COLLECTIO IVRIDICA VNIVERSITATIS DEBRECENIENSIS

VIII.

VESZPRÉMI BERNADETT

Dokumentum-azonosítás az e-közigazgatásban

1. Bevezetés

Felvethető az, hogy a ma társadalmában – bár egyre inkább fejlődünk, új technológiai megoldásokkal próbáljuk megkönnyíteni az életünket – egyáltalán szükség van-e minden területen új informatikai vívmányokat bevezetni, alkalmazni, vagy bevezethetők-e, alkalmazhatók-e. A közigazgatás is egy olyan területnek tekinthető, amely különböző okoknál fogva nem engedi magára kényszeríteni az információs társadalom által kifejlesztett „találmányokat". Miért is van ez? A közigazgatásban dolgozókról és az ott intézett ügyekről még mindig azt tanítják, tanítjuk, hogy a közérdeket képviselik, valamilyen szinten ez egy bizalmi kérdés pl. szociális segély, temetési segély vagy éppen házassági anyakönyvi kivonat kérése esetén. Ezeket az élethelyzeteket (ügyeket) nem szabad és nem is lehet elektronizálni. Olyan mindennapos események ezek, amelyek személyes kontaktust igényelnek az ügyintézőkkel. Mindemellett eddig a technikai háttér sem volt adott, hiszen még az utóbbi években is találkozhattunk olyan önkormányzatokkal, ahol a hivatalban pár számítógép állt rendelkezésre és a településen nem volt kiépítve internet-kapcsolat.

Mégis haladni kell a korral – az Európai Unió ajánlásaiból is ez derül ki –, ezért olyan környezetet kell teremtenünk, amelyben a közigazgatás által kialakított bizalmi jelleget, a biztonságot más úton tudjuk garantálni informatikai eszközök alkalmazása mellett.

Elismerjük, hogy az elektronikus közigazgatás megteremtéséhez nemcsak a rugalmas jogi környezet és az informatikai infrastruktúra kialakítására van szükség, hanem alapvetően a hazai hozzáállás – mind ügyintézői, mind ügyfél oldalon – megváltoztatását igényli. Egy rendszert akkor fognak alkalmazni a közigazgatásban dolgozók, ha önmaguk tapasztalják, hogy az ő érdekeiket szolgálja, munkájukat könnyíti meg. Annak nincs értelme, ha csak az ügyfelek számára biztosítunk lehetőséget az elektronikus ügyindításra és a hatóságokat – akár központi, akár helyi szinten – belekényszerítjük egy olyan helyzetbe, hogy ezen elektronikus dokumentumok fogadására vegyenek meg egy drága szoftvert. Annak sincs értelme, hogy a jogalkotó által támasztott kötelezettséget teljesítve a hatóság a hivatalba érkező elektronikus kérelmet kinyomtatja, és

hagyományos úton folytatja az ügyintézést. Sőt azt is hangsúlyozni kell, hogy jelenleg az országban nincsen egységes, hatósági ügyintézést segítő alkalmazás, csak szigetszerű próbálkozásokról beszélhetünk. Ez nem segít a terjesztésben.

Jelen tanulmány az elektronikus közigazgatásra koncentrálva az azonosítás kérdéseit boncolgatja és a hatályos joganyag bemutatására törekszik. Sajnos ez a terület nem mondható állandónak, már a tanulmány megírása alatt is változások történtek, sőt a megjelenés időpontjában már feltehetően új szabályozás fog érvényesülni (Ket., Ekszt., új végrehajtási rendeletek). Célunk, hogy hirdessük, van jövője az elektronizálásnak a közigazgatásban, de a fokozatosságot, egységességet, szabványosítást, interoperabilitást és költséghatékonyságot szem előtt tartva. Az elektronikus közigazgatás lényege, hogy meggyorsítsa az eljárást, nem az, hogy az ügyfelek, vagy a hatóságok számára új kötelezettségeket állapítson meg.

Az informatikai vívmányok közigazgatásba beépítése kapcsán mindenképpen beszélni kell az azonosításról, hiszen ezen eszközök kiváltják a személyes kontaktust, ezért új formát kell kialakítani az ügyfél és a kérelem megbízható beazonosítására. Ennek egyik vetülete a személyazonosítás,[1] amelynek célja, hogy az ügyben ügyfélként fellépő személy a személyes megjelenés terhe „nélkül" otthonról, akár egy kattintással intézhesse ügyeit. A személyazonosítás mellett azonban ugyanúgy szükség van a dokumentum-azonosításra is, hogy az ügyfél azon túlmenően, hogy a nap 24 órájában képes közigazgatási kérelmet benyújtani, mindig százszázalékosan meg lehessen győződve arról, hogy a hatósághoz ugyanaz a kérelem érkezett be, ugyanolyan tartalommal, mint ahogy ő elküldte, illetve, hogy személyes adatai biztonságban vannak, illetéktelenek nem férhetnek hozzá.

Olyan új területről van szó, amelynek Magyarországon még nincsen túl hosszú időre visszavezethető múltja, amelyből tapasztalatokat gyűjteni, amelyek megalapoznák az emberek bizalmát. Ezért szükség van egy erőteljes marketingre, a bizalom kiépítésére. Ezt egyrészt a kifejlesztett szoftverek egyszerű kezelhetősége, ügyfélbarát jellege, mindenki számára hozzáférhetősége teremtheti meg. Másrészt a jogalkotóknak ezt a helyzetet ösztönöznie, támogatnia kellene, nem pedig megnehezíteni. A jelszó: egyszerűség, átláthatóság, biztonság, fokozatosság. Mindegyik feltételnek egyszerre kell teljesülnie, egyik sem elhanyagolható. A fokozatosságot pedig mindenképpen fontosnak tartom.

Mindemellett egy szabványos, egységes, elfogadott állami szoftverre lenne szükség, amelyet mindegyik önkormányzatnak – a szakrendszerekhez hasonlóan pl. ONKADO,[2] ASZA[3] – a rendelkezésére bocsátanak. Eddig csak a

---

[1] Lásd a szerző Személyazonosítás az e-közigazgatásban című cikkét.??

[2] Önkormányzati Hatáskörbe Tartozó Adók Nyilvántartása.

[3] Anyakönyvi Szolgáltató Rendszer.

belépési pontokra vonatkozóan találhattunk szabályozást (ügyfélkapu, hivatali kapu), de a terület életképességének biztosításához szükség van a kettő közötti kapcsolat megteremtésére, egy, a teljes ügyintézési folyamatot leképező (workflow), a kérelem benyújtásától a döntés közléséig és elektronikus fizetésig terjedő, informatikai, igazgatási jogi alkalmazás kifejlesztésére. Ha megnézzük az Új Magyarország Fejlesztési Terv prioritásait, akkor rögtön feltűnik, hogy az esélyegyenlőség, foglalkoztatás, fenntartható fejlődés, stb. mellett önálló operatív programként jelenik meg az e-közigazgatás és az államreform is. Ennek ellenére ezeken a területeken a kiírt pályázatok száma elhanyagolható. Bár elszórva az országban vannak már olyan fejlesztések, amelyek a CLBPS ajánlás[4] 3-4. szintének megvalósítására képesek, mégis ezek csak elszigetelt próbálkozások, amelyek elterjedését az állam semmilyen eszközzel nem támogatja.

2. Dokumentum-azonosítás

A dokumentum-azonosítás ugyanolyan jelentőséggel bír az elektronikus közigazgatásban, mint a személyazonosítás. Hiszen az a cél, hogy a személyes megjelenést egy azzal azonos biztonságú elektronikus kapcsolattartással váltsuk fel, meggyorsítva és megkönnyítve mindkét oldalon az ügyintézést. Ehhez nemcsak arra van szükség, hogy egyértelműen be tudjuk azonosítani az ügyfelet, hanem arra is, hogy garantálni tudja mind a hatóság, mind az ügyfél a küldött dokumentumok tartalmának változatlanságát.

Bár – az előbb elhangzottak alapján – szabványos elektronikus ügyintézési rendszer bevezetését az állam nem támogatja, azonban a biztonságos elektronikus kapcsolattartás létrehozására történtek már törekvések. Olyannyira, hogy még a mai napig ez egy állandóan változó terület. Szabályozása először a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvényben (továbbiakban: Ket.) jelent meg, majd önálló elektronikus közszolgáltatásként definiálva bekerült a 2009 októberében hatályba lépő elektronikus közszolgáltatásokról szóló 2009. évi LX. törvénybe (továbbiakban: Ekszt.). A törvényhez kapcsolódó végrehajtási rendeletek kidolgozása még várat magára, de feltehetően a hatályos joganyagot ismét meg fogja bolygatni.

---

[4] Common List of Basic Public Services, olyan európai uniós ajánlás, amely az elektronikus közigazgatás 4. szintjét határozza meg.

1.információnyújtás (honlapok létrehozása, ügyleírások)

2.egyirányú interaktivitás (letölthető nyomtatványok)

3.kétirányú interaktivitás (elektronikusan beküldhető nyomtatványok)

4.tranzakció (teljes elektronikus ügyintézés, az elektronikus fizetést is ideértve)

A dokumentum-azonosítás kapcsán a hatályos szabályozást szem előtt tartva az azonosítás két formáját kell elemezni: a központi rendszer kínálta lehetőségeket és az elektronikus aláírást, amely a hitelesítés egyik fajtája.

A dokumentum-azonosítás első, talán legfontosabb jogintézménye a hitelesítés. Attól függően, hogy a dokumentum tartalmának, vagy a továbbításának biztonságát akarjuk elérni, beszélhetünk elektronikus aláírásról vagy elektronikus tértivevényről.

