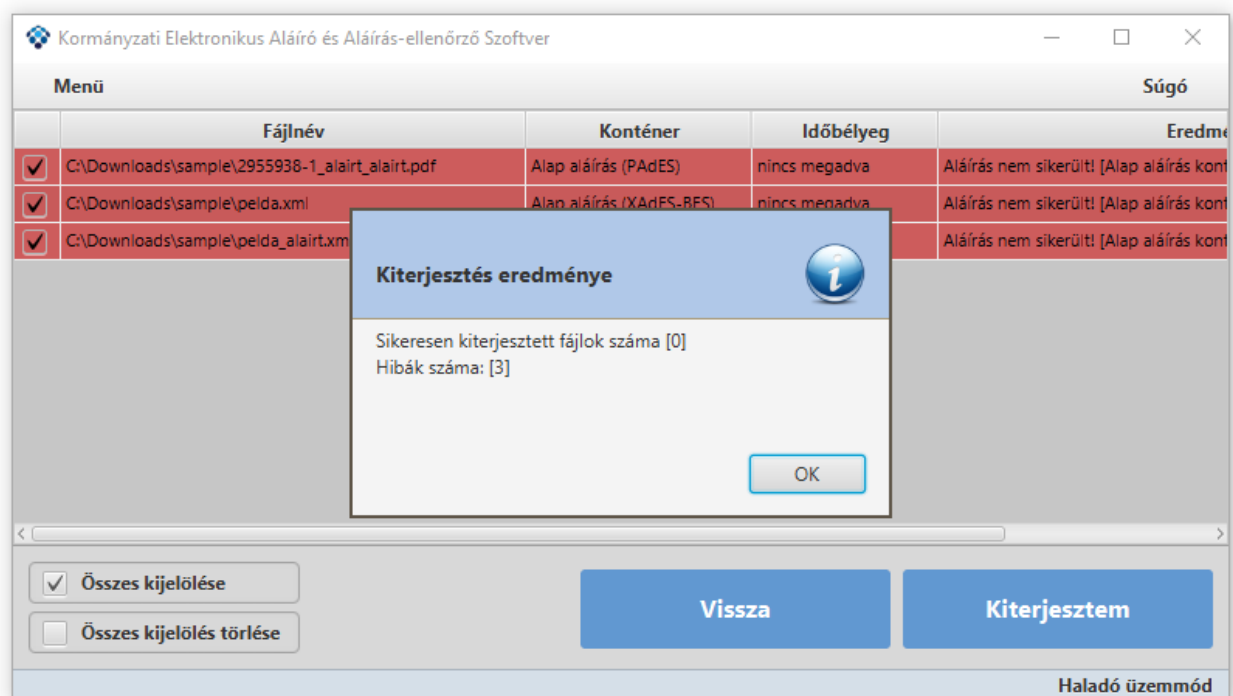


A képernyő bezárásához és az Aláírás kiterjesztése képernyőre való visszatéréshez kattintson a  gombra.

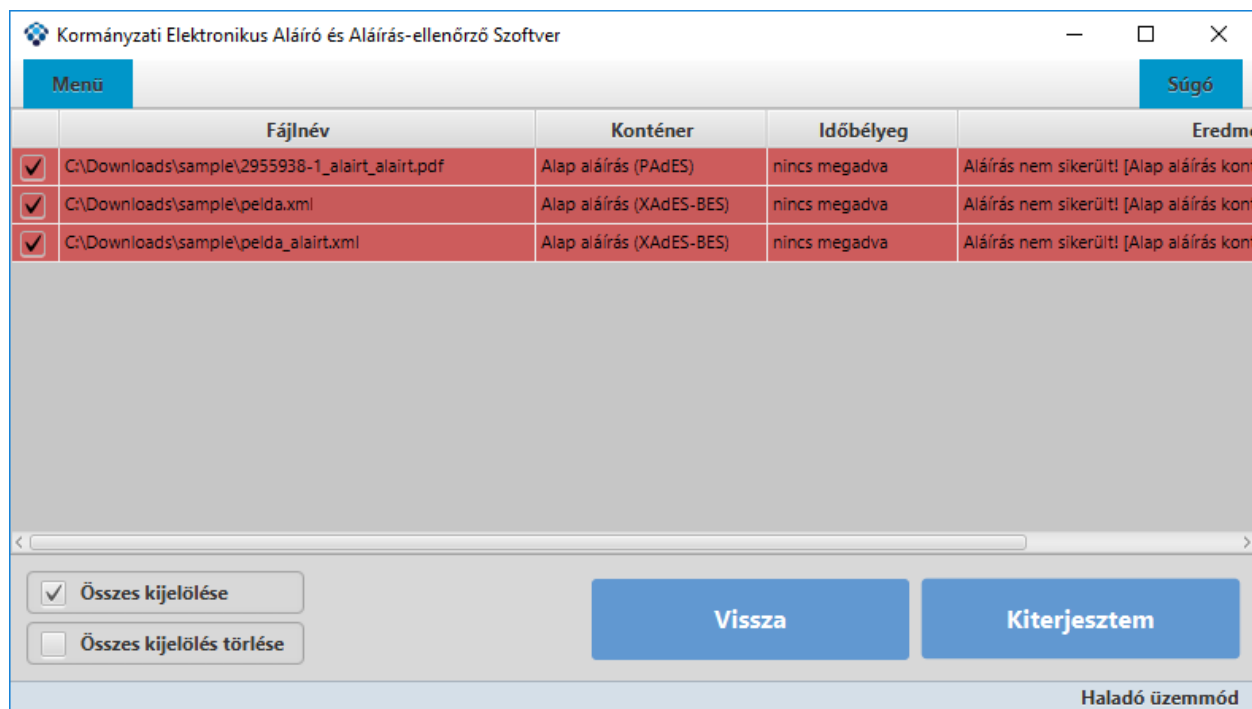
A listában kijelölt dokumentumok kiterjesztéséhez kattintson az  ikonra.

A kiterjesztés eredményéről a program üzenetet küld, amennyiben sikeres, illetve akkor is, ha hibát talál.

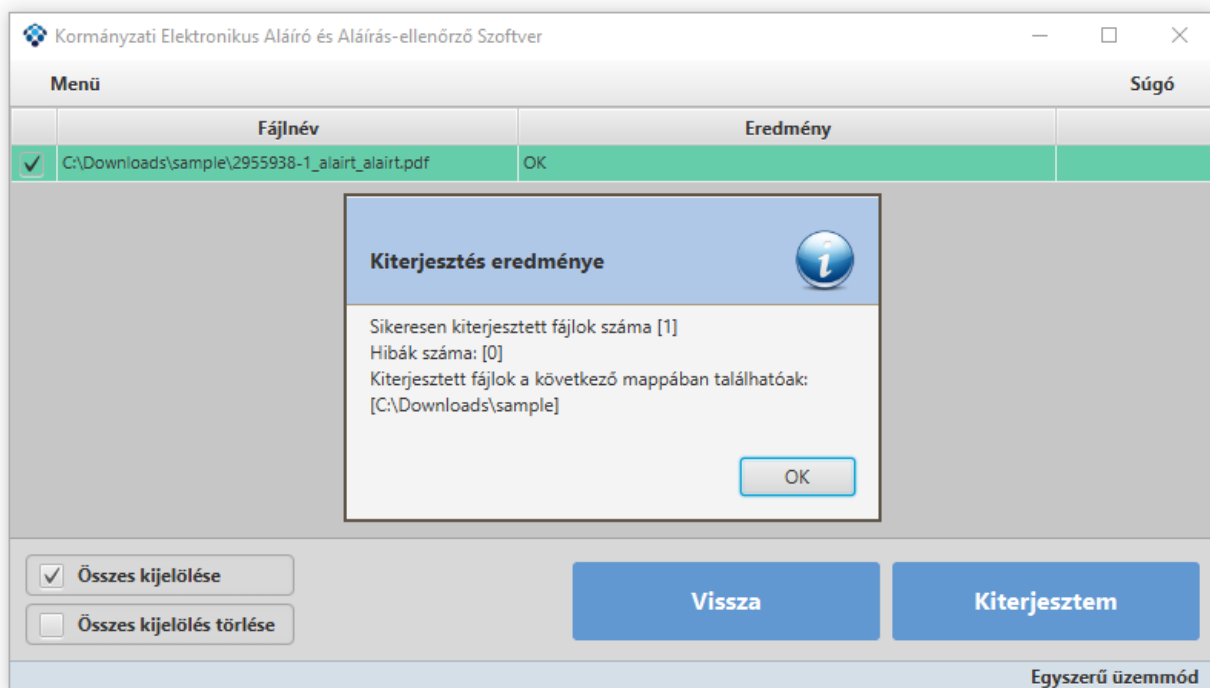
Amennyiben az aláírás kiterjesztés eredménye hibát jelez az alábbi képernyő jelenik meg.



Az **OK** gombra kattintva az információs ablak bezárul és visszatérünk a dokumentum lista képernyőre, ahol az Eredmény oszlopban a program megjeleníti a hiba okát.



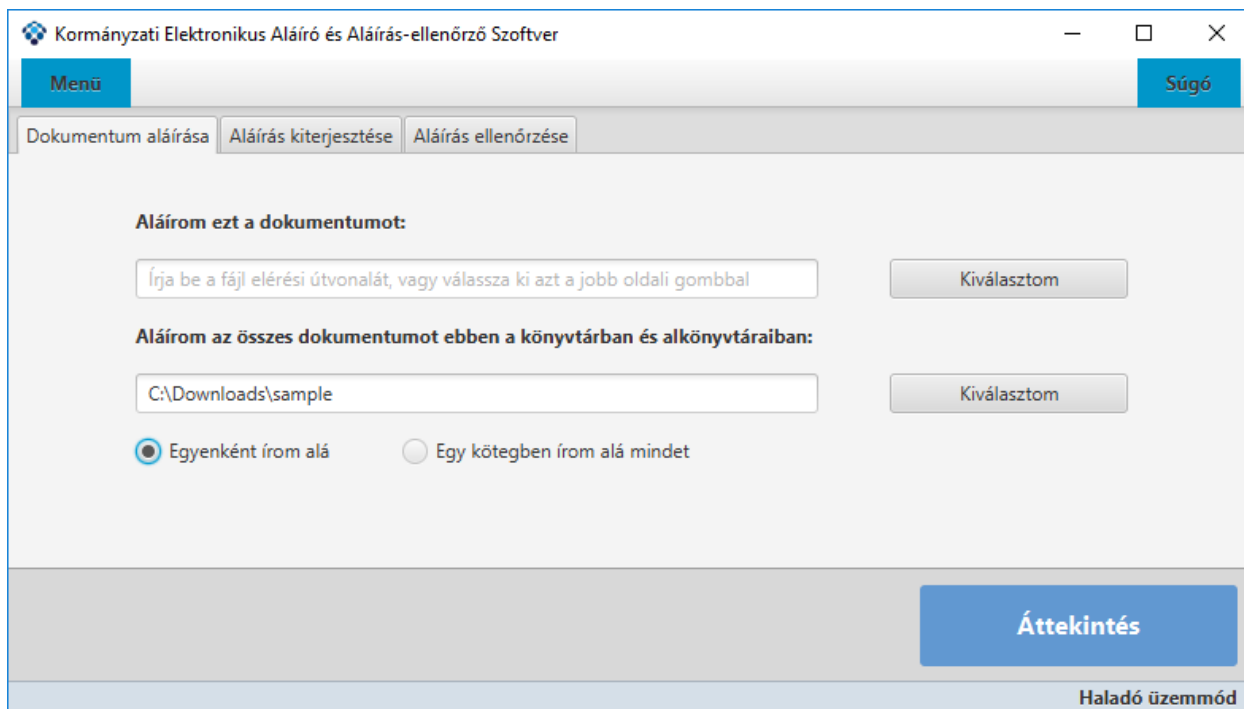
Amennyiben az aláírás eredménye sikeres az alábbi képernyő jelenik meg.



Az **OK** gombra kattintva az információs ablak bezárul és visszatérünk a dokumentum lista képernyőre, ahol az Eredmény oszlopban a program megjeleníti, hogy a kiterjesztés sikerült.

## 5. HALADÓ ÜZEMMÓD

Az alkalmazás haladó üzemmódjába való átlépéshez (amennyiben nem abban van jelenleg, ellenőrizze a jobb alsó sarokban látható üzemmódot) az alapképernyőn található „**Menü**” alatt válassza ki a „**Haladó üzemmód**”-ot.



### 5.1 Menüszerkezet

Válasszon a Dokumentum aláírása és az Aláírás ellenőrzése fülek közül a program alkalmazásának célja szerint.

- A **Dokumentum aláírása** funkcióval aláírhatunk egy vagy több dokumentumot, ezáltal garantálva az aláírt dokumentum(ok) sértetlenségét.
- Az **Aláírás kiterjesztése** funkcióval az aláírt dokumentum(ok) hosszabb távú érvényességgel látható(ak) el.
- Az **Aláírás ellenőrzése** funkcióval megbizonyosodhatunk a dokumentumon lévő aláírás érvényességéről.

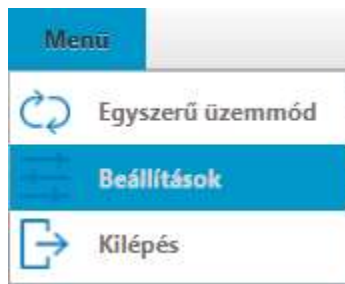
Az alapképernyőn kattintson a Menü ikonra az alábbi funkciók eléréséhez:

- Az **Egyszerű üzemmód** menüpontra kattintva a haladó üzemmódból átválthat egyszerű üzemmódra.
- A **Beállítások** menüpontban lehetőség van az alábbiak megadására:

- 
- Profilok
  - Tanúsítvány profilok
  - Időbélyeg profilok
  - Internet beállítások
  - Általános beállítások
  - Csoportos ellenőrzés fájlípusai
  - Vizuális aláírás beállítások.
- A program bezárásához válassza a Menü alatt a **Kilépés** gombot.

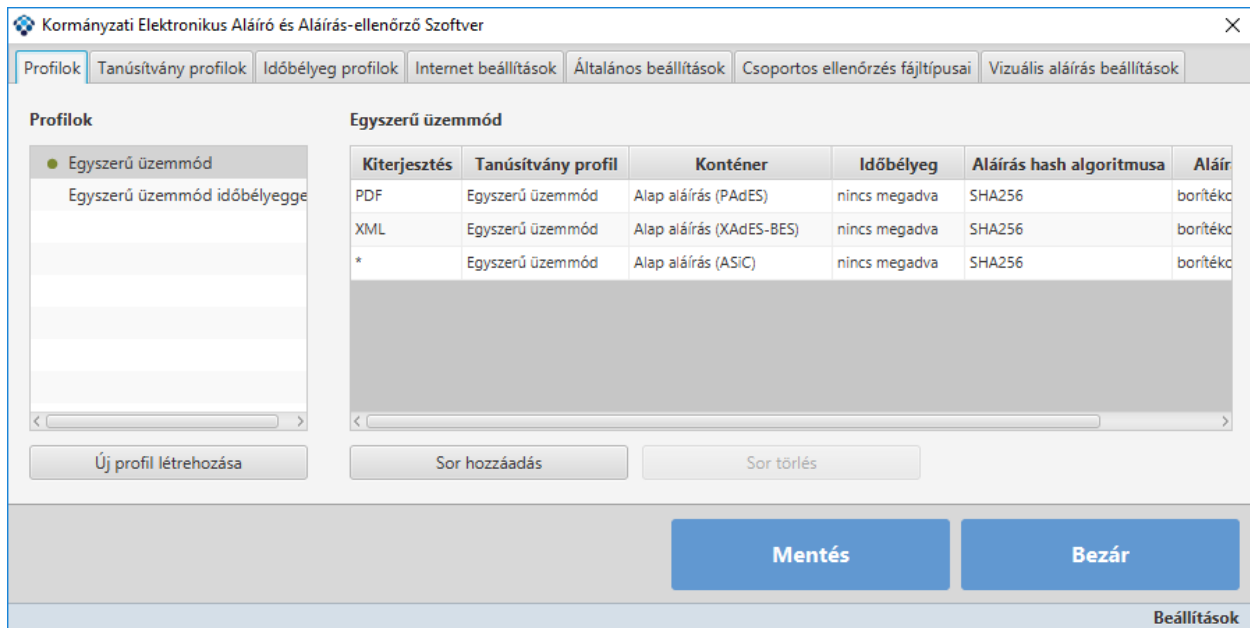
## 5.2 Beállítások

Amikor a program haladó üzemmódban fut a **Menü** ikon alatt a **Beállítások** pontra kattintva lehet elindítani az alkalmazás beállításainak funkciót.



