Elektronikus hitelesítés a gyakorlatban

Tapasztó Balázs
Vezető termékmenedzser
Matáv – Üzleti Szolgáltatások Üzletág

2005. április 1.

matáv
a szavakon túl

Elektronikus hitelesítés a gyakorlatban

1. *Az elektronikus aláírás törvény*
2. *Hitelesítés szolgáltatás*
3. *Az elektronikus aláírás típusai*
4. *Elektronikus aláírás bemutatása egy aláíró szoftverrel*
5. *Elektronikus aláírás igénylése*
6. *Gyakorlati felhasználási lehetőségek*

matáv
a szavakon túl

Az elektronikus aláírás törvény

- *A magyar „elektronikus aláírás” törvény (Eat., 2001/XXXV, illetve 2004/LV) jogi alapot biztosít a hitelesítés szolgáltatások nyújtásához*
- *Ezáltal szabályozza az elektronikus aláírások üzleti/magáncélú felhasználását*
- *A törvény megfelel az európai normáknak (1999/93/EC)*
- *A jogszabályt kiegészíti számos további rendelet (16/2001 MeHVM, 151/2001 MeHVM rendeletek változnak április 1-től !)*
- *Készülőben az archiválásról szóló rendelet*

matáv
a szavakon túl

Hitelesítés szolgáltatás

- *Hatóság (NHH) által nyilvántartásba vett un. Hitelesítés szolgáltató jogosult nyújtani*
- *Szervezetek/személyek azonosítása (hitelesítése), digitális tanúsítvány kiállítása részükre*
- *Digitális tanúsítvány alkalmas elektronikus aláírás készítésére és azonosításra az elektronikus világban (törvény!!!)*
- *Időbélyegzés szolgáltatás: tranzakció időpontjának hitelesítése*
- *A technológia a PKI (Public Key Infrastructure) amely az elektronikus aláírás és titkosítás elfogadott technológiája*

matáv
a szavakon túl

Hitelesítés szolgáltatás

Az elektronikus aláírás és a tikosítás műszaki alapja:
Publikus Kulcsú Infrastruktúra

Aszimmetrikus kulcsú titkosítási eljárások

Mindenfelhasználó rendelkezik egy kulcspárral.

Nyilvános kulcs

Titkos kulcs

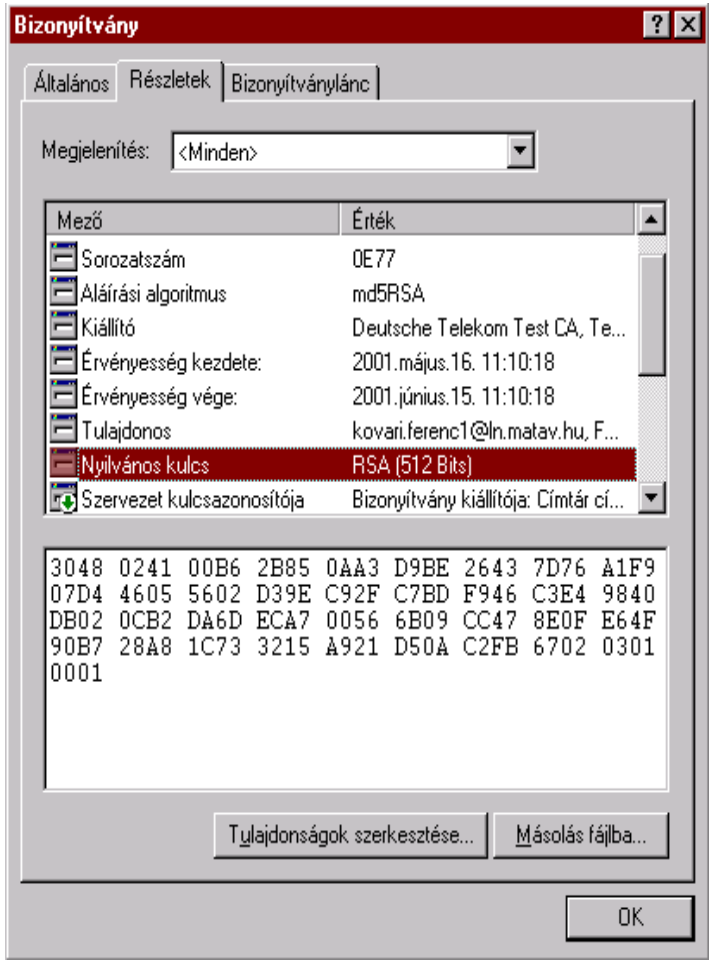
amelyek összetartoznak.

A titkos kulcsot védeni kell, a másikat publikussá kell tenni.

matáv
a szavakon túl

Hitelesítés szolgáltatás

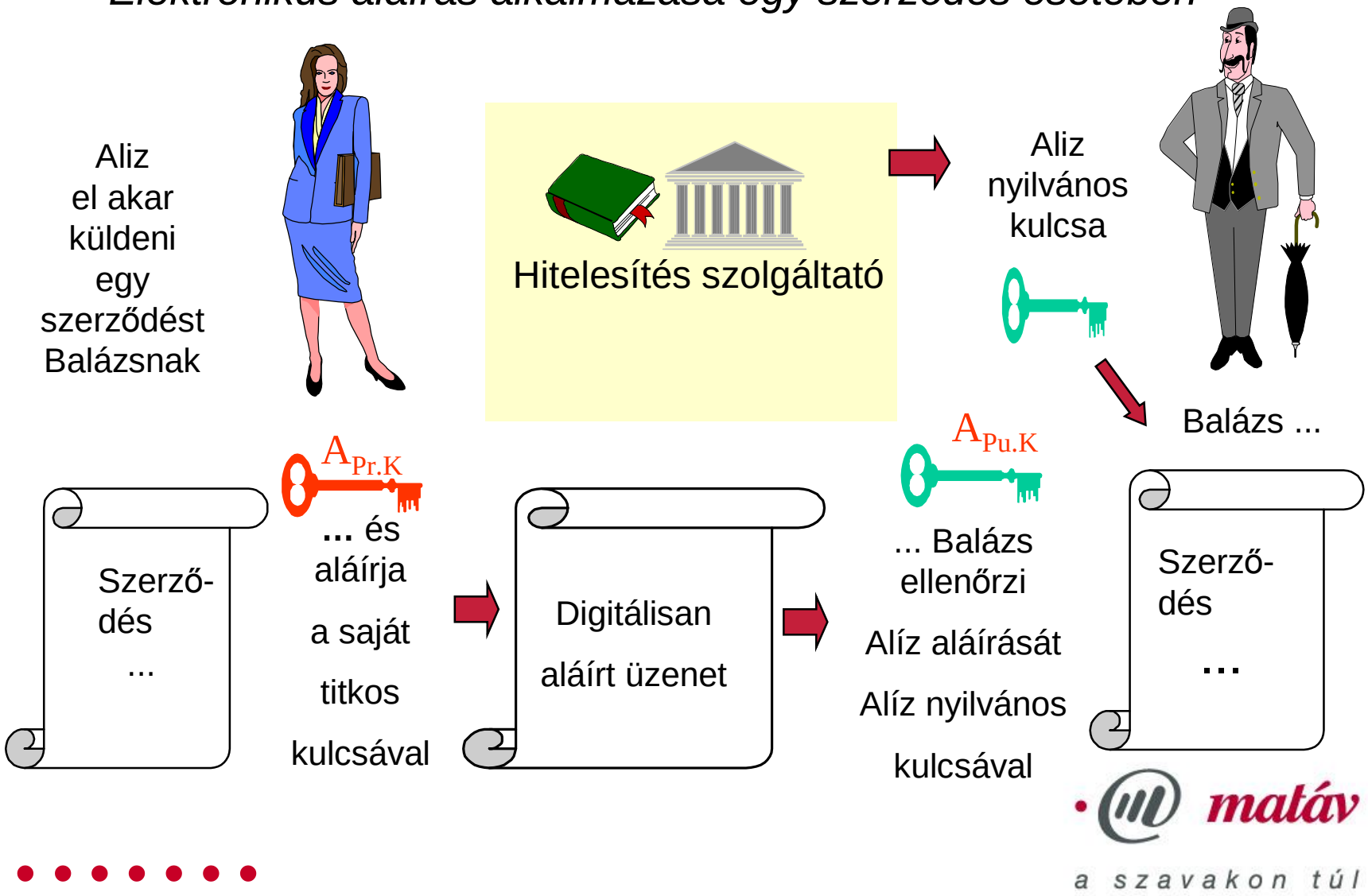
- *A Hitelesítés szolgáltató: Trusted Third Party (megbízhatónak tekintett harmadik fél)*
- *A hitelesség problémájának megoldása: digitális tanúsítvány*
- *A digitális tanúsítvány: a tulajdonos és nyilvános kulcsának összetartozását igazolja*
- *Az elektronikus aláírás (és időbélyegzés) már csak egy lépés*



