MICROSEC
Számítástechnikai Fejlesztő Kft.

PKI gyakorlati kérdések, II

Dr. Berta István Zsolt
istvan.berta@microsec.hu
Microsec Kft.

Miről fogok beszélni?

- Elektronikusan aláírt iratok hosszú távú archiválása, elektronikus archiválás szolgáltatás
- Kereszthitelesítés
- Attribútum tanúsítványok

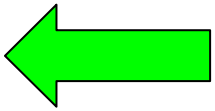
VIGYÁZAT!

- Ebben az eladásban új, még nem letisztult területekről lesz szó.
- Mások, máshol egészen mást is mondhatnak ezen területekről, és az is lehet, hogy „jó”.
- Problémákat vetek majd fel, és a választ gyakran magam sem tudom.
- Sok mondat végén „?” lesz…

Elektronikusan aláírt iratok hosszú távú archiválása, elektronikus archiválás szolgáltatás

Mit értünk aláírás alatt?

- kötelezettségvállalás, egy dokumentum tartalmának elfogadása?



- bizonyíték ezen kötelezettségvállalásra?
  - ...tinta és a papír kapcsolata...
  - ...kriptográfiai művelet...
- bizonyító erő, amivel ez a bizonyíték rendelkezik?

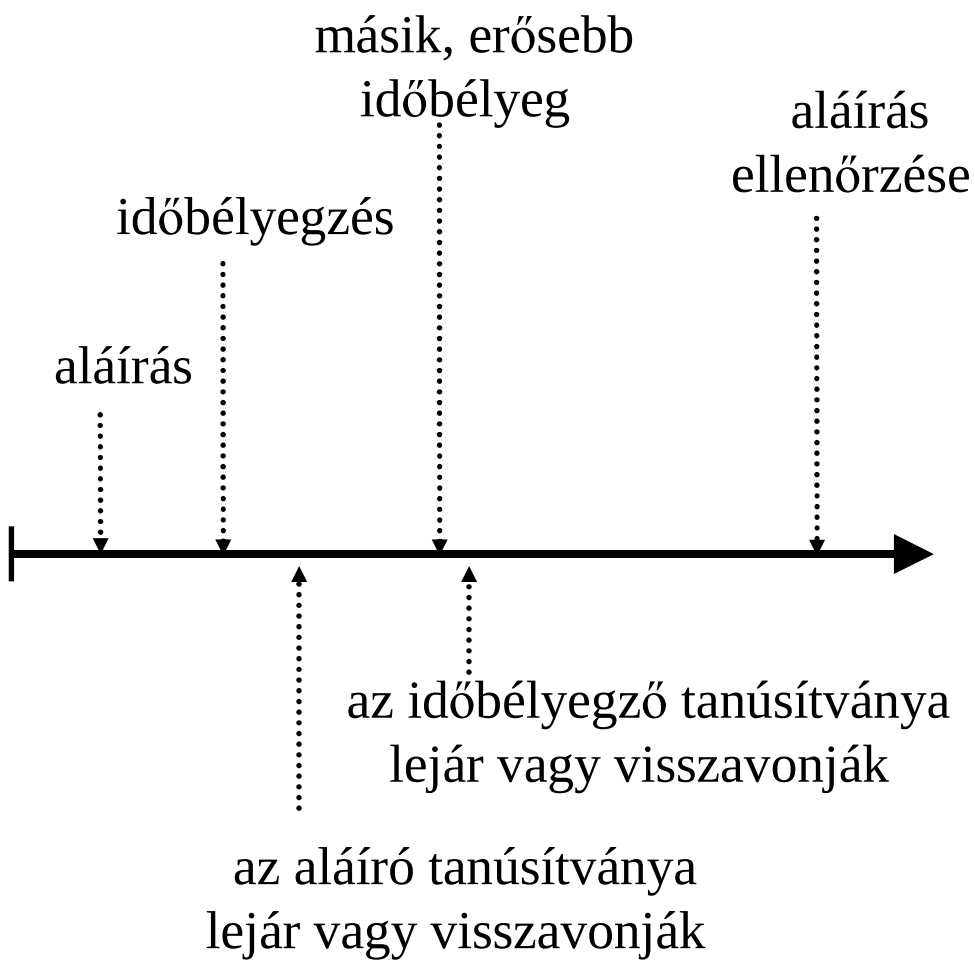
Mitől válhat egy aláírás érvénytelenné?

- A kötelezettségvállalás nem válik érvénytelenné.
  Az fordulhat elő, hogy már nem bizonyítható, hogy a kötelezettségvállalás valóban megtörtént.
- Mi okozhatja ezt?
  - Ha már nem bizonyítható, hogy az aláíró tanúsítványa érvényes volt akkor, amikor az aláírás készült;
    (e probléma időbélyeggel orvosolható)
  - Időbélyegzés szolgáltatók tanúsítványának lejárta;
  - Időbélyegzés szolgáltatók meghibásodása vagy a magánkulcsának kompromittálódása;
  - A tudomány vagy a technológia hirtelen, ugrásszerű fejlődése.

Meddig hiteles egy elektronikus aláírás?

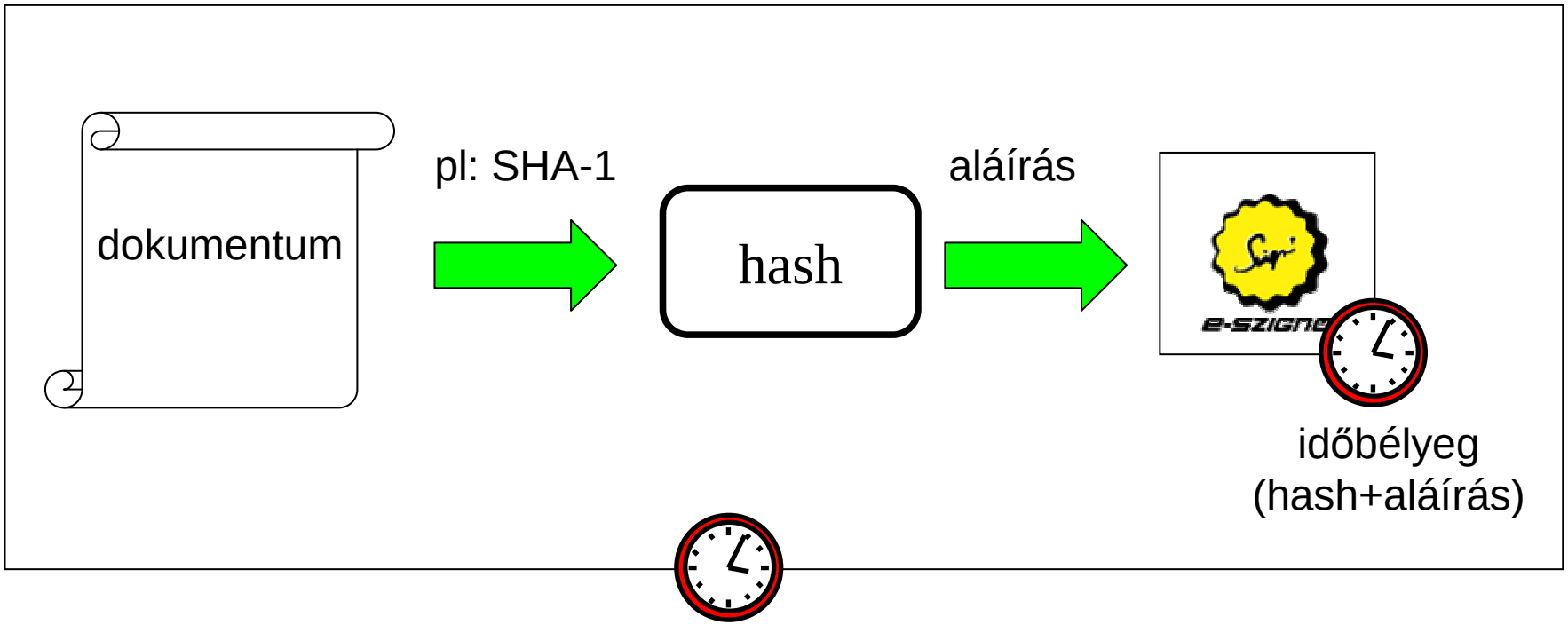
- „Alap” aláírás (-BES):
  - amíg az aláíró tanúsítványa érvényes.
- Időbélyeggel ellátott aláírás (-T):
  - amíg az időbélyegző tanúsítványa érvényes
  - 11 évig (114/2007. GKM r.)
- Ha azt szeretnénk, hogy az elektronikus aláírás ennél tovább is ellenőrizhető maradjon (114/2007. GKM r.):
  - archiválás szolgáltatás vagy
  - rendszeres időbélyegzés (-A)

Hogyan válhat érvénytelenné egy aláírás?



- Ha az aláíró tanúsítványa már nem érvényes, miből állapítható meg, hogy az aláírás akkor készült, amikor az aláíró tanúsítványa még érvényes volt?
- Ha az időbélyegző tanúsítványa már nem érvényes, miből állapítható meg, hogy az időbélyegzés pillanatában érvényes volt-e?

Kriptográfiai algoritmusok elvaulása



Hogyan őrizhetjük meg az aláírás hitelességét?

- Össze kell gyűjteni minden olyan információt, amely igazolja, hogy az aláíró tanúsítványa aláíráskor érvényes volt.
- Mindezt időbélyeggel kell ellátni.
- Folyamatosan figyelni kell, hogy a közeljövőben várhatóan megkérdőjelezhetővé válik-e az időbélyeg hitelessége.
- Szükség esetén az összegyűjtött adatokat további időbélyeggel kell ellátni, de előtte csatolni kell az időbélyeg érvényességét igazoló információkat.
- Archív aláírások (ETSI TS 101 903 - XAdES-A)
- Archiválás szolgáltatás (LTANS, RFC 4810)
- Jogszabály: 114/2007 GKM rendelet

Elektronikusan aláírt adat archiválása

A papír alapú dokumentumokhoz hasonlóan az elektronikusan aláírt dokumentumokat is speciális körülmények között kell archiválni.

