



NETLOCK ARCHER FELHASZNÁLÓI KÉZIKÖNYV

v4.0

TARTALOMJEGYZÉK

(I). Tömeges felülhitelesítés (archiválás)	3
Az archiválásról	3
Törvényi szabályozások	3
A megfogalmazott követelmények megvalósításának lehetőségei	3
Mit jelent az archiválás elektronikus aláírással ellátott dokumentumok esetében	4
XAdES aláírási formátumok	5
▪ XAdES-BES, XAdES-EPES	5
▪ XAdES-T	5
▪ XAdES-C	6
▪ XAdES-A	6
Archiválás NetLock Kliens Oldali Archiváló program segítségével – amit tudni érdemes	8
Mire használható a program	8
A program telepítése és regisztrálása	10
A program telepítése	10
A program regisztrálása	11
A program frissítése	12
A telepítés utáni felhasználói beállítások	12
A program használata	18
1. Bemeneti és Kimeneti könyvtár megadása	18
2. Dossziék keresése, az archiválandó dossziék összeállítása	21
3. Feldolgozás	21
Az archív aláírással ellátott dossziék ellenőrzése	24
További teendők az archív aláírás után	26
(II). Tömeges dosszié készítés, aláírás	27
A program használata	27

(I). TÖMEGES FELÜLHITELESÍTÉS (ARCHIVÁLÁS)

AZ ARCHIVÁLÁSRÓL

TÖRVÉNYI SZABÁLYOZÁSOK

A 114/2007 (XII. 29.) GKM rendelet (a továbbiakban GKM rendelet) – a digitális archiválás szabályairól – 2. § az alábbi alapkövetelményt fogalmazza meg:

(1) A megőrzésre kötelezett a megőrzési kötelezettség lejártáig folyamatosan köteles biztosítani, hogy az elektronikus dokumentumok megőrzése olyan módon történjen, amely kizárja az utólagos módosítás lehetőségét, valamint védi az elektronikus dokumentumokat a törlés, a megsemmisítés, a véletlen megsemmisülés és sérülés, illetve a jogosulatlan hozzáférés ellen.

(2) A megőrzésre kötelezett köteles biztosítani, hogy az őrzött elektronikus dokumentumok értelmezhetősége (olvashatósága) - a dokumentumok megjeleníthetőségét lehetővé tevő szoftver- és hardverkörnyezet biztosításával - a megőrzési kötelezettség időtartama alatt megmaradjon.

A MEGFOGALMAZOTT KÖVETELMÉNYEK MEGVALÓSÍTÁSÁNAK LEHETŐSÉGEI

Fokozott biztonságú vagy minősített elektronikus aláírással ellátott dokumentumok esetében, a GKM rendelet 2. § (1) bekezdésében szabályozott követelményeknek az utólagos módosítás lehetőségének kizárását biztosító **saját megőréssel**, vagy az elektronikus aláírásról szóló 2001. évi XXXV. törvény [a továbbiakban EAT] szerinti elektronikus archiválás szolgáltató igénybevételével lehet eleget tenni.

A szabályozások tehát lehetővé teszik, hogy az elektronikus dokumentumokra vonatkozó megőrzési kötelezettséget a megőrzésre kötelezett önállóan végezze el. Erre vonatkozólag lásd:

1)

„Elektronikusan aláírt dokumentumok hosszú távú megőrzése esetén meg kell oldani az elektronikus aláírás érvényességének ellenőrzését akár több évtizedes időtávon is. Ennek során kezelni kell az elektronikus aláírások „elöregedése” problémáját, ugyanis a folyamatosan növekvő számítási hatékonyság, a hálózatba szerveződés lehetősége és a kriptográfia fejlődése idővel az elektronikus aláírások biztonsági meggyengüléséhez vezethet. Az archivált dokumentumok későbbi megjeleníthetőségét és ellenőrizhetőségét is biztosítani kell, függetlenül attól, hogy az aláírást létrehozó és megjelenítő alkalmazásokat használják-e még.

Amennyiben a megőrzést az érintettek maguk látják el, kezelniük kell a fenti műszaki problémákat. Ha az utólagos módosítás lehetőségének kizárása úgy történik, hogy az elektronikus dokumentumot fokozott biztonságú vagy minősített elektronikus aláírással látják el, és a megőrzésre kötelezett személy a megőrzési kötelezettségnek maga tesz eleget, úgy

- ha több elektronikus dokumentumon helyeztek el egyetlen, legalább fokozott biztonságú elektronikus aláírást, akkor azokat a megőrzés során is együtt kell kezelni.
- a megőrzésre kötelezett személy köteles az elektronikus aláírás érvényességét ellenőrizni, majd az [eat] szerinti minősített időbélyeg-szolgáltató által kibocsátott időbélyeget elhelyeztetni a dokumentum elektronikus aláírásán, ha ilyen még nincs rajta elhelyezve;
- ha a megőrzési kötelezettség időtartama hosszabb, mint az elektronikus aláírás elhelyezésétől számított 11 év, a megőrzésre kötelezett köteles beszerezni és megőrizni az elektronikus aláírás hosszú távú érvényesítéséhez szükséges információkat (az érvényességi láncot), valamint köteles minősített időbélyeg-szolgáltató által kibocsátott időbélyeget elhelyeztetni az érvényességi láncon;
- továbbá a fent meghatározott időbélyegzést köteles megismételni akkor, ha a megőrzés ideje alatt a korábban elhelyezett időbélyeg olyan algoritmuson alapul, amely az [eat] szabályai szerint már nem biztonságos” (In: Nemzeti Hírközlési Hatóság Hivatala: *Elektronikus archiválási szolgáltatással kapcsolatos Hatósági tájékoztató, 2008. június*)

2)

„Az elektronikus iratokra vonatkozó megőrzési kötelezettségnek azonban nem csak archiválási szolgáltató útján lehet eleget tenni. Nincsen akadálya annak sem, hogy a megőrzéssel kapcsolatos kötelezettségeket az ügyvéd **saját maga teljesítsen**, akár úgy is, hogy egyes részkötelezettségei vonatkozásában külső szolgáltatót vesz igénybe.” (In: *Elektronikus archiválás – Általános tájékoztató és vitairat*, Készítette: dr. Homoki Péter ügyvéd, a Budapesti Ügyvédi Kamara informatikai biztosa, a kamara elnökének felkérése alapján, 2009. február 19.)

MIT JELENT AZ ARCHIVÁLÁS ELEKTRONIKUS ALÁÍRÁSSAL ELLÁTOTT DOKUMENTUMOK ESETÉBEN

Az EAT 3. § (1) alapján, ha egy dokumentumot érvényes elektronikus aláírással látnak el, akkor az így hitelesített dokumentum joghatását tekintve egyenrangú a papír alapú iratokkal:

„Elektronikus aláírás, illetve dokumentum elfogadását - beleértve a bizonyítási eszközként történő alkalmazást - megtagadni, jognyilatkozat tételére, illetve joghatás kiváltására való alkalmasságát kétségbe vonni - a (2) bekezdés szerinti korlátozással - nem lehet kizárólag amiatt, hogy az aláírás, illetve dokumentum elektronikus formában létezik.”

A jogszabály azonban csak az érvényes aláíráshoz kapcsol bizonyító erőt, tehát ahhoz, hogy az előírásoknak megfelelően hosszú távon megőrizhessük a dokumentum hitelességét és az elektronikus aláírás érvényességét, megfelelő hitelesítési formátummal kell ellátnunk. Az ETSI által specifikált XAdES aláírás formátum figyelembe veszi a hosszú távú megőrzés során az elektronikus aláírás érvényességének fenntarthatóságát.

Különböző XAdES aláírási formátumot hozhatunk létre, ezek az aláíráshoz csatolt adatok tekintetében különböznek (amelyek alapján a későbbiekben megállapítható, hogy érvényes volt-e aláírásokról az adott tanúsítvány), valamint abban, hogy helyezünk-e el az aláíráson időbélyeget és milyet.

Az archiváláshoz **XAdES-A** formátumú aláírássá kell kiterjesztenünk a meglévő dokumentumainkon szereplő aláírásokat, vagy pedig ilyeneket kell létrehozunk, illetve az ilyen formátumban lévő aláírásokat kell időnként újra archiv időbélyeggel ellátnunk. Az erre a formátumra történő kiterjesztés során beszerzésre kerülnek a tanúsítvány visszavonási állapotára vonatkozó adatok, valamint egy archiv időbélyeg kerül mindezekre. Az ilyen formában lévő aláírás ellenőrzése a későbbiekben lehetséges anélkül is, hogy a tanúsítványt kiadó hitelesítés szolgáltatóhoz kelljen fordulni az érvényesség megállapításához.

XADES ALÁÍRÁSI FORMÁTUMOK

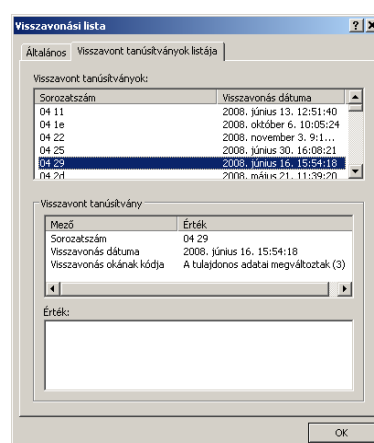
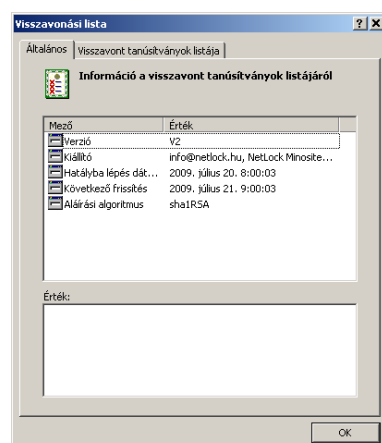
▪ [XAdES-BES, XAdES-EPES](#)

A XAdES-BES olyan rövid érvényességű aláírás, amely tartalmazza az aláírás időpontját, az aláírt dokumentum formátumát, az aláírási szabályzat azonosítóját (XAdES-EPES), valamint az aláíró tanúsítványát (az ebben szereplő nyilvános kulcs segítségével győződhetünk meg ellenőrzéskor arról, hogy a dokumentumot a tanúsítvány tulajdonosa írta alá a csakis nála meglévő privát kulcs segítségével). Ez a hitelesítési formátum nem tartalmaz időbélyeget, így az aláírás időpontját nem megbízható forrásból (a számítógép órája) csatolja az aláírás részletéhez. Az így aláírt dokumentumokkal a későbbiekben a következő problémák merülhetnek fel:

Tegyük fel, hogy az a tanúsítvány, amellyel egy ilyen aláírást létrehoztak lejárt vagy visszavonásra került (pl. mert feltételezhetővé vált, hogy az aláíró kulcshoz illetéktelenek is hozzáférhetnek, azaz kompromittálódott). Egy XAdES-EPES aláírással hitelesített dokumentumból a fenti esetben nem állapítható meg teljes bizonyossággal, hogy az aláírás tényleg akkor készült, amikor a tanúsítvány még érvényes volt! A XAdES-EPES aláírás tehát csak addig érvényes, amíg az aláíró tanúsítvány érvényes. Az ilyen hitelesítési formátummal tehát nem biztosítható a dokumentumok hosszú távú megőrzése, mindenképp időbélyegzéssel együtt írjunk alá (XAdES-T) vagy pedig helyezünk el az ilyen dossziékon időbélyeget a tanúsítvány lejárta előtt (aláírás kiterjesztése).

▪ [XAdES-T](#)

Olyan aláírás, amely a XAdES-EPES által tartalmazott elemeken kívül magában foglal egy időbélyeget, amely egy megbízható időbélyegzés szolgáltató által lett kibocsátva, s amellyel bizonyítható, hogy az elektronikus dokumentum az időbélyegző elhelyezésének időpontjában már létezett, és annak tartalma nem változott (érvényes aláírás esetén). Ennek eredményeképp, ha az aláíró tanúsítványa lejárt vagy visszavonásra került, a korábban (amikor még érvényes volt) készült aláírásai érvényesek maradnak, hiszen az időbélyeg bizonyítja, hogy az aláírás akkor készült, amikor a tanúsítvány még érvényes volt (az időbélyegzés is aláírás, amely során az időbélyeg szolgáltató az általa biztosított megbízható időpont adatot ellátja saját aláírásával). A tanúsítvány lejáratát után ennek ellenére nehézségek merülhetnek fel az ilyen formátummal ellátott aláírások ellenőrzése során. Aláírásakor, valamint az aláírás ellenőrzésekor mindig ellenőrzésre kerül, hogy a tanúsítvány nem lett-e visszavonva. Ennek ellenőrzése megtörténhet úgynevezett visszavonási listák (CRL) használatával. A Hitelesítés Szolgáltatók bizonyos időközönként kibocsátanak ilyen listákat, ezekben szerepelnek a visszavont tanúsítványok sorszámai, visszavonásuk oka és időpontja. Amely tanúsítvány rajta van ezen a listán, azzal nem lehet aláírni!



