

Elektronikus archiválás szolgáltatás

Dr. Berta István Zsolt, PhD, MBA, CISA
Microsec Kft.

istvan.berta@microsec.hu

www.e-szigno.hu

Elektronikus archiválás szolgáltatás

- Az elektronikus aláírással ellátott dokumentumok archiválását jelenti.
- Az archiválás szolgáltató speciális körülmények között tárolja e dokumentumokat, hogy hitelességük, bizonyító erejük hosszú távon (akár 20 vagy 50 évig) is megmaradjon.
- Az elektronikus aláírásról szóló törvény definiálja az elektronikus archiválás szolgáltatást.
- Ma Magyarországon a Microsec Kft. az egyetlen hatóságilag nyilvántartásba vett, minősített elektronikus archiválás szolgáltató.
- A MonDoc irat- és dokumentumkezelő rendszer együtt tud működni ezen archiválás szolgáltatással.

Microsec Kft.

- Alapítva: 1984
- Az Igazságügyi Minisztérium szolgáltatója (1990-től)
- Elektronikus aláírás hitelesítés szolgáltatás és időbélyegzés szolgáltatás 2002-től, minősített szolgáltatások 2005-től
- Az összes magyarországi pénzügyintézet e-szignóval jelenti a számlaszám-változásokat a cégbíróságoknak (2002-től)
- Elektronikus cégeljárás megvalósítása, üzemeltetése (2005-től)
- Elektronikus aláírás **minden közjegyző** részére (2006-tól)

Elektronikus aláírás (e-szignó) (1)

- Az elektronikus aláírás a kódolás egy fajtája.
- Elektronikus aláíráskor ún. aláírás-létrehozó adat alapján kódoljuk a az aláírt dokumentumot.
- A kódolás az aláírás-létrehozó adat nélkül nem végezhető el (nem létezik rá hatékony algoritmus).
- Az aláírást bárki ellenőrizheti, ehhez az aláíró tanúsítványa szükséges, amelyet hitelesítés szolgáltató bocsát ki.
- Az elektronikus aláírást jogszabály is elismeri.

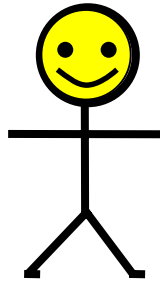
Elektronikus aláírás (e-szignó) (2)



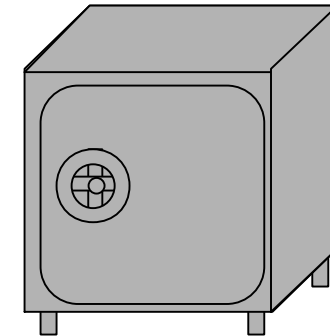
Mit biztosít az elektronikus aláírás?

- Az elektronikusan aláírt dokumentum **hiteles**, tehát bizonyítható, hogy
 - ❑ az aláírás valóban az aláíró kártyájával készült,
 - ❑ az aláírt dokumentum nem változott meg az aláírás óta.
- Az aláírt dokumentum **minden másolata is hiteles**, teljesen egyenértékű az „eredetivel”.
- A dokumentum hitelességét nem befolyásolja, hogy hol illetve kinél van.
- Nem lehet úgy megváltoztatni a dokumentumot, hogy az aláírás érvényes maradjon.

Tanúsítványok és hitelesítés szolgáltatás



Gipsz Jakab



hitelesítés szolgáltató
(minősített / fokozott)



