

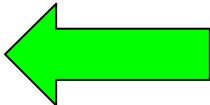
Minősített archiválás szolgáltatás beindítása Magyarországon

Dr. Berta István Zsolt - Endrődi Csilla Éva

istvan.bertha@microsec.hu - csilla@microsec.hu

Microsec Kft.

Mit értünk aláírás alatt?

- n kötelezettségvállalás, egy dokumentum tartalmának elfogadása? 
- n bizonyíték ezen kötelezettségvállalásra?
 - q ...tinta és a papír kapcsolata...
 - q ...kriptográfiai művelet...
- n bizonyító erő, amivel ez a bizonyíték rendelkezik?

Elektronikus aláírás (e-szignó)?

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

Mitől válhat egy aláírás érvénytelenné?

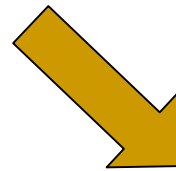
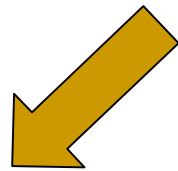
- n A kötelezettségvállalás nem válik érvénytelenné. Az fordulhat elő, hogy már nem bizonyítható, hogy a kötelezettségvállalás valóban megtörtént.
- n Mi okozhatja ezt?
 - q Ha már nem bizonyítható, hogy az aláíró tanúsítványa érvényes volt akkor, amikor az aláírás készült; (e probléma időbélyeggel orvosolható)
 - q Időbélyegzés szolgáltatók tanúsítványának lejárta;
 - q Időbélyegzés szolgáltatók meghibásodása vagy a magánkulcsának kompromittálódása;
 - q A tudomány vagy a technológia hirtelen, ugrásszerű fejlődése.

Meddig érvényes egy elektronikus aláírás?

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

- n Az archiválás szolgáltató megbízható rendszerrel ellenőrzi, és biztonságos módon eltárolja az archiválandó aláírást.
- n Az archiválás időtartama alatt a jogszabályi előírások szerint folyamatosan biztosítja az archivált aláírások hitelességét.
- n Ügyfelei kérésére igazolást állít ki arról, hogy egy adott aláírás érvényes.
- n Ha minősített archiválás szolgáltató archivál egy aláírást, vélelmezni kell, hogy az aláírás érvényes.
- n A szolgáltatást az Eat. definiálja.
- n A minősített archiválás szolgáltatókról a Nemzeti Hírközlési Hatóság vezet nyilvántartást.

Hosszú táv, Változó környezet

- n Az archiválás szolgáltató hosszú távon, hosszú ideig (20 év, 50 év, ...) kell, hogy működjön. Ennyi idő alatt megváltozhatnak
 - q a biztonságos kulcsméretetek, algoritmusok;
 - q az elfogadott gyökér-tanúsítványok;
 - q a szolgáltatók hitelesítési/időbélyegzési rendjei;
 - q az elektronikus aláírás ellenőrzésére vonatkozó követelmények;
 - q az aláírások és érvényességi láncok formátumára vonatkozó specifikációk;
 - q az elektronikus aláírásra és az archiválásra vonatkozó jogszabályok, specifikációk.
 - q ...
- n Alapvetően megváltozhat az aláírás fogalma, és az aláírás ellenőrzésének módja.

Érdekes kérdések - Amiről beszélni fogok...

- n Követelményrendszer, minősítés
- n Aláírt dokumentum vagy aláírt lenyomat archiválása?
- n Az archivált e-akták bizalmassága
- n Hogyan gyűjti össze az archiválás szolgáltató az aláírás ellenőrzéséhez szükséges információkat, hogyan építi fel az érvényességi láncot?
- n Az aláírt dokumentumok hiteles megjeleníthetőségének, értelmezhetőségének biztosítása

Követelményrendszer

Követelményrendszer


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

Milyen best practice-ek léteznek?

- n Az archív aláírás hasonló problémát old meg, és erre léteznek letisztult nemzetközi specifikációk – pl. ETSI TS 101 903 (XAdES)
- n Long-Term Archive and Notary Services
 - q archív szolgáltatást céloz meg, nem archív aláírás, hanem adatbázis-alapon
 - q csak internet draftok vannak/voltak
Első RFC: RFC 4810, 2007 március.
 - q <http://ietfreport.isoc.org/ids-wg-ltans.html>

Archiválás szolgáltatás ↔ Archív aláírás

- n Az archív szolgáltató feladata az aláírások hosszú távú hitelességének biztosítása;
- n Ezt teheti például archív aláírással is, de nem feltétlenül ezt a technológiát kell alkalmaznia.
- n Archív aláírás bizonyíthatja egy aláírás hitelességét, de hosszú távon nem lesz egyszerű értelmezni egy archív aláírást.

