


# Elektronikus archiválórendszer fejlesztése PKI alapokon



Készítette: Kollár Balázs  
2005. február 11.

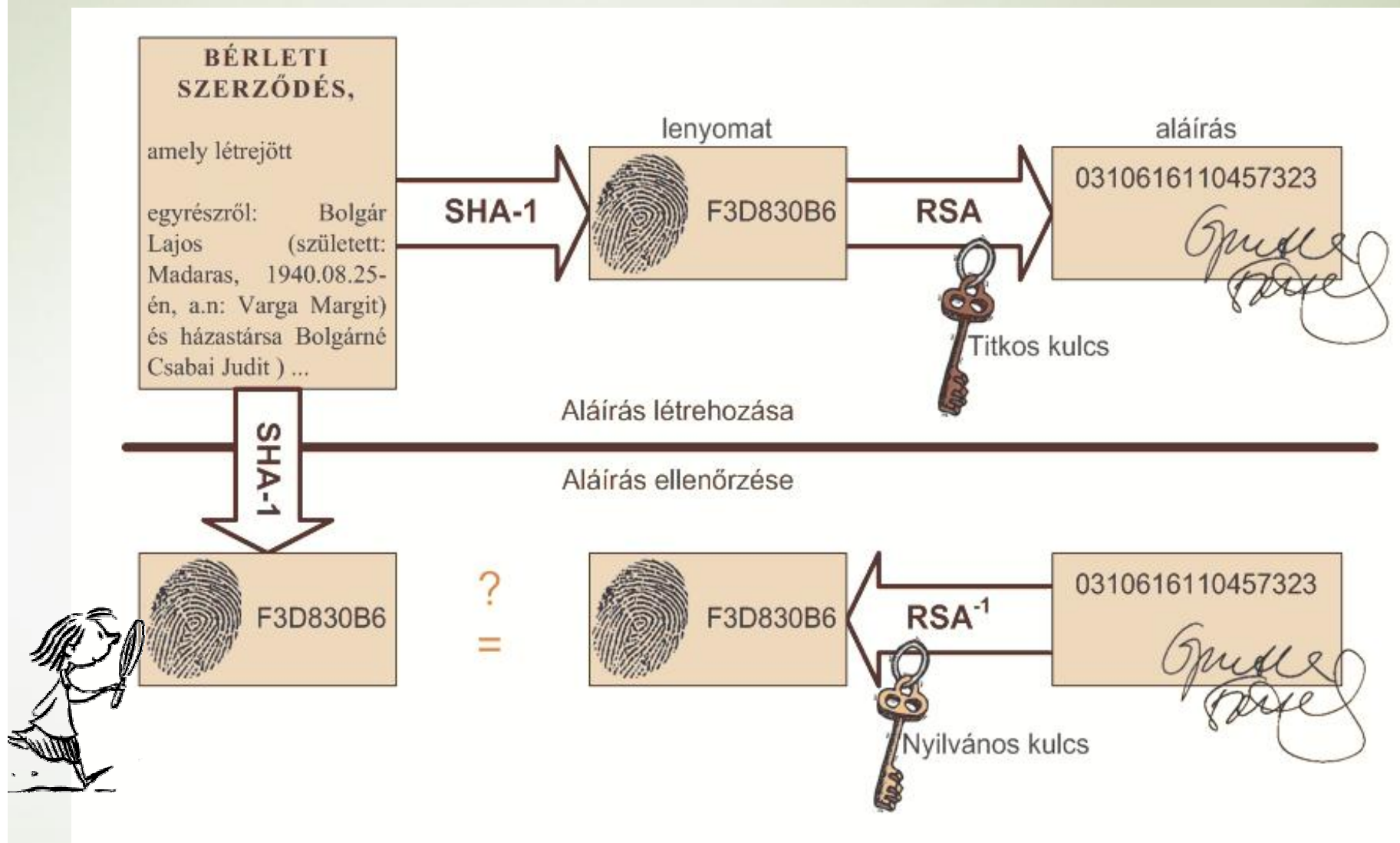
# Tartalom



# Mottó

- Közigazgatási Eljárásról szóló Törvény  
160§ (2) Ha az ügyfél [...] elektronikus aláírással rendelkezik, a kérelem az ügyfél elektronikus aláírásával ellátva [...] benyújtható.
- Hatályos: 2005. november 1-től.