matáv
a szavakon túl

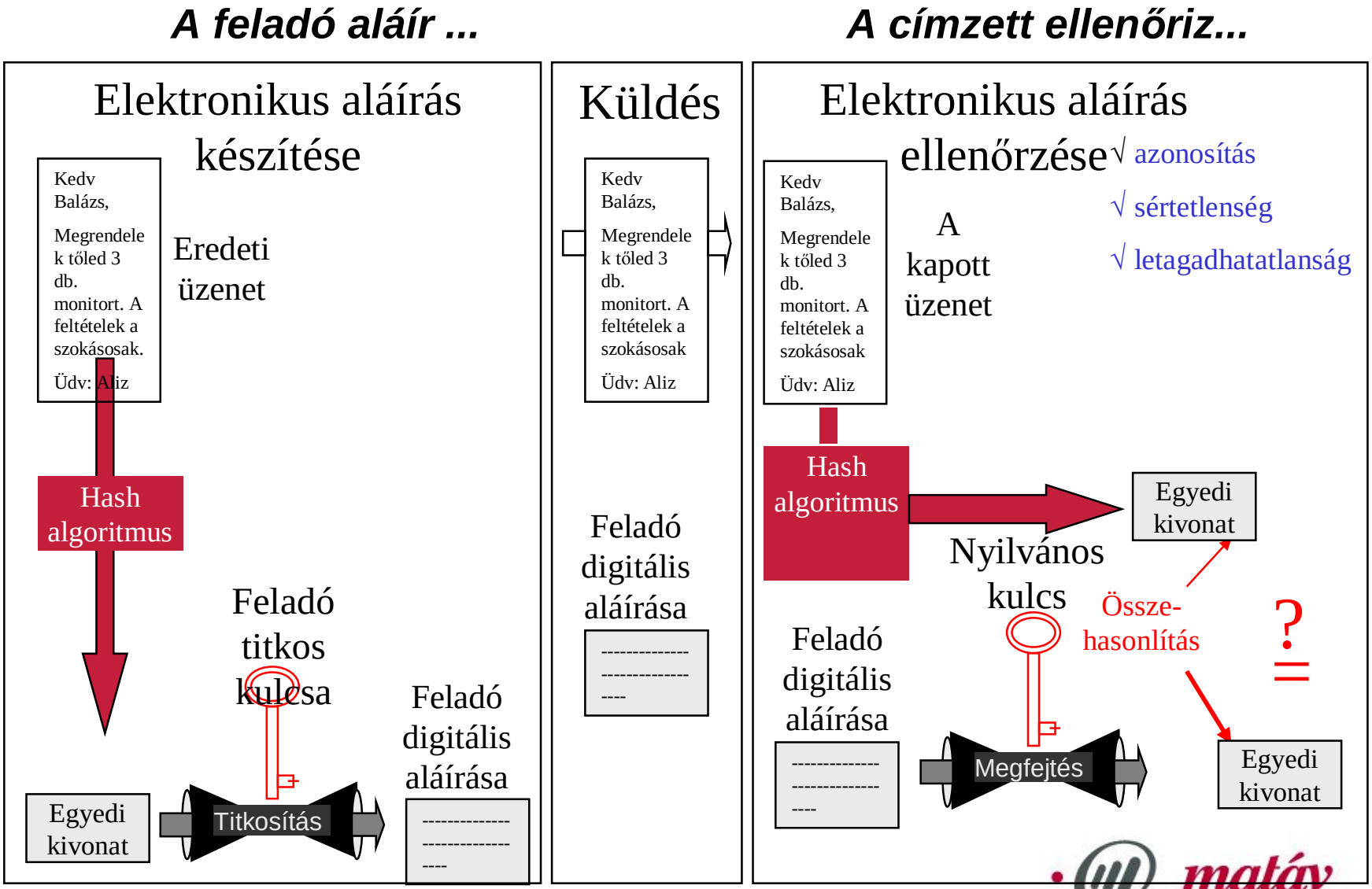
Hitelesítés szolgáltatás

- *Elektronikus aláírás alkalmazása egy szerződés esetében*



matáv
a szavakon túl

… Mindez csak egy kattintás az egérrel …



matáv
a szavakon túl

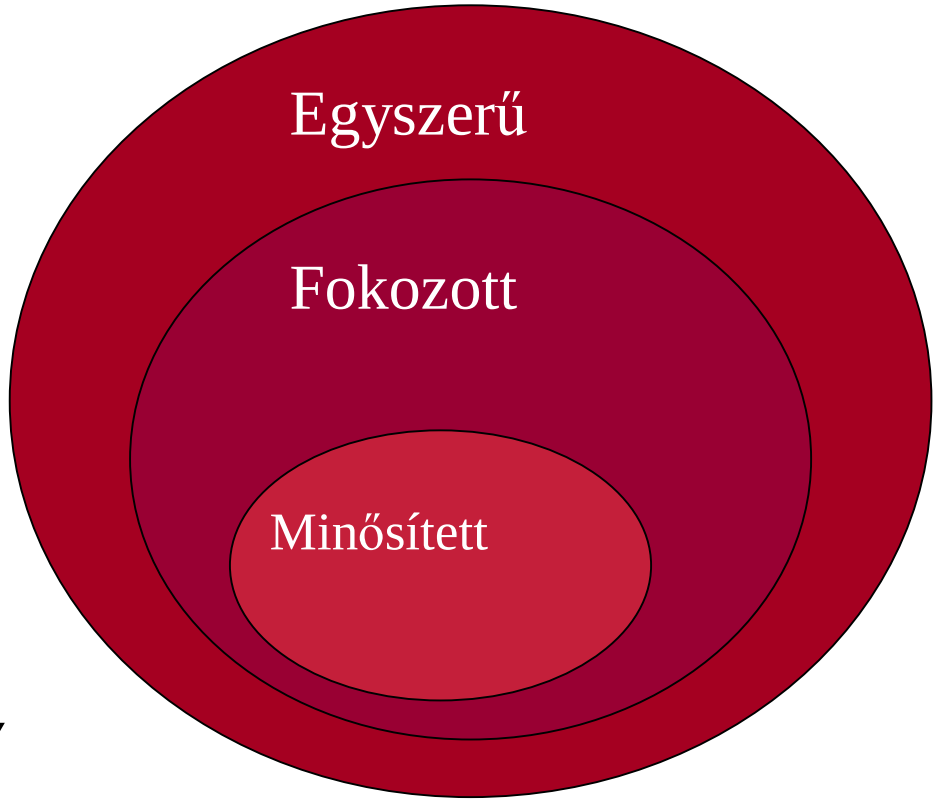
Hitelesítés szolgáltatás

- *A digitális tanúsítvány kiállítása mellett további szolgáltatások*
- *Időbélyegzés szolgáltatás*
  - *Gyakran feledésbe merül, pedig rendkívül fontos (pl. eSzámla)*
  - *Fontos az időforrás hitelessége*
- *Aláírás létrehozó adat elhelyezése aláírás létrehozó eszközön szolgáltatás (???)*
  - *Digitális tanúsítvány elhelyezése chip kártyán vagy egyéb eszközön*
  - *Minősített eszközök (BALE)*
  - *USB token*
- *Titkosító tanúsítványok*

matáv
a szavakon túl

Elektronikus aláírás típusai

- *„Egyszerű” elektronikus aláírás*
- *Fokozott biztonságú elektronikus aláírás*
- *Minősített elektronikus aláírás*



- *Ezek lehetnek üzleti vagy magánszemély tanúsítvány*

matáv
a szavakon túl

Elektronikus aláírás típusai

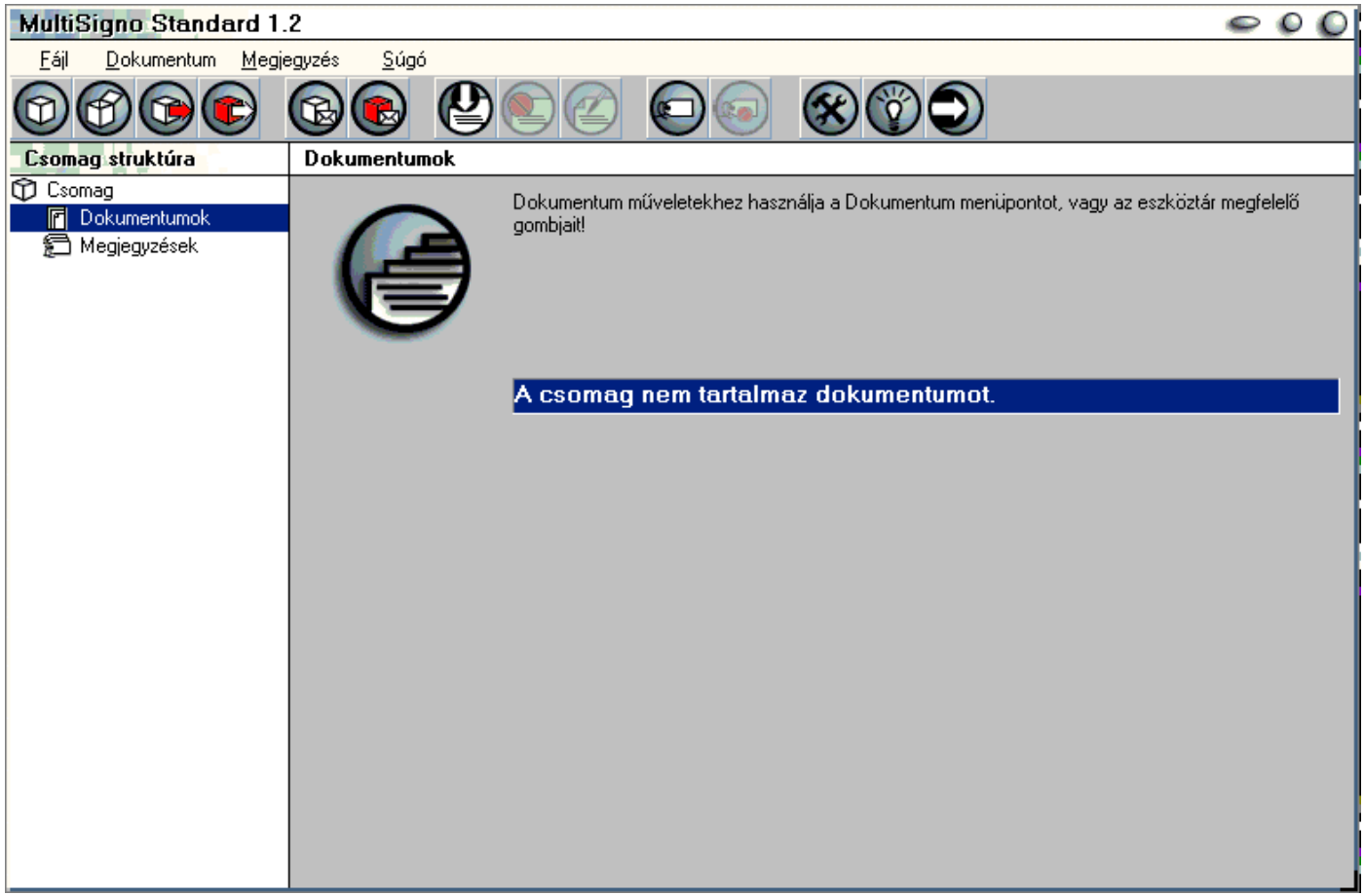
- *Mi szükséges az elektronikus aláíráshoz?*
- *Szükség van egy digitális tanúsítványra (jó ha érvényes és még jobb ha tudjuk a titkos kulcs jelszavát)*
- *Ha a tanúsítvány chip kártyán található, akkor szükség van egy telepített kártyaolvasóra (minősített tanúsítvány esetében kizárólag chip kártyás lehet)*
- *Kell egy olyan alkalmazás amely képes aláírni*
- *Jó ha van internet kapcsolat ellenben hibák léphetnek fel*