	XAdES-A, v1.2.2 e-Szignó v3.1	időbélyeg, vA.B.C e-Szignó vX.Y	időbélyeg, vD.E.F e-Szignó vZ.Q
------------------------------------------------------------------------------------	----------------------------------	------------------------------------	------------------------------------

- n Nincs olyan XAdES-verzió, amelynek ez megfelelné, nincs olyan e-Szignó verzió, amely ilyen aláírást hozna létre...
- n Az archív szolgáltató igazolásainak lesz jelentősége.
- n Döntésünk: csak befogadáskor archív aláírás, később más.

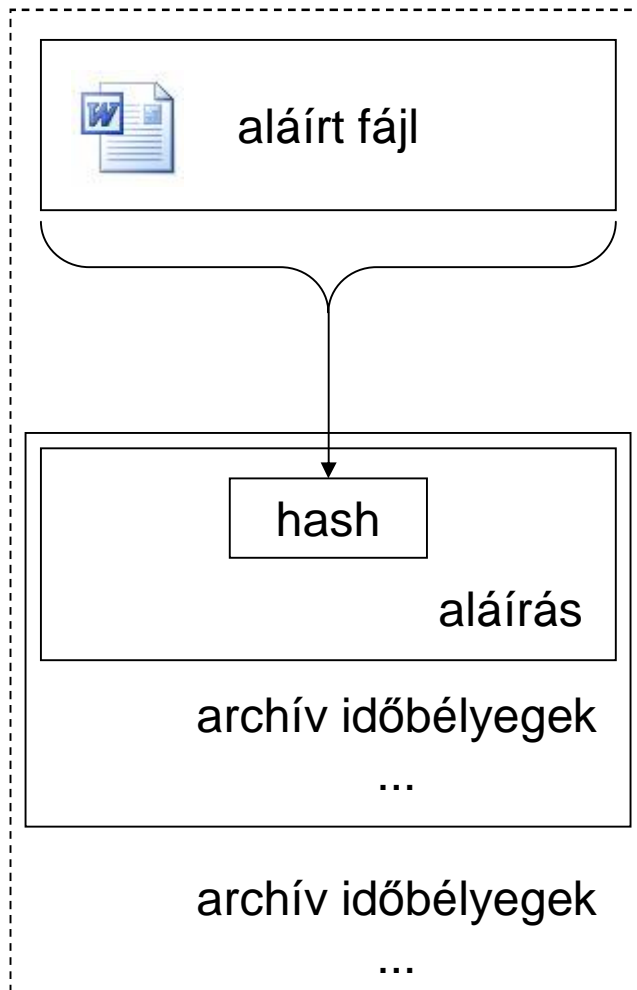
Aláírt dokumentum vagy aláírt lenyomat archiválása

Aláírt dokumentum/lenyomat archiválása

Az Eat. kétféle archiválás szolgáltatást definiál:

- n Az archív szolgáltató az aláírt dokumentumot (e-aktát) archiválja.
 - q logikailag tiszta megoldás
- n Az archív szolgáltató csak az aláírást kapja meg, az aláírt dokumentumot nem:
 - q a bizalmasság biztosítása egyszerű **J**
 - q a dokumentum és az aláírás elválik egymástól **L**
 - q nem véd a hash algoritmus elavulása ellen... **L**

Gondok a csak lenyomat archiválásával



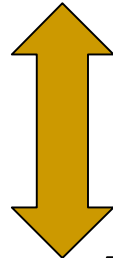
- n nem véd a dokumentum megsemmisülése ellen **L**
- n az ügyfélnek rendszeresen foglalkoznia kell a dokumentummal **L**
- n ha rossz lenyomat jön be, az csak sokára derül ki
- n az ügyfél „bukja” az archiválást, ha nem időben küldi be a lenyomatot **L**

Döntés: A teljes e-akta archiválását választottuk.