Két esetben jelentkezhet ezzel kapcsolatban probléma. Egyik eset amikor – tételezzük fel – a privát kulcsot tároló chipkártyát ellopják – így, az azzal való visszaélésnek még a lehetőségét is kizárható – a tanúsítványt a tulajdonosa vagy a szolgáltató visszavonja. A visszavonás időpontja és a következő CRL kibocsátása között azonban idő telhet el (maximum 4 óra), így utólag nem állapítható meg, hogy az aláírás nem a két időpont között történt-e meg. Továbbá, ha ugyanezzel a tanúsítvánnyal készült aláírást ellenőrizzük a lejáta után, akkor az éppen aktuális CRL-ből nem derül ki, hogy ez a tanúsítvány még a lejáta előtt vissza lett vonva (a lejárt tanúsítványok ugyanis lekerülnek a CRL- listáról).

Lehetőség van **OCSP** használatával is ellenőrizni a tanúsítvány állapotát (OCSP=Online tanúsítványállapot szolgáltatás), e szolgáltatás segítségével rögtön az aláírás pillanatában meggyőződhetünk a tanúsítvány állapotáról, érvényességéről és a válasz aláírt eredményét csatolhatjuk is az aláíráshoz. Ezzel a módszerrel a lejárat után is ellenőrizhető a tanúsítvány aláírás időpontjában való érvényességi státusza, ennek ellenére javasolt olyan aláírási forma létrehozása, amely ezeket az információkat csatolja (aláíráskor vagy még a tanúsítvány lejáta előtt) az aláírás részleteihez, így ezeknek az utólagos beszerzése nem jelenthet majd problémát.

(Továbbá, a GKM rendelet 4. § kifejezetten elő is írja ezen információk beszerzését az olyan dokumentumok esetében, amelyekre 11 évnél hosszabb megőrzési kötelezettség vonatkozik)

▪ [XAdES-C](#)

Ahogy az előbbiekből már kiderült, egy dokumentumon elhelyezett aláírás érvényességének hosszútávon történő megőrizhetősége azon múlik, hogy milyen további adatokat csatolunk az aláíráshoz, amelyek alapján a későbbiekben megbizonyosodhatunk a tanúsítvány aláírás időpontjában való érvényességéről.

Az XAdES-C aláírási forma annyiban különbözik az előzőtől (XAdES-T), hogy **az aláírásba itt bekerülnek azok a – tanúsítványra vonatkozó, aktuális – visszavonási információk is, amelyek beszerzése a későbbiekben amúgy nem volna lehetséges.** Mivel a visszavonási listák szakaszos kibocsátása miatt a tanúsítvány állapotára vonatkozó információt csak a következő (aláírás utáni) CRL tartalmazza; a visszavonási állapot CRL használatával történő ellenőrzése során ilyen aláírást nem is lehet egyetlen lépésben létrehozni; először alá kell írni XAdES-T formátummal, majd a kivárási idő után (általában 4 óra) ki kell terjeszteni XAdES-C formátumra. (A kivárási idő az a legrövidebb időtartam, amelyet a kezdeti ellenőrzéshez ki kell várni, annak érdekében, hogy az aláíró vagy egy más erre feljogosított szereplő által esetlegesen kért visszavonási kérelem megjelenhessen a szolgáltató által biztosított visszavonási állapot információk (CRL) között). A vállalt kivárási időt pedig a Hitelesítés Szolgáltatók határozzák meg szolgáltatási szabályzatukban.

Az XAdES-C aláírás addig érvényes, amíg aláírásra használt kriptográfiai algoritmusok nem gyengülnek meg, avulnak el (a technológia fejlődésével egyre hosszabb kulcsokat, egyre biztonságosabb algoritmusokat használnak a titkosításra, lenyomatképzésre). Egy elavult algoritmussal készült aláírás elveszti bizonyító erejét. A közeljövőben kerül bevezetésre például a biztonságosabb SHA2 algoritmuscsalád; a jelenlegi (SHA1) algoritmussal készült aláírások előbb-utóbb akár megbízhatatlanná is válhatnak (az 512 bit hosszúságú kulccsal készült aláírások például mára elavultnak számítanak).

Ezen problémákkal szemben nyújt védelmet az XAdES-A (archív) aláírás. **Az elektronikus dokumentumok archiválására vonatkozó előírásoknak az XAdES-A hitelesítési formátummal ellátott dokumentumokkal tudunk eleget tenni.**

▪ [XAdES-A](#)

Amennyiben az XAdES-C aláírás által tartalmazott valamennyi elemet (tanúsítványok, időbélyegek, visszavonási információk) egy további – ún. archív – időbélyeggel látjuk el, XAdES-A aláírást kapunk.

Ezzel a „külső” időbélyeggel lehetővé válik az aláírás adatainak (kiadói tanúsítványok, időbélyegző tanúsítványa, visszavonási információk), valamint az aláírásra használt kriptográfiai algoritmusoknak a védelme; alkalmazásával azok lejáta esetén is érvényes marad az aláírás. Ez az időbélyeg ugyanis bizonyítja azt, hogy az aláírás még akkor készült, amikor azok még érvényesek voltak.

Azonban az XAdES-A aláírás is karbantartást igényelhet. Az algoritmusok elavulása ugyanis az aláíráson elhelyezett archív időbélyeget is érinti. Amennyiben új algoritmusok lépnek életbe, válnak kötelezővé, az új algoritmusú aláírásokkal felül kell hitelesítenünk a meglévőket azok érvényességének megőrzése céljából. (Az archív időbélyegek továbbá biztosítékot jelentenek azzal szemben is, ha netán a Hitelesítés Szolgáltatók kiadói tanúsítványainak privát kulcsai kompromittálódnának. Erre ugyan nagyon kicsi az esély, de ez sem hagyható figyelmen kívül).

Az ilyen formátumú aláírás tehát mindaddig érvényes, amíg az aláírás során használt kriptográfiai algoritmusok és kiadói tanúsítványok érvényben vannak. Az aláírás ellenőrzéséhez szükséges valamennyi információ itt csatolva van az aláíráshoz, így egy utólagos ellenőrzéskor nem feltétlen szükséges a tanúsítványt kiadó szolgáltatóhoz fordulnunk.

Ami a rendszeres archív időbélyegzést indokolja az valójában az, hogy amikor egy kiadói tanúsítvány kompromittálódása vagy a használt algoritmus feltörése nyilvánosságra kerül, akkor már utólag nem javítható az aláírás; az új algoritmussal, kiadói tanúsítvánnyal készült időbélyegeket, még ezek előtt kell elhelyezni a dokumentumon. Mivel pedig az ilyen eseményeket senki nem látja előre, a gyakoribb időbélyegzés növeli a biztonságot. Javasolt tehát a Hitelesítés Szolgáltatónktól származó tájékoztatásokra is odafigyelni.

Egyedül az XAdES-A aláírás az, amely ilyen módon karbantartható, és amelynek hosszú távú érvényessége biztosítható. Az aláírások kiterjesztését nem feltétlen kell az aláírónak végezni, bárki megteheti, aki rendelkezik minősített időbélyeg hozzáféréssel.

Mint látható, az elektronikus archiválás gondos odafigyelést, a technológiák nyomon követését igényli, nem beszélve arról, hogy az aláírások folyamatos karbantartása mellett, biztosítani kell az elektronikus dokumentumok - a GKM rendelet 2.§-nak megfelelő - megőrzését, a törlés, a megsemmisítés, a véletlen megsemmisülés és sérülés, illetve a jogosulatlan hozzáférés ellen.

ARCHIVÁLÁS NETLOCK KLIENS OLDALI ARCHIVÁLÓ PROGRAM SEGÍTSÉGÉVEL – AMIT TUDNI ÉRDEMES

A NetLock Archer program azok részére nyújt segítséget, akik az elektronikus dokumentumok megőrzésére vonatkozó kötelezettségüknek önállóan kívánnak eleget tenni, viszont nem jelent komplett archiválási megoldást. Fontos tudni, hogy a program segítségével csak az aláírások ellenőrzése és a szükséges XAdES-A formátumra való kiterjesztése történik meg. Ezzel eleget tehetünk az „utólagos módosítás lehetőségének kizárása” követelménynek (egy aláírás akkor is érvénytelenné válik, ha az aláírt dokumentum tartalma megváltozik az aláírás után), de a törlés, a megsemmisítés, a véletlen megsemmisülés és sérülés, illetve a jogosulatlan hozzáférés ellen további intézkedések megtételére lesz még szükség. További fontos tudnivaló még, hogy az XAdES-A formátumra való kiterjesztés – noha pillanatnyilag valóban megfelel a hosszú távú megőrzésre vonatkozó követelményeknek és előírásoknak – nem biztos, hogy végleges megoldást biztosít. A világ változik és fejlődik, ezért szükséges a vonatkozó szabványok és előírások folyamatos figyelemmel követése, mely esetleg módosításokat tehet szükségessé.

MIRE HASZNÁLHATÓ A PROGRAM

A program segítségével lehetőség van dossziék (e-akták) tömeges archiválására, így valamennyi meglévő dossziénkat egyetlen művelettel archiv aláírással láthatjuk el.

A program ellenőrzi a dosszién (e-aktán) lévő aláírást. **Az ellenőrzés alapértelmezetten OCSP segítségével történik**, így a tanúsítvány visszavonási állapotáról azonnali válasz szerezhető, **nem szükséges kivárási idő használata** (*Kivárási idő: A kivárási idő az a legrövidebb időtartam, amelynek el kell telnie az aláírás létrehozása és a tanúsítványokra vonatkozó visszavonási információ beszerzése (azaz a kezdeti ellenőrzés befejezése) között.*). Amennyiben OCSP-t nem lehet használni az ellenőrzéshez, de CDP információ elérhető, akkor a program CDP használatával ellenőrzi az aláírást (CDP= CRL Distribution Point; a program a tanúsítványból kiolvassa a visszavonási lista elérési címét).

Kérjük, hogy a program használata során az alábbiakra mindenképp legyen figyelemmel:

- Amennyiben az ellenőrzés azt találja, hogy sem a dosszién, sem a dossziében lévő dokumentumon nincs aláírás, vagy az aláírás érvénytelen, esetleg nincs elegendő információ az érvényesség megállapításához, a program felkínálja aláírássra azt. Itt Ön jogosult eldönteni, hogy alá kívánja-e aláírni az állományokat vagy sem. Amennyiben igen, akkor az aláírás után rögtön megtörténik a kiterjesztés is XAdES-A_MELASZ2* vagy XAdES-A formátumra, azaz a program csatolja a teljes tanúsítvány láncot, az aktuális visszavonási listát és OCSP választ, valamint elhelyez egy archiv időbélyeget mindezekben.
- A program más szolgáltatók tanúsítványával aláírt dossziét is sikeresen ki tud terjeszteni XAdES-A formátumra, valamint aláírás is készíthető ilyen tanúsítványokkal, azonban akinek olyan szolgáltató biztosítja az időbélyegzést, amely szolgáltató autentikációt igényel az időbélyegzés során, az nem fogja tudni használni a programot (ebben az esetben kérjük, vegye fel a kapcsolatot Ügyfélszolgálatunkkal, itt tájékoztatást kap arról, hogy hogyan juthat egyedi időbélyeg URL-hez).
- A program használatához szükséges egy bementi-, és egy kimeneti könyvtár létrehozása (Bővebben lásd a „Program használata” pontot). A „bementi könyvtár” az a könyvtár, ahol az archiválásra váró dossziék találhatóak, a „kimeneti

könyvtár” pedig az, ahova a feldolgozott, archivált állományok kerülnek. A kimeneti könyvtár nevét, helyét Ön jogosult meghatározni. Ezen túlmenően lehetőség van arra, hogy Ön egy olyan funkcionalitást válasszon, hogy a bemeneti könyvtárból a hitelesített állományok átmozgatásra kerüljenek a megadott kimeneti könyvtárba.

Vegyük azt a példát, hogy van egy „2009. június” nevű könyvtáram, amiben van 10 db dosszié. Szeretném, ha ez a 10 dosszié archiválásra kerülne és az állományok átmozgatásra kerülnének egy – általam létrehozott –, „Archivált 2009. június” nevű könyvtárba. Ebben az esetben, a hitelesítést követően a 10 db dosszié „eltűnik” a „2009. június” nevű könyvtárból, és helyette az „Archivált 2009. június” nevű könyvtárban lesz megtalálható (amennyiben a program **Beállítások** felületén megadtam egy könyvtárat a „Feldolgozott dossziék könyvtára” opciónál, az eredeti dossziék ide kerülnek bemásolásra).

- A program használatánál kérjük, mindenképpen figyeljen arra, hogy amennyiben az „átmozgatás” funkciót nem választotta ki és a program felületén változatlanul hagyja a „bemeneti könyvtárat” (továbbá a szűrés az „_archivált” jelzővel ellátott fájlokra opciót sem kapcsoljuk be), akkor a bementi könyvtárban lévő valamennyi dosszié minden alkalommal feldolgozásra fog kerülni (bővebben lásd „Program használata” pont).
- Amennyiben Ön a Magyar Államkincstár honlapján beadott kérelmeket is elmenti (nem a befizetési igazolást, amit a Magyar Államkincstár küld vissza, hanem a kérelmet), lehetősége van arra, hogy kiválassza; ezeket az állományokat kívánja-e archiválni (bővebben lásd „Program használata” pont).