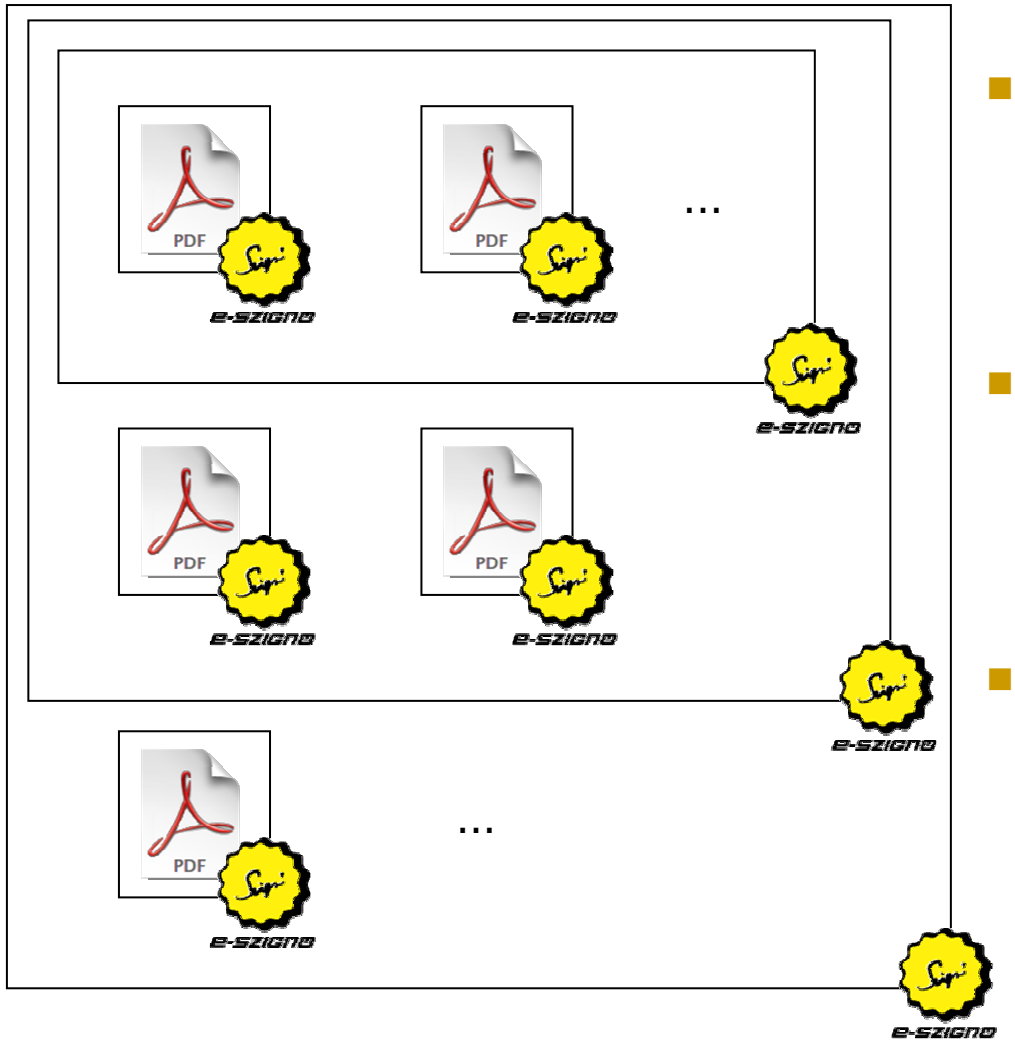
„Saját megőrzés”
pl. archív aláírás
létrehozása
és gondozása

Elektronikus
archiválás
szolgáltató
(Eat. szerinti)

Archiválás szolgáltatás

- Az archiválás szolgáltató megbízható rendszerrel ellenőrzi, és biztonságos módon eltárolja az archiválandó aláírást.
- Az archiválás időtartama alatt a jogszabályi előírások szerint folyamatosan biztosítja az archivált aláírások hitelességét.
- Ügyfelei kérésére igazolást állít ki arról, hogy egy adott aláírás érvényes.
- Ha minősített archiválás szolgáltató archivál egy aláírást, vélelmezni kell, hogy az aláírás érvényes.
- A szolgáltatást az Eat. definiálja.
- A minősített archiválás szolgáltatókról a Nemzeti Média- és Hírközlési Hatóság vezet nyilvántartást.

Mit csinál az archív szolgáltató?



- Rendszeresen egyre biztonságosabb aláírásokkal/időbélyegekkel látja el az archívumot.
- A befoglaló aláírások/ időbélyegek igazolják, hogy a tartalom azt megelőzően készült.
- A befoglalt aláírásoknak a befoglaló aláírásokon lévő időbélyegek pillanatában érvényesnek és biztonságosnak kell lennie.

Hogy működik az archív szolgáltató?

- Archív aláírások alapján
- vagy: más, hasonló elvre épülő módon

- Az archív szolgáltató ugyanazt végzi, mint amit a „saját megőrzés” keretében el lehet végezni...
- Az archív szolgáltató adhat ki Eat. szerinti igazolást...

Hosszú táv, Változó környezet

- Az archiválás szolgáltató hosszú távon, hosszú ideig (20 év, 50 év, ...) kell, hogy működjön. Ennyi idő alatt megváltozhatnak
  - a biztonságos kulcsméretek, algoritmusok;
  - az elfogadott gyökér-tanúsítványok;
  - a szolgáltatók hitelesítési/időbélyegzési rendjei;
  - az elektronikus aláírás ellenőrzésére vonatkozó követelmények;
  - az aláírások és érvényességi láncok formátumára vonatkozó specifikációk;
  - az elektronikus aláírásra és az archiválásra vonatkozó jogszabályok, specifikációk.
  - …
- Alapvetően megváltozhat az aláírás fogalma, és az aláírás ellenőrzésének módja.

Amiről részletesebben is beszélek…

- Követelményrendszer, minősítés
- Aláírt dokumentum vagy aláírt lenyomat archiválása?
- Az archivált e-akták bizalmassága
- Hogyan gyűjti össze az archiválás szolgáltató az aláírás ellenőrzéséhez szükséges információkat, hogyan építi fel az érvényességi láncot?
- Az aláírt dokumentumok hiteles megjeleníthetőségének, értelmezhetőségének biztosítása

Követelményrendszer

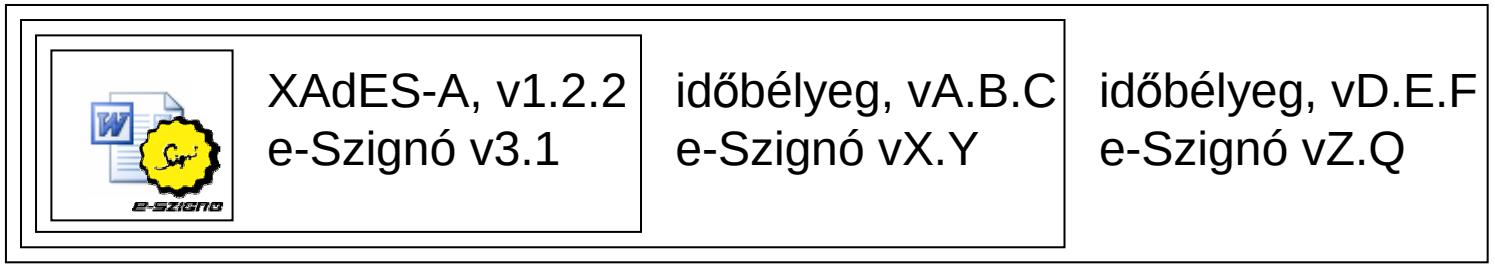
- Az elektronikus archiválás szolgáltatást a magyar Eat. határozza meg.
- Külföldön is ismert fogalom, de ott nem a törvényben van benne.
- Külföldön sem elterjedt jelenség.
- Új terület, nem létezik rá a hitelesítés szolgáltatáséhoz hasonlóan letisztult és elfogadott nemzetközi követelményrendszer, nem beszélhetünk (elterjedt) nemzetközi gyakorlatról sem.
- NHH ajánlások (2008)

Milyen best practice-ek léteznek?

- Az archív aláírás hasonló problémát old meg, és erre léteznek letisztult nemzetközi specifikációk – pl. ETSI TS 101 903 (XAdES)
- Long-Term Archive and Notary Services
  - archív szolgáltatást céloz meg, nem archív aláírás, hanem adatbázis-alapon
  - Pl.: RFC 4810 (2007)
  - http://ietfreport.isoc.org/ids-wg-ltans.html

Archiválás szolgáltatás ↔ Archív aláírás

- Az archív szolgáltató feladata az aláírások hosszú távú hitelességének biztosítása;
- Ezt teheti például archív aláírással is, de nem feltétlenül ezt a technológiát kell alkalmaznia.
- Archív aláírás bizonyíthatja egy aláírás hitelességét, de hosszú távon nem lesz egyszerű értelmezni egy archív aláírást.



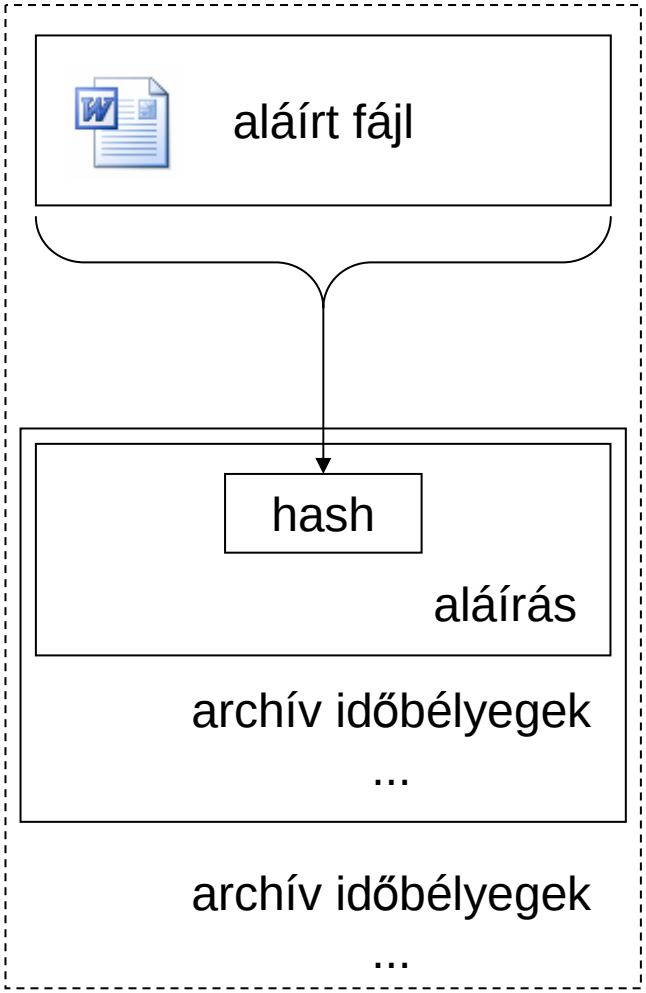
- Nincs olyan XAdES-verzió, amelynek ez megfelelne, nincs olyan e-Szignó verzió, amely ilyen aláírást hozna létre...
- Az archív szolgáltató igazolásainak lesz jelentősége.

Aláírt dokumentum/lenyomat archiválása

Az Eat. kétféle archiválás szolgáltatást definiál:

- Az archív szolgáltató az aláírt dokumentumot (e-aktát) archiválja.
  - logikailag tiszta megoldás
- Az archív szolgáltató csak az aláírást kapja meg, az aláírt dokumentumot nem:
  - a bizalmasság biztosítása egyszerű ☺
  - a dokumentum és az aláírás elválik egymástól ☹
  - nem véd a hash algoritmus elavulása ellen… ☹

Gondok a csak lenyomat archiválásával

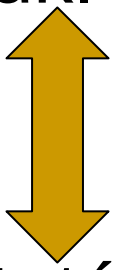


- nem véd a dokumentum megsemmisülése ellen ☹
- az ügyfélnek rendszeresen foglalkoznia kell a dokumentummal ☹
- ha rossz lenyomat jön be, az csak sokára derül ki
- az ügyfél „bukja” az archiválást, ha nem időben küldi be a lenyomatot ☹

Döntés: A teljes e-akta archiválását választottuk.

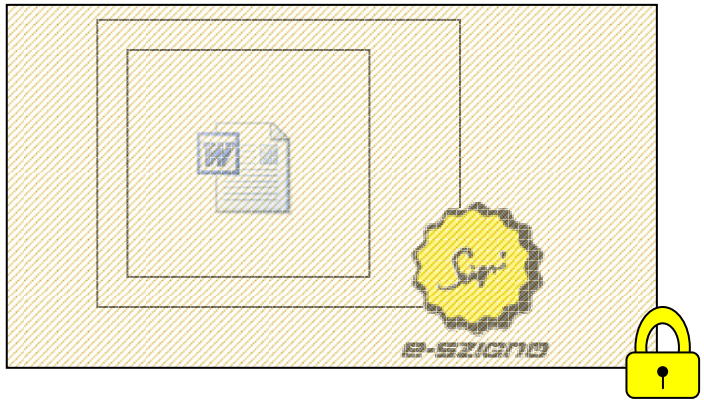
Követelmények bizalmasságra

- Az archív szolgáltató lehetőleg minél ritkábban kezelje a nyílt fájlokat, lehetőleg ne is találkozzon velük.

