Hosszú távú hiteles archiválás elektronikus aláírás segítségével

Krasznay Csaba
BME Informatikai Központ

BME IK
Informatikai Központ

Tartalom

- Szabályok, szabályzatok
- Érvényességi kritériumok
- Szabványos formátumok
- XAdES aláírási formátumok
- Problémák a hosszútávú hitelesség biztosításával
- Archiválási szolgáltatás

BME IK
Informatikai Központ

Bevezetés

- Az elektronikus aláírás hosszú távú használata szükségessé teszi az így hitelesített dokumentumok archiválását
- Ennek törvényi háttere szabályozott
- A törvény alapján alacsonyabb szintű szabályok is alkothatók
- A technológiai megoldás azonban még nem egészen világos, bár szabvány már készült
- A hiteles archiválás eléréshez az elektronikus aláírás témakörében részt vevő összes szereplőnek részt kell vennie

Törvényi háttér

- A törvényi hátteret az elektronikus aláírásról szóló 2001. évi XXXV. törvény módosításáról szóló 2004. évi LV. törvény teremti meg
- Mivel az elektronikus archiválás a közeljövőben elsősorban az állammal való kommunikációban jelenhet meg, figyelembe kell venni az 1995. évi LXVI. törvényt a közokiratokról
- Minden más irat elektronikus archiválását a 2001. évi CVIII. törvény teszi lehetővé, mely az elektronikus kereskedelemről szól
- Bizonyos elektronikus iratokról szóló rendeletekben (pl. elektronikus számla) nincs külön kiemelve az archiválás kérdése, de a papíralapú szabályozásból az következik

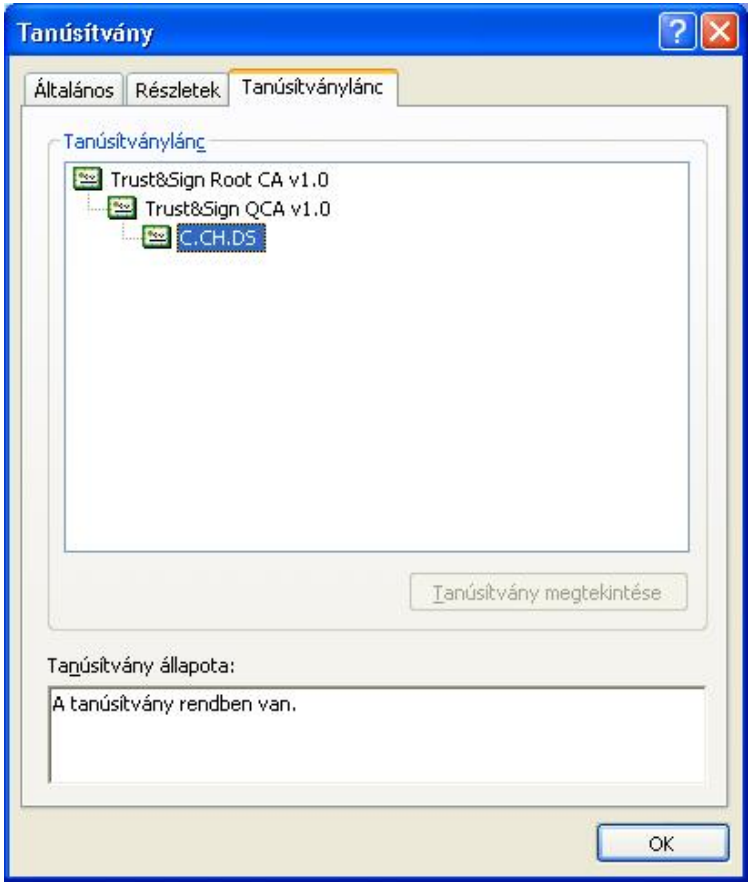
Elektronikus aláírási szabályzat

- Az elektronikus aláírás bevezetése egy szervezetnél nagyon nehéz
- Az iratkezelési szabályzat nem ültethető át egy az egyben elektronikus környezetre
- Figyelembe kell venni:
  - a dokumentumok érvényességi idejét
  - az aláíráshoz szükséges feltételeket
  - a kötelezettségvállalás mértékét
  - az aláírási jogköröket
- Ha a szervezeti szabályokat sikerül is megalkotni, technológiailag még mindig nem megoldott a feladat