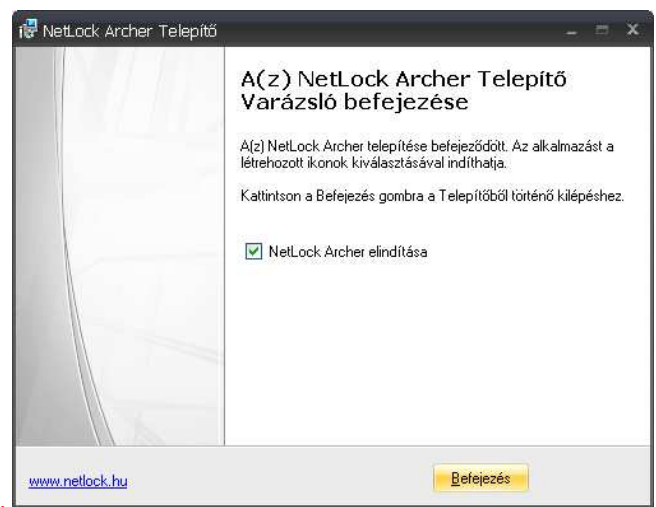
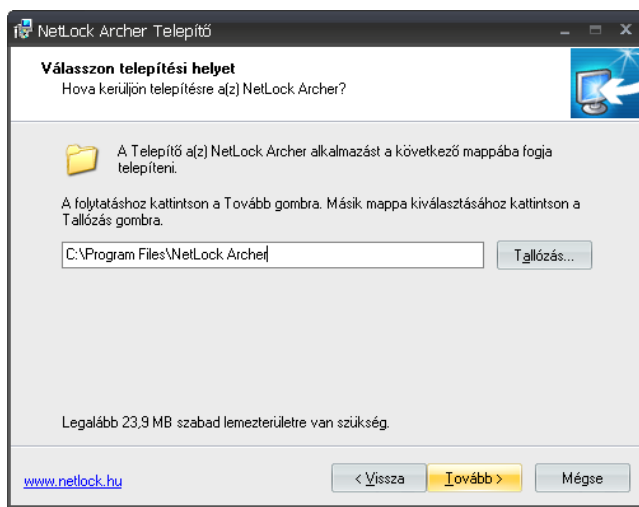
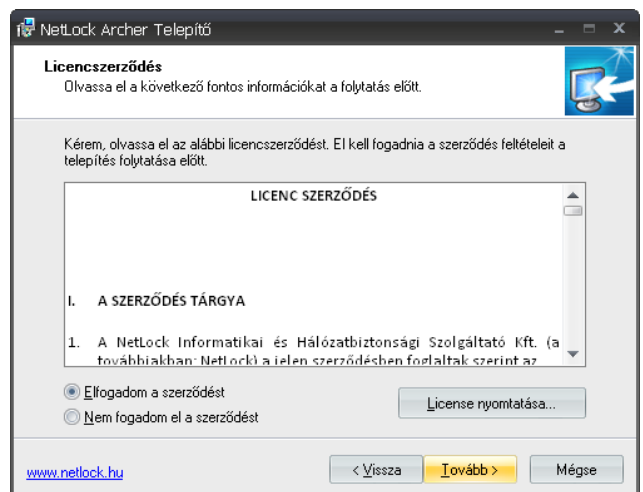
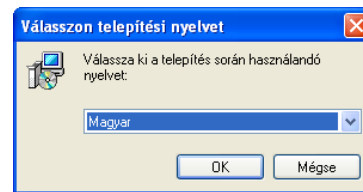
*A MELASZ formátumot az elektronikus aláíró alkalmazás fejlesztő cégek képviselői dolgozták ki (MELASZ=Magyar Elektronikus Aláírási Szövetség). Egy olyan egységes formátum elfogadása és értelmezése volt a cél, mely a letagadhatatlanság céljából készített fokozott biztonságú és minősített elektronikus aláírásokra nézve biztosítja a különböző fejlesztésű hazai alkalmazások együttműködő képességét. A megállapodásnak megfelelő aláírás-létrehozó alkalmazások képesek az egymás által létrehozott aláírásokat ellenőrizni, s azokat (az egységes formátumon belül) azonos eredményre jutva egységesen értelmezni.

A PROGRAM TELEPÍTÉSE ÉS REGISZTRÁLÁSA

A PROGRAM TELEPÍTÉSE

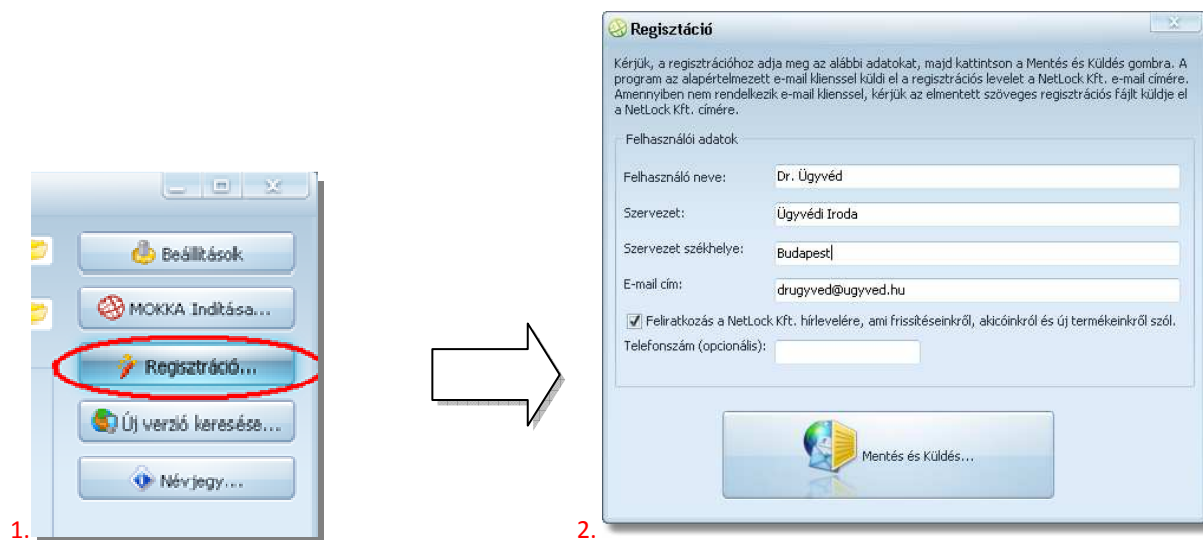
A program telepítését a weboldról letöltött, majd kitömörített állomány elindításával tudjuk megkezdeni.

A telepítési nyelv kiválasztása után, majd a licenc szerződés elfogadása után menjünk végig a telepítési folyamaton a **Tovább** gombbal.

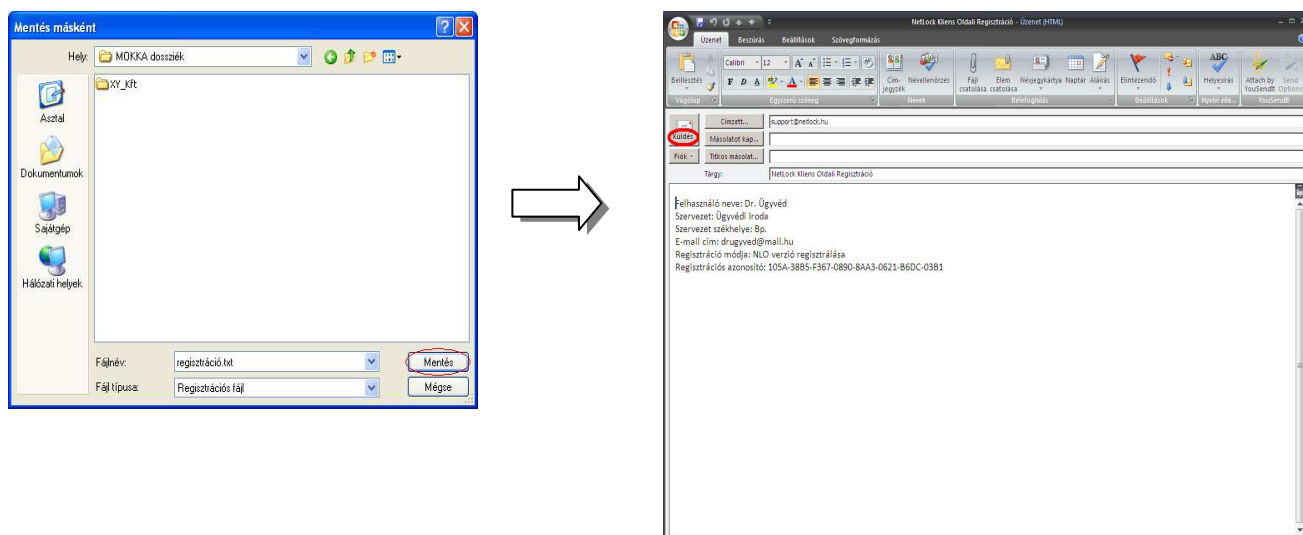


A PROGRAM REGISZTRÁLÁSA

A programot a használathoz regisztrálni kell. Ehhez indítsuk el a programot, majd kattintsunk a **Regisztráció** gombra.



A felhasználói adatok megadása után kattintsunk a **Mentés és Küldés** gombra. A regisztrációs adatokat előbb mentsük el, majd – amennyiben van beállított levelező program a gépünkön – a program az általa meghívott levelezőablakba beilleszti a regisztrációs adatokat. Ezután csak a **Küldés** gombra kell kattintanunk. (Ha nincs beállított levelezőprogramunk, az elmentett (.txt) fájlt csatolva küldjük el az archer@netlock.hu címre).

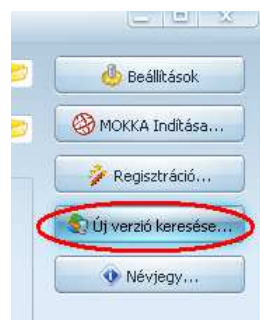


Az elküldött regisztrációs adatok alapján a NetLock Kft. munkatársai elkészítik a licenc fájlt, amelyet válasz e-mailben küldenek vissza. A csatolt **arciver_key.dat** fájlt **le kell menteni a program telepítési könyvtárába**, amely alapértelmezetten a C:\Program Files\NetLock Archer. A regisztrációs kulcs kizárólag arra a gépre érvényes, amelyről a regisztrációt küldték. Amennyiben másik gépre is telepíteni szeretnék a programot, a másik gépről is kell regisztrációs kérelmet küldeni. Sikeres regisztrációról az első indítás után értesítést kapunk.



A PROGRAM FRISSÍTÉSE

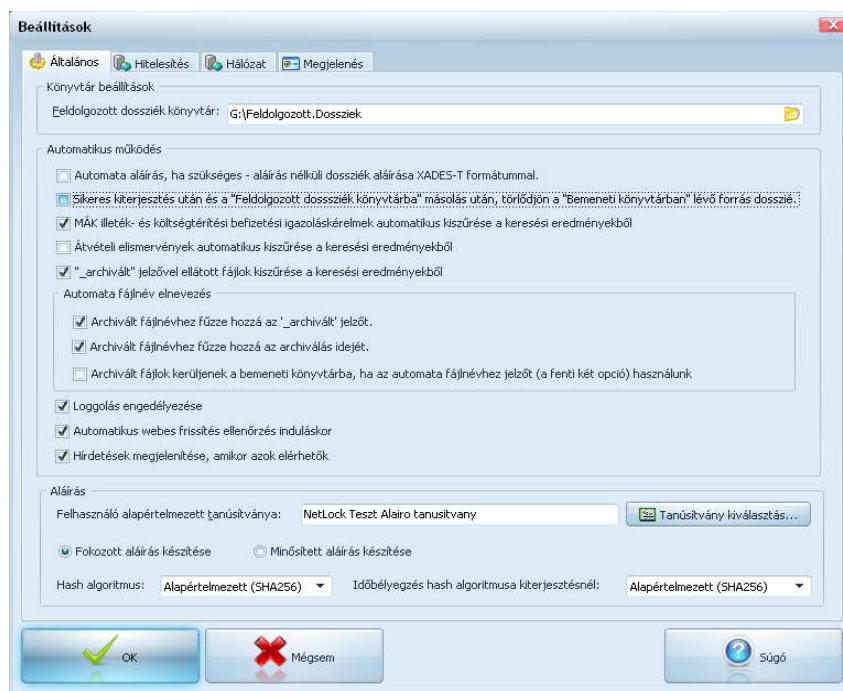
A program minden indításkor ellenőrzi, hogy elérhető-e újabb verzió, amennyiben a *Beállítások* panelen bejelöltük az „Automatikus webes frissítés ellenőrzés induláskor” opciót. Ezt az ellenőrzést az **Új verzió keresése** gombra kattintva is elindíthatjuk.



Amennyiben a program azt érzékeli, hogy van újabb verzió, felkínálja letöltésre annak telepítő csomagját, majd el is indítja azt. A friss verzió telepítésének lépései megegyeznek az első telepítéskoriével.

A TELEPÍTÉS UTÁNI FELHASZNÁLÓI BEÁLLÍTÁSOK

Általános



Könyvtár beállítások

Itt adható meg, hogy a program mely mappába másolja a dossziékat a feldolgozás után. A kiválasztáshoz kattintsunk a sor végén lévő mappa ikonra, majd tallózzunk ki egy létező, erre a célra létrehozott mappát.

Feldolgozott dossziék könyvtár: ide lesznek bemásolva a „Bemeneti könyvtárból” azok az **eredeti** dossziék, amelyek sikeresen feldolgozásra kerültek (megtehetjük, hogy ezt a mezőt üresen hagyjuk, ebben az esetben az eredeti dossziék a helyükön maradnak és másolat sem készül róluk).