matáv
a szavakon túl

Elektronikus aláírás bemutatása

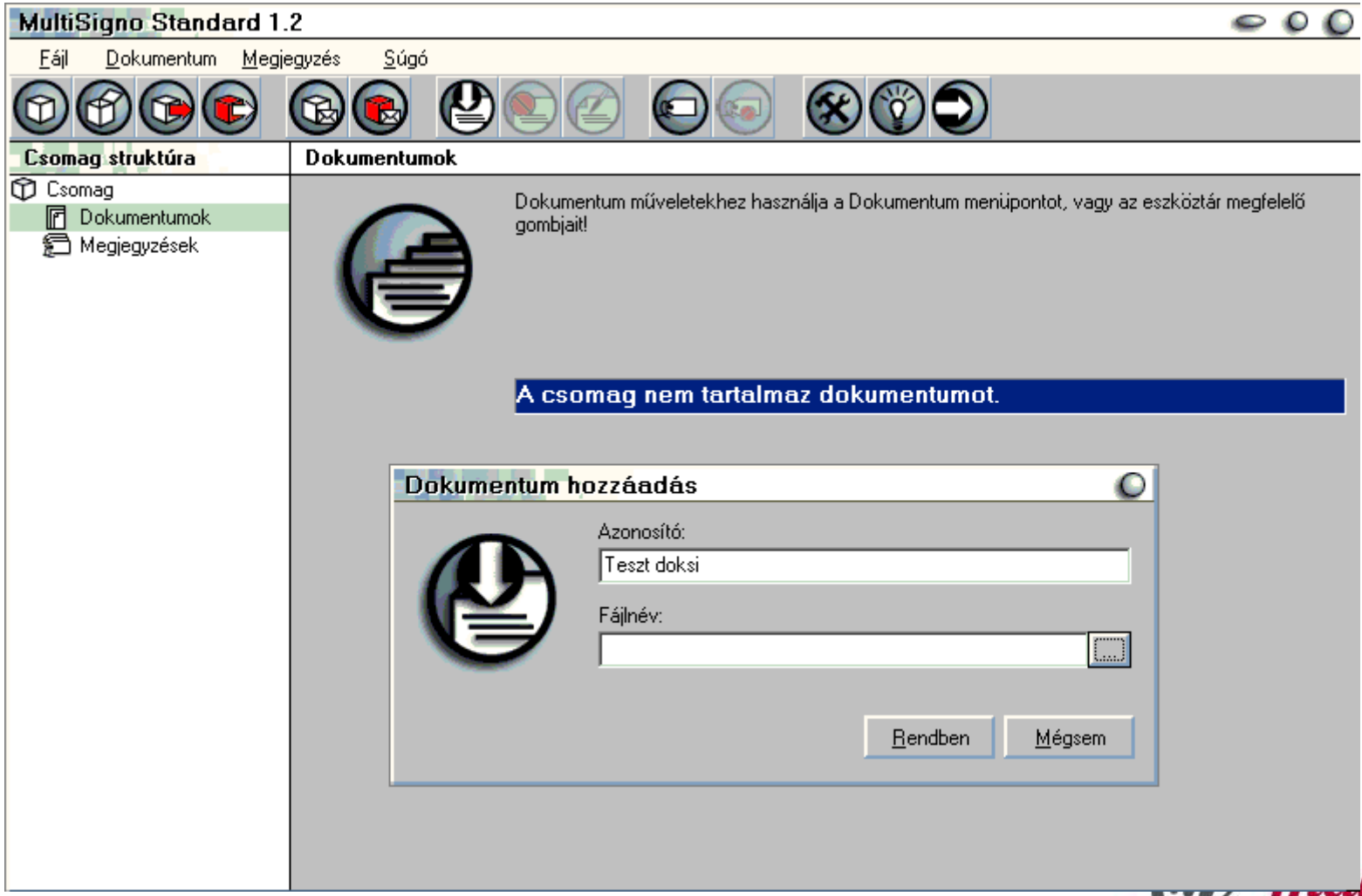
matáv
a szavakon túl

Elektronikus aláírás bemutatása



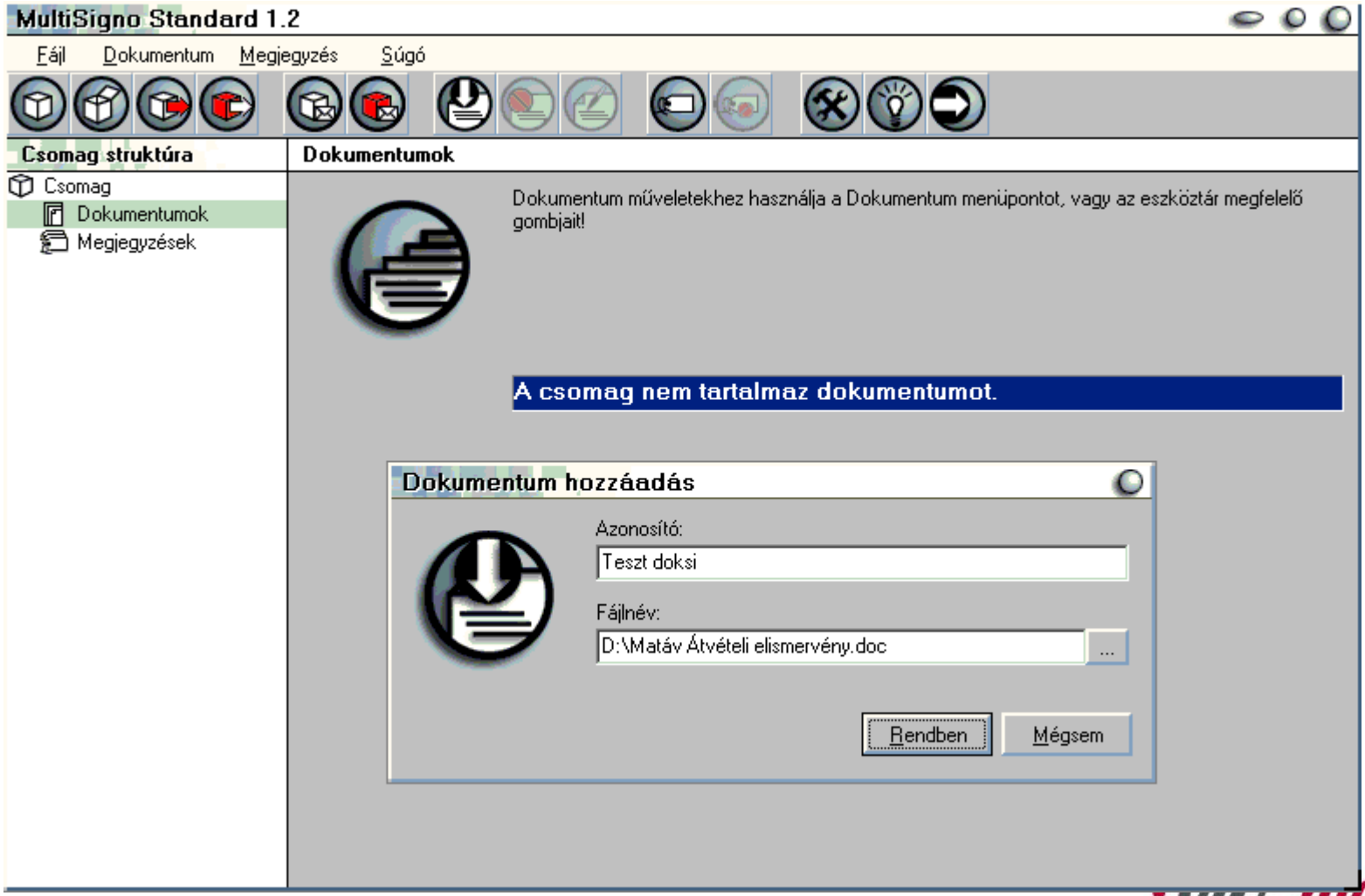
matáv
a szavakon túl

Elektronikus aláírás bemutatása



a szavakon túl

Elektronikus aláírás bemutatása



matáv
a szavakon túl

MultiSigno Standard 1.2

Fájl Dokumentum Megjegyzés Súgó

Csomag struktúra

- Csomag
  - Dokumentumok
    - Teszt doksi
  - Megjegyzések

Dokumentum tulajdonságai

A dokumentum tulajdonságait a dokumentum hozzáadásakor állítjuk be. Ha alá kívánja írni a dokumentumot, használja a Dokumentum/Aláírás menüpontot, vagy az eszköztár megfelelő nyomógombját. Az aláíró tanúsítványának megtekintéséhez duplán kattintson az aláírásra.