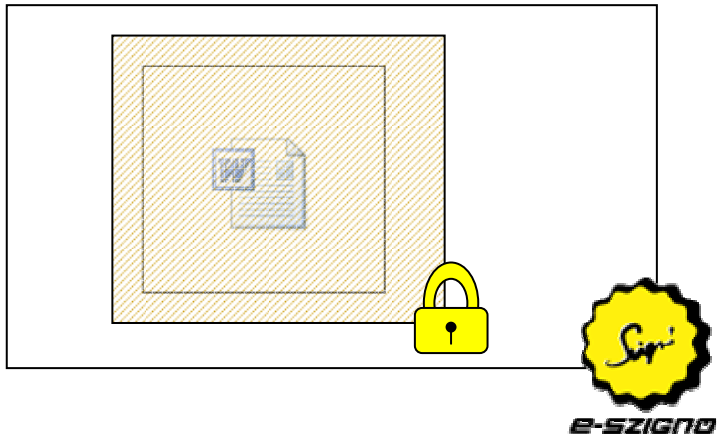


- Az archív szolgáltatónak befogadáskor ellenőriznie kell az elektronikus aláírást.
- Az archív szolgáltatónak rendszeresen időbélyeget (és aláírást) kell elhelyeznie a dokumentumokon.

Titkosítás ↔ Aláírás



- A titkosítás miatt nem lehet ellenőrizni az aláírást.
- Tiszta megoldás, korlátokkal

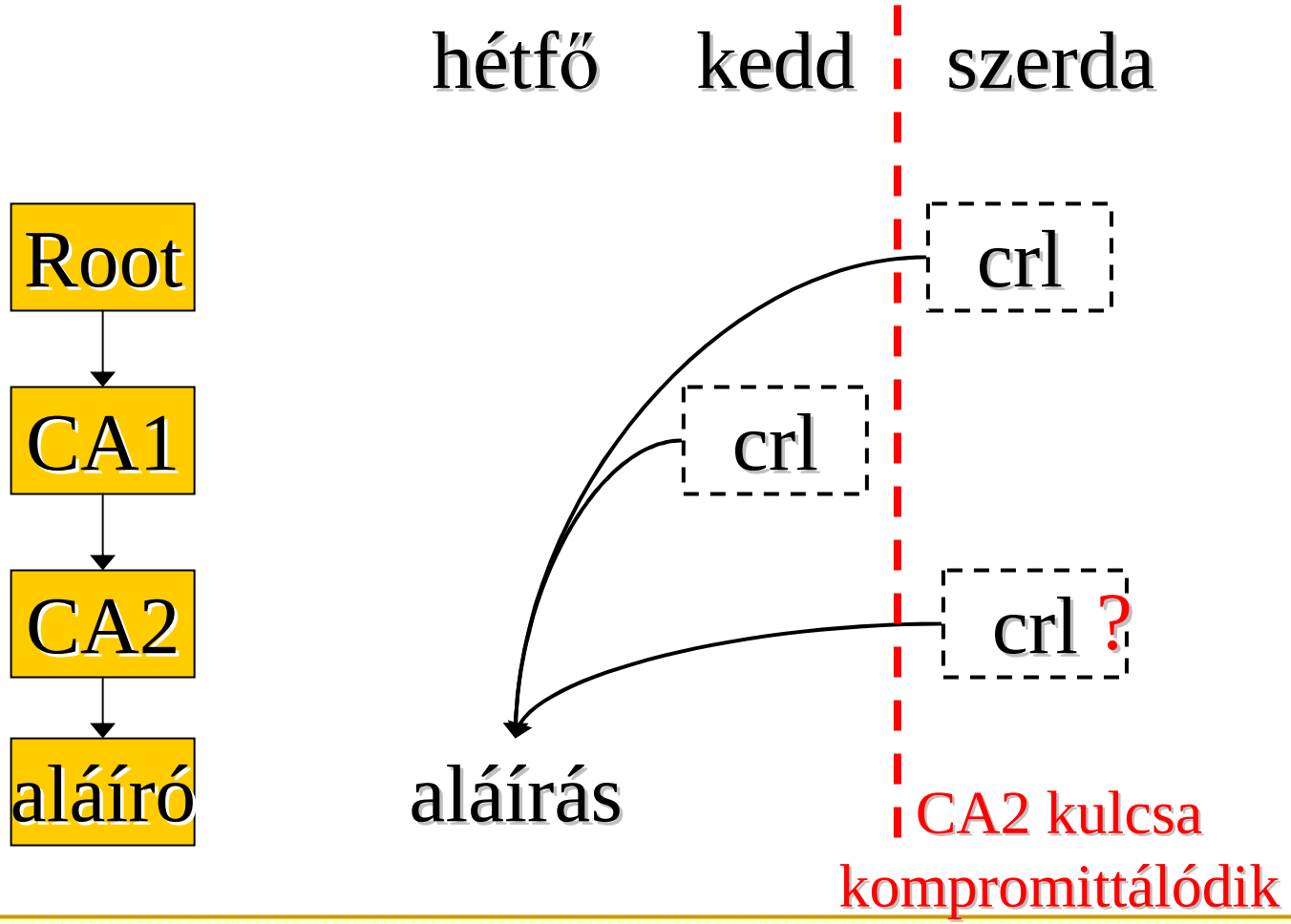


- Hogyan bizonyítjuk, hogy mire vonatkozik az aláírás?
- Alapvető elvi problémák

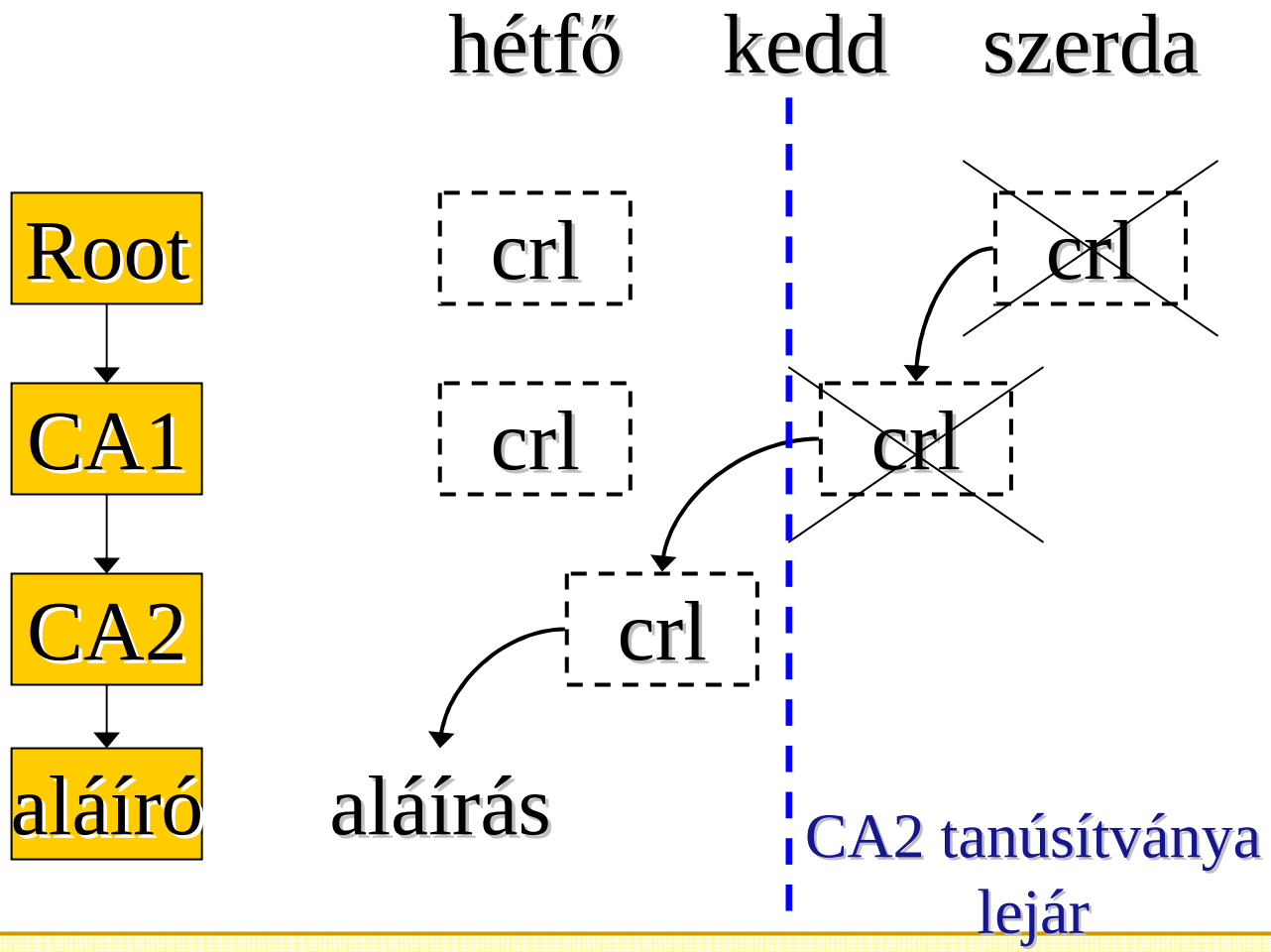
Miért nem CRL?

- Két külön feladat:
  - megbizonyosodni egy aláírás érvényességéről (kivárási idő),
  - beszerezni az aláírás érvényességét igazoló bizonyítékokat.
- CRL alapján bonyolult elvégezni az ellenőrzést. Rendkívül komplex problémák is megjelenhetnek.
- CRL esetén a visszavonási információk különböző időpillanatokból származnak, az archiválás szolgáltató nem tudja ezt befolyásolni.
- (Tapasztalat: CRL alapon általában is nehéz valós problémákat megoldani…)

Az aláírás időpontját követő CRL-ek?



Megköveteljük, hogy a felsőbb CRL az alsóra is vonatkozzon ?



Miért OCSP?