Automatikus működés

Lehetőség van előzetesen megadni, hogy a program hogyan járjon el automatikusan azokkal a dossziékkal, amelyek újbóli aláírást igényelnek (aláíratlan, érvénytelen aláírást tartalmaz, vagy amelynek érvényessége automatikusan nem ellenőrizhető), valamint a kiterjesztett aláírással sikeresen ellátott dossziékkal.

Automata aláírás, ha szükséges: ezen opció bejelölésével a program – azon dossziék esetében, amelyek nem tartalmaznak aláírást vagy érvénytelennek találta azt, illetve amelynek az érvényességéről automatikusan nem tudott meggyőződni –, automatikusan kezdeményezi az aláírást; nem kínálja fel listában az aláírandó dossziékat, hanem rögtön megjelenik a tanúsítvány kiválasztó ablak, majd a PIN-kód kérés. Amennyiben nem jelöljük be ezt, a bemeneti könyvtárban lévő dossziék ellenőrzése után megjelenik azoknak a dossziéknak a listája, amelyeket újra alá kell írni. Lehetőség van a listán szereplő dossziékból kiválasztani, mely dossziék kerüljenek aláírásra és melyek ne.

Sikeres kiterjesztés után és a „Feldolgozott dossziék könyvtárba” másolás után, törlődjen a „Bemeneti könyvtárban” lévő forrás dosszié: ezen opciót akkor jelöljük be, ha nem akarjuk, hogy az eredeti dosszié a „Bemeneti könyvtárban” is megmaradjon. Annyiban javasolt ezt bekapcsolni, hogy a későbbiekben a „Dossziék keresése” gombra kattintva, nem fogja újra felkínálni feldolgozásra azokat a dossziékat, amelyek már egyszer újra alá lettek írva vagy ki lettek terjesztve (az eredeti forrás dossziékat egyébként megtalálhatjuk majd a „Feldolgozott dossziék könyvtárban”).

Akkor is bekapcsolhatjuk ezt az opciót, ha azt szeretnénk, hogy az archivált dossziéink az eredeti helyükre kerüljenek. Ebben az esetben kapcsoljuk be (lentebb) az „Archivált fájlok kerüljenek a bemeneti könyvtárba, ha az automata fájlnevéhez jelzőt használunk”, valamint az „Automata fájlnevé elnevezés” opciót.

Ha nem adtunk meg egy létező mappát a „Feldolgozott dossziék könyvtára” mezőnél, nem fog törlődni a forrás dosszié még akkor sem, ha itt bejelöltük ezt az opciót! Így nem fordulhat elő, hogy a program törli a forrás dossziét anélkül, hogy egy másolatot készítené a kiválasztott mappába.

Használhatjuk úgy is a programot, hogy ezt az opciót nem kapcsoljuk be, hanem minden feldolgozás előtt megadunk egy új bemeneti könyvtárat.

MÁK illeték- és költségtérítési befizetési igazoláskérelmek automatikus kiszűrése a keresési eredményekből: amennyiben ezt bejelöljük, a „bemeneti könyvtárban” lefutott keresési eredményekben nem fognak szerepelni az utalványminták kérésekor letöltött aláírt dossziék (pl. *1035731010718986.dosszie*), így azok kiterjesztése sem fog megtörténni (a program a fájl neve alapján szűr (alapértelmezetten ez az ügyazonosító szám), tehát ha mentéskor átneveztük a kérelmeket, akkor azok megjelennek a keresési eredmények között).

Átvételi elismervények automatikus kiszűrése a keresési eredményekből: az olyan dossziét, amelyet azért hoztunk létre, hogy hitelt érdemlően bizonyíthassuk általa, hogy egy dossziét az aláírás időpontjában átvettük, kihagyhatjuk az archiválási folyamatból ezen opció bekapcsolásával.

Az „archivált” jelzővel ellátott fájlok kiszűrése a keresési eredményekből: ezt az opciót akkor érdemes bekapcsolnunk, ha olyan mappakezelési megoldást választunk (lentebb), hogy az archivált dossziék a bemeneti könyvtárba kerüljenek, „_archivált” jelzővel ellátva. Így a bemeneti könyvtárban lefuttatott (megismételt) „dosszié keresése” parancsra a program nem fogja listázni a korábban már archivált dossziékat.

Automata fájlnev átnevezés

Az itt található beállításokkal módunk van megadni, hogy a program hogyan kezelje, jelölje a feldolgozott (archivált) e-aktákat.

Archivált fájlnevhez fűzze hozzá az ’ archivált’ jelzőt: ebben az esetben az történik, hogy a sikeres feldolgozás után (az általunk megadott helyen; pl. a kimeneti- vagy a bemeneti könyvtárban) létrejött, immár archív időbélyeggel ellátott e-akták fájlneveihez – a későbbi beazonosíthatóság érdekében – hozzáfűzi az „_archivált” jelzőt.

Archivált fájlnevhez fűzze hozzá az archiválás idejét: ennek bejelölése esetén az archivált fájlok neve a feldolgozáskori aktuális dátummal lesz kiegészítve. (e két opció bejelölésével pl. a korábbi, *XY Kft. Bejegyzési kérelme.dosszie* fájlt az archiválás után így találjuk meg: *XY Kft. Bejegyzési kérelme_archivalt_20100211_133616.dosszie*).

Archivált fájlok kerüljenek a bemeneti könyvtárba, ha az automata fájlnevhez jelzőt használunk: a programot használhatjuk olyan beállításokkal is, hogy az archivált e-aktákat nem egy általunk tetszőlegesen megadott kimeneti könyvtárba helyeztetjük, hanem a forrás fájlok eredeti helyére másolatjuk be őket. Ezek a fájlok nevébe illesztett jelző segítségével lesznek megkülönböztethetőek az eredetitől (**_archivalt_datum.dosszie*). Abban az esetben, ha ezen opció bekapcsolása mellett fentebb bejelöltük a „Sikeres kiterjesztés után és a „Feldolgozott dossziék könyvtárba” másolás után, töröljön a „Bemeneti könyvtárban” lévő forrás dosszié” opciót is (valamint megadtunk egy mappát a „feldolgozott dossziéknak” is), a program úgy fog eljárni, hogy minden sikeresen feldolgozott e-aktát az eredeti helyén lecseréli az archivált verzióval, az eredetit pedig átmásolja a „feldolgozott dossziék” mappába.

Loggolás engedélyezése: ezen opció engedélyezésével, a program naplózza a folyamatokat; az esetlegesen előforduló hibák esetén segítségül szolgálhat a hiba okának megállapításában. A log fájlok a felhasználói profil könyvtárában, az Application Data\NetLock Archer könyvtárba kerülnek, dátummal és időponttal ellátott fájlokba (*C:\Documents and Settings\felhasználó\Application Data\NetLock Archer*).

Automatikus webes frissítés ellenőrzés indításkor: ennek bejelölése esetén, minden indításkor ellenőrzi a program, hogy rendelkezésre áll-e újabb program verzió. Ha talál frissebb verziót, akkor erről értesítést ad, és kérésre letölti a telepítő programot, majd el is indítja. Azért javasolt ennek bekapcsolása, mert segítségével értesülhetünk legegyszerűbben az újabb programverzió kiadásra kerüléséről. Fontos, hogy az időnként elvégzendő archív időbélyegzést mindig az aktuális, legfrissebb programmal végezzük, mert az esetleges lenyomatképző algoritmus változásokat, kiadói tanúsítványok megújulását, a fejlesztések során nyomon követjük és az ezekre vonatkozó ellenőrzések beépülnek a programba is.

Felhasználó alapértelmezett tanúsítványa

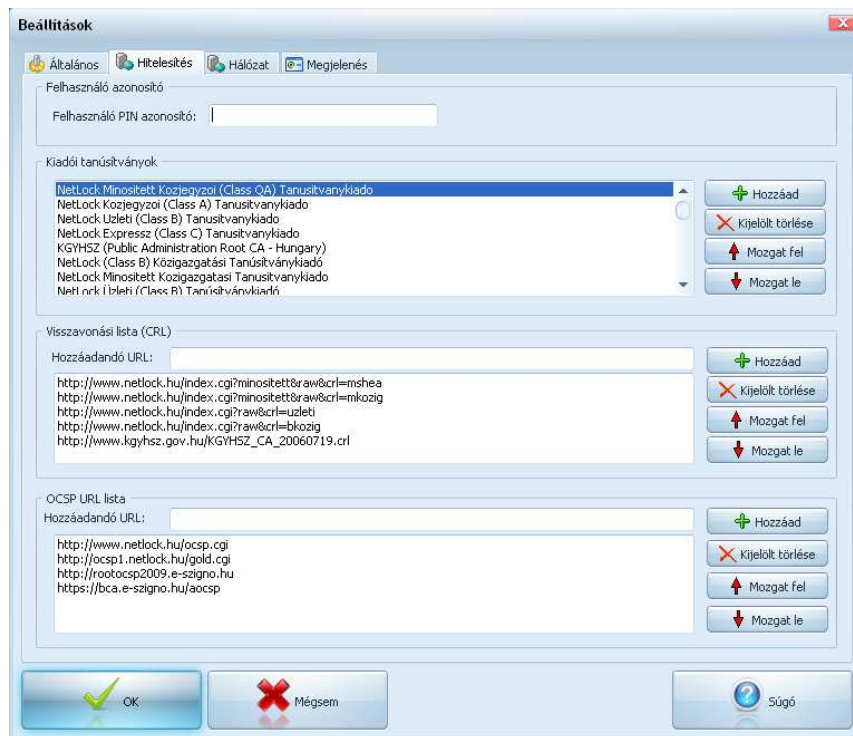
Itt kiválaszthatjuk azt a tanúsítványt, amellyel az esetlegesen újra aláírásra szoruló dossziékat alá kívánjuk írni. Az itt beállított tanúsítvány az aláírás előtt felugró „Tanúsítvány kiválasztás” ablakban ki lesz jelölve, csak a „Kiválasztás” gombbal el kell fogadni. Az aláírás fajtáját (Fokozott biztonságú/Minősített) az aláíró tanúsítványunk típusának megfelelően válasszuk ki.

Aláírás

Lehetőségünk van megadni a programnak, hogy milyen lenyomatképző algoritmust használjon aláíráskor. Az alapértelmezett beállítások módosítására abban az esetben van szükségünk, ha a chipkártyánk nem támogatja a fejlettebb SHA2-es algoritmust

(pl. Micardo kártya, de a szoftveresen tárolt tanúsítványok sem használhatók így Windows XP alatt!). Ebben az esetben a **hash algoritmust** állítsuk át SHA1-re, az időbélyegzés hash algoritmusát pedig ettől függetlenül hagyjuk az SHA2 algoritmusra állítva.

Hitelesítés



Felhasználó PIN azonosító:

Ebbe a mezőbe kell beírni az e-mailben kapott egyedi azonosítót ahhoz, hogy használni tudjuk a programot a rendelkezésre álló kreditünk igénybevételével.

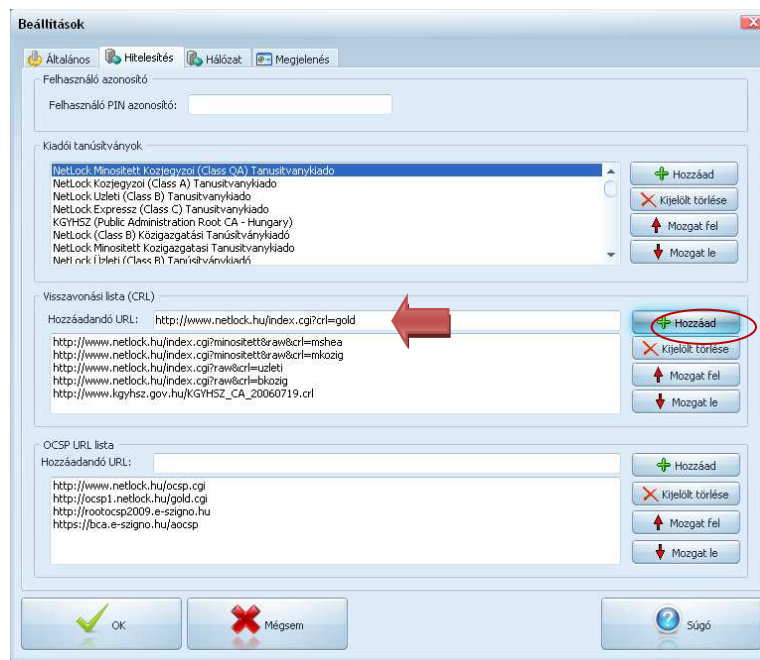
Kiadói tanúsítványok

Itt tudunk kiadói (Root) tanúsítványokat hozzáadni a listához. Az aláírásra használt tanúsítványnak a kiadói gyökértanúsítványa kell, hogy szerepeljen ebben a listában, ugyanis ellenőrzéskor a teljes hitelesítési láncot fel kell építeni; az aláíró tanúsítványt vissza kell vezetni egy megbízható Hitelesítés Szolgáltató tanúsítványára. A hozzáadáshoz kattintsunk a lista melletti **Hozzáad** gombra, ez után kiválaszthatjuk, hogy tanúsítványtárból vagy fájlból (.cer kiterjesztésű fájlok) kívánjuk hozzáadni a listához az új gyökér tanúsítványt.



