Elektronikus archiválórendszer fejlesztése PKI alapokon

Készítette: Kollár Balázs

2005. február 11.

Tartalom

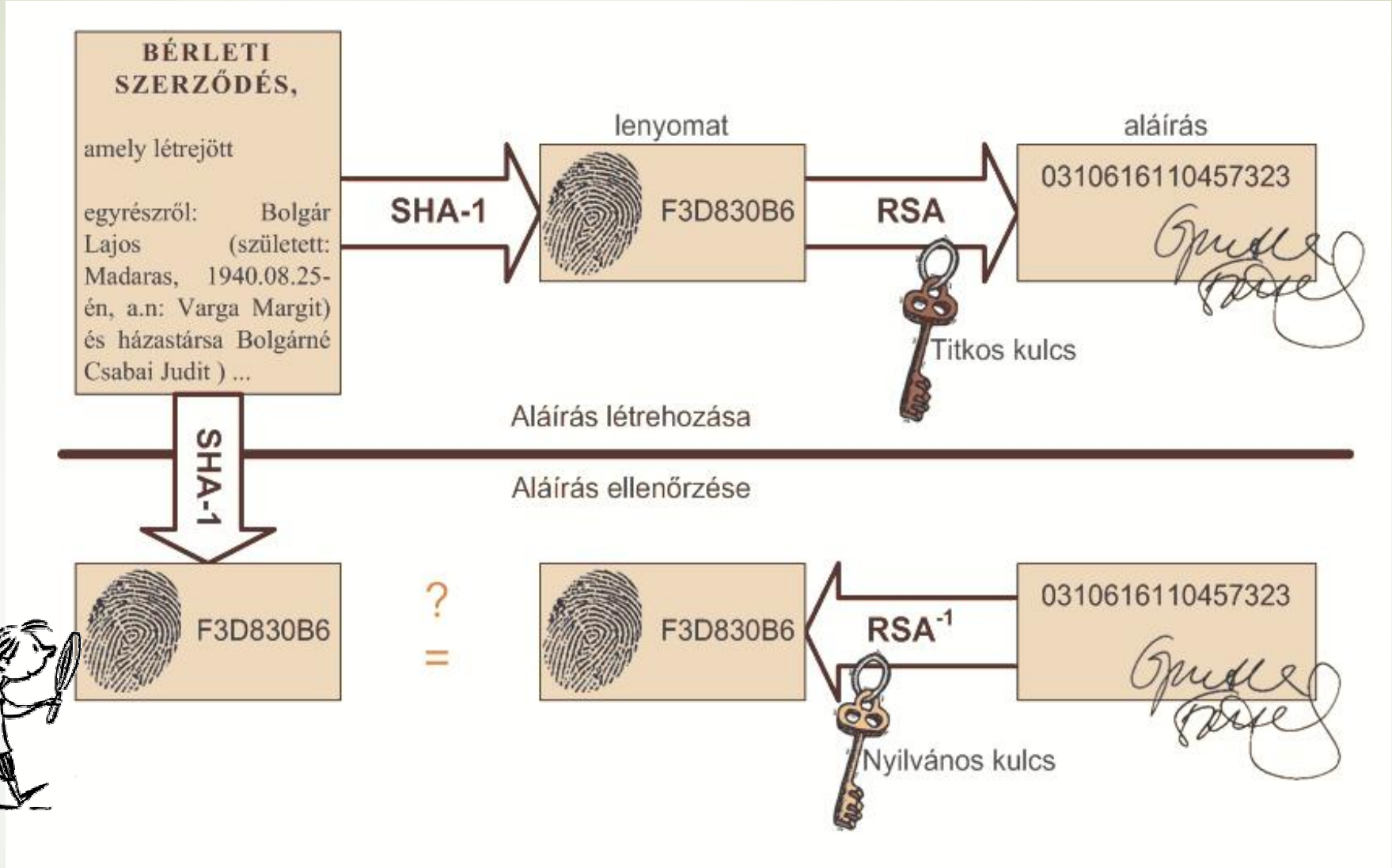

Kriptográfia
Jogi szabályozás
MELASZ ajánlás
Szolgáltatás és felasználók
Megvalósult alkalmazás

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 Uniós direktíva

- 2001. évi XXXV. törvény
  - Hitelesítés szolgáltatók
  - Időbélyegzés szolgáltatók
- 2004. évi LV. Törvény
  - Archiválás szolgáltatók