# Elektronikus aláírás folyamata - 1977



# Szolgáltatás =

- Matematika



+ Jog

+ Szabványok

+ Megvalósítás



# Jogi szabályozás - 2001

- Európai Unió direktíva
- 2001. évi XXXV. törvény
  - Hitelesítés szolgáltatók
  - Időbélyegzés szolgáltatók
- 2004. évi LV. Törvény
  - [Archiválás szolgáltatók](#)



# Archiválni kell, mert...

- A számítógépes adat illékony, ellenben egy elektronikus számlát is hét évig kell őrizni.
- Hosszú távon megszűnhetnek hitelesítés szolgáltatók, dokumentum formátumok, nehéz lehet évekkel később beszerezni a visszavonási listákat.
- Nem lehet majd ellenőrizni egy aláírás érvényességét.

# Szolgáltatás =

• Matematika



+ Jog



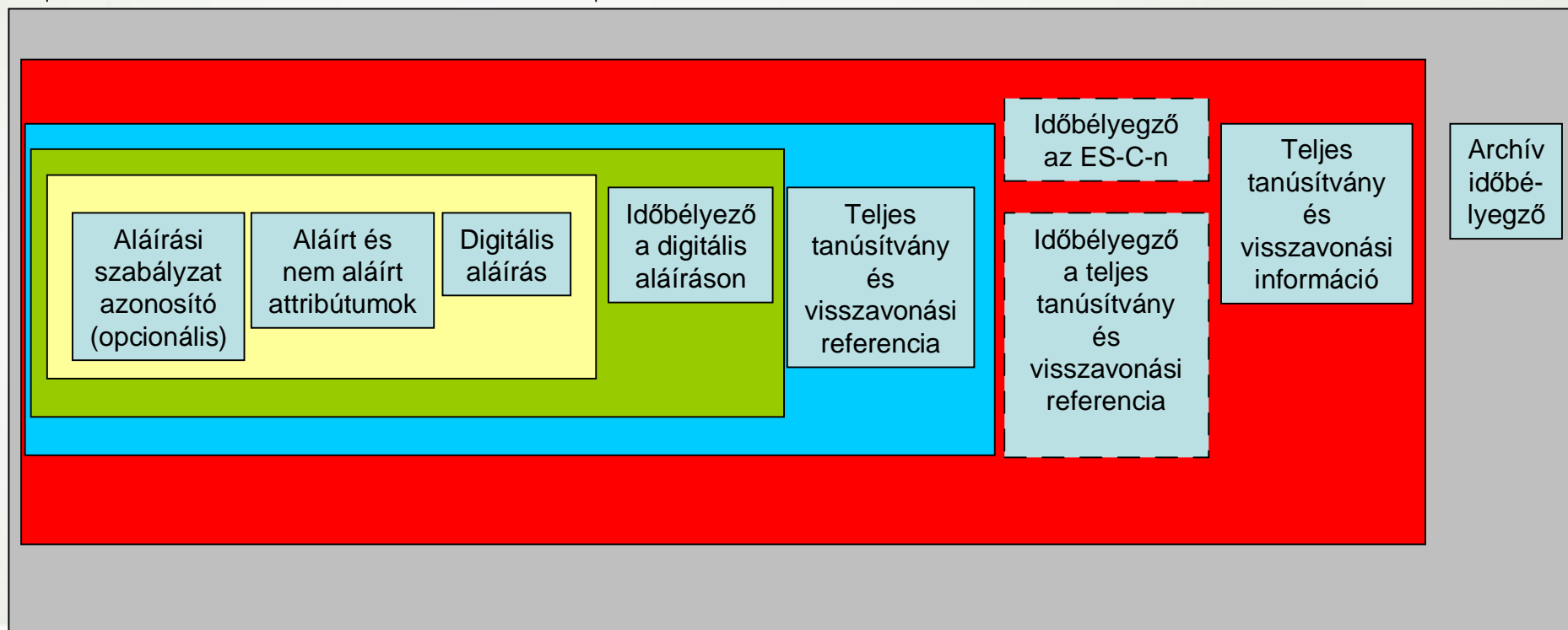
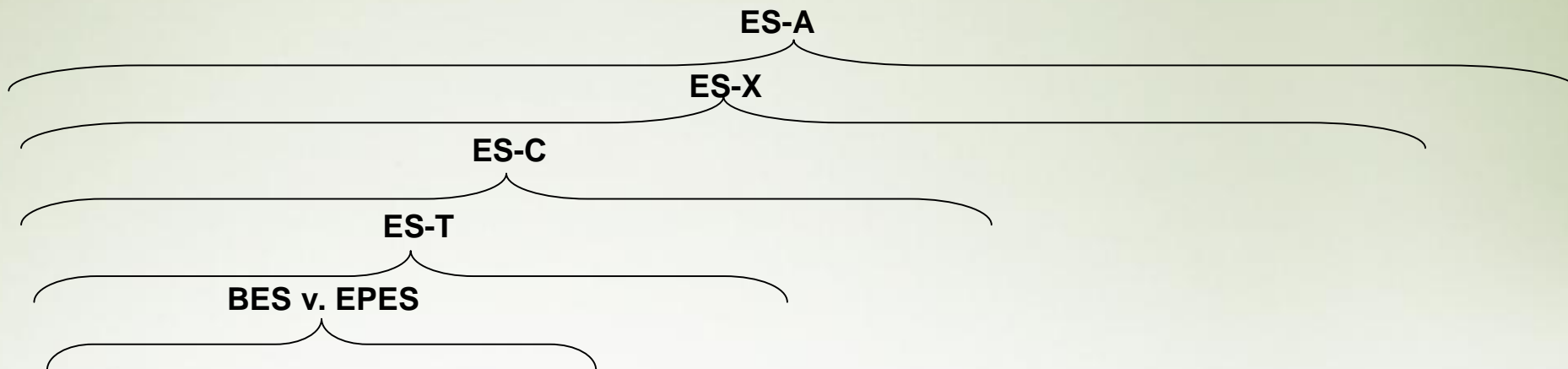
+ Szabványok