- OCSP segítségével az ellenőrzés azonnal elvégezhető, így megoldható, hogy minden visszavonási információ közel egy időpontból származzon.
- Ekkor **sokkal** egyszerűbb problémával állunk szemben.
- Döntés: Az aláírásokat OCSP alapon ellenőrizzük.
- HSZ kulcs kompromittálódás – felelősségi problémák
- Döntés: Induláskor kizárólag az általunk kibocsátott tanúsítványokat fogadjuk el, ezt később kiterjesztjük más „OCSP-s” hitelesítés szolgáltatókra is.
- A közigazgatási, „KGYHSZ-es” tanúsítványokra elvileg sem lehet (értelmesen) archiválás szolgáltatást nyújtani (3/2005 IHM r. ↔ KGYHSZ hitelesítési rend ☺)

Értelmezhetőség, megjeleníthetőség

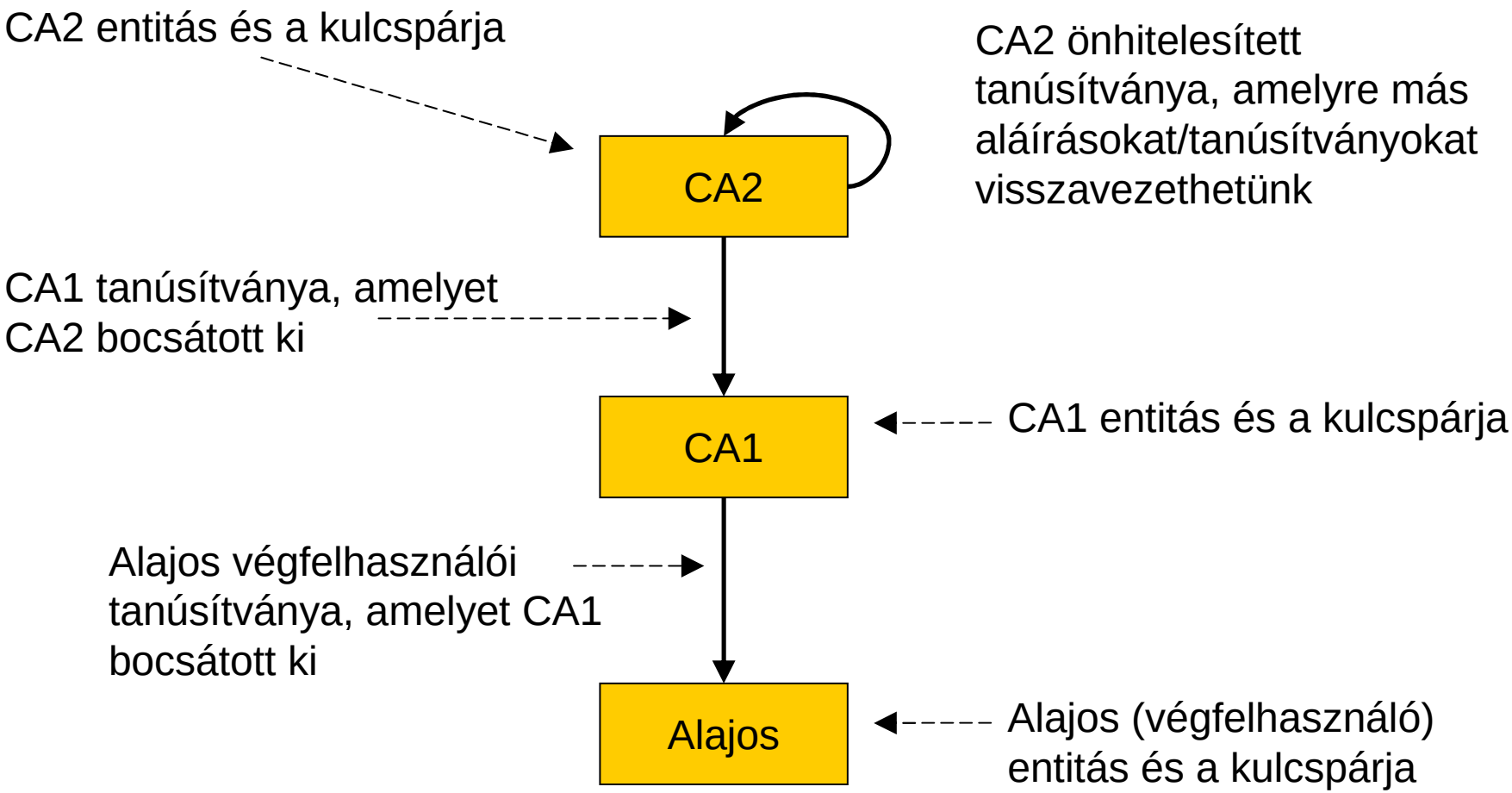
- Aláírás: kötelezettségvállalás valamely értelmes tartalom iránt.
- Az értelmes tartalom egy fájlban (pl. doc, pdf) helyezkedik el.
- Előfordulhat, hogy (pl. 20-30 évvel) később nem lehet majd megjeleníteni a ma használt fájlformátumokat...
- Hiába igazoljuk, hogy milyen bitsorozatot írt alá valaki, az értelmes tartalmat kellene igazolnunk.
- Megjelenítés hitelessége (!)
- Aktív tartalom, makrók (!)

Összegzés

- Az elektronikusan aláírt dokumentumokat speciális körülmények között kell archiválni.
- Az archiválás bonyolult feladat, jelentős szaktudás és drága infrastruktúra szükséges hozzá.
- A minősített archiválás szolgáltató ezeket egységesen, professzionális módon oldja meg:
  - az archiválás szolgáltató anyagi felelősséget vállal azért, hogy az ügyfél iratai megmaradnak és hitelesek;
  - az ügyfél igazolhatja, hogy kellő gondossággal járt el;
  - a bíróságnak vélelmeznie kell, hogy a minősített archiválás szolgáltató által archivált aláírás érvényes („házi” megoldás esetén nincs ilyen jogkövetkezmény);
  - biztosíthat megjeleníthetőséget, értelmezhetőséget.

Kereszthitelesítés

Jelölések


CA2 entitás és a kulcspárja
CA2 önhitelesített tanúsítványa, amelyre más aláírásokat/tanúsítványokat visszavezethetünk
CA2
CA1 tanúsítványa, amelyet CA2 bocsátott ki
CA1
CA1 entitás és a kulcspárja
Alajos végfelhasználói tanúsítványa, amelyet CA1 bocsátott ki
Alajos
Alajos (végfelhasználó) entitás és a kulcspárja

„Root CA”

- A tanúsítványok hitelességét a root CA-ra vezetjük vissza.
- Nincsen a világon egyetlen közös root.
- Az egyes felhasználói közösségek saját gyökerekkel (egy vagy több gyökérrel) rendelkeznek:
  - Magyar Közigazgatás (KGYHSZ, www.kgyhsz.gov.hu),
  - Az egyes kereskedelmi HSZ-ek felhasználói,
  - e-Cégeljárás (Microsec, Netlock),
  - EU tagállamok útleveleit kibocsátó rendszerek,
  - Windows felhasználók,
  - Nemzetközi bankok, multik felhasználói,
  - NATO
  - stb.

Mitől „root”?

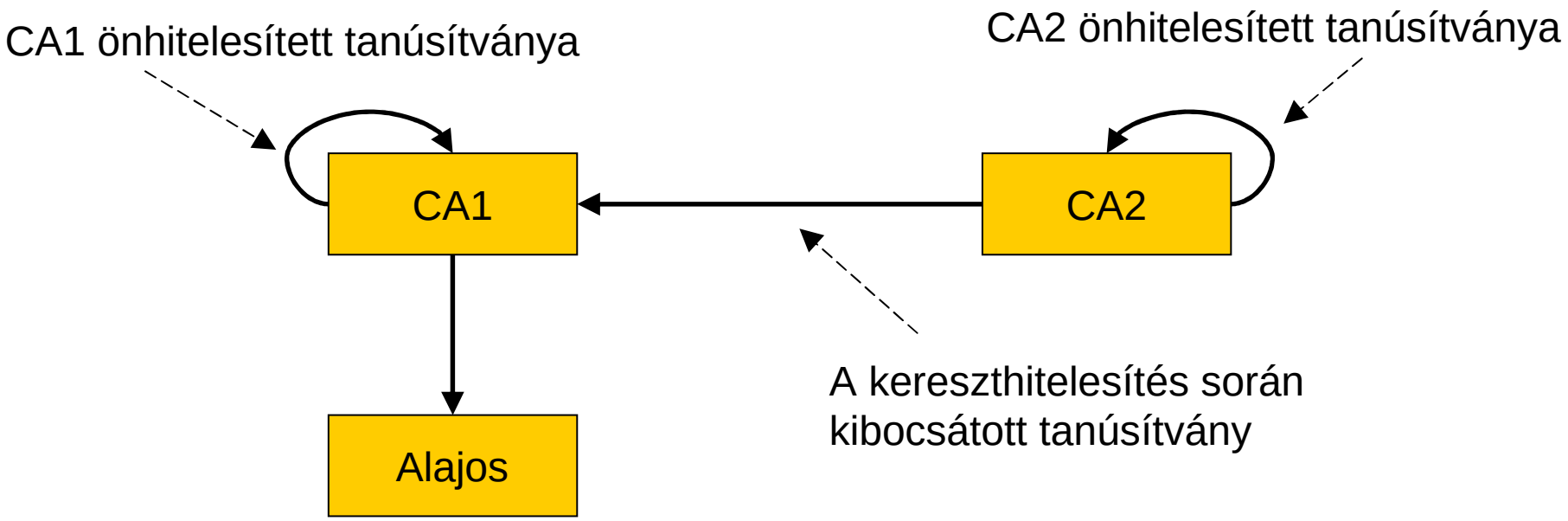
- Önhitelesített tanúsítványa van?
- Használatát jogszabály írja elő?
- Biztonságosan tárolja/kezeli a magánkulcsát?
- A felhasználók megbíznak benne?
- Könnyű rá visszavezetni tanúsítványokat, és ellenőrizni a visszavonási állapotot (pl. OCSP-vel)?
- Felelősséget vállal a tevékenységéért?
- Felelősséget vállal mindenért, amit rá vissza lehet vezetni?
- Elterjedt, és sokan ismerik a nyilvános kulcsát?
- Nagy közösség vezet vissza rá tanúsítványokat?

PKI közösségek összekapcsolása

- Külön PKI közösség - külön root
- Azt szeretnénk, ha az egyik közösség elfogadhatná a másik tanúsítványait
- Láncolja maga alá a root az elfogadott közösségek elfogadott CA-it!

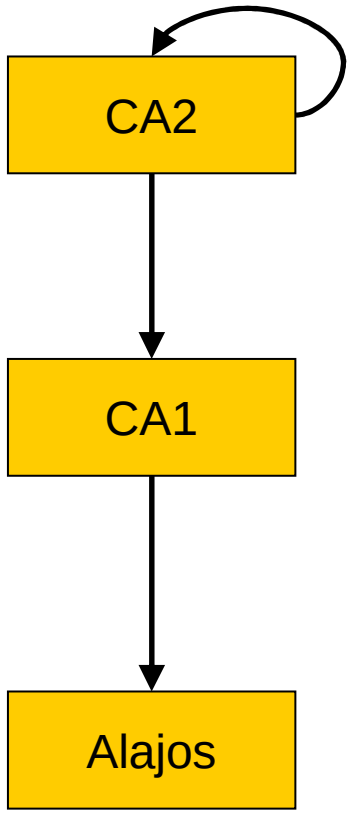
Kereszthitelesítés

- Def: Egy CA egy másik CA számára bocsát ki (CA) tanúsítványt.



