MICROSEC
Számítástechnikai Fejlesztő Kft.

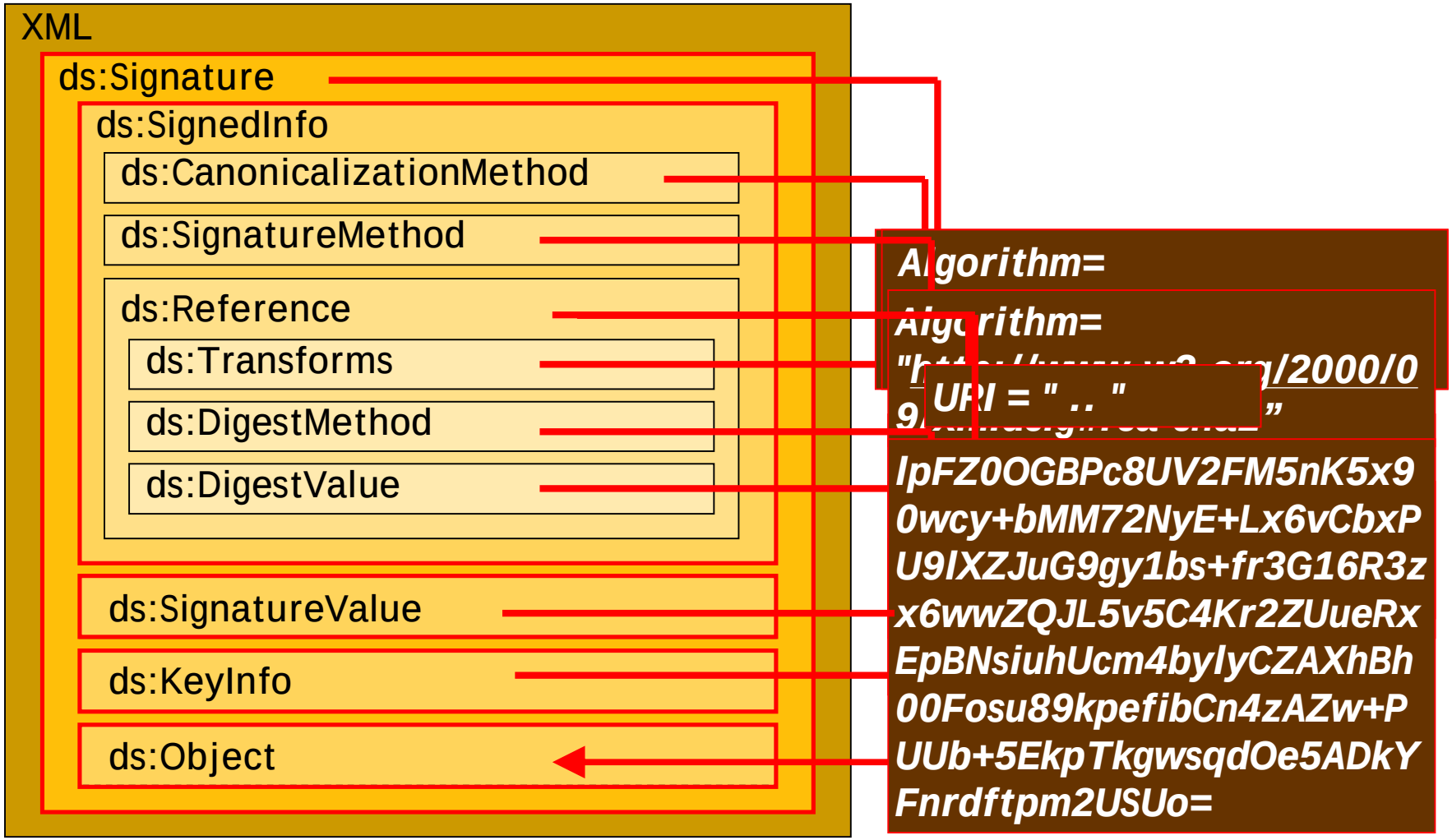
Mire jó az archív aláírás?

Endrődi Csilla
Microsec Kft.