+ Megvalósítás

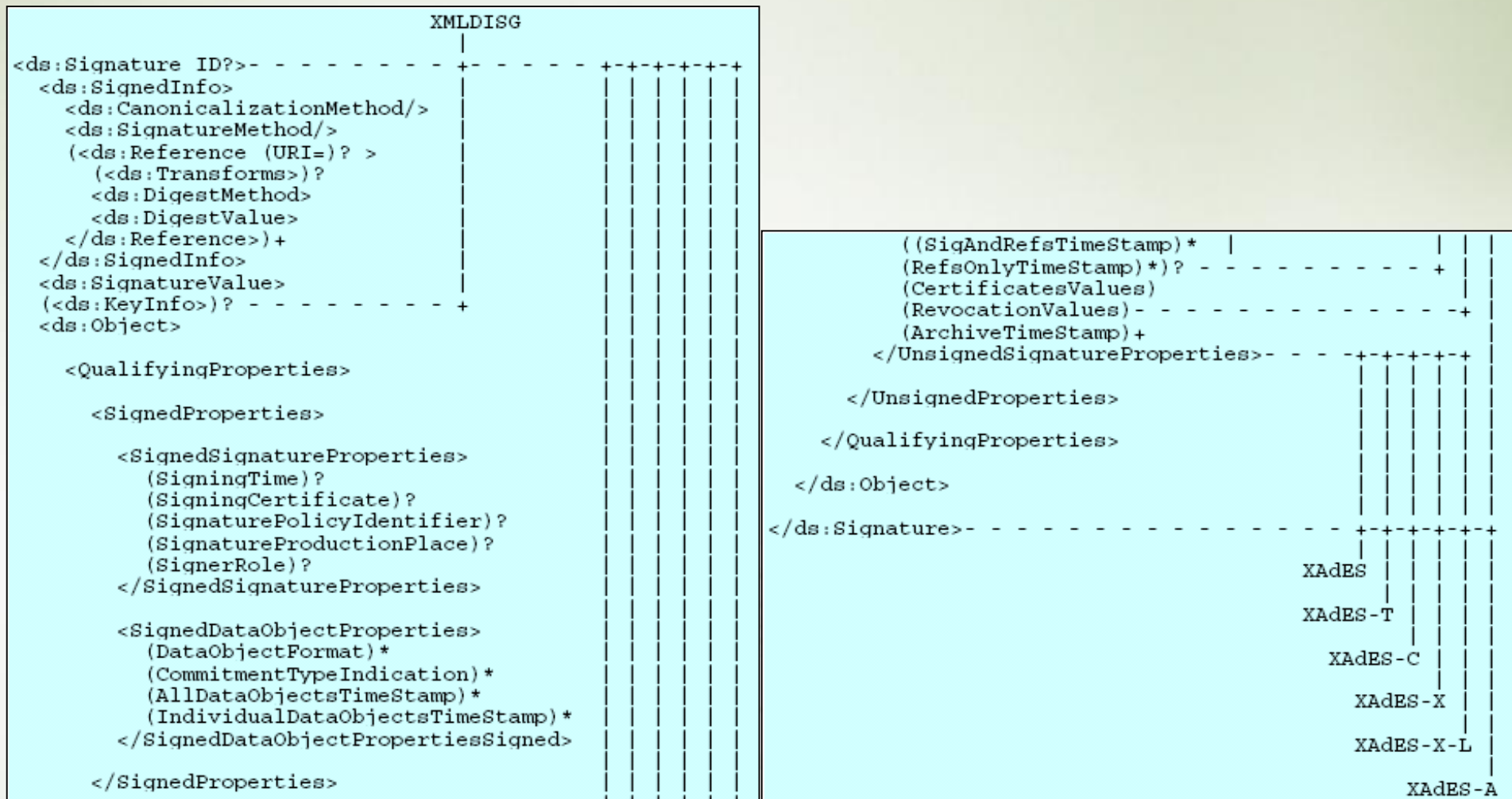




# Egymásra épülő európai szabványok

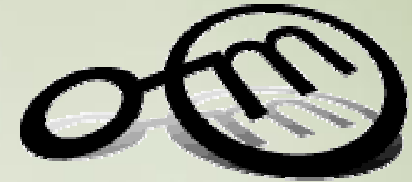


# XAdES hierarchia



# MELASZ ajánlás

- A közös alap a XAdES-ra épülve.
- A hazai fejlesztésű alkalmazások együttműködő képességét szavatolja.
- ✓ Folynak az együttműködési tesztek.
- Megfelel a törvényeinknek és a közigazgatásunk igényeinek.



MELASZ

M a g y a r

E l e k t r o n i k u s

A l á í r á s

S z ö v e t s é g

# Felhasználás

- Általános digitális dossziéként.
- Elektronikus számlák megőrzésére.  
[www.tavszamla.hu](http://www.tavszamla.hu)
- Elektronikus államigazgatásban.  
[www.magyarorszag.hu](http://www.magyarorszag.hu)
- Közigazgatási Eljárásról szóló Törvény (KET)  
2005. november 1-től.

# Szolgáltatás =

• Matematika ✓

+ Jog ✓

+ Szabványok ✓

+ Megvalósítás



# A fejlesztésről

- Hat hónap irodalom tanulmányozás.
- Nyolc hónap fejlesztés.
- 123 kilobájt kód.
- Nyílt technológiákra épül: J2SE, Servlet, JSP, Apache XML Suite
- A piaci szoftverek zöme (MS) operációs rendszer függő, vegyesen kliens és szerver oldali.