Dokumentum neve:
Teszt doksi

Létrehozás dátuma:
2005-02-04 11:14:13

Fájl neve:
Matáv Átvételi elismervény.doc

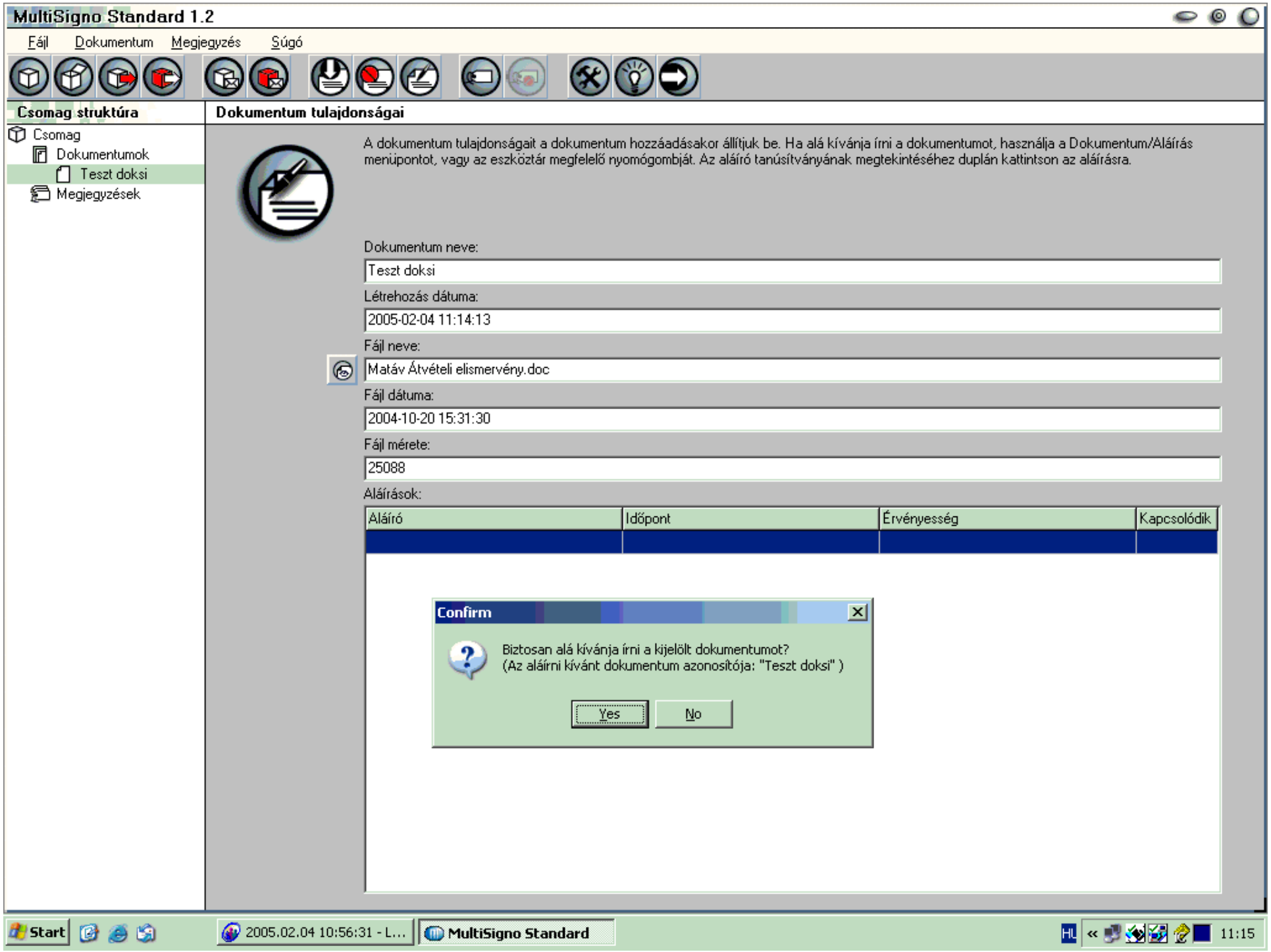
Fájl dátuma:
2004-10-20 15:31:30

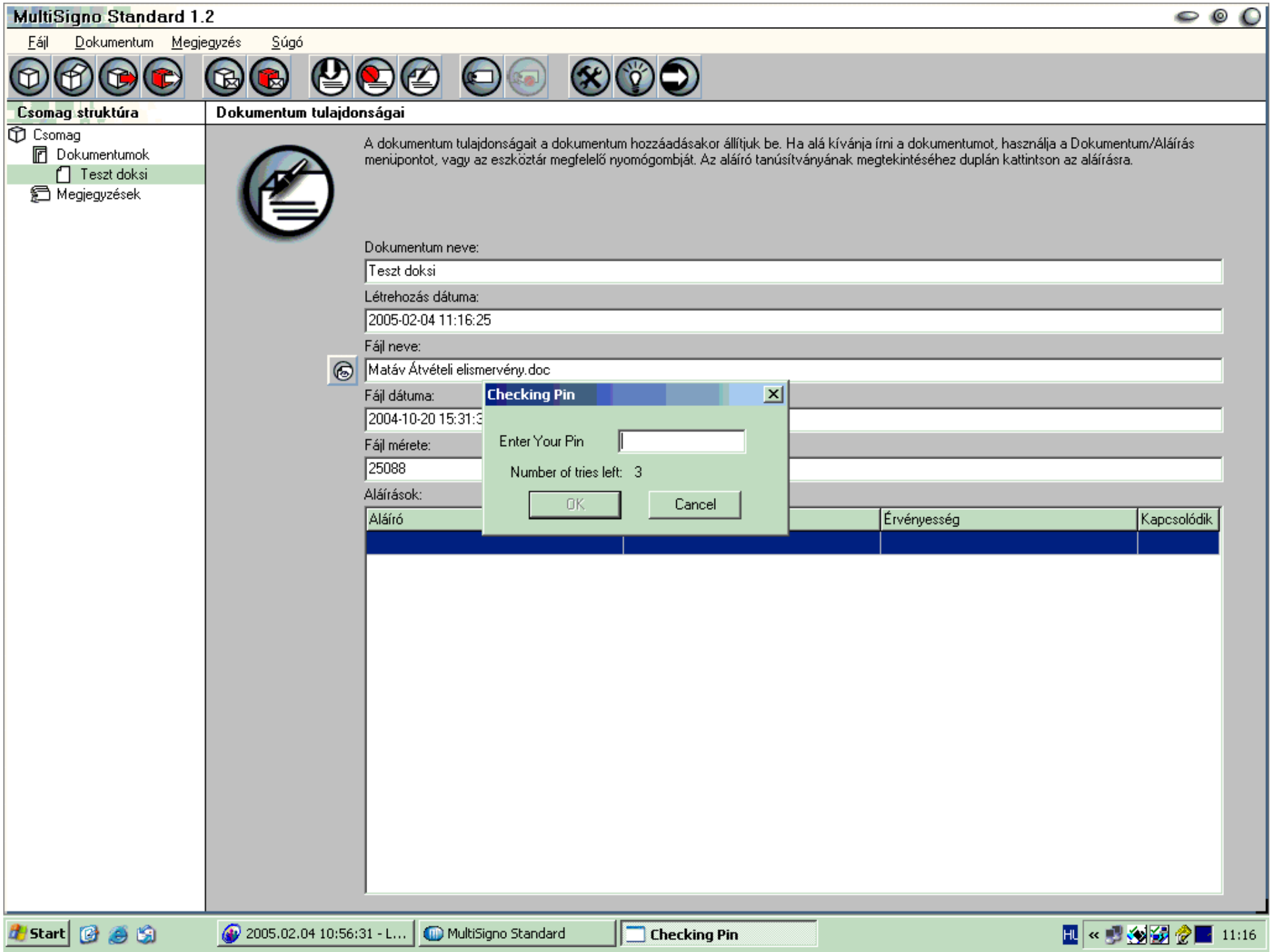
Fájl mérete:
25088

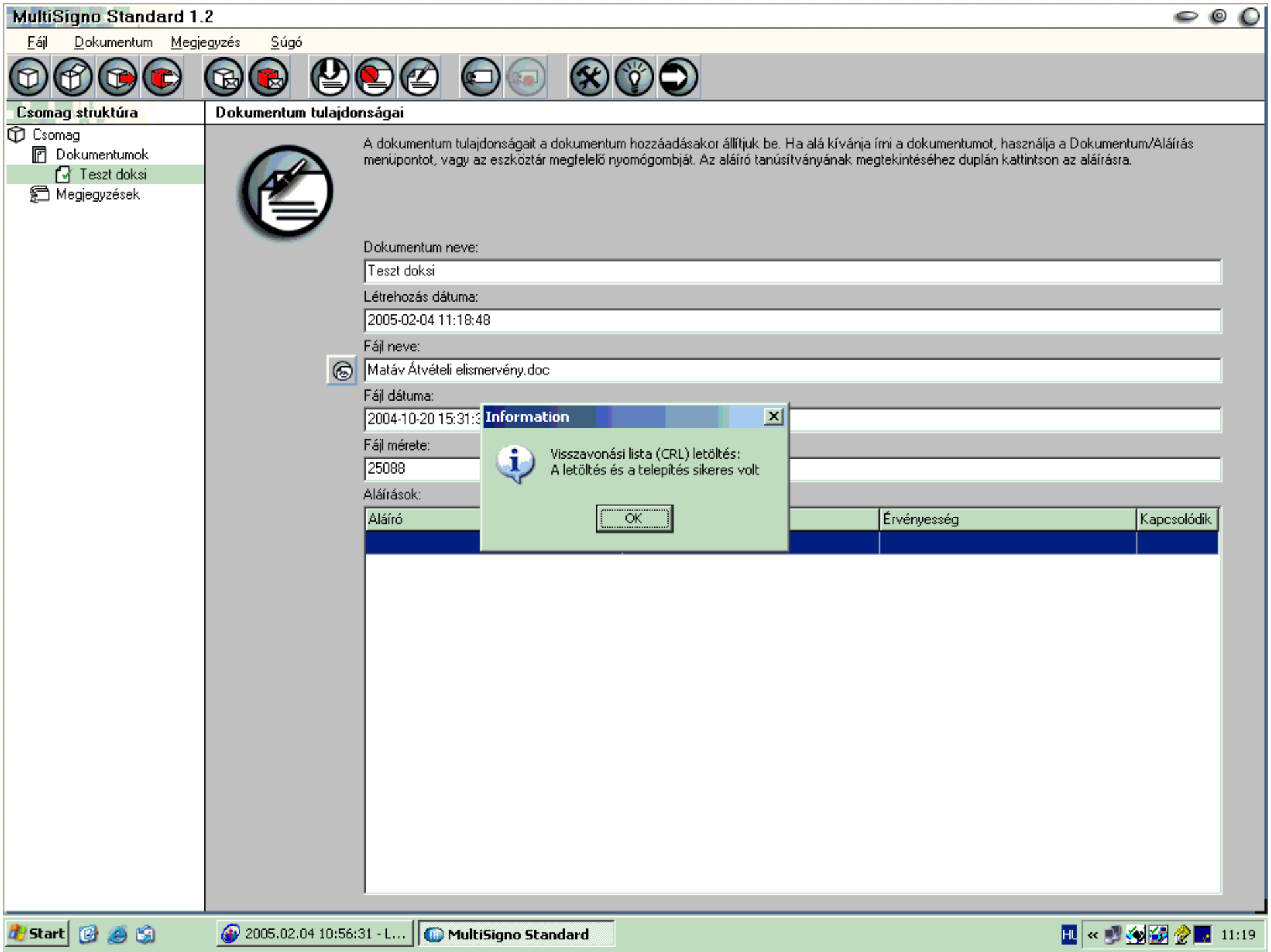
Aláírások:

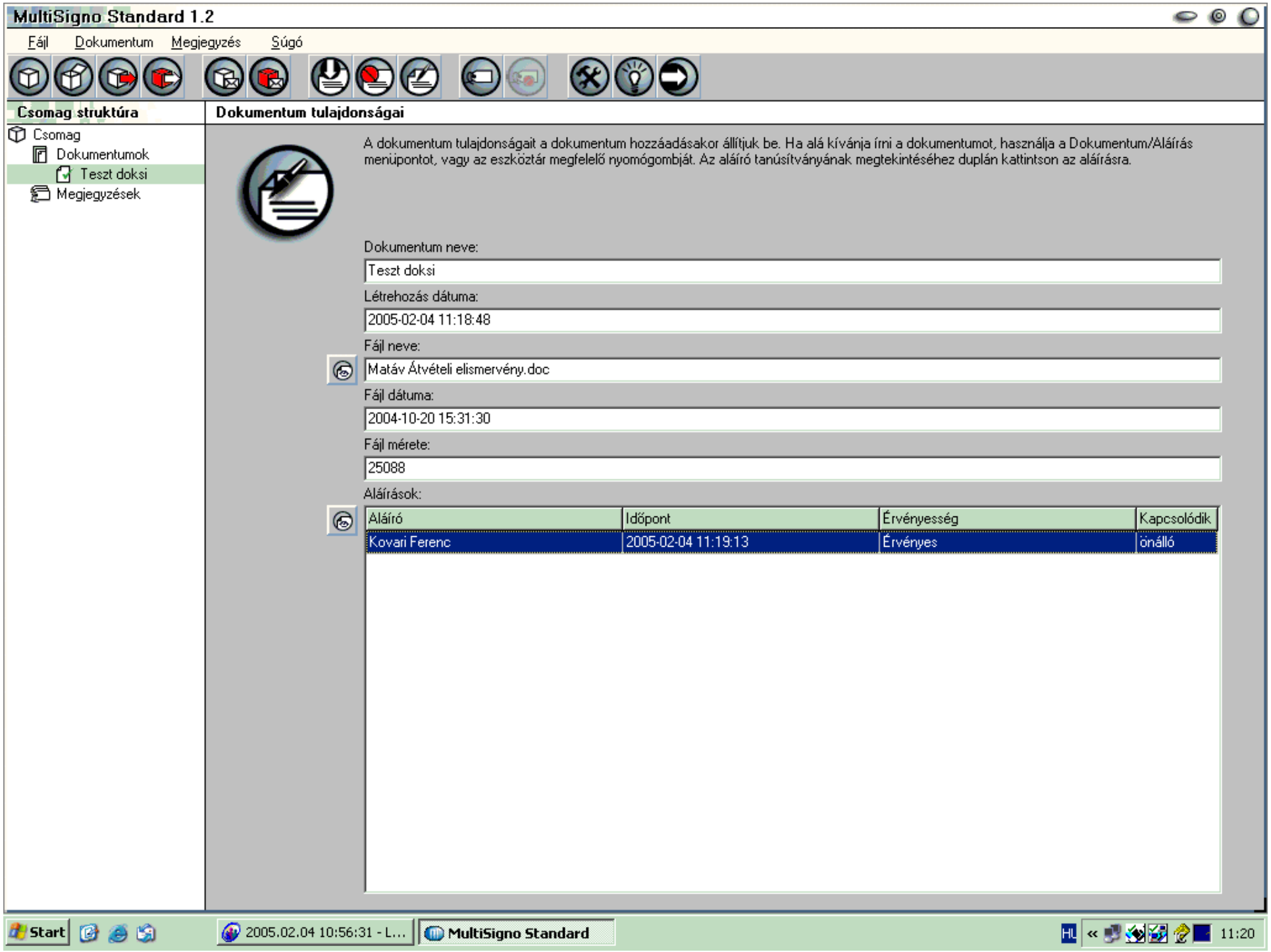
Aláíró	Időpont	Érvényesség	Kapcsolódik

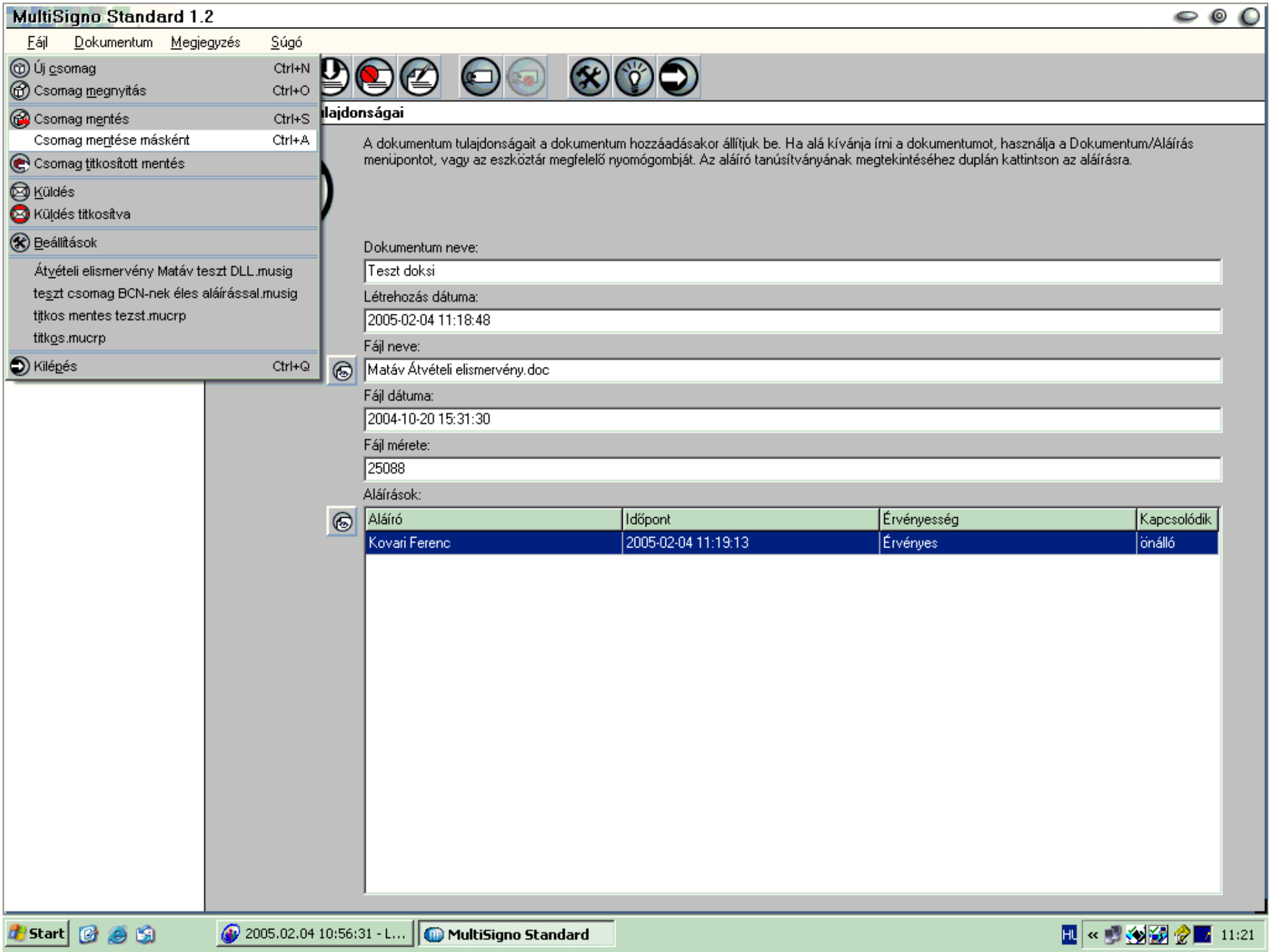
Start 2005.02.04 10:56:31 - L... MultiSigno Standard HU « 11:14

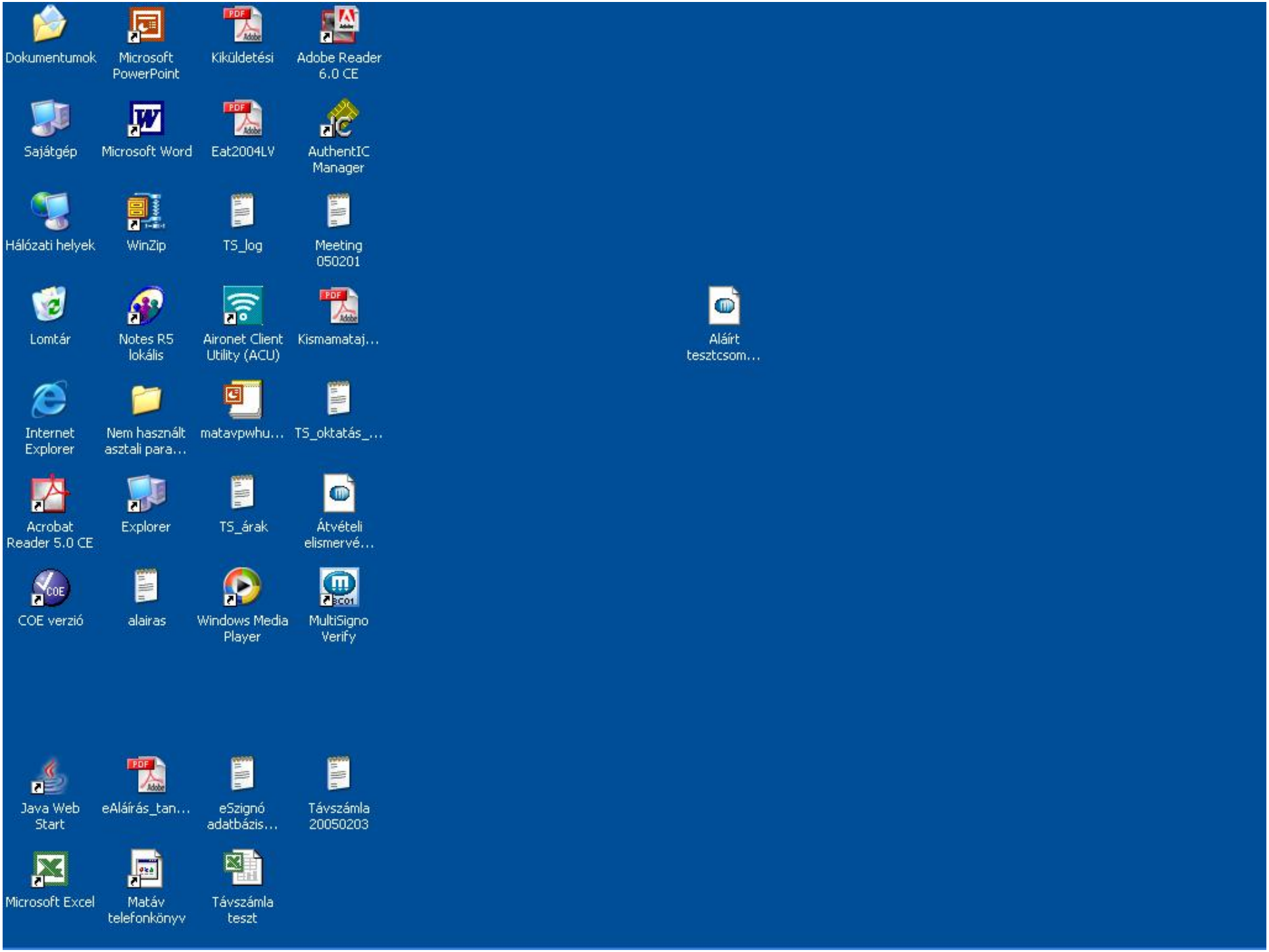

MultiSigno Standard 1.2
Fájl
Dokumentum
Megjegyzés
Súgó
Csomag struktúra
Csomag
Dokumentumok
Teszt doksi
Megjegyzések
Dokumentum tulajdonságai
A dokumentum tulajdonságait a dokumentum hozzáadásakor állítjuk be. Ha alá kívánja írni a dokumentumot, használja a Dokumentum/Aláírás menüpontot, vagy az eszköztár megfelelő nyomógombját. Az aláíró tanúsítványának megtekintéséhez duplán kattintson az aláírásra.
Dokumentum neve:
Teszt doksi
Létrehozás dátuma:
2005-02-04 11:14:13
Fájl neve:
Matáv Átvételi elismervény.doc
Fájl dátuma:
2004-10-20 15:31:30
Fájl mérete:
25088
Aláírások:
Aláíró
Időpont
Érvényesség
Kapcsolódik
Confirm
Biztosan alá kívánja írni a kijelölt dokumentumot?
(Az aláírni kívánt dokumentum azonosítója: "Teszt doksi")
Yes
No
Start
2005.02.04 10:56:31 - L...
MultiSigno Standard
HU
11:15