Az archivált e-akták bizalmassága

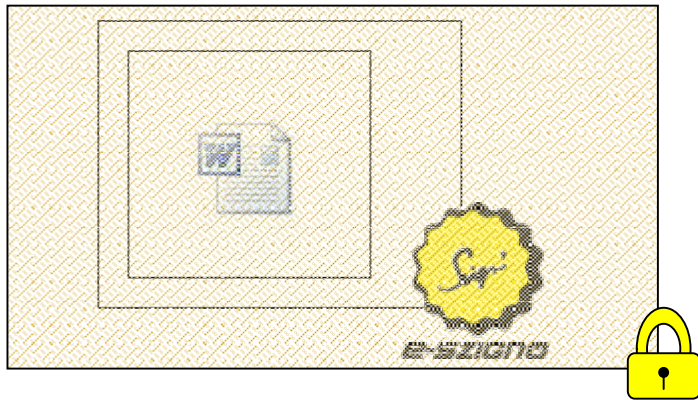
Követelmények bizalmasságra

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

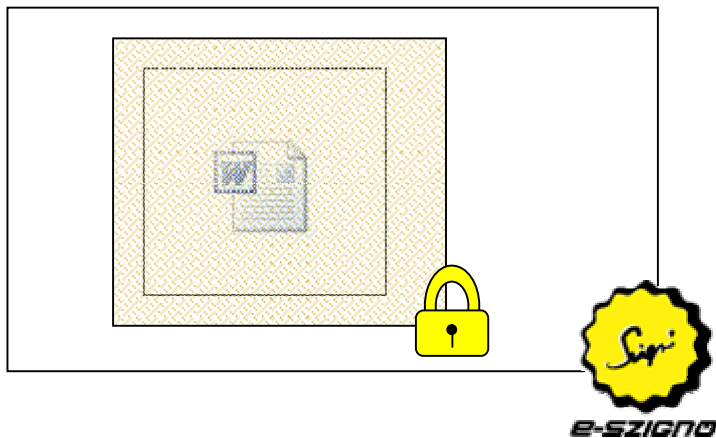


- n Az archív szolgáltatónak befogadáskor ellenőriznie kell az elektronikus aláírást.
- n Az archív szolgáltatónak rendszeresen időbélyeget (és aláírást) kell elhelyeznie a dokumentumokon.

Titkosítás ↔ Aláírás



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



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

Hogyan döntöttünk?

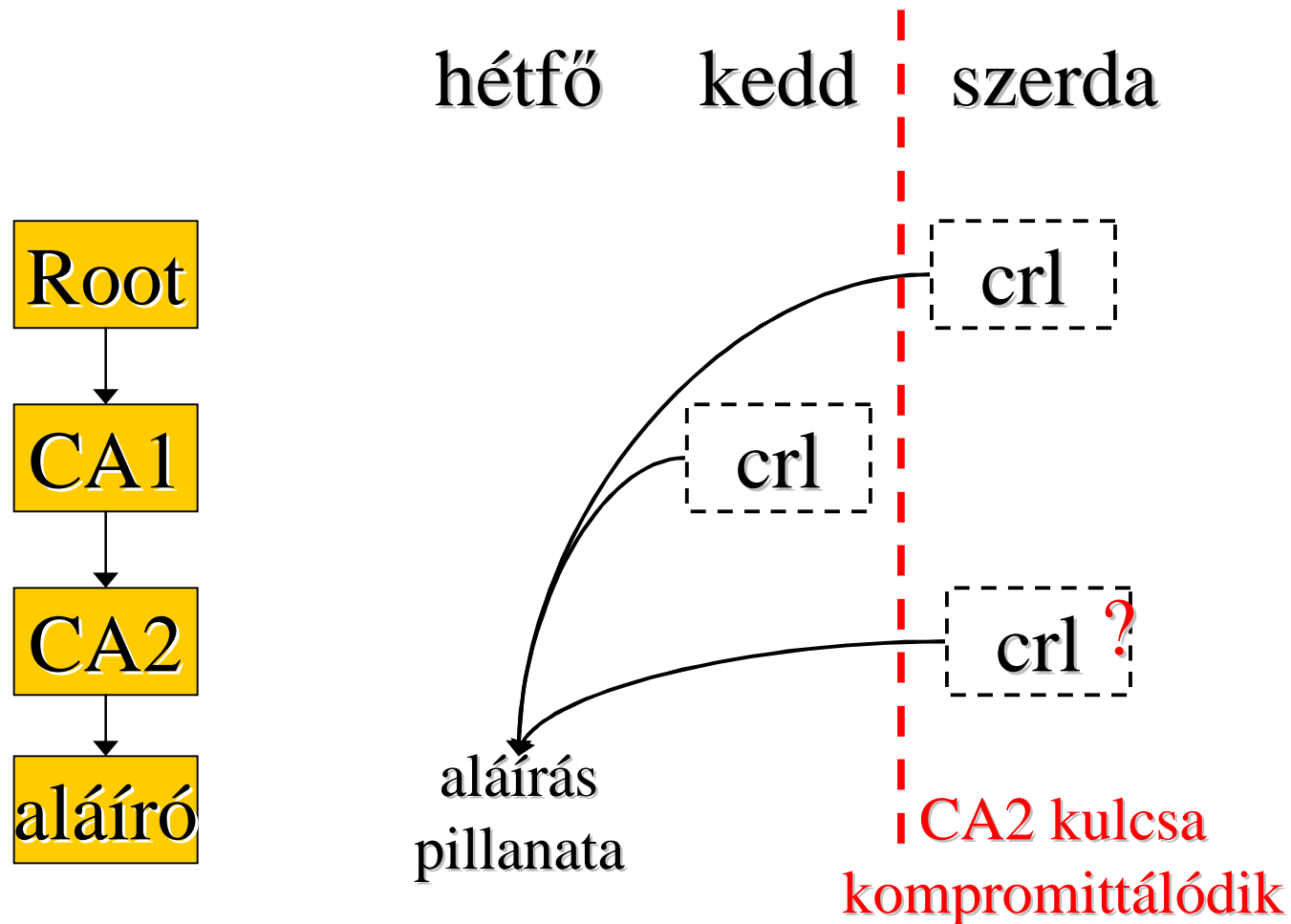
- n Feltöltéskor a nyílt e-aktán automata ellenőrzi az aláírást.
- n Az archív szolgáltató a titkosított e-aktát archiválja.
- n A titkosított e-aktát az ügyfél bármikor letöltheti, visszafejtheti.
- n Az archív szolgáltató különleges eljárás keretében, tudja dekódolni az archivált e-aktákat.
- n A nyílt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