Érvényességi idő

- Elektronikus aláírás témakörében három érvényességi idő ismeretes:
  - azonnali ellenőrzésű dokumentumok: az aláírást az első ellenőrzés után többet nem kell megvizsgálni
  - rövid lejáratú dokumentumok: az elektronikus irat maximum a tanúsítvány lejáratáig vagy visszavonásáig érvényes
  - hosszú lejáratú dokumentumok: az elektronikus irat érvényességét a tanúsítvány lejárta vagy visszavonása után is meg kell tudni állapítani
- A három típushoz különböző tanúsítványokat és visszavonási információkat kell tárolni

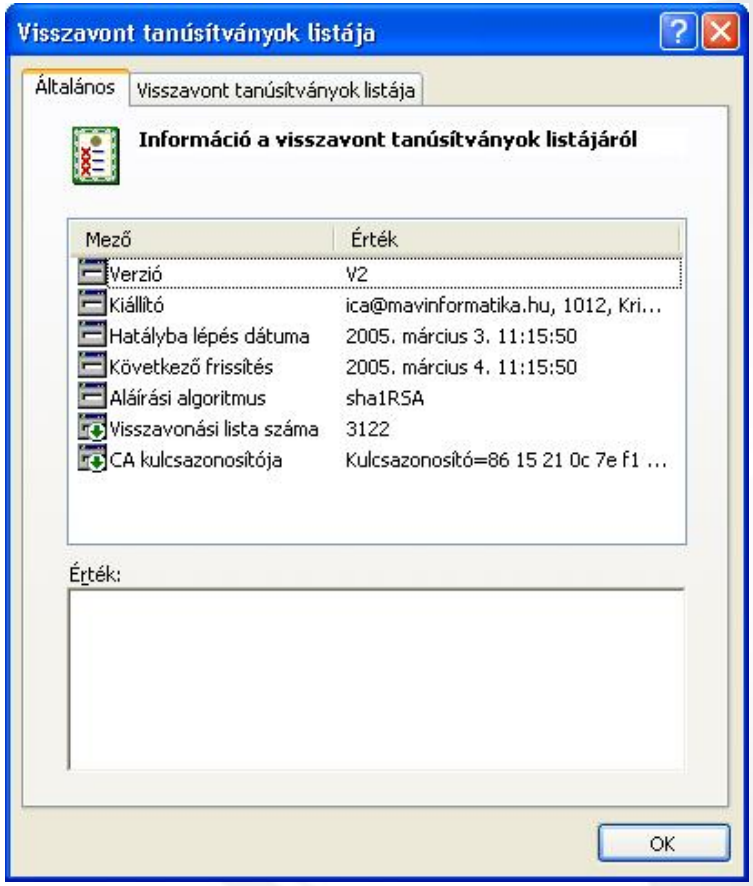
Tanúsítványlánc



- A végfelhasználó tanúsítványát általában a kibocsátási hierarchia harmadik szintjén áll
- Az ilyen tanúsítványokat az ún. produktív CA bocsátja ki
- A hierarchia legfelső szintjén a gyökér vagy root CA áll
- A teljes hitelesítéshez mindhárom tanúsítványra szükség van