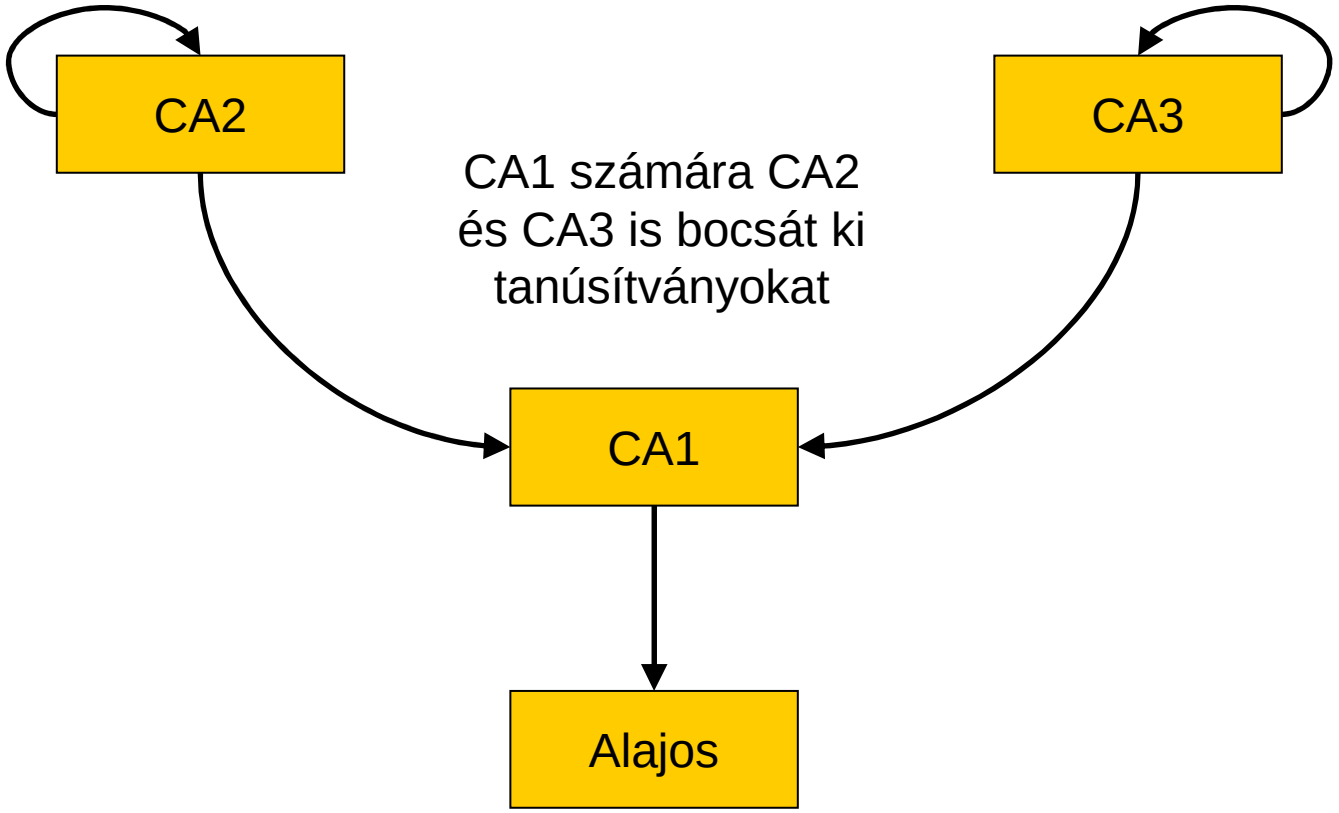
Más, ennél szűkebb/tágabb definíciók is vannak.

Jogi szempontból…



- CA2 felelős CA1 működéséért?
- CA2 azért felelős, hogy CA1 kulcsa CA1 birtokában van?
- CA2 csak részben felelős CA1 működéséért?
- És ha CA1 is tekinthető rootnak?
- Az érintett fél meg kell, hogy bízzon a teljes lánc minden egyes elemében?
- …akkor mire jó ez az egész?

Elágazó tanúsítványlánc

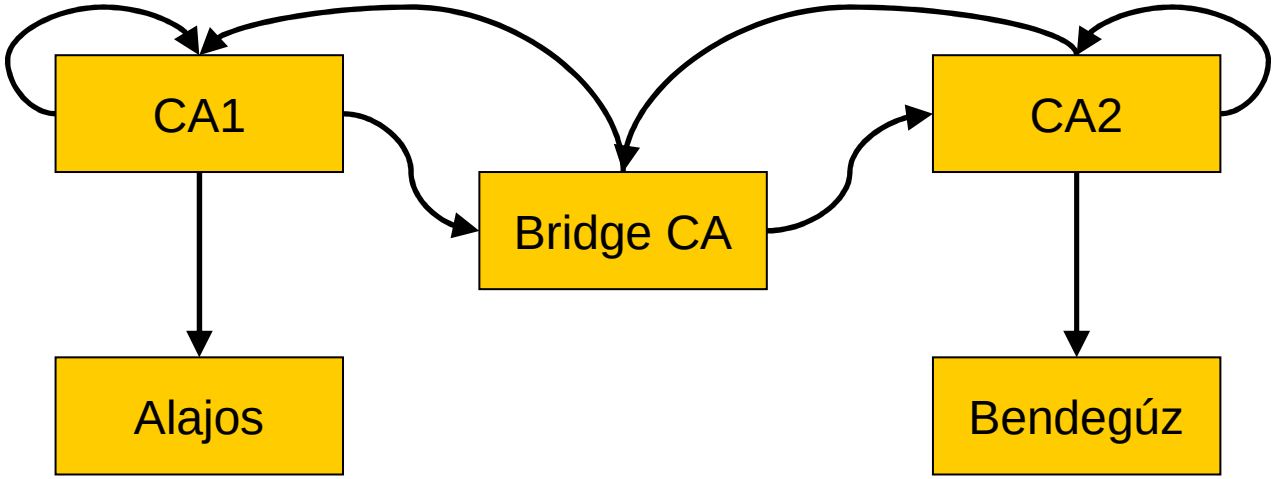


Kölcsönös kereszthitelesítés

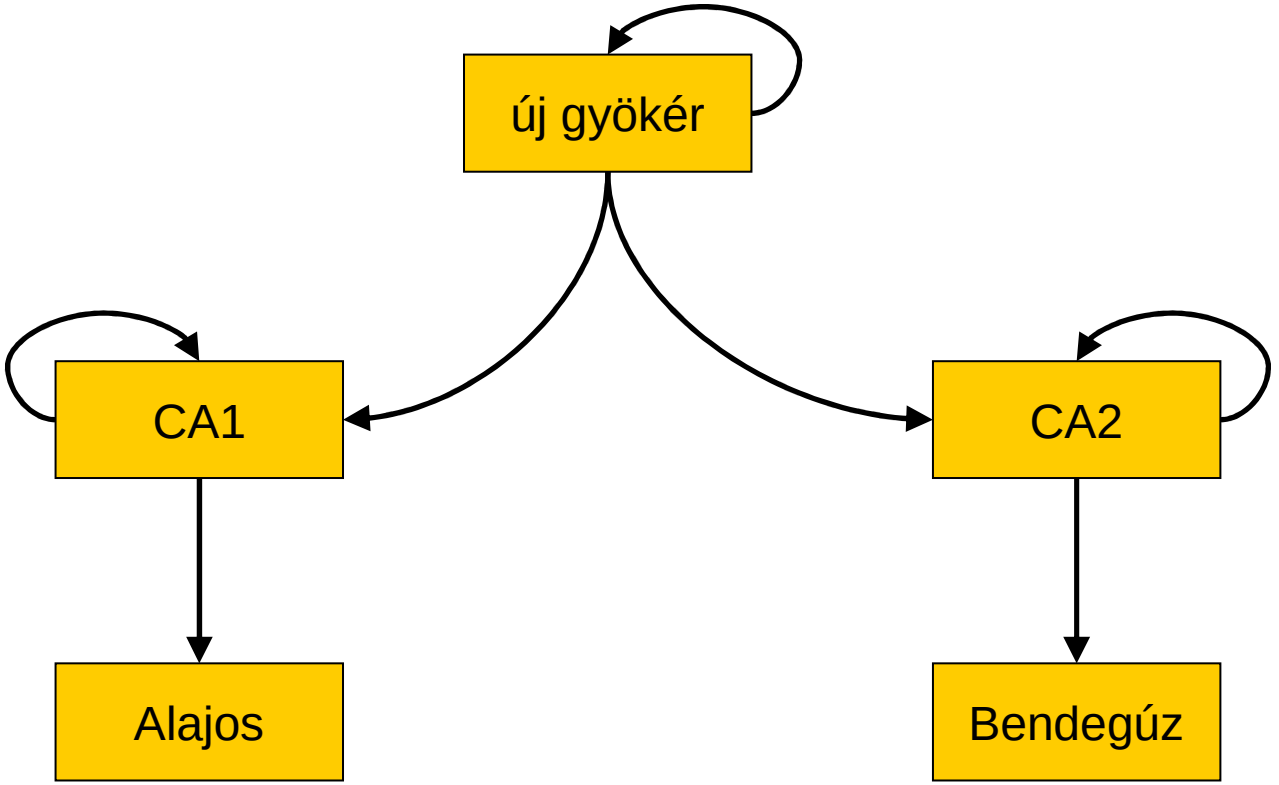
Mindkét végfelhasználó tanúsítványa elfogadható mindkét root alapján.

Bridge CA

Mindkét végfelhasználó tanúsítványa elfogadható mindkét root alapján.



Új gyökér



És ki működteti a gyökeret???

Kérdések

- Melyik tanúsítványlánc az igazi?
- Mi történik, ha az egyik tanúsítványlánc megszakad?
- Egy tanúsítvány és egy aláírás egyszerre lehet érvényes és érvénytelen?

Válaszok

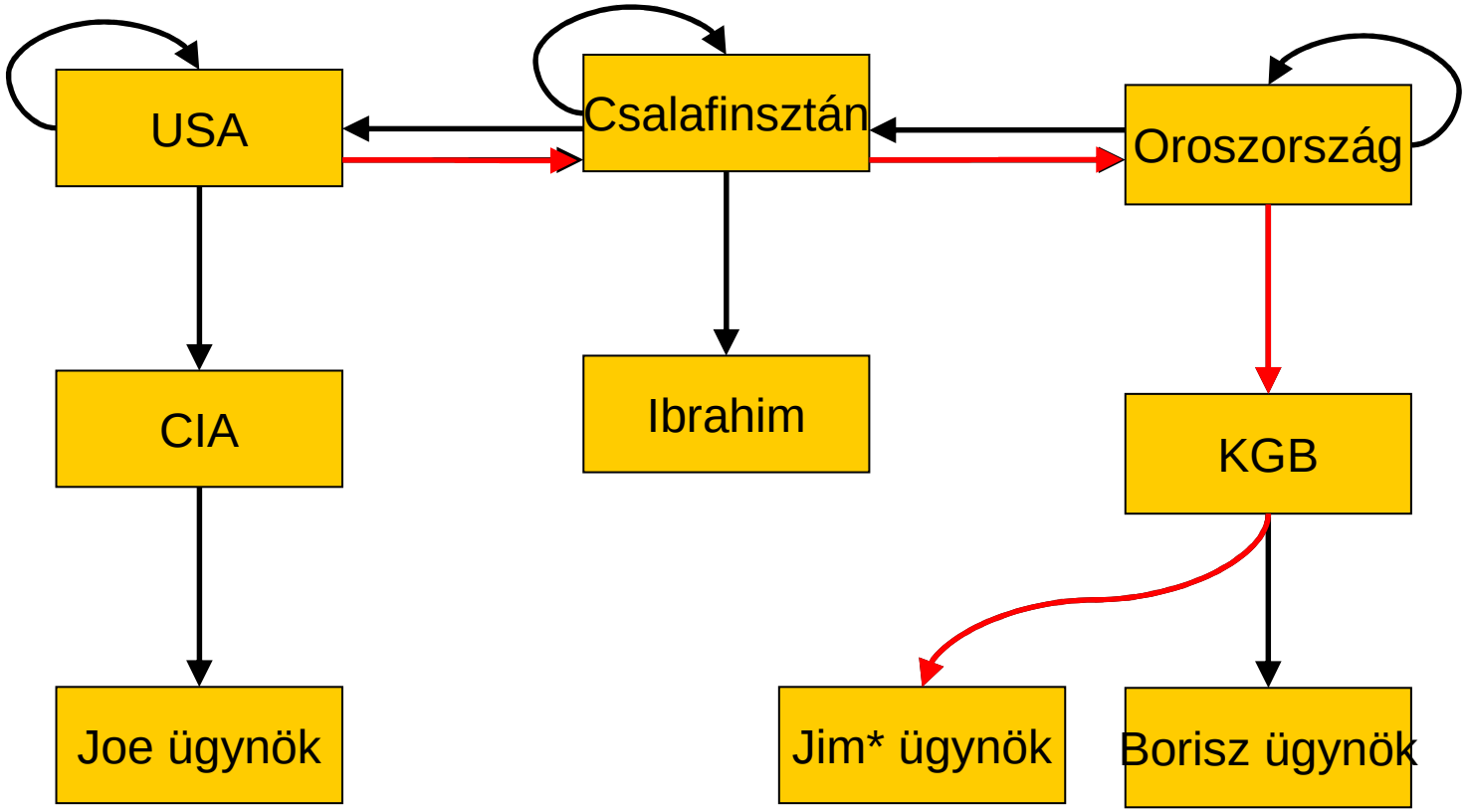
- Az ellenőrzés valamilyen signature policy szerint történik
  - root-ok,
  - visszavonási állapot ellenőrzés,
  - képviseleti jogosultság,
  - időbélyegek
  - stb.
- A policy szerint nem elfogadott root-okra és a csak rájuk visszavezethető tanúsítványokra úgy kell tekinteni, hogy azok nem léteznek.