Archiválni kell, mert…

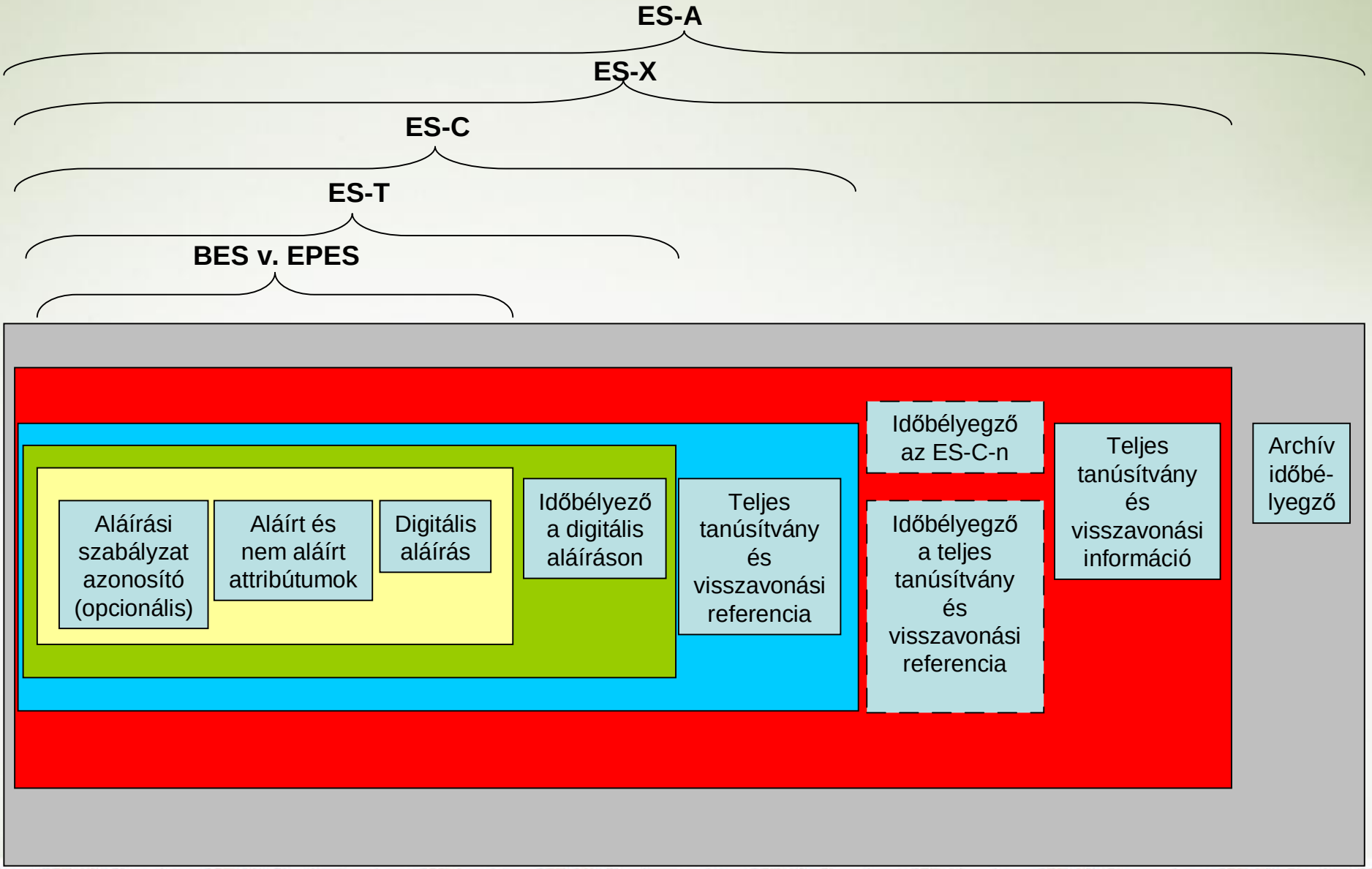
- A számítógépes adat illékony, ellenben egy elektronikus számlát is hét évig kell őrizni.
- Hosszú távon megszűnhetnek hitelesítés szolgáltatók, dokumentum formátumok, nehéz lehet évekkel később beszerezni a visszavonási listákat.

➢ Nem lehet majd ellenőrizni egy aláírás érvényességét.