A hitelesítés jogintézményének – amelyet a hitelesítés-szolgáltató is végez – nemcsak az elektronikus kapcsolatokban van szerepe, hanem a hagyományos jogügyleteknél is. Pl. erre szolgál a személyi igazolvány, amely az arckép rögzítésével igazolja a tulajdonosát és egy aláírást rendel hozzá, amellyel a későbbiek során is azonosítani tudja magát az illető. Az ezen okmányon szereplő aláírás hitelességét a később felmerülő jogviszonyokban szereplők pl. ügyvéd, közjegyző, vagy egyáltalán a felek bizonyítják.

A dokumentum-azonosítás témaköréhez sorolható ezeken túlmenően az időbélyegző is, amely a tartalom hitelesítésére szolgál. A hosszú távú megőrzés is a későbbi azonosításhoz nyújt segítséget, ezért elengedhetetlen a fejezeten belül az elektronikus archiválásról és ehhez kapcsolódva az elektronikus iratkezelésről is szólni.

Új jogintézmény megjelenése van folyamatban: az elektronikus tértivevény. Ez a felek közötti adattovábbítás útjához társít jogkövetkezményeket, biztosítva az elektronikus dokumentum megérkezésének bizonyíthatóságát.

Az elektronikus közigazgatási hatósági eljárás jelenleg két módon kezdeményezhető. Az elektronikus aláírás mellett a központi rendszer keretében működő gerinchálózat[5] jelenti a biztonságos információcserét. Ezért a rendszer működéséről és a benne futó dokumentum-azonosításról is beszélni kell.

2.1. Elektronikus aláírás

Logikailag az elektronikus aláírás témája inkább a személyazonosításhoz tartozik. Hiszen az elektronikus aláírás és az ehhez tartozó eljárások funkciója, hogy egy elektronikus dokumentumot egy adott személyhez kapcsoljon, és ezek összetartozását igazolja, illetve meghatározza az aláíró személyét és letagadhatatlanná tegye az aláírás tényét. Én ennek ellenére mégis a dokumentum-azonosítás egyik fajtájaként említem, mivel ez az informatikai eljárás közvetlenül az elektronikus dokumentumhoz rendel egy elektronikus adatot és mind a létrehozása, mind az ellenőrzése, vagy a későbbiekben tárgyalt

[5] NÉMETH Ildikó, *Az e-közigazgatás fél évtizede Magyarországon* = E-Government Tanulmányok XXII., Budapest, E-Government Alapítvány, 2008, 83.

archiválása a dokumentumhoz kapcsolódik, azon végzett műveleteket jelent, és az aláíró személyének azonosítása ennek az eljárásnak csak egy részét alkotja.

Az elektronikus aláírás azonosítja a dokumentumot és meghatározott eljárások, informatikai eszközök révén az aláíró személyhez köti. Ez az alkalmazás arra szolgál, hogy biztosítja a dokumentum sértetlenségét, és meghatározza, hogy ki volt a magánkulcs tulajdonosa, akitől az adott dokumentum érkezett. Azonban az elektronikus aláírás ténye még nem igazolja az aláíró személyazonosságát, erre a hitelesítés-szolgáltató szolgál, amely a személyes regisztráció, a tanúsítvány kibocsátása és az aláírás-ellenőrzés által alkalmas az aláírást alkalmazó személy azonosítására is. A személyes regisztráció – hasonlóan az okmányirodai regisztrációhoz az ügyfélkapunál[6] – azért jelenti az azonosítás garanciáját, mivel a hitelesítés-szolgáltató nemcsak valamilyen hatósági okmány segítségével állapítja meg az aláírást igénylő személyazonosságát, hanem ezen kívül ezeket az adatokat köteles egyeztetni a személyi adat- és lakcímnyilvántartóval, az útiokmány-nyilvántartóval vagy a gépjárművezetői nyilvántartó szervezetek egyikével.

Fontos felhívni a figyelmet arra, hogy az elektronikus aláírás nem minden esetben az aláíró személyt azonosítja, előfordulhat, hogy csak képviseleti jogosultságot igazol.

„Az Európai Unió 1999-ben fogadta el az elektronikus aláírás közösségi szintű, a magyar jogalkotóra is irányadó szabályozását, az elektronikus aláírás közösségi keretfeltételeiről szóló 1999/93/EK irányelvet. A keretfeltételek közösségi szinten történő rögzítésének célja az, hogy az elektronikus aláíráshoz fűződő jogkövetkezmények tagállamok közötti különbségei és a hitelesítés-szolgáltatók akkreditációjára vonatkozó eltérő feltételek ne hátráltassák az elektronikus kommunikáció és elektronikus kereskedelem fejlődését."[7]

Az elektronikus aláírás elektronikusan aláírt elektronikus dokumentumhoz azonosítás céljából logikailag hozzárendelt vagy azzal elválaszthatatlanul összekapcsolt elektronikus adat.[8]

---

[6] JACSÓ Tamás, *Az ügyfélkapu és az eBEV használata*, Budapest, SALDO Pénzügyi Tanácsadó és Informatikai Rt., 2006, 13.

[7] DÓSA Imre, POLYÁK Gábor, *Informatikai jogi kézikönyv*, Budapest, KJK Kerszöv Jogi és Üzleti Kiadó Kft., 2003, 190.

[8] Az elektronikus aláírásról szóló 2001. évi XXXV. törvény (továbbiakban: Eat.) 2.§ 6. pontja = JOGSZTÁR Hivatalos Jogszabálytár Magyar Közlöny Lap-és Könyvkiadó 2009/3.

„Az aláírás céljai:

- *azonosíthatóság*
- *hitelesség*
- *sértetlenség*
- *letagadhatatlanság"*[9]

„Az elektronikus aláírás a kapcsolódó eljárásokkal együtt alkalmas arra, hogy biztosítsa az aláíró egyértelmű azonosíthatóságát, az aláírás tényének letagadhatatlanságát, továbbá azt, hogy az elektronikus úton aláírt elektronikus irat tartalma nem változott meg azóta, hogy az a személy, akihez az elektronikus aláírás tartozik, az aláírást »elhelyezte« az iraton."[10]

„Az elektronikus aláírás technológiai hátterét úgy kell/kellett kialakítani, hogy az technológia-semleges legyen, hiszen ezen a területen a fejlődés nagyon gyors, szinte követhetetlen, ezért olyan eljárást kell kidolgozni, amely akár évekkel később is alkalmazható. A jogi szabályozás kidolgozásakor azonban mégsem lehet teljesen figyelmen kívül hagyni a jelenleg elfogadott technikai megoldásokból eredő követelményeket."[11]

A nyilvános kulcsú hitelesítési eljárások a kriptográfián, a titkosításon alapulnak. A titkosítás célja, hogy csak az tudja elolvasni az üzenetet, akinek küldték. A rejtjelezés[12] során a szereplők a következők:

– feladó, aki biztonságosan kívánja küldeményét eljuttatni a végcélba;

– a címzett, aki hitelt érdemlően meg kíván bizonyosodni arról, hogy kitől érkezett számára a küldemény;

– a jogosulatlan harmadik személy (lehallgató), aki megpróbál illetéktelenül hozzáférni a küldeményhez vagy magát a feladóként feltüntetve kíván a címzettel kapcsolatba lépni és annak hamis üzenetet küldeni.

Két típusú kriptográfiai algoritmusról beszélhetünk: a szimmetrikus és az aszimmetrikus eljárásokról.

---

[9] BALOGH Zsolt György, *Az elektronikus aláírás technológiai alapjai* = Ünnepi tanulmányok Prof. Dr. Kalas Tibor egyetemi tanár oktatói munkásságának tiszteletére, Miskolc, Z-Press Kiadó, 2008, 49.

[10] *Uo.*, 50.

[11] *Uo.*

[12] A rejtjelezés a szöveg (adatsor) olyan átalakítása, mely után az átalakítás módjába be nem avatottak számára (az algoritmus és/vagy kulcs ismeretének hiányában) az átalakított szöveg (adatsor) nem visszaállítható. ALMÁSI János, *Elektronikus aláírás és társai*, Budapest, Sans Serif Bt., 2002, 291.

2.1.1. Szimmetrikus eljárások

A szimmetrikus eljárás lényege, hogy mind a feladó, mind a címzett birtokában van egy olyan információnak, amellyel titkosítani képesek üzenetváltásukat, míg a lehallgató ezen információhoz nem tud hozzáférni, ezáltal a titkosított üzenet feltörésére és a címzettnek hamis üzenetet küldésére sem képes. *„A titkos információ általában a rejtjelezéshez használt algoritmus egyik paramétere, a kódoló / dekódoló kulcs."*[13]

A szimmetrikus kulcsú rejtjelezésnek hátrányai is vannak. Ilyen alapvető problémát okoz, hogy a címzettnek és feladónak meg kell állapodnia a titkos kulcsban, azonban ennek lebonyolítása is egy biztonságos kapcsolatot vagy személyes megjelenést igényel, amely kommunikációs csatorna – ha informatikai megoldásokra gondolunk – általában nagy költségigényű, vagy esetleg a sebességével vannak gondok, ennek következtében csak a titkos kulcs lekommunikálására alkalmas, nem az egész folyamat levezetésére. Emellett szintén problémát okoz az, hogy minden feladó-címzett kommunikáció során külön titkos kulcsot kell kialakítani, hogy csak az adott jogviszonyban szereplő felek ismerhessék.

Balogh Zsolt megállapítása[14] szerint ez az algoritmus a fent említett problémákon túlmenően nem eléggé biztonságos, mert egy idő után feltörhető, ezért a kulcsokat nem árt bizonyos időközönként cserélni.
Ilyen titkosítási algoritmusok például a következők: DES, 3DES, AES, Blowfish, RC4.