a hitelesítés szolgáltató tanúsítványt állít ki

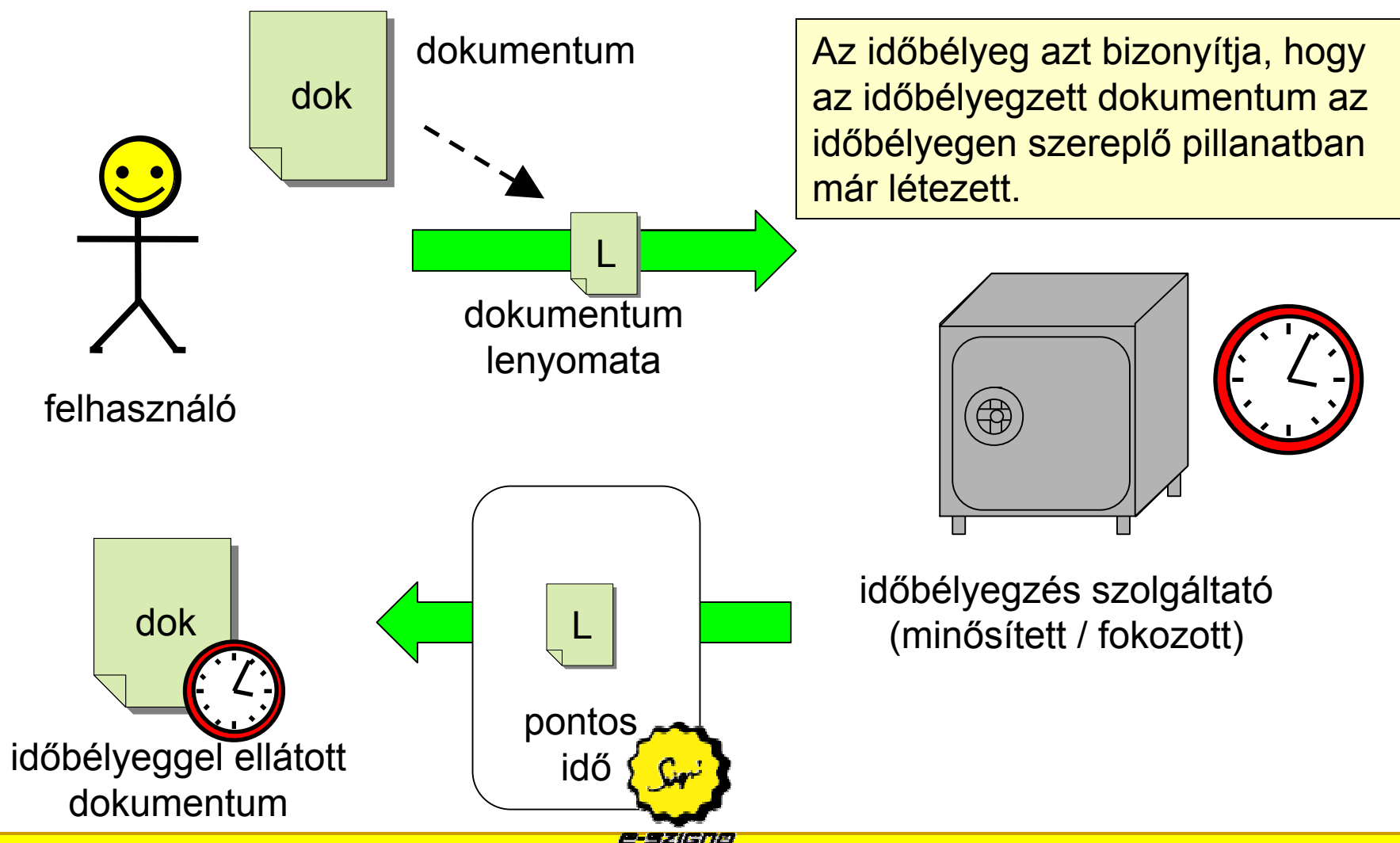
2001. évi XXXV tv. az elektronikus aláírásról

- 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.

Meddig hiteles egy elektronikus aláírás?

- Az aláírás egy kötelezettségvállalás. Az elektronikus aláírás ennek egy bizonyítéka.
- „Egyszerű” aláírás:
 - amíg az aláíró tanúsítványa érvényes.
- Időbélyeggel védett aláírás:
 - amíg az időbélyegző tanúsítványa érvényes.
 - ~10 évig (7/2005. IHM r.)
- Ha azt szeretnénk, hogy az elektronikus aláírás ennél tovább is hiteles maradjon (7/2005. IHM r.):
 - archiválás szolgáltatás vagy
 - saját magunk kell ellátni az archiválás szolgáltató feladatait...