Visszavonási lánc

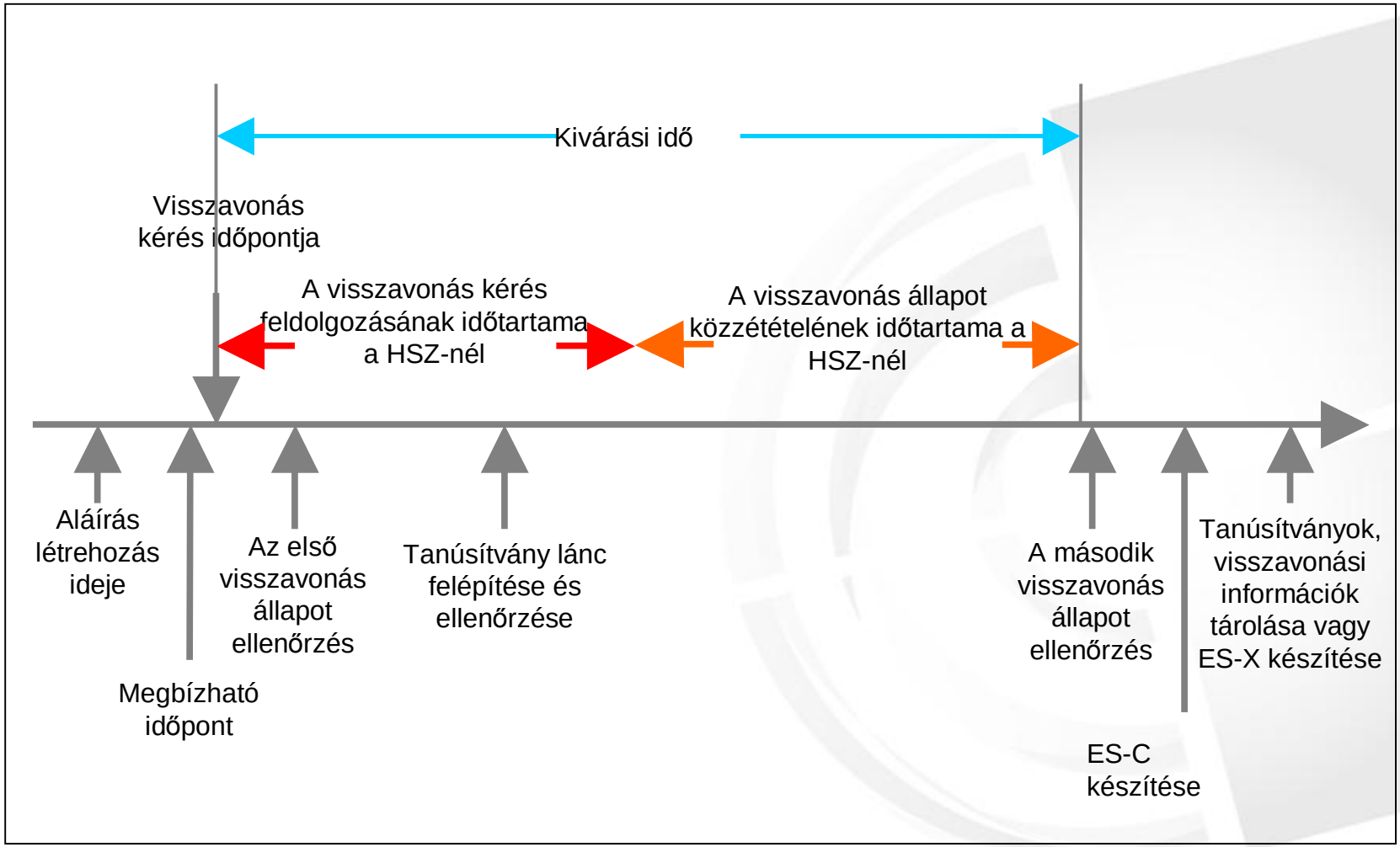
- A végfelhasználói tanúsítványhoz és a produktív CA-hoz tartozik visszavonási lista
- A gyökér CA-nak nincs (legalábbis szabvány szerint nem szükséges) visszavonási listája, a kompromittálódást közzététellel jelzik (out-of-band módon)
- A teljes ellenőrzéshez tehát a gyökér CA-n kívüli összes visszavonási lista kell



Az aláírás hitelességének ellenőrzése

- Az aláírt dokumentum érvényességét három dolog határozza meg:
  - a tanúsítványlánc bármelyik eleme kompromittálódott,
  - a kriptográfiai primitívek erőssége,
  - szervezeti kérdések, pl. a tanúsítványt visszavonták
- Az aláírás időpontja után a lehető leghamarabb valamilyen hiteles, időpontot meghatározó adatot kell szerezni (pl. időbélyegző)
- A „kivárási idő” után minél előbb meg kell szerezni a visszavonási információkat