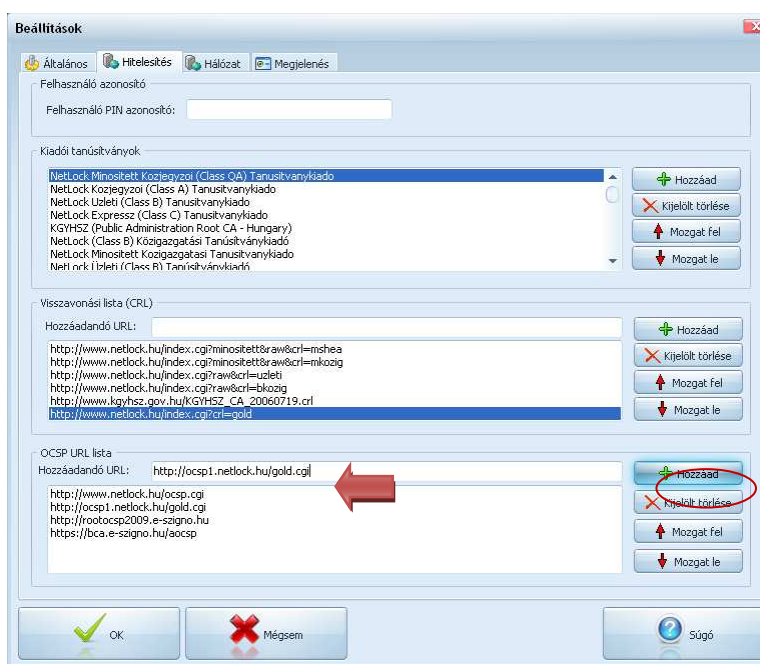
Visszavonási lista (CRL)

Itt azt a – kiadói tanúsítványhoz tartozó – URL listát szerkeszthetjük, amelyeken keresztül elérhető és letölthető az aktuális CRL (visszavont és felfüggesztett tanúsítványokat tartalmazó aláírt lista). Amennyiben olyan tanúsítvánnyal írunk alá, amelynek nem található meg itt ez az URL-je, fel lehet ide venni (a program a tanúsítványokból képes kiolvasni ezt az URL-t és felhasználni az ellenőrzéshez, így erre a funkcióra különösebben nem is lesz szükségünk).

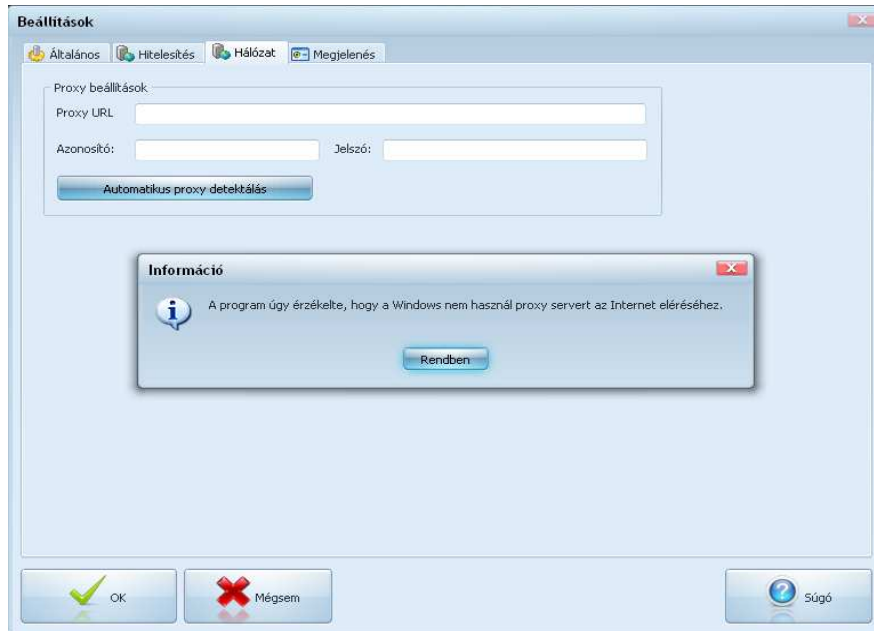


OCSP URL lista

Itt adhatunk meg további Hitelesítés Szolgáltató (tanúsítványához tartozó) OCSP elérési címét (OCSP=Online tanúsítványállapot-szolgáltatás).

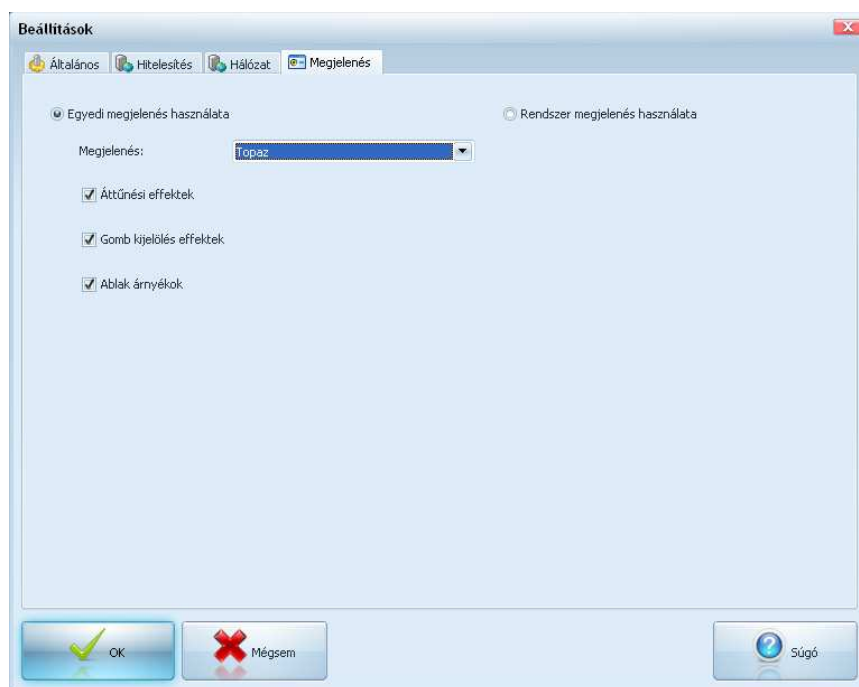


Hálózat

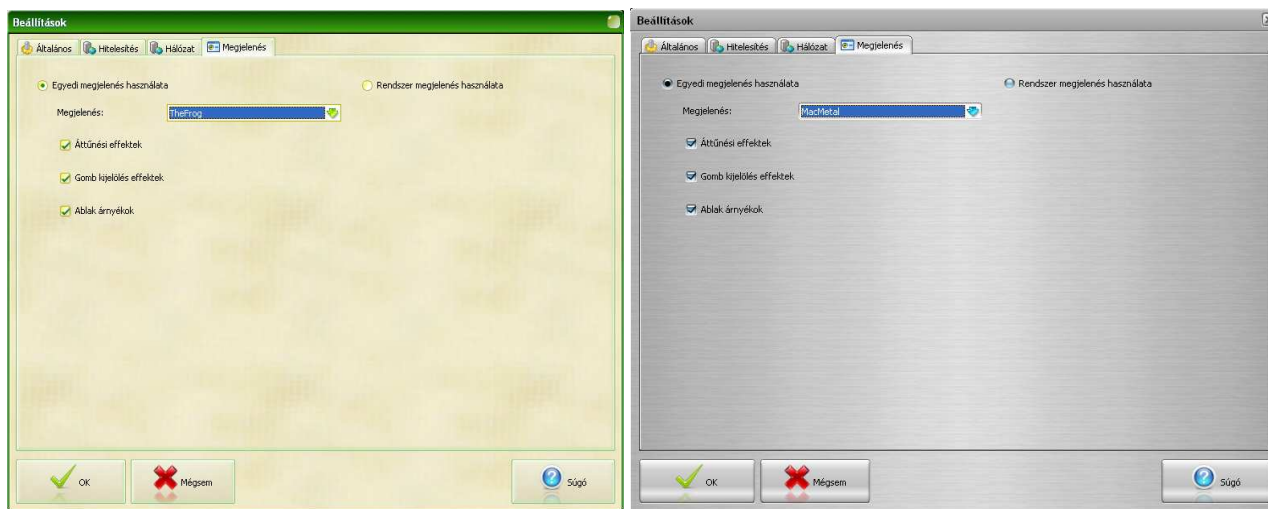


Amennyiben számítógépünk proxy szerveren keresztül csatlakozik a hálózatra, itt tudjuk megadni a programnak a proxy elérési címét. Az automatikus proxy detektálás segítségével a program felismeri az alkalmazott hálózati beállításokat és beilleszti azt. Proxy autentikáció esetén meg kell adni az azonosítót és a jelszót is.

Megjelenés



Lehetőség van a program megjelenését egyedi ízlésünknek megfelelően kiválasztani. Amennyiben a számítógépén a program egyes ablakai lassan jelennek meg, kapcsolja ki itt az effekteket vagy válassza a „Rendszer megjelenés használata” opciót.



A PROGRAM HASZNÁLATA

A sikeres telepítés és regisztráció után meg kell adnunk a **bemeneti és a kimeneti könyvtárat** (a megadott bemeneti könyvtárban fogja megkeresni a program az elektronikus aktákat és listázni az itt találtakat; a megadott kimeneti könyvtárba pedig bemásolja a feldolgozott, archiv időbélyeggel ellátott állományokat).

Ezután, a **Beállítások** menüpontra kattintva megadhatjuk, hogyan kezelje a dossziéinkat a program; pl. a **„Feldolgozott dossziék könyvtára”** mezőnél beállíthatunk egy mappát, ha szeretnénk, hogy a program egy másolatot helyezzen ide az eredeti dossziéről a feldolgozás után. Ezt akkor javasoljuk használni, ha bejelöljük a *„Sikeres kiterjesztés után és a „Feldolgozott dossziék könyvtárba” másolás után, törlődjön a „Bemeneti könyvtárban” lévő forrás dosszié”* opciót (ellenkező esetben az eredeti dossziéink a helyükön maradnak).

Használhatjuk úgy is a programot, hogy a *Beállítások > Általános* felületen bejelöljük az **„Archivált fájlok kerüljenek a bemeneti könyvtárba, ha az automata, fájlnevhez jelző fűzést használunk”** opciót (és persze fölötte is bejelöljük a *„jelző hozzáfűzése”* opciók egyikét legalább). Ekkor nem tudunk kimeneti könyvtárat megadni, a mező sem lesz aktív!

Be kell még másolnunk az egyedi **PIN azonosítót**, amelyet e-mailben küldtünk meg az Ön részére (általában a regisztrációs fájlal együtt).

1. BEMENETI ÉS KIMENETI KÖNYVTÁR MEGADÁSA

A bemeneti és kimeneti könyvtárnak létező könyvtárakat kell megadni (a sor végén lévő mappa ikonra kattintva tudunk tallózni a mappák között). Az itt megadott **bemeneti könyvtár** mappájába kell bemásolni azokat a dossziékat, amelyeket archiválni szeretnénk. Megadhatjuk azt a könyvtárat is, amelyben korábban tároltuk a dossziékat. A program a megadott könyvtár valamennyi mappájában lefuttatja a keresést és az azokban talált dossziékat felkínálja feldolgozásra (megadhatunk akár egy teljes (pl. C:\) meghajtót is).

