MICROSEC
Számítástechnikai Fejlesztő Kft.

Aláírási jogosultság igazolása elektronikusan

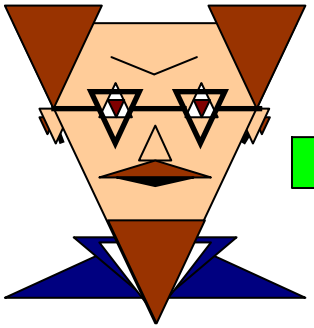
Dr. Berta István Zsolt <istvan.berta@microsec.hu>

Microsec Kft.

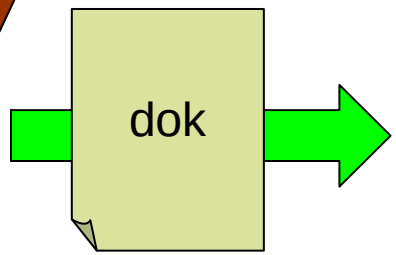
Elektronikus aláírás (e-szignó) (1)

- Az elektronikus aláírás a **kódolás** egy fajtája
- Elektronikus aláíráskor
  ún. aláírás-létrehozó adat alapján kódoljuk
  az aláírandó 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)

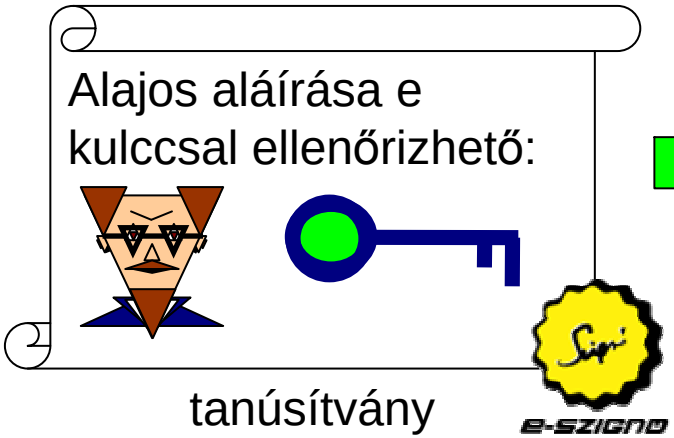


aláíró



aláírás-létrehozó eszköz

aláírt dokumentum



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

- Honnan tudjuk, hogy a tanúsítvány alanya rendelkezik-e egy adott attribútummal?
  1. Implicit kapcsolat
  2. Az attribútum a tanúsítványban szerepel
  3. Az attribútum az alany állításából derül ki
  4. Az attribútumot más rendszerben tartjuk nyilván, és e rendszer igazolja

Implicit kapcsolat

- Pl. csak az léphet be a szerverre, aki egy adott gyökérre visszavezethető tanúsítvánnyal rendelkezik;
- Így csak egyetlen attribútum kezelhető, minden attribútumhoz külön root és külön tanúsítvány kell.
- Elektronikus aláírás esetén nehézkes.
- Nehezen kapcsolható más rendszerekhez, zárt rendszerben használható.
- Nem skálázható. ☹

Attribútum a tanúsítványban (1)

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

- Bármely attribútum változik, a tanúsítványt vissza kell vonni – bonyolult, nehézkes.
- A tanúsítvány cseréje (lejárat, visszavonás, adatváltozás) gondot okozhat
- 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 alany nyilatkozik az attribútumáról