2.1.2. Aszimmetrikus eljárások

„Az aszimmetrikus algoritmus elsőként James H. Ellis, Clifford Cocks és Malcolm Williamson, a Government Communications Headquarters (GCHQ) munkatársai dolgozták ki az 1970-es évek elején, [...] az eljárás felfedezésének pillanatától államtitkot képezett, ugyanis a GCHQ a brit titkosszolgálatok egyike [...] később Diffie-Hellmann kulcscsere eljárásként vált ismertté, miután 1976-ban két amerikai matematikus, Whitfield Diffie és Martin Hellmann már civil felhasználásra szánt módszerként nyilvánosságra hozta. Ez az első gyakorlatban is alkalmazható megoldás olyan biztonságos rejtjelkulcs megosztási rendszerre, amelyet nyilvános célú kommunikációs csatornán keresztül valósítanak meg."[15]

---

[13] BALOGH, *i. m.*, 51.
[14] *Uo.*, 52.
[15] *Uo.*, 53.

Aszimmetrikus rejtjelezés esetén a titkosításhoz már tanúsítványt használnak, a kódolás és dekódolás elválik egymástól, a két kulcs különböző, azonban összetartoznak, de a kulcsok egyike sem határozható meg a másikból. A nyilvános kulcs a tanúsítványban szerepel, amellyel kódolva az adott személy a nyilvános kulcsához tartozó magánkulcsával vissza tudja fejteni az üzenetet. *„Ebben az esetben létrehozható egy olyan nyilvánosan hozzáférhető kódkönyv, amiben mindenkinek szerepel a nyilvános kulcsa, és így a kódkönyvben szereplők bármelyike tud bárki másnak levelet küldeni anélkül, hogy előtte a partnerrel saját titkos kulcsban megállapodtak volna."*[16]

Tehát míg a szimmetrikus kulcsú kriptográfiánál a kulcs ugyanaz, de titkos, addig az aszimmetrikusnál már egy különböző, de összetartozó kulcspárról van szó. Ilyen kriptográfiai algoritmusok például az RSA, ECC.

2.1.3. Nyilvános kulcsú infrastruktúra

Az elektronikus aláírás az aszimmetrikus rejtjelezésen alapul. Itt az elsődleges cél a dokumentum azonosítása, hitelesítése. Itt is érvényesül, hogy a dokumentum nyílt hozzáférésű marad, illetve a kulcspárt itt is alkalmazni kell, azonban vannak a rendszernek olyan elemei is, amelyek a hitelességet biztosítják. *„A technológia megfelelő működését különböző eljárásrendek és szervezetek biztosítják, amelyeket együttesen Nyilvános Kulcsú Infrastruktúrának (Public Key Infrastructure, PKI) nevezünk."*[17] A PKI Az elektronikus aláírás létrehozására, ellenőrzésére, kezelésére, illetve titkos vagy hiteles kommunikációra szolgáló, aszimmetrikus kulcspárokat alkalmazó infrastruktúra, beleértve a mögöttes intézményrendszert, a különböző szolgáltatókat és eszközöket is.[18]

A PKI szereplői a felek (az aláíró és az aláírást ellenőrző), a hitelesítés-szolgáltató; technikai elemei a kulcspár (magán, nyilvános), tanúsítvány a kulcs érvényességéről és a két kulcs összetartozásáról.

Az elektronikus aláírás esetében a kulcspár magánkulcs tagja arra szolgál, hogy azt tulajdonosa titokban tartsa, míg a nyilvános kulcsot a hitelesítés-szolgáltató által elektronikusan aláírt tanúsítványba foglalva nyilvánosságra hozza. Ezáltal a magánkulccsal aláírt dokumentumot a vele matematikai összefüggésbe álló, összekapcsolt nyilvános kulcsával lehet visszafejteni. Elektronikus aláírás esetén ezeket szokták aláírás-létrehozó (Signature Creation Data) és aláírás-ellenőrző adatnak (Signature Verification Data) is nevezni.

---

[16] *Uo.*, 53-54.

[17] *Uo.*, 54.

[18] www.srv.e-szigno.hu

A szolgáltató aláírás-létrehozó eszközön aláírás-létrehozó adatot szolgáltat és ilyenkor tanúsítványt is biztosít az eszközön elhelyezett aláírás-létrehozó adathoz.

Az aláírás-létrehozó adat olyan egyedi adat (jellemzően kriptográfiai magánkulcs), amelyet az aláíró az elektronikus aláírás létrehozásához használ[19]. A PKI-ban a titkos kulcs (magánkulcs, aláírókulcs) tölti be az aláírás-létrehozó adat szerepét.[20] Ennek felhasználása mellett egy hardverre, illetve szoftverre van szükség, amellyel létrehozható az aláírás.[21]

A kulcs sokféle fizikai adathordozón tárolható; az aláíró számítógépén található rejtjelezett adatállományban, flash-memórián, önálló vagy akár mobil telefonra épített chip-kártyán is.[22]

A PKI felhasználási területei:

- elektronikus kapcsolattartás pl. levelezés
- biztonságos kapcsolaton keresztül történő szolgáltatásnyújtás pl. elektronikus kereskedelem területén
- biztonságos elektronikus fizetési módszerek kialakítása pl. banki átutalások netbankkal
- zárt kommunikációs csoportok létrehozása
- elektronikus vásárlások
- elektronikus számlázás
- elektronikus cégbejegyzés, cégeljárás
- elektronikus archiválás (minősített) – az elektronikus dokumentum olyan hosszú távú megőrzése, hogy a joghatások kiváltására később is alkalmas legyen
- felhasználók azonosítása számítógépes rendszerek esetében
- biztonságos adatszolgáltatás, iratkezelés, ügyintézés

„Az elektronikus aláírás és az elektronikus dokumentum egyes típusaihoz fűződő jogkövetkezmények attól függően változnak, hogy az aláírás milyen biztonsággal – milyen valószínűséggel – azonosítja az elektronikus adatok szerzőjét és eredeti tartalmát [...] . A hatályos szabályozás az elektronikus aláírás különböző típusaihoz rendelet jogkövetkezményeket nem csak az aláírás jellemzőitől, hanem az aláírt elektronikus

---

[19] Eat. 2.§ 1. pontja

[20] www.srv.e-szigno.hu

[21] Eat. 2.§ 3. Az aláírás-létrehozó eszköz: olyan hardver, illetve szoftver eszköz, amelynek segítségével az aláíró az aláírás-létrehozó adatok felhasználásával az elektronikus aláírást létrehozza.

[22] BALOGH, *i. m.*, 56.

dokumentum típusától függően is differenciálja." Dósa – Polyák szerint ezt a tartalmi megkülönböztetést nem érdemes fenntartani, mivel *„a dokumentum tartalmának vizsgálata az alaki érvényességtől független kérdés."*[23]

2.1.4. Az egyszerű elektronikus aláírás

Az egyszerű aláírás definícióját az Eat-ban nem találjuk meg, jogkövetkezményt sem társít hozzá a törvény. Elképzelni úgy lehet, amikor egy Word-ben megszerkesztett szöveg végére begépeljük a nevünket.

2.1.5. A fokozott biztonságú aláírás

A fokozott biztonságú elektronikus aláírás meghatározására már sor került az Eat. keretében, hiszen ez az első olyan aláírás, amely kialakításának specialitásai miatt már jogkövetkezmények kiváltására képes, ezáltal alkalmas a közigazgatási hatósági eljárásban a beérkezett kérelmek azonosítására.
A törvényi definíció szerint a fokozott biztonságú aláírásnak a következő követelményeket kell teljesítenie:
– alkalmas az aláíró azonosítására,
– egyedülállóan az aláíróhoz köthető,
– olyan eszközökkel hozták létre, amelyek kizárólag az aláíró befolyása alatt állnak,
– a dokumentum tartalmához olyan módon kapcsolódik, hogy minden – az aláírás elhelyezését követően a dokumentumon tett – módosítás érzékelhető.[24]
Ez az aláírásmód a jogszabályokban előírt írásba foglalás követelményének felel meg.[25]

Ha a magánokiraton levő aláírás valódisága nem vitás vagy bizonyított, illetve a legalább fokozott biztonságú elektronikus aláírás ellenőrzésének eredményéből más nem következik, az aláírást megelőző szöveget – elektronikus okirat esetén az aláírt adatokat – az ellenkező bizonyításáig meg nem hamisítottnak kell tekinteni.[26]

---

[23] DÓSA, POLYÁK, *i. m.*, 191.
[24] Eat. 2.§ 15. pontja
[25] Eat. 4.§ (1) bek.
[26] A polgári perrendtartásról szóló 1952. évi III. törvény (továbbiakban: Pp.) 197.§ (2) bek. = JOGSZTÁR Hivatalos Jogszabálytár Magyar Közlöny Lap- és Könyvkiadó 2009/3., VERBICS János, *Az elektronikus gazdasági kapcsolatok joga*, Budapest, HVG-ORAC Lap- és Könyvkiadó Kft., 2001, 224.

2.1.6. A minősített aláírás

A minősített aláíráshoz csatolják (nemcsak az Eat.) a jogszabályok a legsúlyosabb jogi hatásokat. Ennek következtében informatikailag kialakítása is szigorúbb feltételeknek felel meg, mint a fokozott biztonságú. Többletelemként jelentkezik a biztonságos aláírás-létrehozó eszköz használata, és a minősített tanúsítvány megléte.[27]

Az Eat. egyedül a minősített aláírásról vélelmezi – időbélyegzés nélkül is –, hogy az ezzel ellátott dokumentum tartalma a létrehozás óta nem változott. Az ilyen dokumentumok a bírósági bizonyítási eljárás szempontjából teljes bizonyító erejű magánokiratnak, vagy a közokiratokra előírt követelmények teljesítése esetén közokiratnak számítanak.