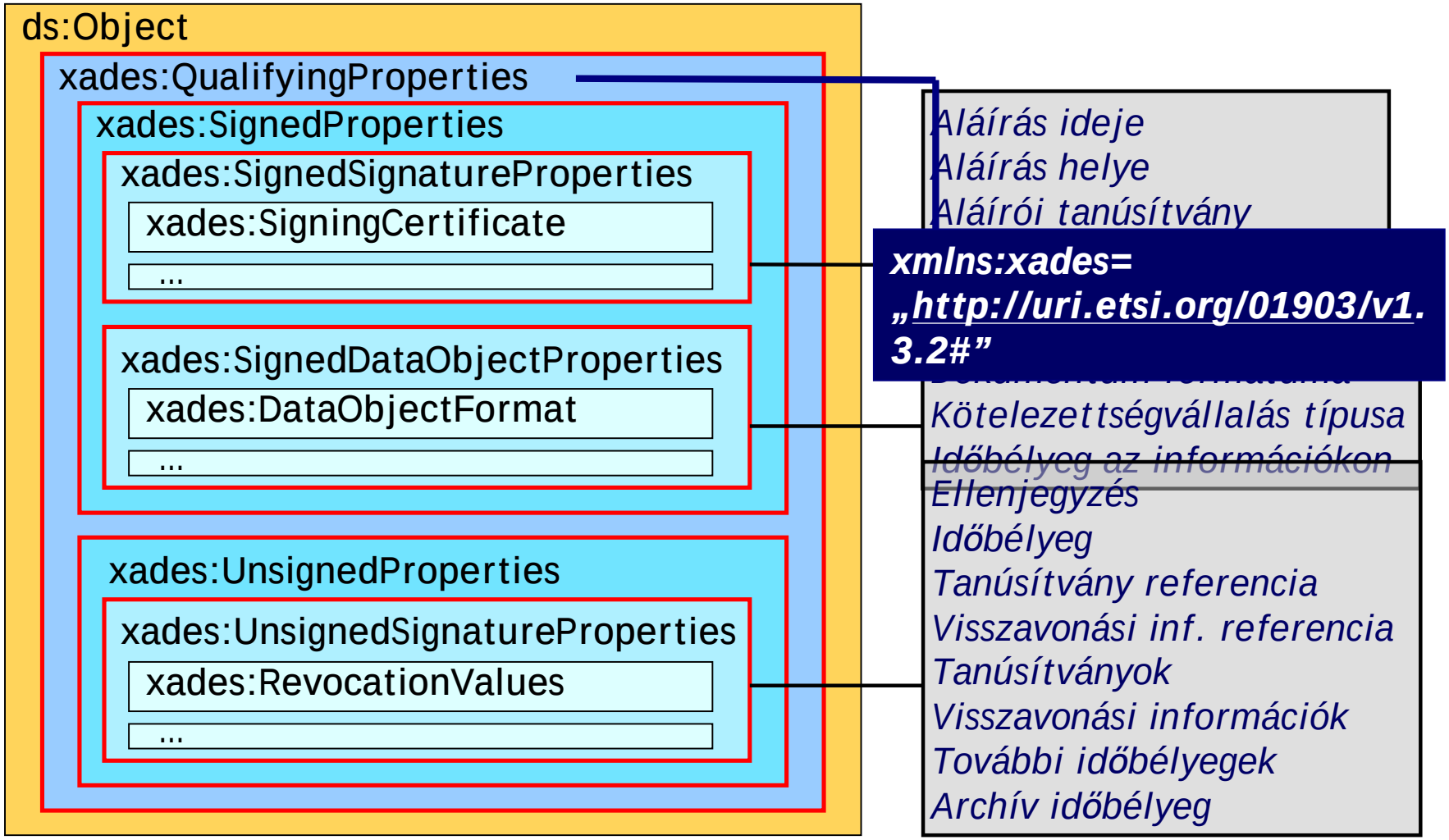
Mi az *archív aláírás*?

- Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható elektronikus aláírás formátumok műszaki specifikációjára (2005. november 22.)
  - pillanatnyi aláírás
  - rövid távú aláírás
  - hosszú távú aláírás
  - archív aláírás
- RFC 3275: XML-Signature Syntax and Processing
- ETSI TS 101 903 v1.3.2.: XML Advanced Electronic Signatures (XAdES)
  - XAdES-BES, -EPES, -T, -C, -X (type1, type2), X-L, -A

XML formátumú aláírás



XML Advanced Electronic Signature



MICROSEC
Számítástechnikai Fejlesztő Kft.

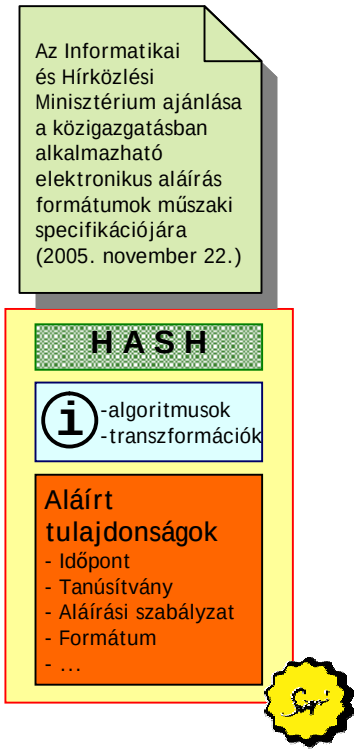
Alap aláírás: XAdES-BES, -EPES

Alapfeladat:

- Lenyomatok összehasonlítása
- Nyilvános kulcs és személy (hiteles) összekapcsolása

- *Csatolandó adatok:*
  - Dokumentum lenyomata
  - Algoritmusok azonosítója (digest, kanonizációs, aláíró)
  - Aláírói tanúsítvány (vagy lenyomat és referencia)
  - EPES: Aláírási szabályzat azonosítója és lenyomata
- *Opcionális adatok:*
  - Aláírás időpontja, helye
  - Kötelezettségvállalás típusa
  - Aláírói szerepkör
  - Aláírt dokumentum formátuma
  - Időbélyeg, Ellenjegyzés

Pillanatnyi aláírás: XAdES-EPES



XAdES-T

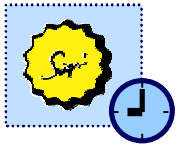
Probléma:

- Tanúsítvány lejárhat, visszavonhatják (felfüggeszthetik, visszaállíthatják)

  ↳ Ismernünk kell az aláírás elkészítésének időpontját

  Ezt NEM rögzítheti maga az aláíró (vagy az ő befolyása alatt álló program)

- *Csatolandó adatok:*
  - **Időbélyeg:**
    Az aláírás és az Időbélyegzés szolgáltató által biztosított hiteles időpont összekapcsolása és aláírása



Ha az aláíráshoz nem kapcsolódik időbélyeg, akkor az ellenőrzést az aktuális (ellenőrzéskori) időpontra vonatkozóan kell elvégezni.

Időbélyeget nem tartalmazó aláírás érvényessége elvész az aláírói tanúsítvány lejártakor!

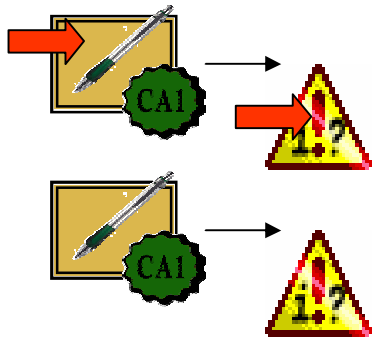
Rövid távú aláírás: XAdES-T

XAdES-C

Probléma:

- Az aláírás ellenőrzéséhez szükséges tanúsítványok és visszavonási információk az eredeti helyen megváltozhatnak, elérhetetlenné válhatnak
  - ↳ Szükséges ezen információk referenciáinak és lenyomatainak eltárolása
  - Opcionálisan magunknak az adategységeknek az eltárolása

- *Csatolandó adatok:*
  - Tanúsítványok referenciája
  - Visszavonási információk referenciája
- *Opcionális adatok:*
  - Tanúsítványok
  - Visszavonási információk (kivárási idő!)



Kivárási idő (grace period): Amennyi idő elteltével a releváns visszavonási információk elérhetővé válnak

Hosszú távú aláírás: XAdES-C

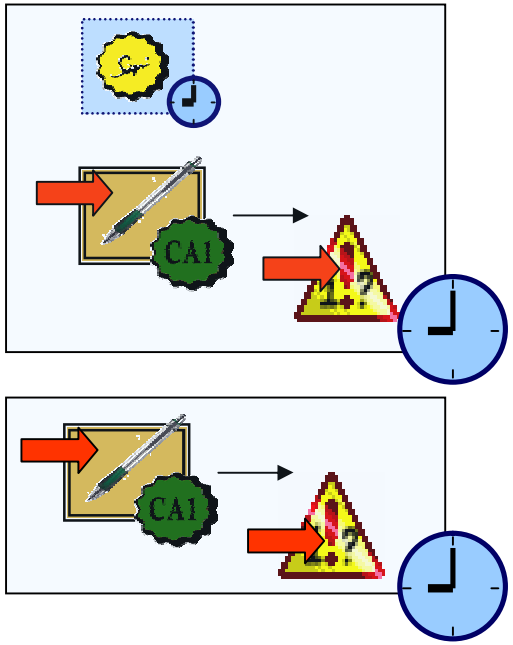
XAdES-X type1, type2

Probléma:

- Hitelesítés szolgáltató, Időbélyegzés szolgáltató, OCSP válaszadó kulcsa kompromittálódhat, lejárhat

  ↳ Az ezek által aláírt adategységek (tanúsítvány, Időbélyeg, CRL, OCSP válasz) időbélyegzése szükséges

