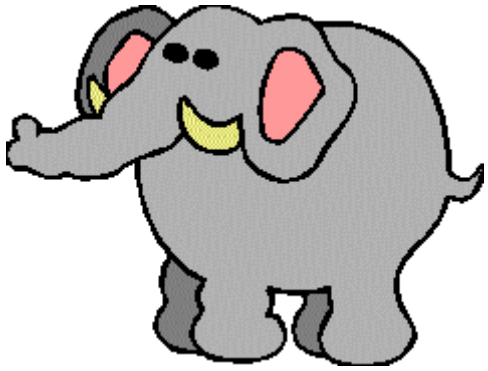
A PKI gyakorlati problémái

BERTA István Zsolt
<istvan.berta@microsec.hu>

Elefánt



- Műszaki kérdések
- Gazdasági kérdések
- Jogi kérdések

Miről fogok beszélni?

- Rövid összefoglalás a PKI-ről
- Hazai helyzet
- Műszaki + gazdasági + jogi aspektus
- Gyakorlati problémák

Bevezetés a PKI-ről

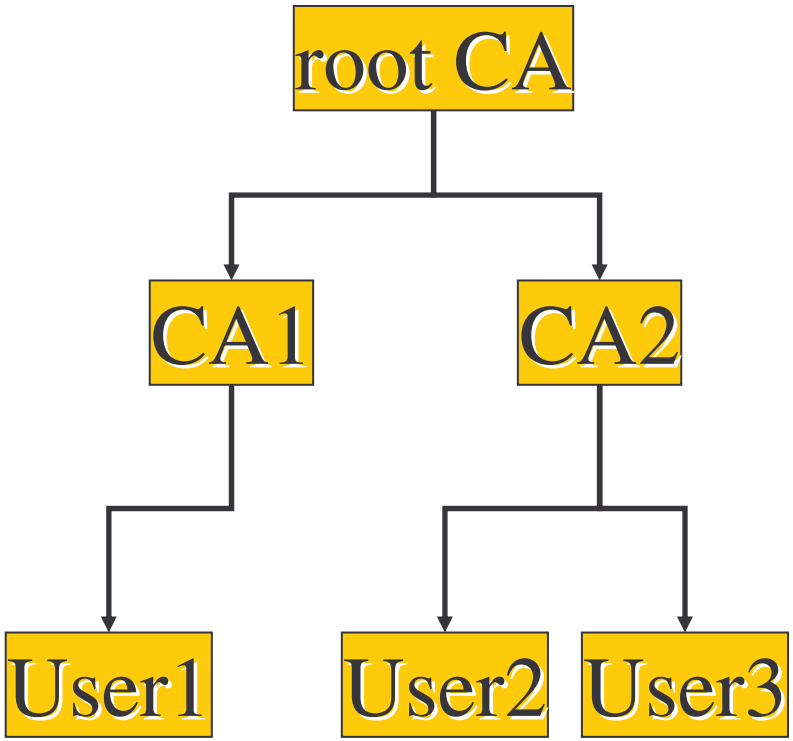
PKI dióhéjban (1)

- Minden résztvevőnek van két kulcsa:
  →**magánkulcs** (csak ő ismeri)
  →**nyilvános kulcs** (bárki megismerheti)
- Ha magánkulcsunkkal kódolunk valamit, a nyilvános kulcsunkkal bárki ellenőrizheti, hogy a kódolást mi végeztük el. Ezt nevezzük **aláírás**nak, hitelesítésnek.
- Ha egy nyilvános kulccsal kódolunk valamit, azt kizárólag a hozzá tartozó magánkulccsal lehet visszafejteni. Ezt nevezzük **titkosítás**nak.
- Csak akkor támaszkodhatunk egy nyilvános kulcsra, ha tudjuk, hogy ki birtokolja a hozzá tartozó magánkulcsot.

PKI dióhéjban (2)

- A **hitelesítés szolgáltató**k olyan szereplők, akik aláírt igazolásokat állítanak ki arról, hogy egy adott nyilvános kulcs (és a hozzá tartozó magánkulcs) kihez tartozik. Ezen aláírt igazolásokat nevezzük **tanúsítvány**nak.
- A tanúsítványokat általában más tanúsítványok alapján ellenőrizhetjük, az ellenőrzést **gyökér** hitelesítés szolgáltatók nyilvános kulcsára vezethetjük vissza; e kulcsokat sokan ismerik és elfogadják.
- Az **időbélyegzés szolgáltató**k olyan aláírt igazolásokat bocsátanak ki arról, hogy egy adott dokumentum egy adott időpontban létezett.
- Jogszabály **bizonyító erő**t rendel
  → a minősített és a fokozott biztonságú aláírásokhoz és
  → a minősített időbélyegekhez.

CA-hierarchia



Mi az a CA?

- Szervezet/vállalat?
- Szervezeti egység?
- Számítógép?
- Domain név?
- Fizikai eszközök összessége?
- Tanúsítvány?
- Kulcspár?

Mivel foglalkozik egy CA?

- A CA azonosítja, regisztrálja a felhasználót…
- Tanúsítványt bocsát ki a számára…
- Nyilvánosságra hozza a tanúsítványokat*…
- Nyilvánosságra hozza, ha a felhasználó visszavonja a tanúsítványt…
- Garanciát vállal (a saját működésére).
- Cserébe rendszeres (pl. éves) díjat kap a felhasználóktól

Hazai helyzet

Hazai piac

- Szabályozott piac, a Nemzeti Hírközlési Hatóság felügyeli a szolgáltatók működését
- Négy kereskedelmi hitelesítés szolgáltató működik Magyarországon:
  - →Microsec, www.e-szigno.hu
  - →Magyar Telekom, eszigno.t-systems.magyartelekom.hu
  - →Máv Informatika, www.mavinformatika.hu/ca
  - →Netlock, www.netlock.hu

  - →Educatio Kht. (csak fokozott)
  - →(+GIRO www.giro.hu)
  - →(+IHM biztonsági HSZ)
  - →(+KGYHSZ)

Mire lehet használni elektronikus aláírást?

- e-Cégeljárás
  - →cégalapítás (2008. július 1-től kizárólag elektronikusan),
  - →cég mérlegének benyújtása,
  - →hatóságok egymás közti kommunikációja.
- Minden magyar közjegyző - archiválás
- PSZÁF - pénzintézetek adatszolgáltatása
- OEP - adatszolgáltatás
- Számlázás (Pl: Díjbeszedő, Malév, Vatera stb.)
- Bankszámlakivonatok (pl: Budapest Bank)
- Adatok archiválása
- ((Ügyfélkapu))

Az elektronikus aláírásról szóló törvény (Eat.)

- 2001. évi XXXV. törvény az elektronikus aláírásról (módosítva 2004-ben), 1999/93 EU direktíva
- Az elektronikus aláírásról szól, nem foglalkozik a titkosítással és a kihívás és válasz alapú azonosítással
- Elektronikus aláírással kapcsolatos szolgáltatások
  - →hitelesítés szolgáltatás,
  - →aláírás-létrehozó eszköz szolgáltatás,
  - →időbélyegzés,
  - →archív szolgáltatás
- Megkülönböztet egyszerű, fokozott biztonságú és minősített aláírást. Elsősorban a minősítettet szabályozza
- A tanúsítványban szerepelhet álnév is!

Minősített elektronikus aláírás

- Minősített elektronikus aláírás: olyan - fokozott biztonságú - elektronikus aláírás, amelyet az aláíró **biztonságos aláírás-létrehozó eszközzel** hozott létre, és amelynek hitelesítése céljából **minősített tanúsítványt** bocsátottak ki.
- „Teljes bizonyító erejű magánokirat”
- Minősített aláírást csak természetes személy készíthet!
- A CA aláírása csak fokozott biztonságú lehet!

Minősített CA-ra vonatkozó biztonsági követelmények

- Önálló, független szervezeti egység
- A minősített és nem minősített rendszereket el kell választani egymástól
- Minőségirányítási és információbiztonság-irányítási rendszer
- Folyamatos rendelkezésre állás (99,9%)
- Bizalmi munkakörök
  - →általánosan felelős vezető
  - →biztonsági tisztviselő
  - →regisztrációs tisztviselő
  - →független rendszervizsgáló
  - →rendszeradminisztrátor, rendszerüzemeltető
- Felelősségbiztosítás

CA-k nyilvános dokumentumai

- Hitelesítési rend (Certificate Policy)
- Szolgáltatási szabályzat (Certificate Practica Statement)
- Tartalmazzák:
  - →tanúsítvány ellenőrzésének módját
  - →a tanúsítványok értelmezését
  - →a tanúsítványok kibocsátásával és a kulcskezeléssel kapcsolatos védelmi intézkedéseket
  - →a tanúsítványhoz tartozó felelősségvállalásokat
  - →a szolgáltatások elérhetőségét

Minősített tanúsítványra vonatkozó főbb követelmények

- Kizárólag minősített hitelesítés szolgáltató bocsáthatja ki
- Biztonságos aláírás-létrehozó eszköz (BALE)
- Személyes azonosítás
- Adategyeztetés közhiteles adatbázisokkal
- Felelősségvállalás!

Tranzakciós limit

- Eat. 9 § (1) A hitelesítés szolgáltató a minősített tanúsítványban meghatározhatja a tanúsítvánnyal egy alkalommal vállalható kötelezettség legmagasabb mértékét.
- A tranzakciós limit segítségével a hitelesítés szolgáltató csökkentheti a kockázatát
- Tranzakciós limit – szolgáltatói felelősségvállalás

Tanúsítványok felépítése

Egy tanúsítvány mezői

- Sorozatszám
- Kiállító DN (azaz a CA)
- Érvényesség kezdete, vége
- Tulajdonos DN (a tanúsítvány alanya)
- Tanúsítvány-irányelv (Certificate Policies)
- QCStatement (csak minősített tanúsítványban)
- Tranzakciós limit (csak minősített tanúsítványban)
- Visszavonási információk elérhetősége
- Kulcshasználat (Key Usage)
- Nyilvános kulcs, a CA aláírása, aláíró és hash algoritmusok megnevezése stb.

A tanúsítvány alanyának DN-je

- Az LDAP szerint definiált Distinguished Name
  - →Common Name, Surname, GivenName stb.
  - →Title
  - →Organization, Organization Unit
  - →Locality
  - →Country
  - →Pseudonym
  - →Email Address
  - →Serial Number, Distinguished Name Qualifier stb.
- Álnév kezelése
- Szervezethez tartozás, szervezet képviselete
- Ki illetve mi igazolja az egyes mezők érvényességét?

Key Usage (RFC 3280)

```
KeyUsage ::= BIT STRING {
             digitalSignature        (0),
             nonRepudiation          (1),
             keyEncipherment         (2),
             dataEncipherment        (3),
             keyAgreement            (4),
             keyCertSign             (5),
             cRLSign                 (6),
             encipherOnly            (7),
             decipherOnly            (8) }
```

Certificate Policies

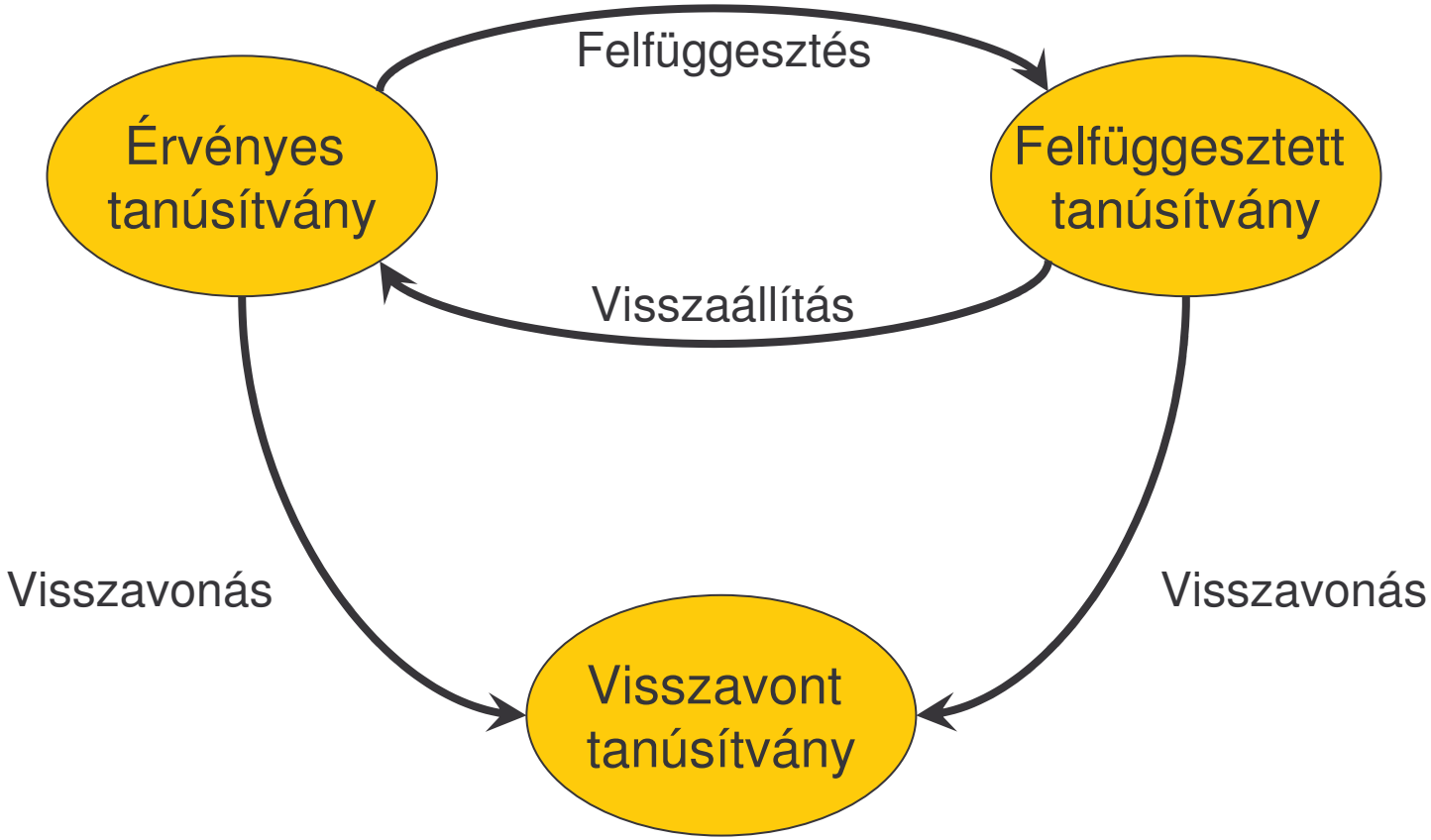
- A hitelesítés szolgáltató hitelesítési rendjére és/vagy szolgáltatási szabályzatára tartalmaz hivatkozást
- Megállapítható belőle, hogy a szolgáltató milyen feltételek mellett bocsátotta ki a tanúsítványt és mekkora felelősséget vállal érte
- QCStatements

CRL és OCSP

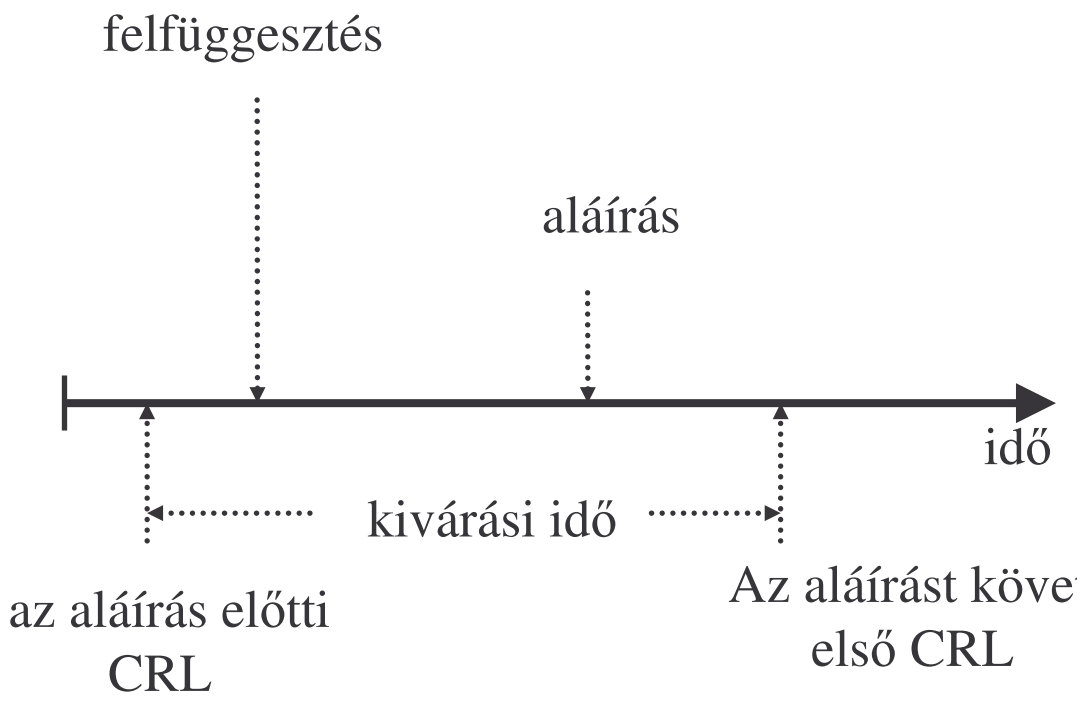
Visszavonási állapot közzététele

- Visszavonási lista (CRL)
  - →A CA által rendszeresen kibocsátott, aláírt lista
  - →Rendkívüli CRL is kibocsátható… Mire jó?
- OCSP – Online Certificate Status Protocol
  - →kérdés: x tanúsítvány érvényes-e
  - →aláírt válasz: igen/nem
  - →lehet úgy használni, hogy friss, pozitív választ adjon ☺
  - →úgy is lehet használni, mint a CRL-t ☹
  - →sokféle implementáció

Felfüggesztés, visszaállítás, visszavonás

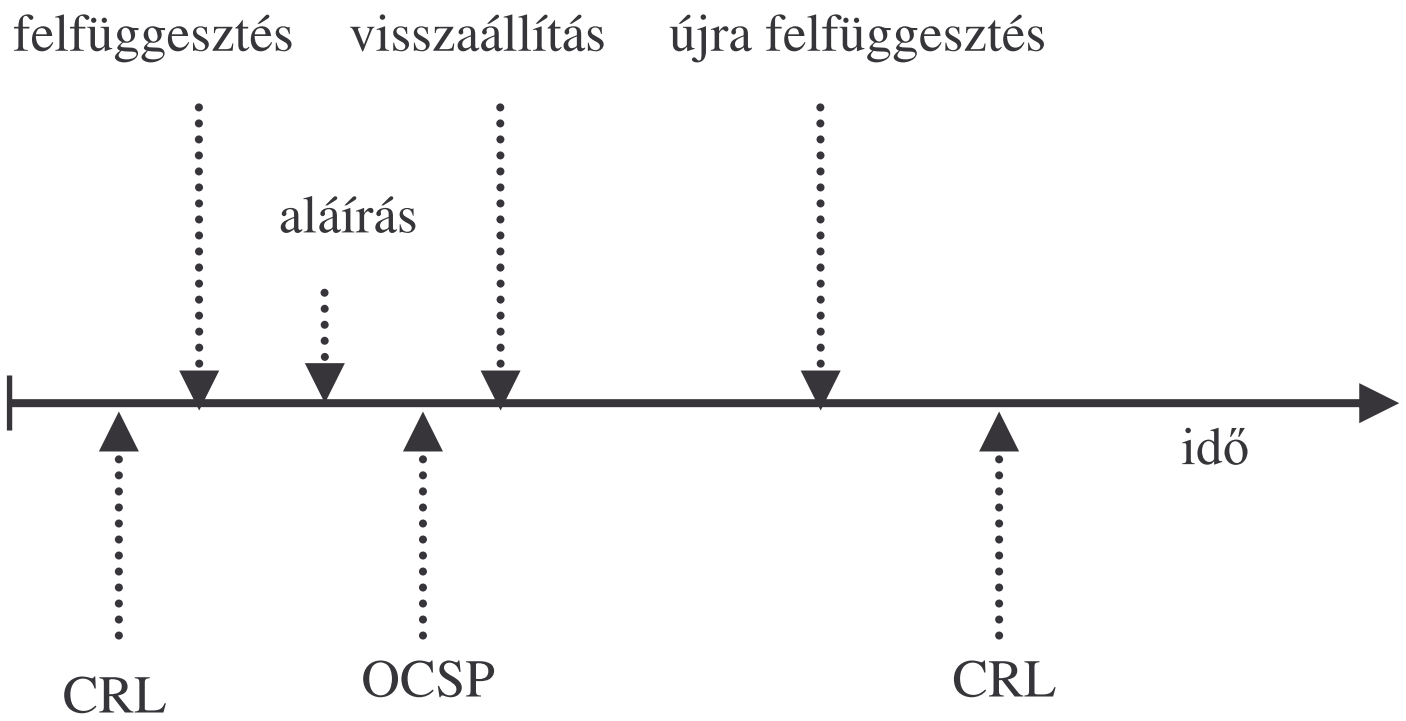


Kivárási idő (grace period)

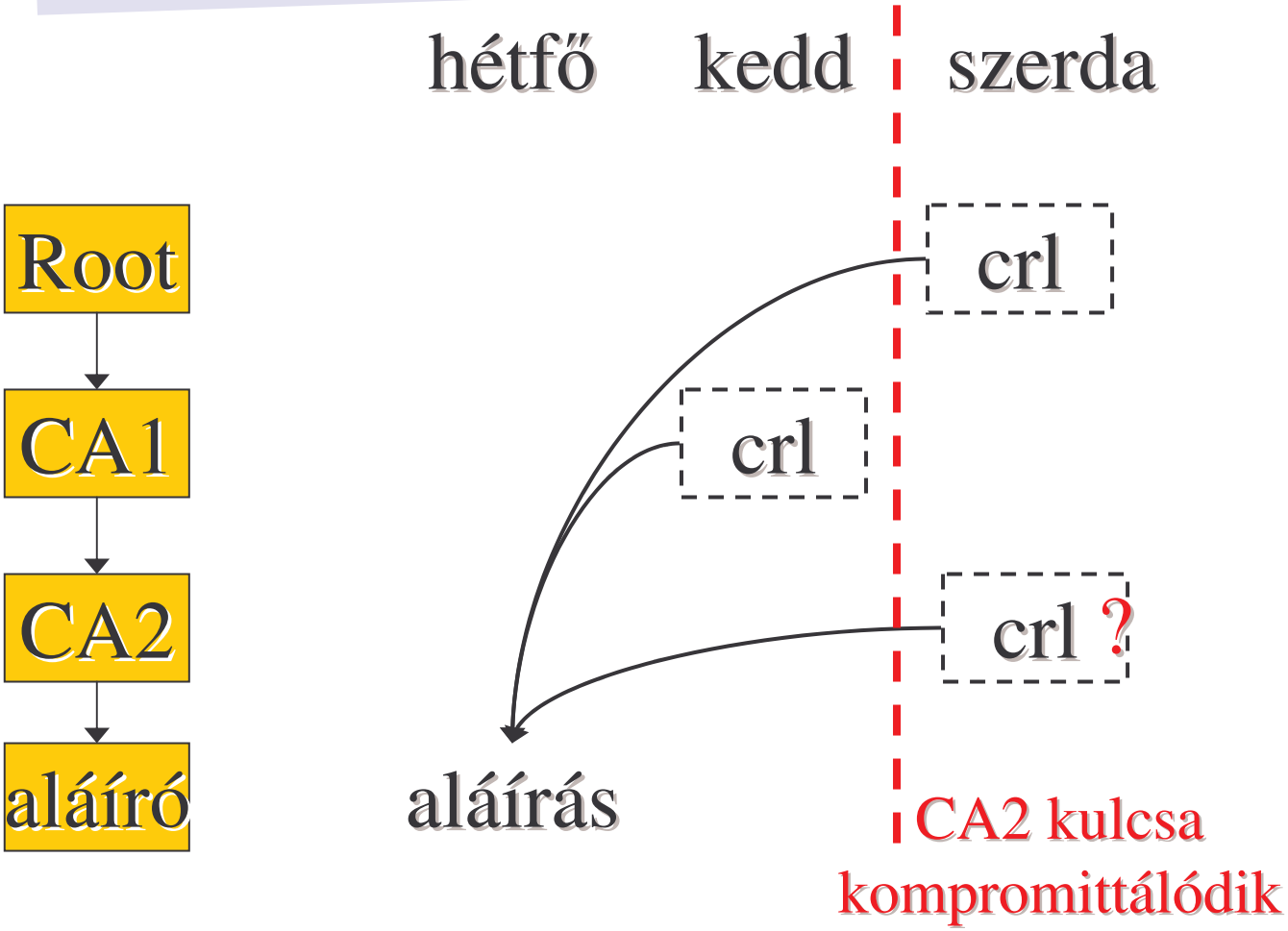


- A következő CRL-t meg kell várni az aláírás ellenőrzéséhez.
- A magyar CA-k általában 24 óránként bocsátanak ki CRL-t.
- Mindezt a tanúsítványlánc minden elemére el kell végezni.
- Mikor ellenőrizhető egy aláírás???

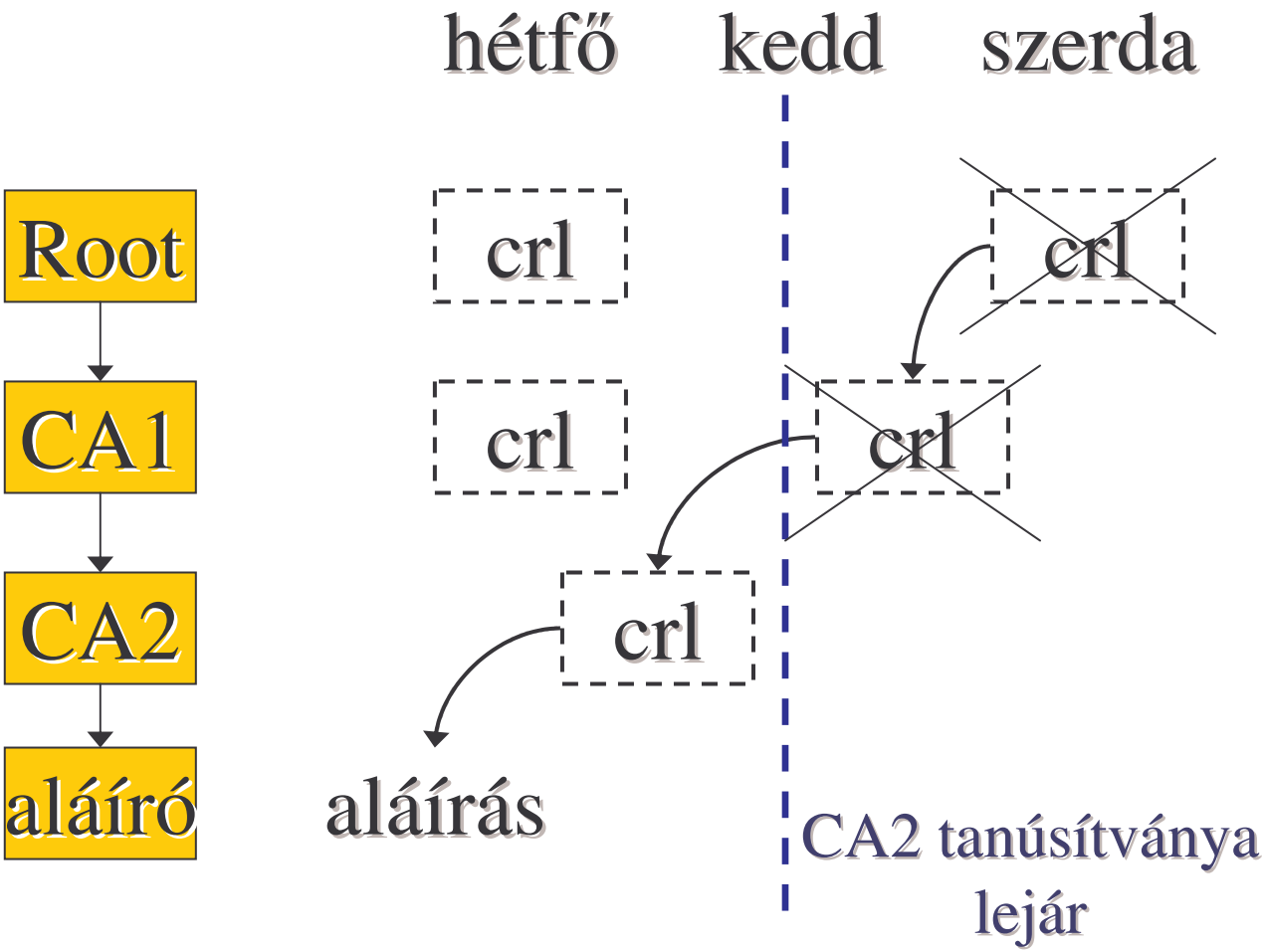
Visszavonás időpontja a CRL-ben



Az aláírást követő CRL-eket követelünk meg ?



Megköveteljük, hogy a felsőbb CRL az alsóra is vonatkozzon ?



Tanulság

- A tanúsítvány érvényességét az aláírás pillanatában kell vizsgálni
- A CRL lehet, hogy csak sokkal később jelenik meg, elképzelhető, hogy a CRL-alapú ellenőrzés nem helyes eredményhez vezet
- A legbiztonságosabb megoldás a tanúsítvány visszavonási állapotát az aláírás pillanatában OCSP segítségével lekérdezni
- OCSP és OCSP között sok különbség lehet
- Minél később ellenőrzünk, annál nehezebb a dolgunk… (?)

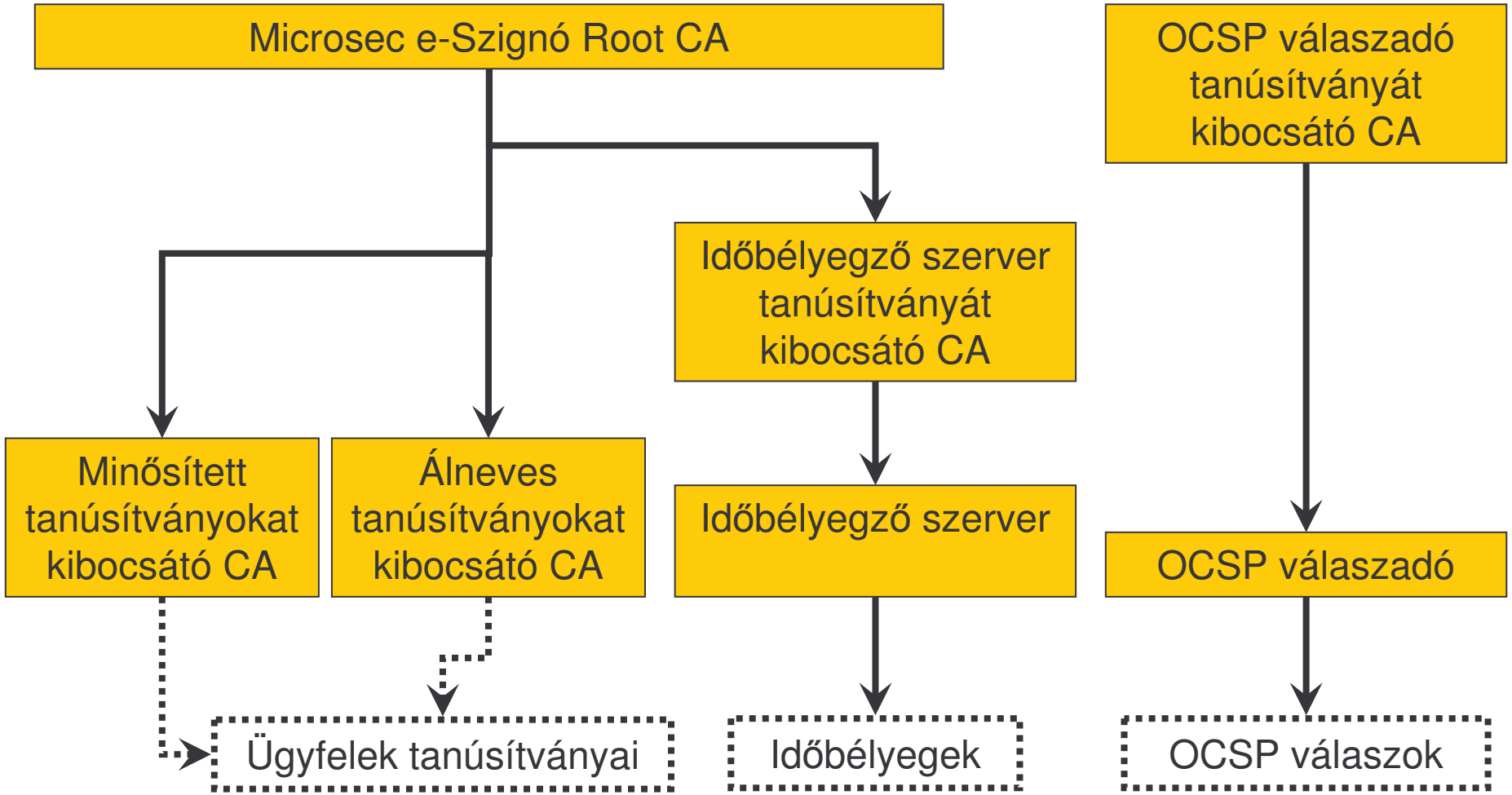
Hogyan ellenőrizzük az OCSP válaszadó tanúsítványát?

- CRL alapján ellenőrizni lassú, annak nincsen értelme.
- OCSP segítségével ellenőrizhetjük, de akkor ki adja a választ?
- Ha nem ellenőrizzük az OCSP válaszadó tanúsítványát, mi történik, ha a válaszadó kulcsa mégis kompromittálódik?

Rövid lejáratú OCSP tanúsítvány

- Az OCSP válaszadó tanúsítványa legfeljebb néhány percig érvényes
- A CA úgy érvényteleníti a kompromittálódott kulcsot, hogy nem ad ki hozzá új tanúsítványt
- A kulcsot megszerző támadó az utolsó tanúsítvány lejárta után nem tud a kulccsal visszaélni
  - → a tanúsítvány már nem érvényes
  - → visszadátumozott időbélyeget nem tud szerezni

Microsec e-Szignó minősített rendszer



Elektronikus aláírás és ellenőrzése

Hogy kell ellenőrizni egy aláírást?

A tanúsítványt kibocsátó hitelesítés szolgáltató által kibocsátott, az adott tanúsítványra vonatkozó hitelesítési rend szerint kell eljárni.

A hitelesítési rendre való hivatkozás megtalálható a tanúsítványban (tanúsítvány irányelv, certificate policies mezők).

Aláírás ellenőrzésének lépései

1. Mi állapítható meg az aláíróról (pl. álnév, képviselet)?
2. Tranzakciós limit ellenőrzése
3. Az aláírás valóban az aláíró tanúsítványához tartozik?
4. Az aláíró tanúsítványa nem járt-e le, vagyis az aláírás időpontja a tanúsítvány érvényességi idején belülre esik? Honnan tudom utólag, hogy mikor történt az aláírás?
5. Ellenőriznie kell a tanúsítvány visszavonási állapotát.
6. A tanúsítványlánc minden elemére el kell végezni a 2., 3. és 4. lépéseket, amíg egy megbízható root tanúsítványhoz (trust anchor) nem jutunk.

Letagadhatatlanság

- Műszaki szempontból létezik letagadhatatlanság, jogi szempontból nem
- Letagadhatatlan az aláírásom, ha
  - →lejárt a tanúsítványom?
  - →nem elérhető a visszavonási információ?

- A minősített aláírásból nem következik, hogy az hosszú távon is letagadhatatlan.

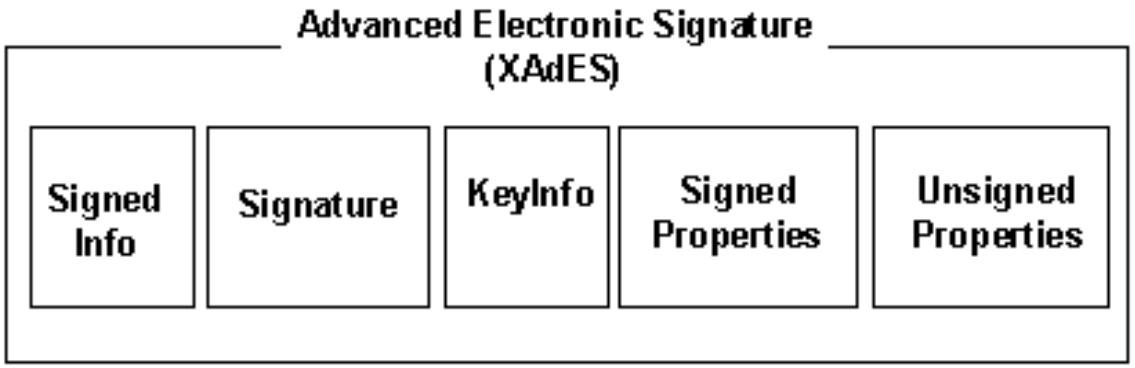
Időbélyeg ellenőrzése

- Az időbélyeg valóban az időbélyegző tanúsítványához tartozik?
- Az időbélyegző tanúsítványának visszavonási állapota
  - →Kulcskompromittálódás miatt visszavont tanúsítványú időbélyegzővel létrehozott minden időbélyeg **visszamenőleg is** érvénytelen
- Ellenőrzés a teljes tanúsítványláncra

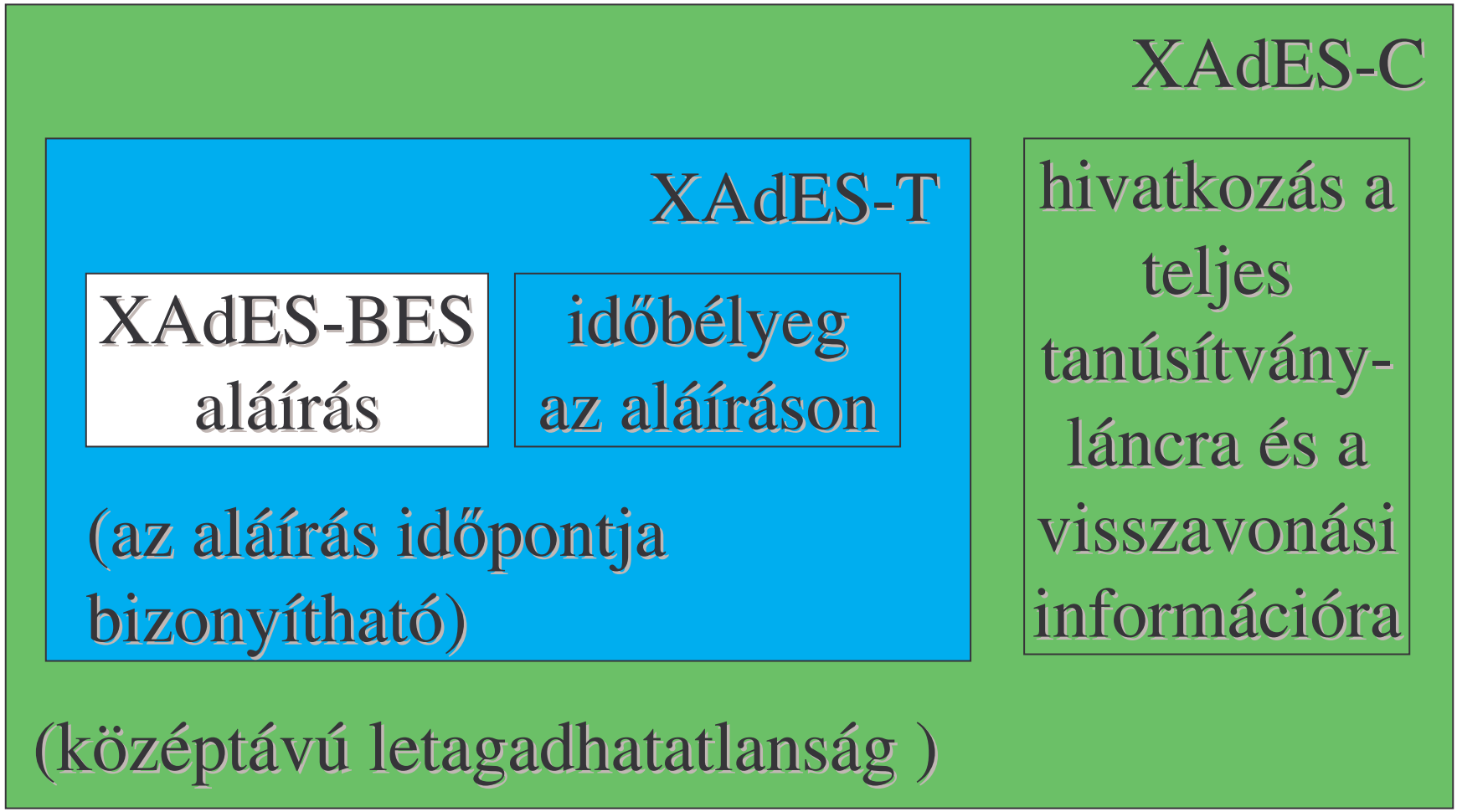
XAdES aláírások

- XML Advanced Electronic Signature
- W3C által kidolgozott formátum
- ETSI TS 101 903 szabvány
- Többfajta aláírást definiál, van közöttük egyszerű, időbélyeggel ellátott, és hosszú távon letagadhatatlan is

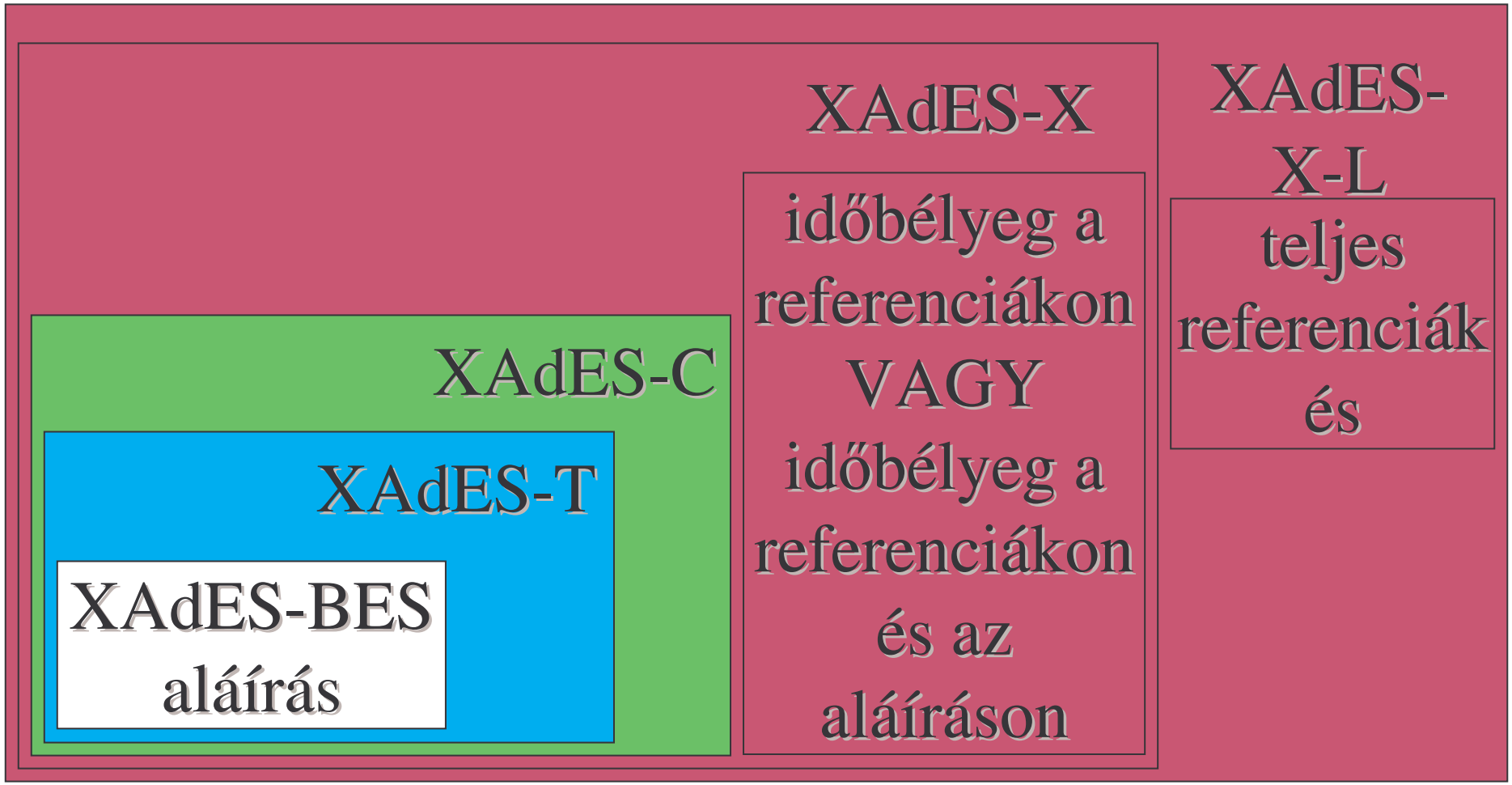
XAdES-BES


Advanced Electronic Signature
(XAdES)
Signed Info
Signature
KeyInfo
Signed Properties
Unsigned Properties

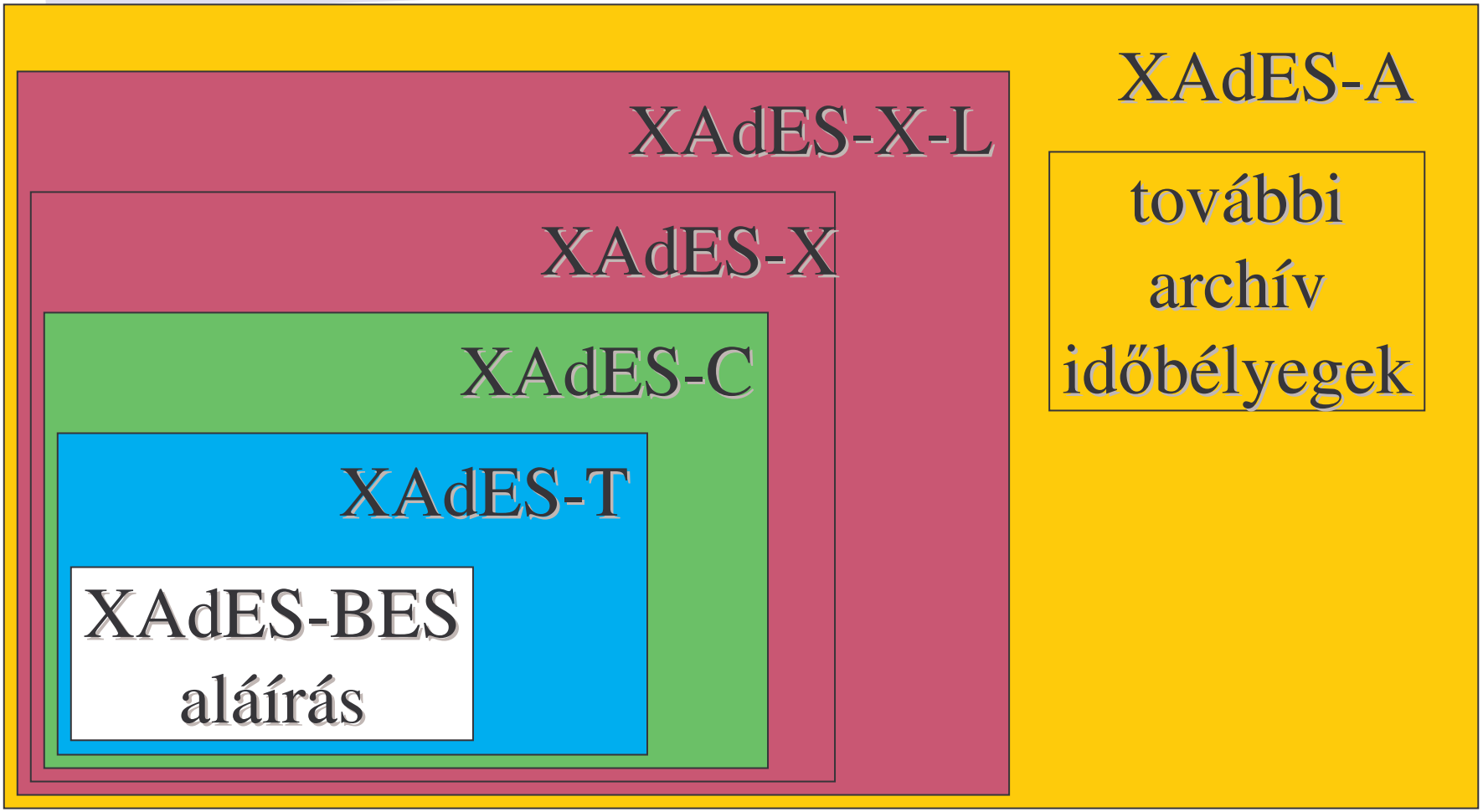
XAdES-T és XAdES-C



XAdES-X és XAdES-XL



XAdES-A, archív aláírás



XAdES formátumok

- XAdES-BES – nem sok mindenre jó
- XAdES-T – igazolható az aláírás időpontja
- XAdES-A – hosszú távú archiválás
  - →nem csak formátum, hanem eljárás
  - →archív szolgáltató

„Root” CA

- Nincsen egyetlen root CA
- Közigazgatási root, KGYHSZ.
- Tanúsítványtár a Windowsban, Mozillában stb.
- Az aláírást létrehozó fél létrehozza az aláírását, visszavezeti a tanúsítványát valamely root-ra.
- Az aláírást fogadó fél is megpróbálja a tanúsítványt egy általa ismert root-ra visszavezetni

Aláírás ellenőrzése

- Elektronikus aláírás érvényességéről
- Aki elektronikusan aláírt iratokat akar befogadni, kezelni, az meg kell, hogy határozza, hogy milyen aláírást fogad el:
  - → aláírás formátuma
  - → elfogadható root-ok
  - → visszavonás-ellenőrzés módja(i)
  - → tranzakciós limit
  - → aláírási jogosultság megállapítása
  - → …

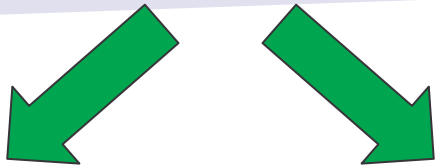
Elektronikusan aláírt dokumentumok hosszú távú hiteles megőrzése

Mi a probléma?

- Szolgáltatók megszűnhetnek, így pl. meg kell őrizni az aláírásra vonatkozó visszavonási információkat
- Időbélyegző-kulcsok kompromittálódhatnak
- Az alkalmazott kriptográfiai technológiák elavulhatnak:
  - → aláíró algoritmusok, kulcsméretek
  - → hash algoritmusok,
  - → időbélyegzők (!)

- Regisztrációs adatok megőrzése !

Megoldások (7/2005. IHM r.)



- XAdES-A formátum,
- rendszeresen frissíteni kell, rendszeres újra-időbélyegzés
- tetszőleges helyen elvégezhető

- Archiválás szolgáltató
- igazolást bocsát ki arról, hogy az aláírás érvényes volt
- a bizonyító erőt nem kizárólag kriptográfia biztosítja

Összefoglalás

- Az elektronikus aláíráshoz kapcsolódó technológiák rendelkezésre állnak
- Jogszabályi háttér szintén létezik
- E kettő összekapcsolása, illetve az alkalmazásokhoz való illesztése még nem teljesen kiforrott

További info

- Előadás fóliák: www.berta.hu
- PKI info: www.e-szigno.hu/?lap=tudasbazis
- Szombaton, a Hacktivity-n
- Miért van ilyen sok fajta tanúsítvány?
  http://srv.e-szigno.hu/menu/anyagok/BertaE2008nws.pdf
- Ha ingyenesen ki akarod próbálni, amit hallottál:
  - → teszt tanúsítványok igénylése
    http://www.e-szigno.hu/?lap=teszt_igenyles
  - → e-Szignó szoftver (aláírás, időbélyegzés, OCSP stb)
    http://www.e-szigno.hu/?lap=eszig_letolt

Köszönöm a figyelmet!