Kivárási idő



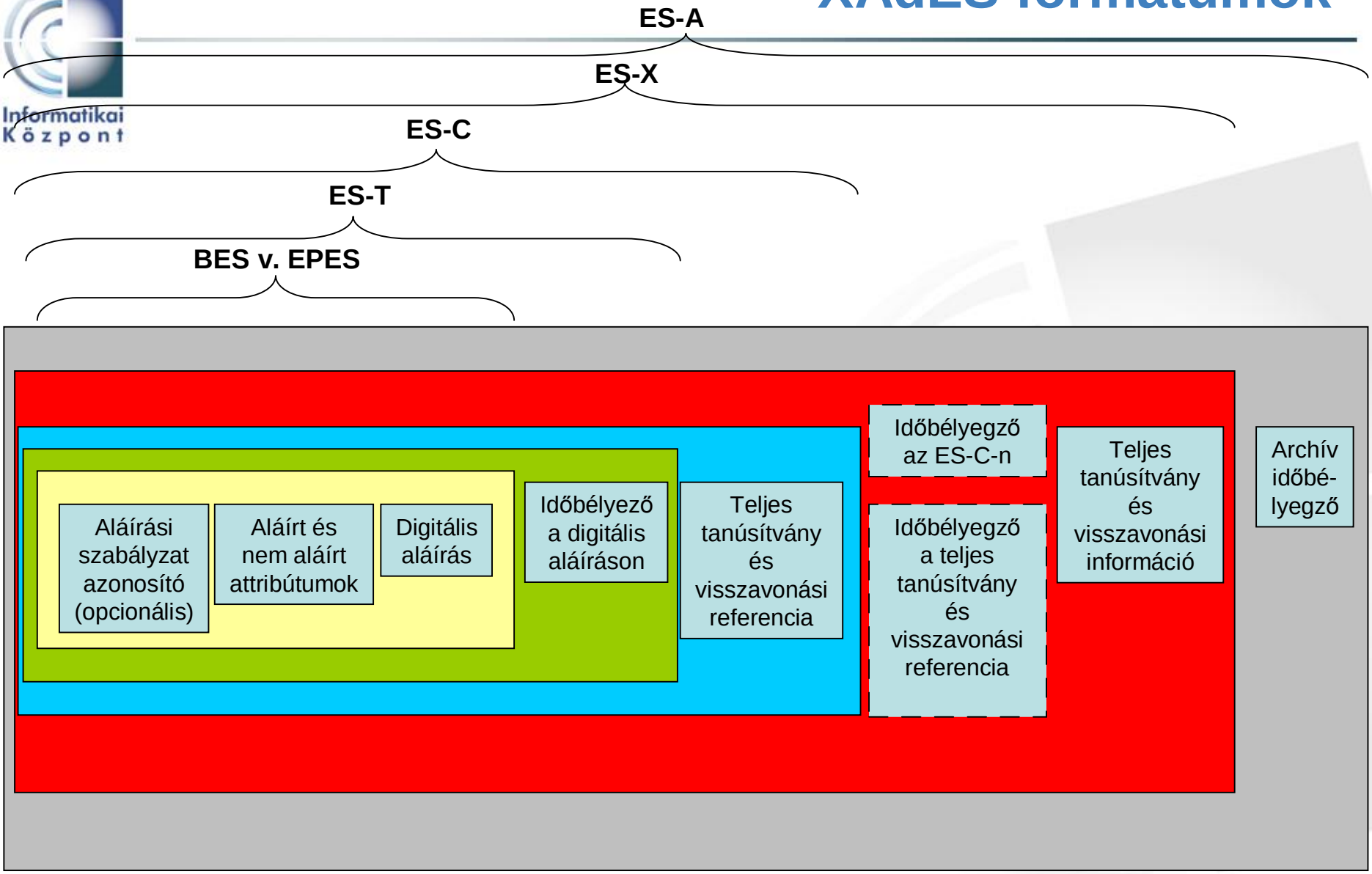
Szabványos aláírás formátumok

- Több szabvány létezik az elektronikus aláírás formátumaival kapcsolatban
- RFC 2633: S/MIME, az elektronikusan aláírt e-mail szabványa
- RFC 3275: XML DSig, az elektronikusan aláírt dokumentumok alapvető XML formátuma
- ETSI TS 101 903: XAdES, az XML DSig kibővített formátuma, mely alkalmas a hosszútávú hitelesség biztosítására

XAdES formátumok

- BES: tartalmazza az elektronikus aláírást és más alapvető információkat, amiket az aláíró ad meg
- EPES: tartalmazza az aláírási szabályzatra mutató hivatkozást
- ES-T: tartalmazza az időbélyegzőt (vagy más, pontos időt meghatározó információt, de ez nem használatos)
- ES-C: tartalmazza a tanúsítási láncra és a visszavonási információkra való hivatkozásokat
- ES-X: tartalmazza a teljes tanúsítási láncot és az összes visszavonási információt
- ES-A: a hosszútávú hitelesség biztosítása egy időbélyegzővel, ami bármikor frissíthető