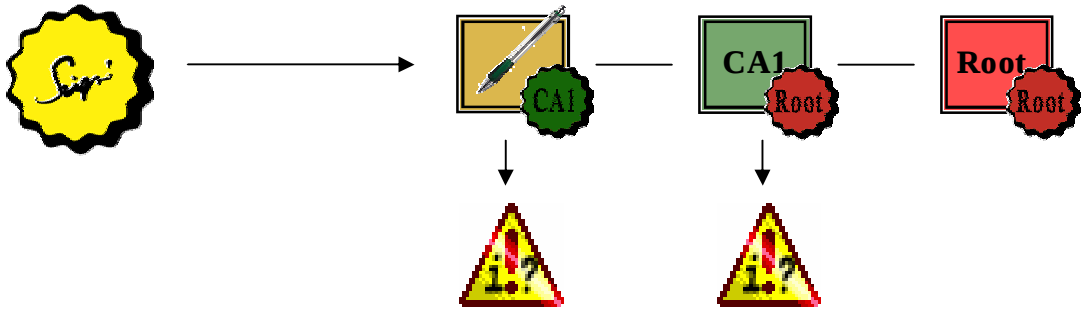
- *Csatolandó adatok:*
  - Type 1: Időbélyeg a következőkön:
    - Aláírás értéke
    - Aláíráson levő időbélyeg
    - Tanúsítványok referenciája
    - Visszavonási információk referenciája
  - Type 2: Időbélyeg a következőkön:
    - Tanúsítványok referenciája
    - Visszavonási információk referenciája



XAdES-X-L

Probléma:

- Az aláírás ellenőrzéséhez szükséges tanúsítványok és visszavonási információk az eredeti helyen megváltozhatnak, elérhetetlenné válhatnak
  - ↳ A szükséges tanúsítványok, visszavonási információk beszerzése
- *Csatolandó adatok:*
  - Tanúsítványok
  - Visszavonási információk



A hosszú távú aláírás is előírja ezeket az elemeket, azonban ott a XAdES-X-nél megkövetelt időbélyegek elhelyezése nem szükséges.

XAdES-A

Probléma:

- A használt kriptográfiai algoritmusok elavulhatnak, az Időbélyegzés szolgáltatók tanúsítványa lejár, kulcsa kompromittálódhat
  - az Időbélyegzés szolgáltató tanúsítványának lejártakor az összes általa kibocsátott ***időbélyeg érvényét veszti***
  - egy kriptográfiai algoritmus törhetővé válása esetében csak a bizonyíthatóan a törés előtt azzal készült elemek használhatóak fel

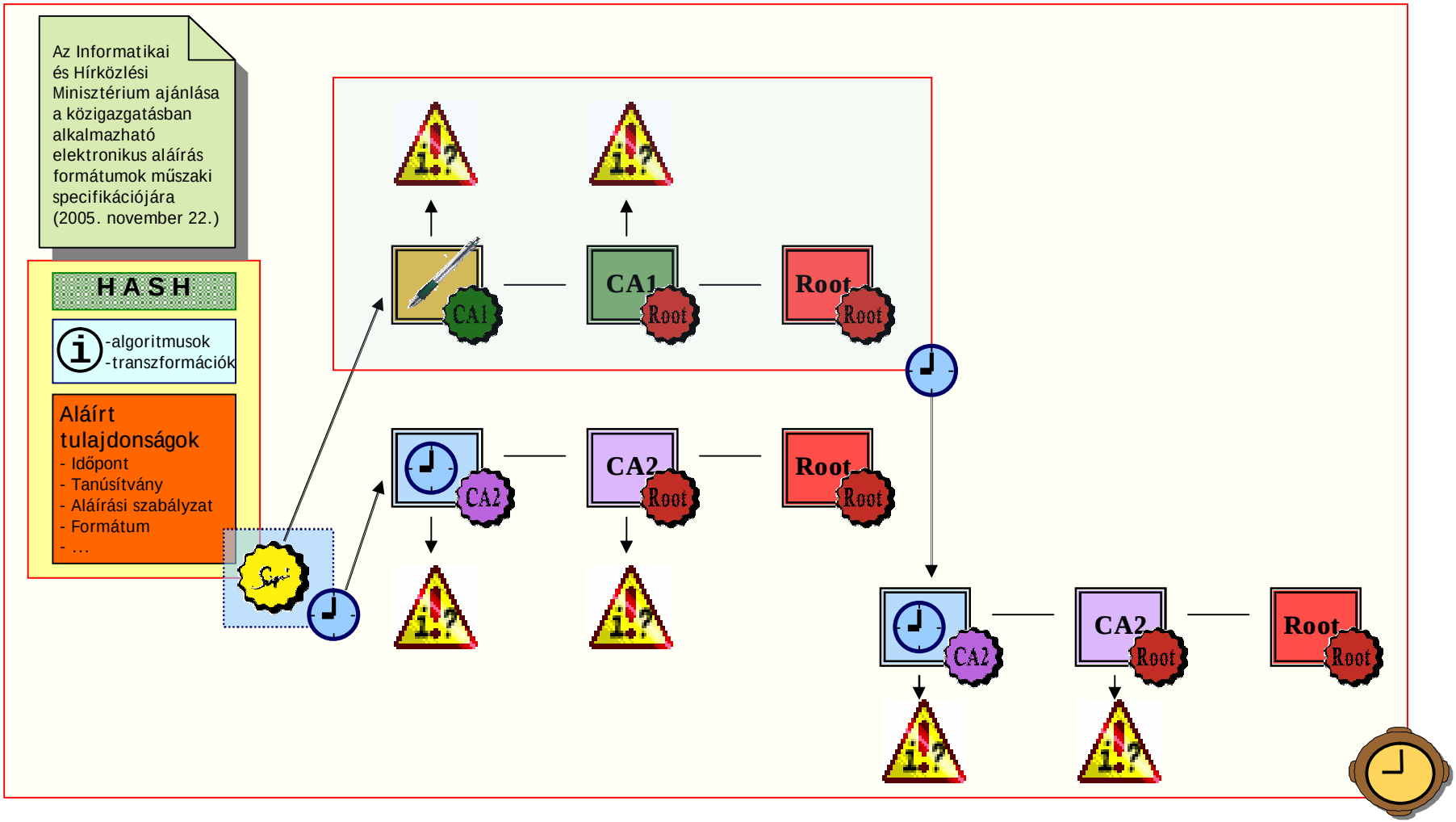
↳ Ezek bármelyikének bekövetkezése **előtt** szükséges egy újabb, ún. Archív időbélyeg elhelyezése