- **Nem objektív, hogy egy aláírás érvényes-e. E kérdés csak a konkrét policy kontextusában válaszolható meg.**

Problémák

- Nem találjuk meg a szükséges láncot
  - hibás vagy rosszul konfigurált alkalmazás
- Nem szándékolt láncot találunk
  - rosszul konfigurált alkalmazás

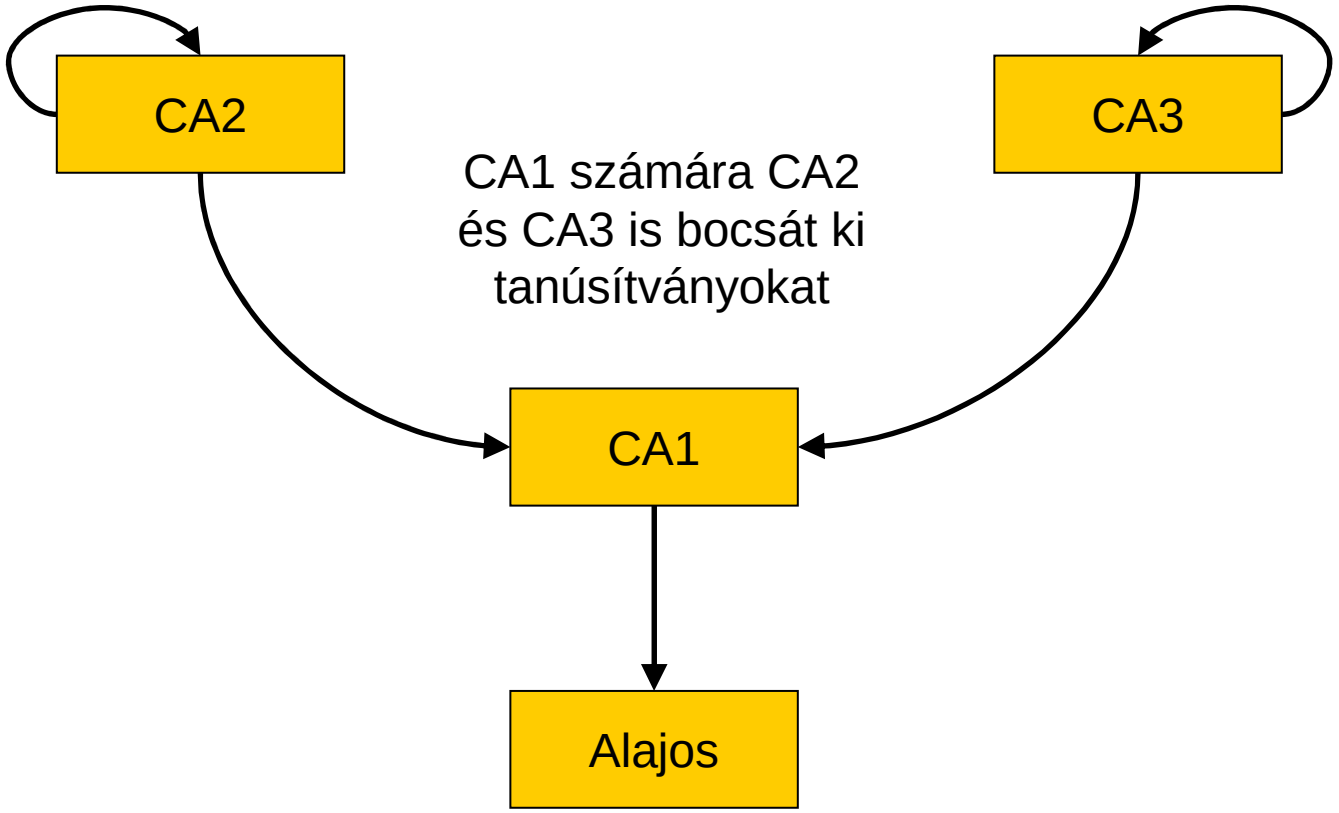
Példa


USA
Csalafinsztán
Oroszország
CIA
Ibrahim
KGB
Joe ügynök
Jim* ügynök
Borisz ügynök

Megoldások

- CP-k használata, ellenőrzése,
- BasicConstraints, PathLenghtConstraints
- PolicyConstraints, NamingConstraints használata
- ...
- JÓ ELLENŐRZŐ-ALKALMAZÁST KELL HASZNÁLNI!