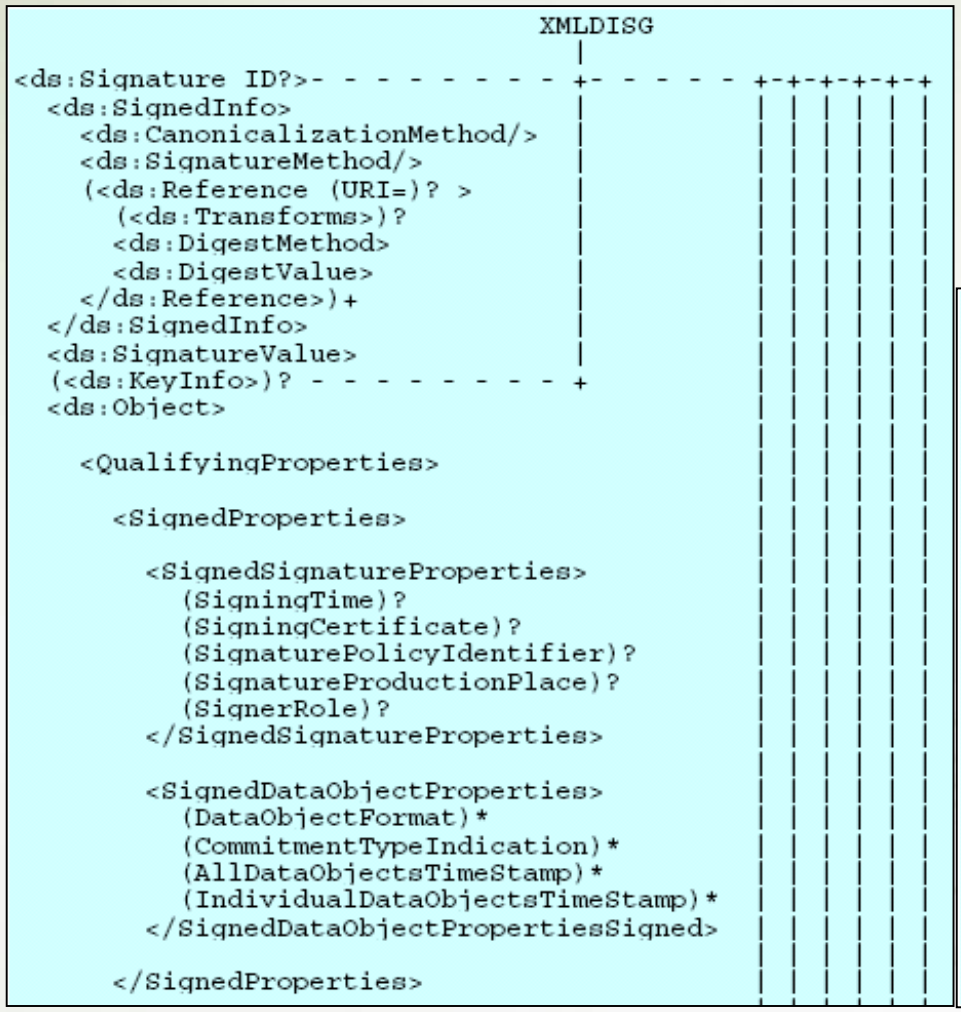
Szolgáltatás =

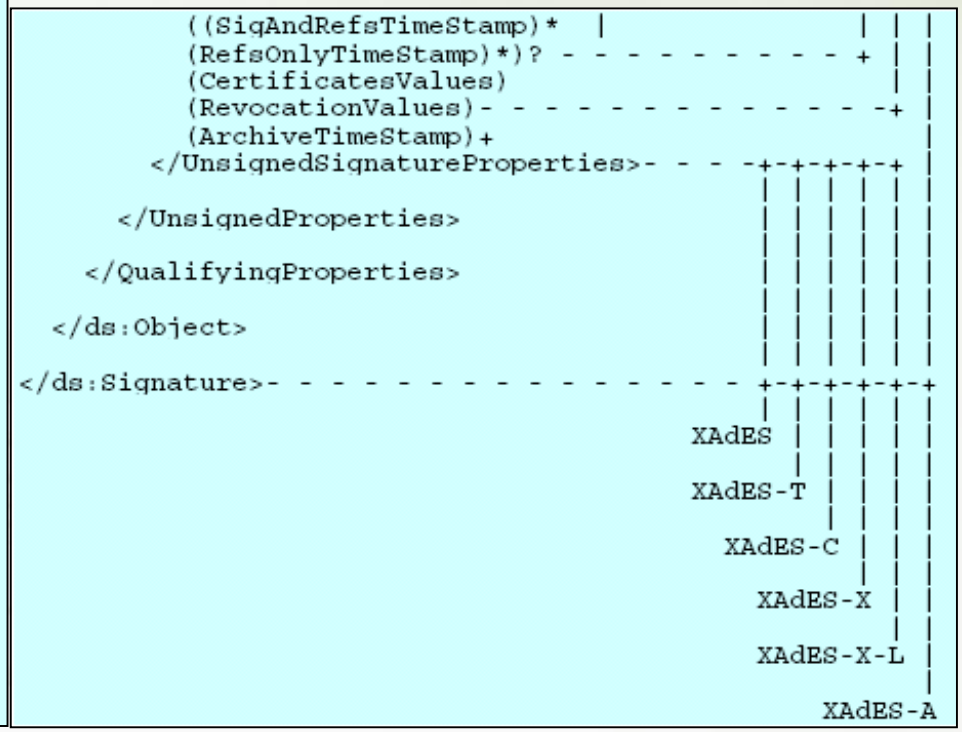
- Matematika 
+ Jog 
+ Szabványok
+ Megvalósítás

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 tövényeinknek és a közigazgatásunk igényeinek.