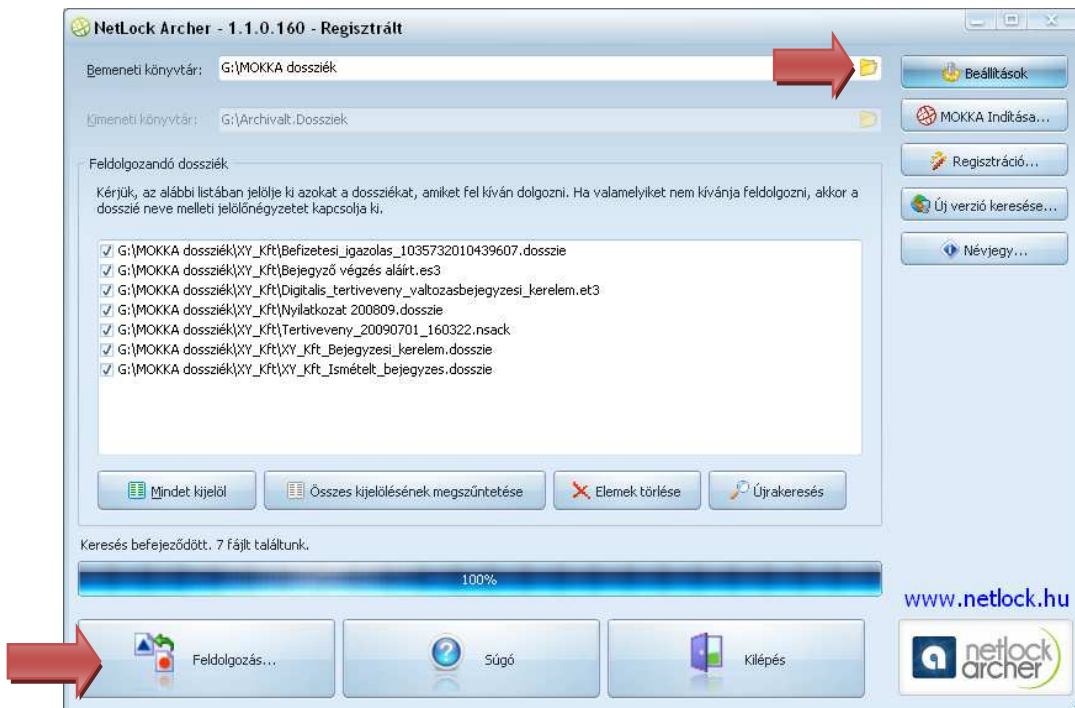
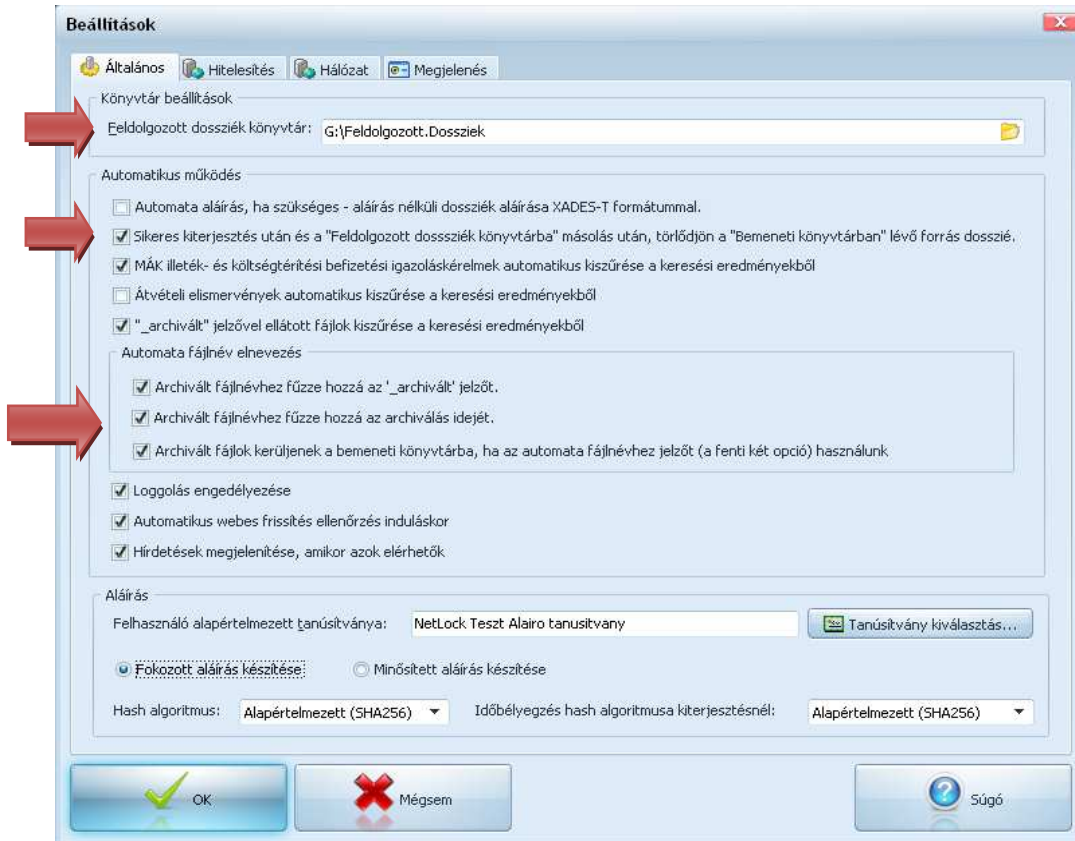
A **kimeneti könyvtár** megadott mappájába kerülnek a sikeresen kiterjesztett, archiválással ellátott dossziék. A program minden feldolgozási folyamat során létrehoz itt egy új mappát, amelynek neve a feldolgozáskori aktuális dátum.

Használhatjuk úgy is a programot, hogy a *Beállítások > Általános* felületen bejelöljük az „Automata fájlnev elnevezés” opciót, valamint az „Archivált fájlok kerüljenek a bemeneti könyvtárba, ha az automata fájlnevhez jelzőt használunk” opciót. Ebben az esetben az **archivált e-aktáink az eredeti helyükre kerülnek** *_archivalt_datum.dosszie fájlnev kiegészítéssel, az eredetiek pedig – a további beállítástól függően – vagy a helyükön maradnak vagy áthelyeződnek az általunk megadott „Feldolgozott dossziék könyvtárba” (ilyenkor kimeneti könyvtárat nem tudunk megadni a program felületén!).

1. lehetőség (külön mappába kerülnek az archivált dossziék):



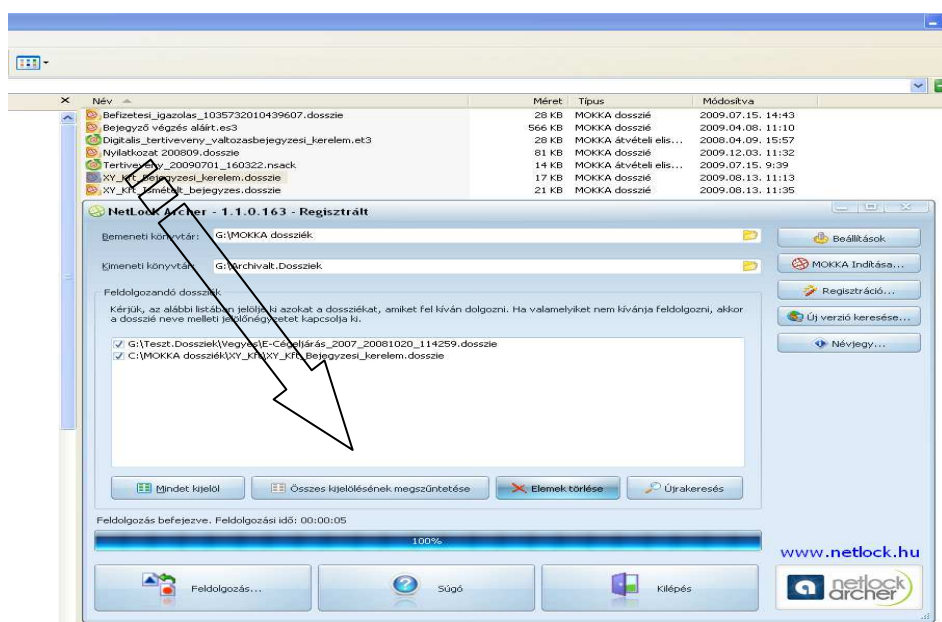
2. lehetőség (az archivált dossziék az eredeti helyükön maradnak):



2. DOSSZIÉK KERESÉSE, AZ ARCHIVÁLANDÓ DOSSZIÉK ÖSSZEÁLLÍTÁSA

A **Dossziék keresése** gombra kattintva, a program listázza a „bemeneti könyvtárban” található dossziékat. A dossziék előtti négyzet bejelölésével választhatjuk ki azokat, amelyeket fel kívánunk dolgozni. A listában lévők tartalmát is megtekinthetjük innen; vagy duplán kattintunk rá, vagy kijelöljük és a „**Mokka indítása**” gombra kattintunk. Ha meg szeretnénk ismételni a keresést, szüntessük meg a kijelöléseket („Összes kijelölés megszüntetése”), ezzel újra aktívá válik a „Dosszié keresése” gomb vagy egyszerűen kattintsunk az „**Újrakeresés**” gombra.

A program lehetőséget ad a **különböző helyeken lévő dossziéink kézzel történő összeválogatására** úgynevezett 'fogd és vidd' (drag and drop) technikával. Ehhez csak annyit kell tennünk, hogy kitallózzuk azokat a dossziékat, amelyet archiválni szeretnénk, kijelöljük a bal egérgombbal, majd a gombot nyomva tartva, egyszerűen behúzzuk az Archer „Feldolgozandó dossziék” listájának helyére őket (ha a tallózás közben tálcára kerülő Archer ikon fölé tartjuk az egér mutatóját, a program ablaka felugrik; az egérgombot a lista mező fölött elengedhetjük).



3. FELDOLGOZÁS

Miután kijelöltük a dossziékat, a **Feldolgozás** gombra kattintva megkezdődik a dossziék ellenőrzése. Amennyiben a **Beállításoknál** bejelöltük az „Automatikus aláírás, ha szükséges” opciót és van olyan dossziénk, amelyet újra alá kell írni (pl. érvénytelen az aláírás vagy nem tartalmaz aláírást), megjelenik a tanúsítvány kiválasztó ablak, majd a PIN kód megadása után a dossziékra aláírás kerül, és megtörténik a kiterjesztés is XAdES-A formátumra. Ha nincs bejelölve az „Automatikus aláírás”, egy ablakban megjelenik az újra aláírást igénylő dossziék listája, itt kiválaszthatjuk, melyek aláírására kerüljön sor. Ebben a listában a következő okok miatt jelenhet meg a dosszié és válhat szükségessé az aláírása:

- sem a dosszié, sem a dossziében lévő dokumentum nincs aláírva,
- a dosszién lévő aláírás érvénytelen (pl. olyan időbélyeg nélküli (XAdES-EPES) aláírás található rajta, amely egy időközben lejárt tanúsítvánnyal készült),

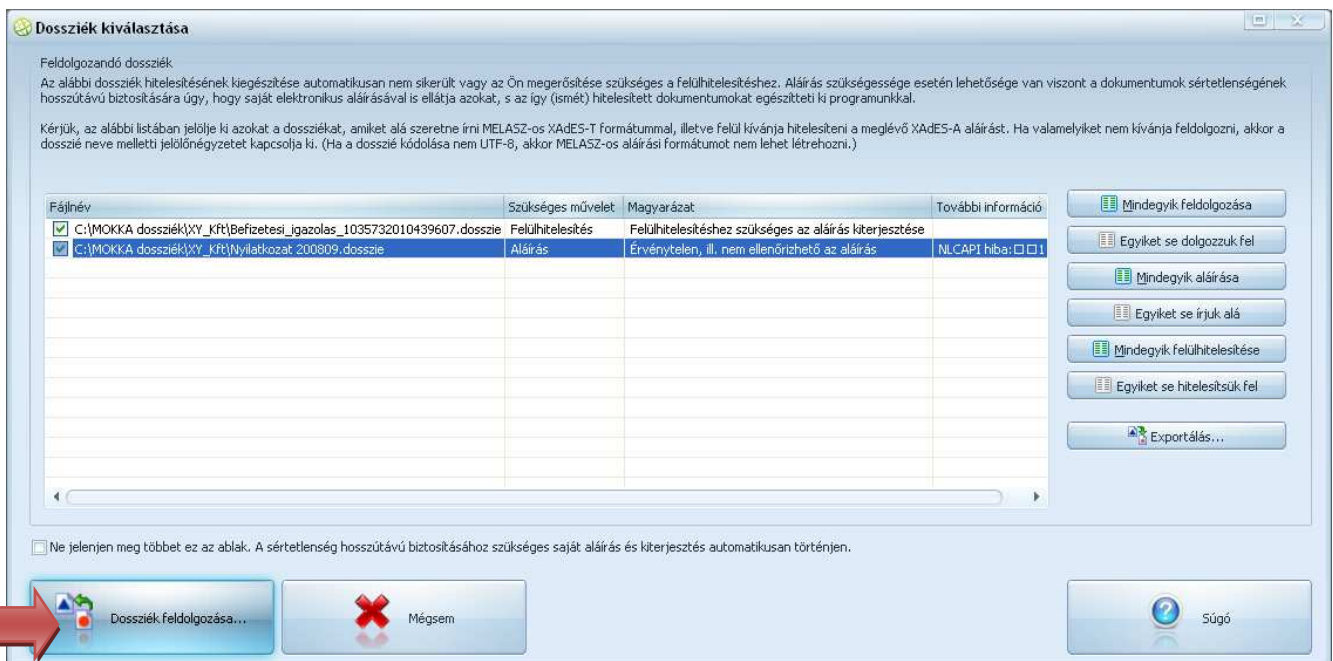
- a dosszién lévő aláírás érvényessége nem állapítható meg (pl. olyan tanúsítvánnyal készült, amelynek a kiadói gyökértanúsítványa nincs felvéve a megbízható kiadók közé a program *Beállítások > Hitelesítés* menüpontja alatt; vagy pedig a tanúsítvány visszavonási állapotáról nem szerezhető be információ),
- az aláírásra használt tanúsítvány jelenleg felfüggesztett vagy visszavont állapotban van.

(Amennyiben az aláíró tanúsítvány érvényessége a tervezett archiválás időpontját megelőzően lejárt, és az eredeti aláírás-csomag visszavonási információt nem tartalmazott, úgy a múltbéli információk automatikus összegyűjtéséhez az aláíró tanúsítványokat és időbélyegeket kibocsátó szolgáltató rendszereinek erre alkalmasnak kell lenniük (a NetLock Kft. ad ilyen szolgáltatást).