- *Csatolandó adatok:*
  - **Archív időbélyeg**, amely aláírja az összes olyan elemet, amely valamilyen kriptográfiai algoritmus felhasználásával készült

Az archív aláíráson rendszeresen újabb archív időbélyeg helyezendő el, az rendszeres „karbantartást” igényel.

Archív aláírás: XAdES-A

Mit tartalmaz archív aláírás?



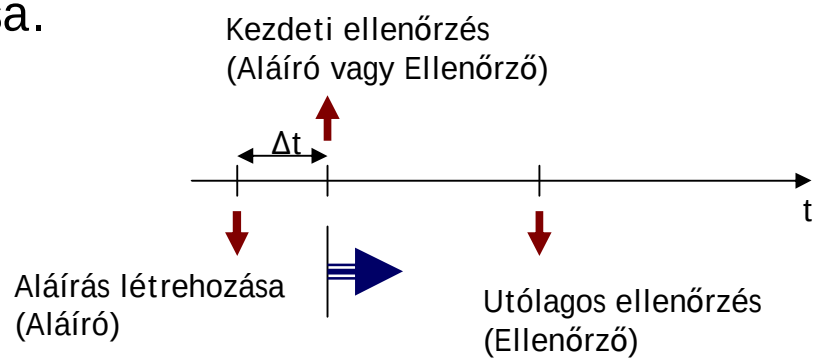
Milyen formátumú aláírást készítsünk?

Minél több adatot tartalmaz („magasabb” formátumú)

- annál több veszélyforrás ellen véd, azonban
- annál költségesebb a létrehozása.

Aláírás létrehozása több lépésben:

- Aláírás létrehozása
- Kezdeti ellenőrzés
- Utólagos ellenőrzés



IHM ajánlás:

- ***Pillanatnyi aláírás***: elektronikus aláírás, amelynek az élettartama rövidebb az aláírást követő első visszavonási állapot információ kiadásánál.
- ***Rövid távú aláírás***: elektronikus aláírás, amelynek az ellenőrzése nem szükséges az aláíró tanúsítványának lejárta után.
- ***Hosszú távú aláírás***: elektronikus aláírás, amelynek az ellenőrzése szükséges a tanúsítványlánc bármely elemének a lejárta után is.
- ***Archív aláírás***: elektronikus aláírás, amelynek az ellenőrzése szükséges az aláírás során használt algoritmusok kriptográfiai elavulása után is.

Néhány esetben jogszabály írja elő az archív aláírás alkalmazását.

Problémás helyzetek:

Visszavonás, felfüggesztés, visszaállítás...

Igény: A titkos kulcs elvesztése, kompromittálódása esetén

- a kulcs és az eredeti tulajdonos „összerendelése” szűnjön meg
- DE ez a korábban készült aláírások érvényességét ne befolyásolja

↳ Visszavonás-kezelés

- Ügyfél kéri a HSz-től a tanúsítvány visszavonását
- A HSz publikálja a visszavonás tényét (CRL, OCSP)

Igény: Az elveszettnek vélt titkos kulcs „megtalálása” esetén a kulcs állapot legyen visszaállítható

↳ Tanúsítvány felfüggesztés, visszaállítás lehetősége

- Felfüggesztett tanúsítvány ugyanúgy „viselkedik”, mint a visszavont
- Csak felfüggesztett tanúsítvány állítható vissza
- Visszaállításkor a tanúsítványt kiveszik a CRL-ből, illetve az OCSP válasz megint „jó” értéket fog tartalmazni