MELASZ

Magyar Elektronikus Aláírás Szövetség

Felhasználás

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

Szolgáltatás =

- Matematika 
+ Jog 
+ Szabványok 
+ Megvalósítás

A fejlesztésről

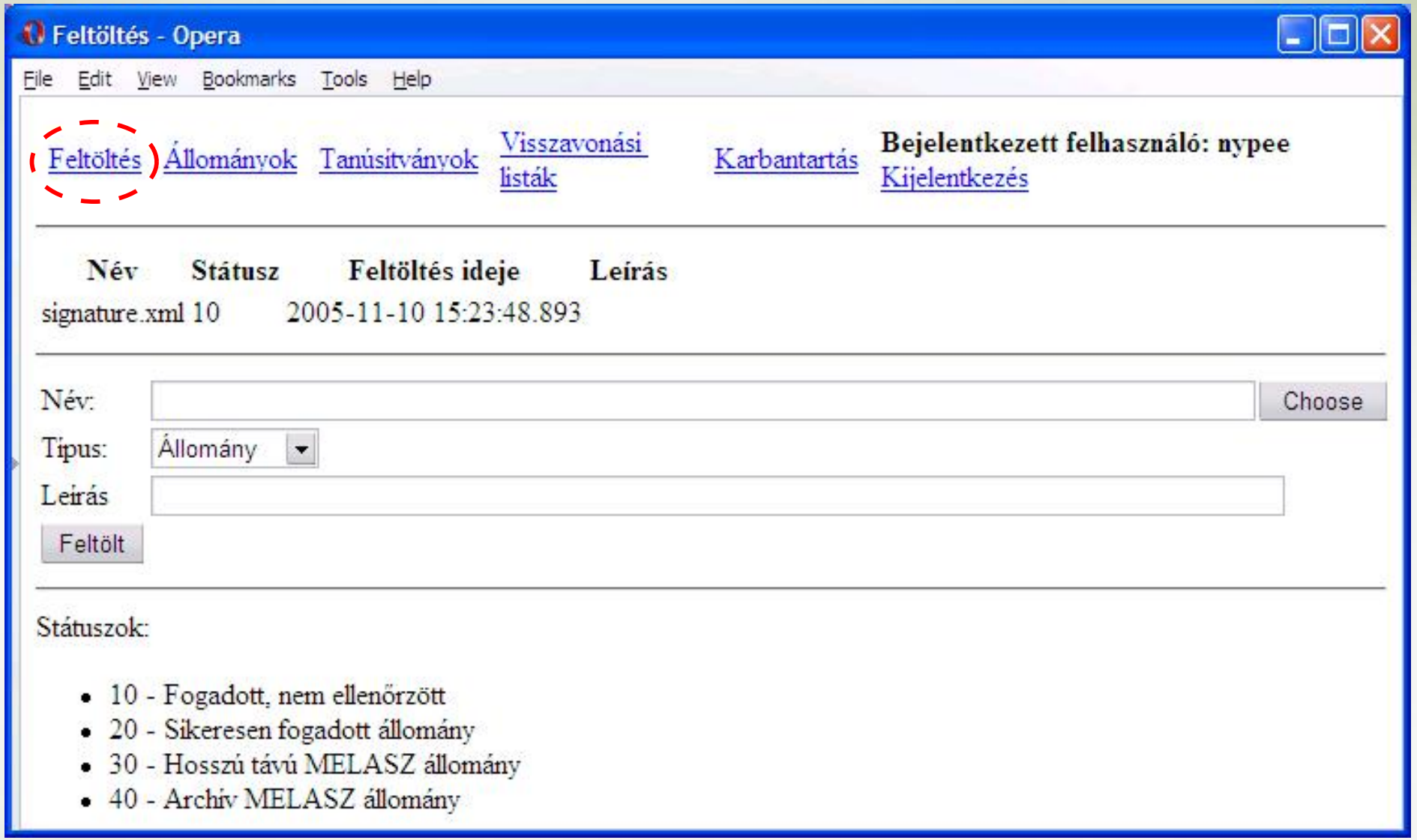
- Hat hónap irodalom tanulmányozás.
- Nyolc hónap fejlesztés.

- 123 kilobájt kód.