A minősített elektronikus aláírással ellátott elektronikus okirat polgári ügyben teljes bizonyító erejű magánokiratnak minősül, azaz az ellenkező bizonyításáig teljes bizonyítékul szolgál arra, hogy kiállítója az abban foglalt nyilatkozatot megtette, illetőleg elfogadta, vagy magára kötelezőnek ismerte el.[28] Ugyanakkor megfelel a teljes bizonyító erejű magánokirat követelményeinek, ha az ügyvéd igazolja, hogy a kiállító minősített elektronikus aláírásával aláírt elektronikus okirat tartalma az ügyvéd által készített elektronikus okiratéval megegyezik.[29] Elektronikus okirat esetében e bizonyító erő megállapításának feltétele az is, hogy a közokirat kiállítására jogosult az okiratot minősített elektronikus aláírással és – ha jogszabály így rendelkezik – időbélyegzővel lássa el.[30]

Az olyan elektronikus okirat, amelyet közigazgatási szerv ügykörén belül, a megszabott alakban állított ki, mint közokirat teljesen bizonyítja a benne foglalt intézkedést vagy határozatot, továbbá az okirattal tanúsított adatok és tények valóságát, úgyszintén az okiratban foglalt nyilatkozat megtételét, valamint annak idejét és módját. Az eredeti papír alapú vagy elektronikus közokiratéval azonos bizonyító ereje van annak a közokiratról készített elektronikus okiratnak, amelyet a közokirat kiállítására jogosult ügykörén belül, a megszabott alakban készített el, és amelyen minősített elektronikus aláírást, valamint – ha jogszabály így rendelkezik – időbélyegzőt helyezett el.[31]

A minősített elektronikus aláírással ellátott elektronikus okiratok bizonyító erejével kapcsolatos további rendelkezéseket tartalmaz a cégnyilvánosságról, a

---

[27] Eat. 2.§ 17. pontja
[28] Pp. 196.§ (1) bek. f.) pontja
[29] Pp. 196.§ (1) bek. e.) pontja
[30] Pp. 195.§ (5) bek.
[31] Pp. 195.§ (1)-(2) bek.

bírósági cégeljárásról és a végelszámolásról szóló 2006. évi V. törvény (továbbiakban: Ct.).

2.1.7. A közigazgatási eljárásban használt/ható elektronikus aláírás

Az Eat. az elektronikus aláírás fajtáinak felsorolásán és a hozzájuk fűződő jogkövetkezmények ismertetésén túlmegy és meghatározza, ezek közül melyek alkalmazhatók közigazgatási felhasználásra és azon belül is melyik oldal (ügyfél, hatóság) adott lépésnél melyik típusú aláírást jogosult vagy köteles alkalmazni.

A törvény – helyesen – elkülöníti az ügyfél és a hatóság által használható aláírásokra vonatkozó követelményeket. Itt is megjelenik az ügyfélbarát jelleg, csakúgy, mint a Ket-ben, hiszen pl. az ügyféltől nem várható el, hogy egy eljárás indításához a legmagasabb biztonsági fokozatú aláírást vegye meg, míg a hatóságtól ez a szint már a hatósági ügyintézés tömeges mérete kapcsán is megkövetelhető, illetve míg egyik oldalon egy személy áll, addig a másikon egy hivatali apparátus, amely a költségvetéséből jobban ki tudja gazdálkodni. (Ezek a felvetések inkább idealisztikusak és a szabályozás kialakulásának elvi hátterét kutatják, nem számítva az aktuális problémákat pl. eladósodás, a kis települések hátrányos helyzete, informatikai elmaradottság, stb.)

A vonatkozó jogi környezetet a közigazgatási hatósági eljárásokban felhasznált elektronikus aláírásokra és az azokhoz tartozó tanúsítványokra, valamint a tanúsítványokat kibocsátó hitelesítés-szolgáltatókra vonatkozó követelményekről szóló 194/2005. (IX. 22.) Korm. rendelet teremtette meg.

Az ügyfél által, a közigazgatási hatósági eljárásban használható elektronikus aláírásra vonatkozó követelményeket egyrészt a Ket.[32], másrészt a 194/2005. (IX.22.) Korm. rendelet határozza meg.

Az elektronikus hatósági eljárás lépései közül a Ket. egyedül az ügyindításnál rendelkezik az ügyfél azonosításának módjáról, amely októberig egyrészt az ügyfélkapu, másrészt a legalább fokozott biztonságú elektronikus aláírás igénybevétele által lehetséges. Ezt követően a jogalkotók az elektronikus kapcsolattartásra csak a központi rendszert említik. Ennek oka az elektronikus aláírás elterjedésének hiánya és nagy költségigénye, amely még a hatóságok oldaláról is gondot okoz, nemhogy a magánszemélyeket illetően. A központi rendszer szolgáltatásainak igénybevétele, azon belül is az ügyfélkapu létesítése (első alkalommal) díjmentes, amely megteremti az esélyegyenlőséget és talán

---

[32] 2009 októberétől a Ket-ből kikerül az elektronikus ügyintézés, a továbbiakban az Ekszt. szabályozza. Az elektronikus kapcsolattartást a Ket. az írásbeli kapcsolattartás egyik formájaként definiálja, amely a központi rendszer igénybevétele útján történik a hatóság-ügyfél és hatóság-hatóság között.

segít az elektronikus ügyintézés népszerűsítésében. Fontos, hogy a később kidolgozásra kerülő cégkapu esetén is biztosítsák a kapu díjmentességét.

Míg az ügyfélkapu esetében a jogalkotók az informatikusokra bízták a teljes elektronikus közigazgatási útvonal megtervezését (ügyfélkapu – gerinchálózat – BEDSZ – hivatali kapu) – és ezen ötleteket öntötték jogi formába – és egy közvetett módon engedélyezik az ügyfélnek a hatósággal való elektronikus kapcsolatfelvételt (www.magyarorszag.hu, elektronikus űrlapok használata és a központi rendszerre való feltöltése által), addig az elektronikus aláírásnál csak a kezdő ponton avatkoznak be, mégpedig az azonosításnál és azt követően az ügyfélre bízzák a tényleges ügyintézés mikéntjét. Ebben az esetben ez jelenthet egy egyszerű e-mailt is a hatósághoz.

Az októberben hatályba lépő Ket. módosítás[33] következtében az elektronikus aláírás szempontjából a változás csak az ügyfeleket érinti, mert a jogalkotók megpróbálják inkább az ügyfélkapu használata felé terelni őket, egyrészt a költséghatékonyság, esélyegyenlőség, másrészt a kormányzati portál jobb kihasználása érdekében, ezért eltűnik az ügyindításnál az aláírás lehetősége.

A másik oldalon a helyzet még nem stabilizálódott, hiszen a 2008. évi CXI. törvény megjelenésekor még nem tudták kiváltani a hatóság részéről a döntés közléséhez alkalmazandó elektronikus aláírást, hiszen az elektronikus ügyintézésre irányadó jogszabályok (és az informatikai háttér) vizsgálata után megállapítható, hogy egyedül a minősített elektronikus aláíráshoz kapcsolható olyan jogkövetkezmény, amelyet egy hatósági döntés pl. bizonyítás, későbbi felhasználás során igényel. Azonban időközben kihirdették az Ekszt-t, amely megváltoztatta a Ket-ben az elektronikus ügyintézésre vonatkozó szabályokat és csak az elektronikus tájékoztatás címet hagyta benne.

Az Ekszt. a központi rendszer minden szolgáltatását elektronikus közszolgáltatásnak nyilvánította, a központi rendszer szolgáltatásaként határozza meg a hiteles elektronikus kapcsolattartást és az azonosítási szolgáltatásokat. Emellett az alapelvek között nevesíti az elektronikus közszolgáltatásokat nyújtó szervezetek azon kötelezettségét, hogy biztosítsák az informatikai biztonságot, ezen belül az elektronikus aláírási technológia alkalmazhatóságát. Tehát októbertől kezdődően elektronikus aláírás alkalmazására továbbra is lehetőség van közigazgatási hatósági eljárásban, de csak a központi rendszeren keresztül.

Bár a Ket. közvetlenül már nem rendelkezik a döntés elektronikus közléséről, a 28/B.§ (1) bekezdés b.) pontja értelmében írásbelinek minősül a kapcsolattartás, ha a hatóság az iratot a központi rendszeren keresztül küldi meg az ügyfélnek. A 194/2005. (IX.22.) Korm. rendelet a közigazgatási hatósá-

[33] A közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény módosításáról szóló 2008. évi CXI. törvény.

gi eljárásban legalább fokozott biztonságú elektronikus aláírás használatát írja elő az ügyfél részéről. Azonban emellett a rendelet többletfeltételeket támaszt, amelyeknek együttes megléte esetén alkalmazható a tanúsítvány közigazgatási hatósági eljárás során:

a) a hitelesítés-szolgáltató a tanúsítványhoz tartozó hitelesítési rendben vállalja a viszontazonosítási kötelezettség teljesítését;

Mit jelent a hitelesítés-szolgáltató?

Kell tehát egy olyan szolgáltató, akitől érvényes elektronikus aláírást lehet venni, és aki ezen túlmenően vállalja a fenti feladatok teljesítését. A hitelesítés-szolgáltató olyan tanúsítványok kibocsátására szolgáló szervezet, amely nyilvántartja az érvényes és érvénytelen magánkulccsal rendelkezőket és jogosult elektronikus aláírások és tanúsítványok kibocsátására.