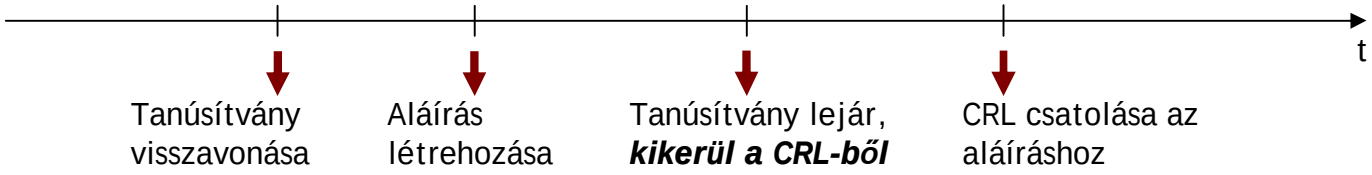
!? A felfüggesztés és visszaállítás között keletkezett aláírásokat érvényesnek vagy érvénytelennek kell tekinteni?

Problémás helyzetek:

CRL-es visszavonási technika

CRL: Certificate Revocation List (RFC 2527)
A visszavont nyilvános kulcsok azonosítóinak listája

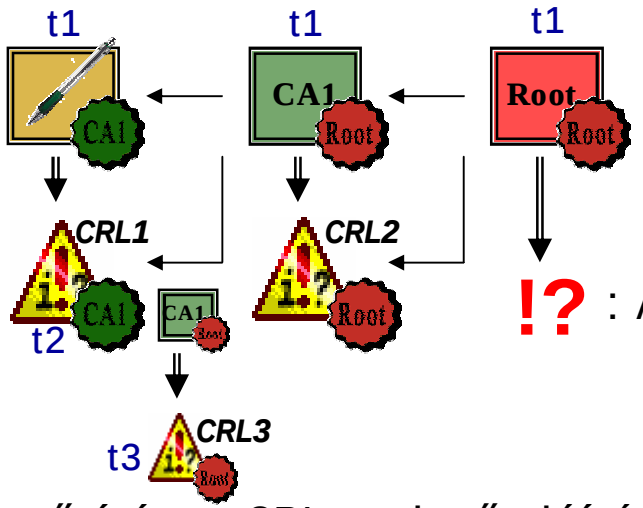
- Nyilvánosságra hozatal:
  - Adott időpontban rendszeresen
    - Eseményvezérelt CRL
  - Általában http, https vagy ldap protokollon keresztül
    - Automatikusan is letölthető (elérési hely beleírandó a tanúsítványba)
- A CRL folyamatosan bővülő lista
  - Delta-CRL
  - Lejárt tanúsítványok kivétele a CRL-ből
    Gond lehet, ha a tanúsítvány lejárta után egészítik ki az aláírást a visszavonási információkkal.



Problémás helyzetek:

CRL-es visszavonási technika folyt.

- A CRL-en levő aláírás ellenőrzése
  - Általában ugyanazzal a kulccsal írják alá, mint az aláírói tanúsítványt



t1: aláírás létrehozása
t2: CRL1 kibocsátása
t3: CRL3 kibocsátása

!? : Alternatív úton

Egyszerűsítés: a CRL-en levő aláírás ellenőrzésének visszavezetése az aláírói tanúsítványon levő aláírás ellenőrzésére

Probléma: A két aláírás különböző időpontokban készült!

Gond lehet, ha a Hitelesítés Szolgáltató kulcsa a dokumentum aláírása és a CRL kibocsátása között kompromittálódik!

Problémás helyzetek:

OCSP-s visszavonási technika

OCSP: Online Certificate Status Protocol (RFC 2560)

Aláírt igazolás egy adott tanúsítvány aktuális visszavonási állapotára vonatkozóan

- Válasz lehet: *jó*, *visszavont*, *ismeretlen*
- Ha „*visszavont*”, akkor a válasz tartalmazza a *visszavonás időpontját*

- Nyilvánosságra hozatal:
  - OCSP protokollon keresztül
    - Elsősorban program által feldolgozható
    - Mindig kell hozzá Internet kapcsolat
  - Mindig az aktuális állapotot tartalmazza

- OCSP-n levő aláírás ellenőrzése
  - Ugyanazzal a kulccsal, mint az aláírói tanúsítványokat?
  - OCSP válaszadó tanúsítványára honnan szerzünk visszavonási információt?

Problémás helyzetek:

OCSP-s visszavonási technika folyt.

OCSP-s architektúrák

1. Maga a CA egység nyújtja az OCSP szolgáltatást

   Kérdés: ki nyújt róla…?

