MICROSEC
Számítástechnikai Fejlesztő Kft.

Aláírási jogosultság igazolása elektronikusan

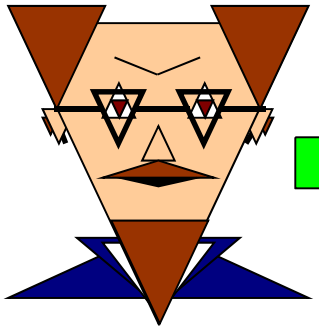
Dr. Berta István Zsolt <istvan.berta@microsec.hu>

Microsec Kft.

Elektronikus aláírás (e-szignó) (1)

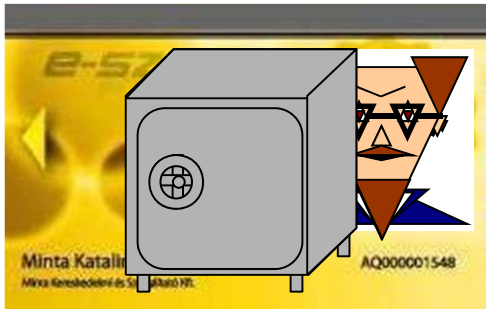
- Az elektronikus aláírás a **kódolás** egy fajtája
- Elektronikus aláíráskor
  ún. aláírás-létrehozó adat alapján kódoljuk
  az aláírt dokumentumot.
- A dokumentum hitelességét a kódolt (aláírt) dokumentum „szerkezete” garantálja.
- A kódolás az aláírás-létrehozó adat nélkül nem végezhető el.
- Az aláírást bárki ellenőrizheti, ehhez az aláíró tanúsítványa szükséges, amelyet hitelesítés szolgáltató bocsát ki.

Elektronikus aláírás (e-szignó) (2)



aláíró

dok

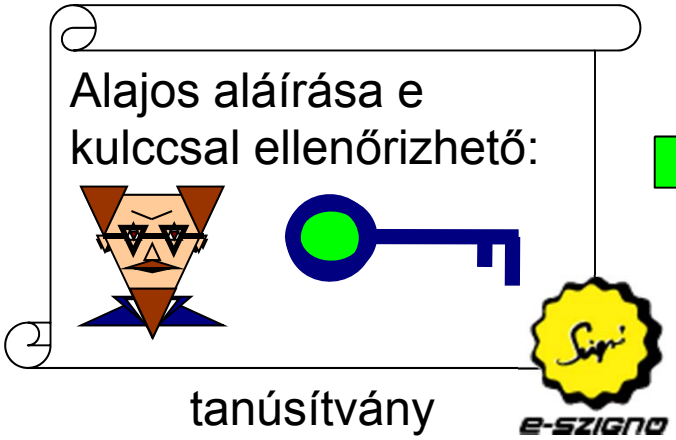


aláírás-létrehozó eszköz

aláírt dokumentum

dok

e-szigno



tanúsítvány

Az aláírt dokumentumról a tanúsítvány alapján egyértelműen megállapítható, hogy melyik aláíró magánkulcsával írták alá.

aláíró tanúsítvány ~
elektronikus aláírási címpéldány

Aláírás és szerepkör

Gyakran nem az a lényeg, hogy **ki** írt alá egy bizonyos dokumentumot, hanem hogy milyen

- szerepkör,
- jogosultság vagy
- tulajdonság

(egy szóval: **attribútum**)

kapcsolódik az aláíráshoz.

Tanúsítvány és attribútum kapcsolata

- Implicit kapcsolat
- Az attribútum a tanúsítványban szerepel
- Az attribútum az alany állításából derül ki
  - az alany felel a saját állításáért, így szükség esetén bíróság elé állítható
- Külön informatikai rendszer kapcsolja össze

Implicit kapcsolat

- Pl. csak az léphet be a szerverre, aki egy adott rootra visszavezethető tanúsítvánnyal rendelkezik;
- Így csak egyetlen attribútum kezelhető, minden attribútumhoz külön root és külön tanúsítvány kell.
- Nehezen kapcsolható más rendszerekhez, zárt rendszerben használható;

- Nem skálázható. ☹

Attribútum a tanúsítványban (1)

Tanúsítvány
CN=Alajos
...
egyetemi hallgató,
a Kókler Bt. alkalmazottja,
egyéni vállalkozó,
XI. kerületi lakos,
cukorbeteg,
az XXX párt tagja,
büntetlen előéletű,
stb.