Mit jelent a tanúsítvány?

A tanúsítvány a hitelesítés-szolgáltató által kibocsátott dokumentum, amely tartalmazza a jogosult nevét, adatait, ezt összekapcsolja a nyilvános kulccsal és valamely tény fennállását igazolja. A tanúsítvány a hitelesítés-szolgáltató által kibocsátott igazolás, amely egy nyilvános kulcsot egy meghatározott természetes vagy nem természetes személyt (alanyt) egyértelműen azonosító adatokhoz, esetleg más kiegészítő adatokhoz kapcsol.

b) a tanúsítvány minősített tanúsítvány, vagy a hitelesítés-szolgáltató a hitelesítési rendje szerint a tanúsítvány kibocsátását megelőző személyazonosítás során a jogszabályban foglaltaknak megfelelően jár el;

Mit jelent a minősített tanúsítvány?

Az Eat. 2. számú mellékletében foglalt követelményeknek megfelelő olyan tanúsítvány, amelyet minősített szolgáltató bocsátott ki.[34] Minősített tanúsítványt csak minősített hitelesítés-szolgáltató bocsáthat ki, kizárólag természetes személy számára, és kizárólag aláírásra használható.[35] Minősített szolgáltatónak minősül az a szervezet, amelyet az elektronikus aláírással kapcsolatos szolgáltatások valamelyikének tekintetében ennek nyilvánítottak, amellyel szemben a következő feltételek fennállnak:

- büntetlen előélet

[34] Eat. 2.§ 19. pontja

[35] www.srv.e-szigno.hu

- szakképesítés
- pénzügyi háttér megléte
- felelősségbiztosítással való rendelkezés
- egyéb feltételek megléte[36]
- átlátható, stabil működés garantálása
- minőségvédelmi auditokon való megfelelés

és a nyilvántartásban így van feltüntetve.

c) a tanúsítványhoz tartozó hitelesítési rendben a hitelesítés-szolgáltató kizárja az álnév használatát, és az álnév használatának kizárása céljából biztosítja, hogy a külön jogszabályban meghatározott személyazonosság igazolására alkalmas hatósági igazolványban foglalt névvel betű szerint azonos a tanúsítványba foglalt név;

d) a tanúsítványhoz tartozó hitelesítési rendben a hitelesítés-szolgáltató a visszavonási állapot nyilvántartással kapcsolatban is vállalja azt, hogy a kérelem fogadásától számított 3 órán belül megállapítja a felfüggesztési vagy visszavonási kérelem érvényességét (a kérelmező jogosultságát), és az érvényes kérelem szerinti visszavonási állapot megváltozását a nyilvántartásában átvezeti. Ennek teljesítését követő 1 órán belül a hitelesítés-szolgáltató a kérelem szerint módosított visszavonási állapotot közzéteszi.

e) a tanúsítvány megfelel a külön jogszabályban foglalt követelményeknek; és

f) a tanúsítvány kibocsátásának alapjául szolgáló hitelesítési rend nyilvántartásban szerepel.

Ha az ügyfél által használt aláírás nem minősített tanúsítványhoz kapcsolódik, regisztráció szükséges a tanúsítvány kibocsátásához. A regisztráció személyes megjelenéshez és személyazonosság igazolásához kötött. A személyazonosság igazolására szolgáló hatósági igazolvány érvényességét a regisztrációt végző szervezet ellenőrizni köteles. Az azonosítás akár kettős is lehet: ha az aláírás-létrehozó eszköz átadására azonnal nem kerül sor, a későbbi átadás alkalmával az ellenőrzést meg kell ismételni.

Célszerűségi szempontok miatt – hogy ne kelljen egy hivatal valamennyi ügyintézője számára megvenni a döntéshozatalhoz szükséges aláírásokat – megjelent a hivatali aláírás is.

A hivatali aláírás fogalmát ismételten a korábban említett 194/2005. (IX.22.) Korm. rendelet tisztázza. A fogalom különlegessége, hogy közigazga-

[36] Eat. 8.§ (1) bek.

tási eljárásokban a hivatali aláírás alfajtájaként nevesíti a minősített aláírást. A másik típusaként a szervezeti aláírás említhető.[37]

A hivatali aláírás egyik jellegzetessége, hogy a tartalmi elemek mellett időbélyegzőt is magában foglal, vagy az időbélyegzővel megegyező formátumban a hatóság saját időforrásán alapuló, szervezeti aláírásával hitelesített időjelzését.[38]

Itt számomra a két fogalom egymásra utalása tűnik elő, hiszen a hivatali aláírás egyik fajtájaként szóltunk a szervezeti aláírásról és a hivatali aláírás egyik tartalmi elemeként jelenik meg ismételten a szervezeti aláírással hitelesített időjelzés. Ezt pontosítani kellene.

A minősített aláírás már személyhez köthető, csak kiadmányozást igénylő esetekben merül fel szükségessége, és a hatóság képviseletére jogosít.

A kiadmányozást nem igénylő dokumentumoknál a Korm. rendelet megint pontatlan, hiszen nem nevezi meg az elektronikus aláírás fajtáját.

Az ügyfél által közigazgatási eljárásban használható aláírások mintájára a rendelet itt is többletkövetelményeket ír elő:

a) a tanúsítvány tartalmazza a közigazgatási szerv nevét;

b) a hitelesítés-szolgáltató megköveteli, hogy a hitelesítési rendje szerint a tanúsítvány kibocsátását megelőző regisztrációt természetes személy esetében előtte, a hatóság által kiállított és közokiratba foglalt meghatalmazással, hatóság kezdeményezése esetében a regisztrációs szervezet a természetes személy azonosítását külső helyszíni regisztráció útján végzi el;

c) a tanúsítványhoz tartozó hitelesítési rendben a hitelesítés-szolgáltató a visszavonási állapot nyilvántartással kapcsolatban is vállalja azt, hogy a kérelem fogadásától számított 3 órán belül megállapítja a felfüggesztési vagy visszavonási kérelem érvényességét (a kérelmező jogosultságát), és az érvényes kérelem szerinti visszavonási állapot megváltozását a nyilvántartásában átvezeti. Ennek teljesítését követő 1 órán belül a hitelesítés-szolgáltató a kérelem szerint módosított visszavonási állapotot közzéteszi

d) a tanúsítványhoz tartozó hitelesítési rend megfelel a külön jogszabályban foglalt követelményeknek;

e) a tanúsítvány kibocsátásának alapjául szolgáló hitelesítési rend szerepel az NHH Hivatala által a közigazgatási felhasználásra vonatkozó követelményeknek megfelelő hitelesítési rendekről vezetett hatósági nyilvántartásában.

Magyarországon minősített aláírás csak a Nemzeti Hírközlési Hatóság által nyilvántartásba vett, minősített hitelesítés-szolgáltató által kibocsátott, minő-

---

[37] 194/2005. (IX. 22.) Korm. rendelet 1.§ (2) bek. a.) pontja

[38] 8.§ (1) bek.

sített tanúsítvány alapján hozható létre, biztonságos aláírás-létrehozó eszköz segítségével.[39]

Összegezhető, hogy az október után hatályba lépő rendelkezéseknek köszönhetően egy kicsit háttérbe kerül a közigazgatási hatósági eljárásokban az elektronikus aláírások használata. A jogszabályok nem zárják ki alkalmazását, a vonatkozó Kormányrendelet rögzíti az ügyfél és a hatóság oldalán is a biztonsági követelményeket, azonban mindez már csak a központi rendszeren keresztül képzelhető el.

Fontos azonban hangsúlyozni, hogy bár a központi rendszer informatikai háttere esetleg szükségtelenné teheti ezen megoldás alkalmazását, bizonyos esetekben mégis hasznosnak minősülhet. Ilyen pl. a többes ügyfél problémaköre. Vannak olyan ügyek, amelyekben több ügyfélnek kell aláírnia a kérelmet. Elektronikus ügyindítás esetén erre nyújthat megoldást az a valamennyi ügyfél által elektronikus aláírással ellátott kérelem.

2.1.8. Hitelesítés-szolgáltatók

Eddig áttekintettük, hogy milyen fajtájú elektronikus aláírások létezhetnek, ezek közül melyek azok, amelyeket a közigazgatási hatósági eljárásban is alkalmazni lehet, illetve hogy ezekhez milyen jogkövetkezmények társulnak. Azonban az Eat-on és a Ket-en kívül még találkozunk végrehajtási rendeletekkel, amelyek szerepe, hogy egyrészt kialakítsák ennek a technológiai, informatikai hátterét, meghatározva a minimum követelményeket és a biztonsági garanciákat, másrészt kijelölve az infrastruktúra felügyeleti szervét és az azon belül az elektronikus aláírási szolgáltatásokat nyújtó szervezeteket.

Az Eat. az elektronikus aláírással kapcsolatban az alábbi szolgáltatásokat különbözteti meg:

1) elektronikus aláírás hitelesítés szolgáltatás
2) aláírás-létrehozó adat elhelyezése aláírás-létrehozó eszközön
3) időbélyegzés-szolgáltatás
4) elektronikus archiválás szolgáltatás[40]

Ezen szolgáltatásokat ellátó szolgáltatókat a Nemzeti Hírközlési Hatóság felügyeli.[41]

---

[39] A minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről szóló 2/2002. (IV.26.) MeHVM irányelv.

[40] Eat. 6.§ (1) bek.

[41] A Nemzeti Hírközlési Hatóságnak az elektronikus aláírással kapcsolatos feladat- és hatásköréről, valamint eljárásának részletes szabályairól szóló 45/2005. (III.11.) Korm. rendelet.