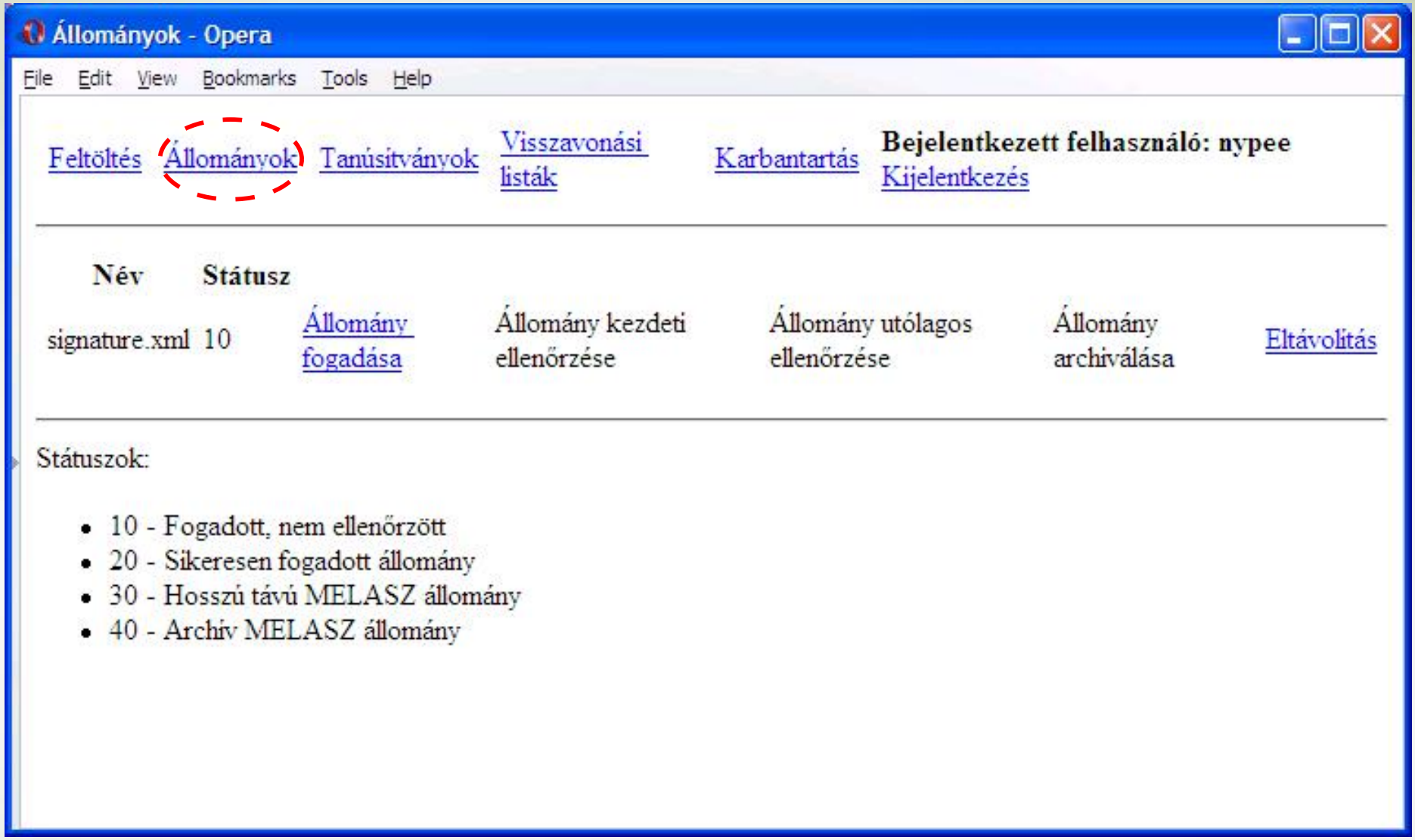
- Nyílt technológiákra épül: J2SE, Servlet, JSP, Apache XML Suite
- A piaci szoftverek zöme (MS) operációs rendszer függő, vegyesen kliens és szerver oldali.

- SQL adatbázisra épülő rendszer.