- Bármely attribútum változik, a tanúsítványt vissza kell vonni – bonyolult, nehézkes.
- A tanúsítvány alapján az alany nem azonosítható – a „másodlagos regisztrációt” felborítja a tanúsítványcsere.
- Most épp melyik jogosultsága szerint használja a tanúsítványt?
- Mi köze a HSZ-nek az attribútumokhoz?
- Biztos jó, hogy minden aláírásban benne van minden attribútum?

Attribútum a tanúsítványban (2)

- Az attribútumok életciklusa nem egyezik meg a tanúsítványok életciklusával.
- Egyes attribútumok nagyon gyorsan változnak.
- A PKI szabályai szerint a tanúsítványt vissza kell vonni, ha **bármilyen** adat megváltozik benne.
- Ha fodrászhoz megyek, mindig új személyit kell csináltatnom?

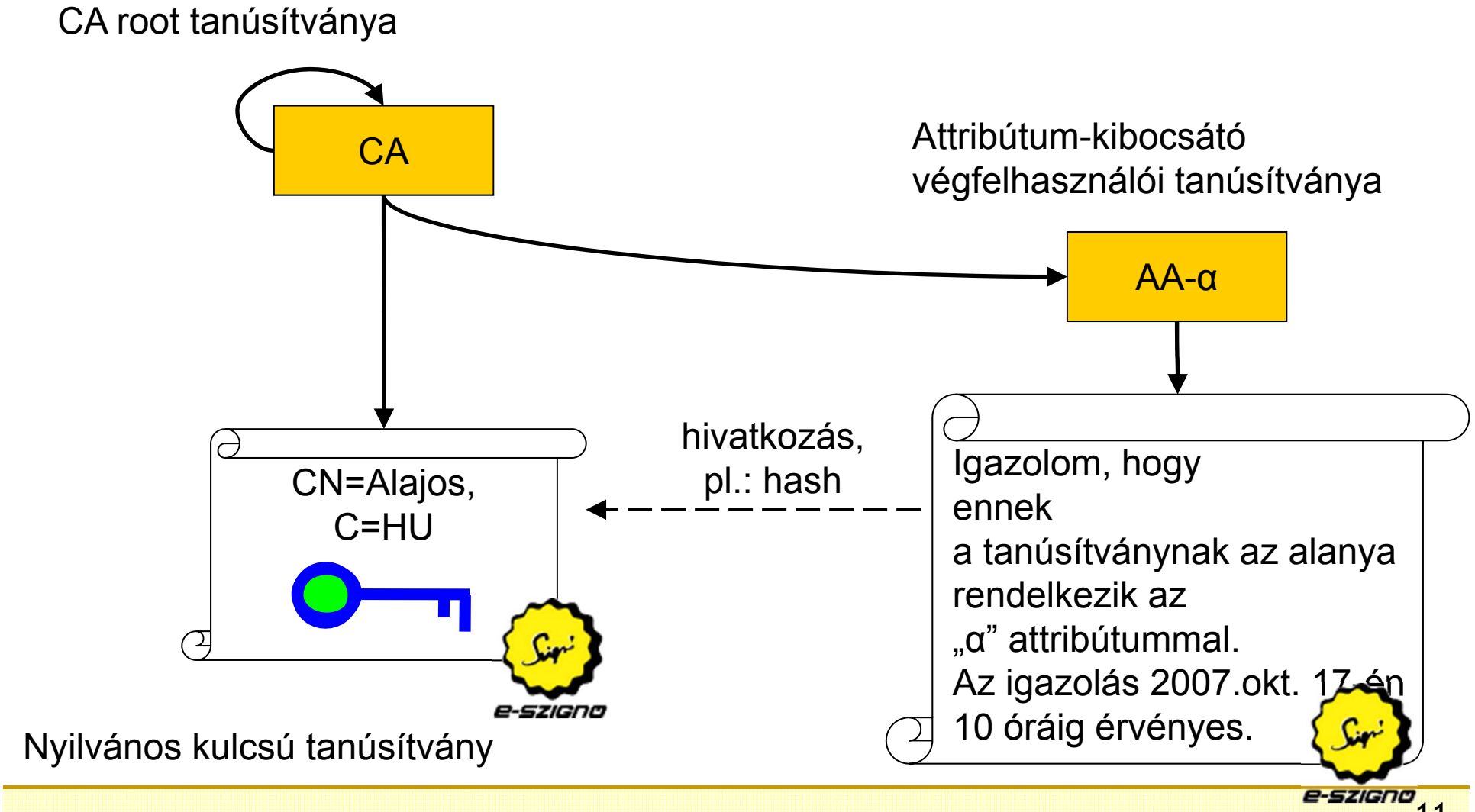
Az attribútum az alany állításából derül ki