A hitelesítés-szolgáltatót a PKI részeként nevesítettük, akinek tényleges szerepét a 194/2005. (IX.22.) Korm. rend. rögzíti.
Olyan természetes személy, jogi személy vagy jogi személyiség nélküli szervezet, aki a hitelesítés szolgáltatás keretében

- azonosítja az igénylő személyét,
- tanúsítványt bocsát ki,
- nyilvántartásokat vezet,
- fogadja a tanúsítványokkal kapcsolatos változások adatait, valamint
- nyilvánosságra hozza a tanúsítványhoz tartozó szabályzatokat, az aláírás-ellenőrző adatokat és a tanúsítvány aktuális állapotára (különösen esetleges visszavonására) vonatkozó információkat.[42]

A hitelesítés-szolgáltatók[43] feladatai:

- tanúsítványok kibocsátása;
- a tanúsítványt igénylő személy azonosítása, adatainak ellenőrzése és annak garantálása, hogy a tanúsítvány birtokosa megegyezik a tanúsítványban szereplő személlyel;
- a tanúsítvány visszavonása és ennek közzététele (visszavonási lista, online tanúsítvány-állapot szolgáltatás) illetéktelen jogszerzés esetén;
- hitelesítési rend kibocsátása.

Tanúsítványokat különböző felhasználási célra, különböző területeken bocsátanak ki. Így célja szerint léteznek aláíró, titkosító, authentikációs tanúsítványok; a birtokos szerint megkülönböztetünk szervezeti, személyes és hivatáshoz kapcsolódó tanúsítványokat; a felhasználási terület szerint csoportosítva vannak közigazgatási területen és magáncélra használt tanúsítványok is. Ezek „fizikailag" nagyon hasonlóak, azonban rendkívül eltérő kezelésmódot igényelnek. Minden tanúsítvány tartalmaz egy nyilvános kulcsot, az aláírónak, illetve a tanúsítvány alanyának megnevezését, és a tanúsítványt kibocsátó hitelesítés-szolgáltató aláírását.

Az aláíró tanúsítvány vagy más néven az elektronikus aláírás létrehozására alkalmas tanúsítvány a nevében hordozza célját: elektronikus aláírás létrehozására szolgál. Ezen belül fokozott biztonságú aláírás létrehozására alkalmas és minősített tanúsítványról beszélhetünk. A minősített tanúsítványra szigorúbb követelményeket ír elő a törvény (Eat.), azonban még ennek ellenére

---

[42] Eat. 6.§ (2) bek.

[43] Kapcsolódó jogszabály: Az elektronikus aláírási termékek tanúsítását végző szervezetekről, illetve a kijelölésükre vonatkozó szabályokról szóló 9/2005.(VII.21.) IHM rendelet rögzíti a jogosultság megszerzésének feltételeit.

sem bizonyítható a későbbiek során, hogy ténylegesen milyen módon állították elő. Ezt a tanúsítványt

- biztonságos aláírás-létrehozó eszközzel
- minősített szolgáltató
- kizárólag természetes személy számára
- kizárólag elektronikus aláírás céljából

hozhatja létre.

A titkosító tanúsítványban szereplő nyilvános kulcshoz tartozó magánkulcs birtokosa képes csak visszafejteni a számára titkosítottan küldött üzenetet.

Az authentikációs tanúsítványok a biztonságos, titkosított és hitelesített kapcsolatot garantálják.

A tanúsítvány igényléséhez egy kérelem és adatlapok kitöltése szükséges. A kérelemben az igénylő – egy adott nyilvános kulcshoz tartozó magánkulcs birtokosa – kéri a nyilvános kulcsának tanúsítványba foglalását és egy általa meghatározott megnevezés feltüntetését. A kérelmet saját kézzel kell aláírni,[44] de ez és az adatlapok postán, illetve elektronikusan is beküldhetőek. Azonban a minősített és a közigazgatási tanúsítványok esetében a kérelem csak személyesen nyújtható be. A beküldött adatok alapján – kártyára kerülő tanúsítvány igénylése esetén – a szolgáltató elkészíti az intelligens kártyát, majd felkészül a tanúsítvány kibocsátására.

A hitelesítés-szolgáltató felfüggeszti a tanúsítványok érvényességét, ha az aláíró vagy a képviselt jelzéssel él – pl. ellopták – és kéri a felfüggesztést, vagy ha a szolgáltató maga szerez tudomást valamilyen rendellenességről,[45] ha megalapozottan feltehető, hogy a tanúsítványban foglalt adatok nem felelnek meg a valóságnak; ha az aláírás-létrehozó adat nem az aláíró kizárólagos birtokában van; vagy ha a Felügyelet jogerős és végrehajtható határozatban így rendelkezik.[46] A tanúsítvány visszavonásra kerül ezen okok mellett, ha a szolgáltató által észlelt rendellenesség nem orvosolható, a feltételezésen túlmenően tudomást szerez az adatok valóságtartalmának megkérdőjelezhetőségéről, ha az aláírás érvényességi ideje lejár, vagy ha a szolgáltató a tevékenységét befejezi.[47]

---

[44] Csak ekkor tekinthetők az adatok hitelesnek.

[45] Ezek a jogszabályban, szolgáltatási szabályzatban vagy az általános szerződési feltételekben vannak meghatározva.

[46] Eat. 14.§ (1) bek.

[47] Eat. 14.§ (2) bek., VEREBICS, *i. m.*, 231.

Mit jelent a visszavonási lista?

Adott hitelesítés szolgáltató által kiadott tanúsítványok közül az – adott időpontban – visszavont és felfüggesztett tanúsítványokat tartalmazó, aláírt lista.[48] A hitelesítés-szolgáltatók által vezetett visszavonási nyilvántartások tartalmazzák azokat az adatokat, amelyek alapján összeállíthatók a visszavonási listák (CRL). Ezek segítségével győződhetnek meg a felhasználók a tanúsítványok visszavonási állapotáról (a beérkező, elektronikusan aláírt dokumentumhoz tartozó tanúsítvány érvényes-e). Ezeket a listákat meghatározott időközönként teszik közzé, ezért sokkal óvatosabbnak kell lenni ezek használata során, hiszen két lista közzététele közötti időben is vonhatnak vissza tanúsítványokat.

Mit jelent az online tanúsítvány-állapotszolgáltatás?

Az online tanúsítvány-állapotszolgáltatás (OCSP) kérelemre információt szolgáltat a tanúsítvány visszavonási állapotáról, azaz adott pillanatban meghatározza, hogy a lekérdezett tanúsítvány érvényes-e vagy sem. A legpontosabb adatokat mindig az aláírás pillanatában (megérkezéskor) kapjuk. Azonban vigyázni kell arra is, hogy OCSP válasz esetén is ellenőrizni kell a válaszon található aláírás érvényességét, illetve, hogy a válasz tényleg a hitelesítés-szolgáltató válaszadójától érkezett-e.

A hitelesítési rend olyan szabálygyűjtemény, amelyben a szolgáltató, igénybe vevő vagy más személy (szervezet) valamely tanúsítvány felhasználásának feltételeit írja elő igénybe vevők valamely közös biztonsági követelményekkel rendelkező csoportja, illetőleg meghatározott alkalmazások számára.[49] A hitelesítés-szolgáltatókról az NHH Hivatala vezet hatósági nyilvántartást.

Az elektronikus aláírás megbízhatóságát növeli – a technikai háttér mellett – a hitelesítés-szolgáltató felelőssége is: vele szerződéses kapcsolatban levő személyekkel szemben a szerződésszegésre vonatkozó kártérítési, polgári jogi szabályok szerint; szerződéses jogviszonyban nem álló harmadik személlyel szemben, csak ha az adott jogviszonyban az ő által kibocsátott tanúsítványt, elektronikus aláírást használták fel. Ebben az esetben a szerződésen kívüli károkozás szabályai szerint, illetve amennyiben az aláírással rendelkező fél is felelős, egyetemlegesen felelnek a felmerült károkért.[50]

---

[48] www.srv.e-szigno.hu

[49] Eat. 2.§ 23. pontja

[50] *Az elektronikus aláírás*, közread. Miniszterelnöki Hivatal Informatikai Kormánybiztosság, Budapest, 2001, 18; VÉRBICS, *i. m.*, 232.

2.1.9. Az elektronikus aláírások ellenőrzése

Valamely dokumentum megérkezésekor az első lépés, hogy ellenőrizni kell az elektronikus aláírást. Ez két részből áll, egyrészt a tanúsítvány, másrészt az aláírás érvényességének vizsgálata szükséges.

A viszontazonosítás célja, hogy a közigazgatási szervek ügyfeleikről megbízható információkhoz jussanak, hiszen a hitelesítés-szolgáltató egyéni lekérésre (az ügyfél által a közigazgatási szerv számára küldött dokumentumhoz tartozó tanúsítvány lenyomatának[51] elküldésével) megállapítja, hogy a tanúsítvány valóban az adott ügyfélhez kapcsolható-e. A viszontazonosítás figyelemmel van az adatvédelmi szempontokra, hiszen csak azt igazolja vissza, hogy a közigazgatási szerv által küldött tanúsítvány és az ügyfél személyazonosító adatai között van-e kapcsolat, egyéb adatokat nem szolgáltat ki. Ez a szolgáltatás https biztonságos kapcsolaton keresztül érhető el. A biztonságot a közigazgatási szerv oldaláról a közigazgatási gyökér hitelesítés-szolgáltató tanúsítványára visszavezethető authentikációs tanúsítvány és elektronikus aláírás, a hitelesítés-szolgáltató oldaláról a válasz meghatározott formátumú elektronikus aláírással való ellátása garantálja.