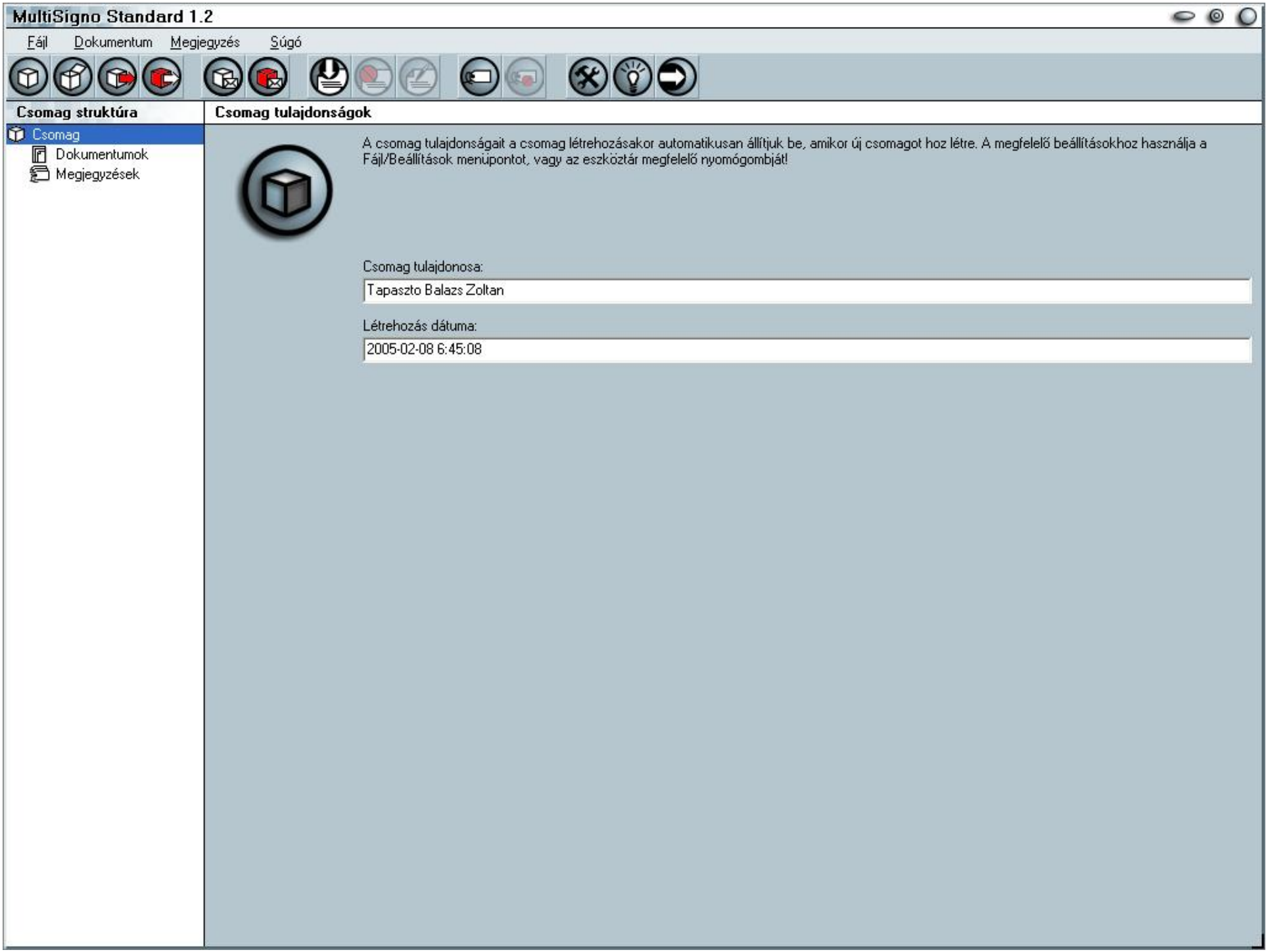

MultiSigno Standard 1.2
Fájl
Dokumentum
Megjegyzés
Súgó
Csomag struktúra
Csomag
Dokumentumok
Teszt doksi
Megjegyzések
Dokumentum tulajdonságai
A dokumentum tulajdonságait a dokumentum hozzáadásakor állítjuk be. Ha alá kívánja írni a dokumentumot, használja a Dokumentum/Aláírás menüpontot, vagy az eszköztár megfelelő nyomógombját. Az aláíró tanúsítványának megtekintéséhez duplán kattintson az aláírásra.
Dokumentum neve:
Teszt doksi
Létrehozás dátuma:
2005-02-04 11:16:25
Fájl neve:
Matáv Átvételi elismervény.doc
Fájl dátuma:
2004-10-20 15:31:3
Fájl mérete:
25088
Aláírások:
Aláíró
Érvényesség
Kapcsolódik
Checking Pin
Enter Your Pin
Number of tries left: 3
OK
Cancel
Start
2005.02.04 10:56:31 - L...
MultiSigno Standard
Checking Pin
HU
11:16

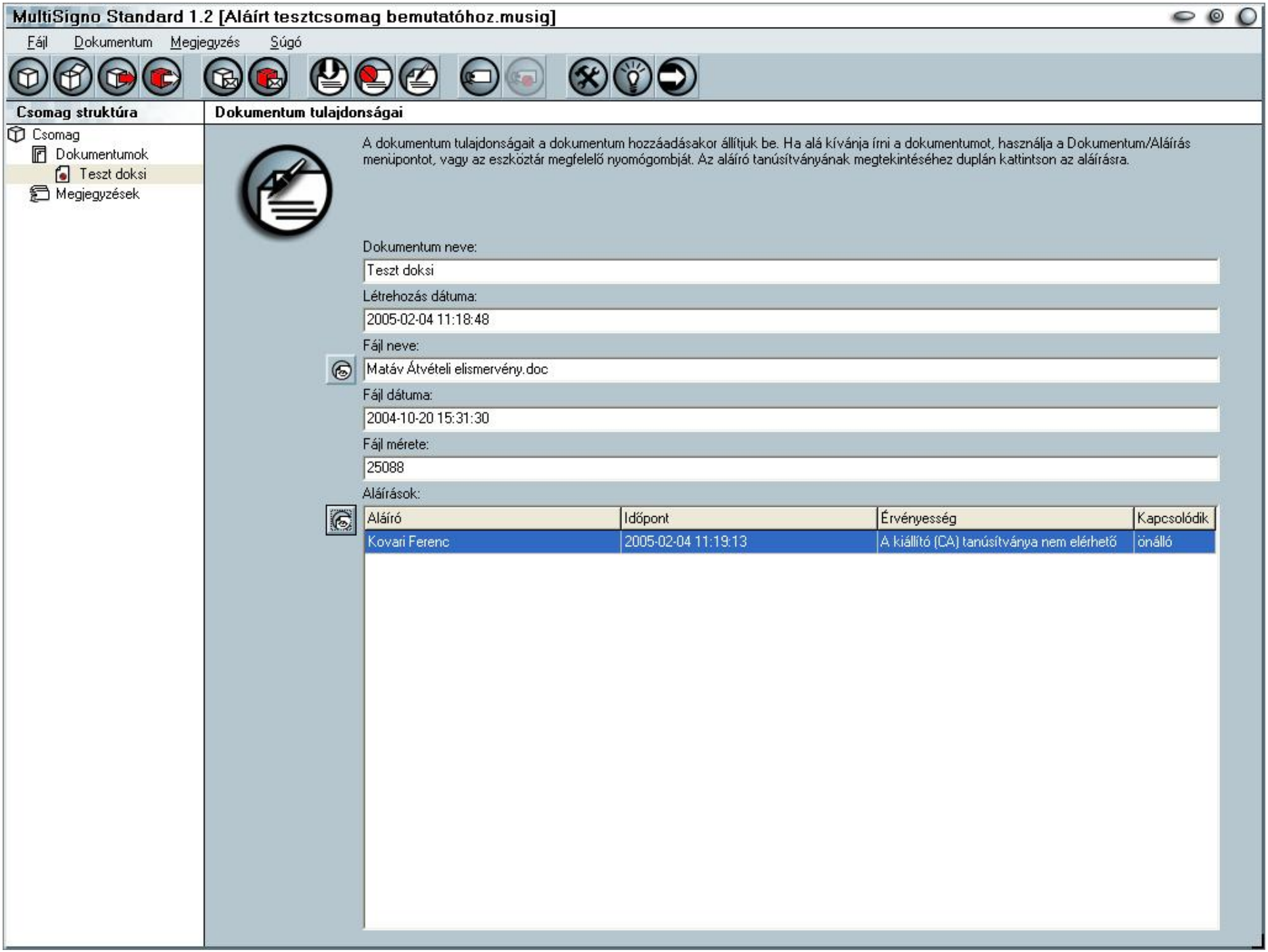

MultiSigno Standard 1.2
Fájl
Dokumentum
Megjegyzés
Súgó
Csomag struktúra
Csomag
Dokumentumok
Teszt doksi
Megjegyzések
Dokumentum tulajdonságai
A dokumentum tulajdonságait a dokumentum hozzáadásakor állítjuk be. Ha alá kívánja írni a dokumentumot, használja a Dokumentum/Aláírás menüpontot, vagy az eszköztár megfelelő nyomógombját. Az aláíró tanúsítványának megtekintéséhez duplán kattintson az aláírásra.
Dokumentum neve:
Teszt doksi
Létrehozás dátuma:
2005-02-04 11:18:48
Fájl neve:
Matáv Átvételi elismervény.doc
Fájl dátuma:
2004-10-20 15:31:3
Fájl mérete:
25088
Aláírások:
Aláíró
Érvényesség
Kapcsolódik
Information
Visszavonási lista (CRL) letöltés:
A letöltés és a telepítés sikeres volt
OK
Start
2005.02.04 10:56:31 - L...
MultiSigno Standard
HU
11:19