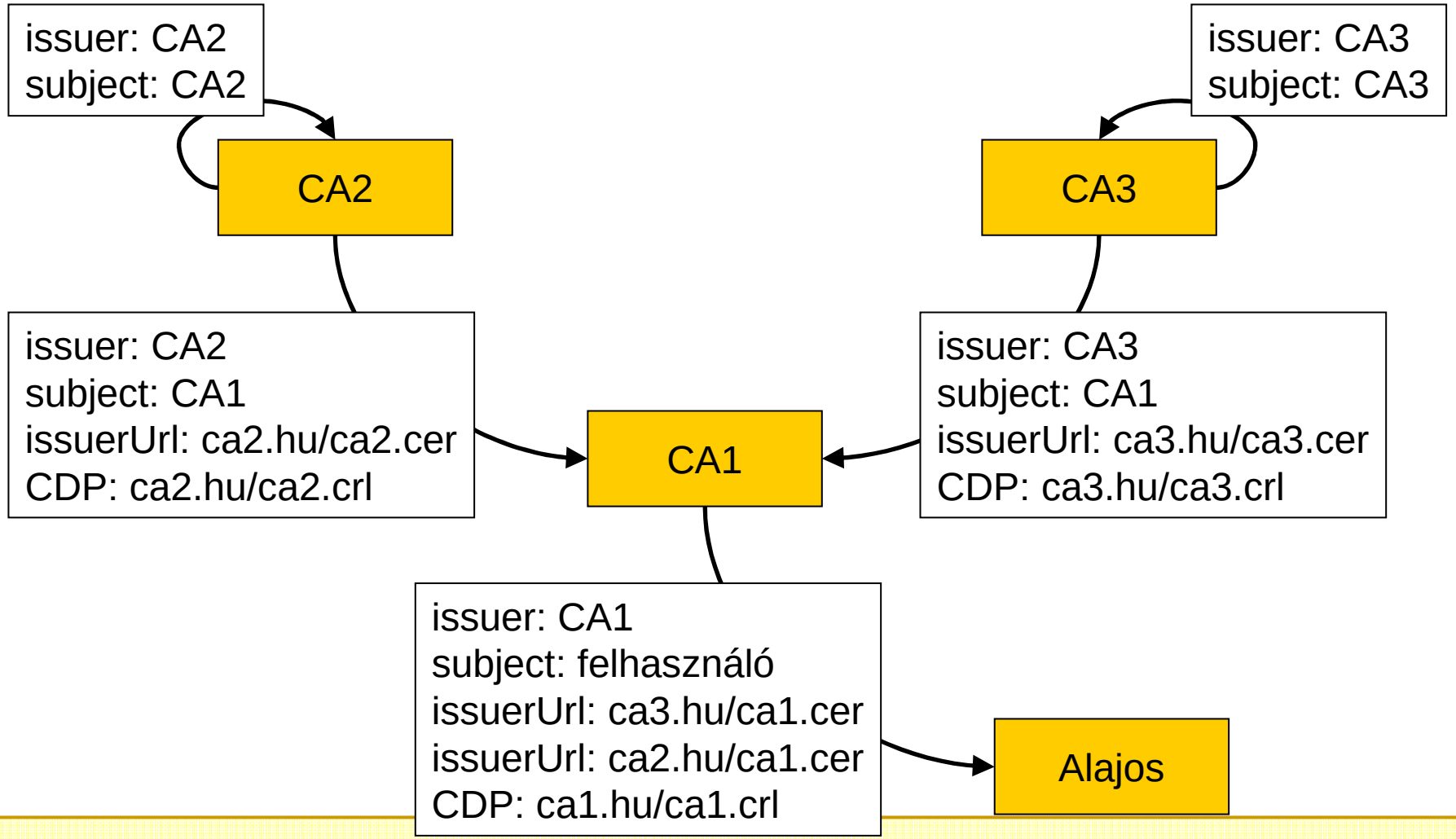
Elágazó tanúsítványlánc



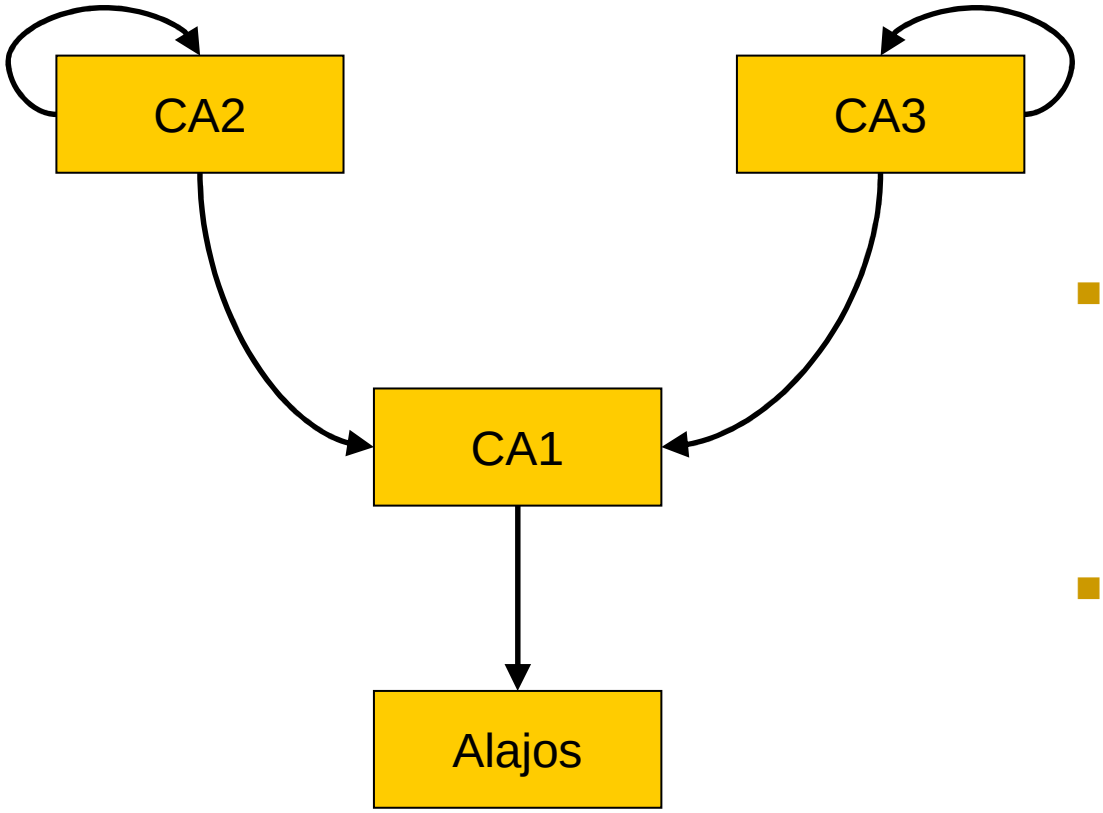
Tanúsítványok visszavezetése

- CA1 tanúsítványa akkor ellenőrizhető CA3 tanúsítványa alapján, ha
  - CA1 tanúsítványa CA tanúsítvány (basicConstraints, certSign KU)
  - CA3 aláírása érvényes CA1 tanúsítványán
  - CA3 vonatkozó hitelesítési rendje ezt nem tiltja
  - CA1.cer/IssuerDN = CA3.cer/SubjectDN
  - Azonos SubjectDN kell, hogy szerepeljen CA1 tanúsítványaiban
  - Kódolás: Azonos szöveg különböző kódolásokkal (pl. UTF-8, ISO8859-2) azonosnak tekinthet-e? Hogyan kell komparálni két különböző kódolású szöveget?

Elágazó tanúsítványlánc

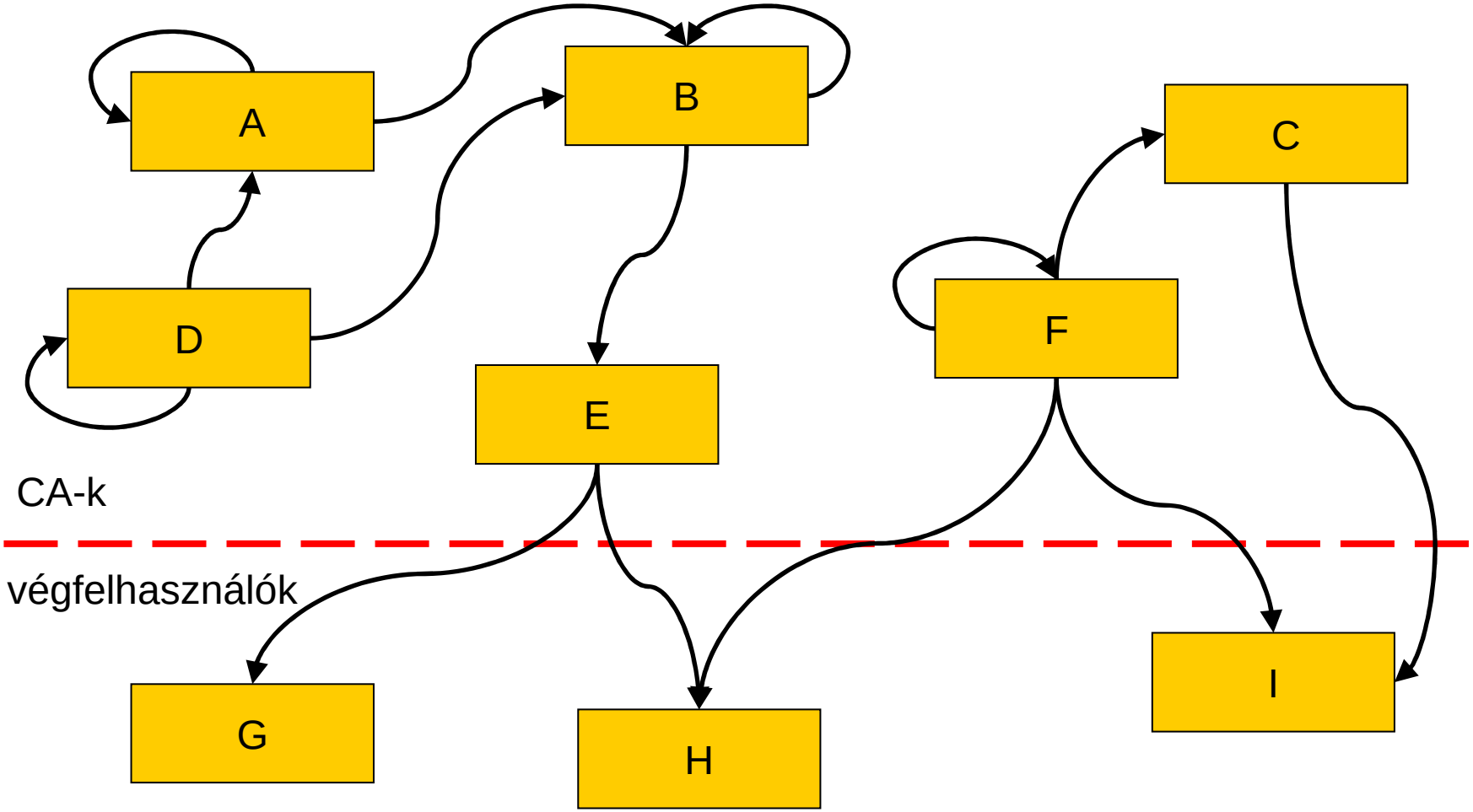


Együttműködés a CA-k részéről

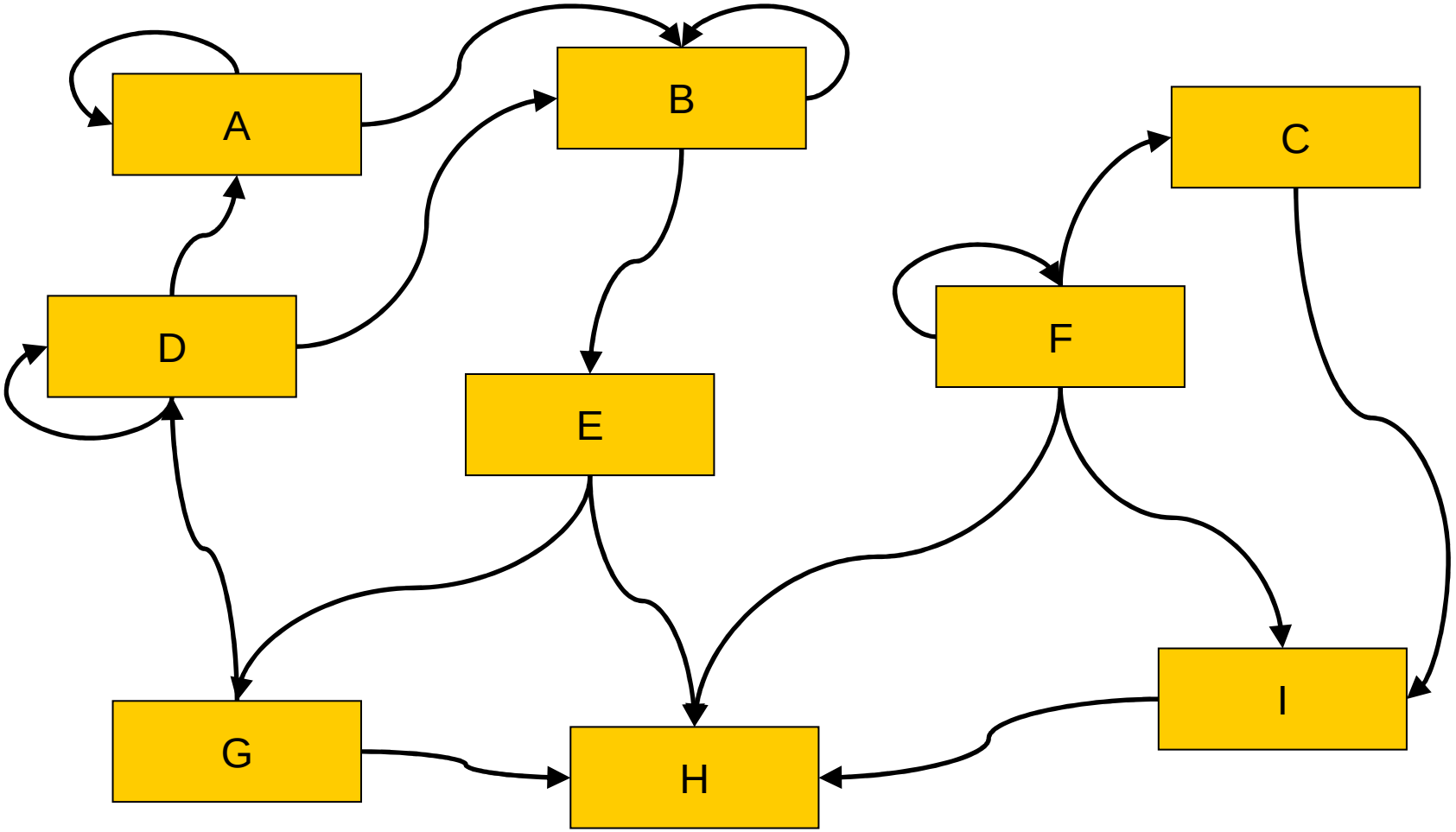


- CA2 nem feltétlenül tud róla, hogy CA1 számára CA3 is bocsátott ki tanúsítványt.
- Sőt, CA1 sem feltétlenül tud róla, hogy több helyről van tanúsítványa.
- CA tanúsítvány: nyilatkozat arról, hogy megbízom az adott CA-ban.

PKI modell



PGP modell



PKI ↔ PGP

- PKI estén egyes entitások hitelesítés szolgáltatók, ők jogosultak tanúsítványt kibocsátani.
- PGP esetén nincs ilyen elkülönítés.
- PKI esetén egyértelmű(bb) felelősségi viszonyok állapíthatóak meg.
- A PKI jobban kontrollálható, ezért a PGP nehezen rúg labdába egy központosított környezetben.

Összegzés

- Bárki lehet root, akinek önhitelesített tanúsítványa van. Kérdés, hogy ezt más elfogadja-e, használja-e.
- A „fent” és a „lent” szubjektív fogalmak, csak egy adott tanúsítványlánc kontextusában értelmezhetőek.
- Csak azt lehet kontrollálni, hogy valaki kinek bocsát ki tanúsítványt, azt nem, hogy kitől kap.
- Nem objektív, hogy egy tanúsítvány/aláírás érvényes-e. Ez is csak egy adott policy kontextusában lehet objektív.
  (...ha a jó a policy…)

Attribútum tanúsítványok

Attribútum

- Egy tanúsítvány alanyának/aláírójának attribútuma lehet
  - szerepkör,
  - tulajdonság,
  - jogosultság
  - stb.

Tanúsítvány és attribútum kapcsolata

- Implicit kapcsolat
- Az attribútum a tanúsítványban szerepel
  - subject DN (organization? title?)
  - hitelesítési rend
  - máshol (subjectDirectoryAttributes)
- 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 - macerás.
- 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.