- Mi történik, ha kiderül, hogy az alany hazudik az attribútumáról?
- Felelősségre lehet vonni az alanyt? Lehet, hogy
  - megszökött vagy meghalt,
  - nem tudja megtéríteni a kárt,
  - nem tehető felelőssé,
  - ...
- Az aláírás alapján hozott döntést vissza lehet csinálni?
- Papír alapon ugyanezen problémák merülnek fel
- Sokszor mégis ez a jó megoldás, mérlegelni kell...

Attribútum tanúsítvány

- Az attribútum-tanúsítvány olyan igazolás, amely egy nyilvános kulcsú tanúsítványhoz, vagy a nyilvános kulcsú tanúsítvány alanyához kapcsolódik, és alkalmas a nyilvános kulcsú tanúsítvány alanyához tartozó egy vagy több szerepkör, jogosultság, tulajdonság (együttesen: attribútum) igazolására.

Attribútum tanúsítvány (AT)



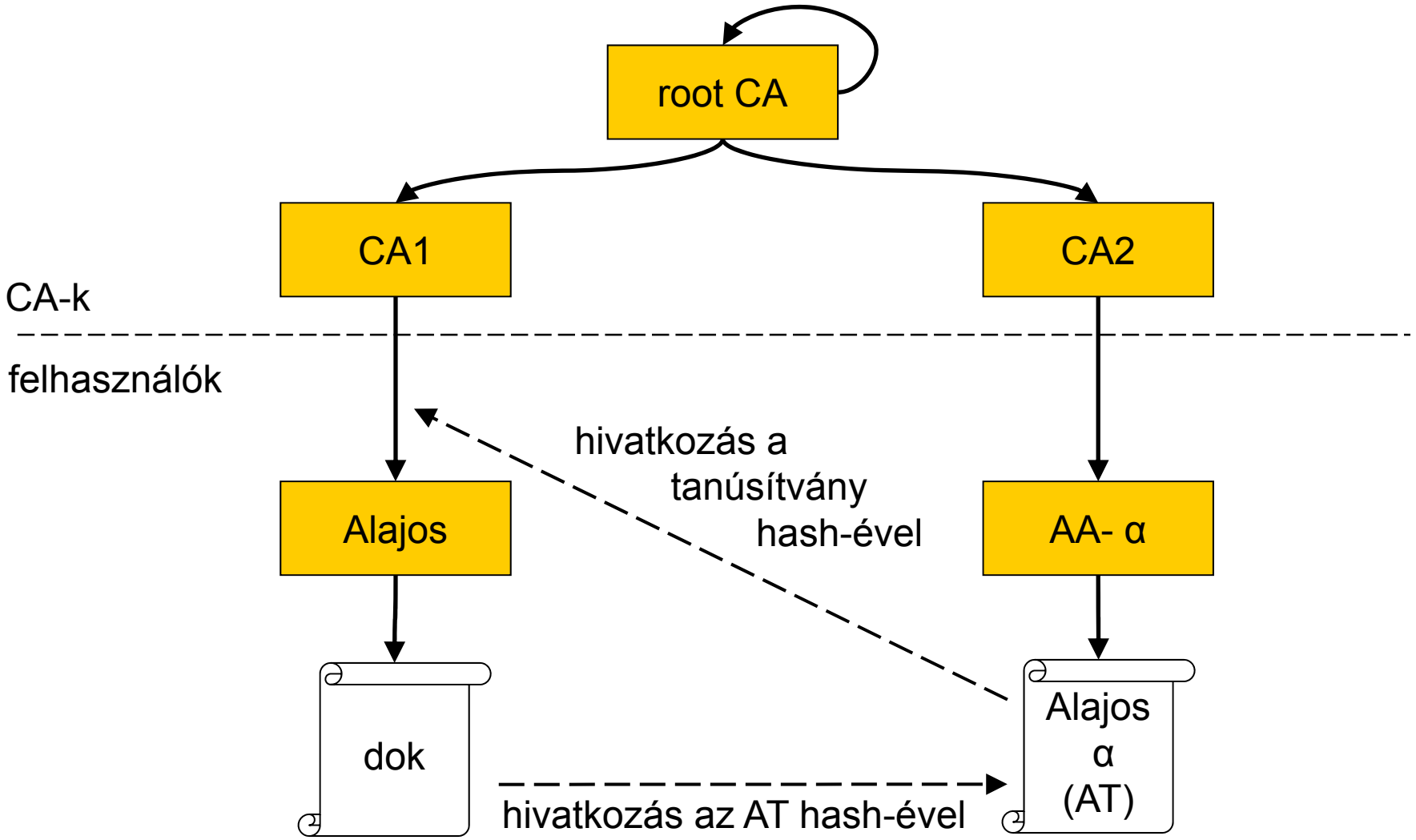
Ki bocsátja ki az AT-t?

