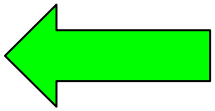
MICROSEC
Számítástechnikai Fejlesztő Kft.

Minősített archiválás szolgáltatás beindítása Magyarországon

Dr. Berta István Zsolt - Endrődi Csilla Éva
istvan.berta@microsec.hu - csilla@microsec.hu
Microsec Kft.

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?

Elektronikus aláírás (e-szignó)?

- Az elektronikus aláírás a kódolás egy fajtája;
- Elektronikus aláíráskor az aláírás-létrehozó adat (magánkulcs) alapján kódoljuk az aláírt dokumentumot;
- A kódolás az aláírás-létrehozó adat ismeretében „könnyű”, nélküle „nehéz” feladat;
- Az aláírást bárki ellenőrizheti az aláíró tanúsítványa alapján.

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 érvényes egy elektronikus aláírás?

- „Alap” aláírás:
  - amíg az aláíró tanúsítványa érvényes.
- Időbélyeggel ellátott aláírás:
  - amíg az időbélyegző tanúsítványa érvényes
  - ~10 évig (7/2005. IHM r.)
- Ha azt szeretnénk, hogy az elektronikus aláírás ennél tovább is érvényes maradjon (7/2005. IHM r.):
  - archiválás szolgáltatás vagy
  - rendszeres időbélyegzés

Elektronikusan aláírt adat archiválása

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

„Házilag”
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 Hírközlési Hatóság vezet nyilvántartást.

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.

Érdekes kérdések – Amiről beszélni fogok…

- 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

Követelményrendszer

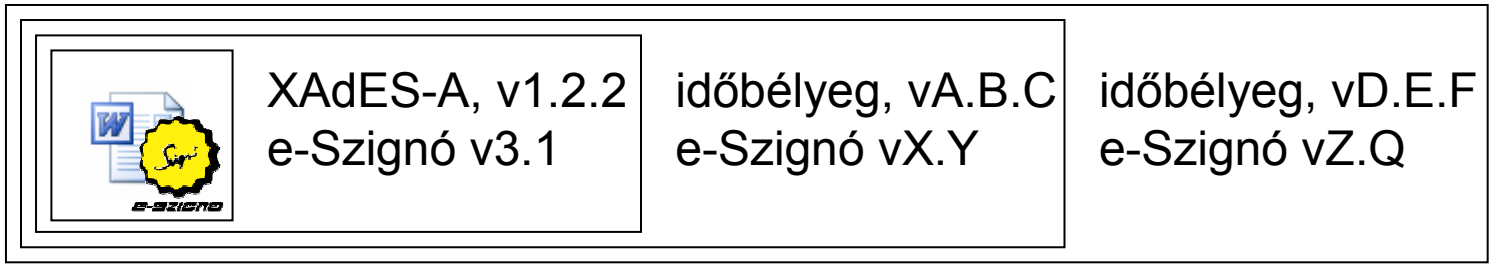
- Az elektronikus archiválás szolgáltatást a magyar Eat. határozza meg.
- Külföldön is ismert fogalom, de ott nem a törvényben van benne.
- Külföldön sem elterjedt jelenség.
- Új terület, nem létezik rá a hitelesítés szolgáltatáséhoz hasonlóan letisztult és elfogadott követelményrendszer, nem beszélhetünk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

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
  - csak internet draftok vannak/voltak
    Első RFC: RFC 4810, 2007 március.
  - 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.
- Döntésünk: csak befogadáskor archív aláírás, később más.

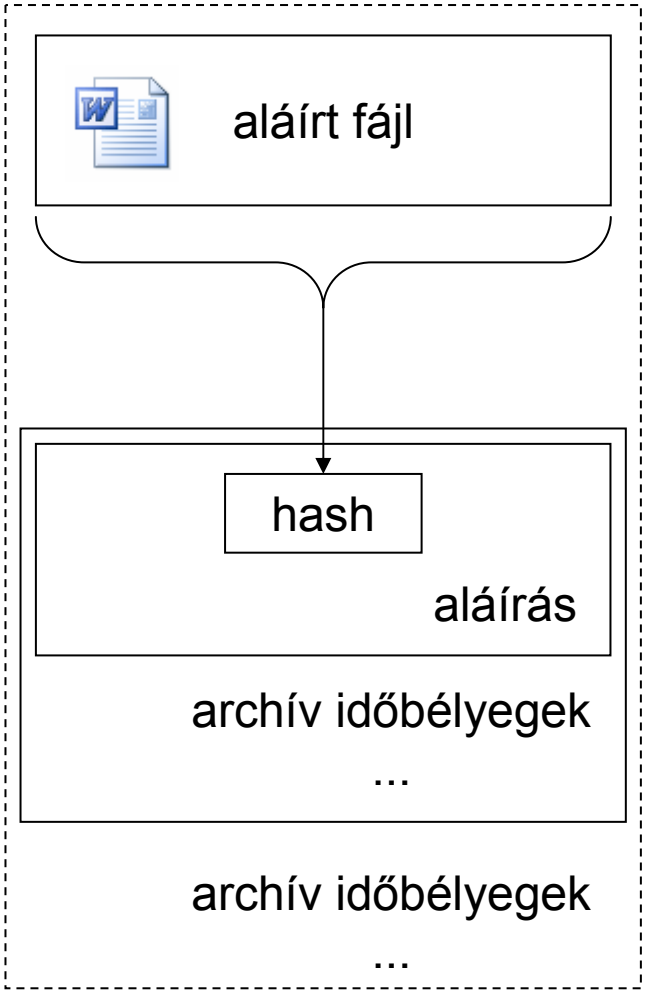
Aláírt dokumentum vagy aláírt lenyomat archiválása