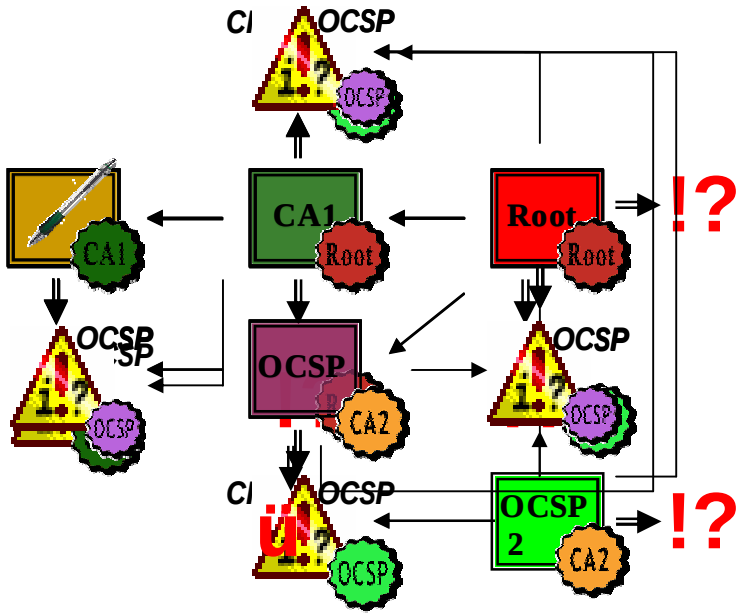
   Információ beszerzése alternatív úton!

2. OCSP szolgáltató külön egység, de az ő tanúsítványáról CRL érhető el

   OCSP előnyei elvesznek,
   a problémát csak odébb tolja …

3. OCSP szolgáltató tanúsítványát egy másik OCSP szolgáltató igazolja

   A problémát csak odébb tolja…



4. Rövid lejáratú OCSP tanúsítványok

   OCSP válaszadó tanúsítványának visszavonási állapotát nem kell ellenőrizni!

Problémás helyzetek:

CRL kontra OCSP…

- CRL kibocsátása szakaszos
- OCSP az aktuális állapotot tartalmazza

A különböző technikákon alapuló ellenőrzés eltérő eredményt adhat!

↳ **Kivárási idő**: A visszavonás-kérés feldolgozásának + a nyilvánosságra hozatalának időtartama

Vállalt kivárási idő: Amelyet a Hitelesítés Szolgáltató vállal.

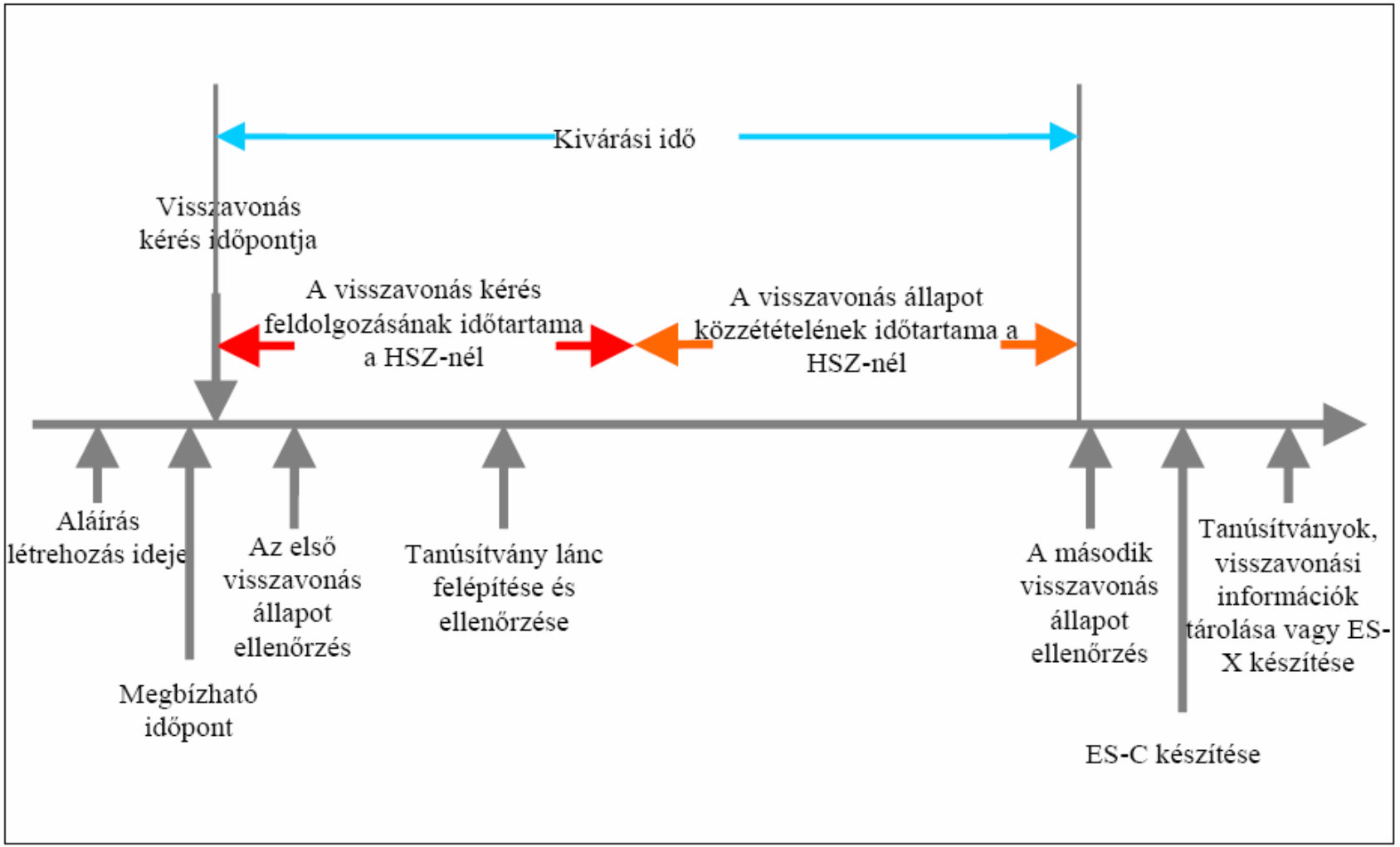
Előírt kivárási idő: Amelyet egy szervezet előír a befogadandó aláírásokra.