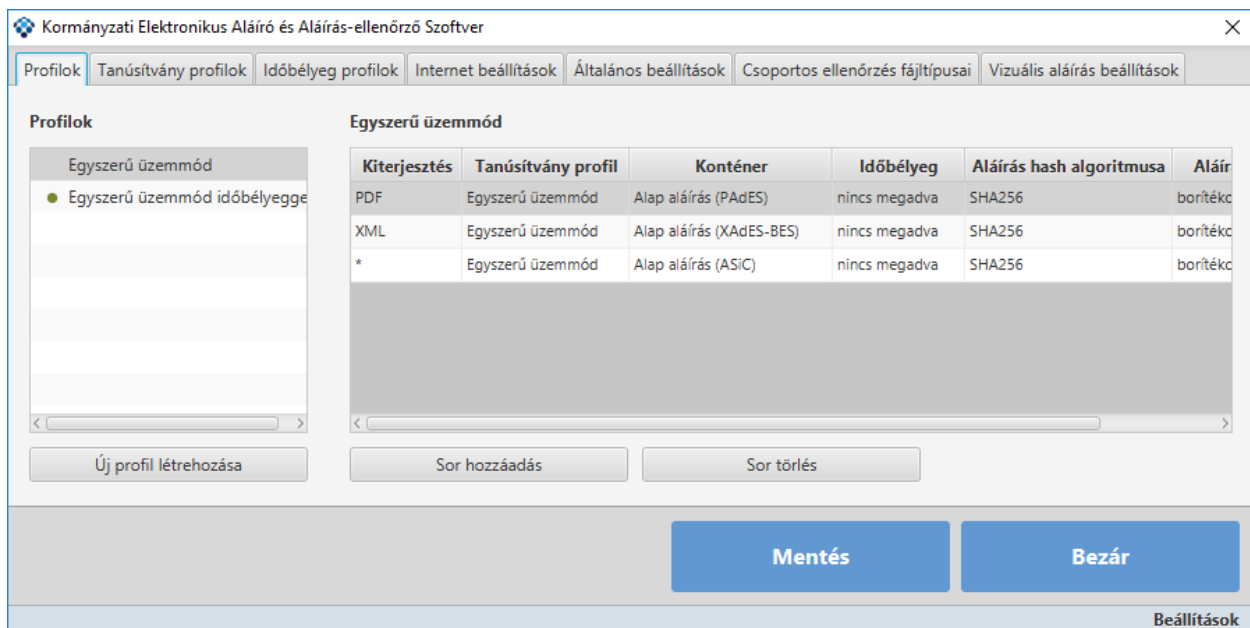
A haladó üzemmódban a **Beállítások** képernyőn az alábbi lehetőségek állnak rendelkezésre:

- Profilok
- Tanúsítvány profilok
- Időbélyeg profilok
- Internet beállítások
- Általános beállítások
- Csoportos ellenőrzés fájlípusai
- Vizuális aláírás beállítások

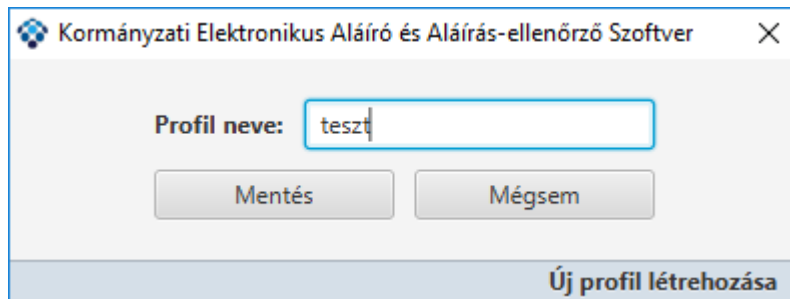


## 5.2.1 Profilok

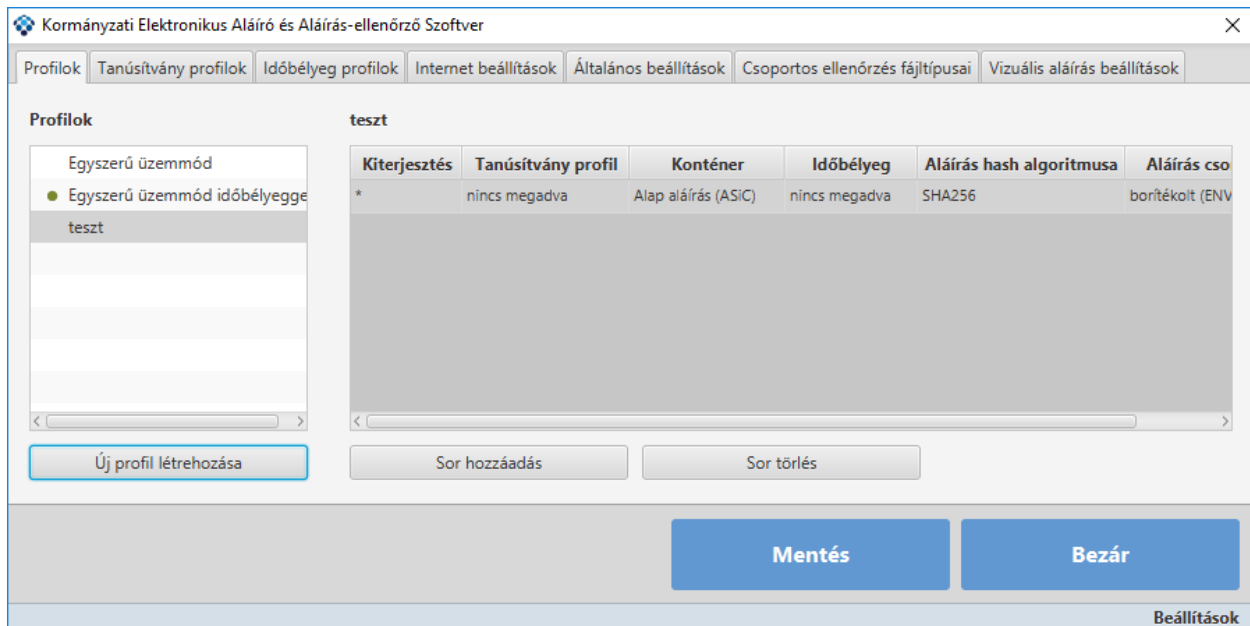
A haladó üzemmódban a **Menü/Beállítások** ikonra kattintva a megjelenő Profil felületen lehet létrehozni új profilokat. Egy profil során minden fájlkiterjesztésre külön megadható, hogy milyen módon készüljön az aláírás. Amelyik fájlkiterjesztésre nem vettünk fel sort, ott a \*-al megjelölt fájlkiterjesztés kerül használatra.



Az „**Új profil létrehozása**” gombra kattintva a megjelenő ablakban a Profil neve mezőbe kell beírni a létrehozni kívánt profil elnevezését.



A **Mentés** gombra kattintva az új profil mentésre kerül és a Profilok között megjelenik.

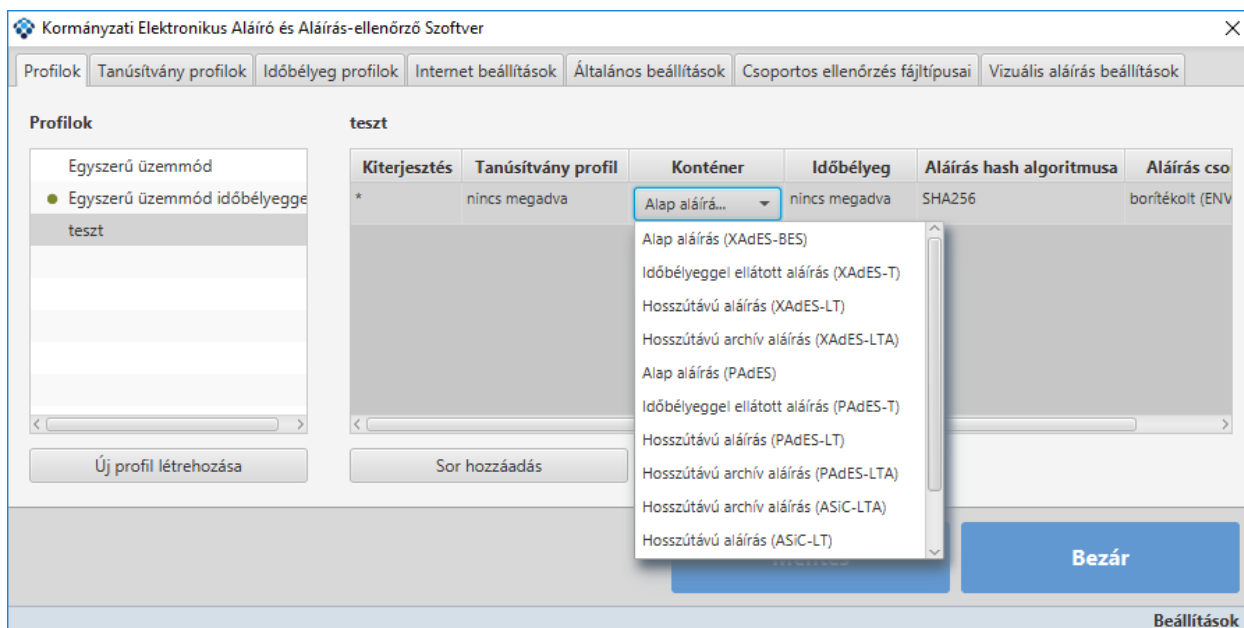


A profilhoz tartozó adatokat a képernyő jobb oldalán megjelenő táblázatban tudjuk megadni. Ehhez ki kell jelölni az adott profilt, majd a táblázat sorába kattintva adhatjuk meg az alábbi adatokat:

- Kiterjesztés – aláírás/aláírás kiterjesztése során ezen kiterjesztésű fájl esetén a soron belül megadott beállítások lesznek érvényben
- Tanúsítvány profil – kiválasztható, hogy melyik előzőleg létrehozott tanúsítványprofil alapján legyen az aláírói tanúsítvány beállítva
- Konténer
  - XML Alap aláírás (**XAdES-BES**)
  - XML Időbélyeggel ellátott aláírás (**XAdES-T**)
  - XML Hosszútávú aláírás (**XAdES-LT**)
  - XML Hosszútávú archív aláírás (**XAdES-LTA**)
  - PDF Alap aláírás (**PAdES**)
  - PDF Időbélyeggel ellátott aláírás (**PAdES-T**)
  - PDF Hosszútávú aláírás (**PAdES-LT**)
  - PDF Hosszútávú archív aláírás (**PAdES-LTA**)

- ASiC Alap aláírás (**ASiC**)
- ASiC Időbélyeggel ellátott aláírás (**ASiC-T**)
- ASiC Hosszútávú aláírás (**ASiC-LT**)
- ASiC Hosszútávú archív aláírás (**ASiC-LTA**)
- Időbélyeg - kiválasztható, hogy melyik előzőleg létrehozott időbélyegprofil alapján legyen az időbélyegzés végrehajtva (minimum **T**-s konténer esetén)
- Aláírás hash algoritmus
  - SHA256
  - SHA512
- Aláírás csomagolása
  - borítékolt (ENVELOPED)
  - borítékolással befoglalt (ENVELOPING)
  - különálló (DETACHED)

A kiválasztott profilhoz kapcsolódóan az egyes adatmezőkbe kattintva értéklistánból választhatók az adatok.

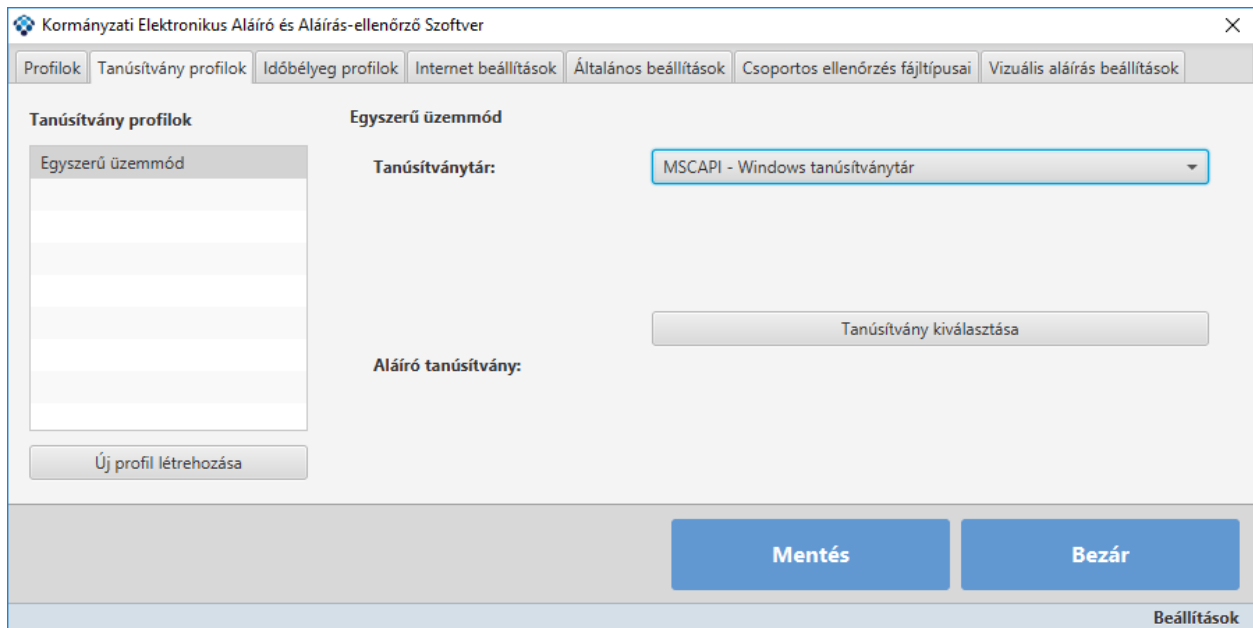


A „**Sor hozzáadása**” gombra kattintva az adott profilhoz újabb adatsort tudunk hozzáadni. A profilra vonatkozó adatokat az adatmezőkbe kattintva tudjuk értéklistánból kiválasztva rögzíteni.

A „**Sor törlése**” gombra kattintva a kijelölt sor törlésre kerül.

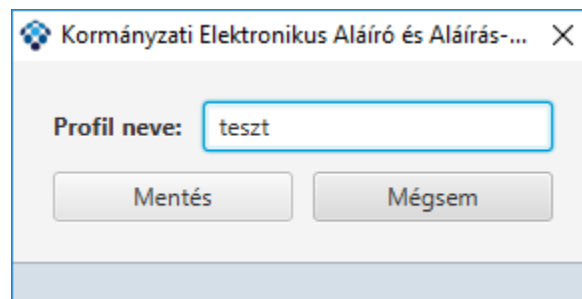
## 5.2.2 Tanúsítvány profilok

A haladó üzemmódban a Beállítások funkció alatt a Tanúsítvány profilok fülre kattintva a megjelenő felületen új tanúsítvány profilt lehet létrehozni tanúsítványtár és Aláíró tanúsítvány megadásával.



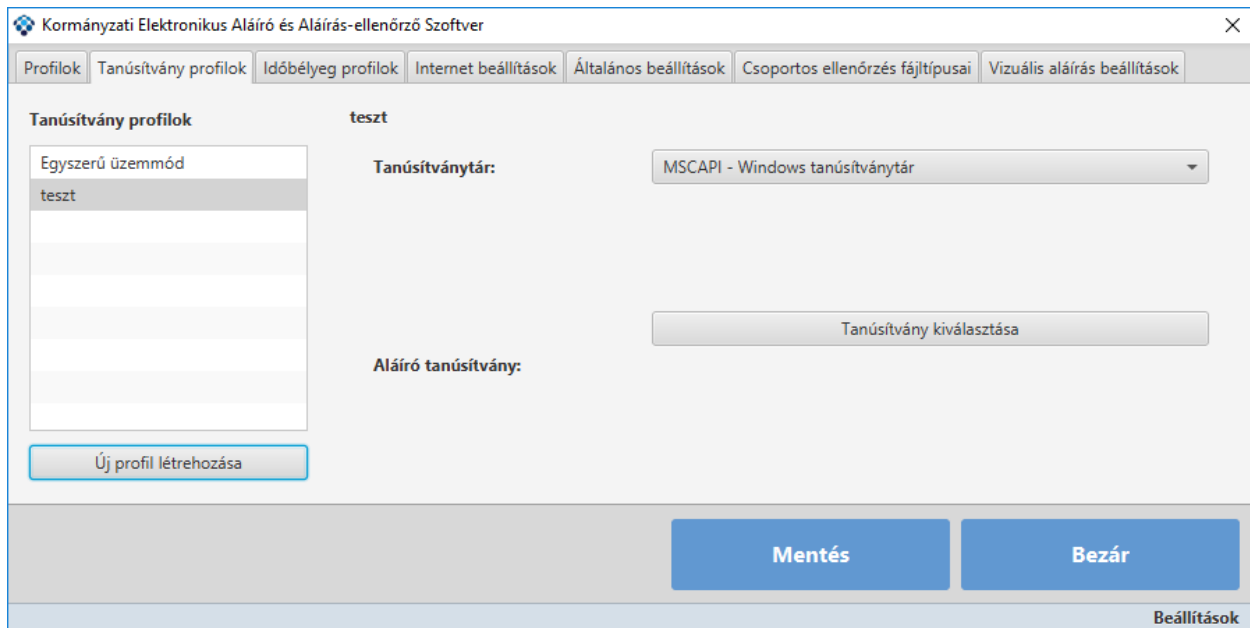
### 5.2.2.1 Új tanúsítvány profil létrehozása

Az új tanúsítvány profil létrehozásához kattintson az „**Új profil létrehozása**” gombra, majd a megjelenő ablakban adja meg a tanúsítvány profil nevét.



Amennyiben a Profil neve rögzítésre kerül, kattintson a **Mentés** gombra.

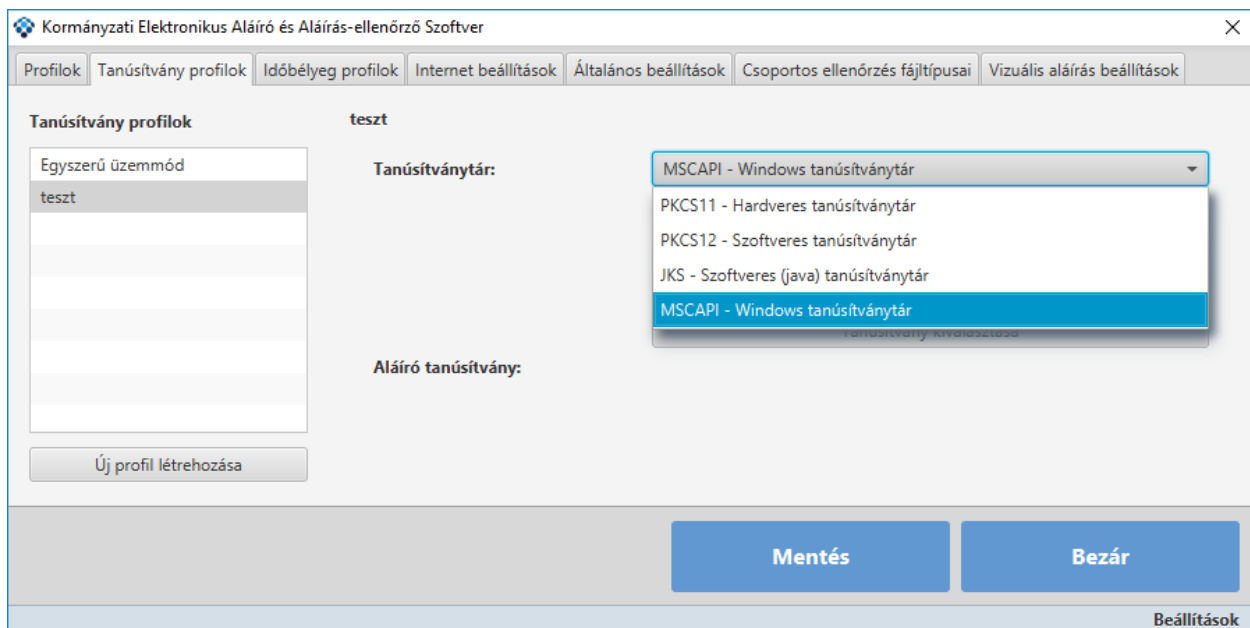
Amennyiben visszatér a Tanúsítvány profilok felületre és nem akarja menteni a megadott adatot kattintson a **Mégsem** gombra.