- SQL adatbázisra épülő rendszer.

# Állomány feltöltése

Feltöltés - Opera

File Edit View Bookmarks Tools Help

[Feltöltés](#) [Állományok](#) [Tanúsítványok](#) [Visszavonási listák](#) [Karbantartás](#) **Bejelentkezett felhasználó: nypee** [Kijelentkezés](#)

Név	Státusz	Feltöltés ideje	Leírás
signature.xml	10	2005-11-10 15:23:48.893	

Név:  Choose

Típus:

Leírás:

Feltölt

Státuszok:

- 10 - Fogadott, nem ellenőrzött
- 20 - Sikeresen fogadott állomány
- 30 - Hosszú távú MELASZ állomány
- 40 - Archiv MELASZ állomány



# Alapállapot feltöltés után

Állományok - Opera

File Edit View Bookmarks Tools Help

[Feltöltés](#) [Állományok](#) [Tanúsítványok](#) [Visszavonási listák](#) [Karbantartás](#) **Bejelentkezett felhasználó: nypee**  
[Kijelentkezés](#)

---

Név	Státusz				
signature.xml 10	<a href="#">Állomány fogadása</a>	Állomány kezdeti ellenőrzése	Állomány utólagos ellenőrzése	Állomány archiválása	<a href="#">Eltávolítás</a>

---

Státuszok:

- 10 - Fogadott, nem ellenőrzött
- 20 - Sikeresen fogadott állomány
- 30 - Hosszú távú MELASZ állomány
- 40 - Archiv MELASZ állomány