Következmény:

- Nem lehet egy lépésben aláírást készíteni
- A tanúsítvány-lánc további elemeire általában még ritkábban bocsátanak ki CRL-t (pl. havonta/évente): ez a gyakorlatban kivárhatatlan!
- A CRL-en levő aláírás ellenőrzésének problémája tovább bonyolódik…

Problémás helyzetek:

Kivárási idő (grace period)



Problémás helyzetek:

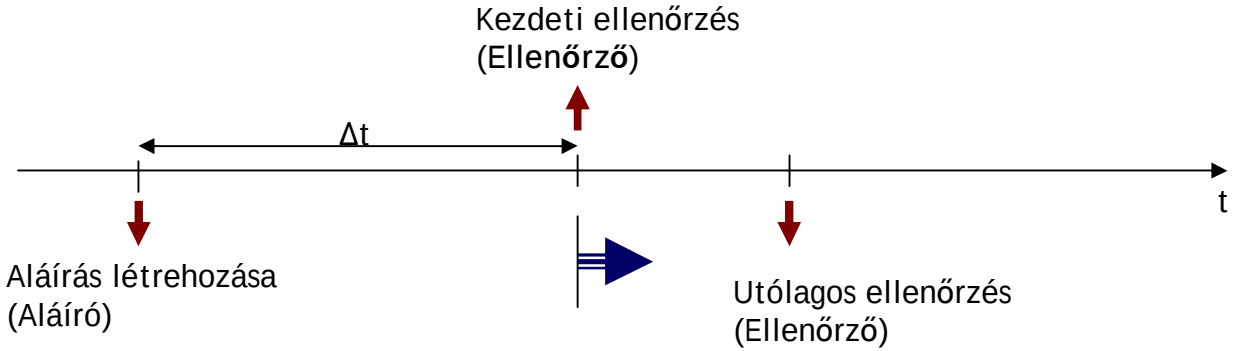
Időbélyeg később kerül az aláírásra

IHM-es ajánlás által elképzelt modell:

Az ügyfelek XAdES–EPES aláírást nyújtanak be, időbélyeget (időjelet) a befogadó fél (hivatal) helyez rá.

Következmény: Az aláírás létrehozása és az időbélyeg elhelyezése között eltelt idő az ügyfél kockázata:

- lejárhat a tanúsítványa,
- ha elveszti a titkos kulcsát, lehet, hogy nem meri visszavonni, mert akkor érvényét veszítheti a korábban benyújtott aláírása.



Problémás helyzetek:

„Apróságok”

- Szükséges az egységes aláírás formátum, kompatibilis szoftverek
  - XMLDSIG (RFC 3275)
  - XAdES (ETSI TS 101 903)
    - IHM ajánlás
    - ETSI TS 102 904 (Profiles…)
    - MEASZ-Ready
- Megbízható HSz tanúsítványának beszerzése
  - *Személyes átvétel,*
  - *Fingerprint ellenőrzése,*
  - *Szoftver telepítő-csomagjával együtt*
- Tanúsítványban levő korlátozások figyelembe vétele
  - pl. tranzakciós limit, Hitelesítési rend, szerep
- Aláírási szabályzatban foglaltak figyelembe vétele

Köszönöm a figyelmet!

Endrődi Csilla
<csilla@microsec.hu>

MICROSEC Kft.
http://www.microsec.hu
http://www.e-szigno.hu