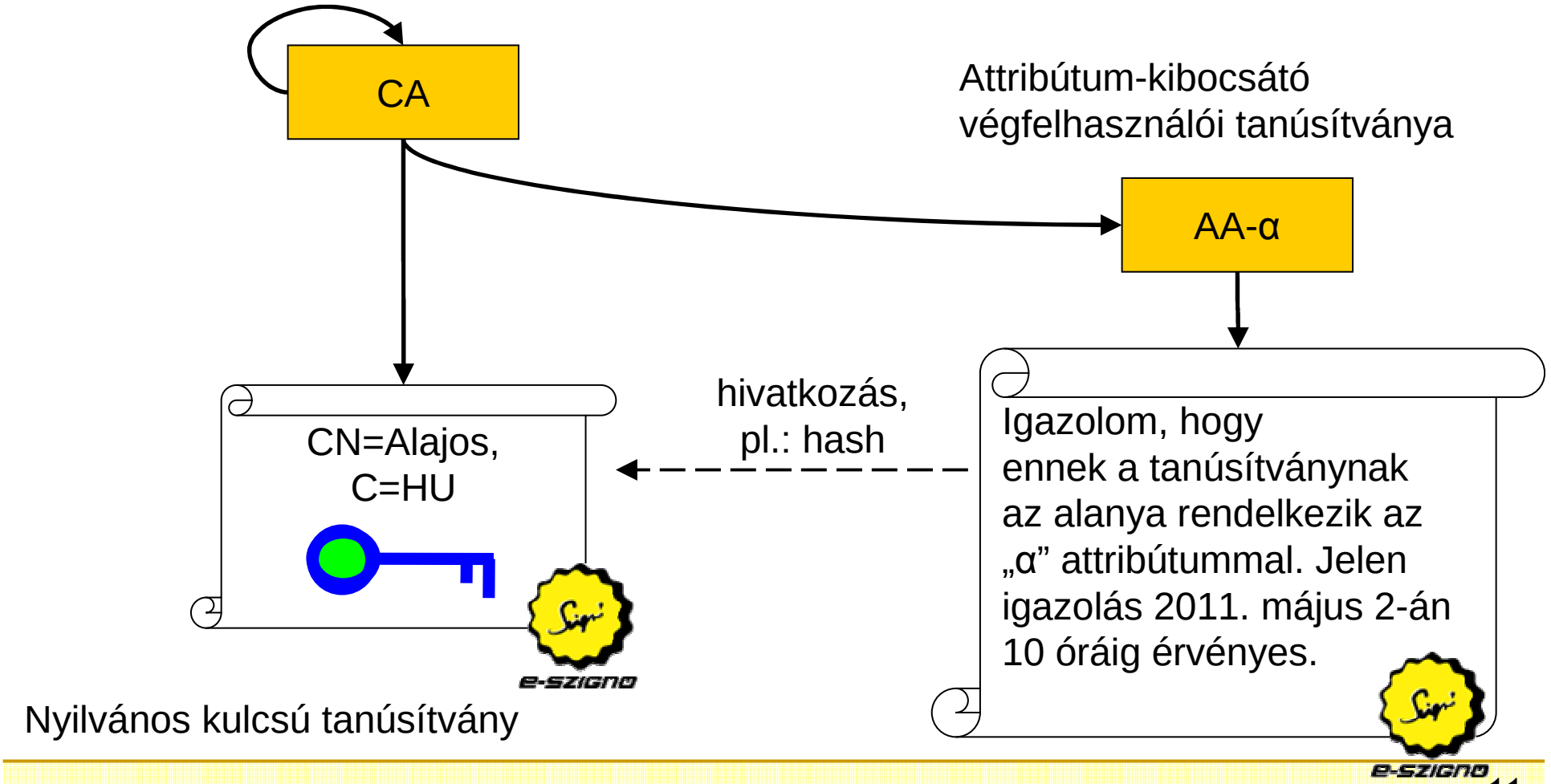
- … és ha hazudik?
- Felelősségre lehet vonni? Lehet, hogy
  - megszökött vagy meghalt,
  - nem tudja megtéríteni a kárt, …
- Az aláírás alapján hozott döntést vissza lehet csinálni?
- Papír alapon ugyanezen problémák merülnek fel
- Sokszor mégis ez a jó megoldás, mérlegelni kell...

Más rendszer igazolja az attribútumot

- **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)

A hitelesítés szolgáltató gyökértanúsítványa



Nyilvános kulcsú tanúsítvány

Jogi szemmel

- A magyar elektronikus aláírás törvény (Eat) nem fogalmaz meg követelményeket az attribútum-tanúsítványokra
- Jogi értelemben az attribútum-tanúsítvány egy **elektronikusan aláírt dokumentum**, és ennek megfelelő joghatás kapcsolódik hozzá
- Az Eat. szerint nehezen képzelhető el általános, bármilyen attribútumot igazolni tudó attribútum szolgáltató, de…
- A saját hatáskörében bárki bocsáthat ki igazolást – papíron is, elektronikusan is.

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?

Hogyan használjunk attribútum-tanúsítványt?