# Állomány fogadása

Állományok - Opera

File Edit View Bookmarks Tools Help

[Feltöltés](#) **(Állományok)** [Tanúsítványok](#) [Visszavonási listák](#) [Karbantartás](#) **Bejelentkezett felhasználó: nypee** [Kijelentkezés](#)

Név	Státusz				
signature.xml	20	<b>Állomány fogadása</b>	<a href="#">Állomány kezdeti ellenőrzése</a>	Állomány utólagos ellenőrzése	Állomány archiválása <a href="#">Eltávolítás</a>

- SignedInfo elem megvan.
- SignatureValue elem megvan.
- KeyInfo elem megvan.
- SigningTime elem megvan.
- SigningCertificate elem megvan.
- SignaturePolicyIdentifier elem megvan!
- DataObjectFormat elem megvan.
- CompleteCertificateRefs elem megvan.
- SignatureTimeStamp megvan.
- RevocationRef EMAILADDRESS=ica@mavinformatika.hu, OID.2.5.4.17=1012, STREET=Krisztina krt. 37/A, CN=Trust&Sign Test CA v1.0, OU=PKI Services BU, O=MAV INFORMATIKA Kft., L=Budapest, C=HU kiállítóhoz hozzáadva.
- CertValue elemek megvannak.
- Kriptográfiai ellenőrzés érvényes.
- **Sikeres fogadás!**

# Állomány kezdeti ellenőrzése

The screenshot shows a web browser window with the title 'Állományok - Opera'. The menu bar includes 'File', 'Edit', 'View', 'Bookmarks', 'Tools', and 'Help'. The main content area has a navigation bar with links: 'Feltöltés', 'Állományok' (circled in red), 'Tanúsítványok', 'Visszavonási listák', 'Karbantartás', and 'Bejelentkezett felhasználó: nypee' with a 'Kijelentkezés' link below it.

Név	Státusz				
signature.xml	30	Állomány fogadása	Állomány kezdeti ellenőrzése (circled in red)	Állomány utólagos ellenőrzése	Állomány archiválása
<a href="#">Eltávolítás</a>					

• Visszavonási lista EMAILADDRESS=ica@mavinformatika.hu, OID.2.5.4.17=1012, STREET=Krisztina krt. 37/A, CN=Trust&Sign Test CA v1.0, OU=PKI Services BU, O=MAV INFORMATIKA Kft., L=Budapest, C=HU kiállítóhoz hozzáadva.

• Állomány érvényes.

• **Sikeres kezdeti ellenőrzés!**

Státuszok:

- 10 - Fogadott, nem ellenőrzött
- 20 - Sikeresen fogadott állomány
- 30 - Hosszú távú MELASZ állomány
- 40 - Archiv MELASZ állomány

# Állomány utólagos ellenőrzése

Állományok - Opera

File Edit View Bookmarks Tools Help

[Feltöltés](#) ([Állományok](#)) [Tanúsítványok](#) [Visszavonási listák](#) [Karbantartás](#) **Bejelentkezett felhasználó: nypee** [Kijelentkezés](#)

---

Név	Státusz				
signature.xml 30	Állomány fogadása	Állomány kezdeti ellenőrzése	<a href="#">Állomány utólagos ellenőrzése</a>	<a href="#">Állomány archiválása</a>	<a href="#">Eltávolítás</a>

- Állomány érvényes!