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



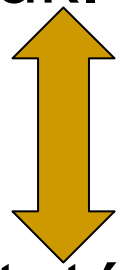
- nem véd a dokumentum megsemmisülése ellen ☹
- az ügyfélnek rendszeresen foglalkoznia kell a dokumentummal ☹
- ha rossz lenyomat jön be, az csak sokára derül ki
- az ügyfél „bukja” az archiválást, ha nem időben küldi be a lenyomatot ☹

Döntés: A teljes e-akta archiválását választottuk.

Az archivált e-akták bizalmassága

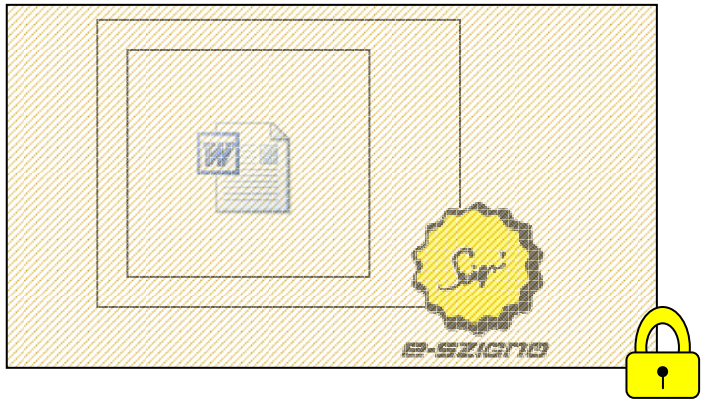
Követelmények bizalmasságra

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

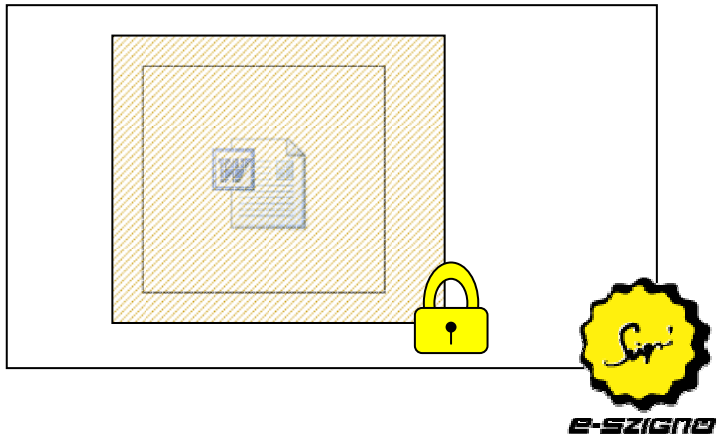


- Az archív szolgáltatónak befogadáskor ellenőriznie kell az elektronikus aláírást.
- Az archív szolgáltatónak rendszeresen időbélyeget (és aláírást) kell elhelyeznie a dokumentumokon.

Titkosítás ↔ Aláírás



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



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

Hogyan döntöttünk?