- Attribute Authority (az AT-t kibocsátja) vs. Attribute Granting Authority (az attribútumról dönt)
- Általános attribútum szolgáltató (bármilyen attribútumot igazolhat) vs. mindenki egy attribútum igazolására jogosult

AT felhasználása

- Push modell
  - aki igazolni szeretné a saját szerepkörét, beszerzi a szükséges AT-t, és eljuttatja a befogadóhoz (pl. csatolja az aláírásához, esetleg alá is írja)
  - a XAdES aláírásokban van helye az AT-nek
- Pull modell
  - aki ellenőrizni szeretne egy attribútumot, az gyűjti be a szükséges AT-t
  - ki jogosult lekérdezni az attribútumokat?

AT egy aláírásban



AT ellenőrzése

- Az AT-n aláírás van, ennek megfelelően kell
- ellenőrizni…
  - tanúsítványlánc felépítése,
  - visszavonási állapot (az AT-re és a tanúsítványlánc elemeire),
  - aláírás időpontja
  - stb.
- Policy szerint... ☺

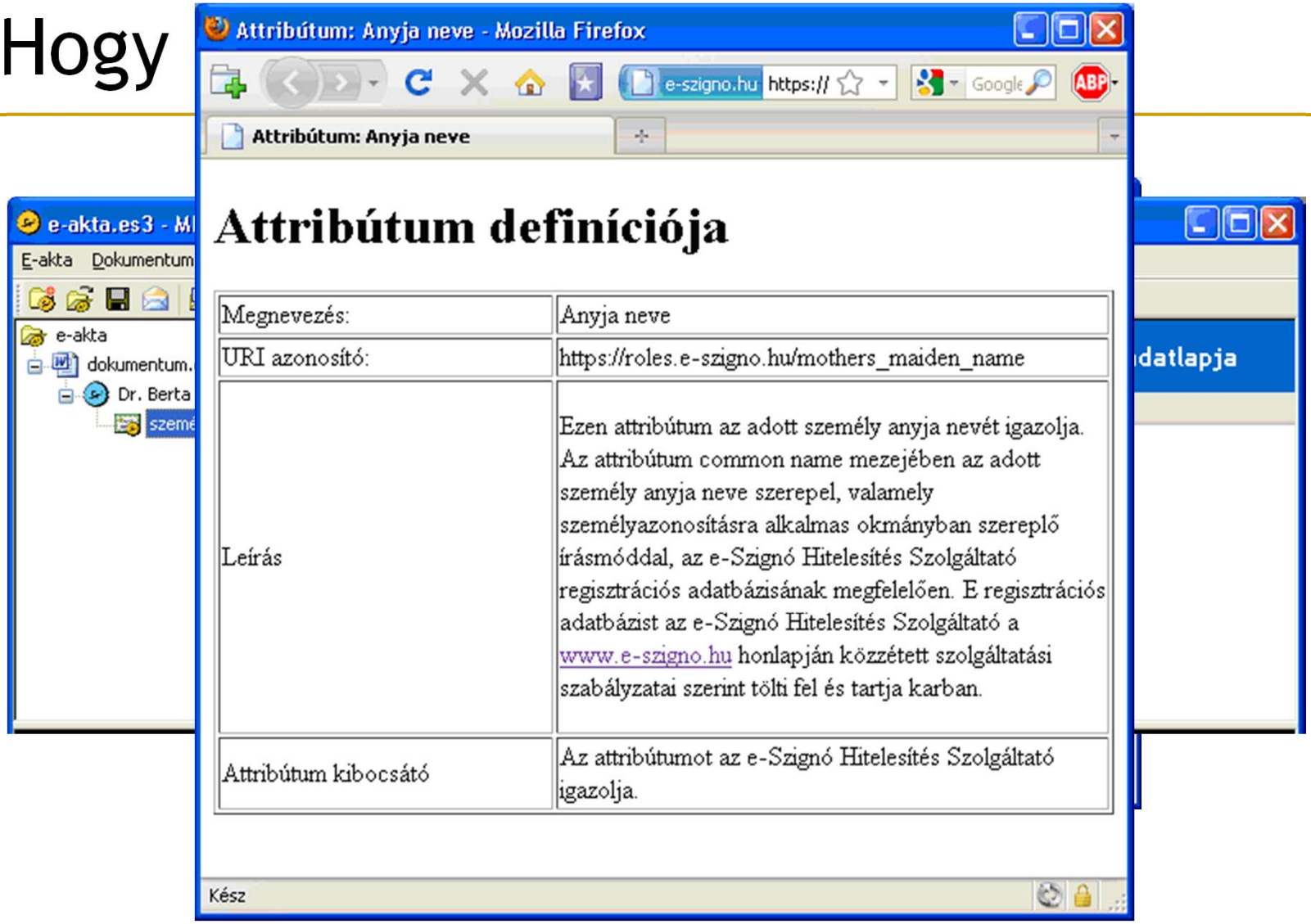
Hogyan jelenik meg az attribútum?