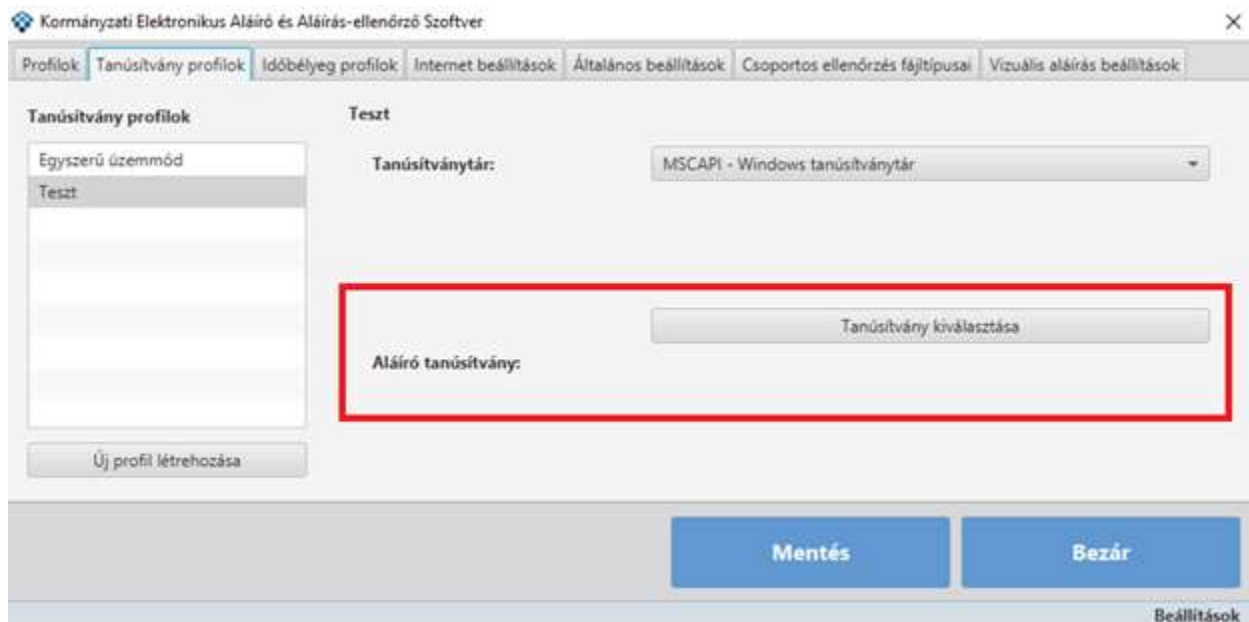
### 5.2.2.2 Tanúsítványtár és Aláíró tanúsítvány megadása

A létrehozott Tanúsítvány profilhoz Tanúsítványtárat és Aláíró tanúsítványt lehet megadni.

A **Tanúsítványtár** értékmezőben a nyílra kattintva a megjelenő értéklistából válassza ki a rögzíteni kívánt tanúsítványtár típust.



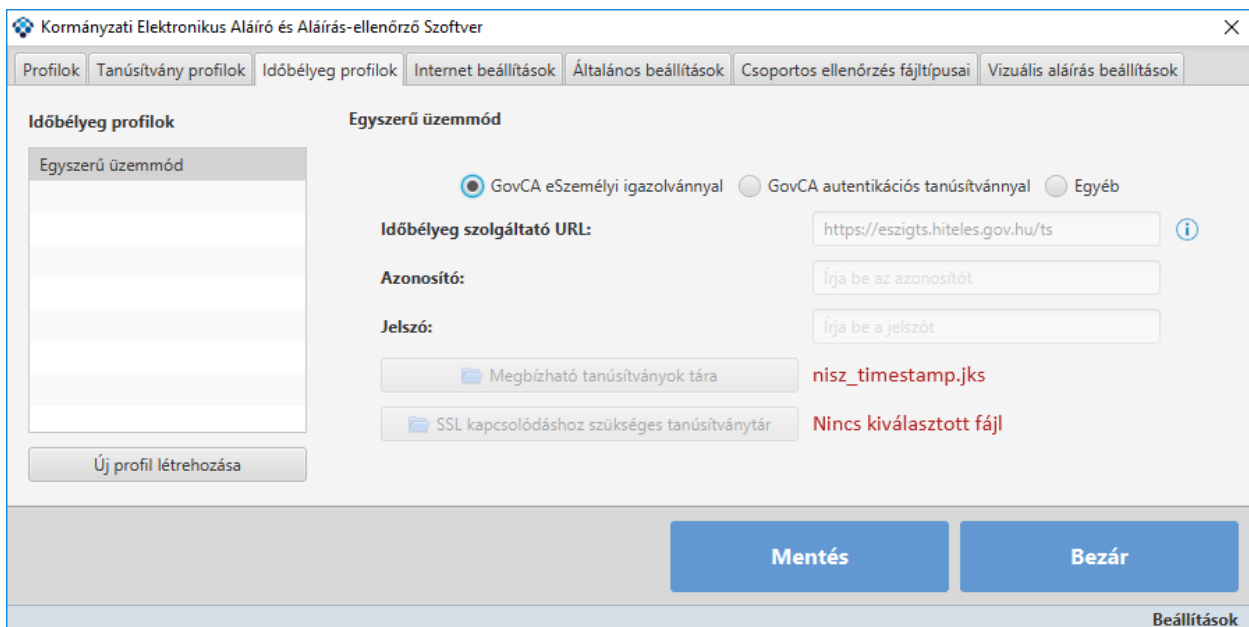
Az **Aláíró tanúsítvány** megadásához kattintson a „**Tanúsítvány kiválasztása**” gombra, majd a megjelenő felületen válassza ki az aláíró tanúsítványt.



### 5.2.3 Időbélyeg profilok

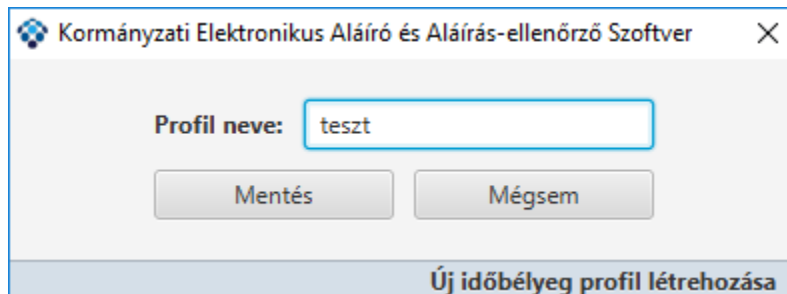
A haladó üzemmódban a Beállítások funkció alatt az Időbélyeg profilok fülre kattintva a megjelenő felületen új időbélyeg profilt lehet létrehozni. Az időbélyeg profil típusa a következők lehetnek:

- GovCA eSzemélyi igazolvánnyal
- GovCA autentikációs tanúsítvánnyal
- Egyéb



### 5.2.3.1 Új időbélyeg profil létrehozása

Az új időbélyeg profil létrehozásához kattintson az „**Új profil létrehozása**” gombra, majd a megjelenő ablakban adja meg az Időbélyeg profil nevét.



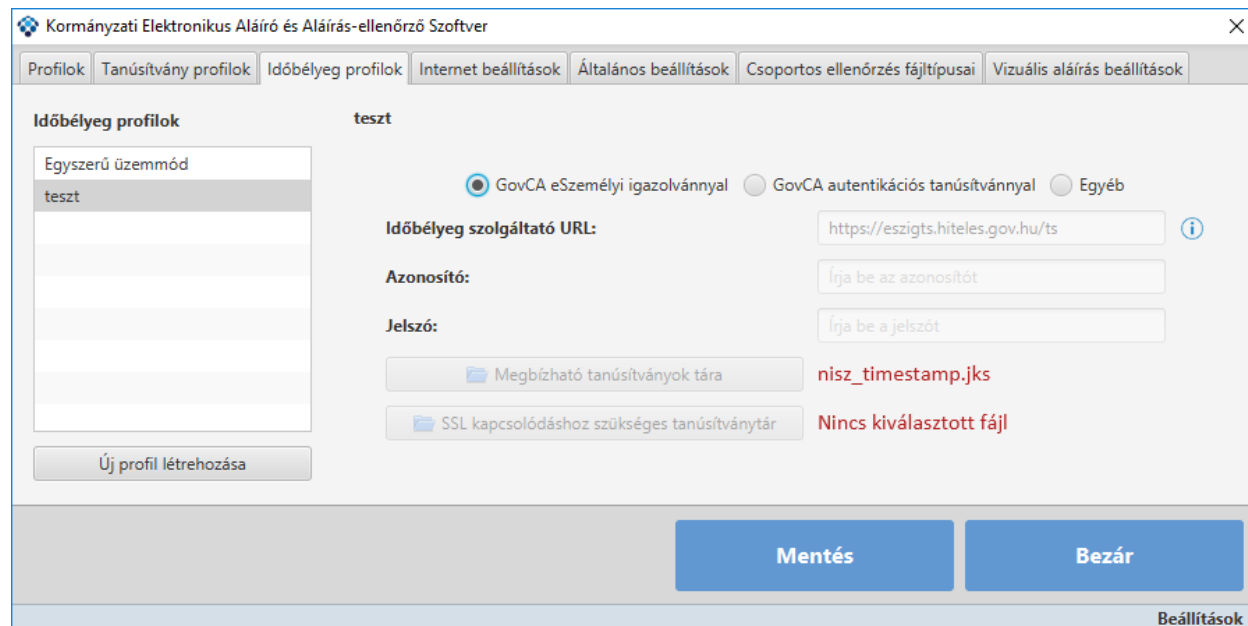
Amennyiben a Profil neve rögzítésre kerül, kattintson a **Mentés** gombra.

Amennyiben visszatér a Tanúsítvány profilok felületre és nem akarja menteni a megadott adatot kattintson a **Mégsem** gombra.

Időbélyeg profil típusának kiválasztása:

#### GovCA eSzemélyi igazolvánnyal

Ennél a típusnál az eSzemélyi igazolvánnyal történő aláírásnál használt tanúsítvánnyal lesz az időbélyegkézés is aláírva. Mivel az időbélyegzés kérés az **eSzemélyin** lévő tanúsítvánnyal lesz aláírva, ezen funkció használatához **eSzemélyi** szükséges.




#### GovCA autentikációs tanúsítvánnyal

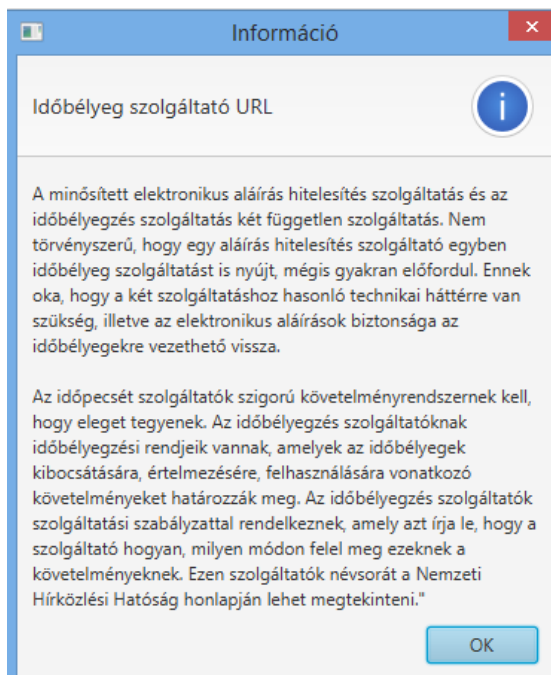
GovCA autentikációs tanúsítvány kiválasztása esetén GovCA irányába történik egy időbélyegkérés. Ehhez az időbélyegkéréshez szükséges egy autentikációs tanúsítvány, amelyet az SSL kapcsolódáshoz szükséges tanúsítványtár gombra kattintva állíthat be.

## Egyéb

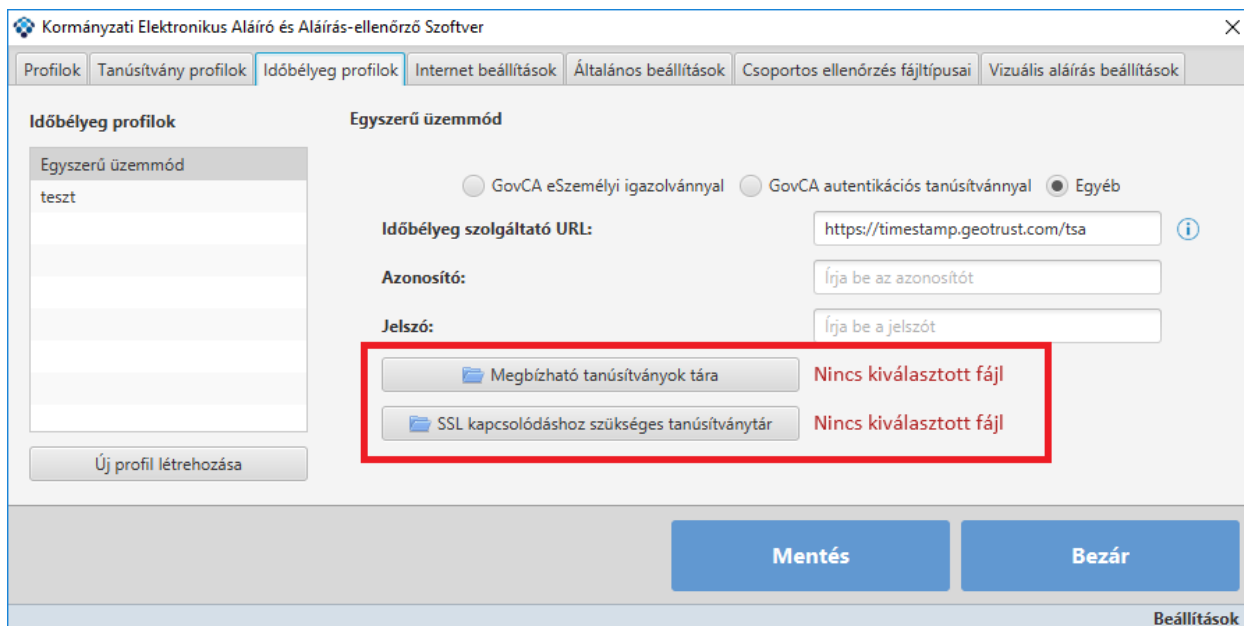
Általános időbélyegkéréshez szükséges beállításokat itt lehet megadni. Tájékozódjon időbélyeg szolgáltatójánál, a szükséges beállítások tekintetében.


Írja be az Időbélyeg szolgáltató URL mezőbe az Időbélyeg szolgáltató URL címét, és amennyiben azonosító/jelszó páros szükséges az azonosításhoz (alap autentikáció (basic authentication)), akkor azt szintén megadhatja.

Az az Időbélyeg szolgáltató URL adatmező melletti  gombra kattintva információt olvashat az időbélyeg szolgáltatással kapcsolatban.



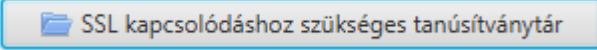
Az **OK** gombra kattintva az információs ablak bezárul.



A  **Megbízható tanúsítványok tára** ikonra kattintva a Fájlközelítőből ki lehet választani egy megbízható tanúsítványtárat.(angol neve: TrustStore), ezt a beállítást csak HTTPS protokollt használó Időbélyeg szolgáltató esetén szükséges kitölteni. A kiválasztott tanúsítványtár az időbélyeg szolgáltató szerver

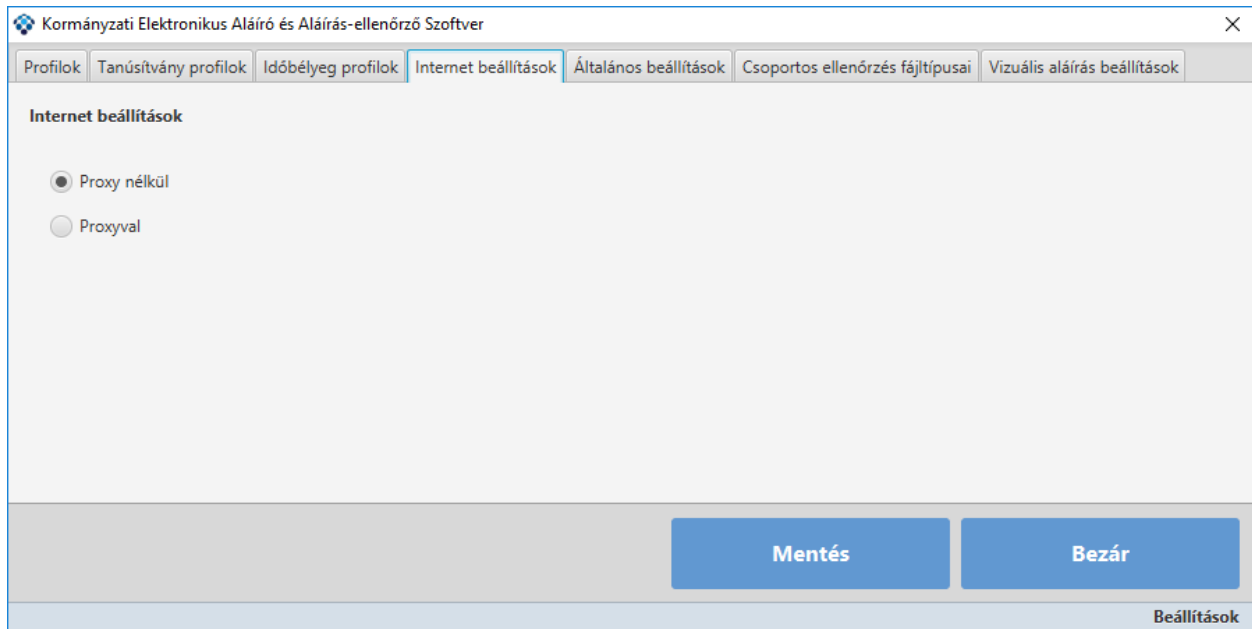
---

tanúsítványát kell tartalmazza.

Az  ikonra kattintva a Fájlközpontból ki lehet választani az SSL kapcsolódáshoz szükséges tanúsítványtárat.(angol neve: KeyStore), ezt a beállítást csak HTTPS protokollt használó Időbélyeg szolgáltató esetén szükséges kitölteni. A kiválasztott tanúsítványtár a kliens autentikálásához szükséges tanúsítványt kell tartalmaznia.

## 5.2.4 Internet beállítások

Az Internet beállítások funkció a haladó üzemmódban megegyezik az egyszerű üzemmódnál leírtakkal. (lásd 4.2.2 fejezet).



## 5.2.5 Általános beállítások

A haladó üzemmódban a **Beállítások** funkció alatt az **Általános beállítások** fülre kattintva a megjelenő felületen az alábbi beállításokat lehet megadni.

Kormányzati Elektronikus Aláíró és Aláírás-ellenőrző Szoftver

[Profilok](#)
[Tanúsítvány profilok](#)
[Időbélyeg profilok](#)
[Internet beállítások](#)
[Általános beállítások](#)
[Csoportos ellenőrzés fájltypusai](#)
[Vizuális aláírás beállítások](#)

### Általános beállítások

**Kimeneti mappa:**
 **Fájlokkal megegyező helyen**
 Tallózza ki a könyvtárat

**Aláírt utótag (postfix):**

**Kiterjesztett utótag (postfix):**

**Automatikus frissítések keresése:**

**Nem kérek figyelmeztetést időbélyeg kérés előtt:**

Beállítások

### 5.2.5.1 Kimeneti mappa

Amennyiben a **Kimeneti mappa** a fájlokkal megegyező helyen legyen, kattintson a **Fájlokkal megegyező helyen** radio gombra.

**Kimeneti mappa:**
 **Fájlokkal megegyező helyen**
 Tallózza ki a könyvtárat

Amennyiben más helyen legyen a Kimeneti mappa, kattintson a  gombra és a megjelenő fájlkezelőben válassza ki a mappa helyét.

### 5.2.5.2 Kimeneti fájl utótagjai (postfix-ek)

Itt adható meg az aláírás/kiterjesztett fájl elnevezésében szereplő utótag. Alapesetben, az adatmezőben az „**alairt**”/ „**kiterjesztett**” szöveg jelenik meg, amennyiben más elnevezést kíván megadni, kattintson a megfelelő adatmezőbe és írja be az utótag szövegét.