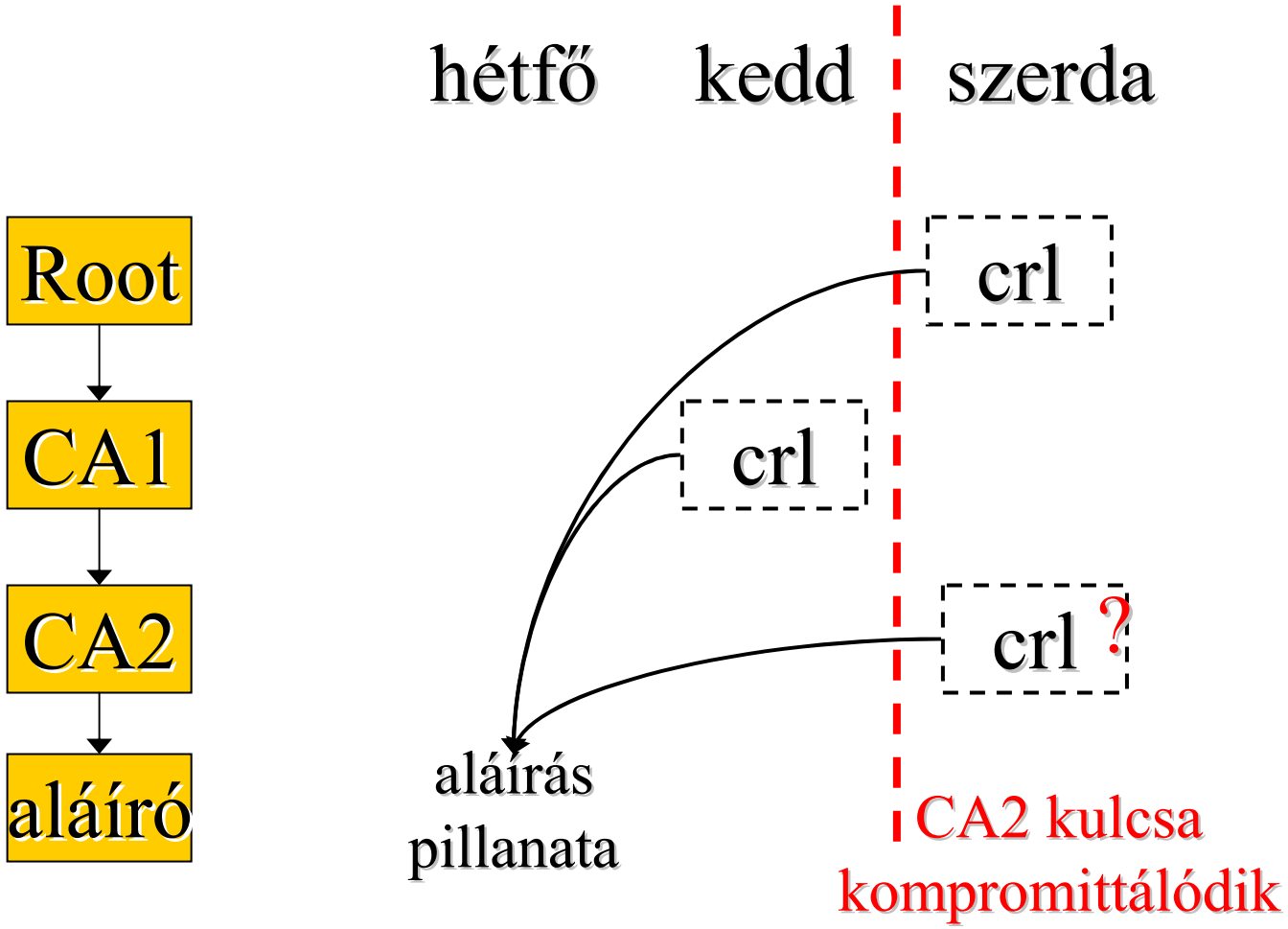
- Feltöltéskor a nyílt e-aktán automata ellenőrzi az aláírást.
- Az archív szolgáltató a titkosított e-aktát archiválja.
- A titkosított e-aktát az ügyfél bármikor letöltheti, visszafejtheti.
- Az archív szolgáltató különleges eljárás keretében, tudja dekódolni az archivált e-aktákat.
- A nyílt e-aktára ritkán van szükség:
  - ha a használt hash algoritmus elavulása fenyeget.
  - ha valamely titkosító algoritmus elavulása fenyeget
  - ha az ügyfél titkosító tanúsítványa változik
- Más esetben nem fejtjük vissza az e-aktát.

Az érvényességi lánc felépítése

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…)

Példa: Az aláírás időpontja utáni CRL…



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 biztosítása

Értelmezhetőség, megjeleníthetőség

- Aláírás: kötelezettségvállalás valamely értelmes tartalom iránt.
- Az értelmes tartalom egy fájlban (pl. doc, pdf) helyezekedik 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 (!)

Összefoglalás

- 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.

Köszönöm a figyelmet!

MICROSEC
Számítástechnikai Fejlesztő Kft.

Minősített archiválás szolgáltatás beindítása Magyarországon

Dr. Berta István Zsolt - Endrődi Csilla Éva
istvan.berta@microsec.hu - csilla@microsec.hu
Microsec Kft.