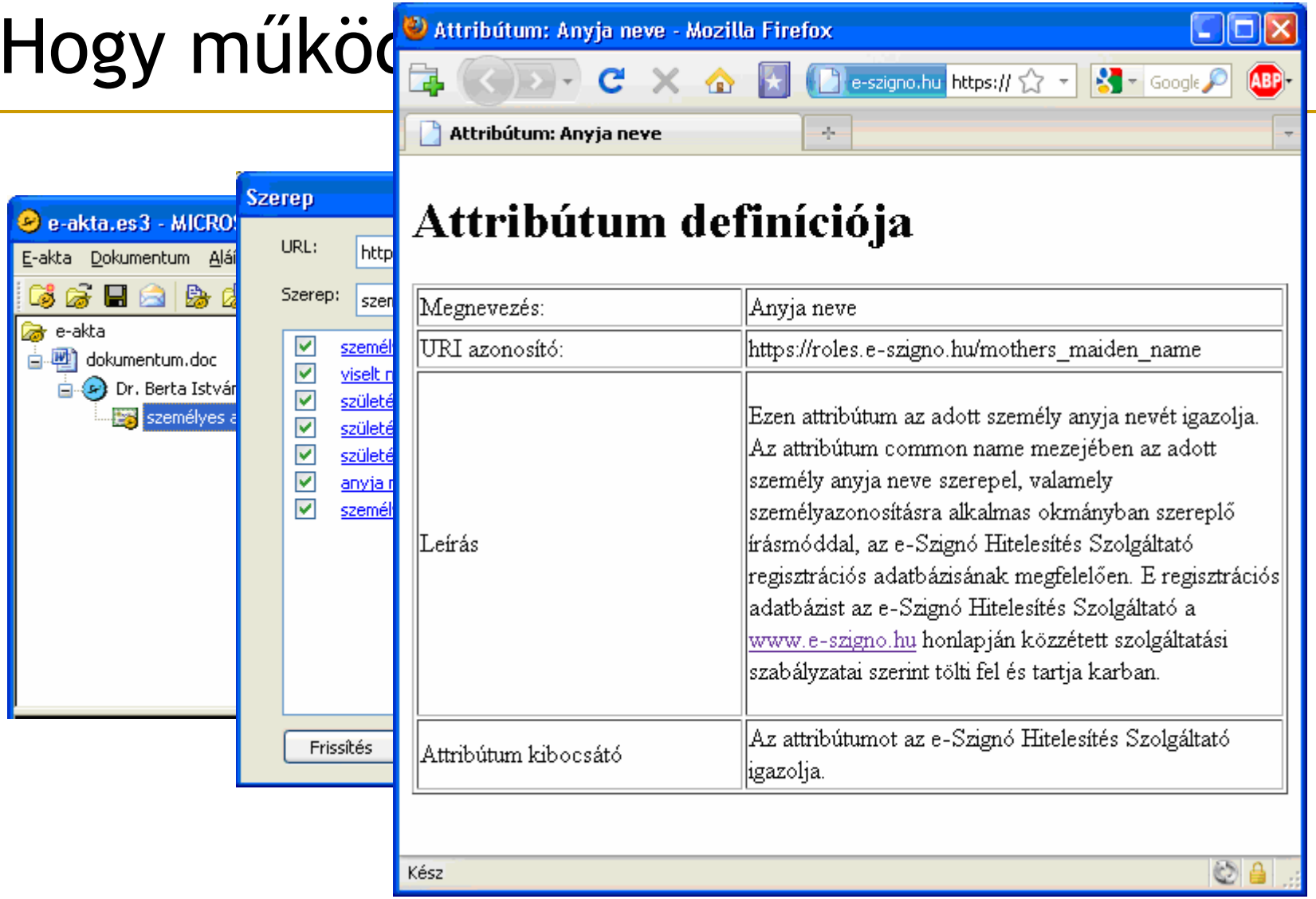
Javaslat

1. Elkészítem az aláírandó dokumentumot, amelyet az α szerepkörben szeretnék aláírni.
2. Kapcsolatba lépek az α attribútum igazolására jogosult féllel, beszerzek egy attribútum-tanúsítványt.
3. Csatolom az AT-t az aláírandó dokumentumhoz, és a kettőt együttesen írom alá.
4. Az aláírást időbélyeggel látom el.