**Aláírt utótag (postfix):**

**Kiterjesztett utótag (postfix):**

### 5.2.5.3 Automatikus frissítések keresése

Az alkalmazás lehetőséget biztosít az alkalmazás frissítésének (új verziójának) automatikus kereséséhez

a program indítása során. A frissítések automatikus keresését az alábbi jelölőnégyzet kiválasztásával állíthatja be.

Automatikus frissítések keresése:

#### 5.2.5.4 Figyelmeztetés Időbélyeg kérés előtt

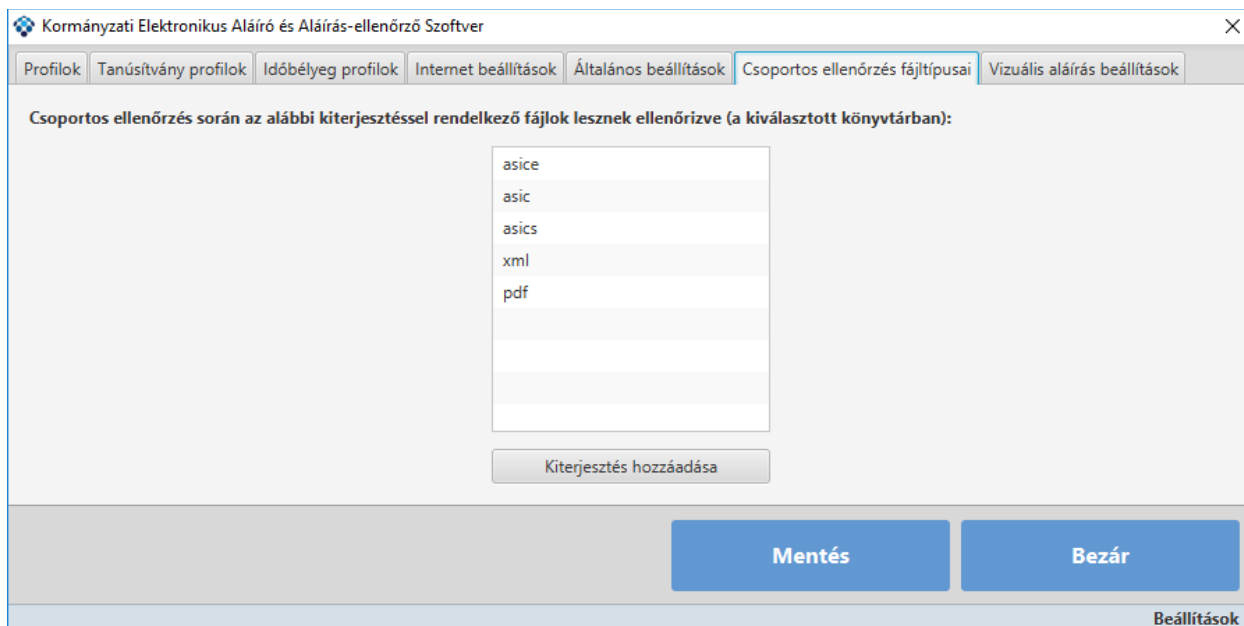
GovCA eSzemélyi igazolvánnyal típusú időbélyeg kérések esetén az időbélyegzés kérés is aláírásra kerül az eSzemélyin lévő tanúsítvánnyal. Annak érdekében, hogy a felhasználó lássa, hogy mit ír alá, ezért az aláírandó időbélyeg kérés tartalmát szükséges felmutatni. Amennyiben ezt nem kívánja megtekinteni (ne jöjjön fel minden ilyen aláírás esetén) ez a funkció ki is kapcsolható.

Nem kérek figyelmeztetést időbélyeg kérés előtt:

#### 5.2.6 Csoportos ellenőrzés fájltypusai

A csoportos ellenőrzés fájltypusai felületen lehet megadni, hogy milyen kiterjesztésű fájlokat ellenőrizzen a program, amikor a felhasználó kiválaszt egy könyvtárat ellenőrzésre.

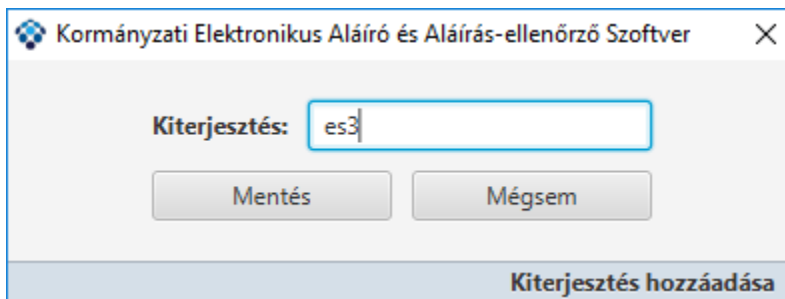
A felület megnyitásakor látszódik egy lista azokkal a kiterjesztésekkel, amelyek a programban alapértelmezettként beállításra kerültek. Az alapbeállításban szereplő fájltypusok törölhetők, illetve újabbak is hozzáadhatók.



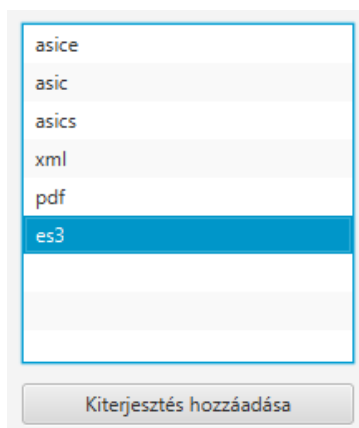
##### 5.2.6.1 Fájltypus hozzáadása a listához

---

Újabb fájl típus hozzáadásához kattintson a „**Kiterjesztés hozzáadása**” gombra majd írja be a kiterjesztés nevét és nyomja meg a „**Mentés**” gombot.

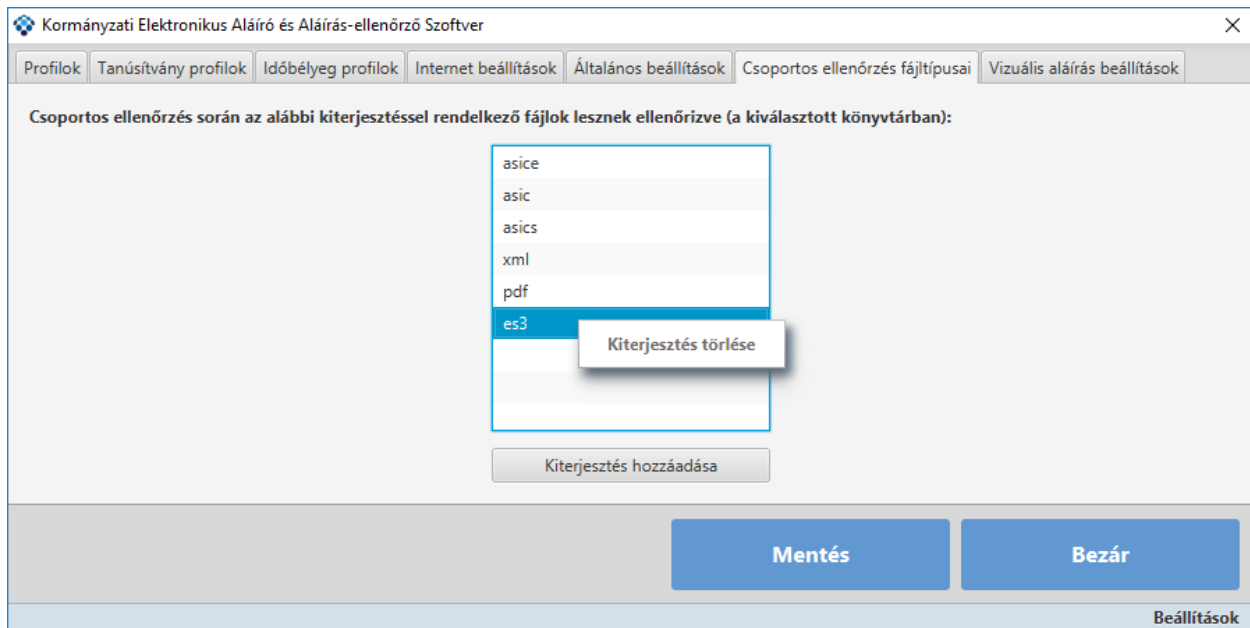


A mentés gombra kattintva a megadott fájl kiterjesztés a listában megjelenik.

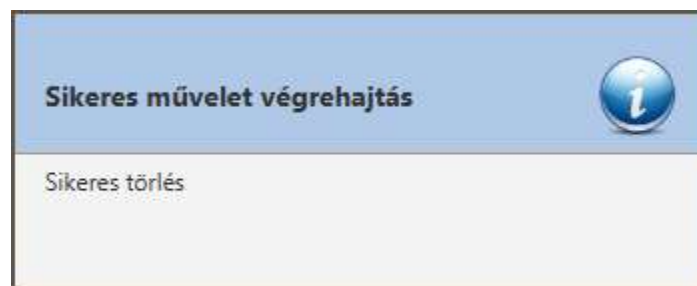


### 5.2.6.2 Fájl típus törlése a listából

Amennyiben a listából törölni szeretne, jelölje ki a törölni kívánt kiterjesztést, majd nyomja meg a jobb egér gombot, majd kattintson a „**Kiterjesztés törlése**” gombra.

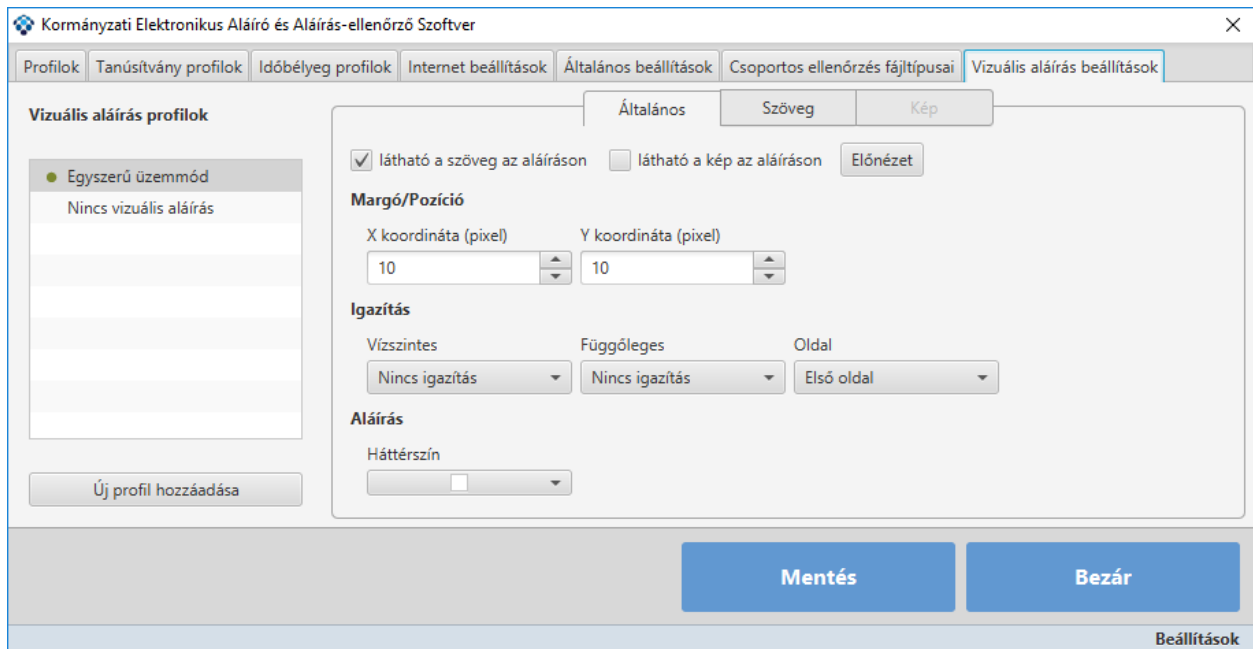


A kiterjesztés törléséről a program az alábbi rendszerüzenetet küldi.



## 5.2.7 Vizuális aláírás beállítások

A vizuális aláírás beállítások felület a Haladó üzemmódban a „**Menü**” ikon alatt a Beállítások menüpontra kattintva jelenik meg. Ezen a felületen lehetőség van beállítani az elektronikus aláírással ellátott dokumentum felületén az aláírás elhelyezkedését illetve a vizuális megjelenését.

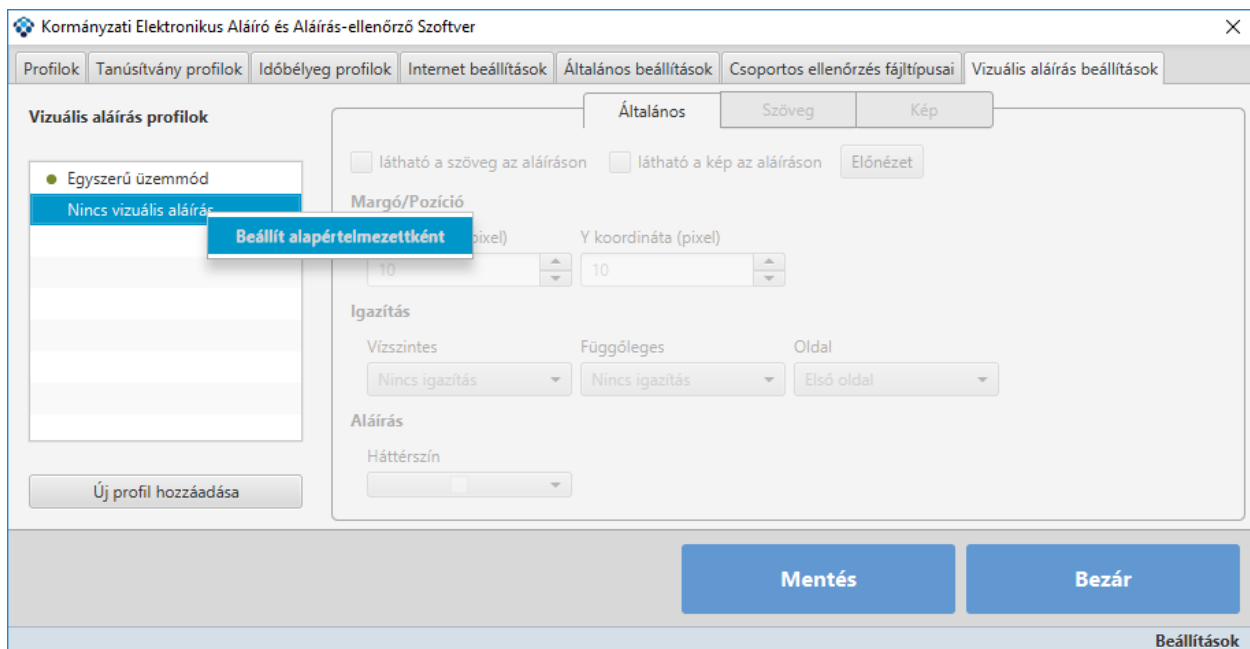


A haladó üzemmódban a vizuális aláírás beállítások funkció működése fő vonalakban megegyezik az egyszerű üzemmódban leírt működéssel, amelynek leírását a 4.2.3 fejezet tartalmazza. A különbség a haladó mód esetében az, hogy lehetőség van profilok létrehozására is.

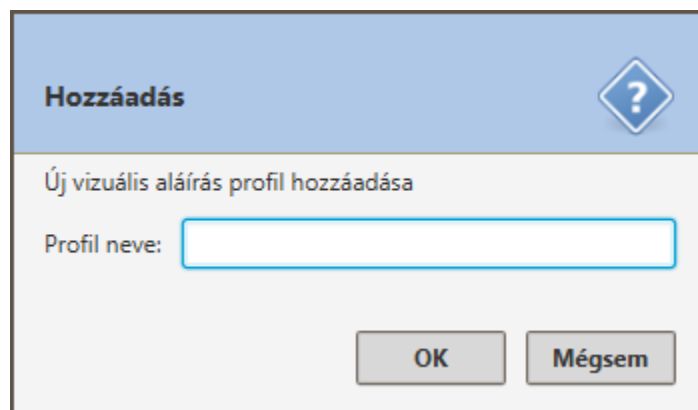
A profilok között két nem törölhető profil van:

- Egyszerű üzemmód (az egyszerű üzemmódban beállított tulajdonság ebben a profilban kerül beállításra)
- Nincs vizuális aláírás (ahogy a neve is mutatja, nincs vizuális aláírás megjelenítés)

A haladó mód által használt profilt az alapértelmezett profil tulajdonsággal tudjuk beállítani a context menüben (egér jobb gomb a kiválasztott profilnéven)

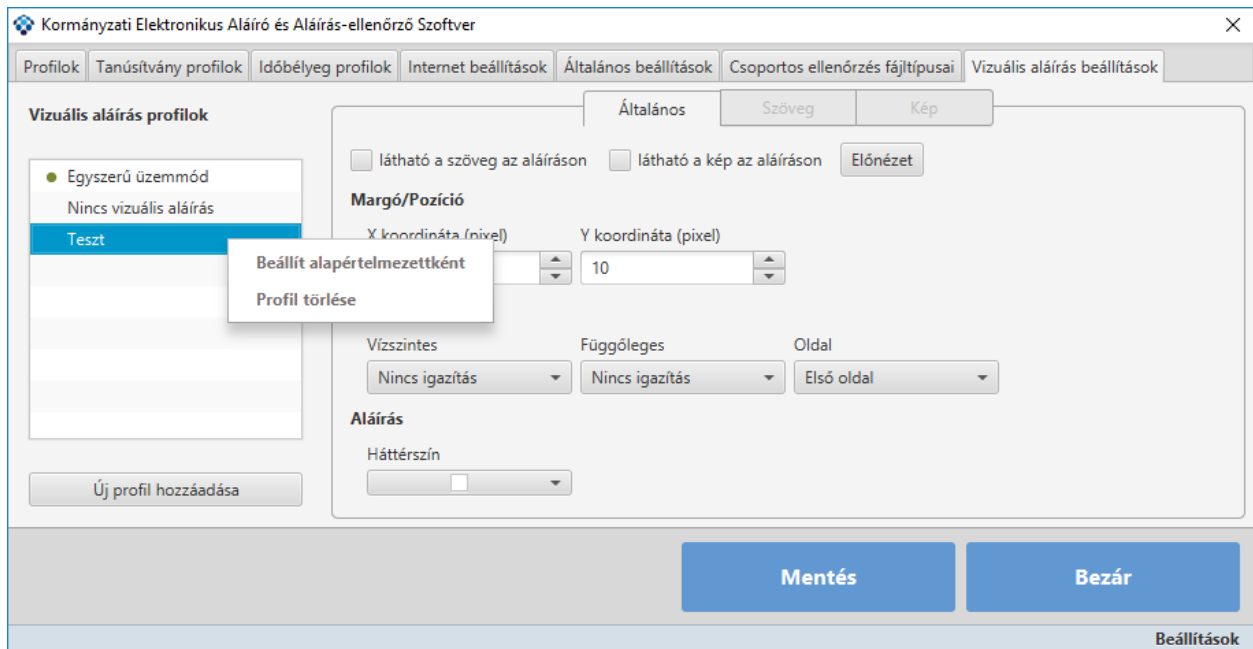


Új profil létrehozás az „Új profil hozzáadása” gomb segítségével lehetséges.