Azt kell megnézni, hogy az aláírás és a dokumentum összetartozik-e, a dokumentumot az aláíró tanúsítványában szereplő nyilvános kulcshoz tartozó titkos kulccsal írták-e alá, illetve az aláíró tanúsítvány az aláírás időpontjában érvényes volt-e. Ezen túlmenően meg kell vizsgálni, hogy az aláíró tanúsítványát valóban a feltüntetett hitelesítés-szolgáltató bocsátotta-e ki, illetve a hitelesítés-szolgáltató tanúsítványának valódiságát, érvényességét is érdemes továbbkutatni (tanúsítványlánc) egészen a megbízható gyökértanúsítványig. Nem árt mindkét szervezet visszavonási listáját ellenőrizni, hogy a tanúsítványokat nem vonták-e vissza.

---

[51] Az elektronikus aláírás elkészítése alapszinten az aláírandó dokumentum lenyomatképzését, majd a lenyomaton a titkos kulccsal való kriptográfiai művelet elvégzését jelenti, az így előálló értéket nevezzük szoros értelemben aláírásnak. Az ellenőrzés során ennek megfelelően újból el kell készíteni az ellenőrizendő dokumentum lenyomatát, majd az aláírás értékén el kell végezni a kriptográfiai művelet ellentettjét az aláíró fél nyilvános kulcsának felhasználásával, és ezt összehasonlítani az újonnan képzett lenyomati értékkel. A kettő egyezése jelenti – szűk értelemben véve – az aláírás érvényességét. ENDRŐDI Csilla, BERTA István Zsolt, *Mire jó az archív aláírás?* 2. = www.srv.e-szigno.hu

Mit jelent a gyökértanúsítvány?

A megbízható gyökértanúsítvány egy megbízhatónak tartott hitelesítés-szolgáltató adott hitelesítési egységének önaláírt tanúsítványa.[52]

A közigazgatási gyökértanúsítvány a közigazgatási gyökér-hitelesítés-szolgáltató által kibocsátott tanúsítvány, amelyben a közigazgatási gyökér-hitelesítés-szolgáltató elektronikus aláírásával hitelesíti az e rendeletben meghatározott követelményeknek megfelelő tanúsítványt kibocsátó hitelesítés-szolgáltató nyilvános kulcsát és tanúsítja, hogy a tanúsítvány által megjelölt hitelesítés-szolgáltató közigazgatási felhasználásra vonatkozó követelményeknek megfelelő tanúsítványt bocsát ki.[53]

Ezek ún. PKI bizonyítékok, amelyek tulajdonképpen informatikai szempontból igazolják azt, hogy egy érvényes aláírással ellátott dokumentum érkezett be hozzánk, amelynek a tulajdonosát is meg tudjuk állapítani. Azonban – mint a jogi ügyleteknél/ügyeknél általában – az ügy összes körülményét mérlegelni kell és a rendelkezésre álló összes információt figyelembe kell vennünk, mielőtt az aláírást és egyáltalán a dokumentumot elfogadjuk. Pl. előfordulhat, hogy maga az elektronikus aláírás érvényes volt és a tulajdonosa birtokában volt, azonban a dokumentum megírására és elküldésére kényszer hatására került sor. Ezt a fenti bizonyítékok alapján nem tudjuk megállapítani. Tehát mindenképpen elengedhetetlen az egyéb információk begyűjtése is.

Időbélyeg segítségével a visszavonási információkból akár szabványos pl. XAdES-C vagy XAdES-A formátumú blokk képezhető a saját védelmünk érdekében – azaz hogy az ellenőrzésünk teljes körű és mindenre kiterjedő volt –, mellyel később is igazolhatjuk, hogy a szükséges ellenőrzési lépéseket elvégeztük.[54]

2.2. Időbélyegző

Az elektronikus aláírás által biztosított azonosíthatóság mellett másik ilyen fontos tényező annak megállapítása, hogy az aláírás időpontjában legyen érvényes a tanúsítvány, mivel a későbbiek folyamán ez bármikor megváltozhat, azonban ha abban az időpontban még érvényes volt, akkor a hozzá kapcsolódó jogkövetkezmények alkalmazhatók. Az aláírás időpontjának pontos meghatározására szolgálhat az időbélyeg.

---

[52] www.srv.e-szigno.hu

[53] 194/2005. (IX. 22.) Korm.rend. 1.§ (2) bek. c.) pontja

[54] BERTA István Zsolt, *A CRL és az OCSP technológiák összehasonlítása*, 2008. november = www.srv.e-szigno.hu

Az időbélyegző egyértelműen a dokumentumhoz köthető. Irreleváns az aláíró személye, nem tartalmaz információt rá vonatkozóan, a dokumentum-azonosítást, illetve a dokumentum sérthetetlenségét, letagadhatatlanságát, adott időpontban való létezését és állapotát, tartalmát igazolja.

Egy időbélyeg azt igazolja, hogy egy adott dokumentum egy adott időpillanatban már létezett. Az időbélyeget időbélyegzés-szolgáltató állítja ki. Az időbélyeg egy olyan adat, amely tartalmazza az időbélyegzett dokumentum lenyomatát, és az időbélyegzés időpontját, egy elektronikus dokumentumhoz végérvényesen hozzárendelt vagy azzal logikailag összekapcsolt adat, amely segítségével igazolható, hogy a dokumentum változatlan az időbélyeg elhelyezésének időpontjában létező állapothoz képest.[55] Az időbélyeg az elektronikus aláírt / vagy alá nem írt dokumentumhoz kapcsolódik, külön erre a célra szolgáló szolgáltató helyezi el rajta és plusz biztosítékként ellátja elektronikus aláírásával is.

A központi rendszer részeként működő BEDSZ az ügyfélkapus azonosítást követően a beérkező dokumentumokkal szemben alkalmazza ezt a szolgáltatást, hogy rögzítse a beérkezés pontos időpontját és állapotát.

Mit jelent a lenyomat?

Műszakilag a lenyomat valamely dokumentumból kriptográfiai lenyomatképző eljárással képzett, a dokumentumra egyedileg jellemző, adott hosszúságú bitsorozat.[56]

Olyan meghatározott hosszúságú, az elektronikus dokumentumhoz rendelt bitsorozat, amely egyértelműen jellemző az adott szövegre, és amelynek képzése során a használt eljárás (hash-transzformáció) a képzés időpontjában teljesíti a következő feltételeket:

a) a képzett lenyomat egyértelműen származtatható az adott elektronikus dokumentumból;

b) a képzett lenyomatból az elvárható biztonsági szinten belül nem lehetséges az elektronikus dokumentum tartalmának meghatározása vagy a tartalomra történő következtetés és az eredeti dokumentum sem állítható vissza (egyirányúság, őskép-ellenállóság);

c) a képzett lenyomat alapján az elvárható biztonsági szinten belül nem lehetséges olyan elektronikus dokumentum utólagos létrehozatala, amelyre alkalmazva a lenyomatképző eljárás eredményeképp az adott lenyomat keletkezik (ütközés-ellenállóság, ütközésmentesség)

---

[55] www.srv.e-szigno.hu, Eat. 2.§ 16. pontja

[56] www.srv.e-szigno.hu

d) a dokumentumban való legapróbb módosítás is óriási változást okoz a lenyomatban (lavinahatás).[57]

A dokumentum véglegesítését követően egy program segítségével el kell készíteni a dokumentum lenyomatát. Ez azt biztosítja, hogy a szolgáltató felé nem szükséges az egész dokumentumot elküldeni, ő csak ezt a matematikai adatsorozatot fogja látni és ennek alapján készíti el az időbélyeget, amelyet aláírásával ellátva küld vissza a feladónak. Az Eat. törvényi vélelmet társít hozzá: vélelmezni kell, hogy a dokumentum már létezett az időbélyegzés időpontjában.

Tehát következtetésképpen elmondható, hogy az aláírás már fent említett céljait – azonosíthatóság, hitelesség, sértetlenség, letagadhatatlanság – az időbélyeggel együtt valósítja meg minden kétséget kizáróan és akár visszavonás után is igazolni tudjuk, hogy az aláírás pillanatában a dokumentumot még érvényes elektronikus aláírással láttuk el és a tartalma azóta nem változott.

2.3. Elektronikus archiválás

A dokumentum-azonosítás témakörénél esetleg bővebben lehetne beszélni az elektronikus archiválásról is, hiszen ez a hosszú távú megőrzését biztosítja a dokumentumnak a hitelesség és a jogkövetkezmények kiváltására alkalmasság garantálása mellett. Az archiválás célja az elektronikus dokumentum oly módon történő megőrzése, amely kizárja az utólagos módosítás lehetőségét, védi a törlés, megsemmisítés, a véletlen megsemmisülés, sérülés és jogosulatlan hozzáférés ellen.[58]

A dokumentum megőrzése történhet a fokozott biztonságú elektronikus aláírással ellátott dokumentum esetén a hitelesítés-szolgáltató megbízásával is (egyéb esetben meghatározott zárt rendszer vagy elektronikus adatcsere-rendszer igénybevételével).

Elektronikus archiválás szolgáltatás keretében a szolgáltató a letagadhatatlanság biztosítása és a dokumentumok hiteles megőrzése céljából archiválja az archiválás időpontjában létező érvényességi láncot; biztosítja az érvényességi lánc sérthetetlenségét az ahhoz tartozó elektronikus aláírások érvényességének hosszú távú ellenőrizhetősége érdekében; az érvényességi láncot az igénybe vevő kérésére részére haladéktalanul átadja; kérelemre igazolást bocsát ki az általa archivált elektronikus dokumentummal vagy érvényességi lánccal kapcsolatban.[59]

---

[57] Eat. 2.§ 26. pontja

[58] A digitális archiválás szabályairól szóló 114/2007.(XII.29.) GKM rend. 2.§ (1) bek.