XAdES formátumok



Problémák hosszútávú archiválás esetén

- Nem érhető el a teljes tanúsítványlánc
- Elképzelhető, hogy az elektronikusan aláírt dokumentum életciklusa alatt megszűnik a végfelhasználói vagy a CA tanúsítványok elérhetősége
- Ez lehetetlenné teszi az aláírás hitelességének ellenőrzését
- Megoldás: tároljuk a teljes tanúsítási láncot az XML struktúrában

Problémák hosszútávú archiválás esetén

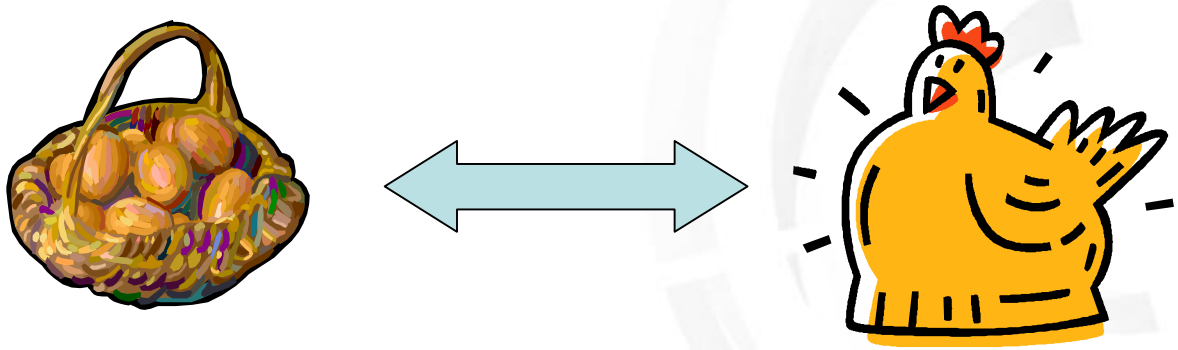
- Egy olyan visszavonási listát kell szerezni, ami az aláírás időpontja után, de még a tanúsítvány lejárta előtt lett kiadva
- A lejárat után kiadott visszavonási listákban már nem szerepel a visszavont tanúsítvány
- Ez a végfelhasználói tanúsítványra viszonylag egyszerűen megoldható, de a CA visszavonási listáját van úgy, hogy csak fél évente adják ki
- A teljes visszavonási lánc felépítése, így a teljesen hiteles elektronikus aláírás lehet, hogy csak fél év alatt építhető fel
- Ráadásul minden visszavonási információt tárolni kell az XML struktúrában, ami adott esetben aránytalanul nagy állományt eredményezhet
- Megoldás (lenne): OCSP válasz, ami azonban még nincs a magyar piacon, és nem is lesz egyhamar

Problémák hosszútávú archiválás esetén

- Az aláírási szabályzat szükséges egy aláírás érvényességének eldöntéséhez szervezeti szempontból
- Erre azonban csak egy link mutat, így évekkel később nehézkes megszerezni
- Ráadásul ennek szentelik a legkisebb figyelmet, holott ezzel lehetnek a legnagyobb visszaélések
- Megoldás: az aláírás időpontjában aktuális aláírási szabályzat tárolása (nem megoldott)