Itt a név megadása után válasszuk az „OK” gombot, amennyiben létre kívánjuk hozni az új vizuális aláírás profilt.

A profil törlése a context menün keresztül lehetséges.



Majd választásunkat a megerősítés ablakon erősítsük meg, amennyiben törölni szeretnénk.

## 5.3 Dokumentum aláírása

A haladó üzemmódban a Dokumentum/dokumentumok aláírásához válasszon az alábbi két lehetőség közül:

- **Aláírom ezt a dokumentumot** (ebben a mezőben csak egy dokumentum választható ki): a „Kiválasztom” gombra kattintva a megjelenő Fájlkezelőben válassza ki az aláírandó dokumentumot.
- **Aláírom az összes dokumentumot ebben a könyvtárban és alkönyvtárban** (a választott könyvtárban az összes dokumentum aláírásra kerül): a „Kiválasztom” gombra kattintva a Fájlkezelőben válassza ki az aláírandó dokumentumokat tartalmazó könyvtárat vagy alkönyvtárat.
- **Egyenként írom alá**: az „Egyenként írom alá” kijelölő radio gombra kattintva a kiválasztott dokumentumokat egyenként lehet aláírni.
- **Egy kötegben írom alá mindet**: „Egy kötegben írom alá mindet” kijelölő radio gombra kattintva a kiválasztott dokumentumokat egyszerre tudjuk aláírni. A két radio gomb közül csak az egyik lehet aktív.

### 5.3.1 Aláírás egyenként

A Dokumentum aláírás felületen rá kell kattintani az „Egyenként írom alá” gombra majd a „Kiválasztom” gombra. A fájlkezelőben ki kell választani azt a fájlt, amely aláírásra kerül.

Kormányzati Elektronikus Aláíró és Aláírás-ellenőrző Szoftver

Menü Súgó

Dokumentum aláírása | Aláírás kiterjesztése | Aláírás ellenőrzése

**Aláírom ezt a dokumentumot:**

Írja be a fájl elérési útvonalát, vagy válassza ki azt a jobb oldali gombbal Kiválasztom

**Aláírom az összes dokumentumot ebben a könyvtárban és alkönyvtáraiban:**

Írja be a könyvtár elérési útvonalát, vagy válassza ki azt a jobb oldali gombbal Kiválasztom

Egyenként írom alá  Egy kötegben írom alá mindet

**Áttekintés**

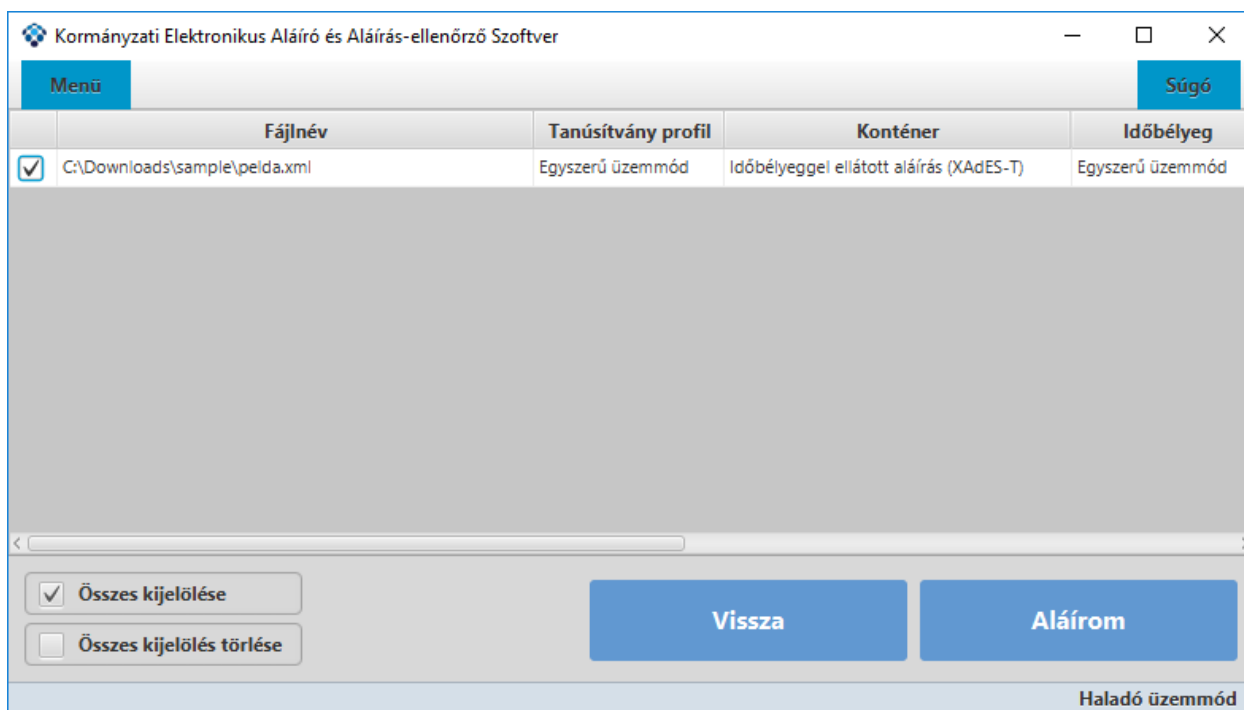
Haladó üzemmód

---

Miután a dokumentum(ok) kiválasztásra került(ek) kattintson az **Áttekintés** ikonra. Ezt követően megjelenik az alábbi felület a következő adatokkal:

- Fájlnév
- Tanúsítvány profil
- Konténer
- Időbélyeg
- Aláírás hash algoritmus
- Aláírás csomagolása
- Eredmény

Kattintson a táblázatban a sorok elején megjelenő kijelölő négyzetbe az aláírandó dokumentum/dokumentumok kiválasztásához.

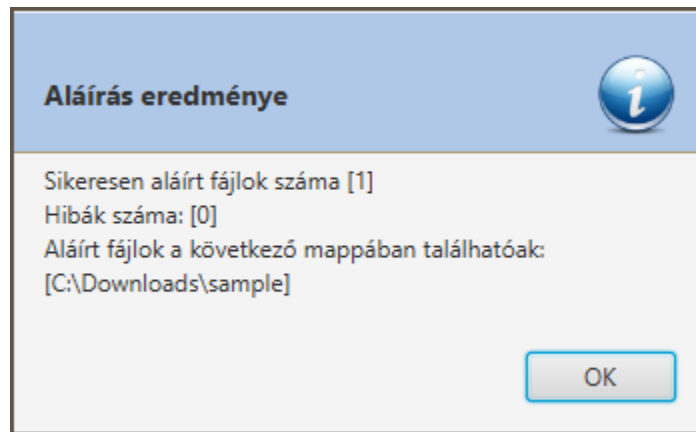


A képernyő bezárásához és a Dokumentum aláírása képernyőre való visszatéréshez kattintson a **Vissza** ikonra.

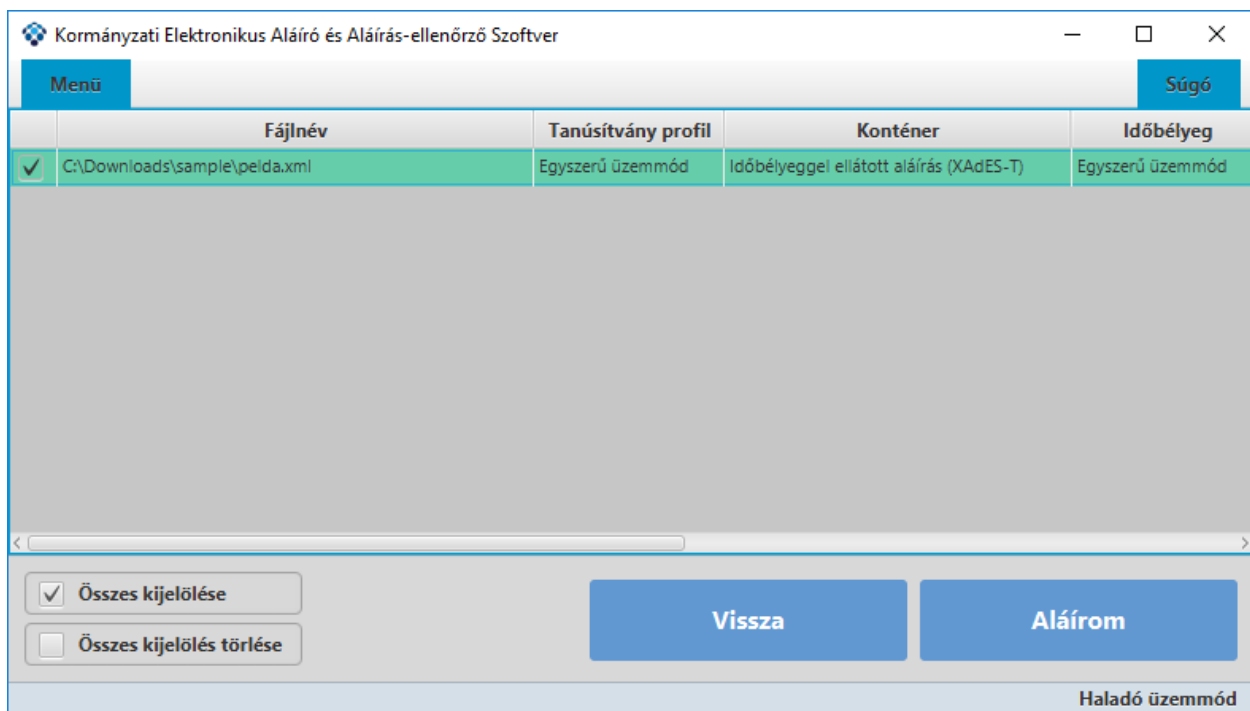
A listában kijelölt Dokumentumok aláírásához kattintson az **Aláírom** ikonra.

Az aláírás eredményéről a program üzenetet küld, amennyiben sikeres, illetve akkor is, ha hibát talál.

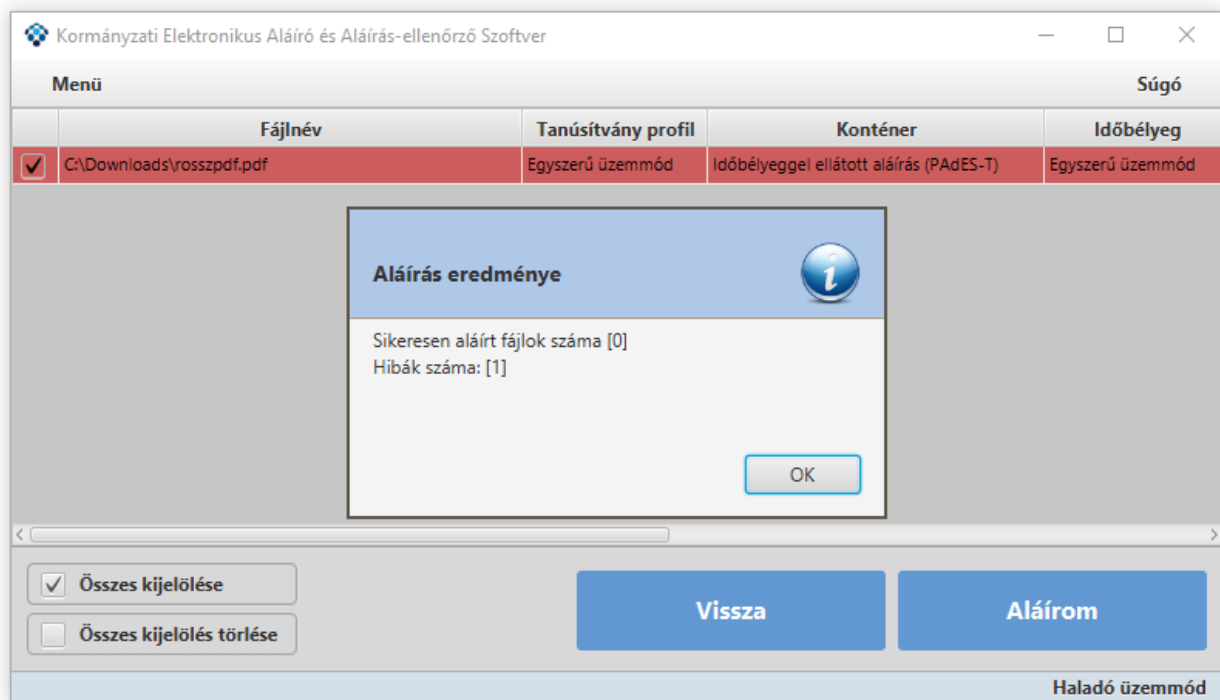
Amennyiben az aláírás eredménye sikeres az alábbi képernyő jelenik meg.



Az **OK** gombra kattintva az üzenetablak bezárul és a képernyőn a listában zöld színnel kerül kiemelésre a sikeresen aláírt fájl sora, majd az Eredmény oszlopban az **OK** információ jelenik meg.



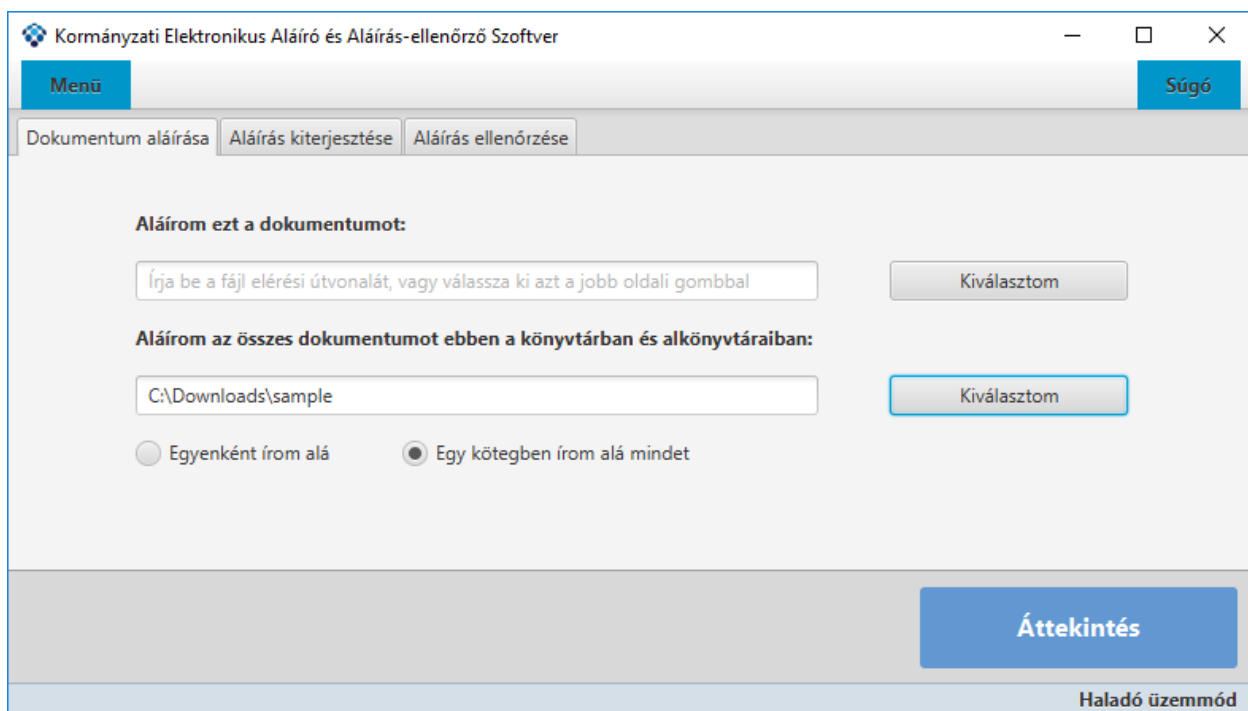
Amennyiben az aláírás eredménye sikertelen az alábbi képernyő jelenik meg.



Az **OK** gombra kattintva az üzenetablak bezárul és a képernyőn a listában piros színnel kerül kiemelésre a hibás sor, majd az Eredmény oszlopban a hibára vonatkozó információ jelenik meg.

### 5.3.2 Aláírás kötegben

A dokumentumok egy kötegben történő aláírása haladó üzemmódban az alábbi felületen történik.



A Dokumentum aláírás felületen rá kell kattintani az „Egy kötegben írom alá mindet” gombra majd a „Kiválasztom” gombra. A fájlkezelőben ki kell választani azt a könyvtárt, amelynek fájllai egy kötegben aláírásra kerülnek. Amennyiben a kiválasztott könyvtár alkönyvtárt tartalmaz, annak fájl tartalma is az aláírandó kötegbe kerül.

**Aláírom az összes dokumentumot ebben a könyvtárban és alkönyvtáraiban:**

C:\Downloads\sample Kiválasztom

Egyenként írom alá  Egy kötegben írom alá mindet

A könyvtár kiválasztását követően az Áttekintés gombra kell kattintani, ekkor megjelenik az alábbi képernyő, ahol a kijelölt fájlok felsorolásra kerülnek.

| Tanúsítvány profil | Konténer            | Időbélyeg     | Aláírás hash algoritmus | Aláírás csomagolása    |
|--------------------|---------------------|---------------|-------------------------|------------------------|
| Egyszerű üzemmód   | Alap aláírás (ASIC) | nincs megadva | SHA256                  | borítékolt (ENVELOPED) |

Fájlnév

- C:\Downloads\sample\KEAASZ\_alairt.pdf
- C:\Downloads\sample\pelda.xml
- C:\Downloads\sample\pelda\_alairt.xml

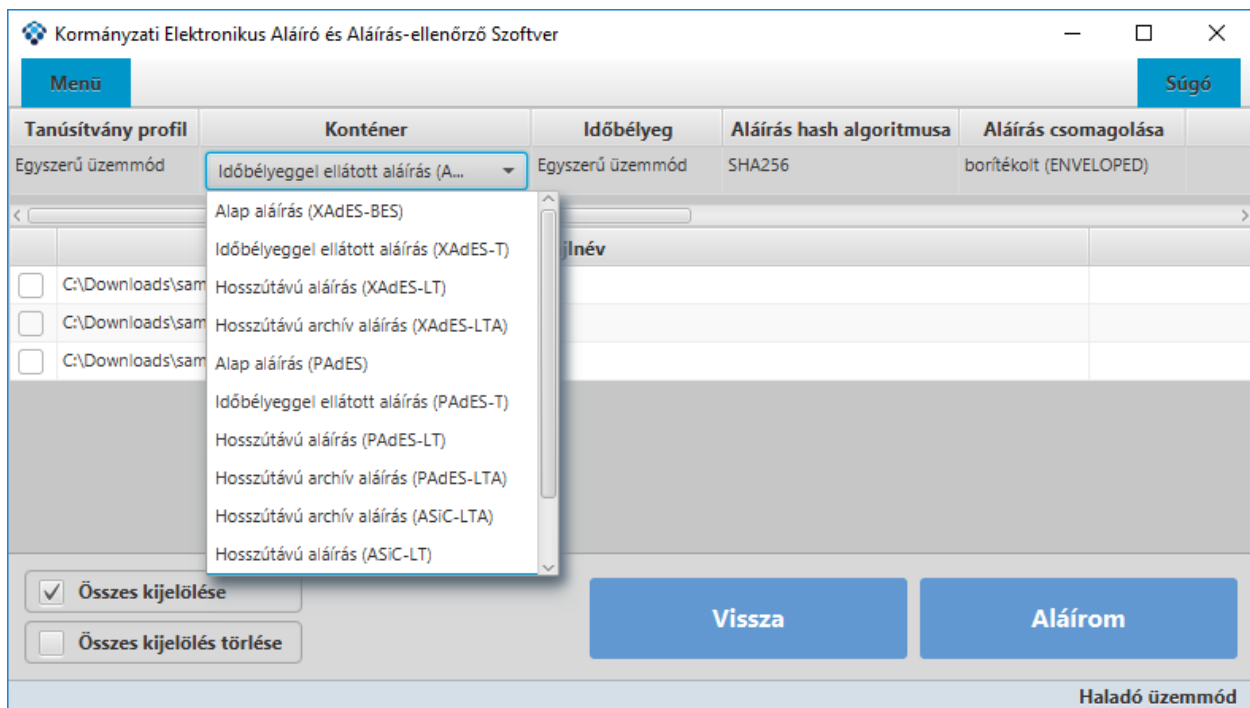
Összes kijelölése  Összes kijelölés törlése

Vissza Aláírom

Haladó üzemmód

Az aláírandó fájlokat ki kell jelölni a fájl név előtt lévő kijelölő négyzetbe kattintva. Amennyiben az összes fájl aláírásra kerül az „Összes kijelölése” négyzetbe kell kattintani, ekkor az összes fájl kijelölésre kerül. Az összes kijelölés törléséhez a „Összes kijelölés törlése” négyzetbe kell kattintani.