- Géppel értelmezhető megoldások
  - OID,
  - URI,
  - …
- Ember számára értelmezhető megoldások
  - szövegesen,
  - DN,
  - …

Hol használnak attribútum tanúsítványt?

- Nemigen használnak attribútum tanúsítványt.
- Nyilvános kulcsú tanúsítványt is csak nagyon kevés helyen használnak, az attribútum tanúsítványokhoz nyilvános kulcsú tanúsítványok kellenek.
- Az attribútum tanúsítványok lehetővé tennék, hogy egy nyilvános kulcsú tanúsítványt több célra is fel lehessen használni.

Hogy


Attribútum: Anyja neve - Mozilla Firefox
e-szigno.hu
https://
Google
Attribútum: Anyja neve
Attribútum definíciója
Megnevezés:
Anyja neve
URI azonosító:
https://roles.e-szigno.hu/mothers_maiden_name
Leírás
Ezen attribútum az adott személy anyja nevét igazolja. Az attribútum common name mezejében az adott személy anyja neve szerepel, valamely személyazonosításra alkalmas okmányban szereplő írásmóddal, az e-Szignó Hitelesítés Szolgáltató regisztrációs adatbázisának megfelelően. E regisztrációs adatbázist az e-Szignó Hitelesítés Szolgáltató a www.e-szigno.hu honlapján közzétett szolgáltatási szabályzatai szerint tölti fel és tartja karban.
Attribútum kibocsátó
Az attribútumot az e-Szignó Hitelesítés Szolgáltató igazolja.
Kész
e-akta.es3 - M
E-akta
Dokumentum
e-akta
dokumentum.
Dr. Berta
datlapja

Összefoglalás

- Sok hátránya van annak, hogy az attribútumok a nyilvános kulcsú tanúsítványban szerepeljenek
  - attribútumok és tanúsítványok eltérő életciklusa
  - adatvédelmi kérdések
- Az AT hivatkozik a nyilvános kulcsú tanúsítványra vagy annak alanyára, és igazolja a hozzá tartozó attribútumot.
  - nyilvános kulcsú tanúsítvány: kulcs-alany összerendelés
  - AT: az alany attribútumai
- Az AT-k segítségével egy nyilvános kulcsú tanúsítványt több célra lehetne használni…
- Az AT-k kibocsátása, kezelése, felhasználása stb. még közel nem kiforrott.

Köszönöm a figyelmet! ☺