Archiválási szolgáltatók

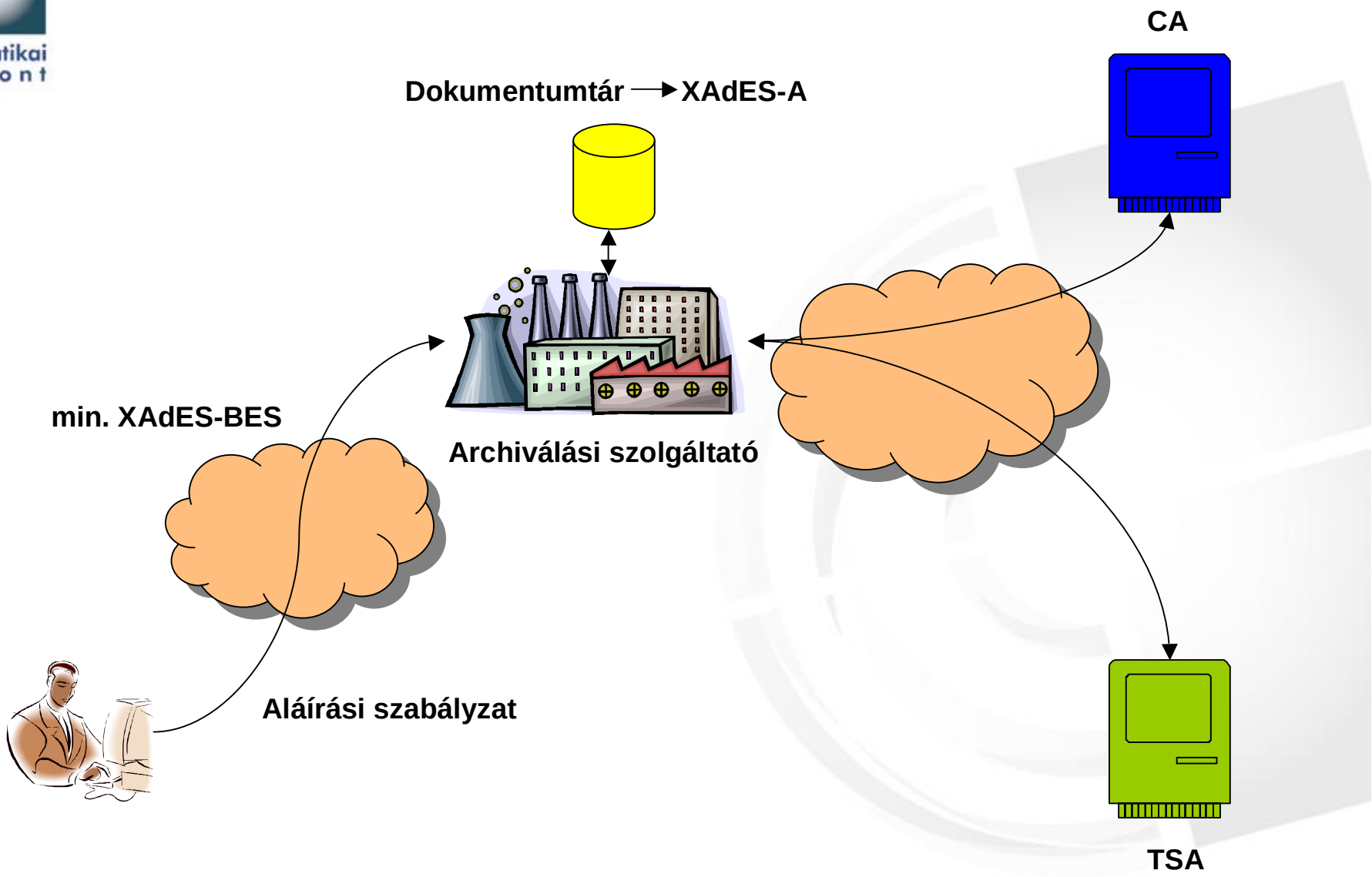
- A fenti problémák megoldása lehet egy archiválási szolgáltató
- Egy készülő IHM rendelet ezeknek is olyan feltételeket szab meg, mint a minősített hitelesítés-szolgáltatóknak
- Kellő rendelkezésre-állással és tárhellyel kell rendelkezniük
- Itt is jelentkezik a hitelesítés-szolgáltatás tyúk-tojás problémája