A képernyőn megjelennek az aláírási beállításokhoz szükséges paraméterek, amelyeket az adott mezőbe kattintva a megjelenő értéklista szerint állíthatók.



A **Vissza** gombra kattintva a képernyő bezárul és visszatérünk a Dokumentum aláírása felületre.

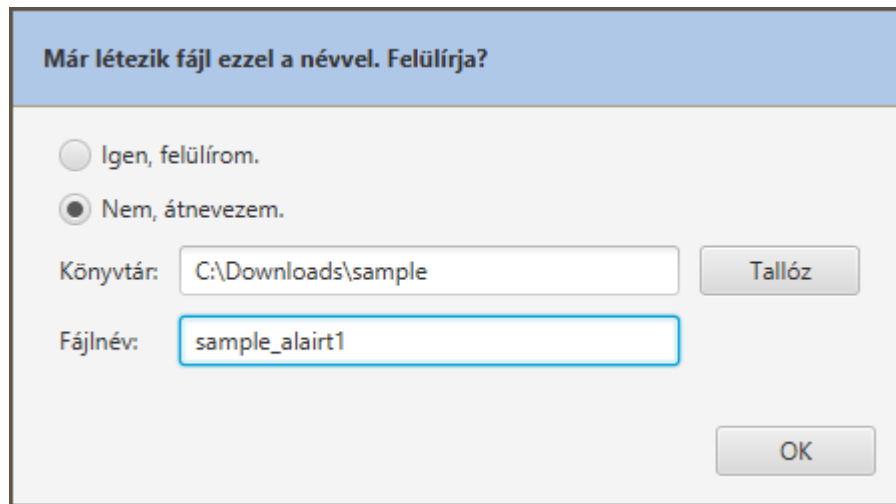
Amikor az aláírandó fájlok megjelölésre kerültek az aláírás elvégzéséhez az **Aláírom** gombra kell kattintani.

Amennyiben már létezik a kijelölt könyvtár nevével ellátott aláírt fájl, a program az alábbi üzenetet küldi. Amennyiben a fájlnev felülírásra kerül az „**Igen, felülírom**” gombra kell kattintani.

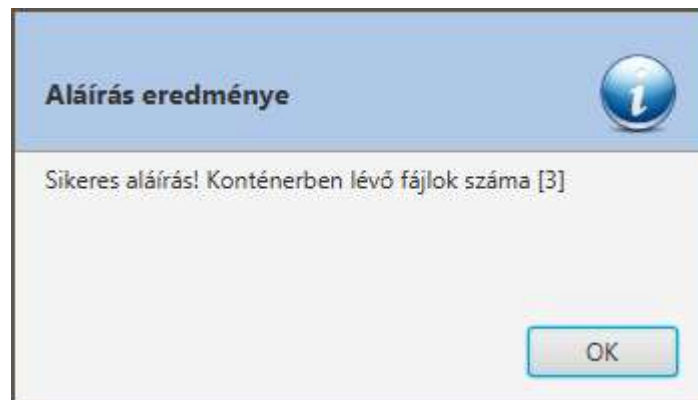


---

Amennyiben a fájlnev átnevezésre kerül a „**Nem, átnevezem**” gombra kell kattintani és a Fájlnev mezőben a név átírható, illetve a Könyvtár mezőben a „**Tallóz**” gombra kattintva a mentés helyét lehet megadni.



Az aláírás eredményéről a program az alábbi üzenetet küldi.



Az **OK** gombra kattintva az üzenet bezárul és az alábbi képernyő jelenik meg, ahol a képernyő felső részén az Eredmény sorban látható, hogy az aláírt fájlokat tartalmazó „Konténer fájl” melyik könyvtárba került mentésre.

Kormányzati Elektronikus Aláíró és Aláírás-ellenőrző Szoftver

Menu Súgó

| Tanúsítvány profil | Konténer            | Időbélyeg     | Aláírás hash algoritmus | Aláírás csomagolása    |                               |
|--------------------|---------------------|---------------|-------------------------|------------------------|-------------------------------|
| Egyszerű üzemmód   | Alap aláírás (ASIC) | nincs megadva | SHA256                  | borítékolt (ENVELOPED) | Aláírva! Konténer fájl elérhe |

<  >

| Fájlnév                             |                                       |
|-------------------------------------|---------------------------------------|
| <input checked="" type="checkbox"/> | C:\Downloads\sample\KEAASZ_alairt.pdf |
| <input checked="" type="checkbox"/> | C:\Downloads\sample\pelda.xml         |
| <input checked="" type="checkbox"/> | C:\Downloads\sample\pelda_alairt.xml  |

Összes kijelölése
  Összes kijelölés törlése
Vissza
Aláírom

Haladó üzemmód

## 5.4 Aláírás kiterjesztése

Amennyiben a haladó üzemmódban a dokumentum(ok) aláírását szeretné kiterjeszteni, válasszon az alábbi két lehetőség közül:

- **Dokumentum aláírásának kiterjesztése** (ebben a mezőben csak egy dokumentum választható ki): a „**Kiválasztom**” gombra kattintva a megjelenő Fájlkezelőben válassza ki a kiterjesztendő dokumentumot.
- **Kiterjesztem az aláírást az összes dokumentumon ebben a könyvtárban** (a választott könyvtárban az összes dokumentum kiterjesztésre kerül): a „**Kiválasztom**” gombra kattintva a Fájlkezelőben válassza ki a kiterjesztendő dokumentumokat tartalmazó könyvtárat.

Kormányzati Elektronikus Aláíró és Aláírás-ellenőrző Szoftver

Menü Súgó

Dokumentum aláírása Aláírás kiterjesztése Aláírás ellenőrzése

**Dokumentum aláírásának kiterjesztése:**

Írja be a fájl elérési útvonalát, vagy válassza ki azt a jobb oldali gombbal Kiválasztom

**Kiterjesztem az aláírást az összes dokumentumon ebben a könyvtárban:**

C:\Downloads\sample Kiválasztom

**Áttekintés**

Haladó üzemmód

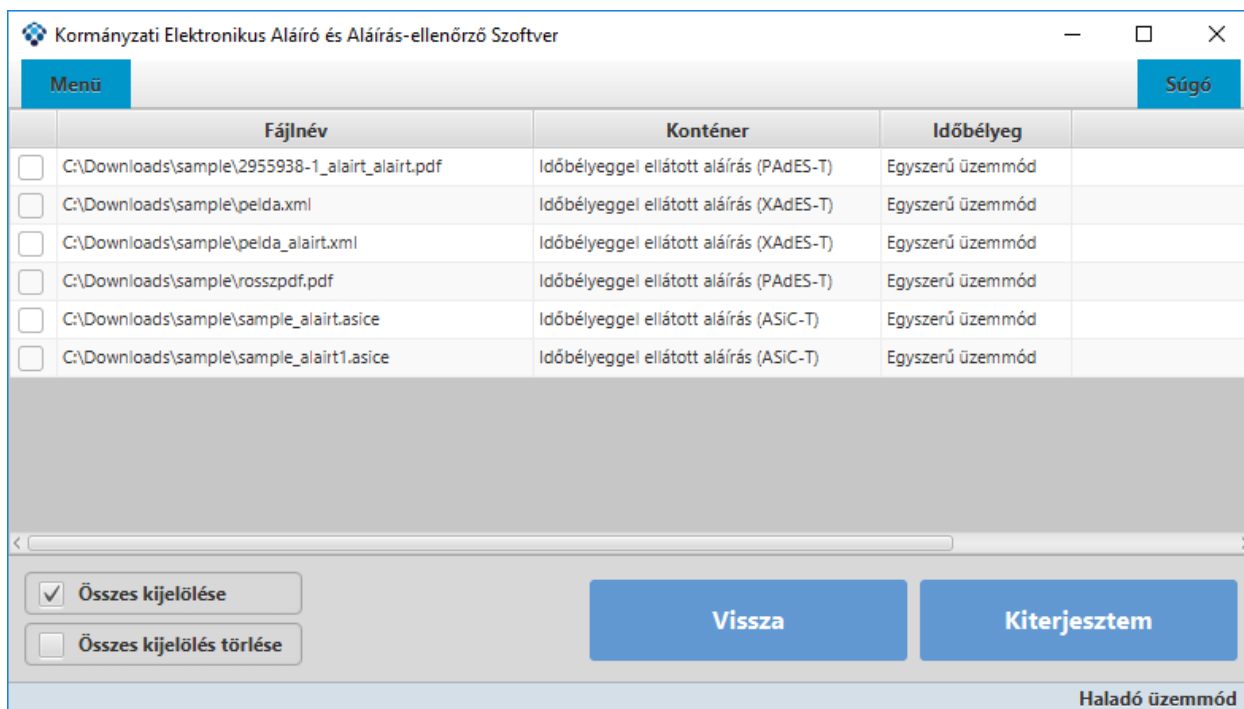
Miután a dokumentum(ok) kiválasztásra került(ek) kattintson az **Áttekintés** ikonra. Ezt követően megjelenik az alábbi felület a következő adatokkal:

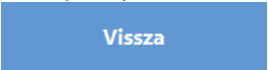
- Fájlnev
- Konténer
- Időbélyeg
- Eredmény


Kattintson a táblázatban a sorok elején megjelenő kijelölő négyzetbe a kiterjesztendő dokumentum(ok) kiválasztásához.

Az összes dokumentum kijelöléséhez kattintson az „**Összes kijelölése**” gombra.

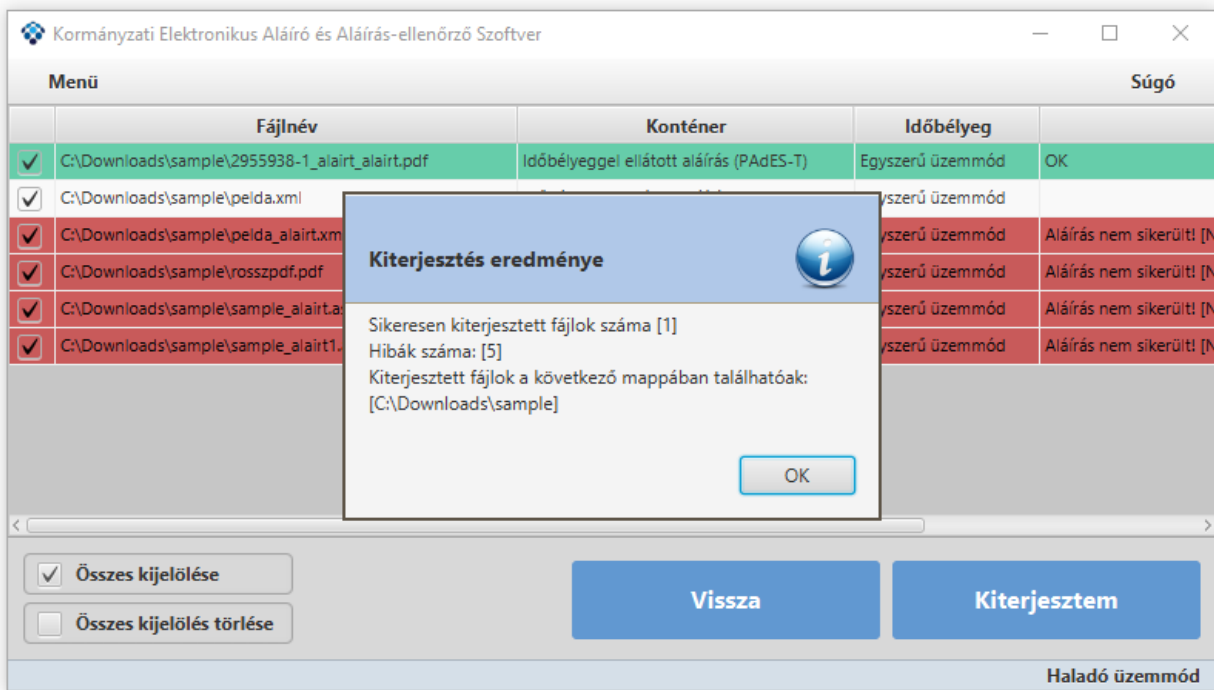
Amennyiben az összes kijelölést törölni szeretné, kattintson az „**Összes kijelölés törlése**” gombra.



A képernyő bezárásához és az Aláírás kiterjesztése képernyőre való visszatéréshez kattintson a  gombra.

A listában kijelölt dokumentumok kiterjesztéséhez kattintson a  ikonra.

A kiterjesztés eredményéről a program üzenetet küld, amennyiben sikeres, illetve akkor is, ha hibát talál.



Az **OK** gombra kattintva az információs ablak bezárul és visszatérünk a dokumentum lista képernyőre, ahol az Eredmény oszlopban a program megjeleníti a kiterjesztés eredményét.

## 6. ALÁÍRÁS ELLENŐRZÉSE

A dokumentumon lévő aláírás érvényességének ellenőrzéséhez kattintson a megjelenő felületen az **Aláírás ellenőrzése** fülre. Válasszon az alábbi két lehetőség közül:

- **Ellenőrzöm a dokumentumot:** a „Kiválasztom” gombra kattintva válassza ki a fájlkezelőben az adott, korábban elektronikusan aláírt dokumentumot. (ebben a mezőben csak egy dokumentum választható ki)
- **Az aláíráshoz tartozó eredeti dokumentumot is kiválasztom az ellenőrzéshez:** kattintson a kijelölő négyzetbe, így a mező aktívá válik. A „Kiválasztom” gombra kattintva válassza ki a fájlkezelőben az eredeti dokumentumot. Eredeti dokumentumot csak abban az esetben csatoljon, amennyiben az ellenőrizendő dokumentum nem tartalmazza az eredeti dokumentumot. Ez olyan esetben lehetséges, amikor az aláírás és az aláírt dokumentum külön fájlban találhatóak. (Ez az úgynevezett DETACHED aláírási mód.)
- **Ellenőrzöm a fájlokat ebben a könyvtárban:** a „Kiválasztom” gombra kattintva válassza ki a fájlkezelőben az ellenőrizni kívánt könyvtárat.

Kormányzati Elektronikus Aláíró és Aláírás-ellenőrző Szoftver

Menü Súgó

Dokumentum aláírása Aláírás kiterjesztése **Aláírás ellenőrzése**

**Ellenőrzöm ezt a dokumentumot:**

Írja be a fájl elérési útvonalát, vagy válassza ki azt a jobb oldali gombbal Kiválasztom

**Az aláíráshoz tartozó eredeti dokumentumot is kiválasztom az ellenőrzéshez:**

Írja be a fájl elérési útvonalát, vagy válassza ki azt a jobb oldali gombbal Kiválasztom

**Ellenőrzöm a fájlokat ebben a könyvtárban:**

Írja be a könyvtár elérési útvonalát, vagy válassza ki azt a jobb oldali gombbal Kiválasztom

**Ellenőrzöm**

Haladó üzemmód

A kiválasztott dokumentum aláírás ellenőrzéséhez kattintson az **Ellenőrzöm** ikonra.