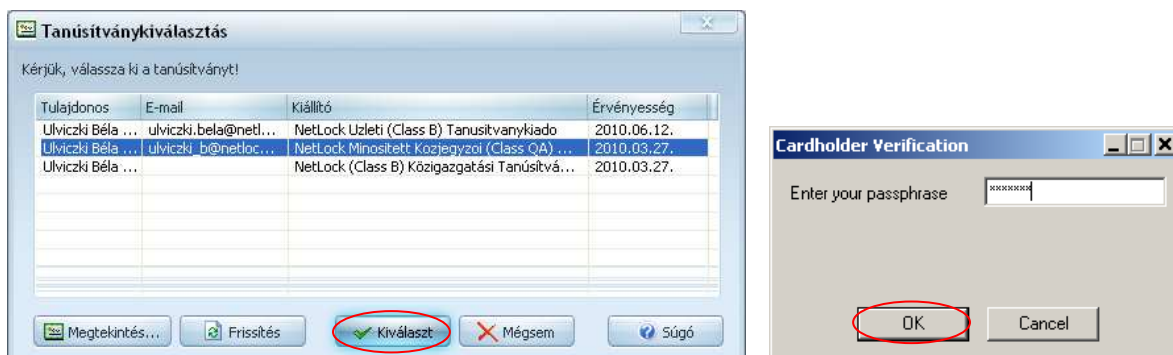
Amennyiben az aláíró tanúsítványokat és időbélyegeket kibocsátó szolgáltató múltbéli információkérések automatikus kiszolgálására nem alkalmas, úgy a szükséges visszavonási információk automatikusan összegyűjtése nem lehetséges és ezért az aláírás kiterjesztésre nem kerülhet sor. Ebben az esetben a visszavonási információkat más módon kell összegyűjteni (pl. közvetlen humán kapcsolatfelvétel az érintett szolgáltatóval), vagy pedig a dosszié ismételt aláírására (mintegy "felülhitelesítésére") olyan aláírás-formátummal, amely már tartalmaz minden, a későbbi ellenőrzéshez szükséges információt, tehát a visszavonási információt is (archív aláírás)).

A **Dossziék kiválasztása** ablakban lehetőségünk van kiválasztani mely dossziék kerüljenek *(újra) aláírásra*, illetve *felülhitelesítésre (archív időbélyegzésre)*. A felülhitelesítés opciót olyan dossziék esetében kínálja fel a program, amelyek már rendelkeznek (legalább egy) archív időbélyeggel (azaz a rajta lévő aláírás formátuma XAdES-A). Javasolt egyébként ezeket a dossziékat is ellátni újabb archív időbélyeggel, ugyanis ezek már a fejlettebb SHA-2 lenyomatképző algoritmussal fognak készülni!

Miután tehát kijelöltük azokat a dossziékat, amelyeket alá akarunk írni XAdES-A formátummal, illetve amelyeken újabb archív időbélyeget szeretnénk elhelyezni, kattintsunk a **Dossziék feldolgozása** gombra. **A feldolgozás elindítása előtt győződjünk meg arról, hogy a chipkártyánk az olvasóban van!**

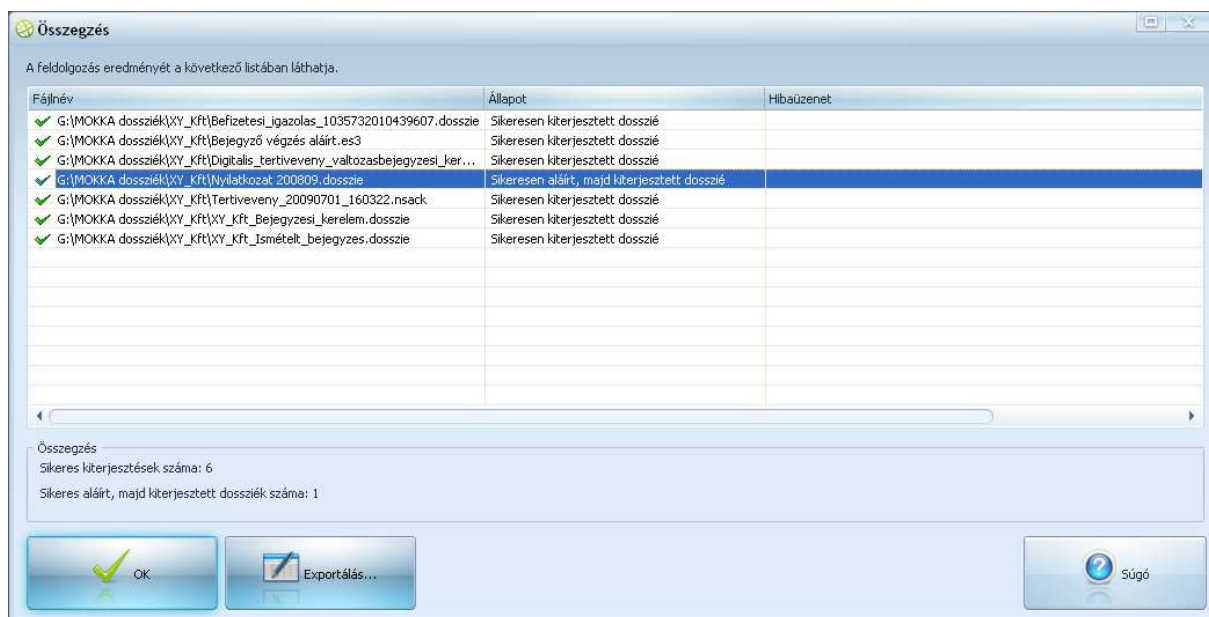


Válasszuk ki a tanúsítványt, amellyel alá szeretnénk írni, majd adjuk meg a kártya PIN kódját. Amennyiben elfelejtettük volna behelyezni a kártyánkat az olvasóba, tegyük be most és kattintsunk a **Frissítés** gombra.



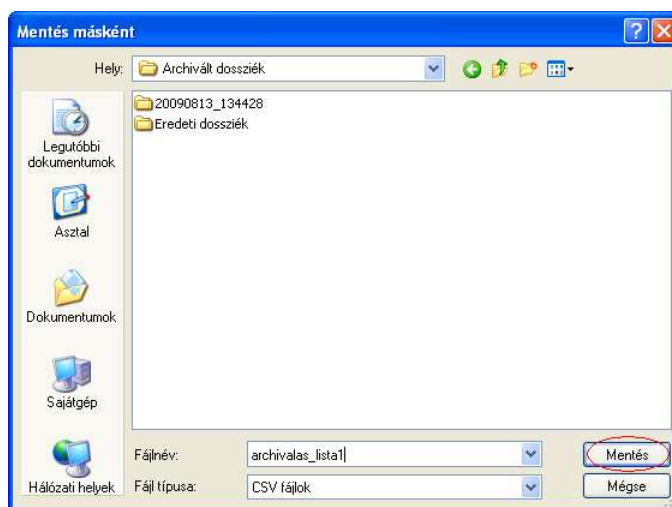
A NetLock által forgalmazott chipkártyák használata esetén elég egyszer megadunk a PIN kódot a tömeges dosszié aláíráshoz, azonban más típusú kártyáknál előfordulhat, hogy minden egyes dosszié aláírása előtt megjelenik a PIN kód bekérő ablak és újra be kell írunk a PIN kódunkat.

Az aláírás után megtekinthetjük a feldolgozás eredményét az „Összegzés” ablakban. Sikeres aláírás és kiterjesztés esetén „Sikeresen aláírt, majd kiterjesztett dosszié” üzenet szerepel a listában.



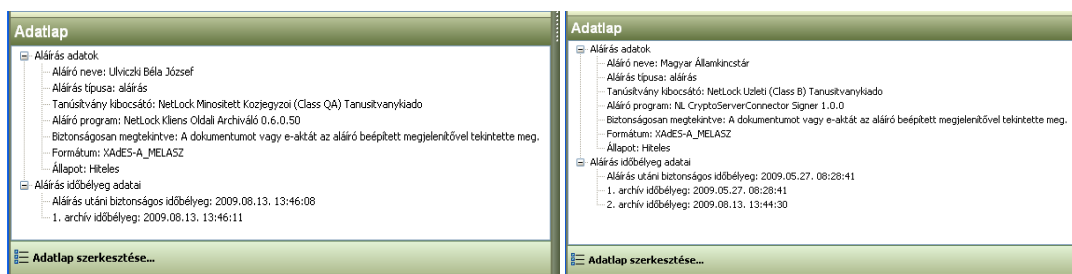
Amennyiben nem volt sikeres a feldolgozás, a hiba okáról kapunk itt értesítést; az adott sorra duplán kattintva megtekinthetjük a teljes hibaüzenetet.

Lehetőségünk van a feldolgozás eredményét elmentenünk. Az **Exportálás** gombra kattintva CSV fájlba menthetjük a feldolgozott dossziék listáját, a feldolgozás eredményével együtt. A CSV fájl arra alkalmas programmal – pl. Excellel – betölthetjük a könnyebb megtekintés érdekében.



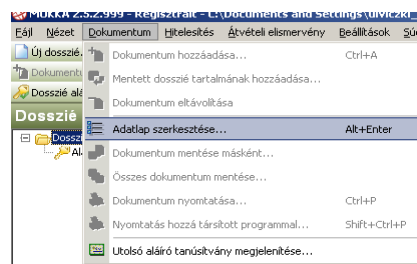
AZ ARCHÍV ALÁÍRÁSSAL ELLÁTOTT DOSSZIÉK ELLENŐRZÉSE

Tallózzuk ki azt a mappát, amelyet „Kimeneti könyvtárként” megadtunk és nyissuk meg az egyik mappát, amelyet a feldolgozás során létrehozott a program. Nyissunk meg egy itt lévő dossziét a MOKKA programmal. A megnyílt dosszién jelöljük ki az aláírást, majd itt jobb egérgombot megnyomva, a megjelenő menüsorból válasszuk ki az aláírás újra ellenőrzése funkciót. Az adatlapon megtekinthetjük az aláírás és az időbélyegzés adatait. Minden egyes archiválás után újabb archiv időbélyeg kerül az aláírásra, ennek elvégzését kb. kétévenként javasolt megismételni.

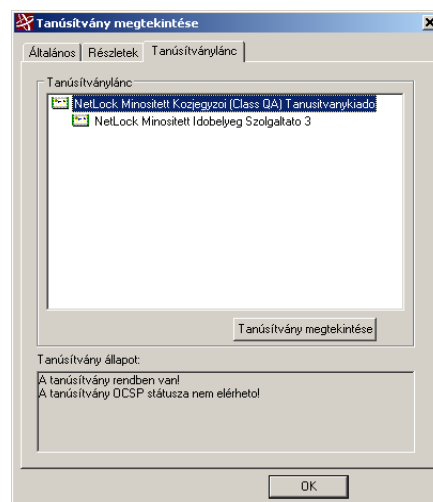
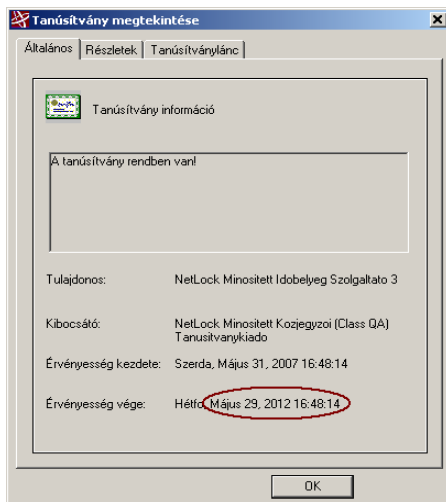
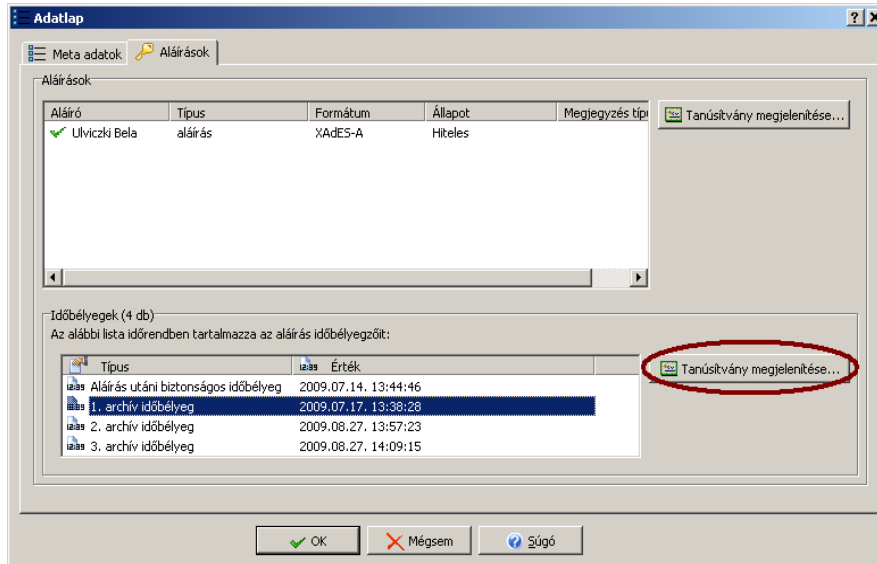


Lehetőségünk van a MOKKA program segítségével a dossziékon lévő aláírói-, kiadói-, időbélyegző tanúsítványok érvényességi idejéről is meggyőződni. Ezáltal tudhatjuk azt az időpontot, ami előtt javasolt újra archiv időbélyegzőt elhelyeznünk a dosszién. (Erre azért lehet szükség, mert egyes aláírás ellenőrző alkalmazások (nem feltétlen helyesen) érvénytelennek tekintik azokat az aláírásokat, amelyeken az időbélyegző kiadói tanúsítványa lejárt.)

A megnyitott dosszién jelöljük ki az adott aláírt dosszié nevét, majd a menüsor **Dokumentum** menüpontjára kattintva, a legördülő menüből válasszuk ki az **Adatlap szerkesztése** parancsot.