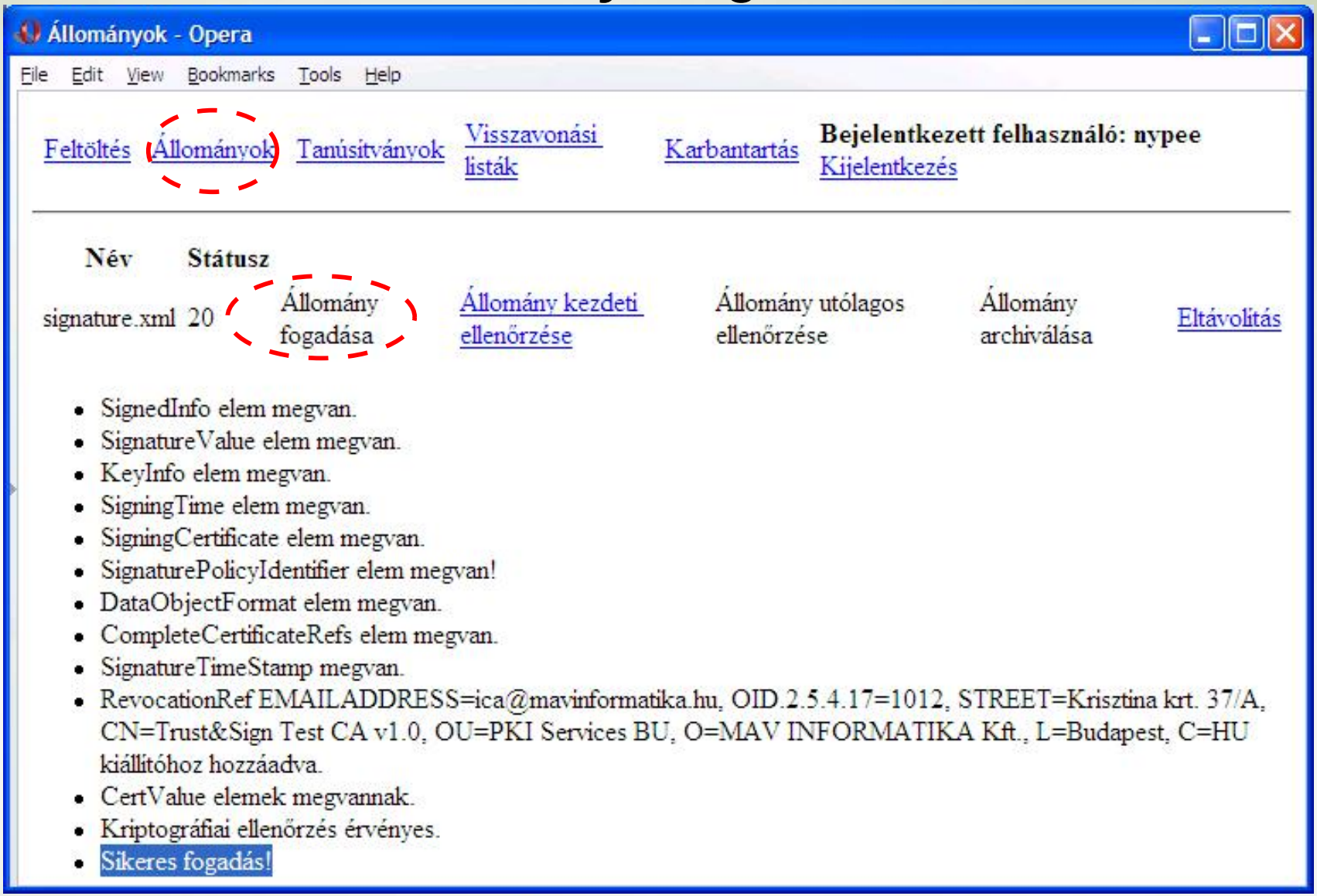
Állomány feltöltése



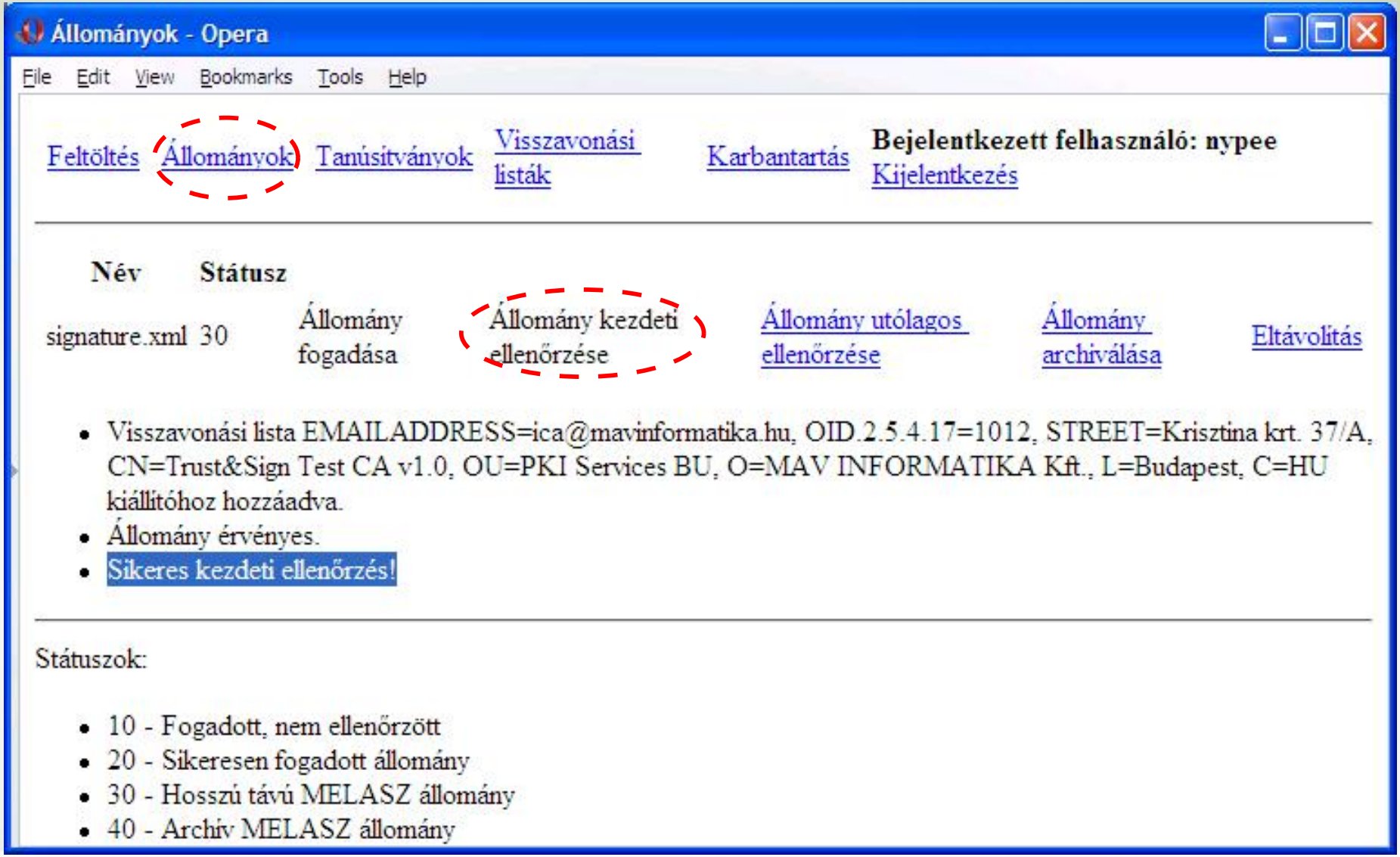
Alapállapot feltöltés után