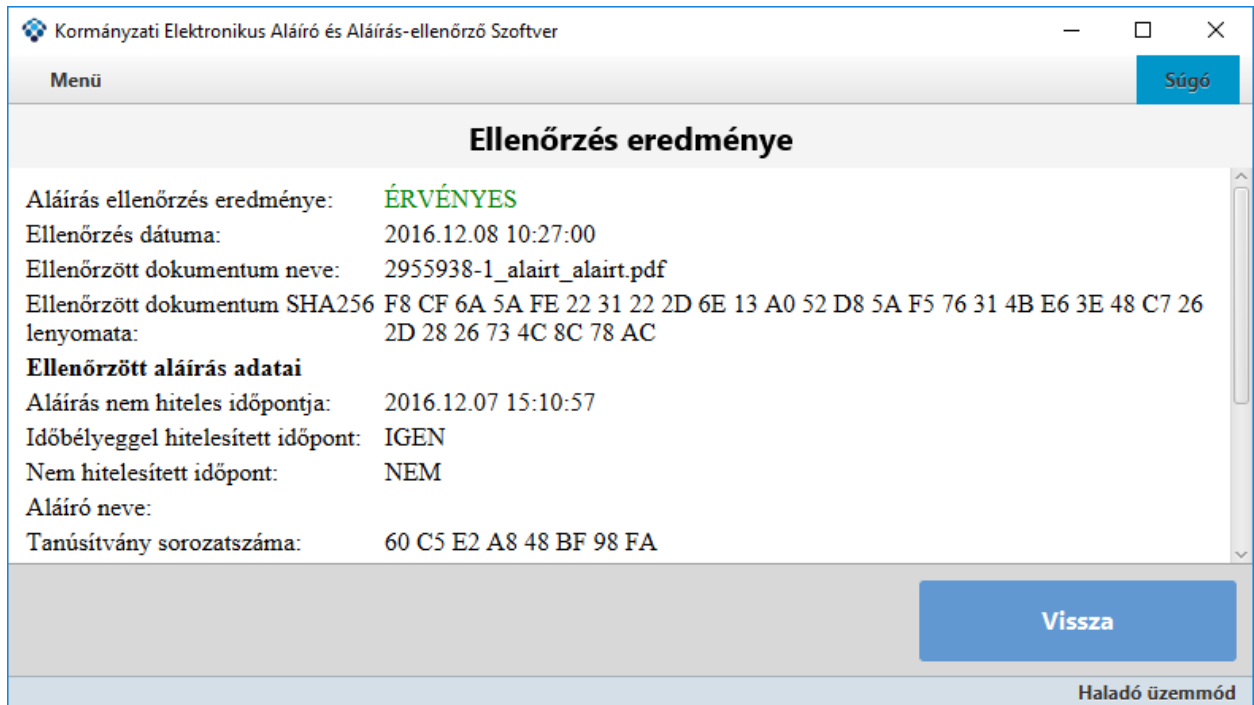
Az aláírás ellenőrzés eredményei az alábbiak lehetnek:

- érvényes
- érvénytelen
- nincs aláírás

- nem megállapítható
- hiba

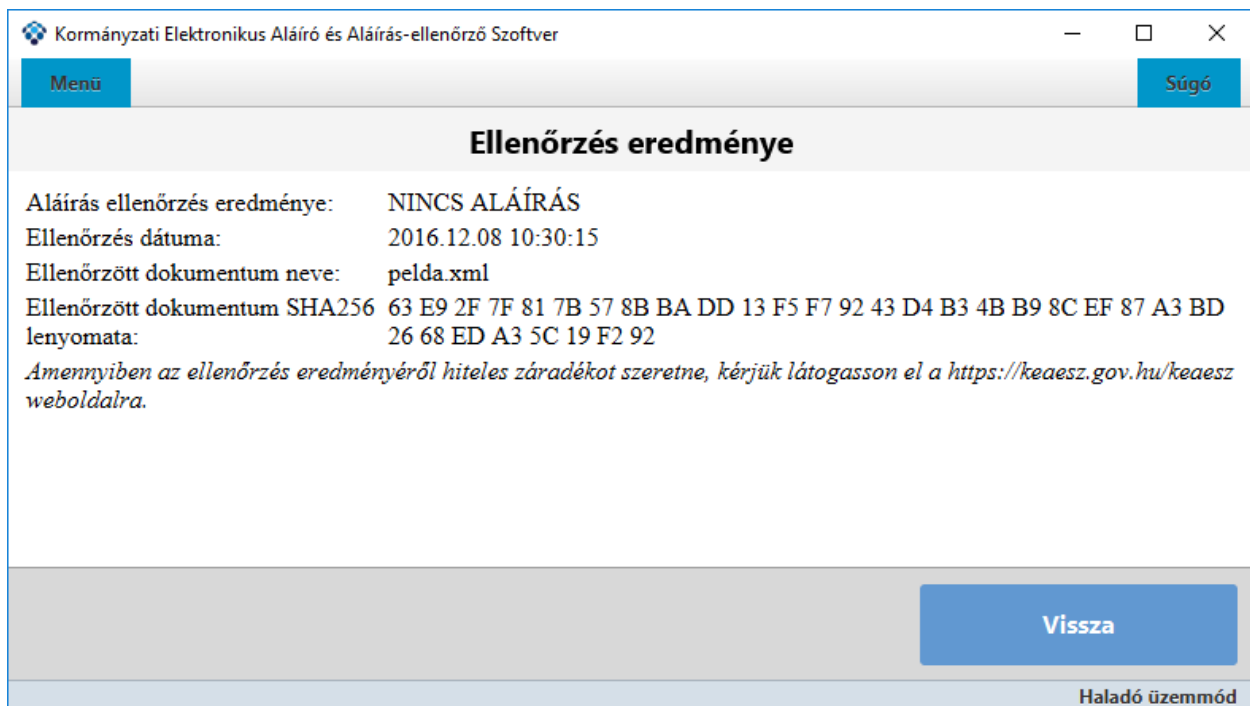
### Érvényes aláírás

Az alábbi képernyőn egy érvényes aláírás ellenőrzés eredménye látható.



### A dokumentum nem tartalmaz aláírást

Az alábbi képernyőn a nincs aláírás eredmény látható.



### **Aláírás nem megállapítható**

Az alábbi képernyőn az aláírás nem megállapítható esetén megjelenő képernyő látható.

Kormányzati Elektronikus Aláíró és Aláírás-ellenőrző Szoftver

Menü Súgó

### Ellenőrzés eredménye

Aláírás ellenőrzés eredménye: **NEM MEGÁLLAPÍTHATÓ**

Ellenőrzés indoklása: Az érvényesítési lánc nem megbízható, nincs megbízható gyökértanúsítvány.

Ellenőrzés dátuma: 2016.12.08 17:30:07

Ellenőrzött dokumentum neve: Eric Berne - Emberi játszmák-olvasOM\_alairt.pdf

Ellenőrzött dokumentum SHA256 lenyomata: 25 ED E7 12 E1 C6 61 D1 FA C7 EC 9C DA 39 A3 D9 4B 3B 55 69 D6 6F DF B6 21 15 C6 76 B6 0B 7B A0

**Ellenőrzött aláírás adatai**

Aláírás nem hiteles időpontja: 2016.12.08 16:54:48

Időbélyeggel hitelesített időpont: NEM

Nem hitelesített időpont: IGEN

Aláíró neve: adam3

Tanúsítvány sorozatszama: 58 49 5F 48

Tanúsítvány érvényessége: 2017.12.08 14:26:22

Tanúsítvány kibocsájtója: adam3

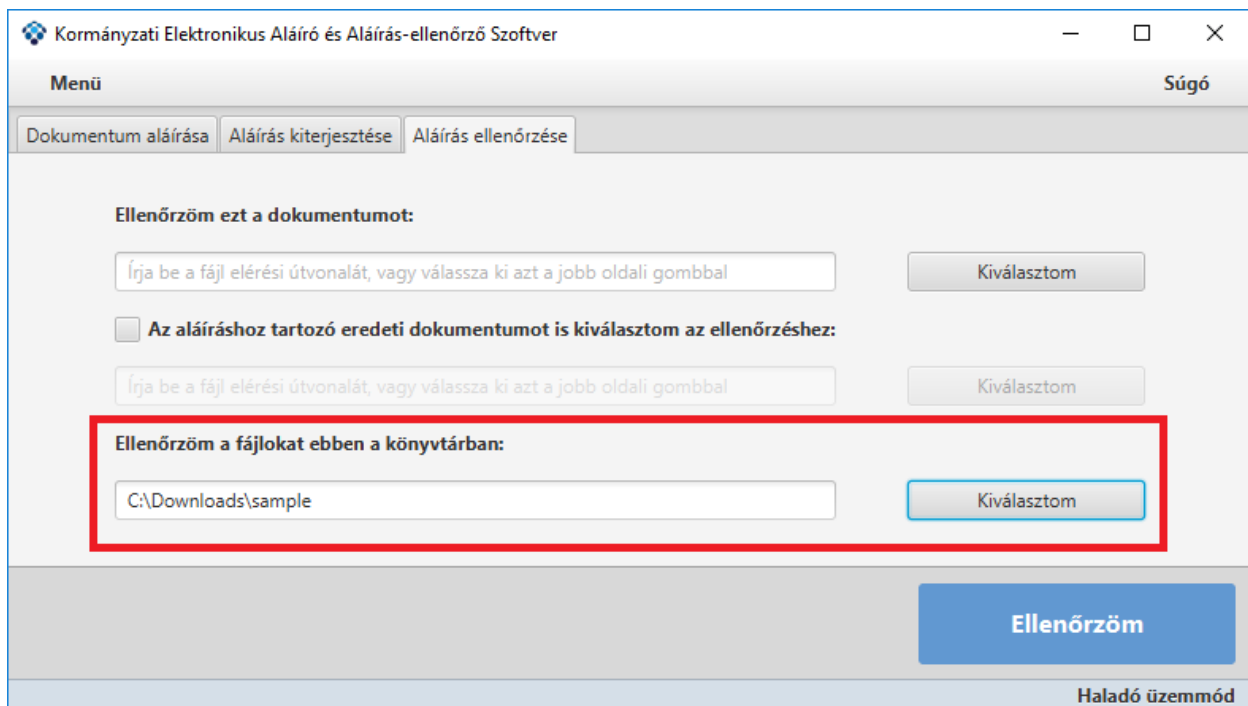
*Amennyiben az ellenőrzés eredményéről hiteles záradékot szeretne, kérjük látogasson el a <https://keasz.gov.hu/keasz> weboldalra.*

**Vissza**

Egyszerű üzemmód

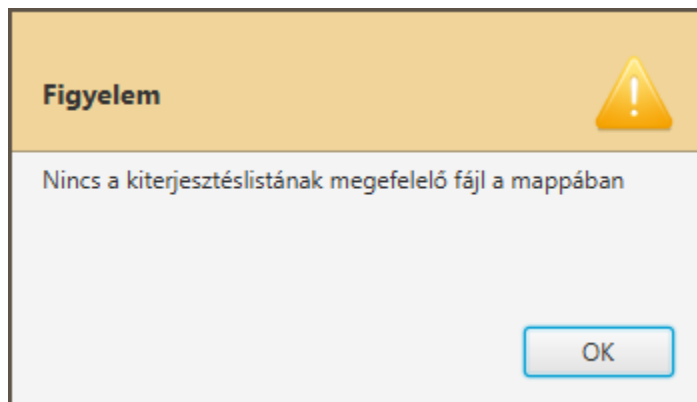
Az aláírás ellenőrzése felületre való visszatéréshez kattintson a  gombra.

### Könyvtárban lévő fájlok aláírásainak ellenőrzése



A fájlkezelőben kijelölt könyvtár fájljainak aláírás ellenőrzését az **Ellenőrzöm** gombra kattintva kell elindítani.

Amennyiben a program a Könyvtár kiválasztása után nem talál a beállításokban megadott kiterjesztéseknek megfelelő fájlt az adott könyvtárban, akkor az alábbi hibaüzenetet küldi.



Az „OK” gombra kattintva a képernyő bezárul.

Az ellenőrzés eredménye az alábbi képernyőn jelenik meg.

Az ellenőrzés eredménye táblázatban a kijelölt könyvtár fájljai szerepelnek az alábbi adatokkal:

- Fájlnev
- Eredmény
- Hiba

Kormányzati Elektronikus Aláíró és Aláírás-ellenőrző Szoftver

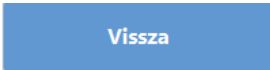
Menü Súlyó

### Ellenőrzés eredménye

| Fájlnév            | Eredmény                 | Hiba  |
|--------------------|--------------------------|---|
| rosszpdf.pdf       | Nem támogatott formátum! |   |
| pelda.xml          | Nincs aláírás!           |   |
| pelda_alairt.xml   | Nem megállapítható!      | Az érvényesítési lánc nem megbízható, nincs megbízható gyökértanúsítvány. |
| pelda_alairt.asice | Nem megállapítható!      | Az érvényesítési lánc nem megbízható, nincs megbízható gyökértanúsítvány. |
| KEAASZ_alairt.pdf  | Aláírás érvényes!        |   |

Vissza

Haladó üzemmód

Az aláírás ellenőrzése felületre való visszatéréshez kattintson a  gombra.

---

## 7. ASiC FÁJLOK KEZELÉSE

Az **ASiC** (Associated Signature Containers) egy nemzetközi szabványokon alapuló, korszerű konténer (hordozó) adatformátum, amely elektronikus dokumentumokat, valamint azok jellemzőit és a hozzájuk tartozó elektronikus aláírásokat egyetlen fájlban fogja össze. Egy **ASiC** konténerbe tetszőleges típusú dokumentumot, vagy adatot elhelyezhetünk, ezzel univerzális lehetőséget biztosít olyan adatok elektronikus aláírására és időbélyegzésére is, melyek eredetileg nincsenek felkészítve ezen kiegészítések hordozására.

A **KEAASZ** szoftver aktuális változata alkalmas szabványos ASiC konténerek létrehozására, feltöltésére és ellenőrzésére, de egyelőre nem alkalmas a konténer tartalmának böngészésére.

Amennyiben Önnek mégis szüksége van arra, hogy a konténer tartalmát megtekintse, felhasználja a benne foglalt dokumentumokat, erre egy ASiC konténer megnyitására és megjelenítésre alkalmas szoftvert kell beszereznie.

Mivel az **ASiC** konténer külső adatrétege valójában egy ZIP tömörített archívum, megnyitására tetszőleges, ZIP formátumot támogató program (például fájlmenedzserek, mint a FAR Manager, FreeCommander, vagy Total Commander), illetve az újabb Windows operációs rendszerek is alkalmasak. E programok beállításai között meg kell keresni az archívumok kezelésének paramétereit és megadni, hogy az asice (vagy .asics) kiterjesztésű állományokat is ZIP archívumként nyissák meg. Amennyiben ezt a beállítást nem találja, vagy nem kívánja megváltoztatni, áthidaló megoldásként az is megfelel, ha az **ASiC** fájlról készít egy .zip kiterjesztésű másolatot és ezt nyitja meg a ZIP formátum kezelésére alkalmas programmal.

A fenti módon megnyitott archívum főkönyvtárában találja az aláírt dokumentumokat eredeti formájukban, valamint a konténer típusát leíró, mimetype nevű kiegészítő adatállományt. A dokumentumokhoz tartozó egyéb adatokat, mint az elektronikus aláírások, vagy időbélyegek, a META-INF nevű alkönyvtár tartalmazza, elsősorban gépi feldolgozásra alkalmas XML formátumban.

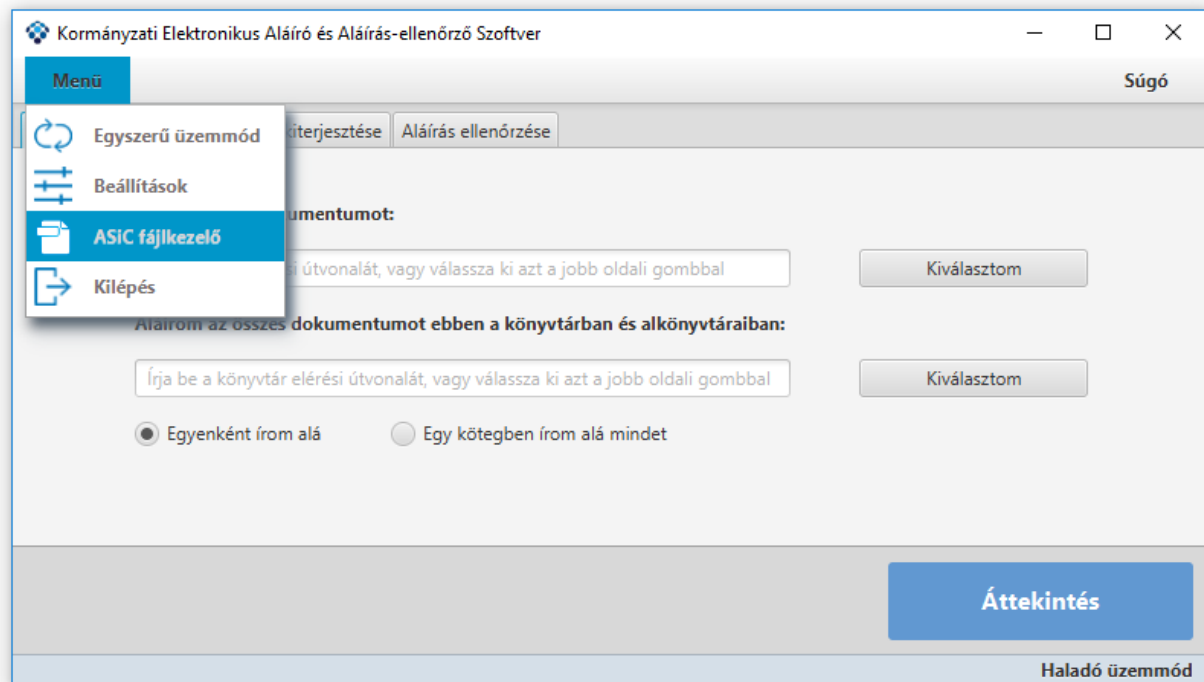
Az alábbi képernyőképen egy FreeCommander használatával megnyitott ASiC konténer tartalmát láthatja, benne két elektronikus dokumentummal:

| Name                      | Size Auto  | Modified         | Type                   |
|---------------------------|------------|------------------|------------------------|
| ..                        |            | 2015.12.21 18:44 |                        |
| META-INF                  |            | 1899.12.30 00:00 | Fájlmappa              |
| alairatlan_dokumentum.odt | 9 kB       | 1899.12.30 00:00 | OpenDocument-szöveg    |
| meghatalmazo.pdf          | 354 kB     | 1899.12.30 00:00 | Adobe Acrobat Document |
| mimetype                  | 31 Byte(s) | 1899.12.30 00:00 | Fájl                   |

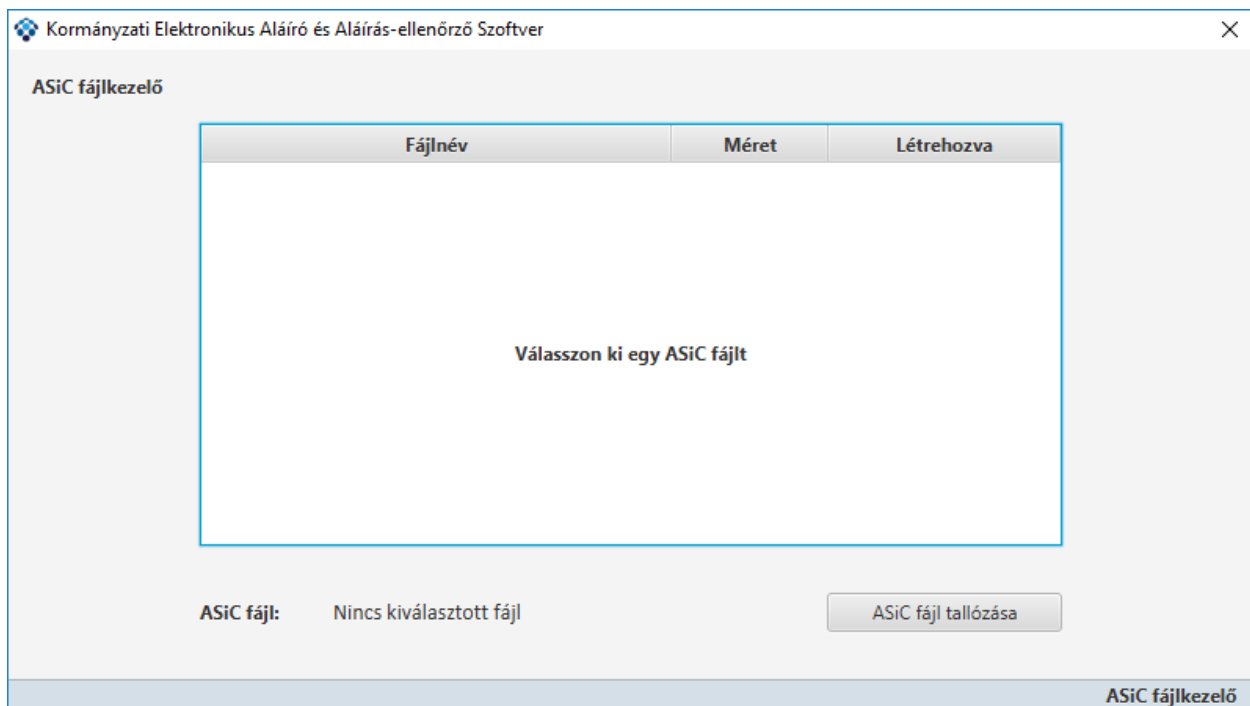
---

## 7.1 ASIC FÁJLKEZELŐ

Az **ASIC fájlkezelő** képernyőt az alkalmazás főmenüjében található **ASIC fájlkezelő** menüpont kiválasztásával lehet indítani.