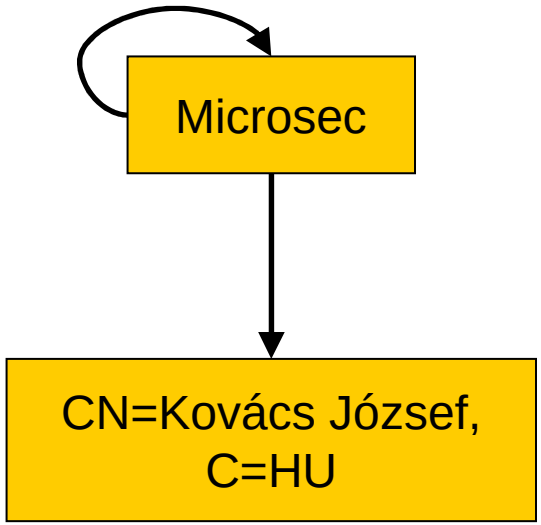
Egyértelmű hivatkozás egy alanyra/tanúsítványra?

Hogy lehet egyértelműen hivatkozni egy alanyra/tanúsítványra?

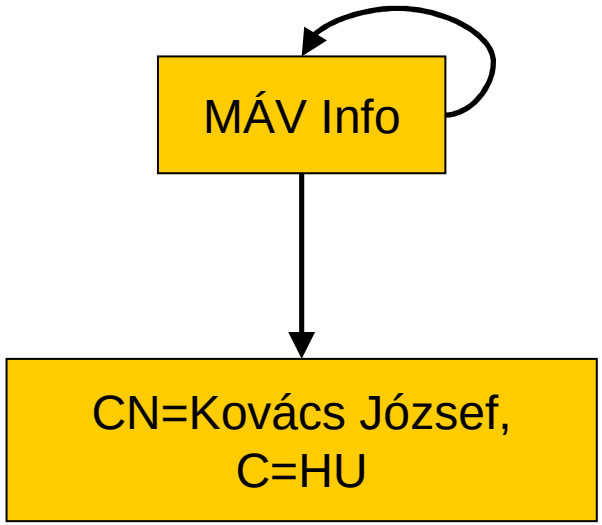
1. Subject Distinguished Name
2. Issuer Distinguished Name + certSerialNumber
3. magával a tanúsítvánnyal vagy annak lenyomatával (esetleg: a nyilvános kulcs lenyomatával)

- Az (1) az alanyra hivatkozik, így a tanúsítvány lecserélése nem zavarja meg. A másik kettő a tanúsítványra hivatkozik, így a visszavonás érinti

Subject DN → alany



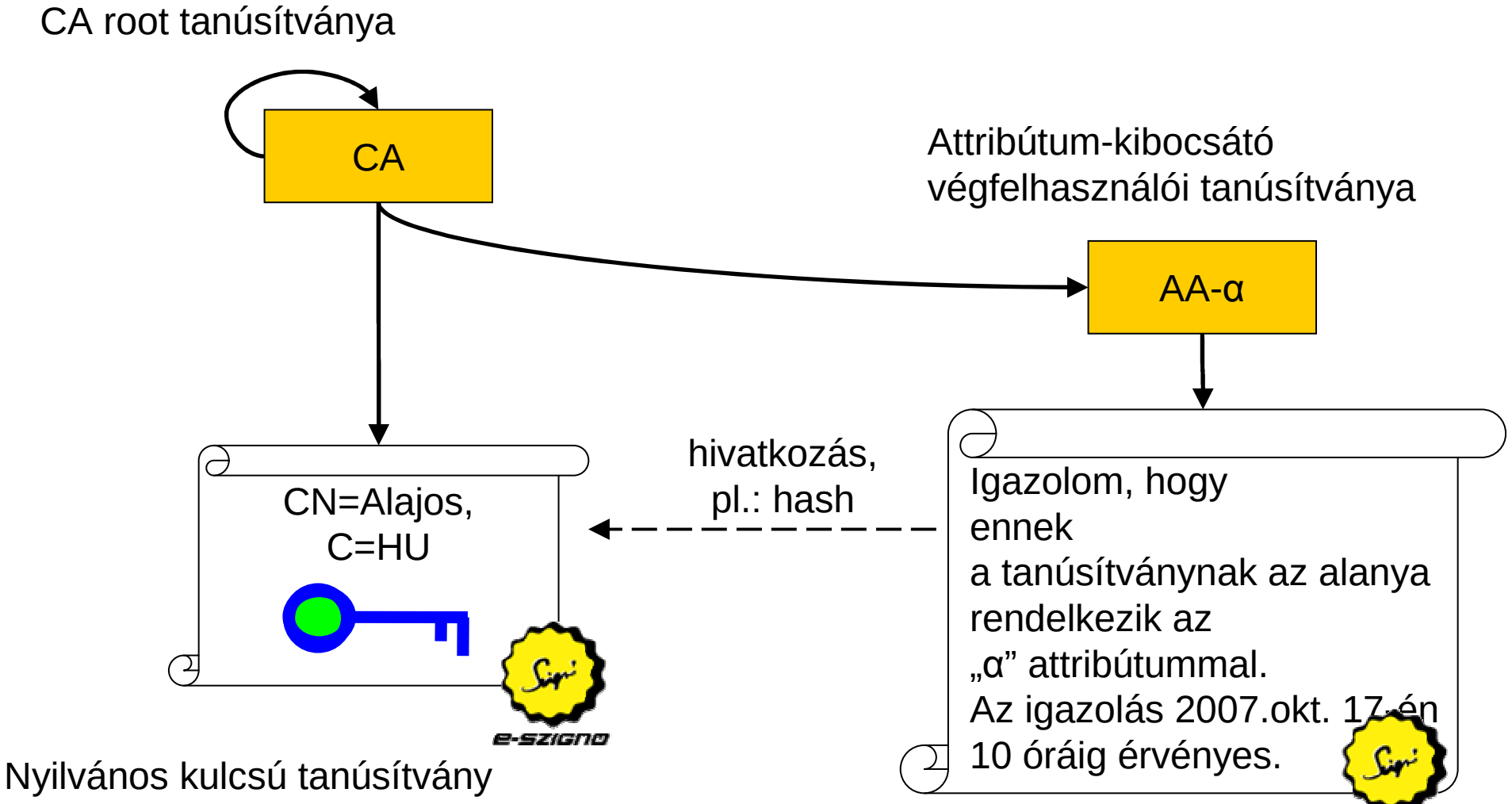
Anyja neve: Nagy Margit,
Szül. id: 1963. január 2.



Anyja neve: Tóth Izabella,
Szül. id: 1997. december 1.

A DN csak CA-n belül egyedi, globálisan nem az, így heterogén rendszerben nem egyedi hivatkozás.
Ugyanez igaz az issuerDN+certSerialNumber megoldásra
↔ X.509...?

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

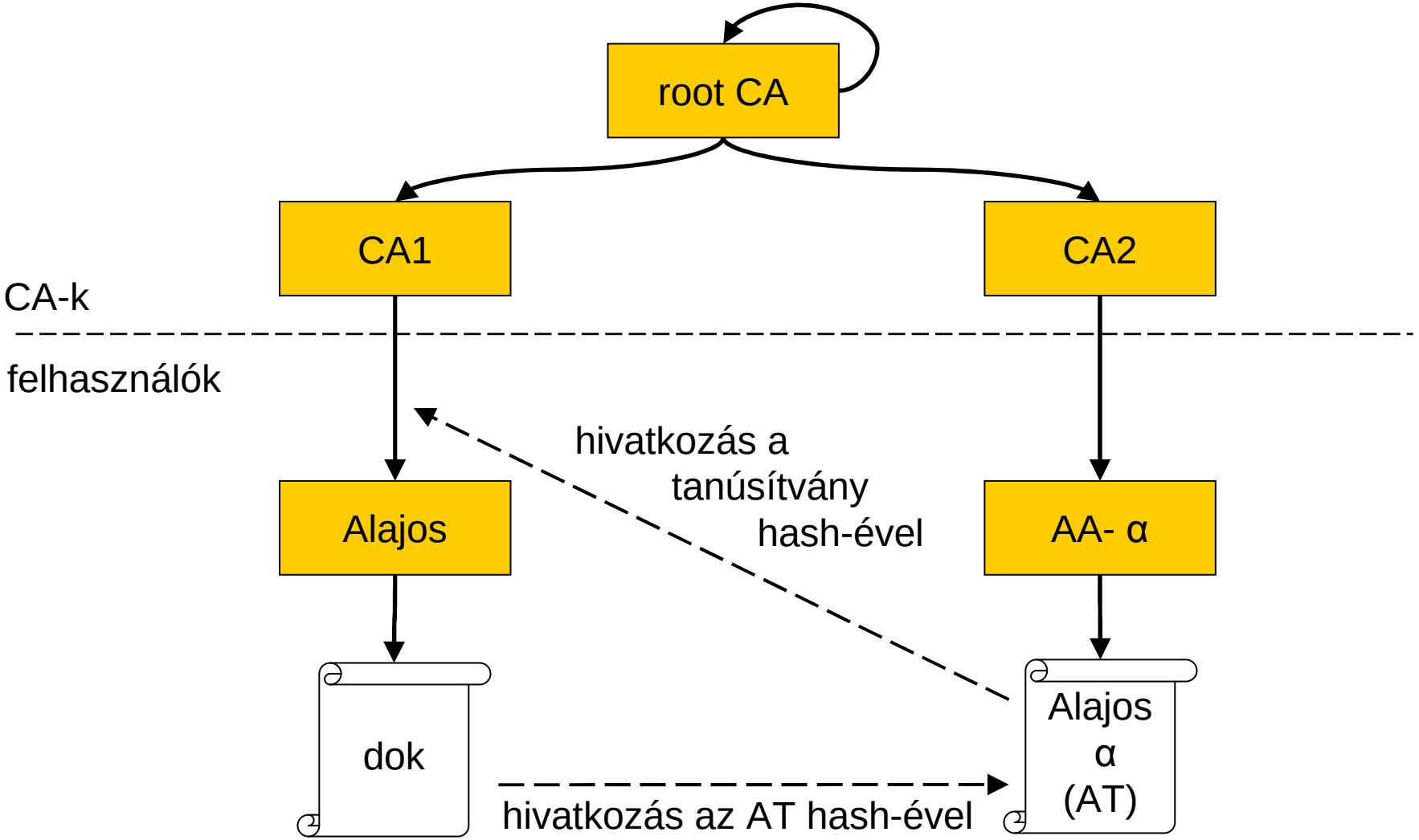
AA tanúsítványa

- Hogyan ismerhető fel az AA tanúsítványa?
- Az érintett felek „ismerik”? - skálázhatóság
- Dedikált AA-root?
- Spec. hitelesítési rend?
- Honnan lehet tudni, hogy az AA mely attribútum(ok) tanúsítására jogosult?
- Hogyan történik mindez papír alapon?

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... ☺

AT felépítése (ez is X.509)

- Kötelez mezők
  - Version
  - Holder (3 féle módon hivatkozhat)
  - Issuer (DN)
  - Signature
  - Serial Number
  - Attributes
  - …
- Lehetséges kiterjesztések
  - CRL distribution point
  - No Revocation Available
  - Authority Information Access
- …

Hogyan jelenik meg az attribútum?

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

Hol használnak attribútum tanúsítványt?

- Kevesen 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.

Összegzés

- Sok hátránya van annak, hogy az attribútumok a nyilvános kulcsú tanúsítványban szerepeljenek
  - attribútumok és tanúsítványok eltér 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! ☺