Az érvényességi lánc felépítése

Miért nem CRL?

- n Két külön feladat:
 - q megbizonyosodni egy aláírás érvényességéről (kivárási idő),
 - q beszerezni az aláírás érvényességét igazoló bizonyítékokat.
- n CRL alapján bonyolult elvégezni az ellenőrzést. Rendkívül komplex problémák is megjelenhetnek.
- n CRL esetén a visszavonási információk különböző időpillanatokból származnak, az archiválás szolgáltató nem tudja ezt befolyásolni.
- n (Tapasztalat: CRL alapon általában is nehéz valós problémákat megoldani...)

Példa: Az aláírás időpontja utáni CRL...



Miért OCSP?

- n OCSP segítségével az ellenőrzés azonnal elvégezhető, így megoldható, hogy minden visszavonási információ közel egy időpontból származzon.
- n Ekkor **sokkal** egyszerűbb problémával állunk szemben.
- n Döntés: Az aláírásokat OCSP alapon ellenőrizzük.
- n HSZ kulcs kompromittálódás – felelősségi problémák
- n Döntés: Induláskor kizárólag az általunk kibocsátott tanúsítványokat fogadjuk el, ezt később kiterjesztjük más „OCSP-s” hitelesítés szolgáltatókra is.
- n A közigazgatási, „KGYHSZ-es” tanúsítványokra elvileg sem lehet (értelmesen) archiválás szolgáltatást nyújtani (3/2005 IHM r. ↔ KGYHSZ hitelesítési rend J)

Értekezhetőség biztosítása

Értelmezhetőség, megjeleníthetőség

- n Aláírás: kötelezettségvállalás valamely értelmes tartalom iránt.
- n Az értelmes tartalom egy fájlban (pl. doc, pdf) helyezkedik el.
- n Előfordulhat, hogy (pl. 20-30 évvel) később nem lehet majd megjeleníteni a ma használt fájlformátumokat...
- n Hiába igazoljuk, hogy milyen bitsorozatot írt alá valaki, az értelmes tartalmat kellene igazolnunk.
- n Megjelenítés hitelessége (!)
- n Aktív tartalom, makrók (!)

Összefoglalás

- n Az elektronikusan aláírt dokumentumokat speciális körülmények között kell archiválni.
- n Az archiválás bonyolult feladat, jelentős szaktudás és drága infrastruktúra szükséges hozzá.
- n A minősített archiválás szolgáltató ezeket egységesen, professzionális módon oldja meg:
 - q az archiválás szolgáltató anyagi felelősséget vállal azért, hogy az ügyfél iratai megmaradnak és hitelesek;
 - q az ügyfél igazolhatja, hogy kellő gondossággal járt el;
 - q a bíróságnak vélelmeznie kell, hogy a minősített archiválás szolgáltató által archivált aláírás érvényes („házi” megoldás esetén nincs ilyen jogkövetkezmény);
 - q biztosíthat megjeleníthetőséget, értelmezhetőséget.

Köszönöm a figyelmet!

Minősített archiválás szolgáltatás beindítása Magyarországon

Dr. Berta István Zsolt - Endrődi Csilla Éva

istvan.bertha@microsec.hu - csilla@microsec.hu

Microsec Kft.