Időbélyegzés szolgáltatás



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 nem bizonyítható, hogy az aláírás mikor készült;
(e probléma időbélyeggel orvosolható)
 - Időbélyegzés szolgáltatók tanúsítványának lejárta;
 - Időbélyegzés szolgáltatók meghibásodása vagy a magánkulcsának kompromittálódása;
 - A tudomány vagy a technológia hirtelen, ugrásszerű fejlődése.

Hogyan őrizhetjük meg az aláírás hitelességét?

- Össze kell gyűjteni minden olyan információt, amely igazolja, hogy az aláíró tanúsítványa aláíráskor érvényes volt.
- Mindezt időbélyeggel kell ellátni.
- Folyamatosan figyelni kell, hogy az várhatóan megkérdőjelezhetővé válik-e az időbélyeg hitelessége.
- Szükség esetén az összegyűjtött adatokat további időbélyeggel kell ellátni, de előtte csatolni kell az időbélyeg érvényességét igazoló információkat.
- Archív aláírások (ETSI TS 101 903)
- LTANS (RFC 4810)
- Jogszabály: 7/2005 IHM rendelet

Archiválás szolgáltató

- Az archiválás szolgáltató megbízható, bevizsgált 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, és a dokumentumot nem változtatták meg.
- A minősített archiválás szolgáltatókról a Nemzeti Hírközlési Hatóság vezet nyilvántartást.

Biztonság

- Feltöltés, letöltés védett csatornákon (pl. ssl) keresztül
- Az archivált fájlokat fizikailag biztonságos környezetben tároljuk, titkosítva. A titkosítást a beküldő mellett az archiválás szolgáltató fejtheti vissza
 - bevizsgált, különleges eljárás, több bizalmi munkakört betöltő tisztviselő együttes jelenlétében,
 - csak előre meghatározott esetekben kerül rá sor,
 - a dekódoló kulcs nincsen jelen a rendszerben.
- Redundáns rendszer, két fizikai helyszín
- Az integritást aláírások + időbélyegek biztosítják
- Megjeleníthetőség, értelmezhetőség biztosítása
- Felelősségbiztosítás
- ISO 9001, ISO 27001, NHH felülvizsgálat

Hogyan lehet használni?

- e-Szignó automata (MonDoc-ba integrálva)
 - megfelelő formátumú aláírás elkészítése,
 - kiegészítés metaadatokkal,
 - titkosított fájlok kezelése
 - az archívum által visszaadott tértivevény értelmezése
- Beküldés az archívumba (MonDoc)
 - https
 - smtp + ssl
- Letöltés
 - https
 - titkosított állomány tölthető le

Mikor szükséges, mire jó?

- Ha az elektronikusan aláírt dokumentumokat hosszú távon is meg kell őrizni, gondoskodni kell a hiteles archiválásukról.
- Ha egy (nem aláírt) elektronikus dokumentumról hosszú távon is igazolnunk kell, hogy változatlan formában létezett.
- Megfelel az archiválásról szóló rendelet (7/2005 IHM r.) követelményeinek is.
- Elektronikus számlák archiválása.

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, egyúttal:
 - tevékenységéért pénzügyi felelősséget vállal;
 - az ügyfél igazolhatja, hogy kellő gondossággal járt el;
 - bizonyító erő kapcsolódik hozzá;
 - megjeleníthetőség, értelmezhetőség.
- Mindez elérhető a MonDoc rendszerbe integrált komponens segítségével.

Köszönöm a figyelmet!

Elektronikus archiválás szolgáltatás

Dr. Berta István Zsolt, PhD, MBA, CISA
Microsec Kft.

istvan.berta@microsec.hu

www.e-szigno.hu