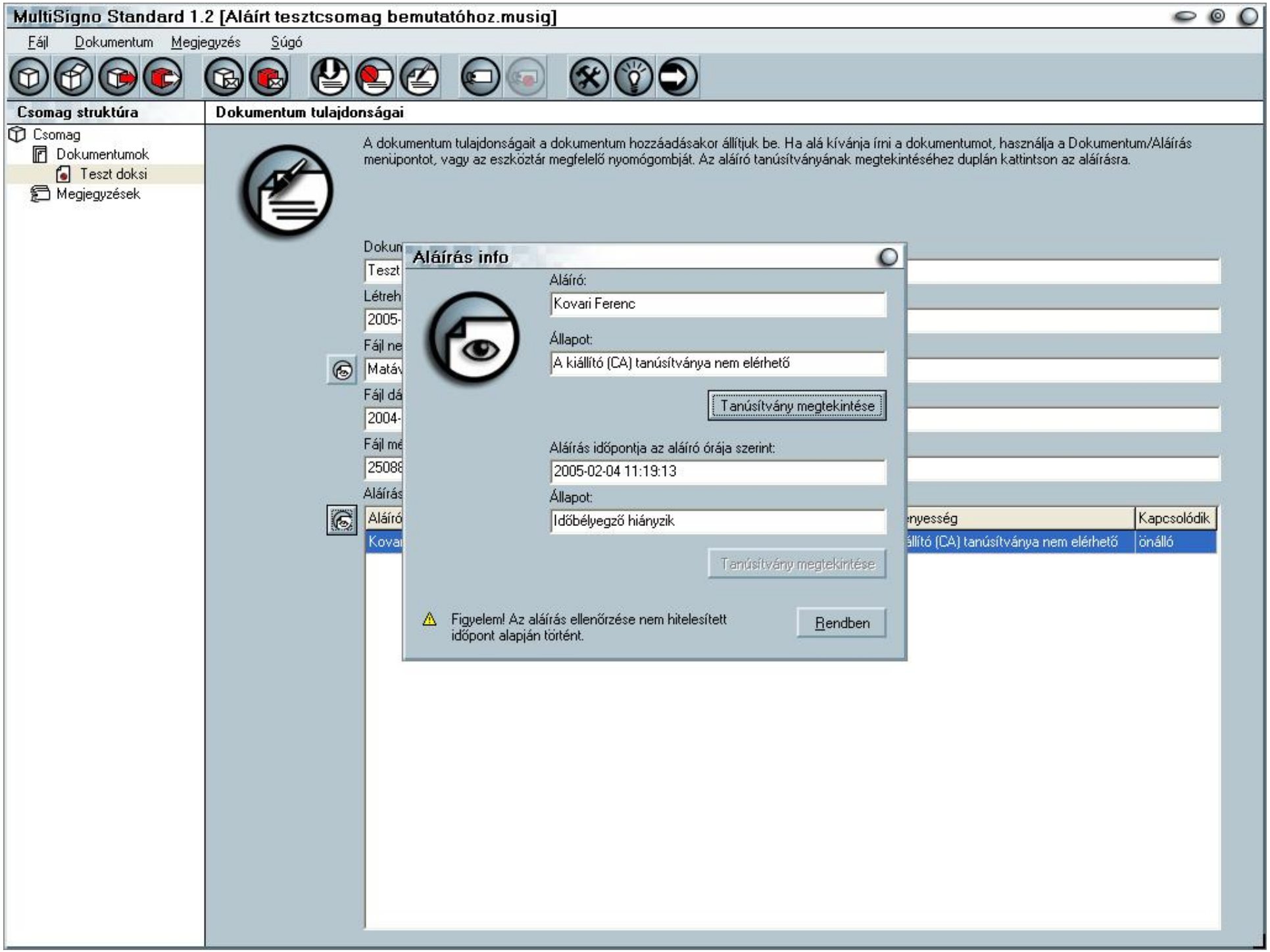

MultiSigno Standard 1.2
Fájl
Dokumentum
Megjegyzés
Súgó
Csomag struktúra
Csomag
Dokumentumok
Teszt doksi
Megjegyzések
Dokumentum tulajdonságai
A dokumentum tulajdonságait a dokumentum hozzáadásakor állítjuk be. Ha alá kívánja írni a dokumentumot, használja a Dokumentum/Aláírás menüpontot, vagy az eszköztár megfelelő nyomógombját. Az aláíró tanúsítványának megtekintéséhez duplán kattintson az aláírásra.
Dokumentum neve:
Teszt doksi
Létrehozás dátuma:
2005-02-04 11:18:48
Fájl neve:
Matáv Átvételi elismervény.doc
Fájl dátuma:
2004-10-20 15:31:30
Fájl mérete:
25088
Aláírások:
Aláíró
Időpont
Érvényesség
Kapcsolódik
Kovari Ferenc
2005-02-04 11:19:13
Érvényes
önálló
Start
2005.02.04 10:56:31 - L...
MultiSigno Standard
HU
11:20


MultiSigno Standard 1.2
Fájl
Dokumentum
Megjegyzés
Súgó
Új csomag Ctrl+N
Csomag megnyitás Ctrl+O
Csomag mentés Ctrl+S
Csomag mentése másként Ctrl+A
Csomag titkosított mentés
Küldés
Küldés titkosítva
Beállítások
Átvételi elismervény Matáv teszt DLL.musig
teszt csomag BCN-nek éles aláírással.musig
titkos mentes tezst.mucrp
titkos.mucrp
Kilépés Ctrl+Q
lajdonságai
A dokumentum tulajdonságait a dokumentum hozzáadásakor állítjuk be. Ha alá kívánja írni a dokumentumot, használja a Dokumentum/Aláírás menüpontot, vagy az eszköztár megfelelő nyomógombját. Az aláíró tanúsítványának megtekintéséhez duplán kattintson az aláírásra.
Dokumentum neve:
Teszt doksi
Létrehozás dátuma:
2005-02-04 11:18:48
Fájl neve:
Matáv Átvételi elismervény.doc
Fájl dátuma:
2004-10-20 15:31:30
Fájl mérete:
25088
Aláírások:
Aláíró
Időpont
Érvényesség
Kapcsolódik
Kovari Ferenc
2005-02-04 11:19:13
Érvényes
önálló
Start
2005.02.04 10:56:31 - L...
MultiSigno Standard
HU
11:21


Dokumentumok
Microsoft PowerPoint
Kiküldetési
Adobe Reader 6.0 CE
Sajátgép
Microsoft Word
Eat2004LV
AuthentIC Manager
Hálózati helyek
WinZip
TS_log
Meeting 050201
Lomtár
Notes R5 lokális
Aironet Client Utility (ACU)
Kismamataj...
Aláírt tesztcsom...
Internet Explorer
Nem használt asztali para...
matavpwhu...
TS_oktatás_...
Acrobat Reader 5.0 CE
Explorer
TS_árak
Átvételi elismervé...
COE verzió
alairas
Windows Media Player
MultiSigno Verify
Java Web Start
eAláírás_tan...
eSzignó adatbázis...
Távszámla 20050203
Microsoft Excel
Matáv telefonkönyv
Távszámla teszt


MultiSigno Standard 1.2
Fájl
Dokumentum
Megjegyzés
Súgó
Csomag struktúra
Csomag
Dokumentumok
Megjegyzések
Csomag tulajdonságok
A csomag tulajdonságait a csomag létrehozásakor automatikusan állítjuk be, amikor új csomagot hoz létre. A megfelelő beállításokhoz használja a Fájl/Beállítások menüpontot, vagy az eszköztár megfelelő nyomógombját!
Csomag tulajdonosa:
Tapaszto Balazs Zoltan
Létrehozás dátuma:
2005-02-08 6:45:08


MultiSigno Standard 1.2 [Aláírt tesztcsomag bemutatóhoz.musig]
Fájl
Dokumentum
Megjegyzés
Súgó
Csomag struktúra
Csomag
Dokumentumok
Teszt doksi
Megjegyzések
Dokumentum tulajdonságai
A dokumentum tulajdonságait a dokumentum hozzáadásakor állítjuk be. Ha alá kívánja írni a dokumentumot, használja a Dokumentum/Aláírás menüpontot, vagy az eszköztár megfelelő nyomógombját. Az aláíró tanúsítványának megtekintéséhez duplán kattintson az aláírásra.
Dokumentum neve:
Teszt doksi
Létrehozás dátuma:
2005-02-04 11:18:48
Fájl neve:
Matáv Átvételi elismervény.doc
Fájl dátuma:
2004-10-20 15:31:30
Fájl mérete:
25088
Aláírások:
Aláíró
Időpont
Érvényesség
Kapcsolódik
Kovari Ferenc
2005-02-04 11:19:13
A kiállító (CA) tanúsítványa nem elérhető
önálló


MultiSigno Standard 1.2 [Aláírt tesztcsomag bemutatóhoz.musig]
Fájl
Dokumentum
Megjegyzés
Súgó
Csomag struktúra
Csomag
Dokumentumok
Teszt doksi
Megjegyzések
Dokumentum tulajdonságai
A dokumentum tulajdonságait a dokumentum hozzáadásakor állítjuk be. Ha alá kívánja írni a dokumentumot, használja a Dokumentum/Aláírás menüpontot, vagy az eszköztár megfelelő nyomógombját. Az aláíró tanúsítványának megtekintéséhez duplán kattintson az aláírásra.
Aláírás info
Aláíró:
Kovari Ferenc
Állapot:
A kiállító (CA) tanúsítványa nem elérhető
Tanúsítvány megtekintése
Aláírás időpontja az aláíró órája szerint:
2005-02-04 11:19:13
Állapot:
Időbélyegző hiányzik
Tanúsítvány megtekintése
Figyelem! Az aláírás ellenőrzése nem hitelesített időpont alapján történt.
Rendben
Kapcsolódik
önálló

Elektronikus aláírás igénylése

- *Hitelesítés szolgáltató adja ki a tanúsítványt*
- *Hitelesítés szolgáltató azonosítja az igénylőt*
  - *Személyes regisztráció*
  - *Adatok ellenőrzése (cégadatbázis)*
  - *Kártyaperszonalizáció (chip kártya esetén)*
  - *Fokozott tanúsítványt postán vagy letölthető formában, míg a minősített tanúsítványt személyesen átadja az igénylőnek*
- *Lehetőség van a tanúsítványok felfüggesztésére ill. visszavonására*
- *Visszavonási lista (CRL) és tanúsítványtár publikálása*

matáv
a szavakon túl

Gyakorlati felhasználási lehetőségek

- *A jogszabály meghatározza a felhasználási kört*
- *Fokozott tanúsítványok szinte minden tranzakcióhoz használhatóak, azonban van néhány kivétel*
- *Minősített aláírás magán nyugdíjpénztári bevallások esetében használható 2005. január 1-től!*
- *Az ehhez szükséges szoftvert a PSZÁF biztosítja*
- *Elektronikus számla: fokozott aláírás és időbélyegzés szükséges*

matáv
a szavakon túl

Köszönöm a figyelmet!

Tapasztó Balázs
Tel: 457-41-37
E-mail: tapaszto.balazs@ln.matav.hu

matáv
a szavakon túl