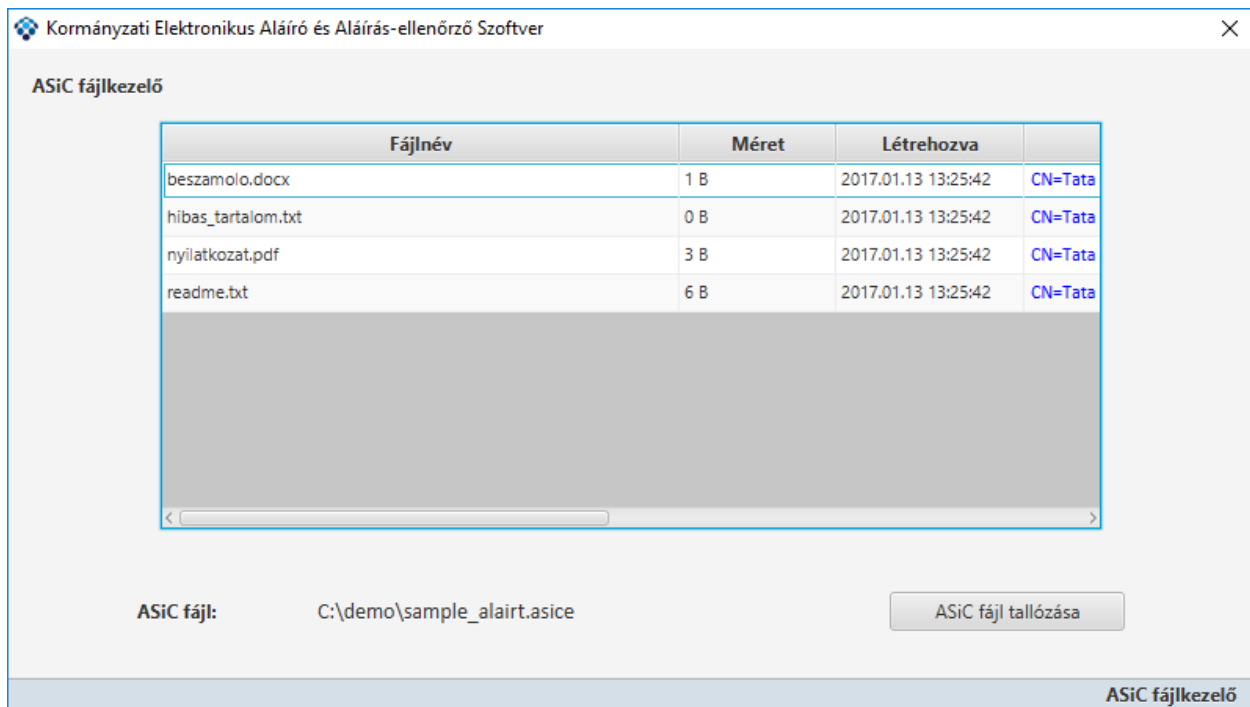


Az ASIC fájlkezelő képernyője:



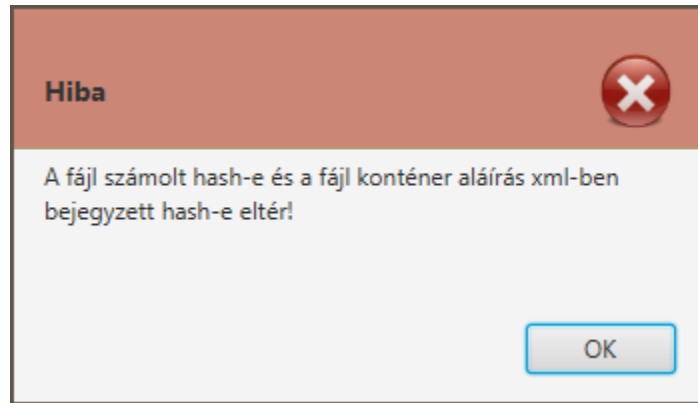
Egy ASiC fájl megnyitását az „**ASiC fájl tallózása**” gombra kattintva kezdeményezheti. A fájlválasztó ablakban (csak **asic**, és csak **asice** kiterjesztésű fájlok választhatóak) válassza ki a megnyitni kívánt ASiC fájlt, majd kattintson a „**Megnyitás**” gombra.

A fájl kiválasztása után a képernyőn az ASiC fájlba csomagolt fájlok láthatóak:

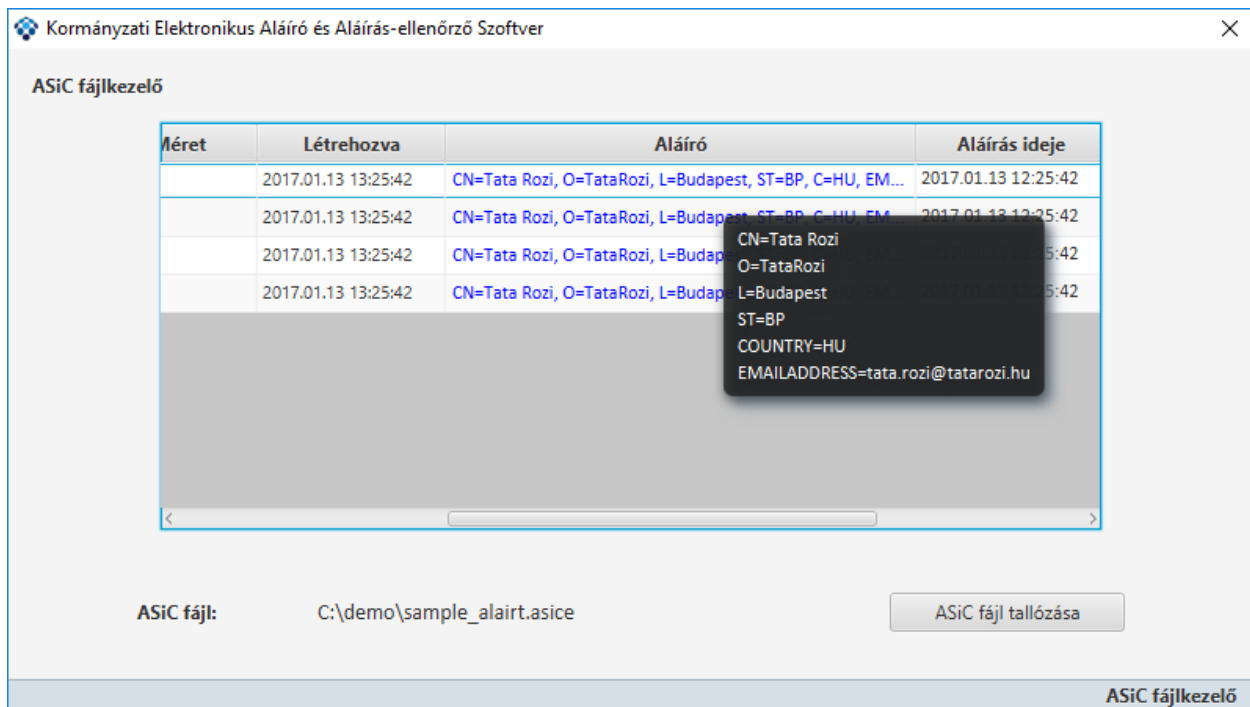


Az ASiC fájlkezelő bezárásához, a jobb felső sarokban található ablak bezárása „X” gombot válassza.

Az ASiC fájlba csomagolt fájlokról a fájl nevét, méretét, létrehozás dátumát, aláíróját, aláírás dátumát láthatja, valamint amennyiben van, leírást olvashat róla. Ha a fájl nevére duplán kattint akkor az adott fájl megnyílik. Ha fájl számolt hash-e és a fájl konténer aláírás XML-ben bejegyzett hash érték eltér akkor a fájlt nem lehet megnyitni.



Ha az „Aláíró” oszlopban található aláírások fölé viszi az egerét, akkor egy ablak jelenik meg amiben az aláírás fontosabb adatait olvashatja:



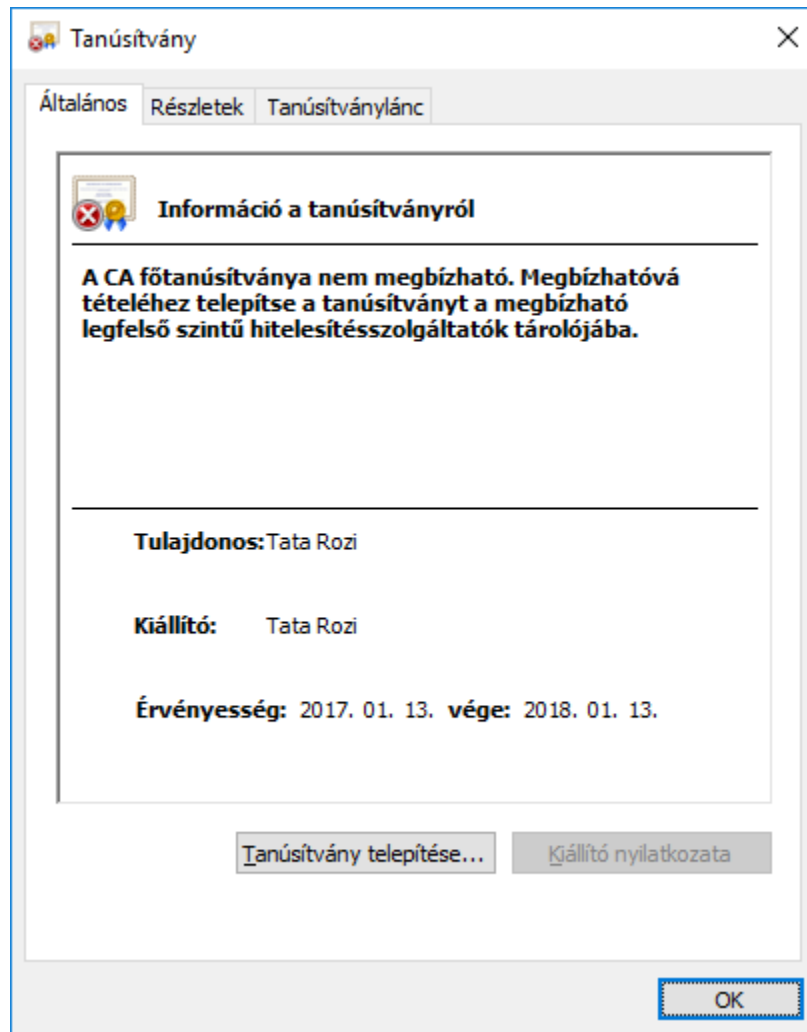
| Méret | Létrehozva          | Aláíró   | Aláírás ideje       |
|-------|---------------------|--|---------------------|
|       | 2017.01.13 13:25:42 | CN=Tata Rozi, O=TataRozi, L=Budapest, ST=BP, C=HU, EM... | 2017.01.13 12:25:42 |
|       | 2017.01.13 13:25:42 | CN=Tata Rozi, O=TataRozi, L=Budapest, ST=BP, C=HU, EM... | 2017.01.13 12:25:42 |
|       | 2017.01.13 13:25:42 | CN=Tata Rozi, O=TataRozi, L=Budapest, ST=BP, C=HU, EM... | 2017.01.13 12:25:42 |
|       | 2017.01.13 13:25:42 | CN=Tata Rozi, O=TataRozi, L=Budapest, ST=BP, C=HU, EM... | 2017.01.13 12:25:42 |

ASiC fájl: C:\demo\sample\_alairt.asice

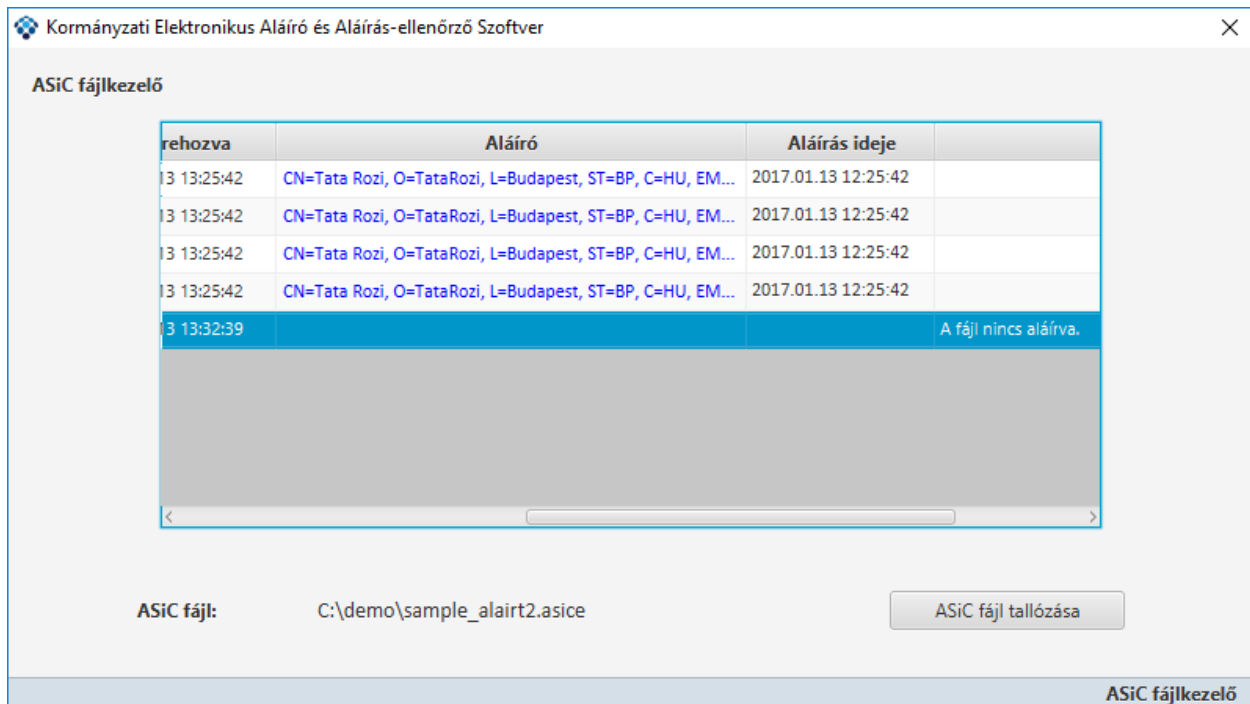
ASiC fájl tallózása

ASiC fájlkezelő

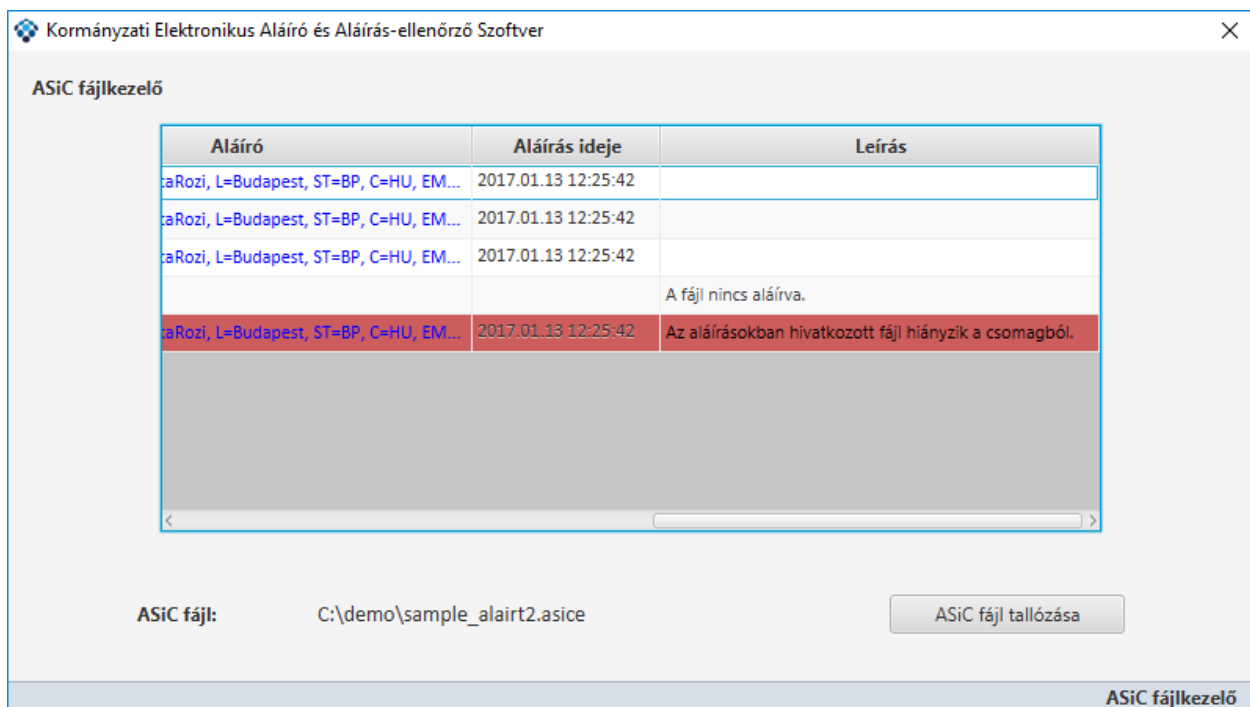
Ha további információkra kíváncsi az aláírással kapcsolatban, akkor ha rákattint az aláírás adataira, az alábbi tanúsítvány ablak jelenik meg:



A „Leírás” mezőben a fájl aláírásával kapcsolatos rendkívüli esetekre kaphat tájékoztatás. Egyik ilyen eset ha a konténer tartalmaz egy olyan fájlt ami nincs aláírva. Ebben az esetben az alábbi üzenet jelenik meg:



Ha van olyan hivatkozás az aláírásokban ami olyan fájlra vonatkozik ami nincs a csomagban akkor a sor piros háttérű lesz és a leírásban olvashatja az erre vonatkozó üzenetet:



Az is előfordulhat, hogy egy fájl több aláírásban is szerepel a kódolásuk nem tér el, de a hash-ek mégse egyeznek meg:

Kormányzati Elektronikus Aláíró és Aláírás-ellenőrző Szoftver

ASiC fájlkezelő

| Aláíró                                | Aláírás ideje       | Leírás   |
|---------------------------------------|---------------------|--|
| SERIALNUMBER=IDCHU-005007AE, ...      | 2017.01.10 13:32:41 |  |
| SERIALNUMBER=IDCHU-005007AE, ...      | 2017.01.10 13:32:41 | A fájlhoz több azonos kódolású de eltérő hash is tartozik. |
| 3., OID.2.5.4.17=1081, CN=Heitler ... | 2017.01.10 13:56:12 |  |

ASiC fájl: C:\Users\Dull Botond\Downloads\ag\20170110\_alairt.asice

ASiC fájl tallózása

ASiC fájlkezelő