Piac

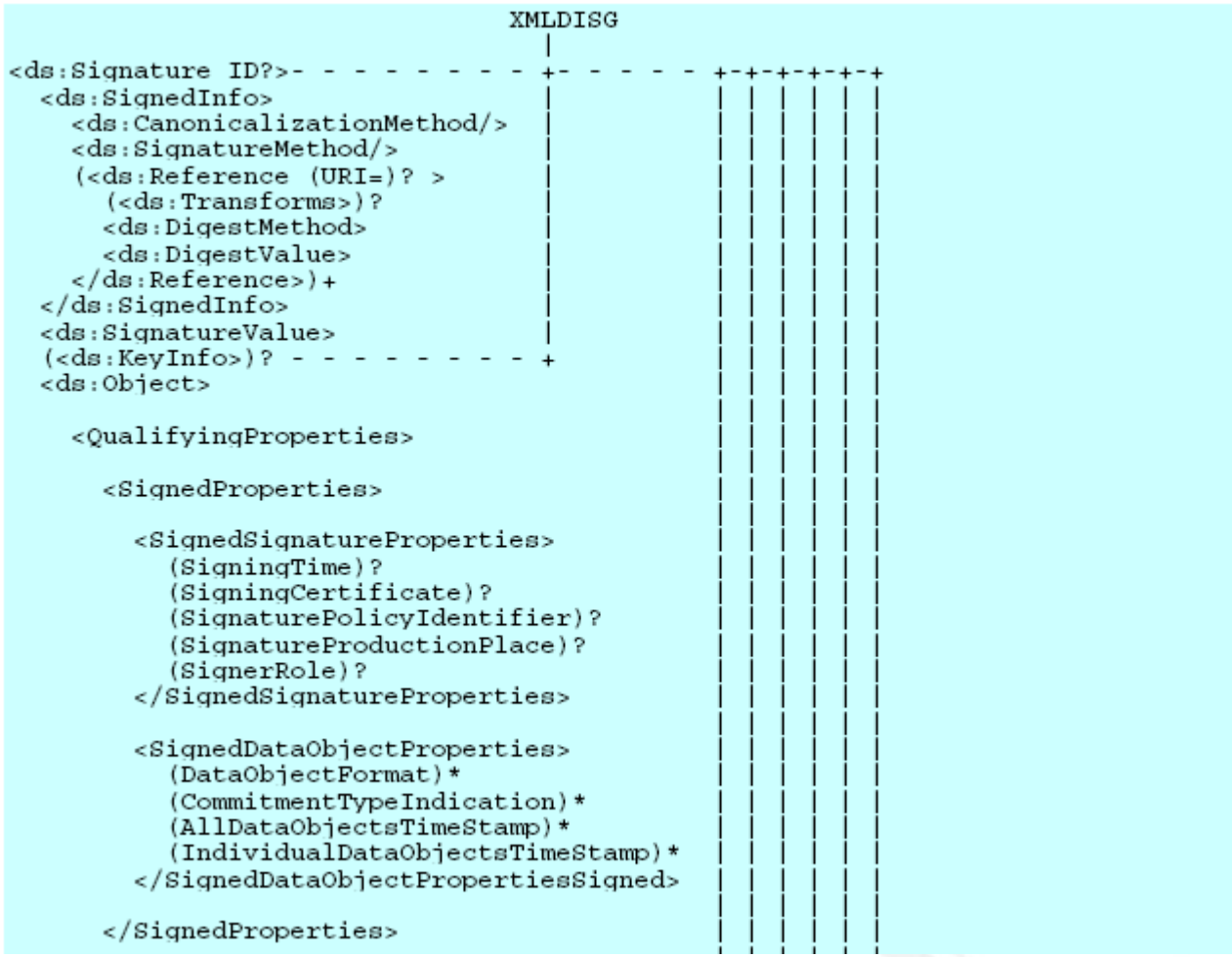
Szolgáltatás

Az archiválási szolgáltató architektúrája

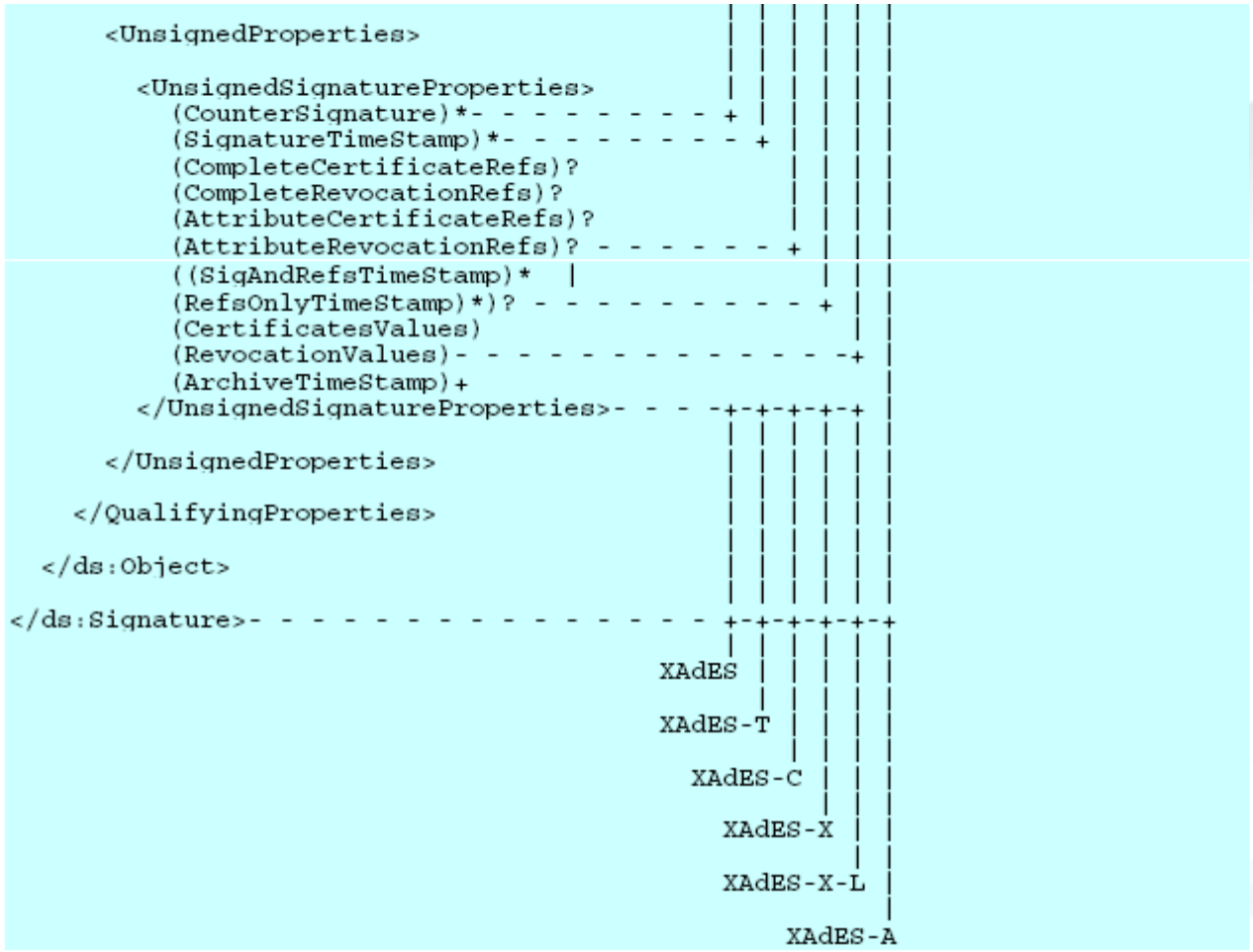


BME IK
Informatikai Központ

XAdES struktúra



XAdES struktúra



Archív időbélyegző

- Mielőtt
  - egy kulcs, algoritmus vagy más kriptográfiai adat, melyet az ES-C létrehozásához felhasználtak, gyengévé válna, vagy
  - az első időbélyegzőhöz felhasznált tanúsítvány lejárna
  - a teljes struktúrát újra időbélyegezni kell.
- Ekkor erősebb algoritmusok vagy hosszabb kulcsok is felhasználhatók
- Az időbélyegzési eljárás bármennyiszer felhasználható a korábbi ES-A struktúrán
- Ez praktikusan sok időbélyegző hozzáadását jelenti a kiinduló állapothoz képest

XAdES-A megvalósítások

- A létrehozási és tárolási nehézségek miatt eddig még nem nagyon készültek implementációk
- Németországban van olyan szolgáltató, aki a fenti elvet használja
- Ausztriában készült szoftver, amit képes XAdES-A-t előállítani
- A Microsoft európai fejlesztői jelen vannak ezen a területen
- Magyarországon az elektronikus közigazgatási keretrendszer megemlíti, de rövidtávon nem számol vele
- A Neptun.Net rendszer elektronikus számlázó moduljában megjelenik ez a szabvány
- Ez lesz valószínűleg egész Európában az első tömeges használata a hitelesen archivált elektronikus dokumentumoknak

Források

- CEN CWA 14171: General guidelines for electronic signature verification
- ETSI TS 101 903 v.1.2.2.: XML Advanced Electronic Signatures (XAdES)
- Szabó Áron cikkei az IT.News.hu oldalon
- A Magyar Elektronikus Aláírás Szövetség (MELASZ) formátum munkacsoportjának ülései

Köszönöm figyelmüket!

Krasznay Csaba

Budapesti Műszaki és Gazdaságtudományi Egyetem

Informatikai Központ

krasznay@ik.bme.hu