Attribútum-tanúsítvány befogadása

- Az aláírást ellenőrző fél az attribútum-tanúsítványt is ellenőrizni szeretné
- Az attribútum-tanúsítványon is aláírás van, ennek megfelelően kell ellenőrizni:
  - tanúsítványlánc felépítése,
  - visszavonási állapot (az AT-re és a tanúsítványlánc elemeire),
  - aláírás időpontja
  - stb.

Hogy működ


e-akta.es3 - MICRO
E-akta Dokumentum Aláí
e-akta
dokumentum.doc
Dr. Berta István
személyes a
Szerep
URL:
http
Szerep:
szer
személ
viselt n
születé
születé
születé
anyja n
személ
Frissítés
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

További információ

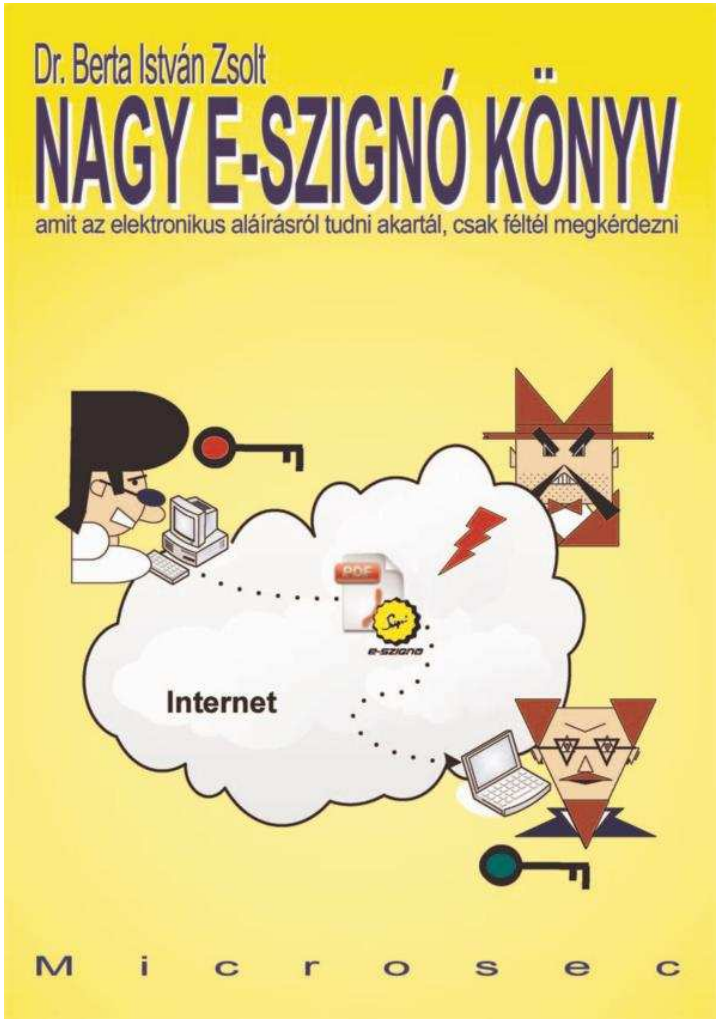
- Szabványok:
  - ITU X.509
  - ETSI TR 102 042 – reqs for role and attr. certs
  - ETSI TS 102 158 – policy requirements
  - RFC 3281 – attr. cert framework
- Könyvek:
  - Almási J. et al. – Elektronikus hitelesség, elektronikus aláírás, 2009.
  - Berta I. Zs. – NAGY E-SZIGNÓ KÖNYV, 2011.

NAGY E-SZIGNÓ KÖNYV

(amit az elektronikus aláírásról tudni akartál, csak féltél megkérdezni)

Ingyenesen letölthető:

- www.berta.hu
- www.e-szigno.hu



Összefoglalás

- Nem szerencsés, ha az attribútum az aláírói tanúsítványban szerepel
  - adatvédelmi kérdések
  - tanúsítványcserék okozta nehézségek
- Attribútum-tanúsítvány: igazolja, hogy egy (aláíró) tanúsítvány alanya rendelkezik adott attribútummal
- Így egyazon aláíró tanúsítvány több célra is felhasználható ☺

Köszönöm a figyelmet! ☺