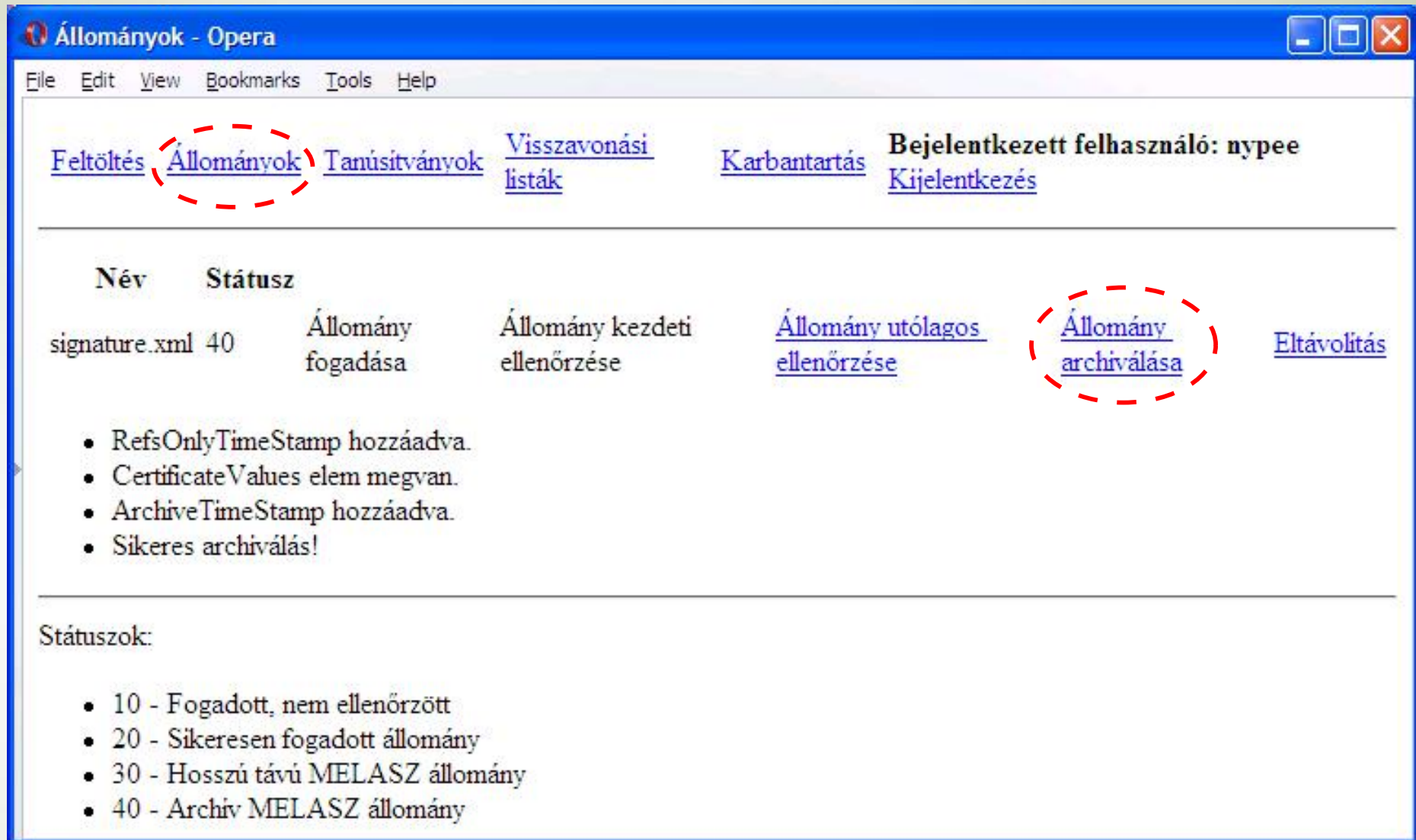
---

Státuszok:

- 10 - Fogadott, nem ellenőrzött
- 20 - Sikeresen fogadott állomány
- 30 - Hosszú távú MELASZ állomány
- 40 - Archiv MELASZ állomány



# Állomány archiválása



Állományok - Opera

File Edit View Bookmarks Tools Help

[Feltöltés](#) [Állományok](#) [Tanúsítványok](#) [Visszavonási listák](#) [Karbantartás](#) **Bejelentkezett felhasználó: nypee** [Kijelentkezés](#)

---

Név	Státusz				
signature.xml	40	Állomány fogadása	Állomány kezdeti ellenőrzése	<a href="#">Állomány utólagos ellenőrzése</a>	<a href="#">Állomány archiválása</a> <a href="#">Eltávolítás</a>

- RefsOnlyTimeStamp hozzáadva.
- CertificateValues elem megvan.
- ArchiveTimeStamp hozzáadva.
- Sikereres archiválás!

Státuszok:

- 10 - Fogadott, nem ellenőrzött
- 20 - Sikeresen fogadott állomány
- 30 - Hosszú távú MELASZ állomány
- 40 - Archiv MELASZ állomány

# Értékelés

- A szoftver minden lényeges funkciója működik.
- Szeretnék kiterjedt tesztelést végezni, ennek keretében összehangolni a többi hazai alkalmazással.
- Robosztusabb technológiai alapokra fogom helyezni a működést. (EJB 3.0)
- Kliensoldali kártya API-val fogom az alkalmazást bővíteni.

Köszönöm a megtisztelő figyelmet!