A megjelenő Adatlapon válasszuk az **Aláírások** opciót, majd jelöljük ki azt az aláírást vagy időbélyeget, amelynek a tanúsítványát meg kívánjuk tekinteni.



A **Tanúsítványlánc** fülre kattintva láthatjuk a teljes tanúsítványláncot, ennek elemeit szintén meg tudjuk tekinteni.

TOVÁBBI TEENDŐK AZ ARCHÍV ALÁÍRÁS UTÁN

Az archív aláírással ellátott dokumentumokkal kapcsolatban további biztonsági intézkedések megtételére van szükség ahhoz, hogy biztosíthassuk az elektronikus dokumentumok hosszú távú megőrzésére vonatkozó, előírt követelményeknek való megfelelést. Meg kell oldani ugyanis a törlés, a megsemmisítés, a véletlen megsemmisülés és sérülés, illetve a jogosulatlan hozzáférés elleni védelmet is.

Erre a célra a következő lehetőségeket ajánljuk:

- Az archív aláírás elhelyezése után írjuk ki lemezre a dokumentumokat két példányban pl. SecurDisk technológiával. Ez lehetővé teszi az adatok jelszóval való védelmét az illetéktelen hozzáféréssel szemben. A technológia a sérülésekkel szemben is védelmet biztosít azáltal, hogy a lemezen lévő összes szabad helyre másolatként felírja az adatokat, így egy esetleges karcoldás után is visszanyerhető a lemezre kiírt adat.
- Az adathordozókat elzárt széfben tároljuk.
- Az lemezeket 2 évente írjuk újra (a jelenlegi kutatások alapján 2 évente javasolt a korábban felírt adathalmaz új adathordozóra másolása, a lemezek tárolási képességének romlása miatt.)

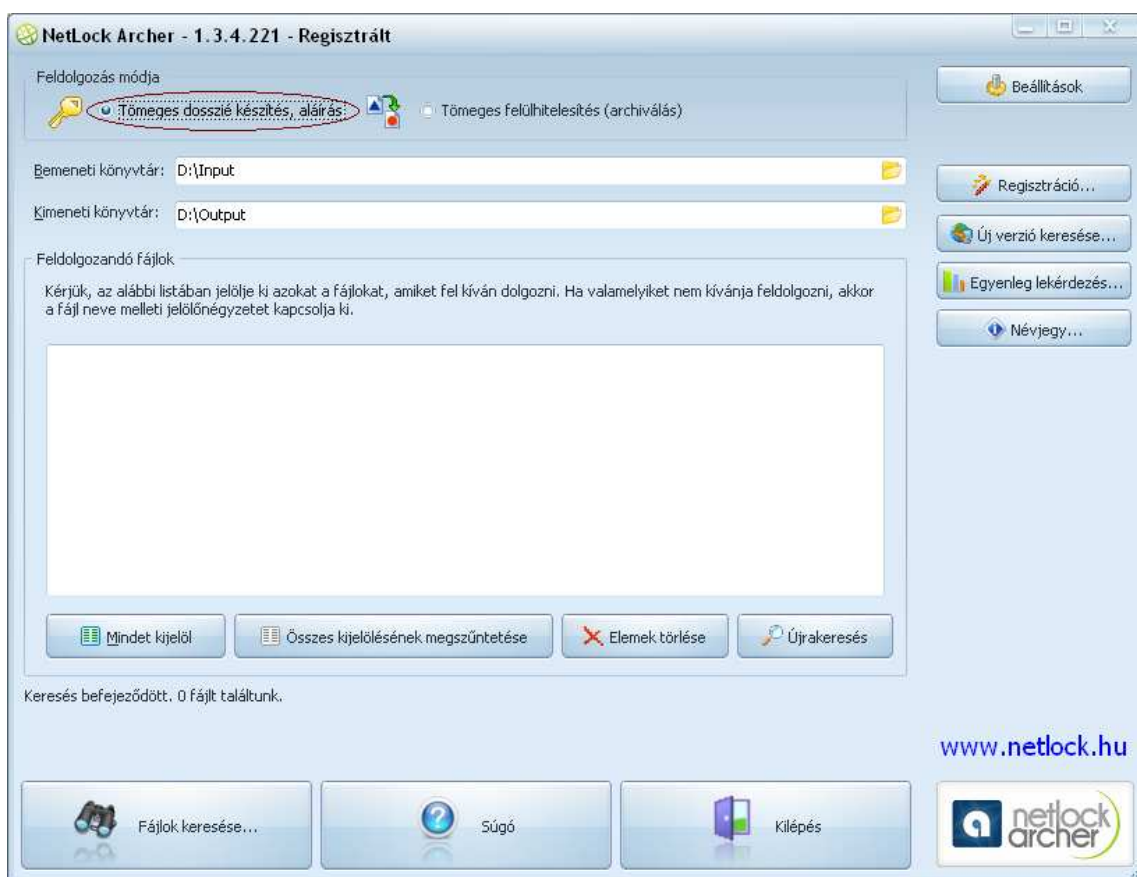
(II). TÖMEGES DOSSZIÉ KÉSZÍTÉS, ALÁÍRÁS

A program e funkcióját csak speciális licenccel lehet elérni, ez ügyben kérjük, vegye fel a kapcsolatot ügyfélszolgálatunkkal.

A Tömeges dosszié készítés opciót kiválasztva a program segítségével lehetőségünk van bármilyen kiterjesztésű fájlt digitálisan aláírt (hitelesített) e-aktába helyezni, mindezt tömeges feldolgozással, azaz a műveletet egyetlen lépésben végrehajthatjuk a bemeneti könyvtárban lévő valamennyi állományon. (Az általában használt aláíró alkalmazásokkal ez (dokumentum csatolása, aláírás) meglehetősen időigényes lenne).

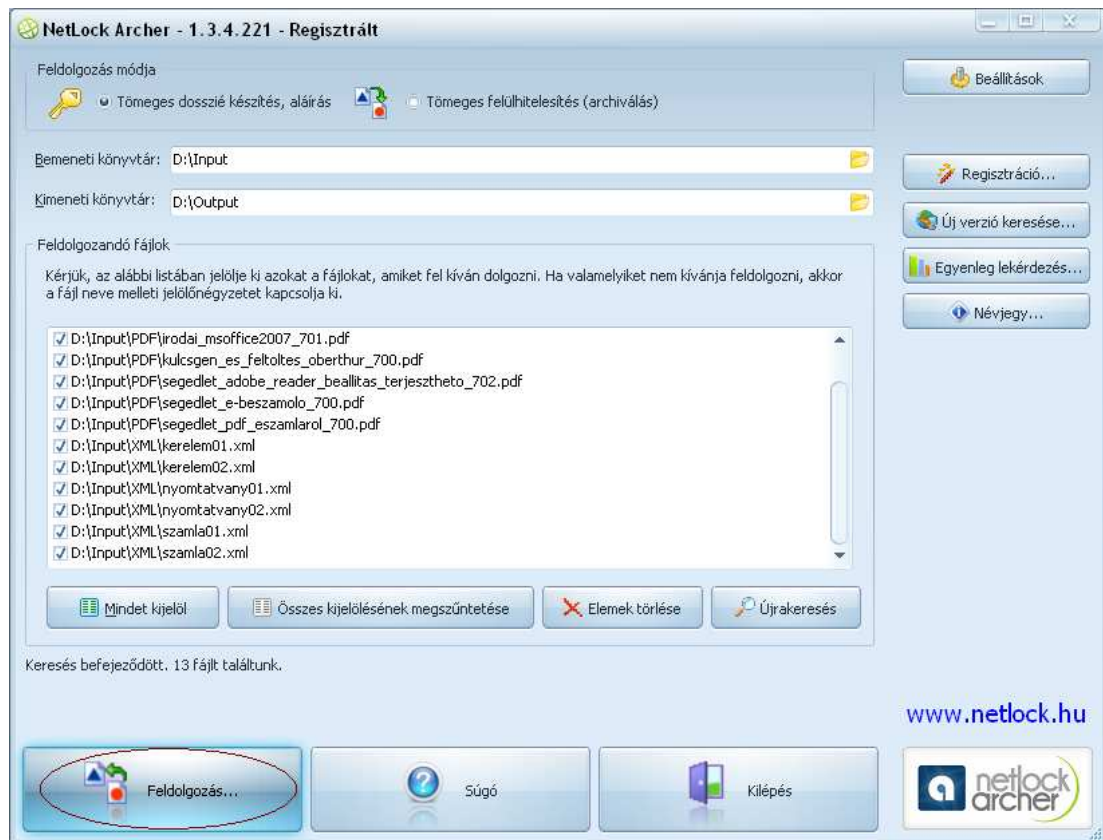
A PROGRAM HASZNÁLATA

- Amennyiben rendelkezünk megfelelő licenccel, a program felületén a *Feldolgozás módja* menü alatt válasszuk ki a „Tömeges dosszié készítés, aláírás” opciót:

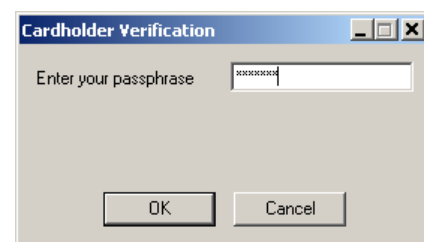
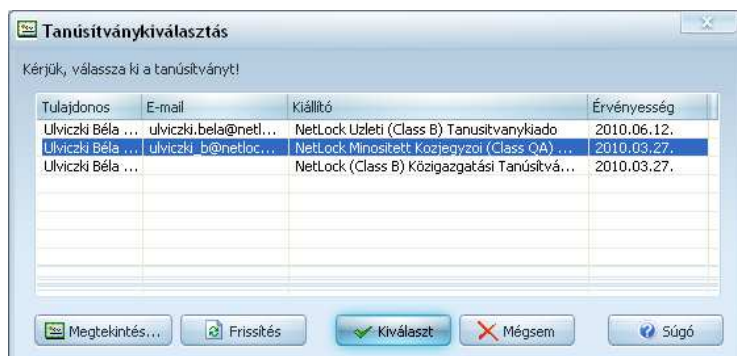


- Adjuk meg a **bemeneti könyvtárat** (feldolgozandó fájlokat tartalmazó mappa), valamint a **kimeneti könyvtárat** (ide kerülnek a feldolgozott fájlok, az aláírt dossziék).
- Végezzük el a szükséges beállításokat a **Beállítások** gombra kattintás után (lásd „A telepítés utáni felhasználói beállítások” fejezetet).

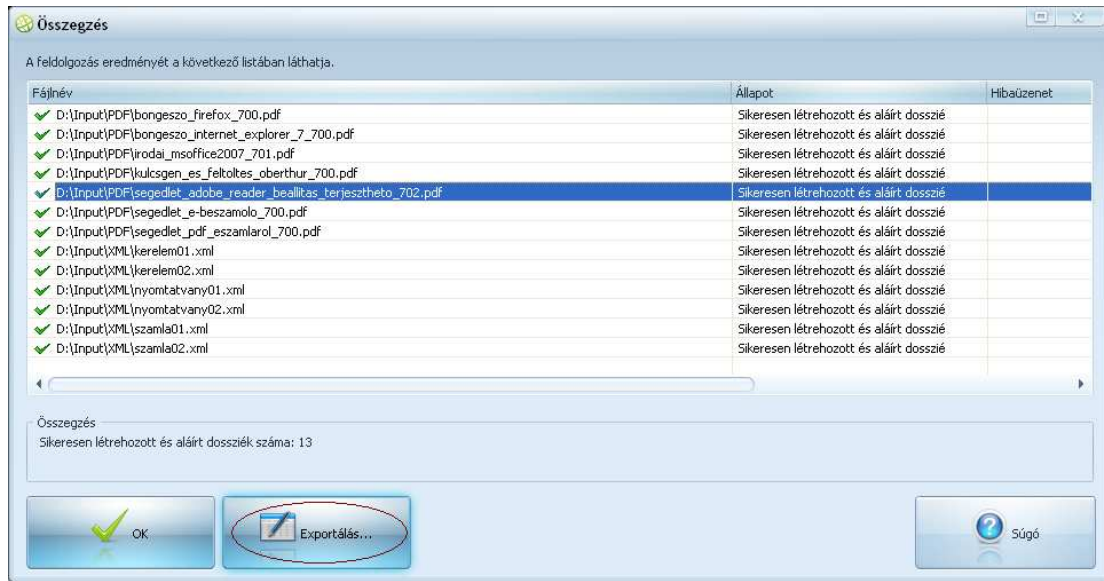
4. Kattintsunk a „**Fájlok keresése**” gombra, majd indítsuk el a feldolgozást.



5. Válasszuk ki az aláíró tanúsítványunkat, illetve chipkártya használata esetén adjuk meg a kártya PIN kódját.



6. A feldolgozás végén lehetőségünk van a feldolgozás eredményét elmentenünk. (Hibaüzenet esetén az adott sorra duplán kattintva, megtekinthetjük a teljes hibaüzenetet).



7. Az aláírt állományokat ellenőrizhetjük; tallózzuk ki azt a mappát, amelyet kimeneti könyvtárként megadtunk és nyissunk meg egy benne lévő dossziét Netlock MOKKA programmal. Az adatlapon láthatjuk az aláírás adatait:

