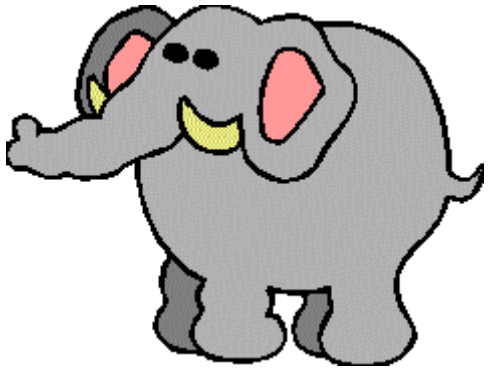
Gyakorlati problémák a PKI területén

BERTA István Zsolt
Microsec Kft., K+F és folyamatszervezési igazgató
<istvan.berta@microsec.hu>

Elefánt



- Műszaki kérdések
- Gazdasági kérdések
- Jogi kérdések

Miről fogok beszélni?

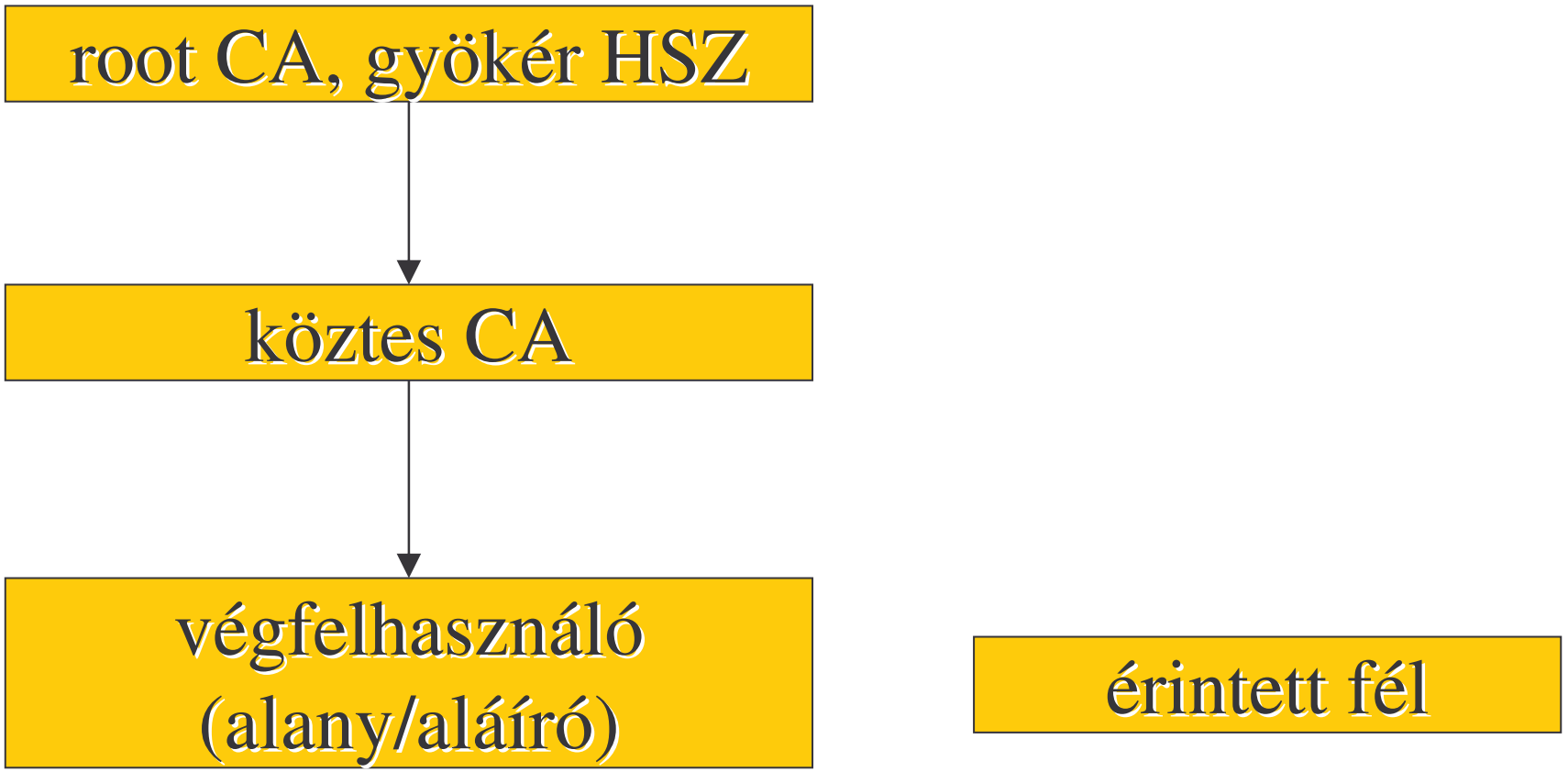
- Rövid összefoglalás a PKI-ről
- Hazai helyzet
- Műszaki + gazdasági + jogi aspektus
- Gyakorlati problémák

Bevezetés a PKI-ről

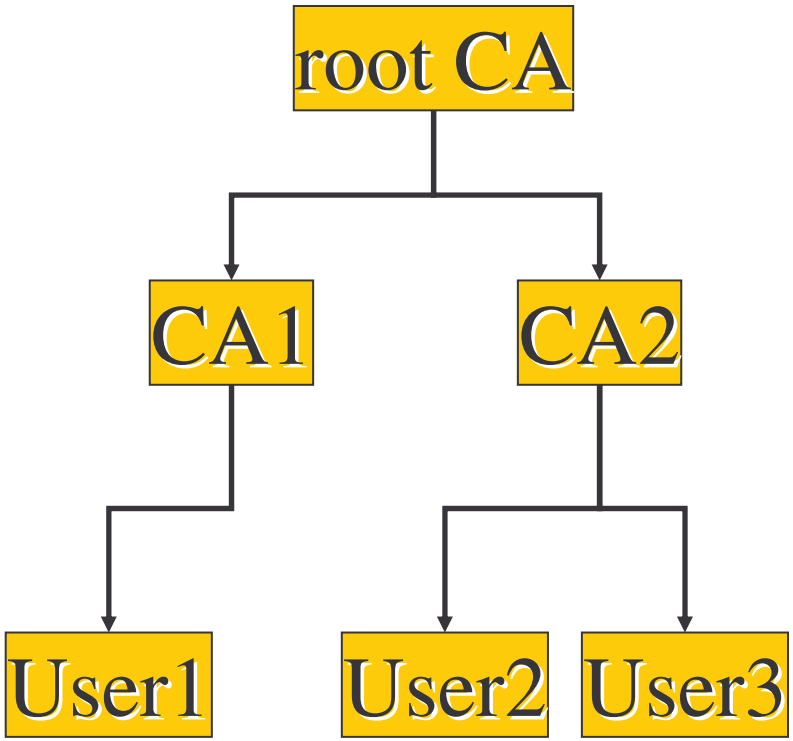
PKI röviden

- Minden résztvevőnek van magánkulcsa (csak ő ismeri) és hozzá tartozó nyilvános kulcsa (bárki megismerheti).
- A nyilvános kulccsal titkosítunk, a magánkulccsal lehet visszafejteni. A magánkulccsal aláírunk, a nyilvános kulccsal lehet ellenőrizni.
- Más nyilvános kulcsához hiteles módon kell hozzájutni, pl. úgy, hogy egy hitelesítés szolgáltató tanúsítványba foglalja és aláírja. Minden szereplő ismeri és elfogadja bizonyos „gyökér” hitelesítés szolgáltatók nyilvános kulcsát.
- Egyes szereplők tanúsítványuk szerint időbélyegzés szolgáltatók. Ha ők állítják valamiről, hogy mikor készült.
- Az elektronikus aláíráshoz (minősített/fokozott) és az időbélyegzéshez (minősített) jogkövetkezmény is kapcsolódik.

Terminológia



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

2001. évi XXXV tv. az elektronikus aláírásról

- EU direktíva (1999/93) az elektronikus aláírásról
- Elektronikus aláírással kapcsolatos szolgáltatások meghatározása
  - → hitelesítés szolgáltatás (tanúsítvány-kibocsátás)
  - → időbélyegzés szolgáltatás
  - → eszköz szolgáltatás
  - → archiválás szolgáltatás
- Minősített és nem minősített szolgáltatók, és a szolgáltatásaikhoz kapcsolódó bizonyító erő
- Nyilvántartás, felügyelet (Nemzeti Hírközlési Hatóság)
- A szolgáltatókra vonatkozó biztonsági követelmények, szolgáltatók felelőssége stb.

Hazai piac

- Szabályozott piac
- A hitelesítés szolgáltatók vállalatok, a Nemzeti Hírközlési Hatóság felügyeli a működésüket
- Négy 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
  - →+GIRO, www.giro.hu
  - →IHM, Biztonsági Hitelesítés Szolgáltató (nem működik)
- e-Cégeljárás
- korábban: Ügyfélkapu, Magánnyugdíjpénztári bevallás

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 (ISO9000) és információbiztonság-irányítási rendszer (BS7799, ISO27001)
- Folyamatos rendelkezésre állás (99,9%)
- Bizalmi munkakörök
  - →általánosan felelős vezető
  - →biztonsági tisztviselő
  - →regisztrációs tisztviselő
  - →független rendszervizsgáló
  - →rendszeradminisztrátor, rendszerüzemeltető
- Felelősségbiztosítás, bankgarancia

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 (érintett fél felé) vs. szolgáltatói felelősségvállalás (ügyfél felé)

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) }
```

Aláírás, titkosítás, authentikáció

- Az Eat. kizárólag az aláírásról szól, a másik két területre nemigen van szabályozás.
- Eat 13. § (4) „Az aláíró az aláírás-létrehozó adatot kizárólag az aláírás létrehozására használhatja, betartva a tanúsítványban jelzett esetleges egyéb korlátozásokat is.”
- E három területet szét szokás választani egymástól.
- E három esetben masszívan különböző kulcsmenedzsmentre van szükség.

Aláírás - NR (+DS)

- Az Eat. kizárólag aláírásról szól.
- A magánkulcsot kulcsot felesleges/tilos letétbe helyezni.
- A magánkulcs megsemmisülése nem okoz problémát.
- A lejárt tanúsítvány cserélhető, a magánkulcsa nem kell.
- A tanúsítványt egy korábbi időpontra (a magánkulcs használatának időpontjára) vonatkozóan kell ellenőrizni (letagadhatatlanság). Célszerű kivárási időt alkalmazni.
- A visszavont tanúsítvánnyal már nem lehet visszaélni, de a felfüggesztettel igen, ha később visszaállítják.
- Az Eat. szerint el kell választani minden más funkciótól.

Authentikáció, hitelesítés (DS+KA+...)

- Az Eat. nem vonatkozik rá.
- A magánkulcsot kulcsot felesleges/tilos letétbe helyezni.
- A magánkulcs megsemmisülése nem okoz problémát.
- A lejárt tanúsítvány cserélhető, a magánkulcsa nem kell.
- A tanúsítványt mindig az aktuális időpontra vonatkozóan kell ellenőrizni. Értelmetlen kivárási időt alkalmazni.
- A visszavont tanúsítvánnyal már nem lehet visszaélni, és a felfüggesztettel sem.
- A magánkulccsal véletlen kihívást kódolunk, vigyázni kell, nehogy aláírjunk/dekódoljunk valamit.

Titkosítás/dekódolás - KE+DE

- Az Eat. nem vonatkozik rá.
- A magánkulcsot letétbe szokás helyezni.
- A magánkulcs megsemmisülése óriási károkat okozhat.
- Ha lecseréljük a tanúsítványt/magánkulcsot, vagy mindent át kell titkosítani, vagy a korábbi kulcsokat is használni kell…
- A tanúsítványt az aktuális időpontra vonatkozóan kell ellenőrizni - ez is tökéletlen megoldás.
  Értelmetlen kivárási időt alkalmazni.
- A felfüggesztés/visszavonás nem akadályozza meg a támadót, hogy visszaéljen a magánkulccsal, csak a későbbi károkat enyhíti az érintett felek értesítésével.

Certificate Policies

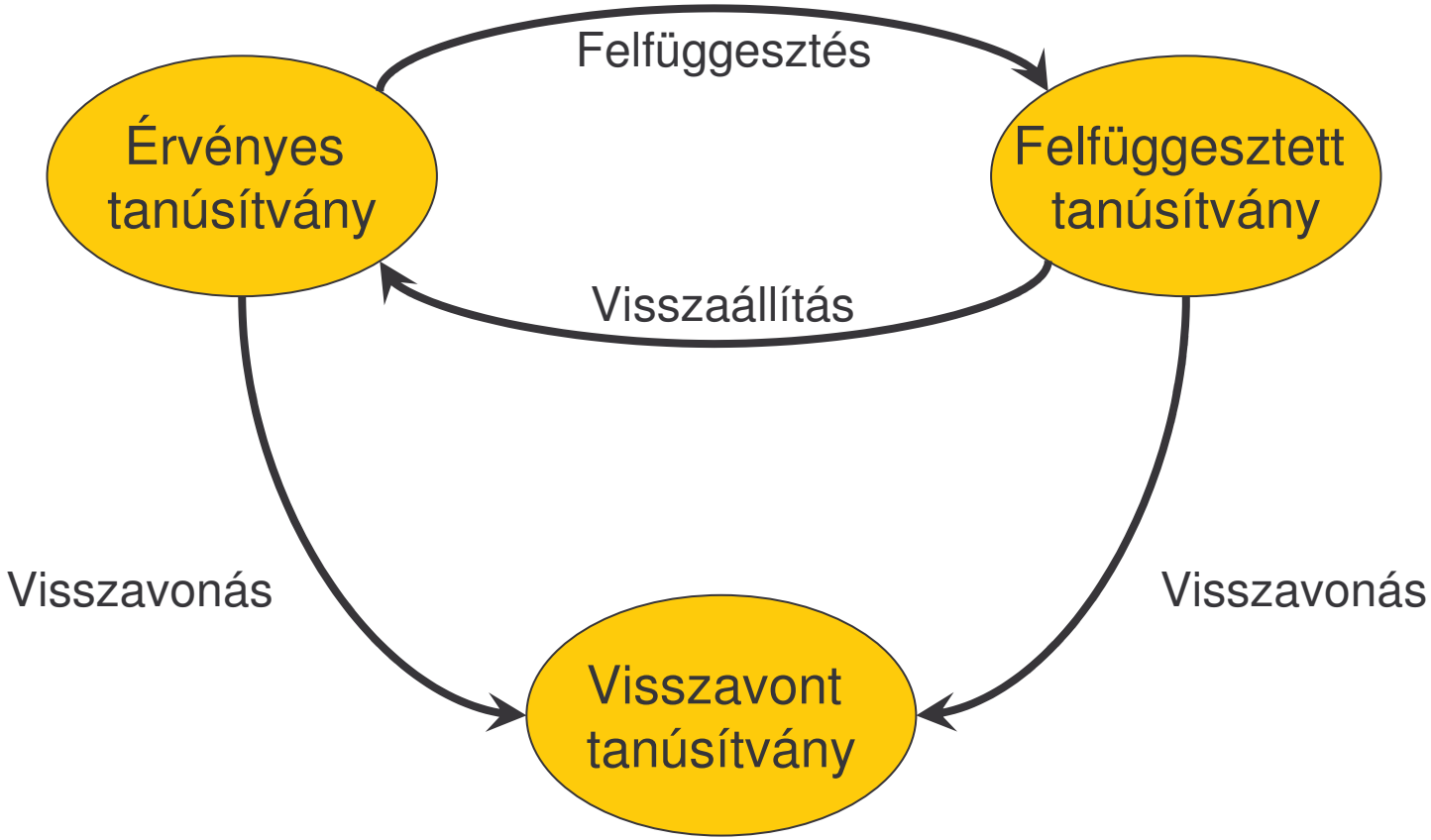
- A hitelesítés szolgáltató hitelesítési rendjére és/vagy szolgáltatási szabályzatára tartalmaz hivatkozást
- Megállapítható belőle, hogy a szolgáltató milyen feltételek mellett bocsátotta ki a tanúsítványt és mekkora felelősséget vállal érte
- QCStatements

CRL és OCSP

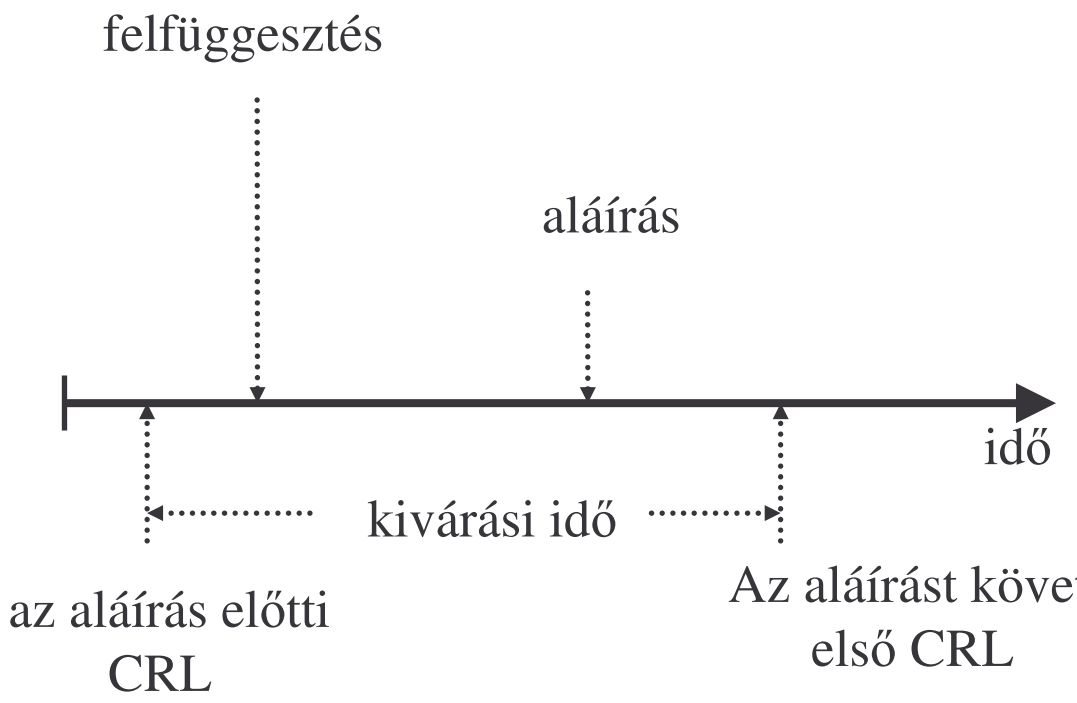
Visszavonási állapot közzététele

- Visszavonási lista (CRL)
  - →A CA által rendszeresen kibocsátott, aláírt lista
- Eseményvezérelt CRL
- Delta CRL
- OCSP – Online Certificate Status Protocol
  - →kérdés: x tanúsítvány érvényes-e
  - →aláírt válasz: igen/nem

Felfüggesztés, visszaállítás, visszavonás

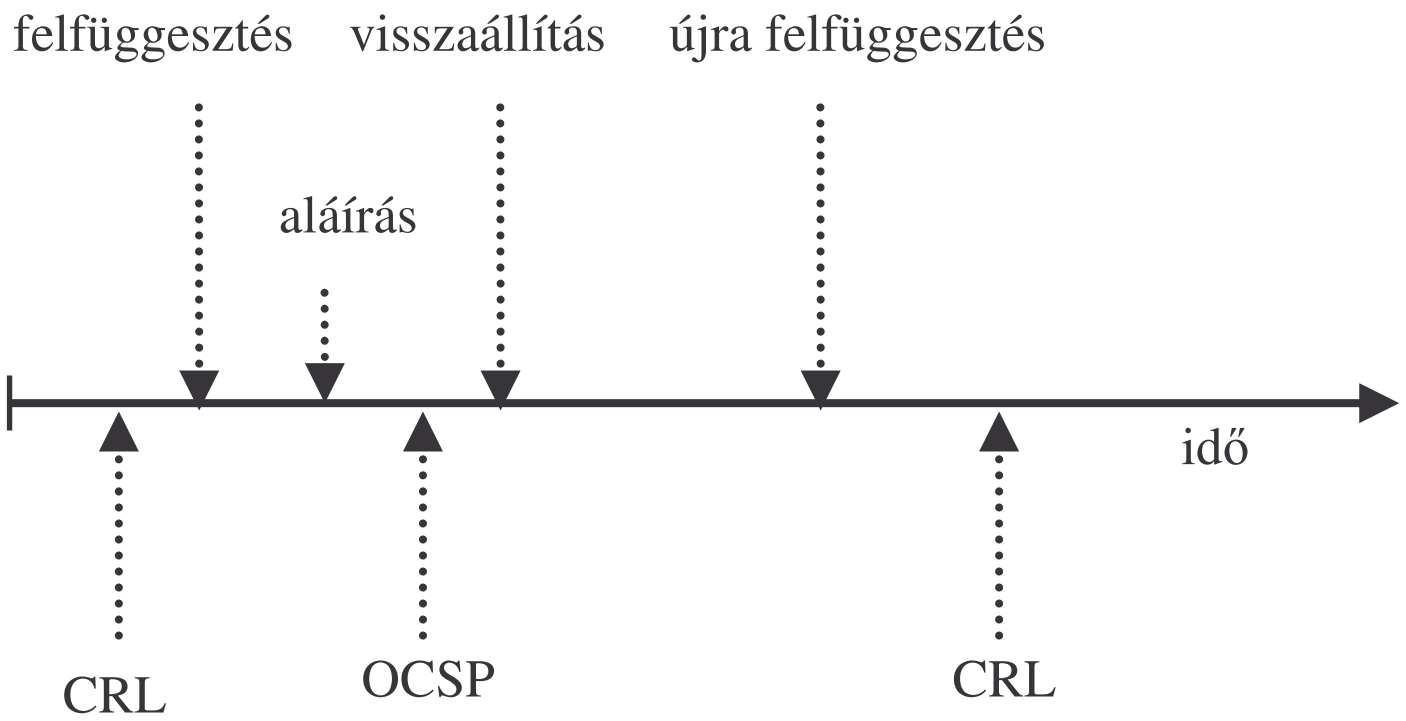


Kivárási idő (grace period)



- 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



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

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 hierarchia

www.e-szigno.hu/?lap=szolgaltatoi_tanusitvanyok

Elektronikus aláírás és ellenőzése

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

OCSP válasz ellenőrzése

- OCSP válasz kizárólag akkor érvényes, ha
  - → a válaszadó tanúsítványa még érvényes
  - → az OCSP válaszon időbélyeg van, és a válaszadó tanúsítványa az időbélyegen szereplő időpontban érvényes volt

Szabványos aláírás-formátumok

„Alap” aláírások:

- CMS - cryptographic message syntax (ASN1)
- XMLDSIG - xml alapon

Egyéb információkat is csatolni szokás:

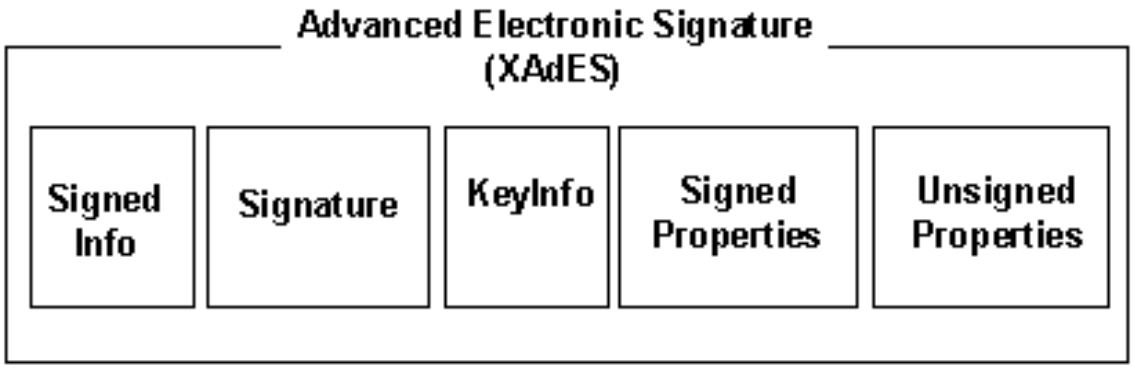
- XMLDSIG → **XAdES**
- CMS → CAdES

Alapvetően ugyanazokat a funkciókat oldják meg ASN1, illetve XML alapon.

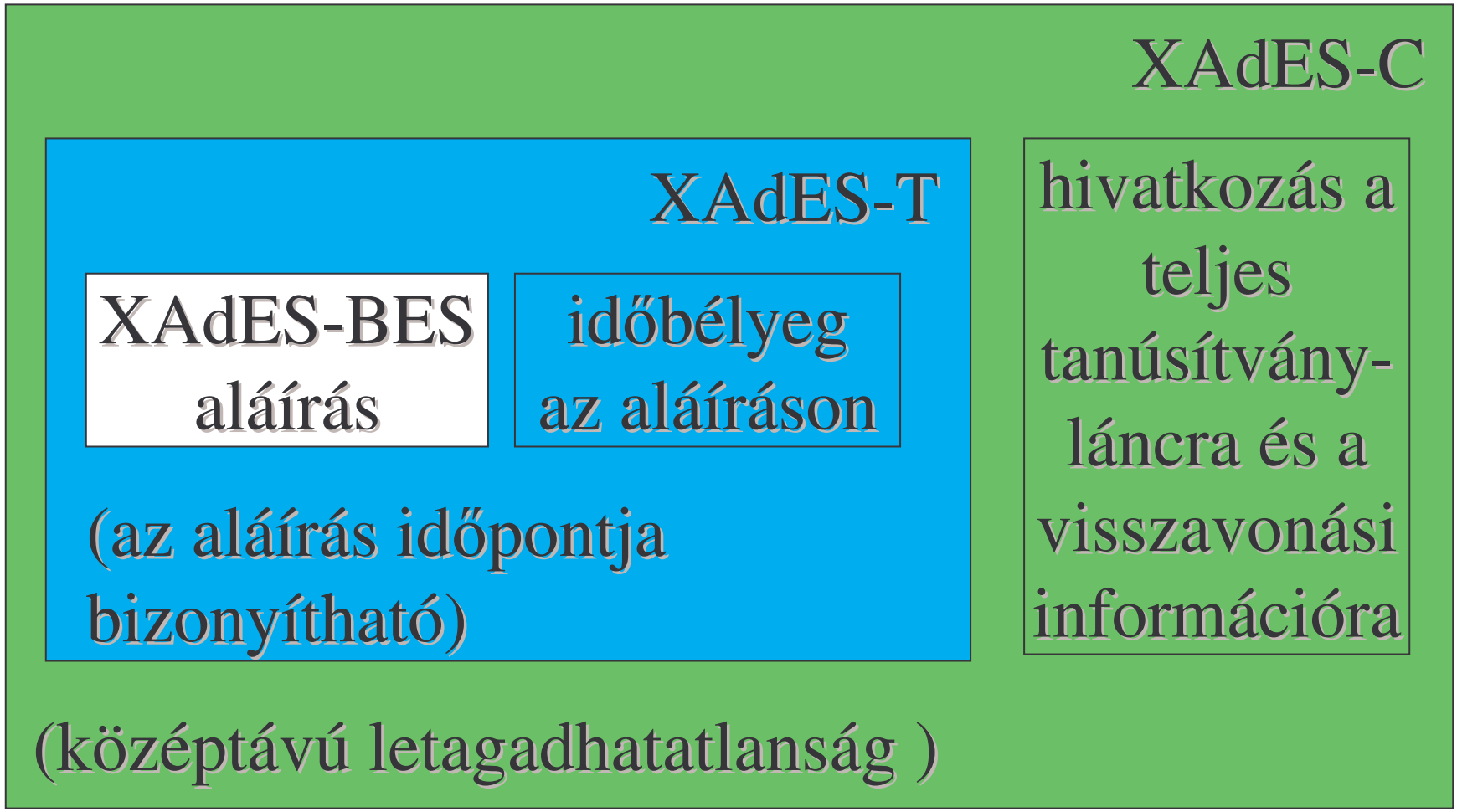
XAdES aláírások

- 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

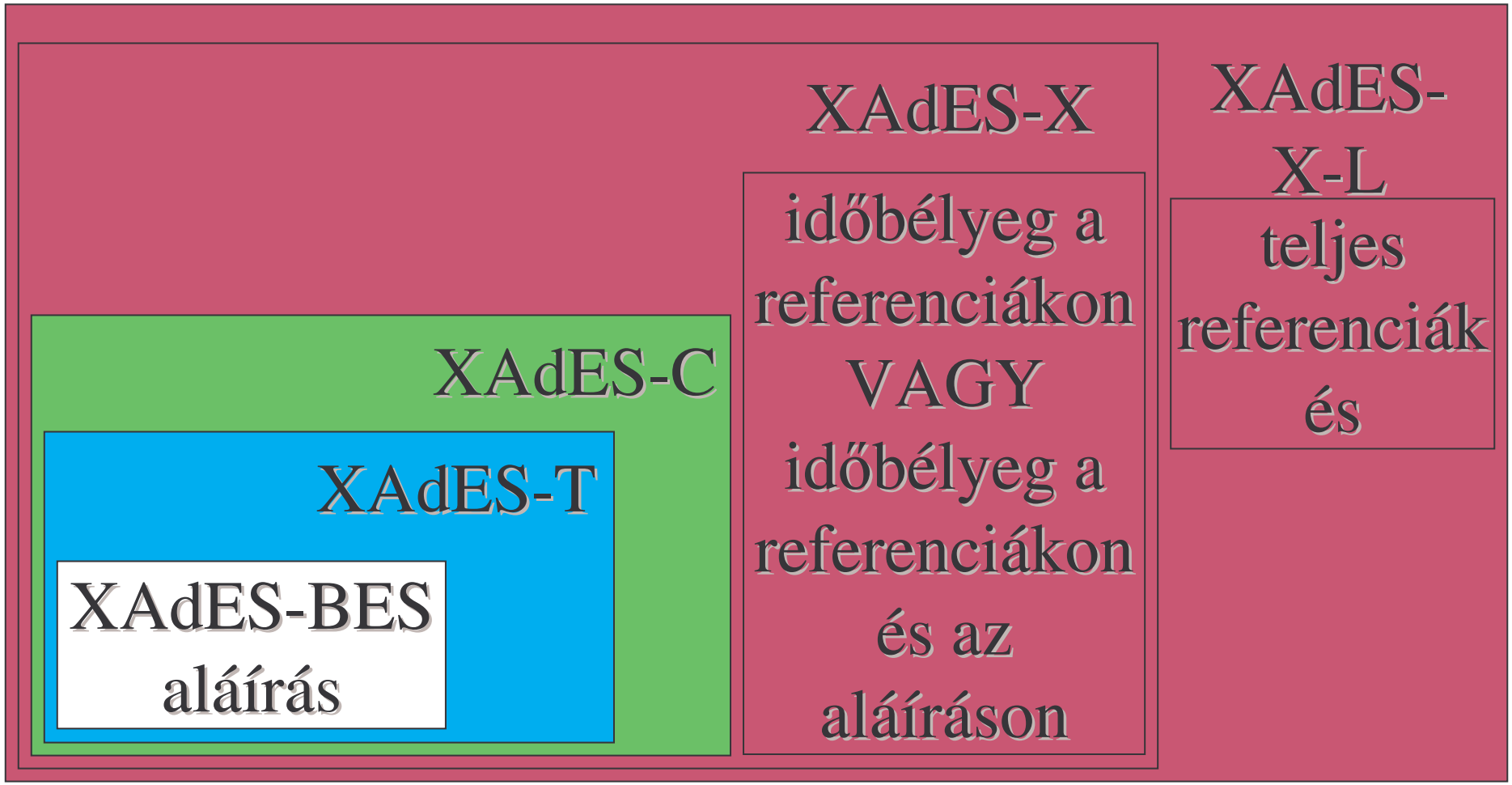
XAdES-BES


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

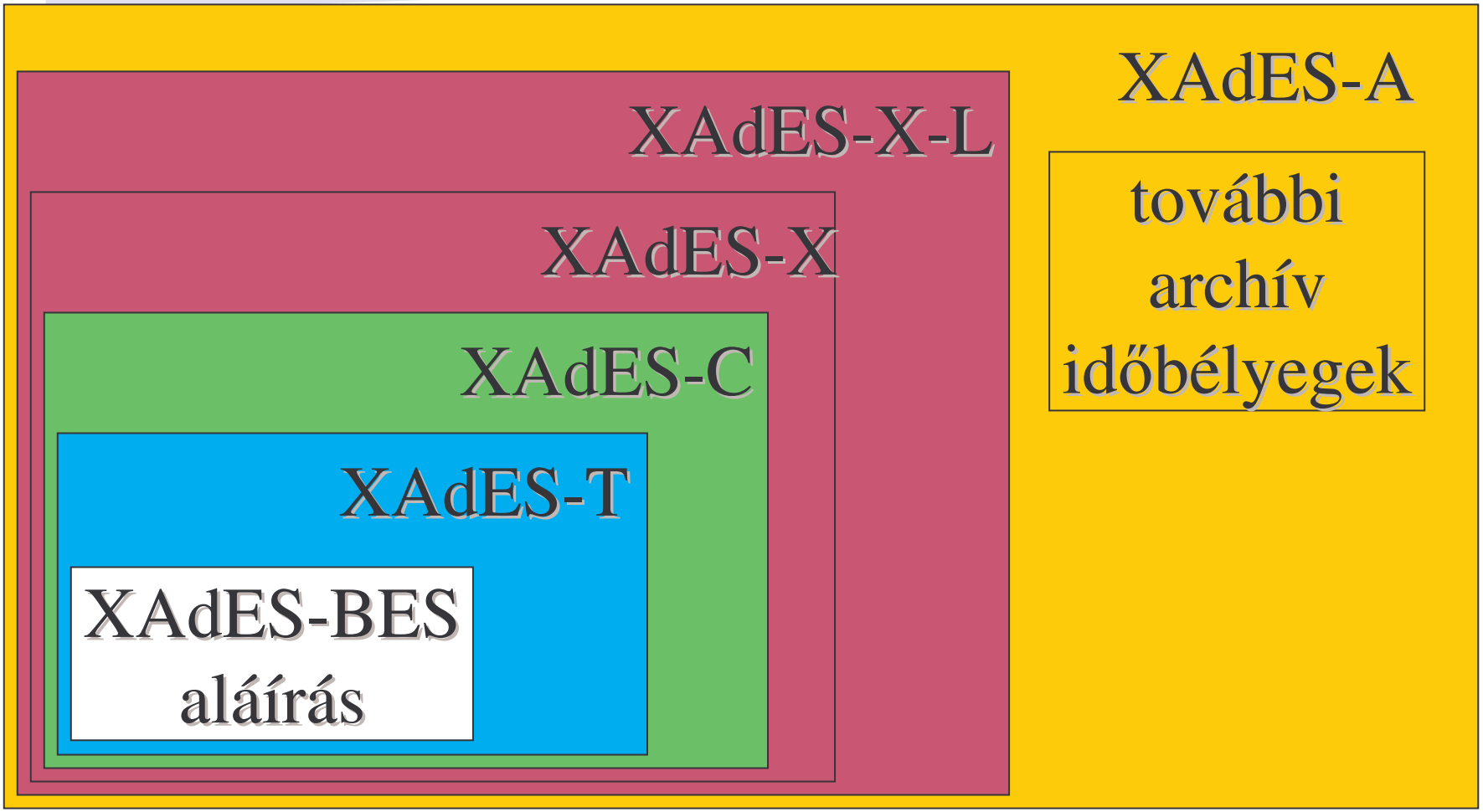
XAdES-T és XAdES-C



XAdES-X és XAdES-XL



XAdES-A, archív aláírás



XAdES formátumok

- XAdES-BES – nem sok mindenre jó
- XAdES-T – igazolható az aláírás időpontja
- XAdES-C – középtávú letagadhatatlanság
- XAdES-X-L – minden információt tartalmaz
- XAdES-A – hosszú távú archiválás
  - →nem csak formátum, hanem eljárás
  - →archív szolgáltató

„Root” CA

- Nincsen egyetlen root CA
- Magyar nemzeti root?, közigazgatási root?
- 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

PKI alkalmazások tesztelése

- Az alkalmazásokat tesztelni kell.
- PKI esetén hitelességet nem a dokumentumok helye, hanem a dokumentumok kódolása biztosítja.
- Az éles rendszer „leklónozásával” nem „homokozó” tesztrendszert, hanem másik éles rendszert kapunk.
- Külön tesztrendszereket szokás felállítani, külön kulcsokkal. Ez különbözik az éles rendszertől.
- Az éles rendszerben éppen a kulcsokat kell megváltoztatni, így épp a kulcskezelést nem könnyű tesztelni…

Microsec e-Szignó teszt rendszerek

- Teszt hitelesítés, időbélyeg stb. szolgáltatás:
  →http://www.e-szigno.hu/?lap=teszt_bevezeto
- e-Szignó program:
  →http://www.e-szigno.hu/e-Szigno_bemutato

- További info:
  →http://www.e-szigno.hu/?lap=szakembereknek

Összefoglalás

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

Köszönöm a figyelmet!

Gyakorlati problémák a PKI területén

BERTA István Zsolt
Microsec Kft., K+F és folyamatszervezési igazgató
<istvan.berta@microsec.hu>