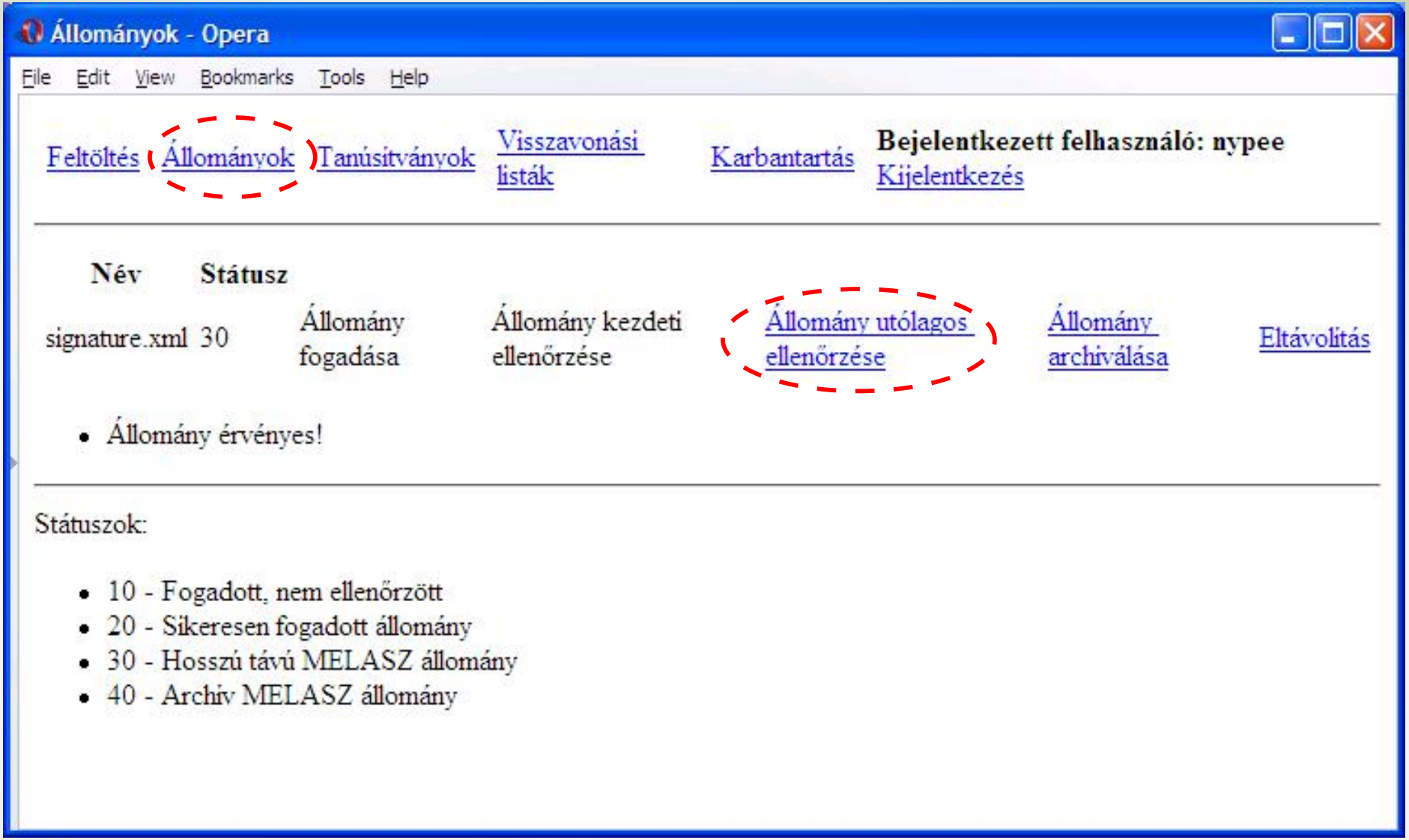
Állomány fogadása



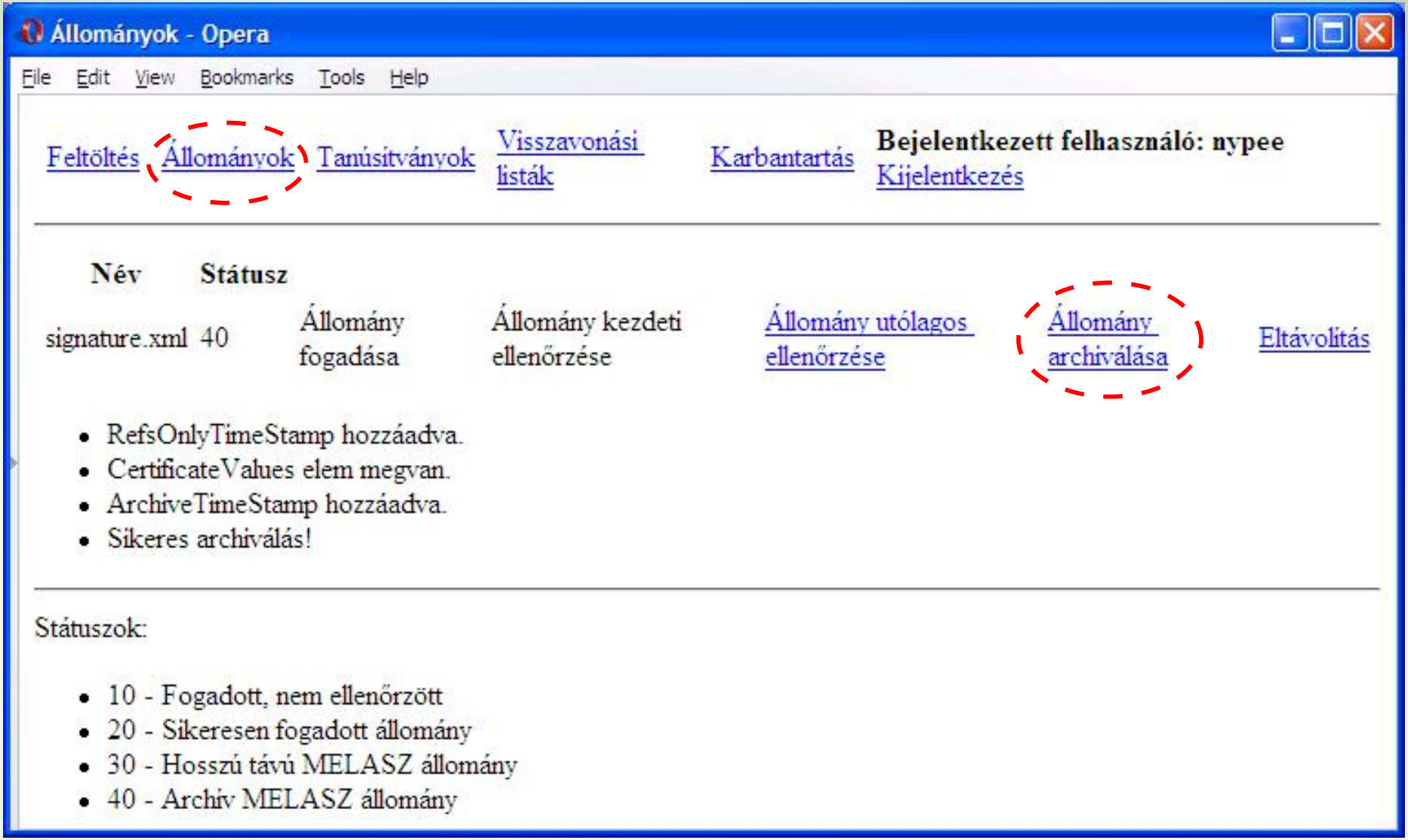
Állomány kezdeti ellenőrzése



Állomány utólagos ellenőrzése



Állomány archiválása



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!