[59] Eat. 6.§ (4) bek.

Mit jelent az érvényességi lánc?

Az elektronikus dokumentum vagy annak lenyomata, és azon egymáshoz rendelhető információk sorozata (így különösen azon tanúsítványok, a tanúsítványokkal kapcsolatos információk, az aláírás-ellenőrző adatok, a tanúsítvány aktuális állapotára, visszavonására vonatkozó információk, valamint a tanúsítványt kibocsátó szolgáltató elektronikus aláírás ellenőrző adatára és annak visszavonására vonatkozó információk), amelyek segítségével megállapítható, hogy az elektronikus dokumentumon elhelyezett fokozott biztonságú vagy minősített elektronikus aláírás, illetve időbélyegző, valamint az azokhoz kapcsolódó tanúsítvány az aláírás és időbélyegző elhelyezésének időpontjában érvényes volt.[60]

Az elektronikus aláírással ellátott dokumentum esetében első lépésben ellenőrzik az aláírás érvényességét, aztán a minősített szolgáltató az aláíráson időbélyegzőt helyez el. Ha a megőrzési kötelezettség hosszabb, mint 11 év, gondoskodik az elektronikus aláírás hosszú távú érvényesítéséhez szükséges információk (az érvényességi lánc) beszerzéséről és megőrzéséről és minősített szolgáltató által kibocsátott időbélyegzőt helyeztet el az érvényességi láncon, és ez utóbbi lépést megismétli akkor, ha az már nem minősül biztonságosnak.[61]

2.4. Elektronikus tértivevény

Mind az időbélyegző, mind az elektronikus aláírás a dokumentum- és személyazonosításnak új típusú informatikai módszerét adják, azonban egyik sem jelent garanciát arra nézve, hogy maga az elektronikus út, amelyen keresztül a feladótól a címzettig eljut a küldemény, biztonságosnak tekinthető-e – kivéve az ügyfélkaput –, illetve, hogy az adattovábbításhoz kapcsolódó tények (feladás, megérkezés ténye, időpontja, stb.) egyértelműen bizonyíthatók-e.

Elektronikus tértivevény az az elektronikus okirat, amely alapján a hivatalos iratot feladó hivatalos szerv hitelt érdemlő módon megbizonyosodhat arról, hogy az átvételre jogosult személy az elektronikusan kézbesített küldeményt átvette, és ez mely időpontban történt meg. Az elektronikus tértivevény közokirat.[62]

---

[60] Eat. 2.§ 14. pontja

[61] A digitális archiválás szabályairól szóló 114/2007.(XII.29.) GKM rend. 3-4.§

[62] A hivatalos iratok elektronikus kézbesítéséről és az elektronikus tértivevényről szóló 2009. évi LII. törvény 1.§ (3) bek.

Az elektronikus tértivevényt szabályozó törvény az Eat-hoz hasonlóan általános alkalmazási területet biztosít a tértivevénynek, hiszen már a címében hordozza, hogy mind a közigazgatásban, mind a polgári jogi ügyletekben fel lehet használni.

A Ket. külön tárgyalja a papír alapú dokumentumok közlésének rendjét és kézbesítési vélelmet állapít meg az egyes esetekre – nem kereste, nem vette át a címzett a küldeményt –, azonban az elektronikus ügyintézésről szóló fejezetében szervesen elválasztja az elektronikus dokumentumok érkeztetését, közlését. Az elektronikus ügyintézés részletes szabályairól szóló 193/2005. (IX.22.) Kormányrendelet határozza meg az elektronikus dokumentumok esetén képzendő érkeztetési számot. Ezt a rendszer automatikusan generálja és küldi az ügyfélnek az általa küldött kérelem megérkezésekor.

Ezen rendelkezéseknek és a vonatkozó jogszabályi környezetnek[63] köszönhetően megállapítható, hogy az elektronikus dokumentumok akkor tekinthetők kézbesítettnek, ha az ügyfél a visszaigazolást elküldte. Mivel az elektronikus út csak lehetőség az ügyfél számára és nem kötelezettség – bizonyos jogszabályok ez alól kivételt jelentenek pl. Art. –, ezért a Ket. úgy fogalmaz, hogy a visszaigazolás[64] hiányában az ügyintézés formája megváltozik és ugyanazt a küldeményt postán is ki kell küldeni és csak az ehhez kapcsolódó kézbesítés vagy vélelem beállta esetén tekinthető kézbesítettnek.

Az elektronikus tértivevény a hagyományoshoz hasonlóan arra hivatott, hogy magát a küldés és fogadás tényét igazolja, tehát az azonosítás mellett ezzel már leképezhető az egész küldési folyamat. Az elektronikus tértivevény megjelenésével már az elektronikus dokumentumokhoz is egyfajta kézbesítési vélelmet kapcsol az új törvény, mivel azt írja, hogy ha az átvétel az értesítési tárhelyen történő elhelyezést követő ötödik munkanapig nem történik meg, az azt követő munkanapon kézbesítettnek kell tekinteni.[65] Ezzel megerősíti a központi rendszer helyzetét az eddigi rendelkezésekhez képest.[66] Azonban a kézbesítési vélelem mellett kis „méltányosságot" gyakorol az ügyfél irányában, mivel munkanapokban állapítja meg a határidőt. Tágítja is a keretet, már nemcsak értesítésekről, döntésekről beszél, hanem általában a hivatalos iratokról.

Emellett az elektronikus tértivevényről szóló törvény azt is garantálja – mintegy kettősen megerősíti az így kézbesített dokumentumok jellegét –, hogy az Állami Elektronikus Kézbesítő Szolgáltatón keresztül kézbesített hivatalos

---

[63] A központi elektronikus szolgáltató rendszerről szóló 182/2007. (VII.10.) Kormány rendelet (továbbiakban: KR rend.), a közfeladatot ellátó szervek iratkezelésének általános követelményeiről szóló 335/2005. (XII.29.) Kormány rendelet (továbbiakban: Keir.)

[64] 5 napon belül kell.

[65] 6.§ (1) bek.

[66] A Ket. eddig átterelte hagyományos útra az eljárást, ha az ügyfél nem reagált elektronikusan.

iratok az ügyféltől érkezés esetén – a jogszabályi feltételek teljesülése mellett – teljes bizonyító erejű magánokiratnak, közokirat kiállítására jogosult hatóság esetén közokiratnak minősülnek. (Meg kell jegyezni, eddig ez csak a minősített elektronikus aláíráshoz társított jogkövetkezmény volt.)

2.5. A központi elektronikus szolgáltató rendszerben futó dokumentumok azonosítása

A visszaigazolás jogintézménye a központi rendszer elemeinek ismertetése és az elektronikus tértivevény mellett itt is megemlíthető ismételten. A korábban kifejtettek alapján összefoglalva célja kettős: egyrészt az elektronikus dokumentum hatóság általi befogadásáról, hatósághoz való megérkezéséről tájékoztatja az ügyfelet, automatikus érkeztető számot generálva; másrészt az ügyfél is köteles visszajelezni a hatóságnak meghatározott okiratok megérkezéséről, ezáltal a dokumentum-azonosítás és a sikeres küldés oda-vissza garantálva van.

A Ket. a 162.§ (8) bekezdésében rögzíti az elektronikus űrlap rendszeresítésének jogát. Ezt a rendelkezést tartalommal a KR rendelet 3.§ (8) bekezdése tölti meg, amikor azt mondja, hogy a csatlakozott szervezet a központi rendszer útján

- elektronikus űrlapot vagy
- ingyenesen letölthető, megfelelő biztonságú segédprogramot

bocsáthat az ügyfél rendelkezésére oly módon, hogy a kormányzati portálon erre a célra fenntartott elektronikus mutatógyűjteménybe elhelyezésre kerül a csatlakozott szervezet saját honlapján az űrlapokat, segédprogramokat tartalmazó oldalra vezető elektronikus mutató.

A részletszabályokat a rendelet, az adott ügytípusra vonatkozó speciális jogszabályok és a központi elektronikus szolgáltató rendszer és a kapcsolódó rendszerek biztonsági követelményeiről szóló 84/2007. (IV.25.) Kormány rendelet (továbbiakban: KR biztonsági Korm. rend.) állapítja meg.

Az elektronikus űrlap használatának megvalósítása érdekében a KR rendelet új fogalmakat határoz meg: általános nyomtatványkitöltő,[67] BEDSZ.[68]

---

[67] KR rend. 2.§ a.) általános nyomtatványkitöltő: olyan program, amellyel kitölthető a csatlakozott szervezet számára a központi elektronikus szolgáltató rendszeren keresztül is beküldhető, az általános nyomtatványtervezővel készített nyomtatvány.

[68] KR rend. 2.§ d.) biztonságos elektronikus dokumentumtovábbító szolgáltatás (továbbiakban: BEDSZ): a központi elektronikus szolgáltató rendszer azon szolgáltatása, amely lehetővé teszi a csatlakozott szervezet és az ügyfél egymás közötti kétirányú hiteles és az átvétel tényét tanúsító, dokumentumalapú, biztonságos kommunikációját.

Ezen programok alkalmazása során a Ket. biztonságos iratkezelésről szóló általános szabályaira[69] is tekintettel kell lenni, azaz biztosítani kell

- az elektronikus ügyirat sértetlenségét, megváltoztathatatlanságát;
- olyan informatikai megoldások igénybevételét, amelyek a hatósággal való kommunikációt, az adatmegőrzést, az ezekhez való hozzáférést és az elektronikus kapcsolattartás biztonságosságát teszik lehetővé;
- az iratokba való betekintés jogát, hiteles másolat készítését;[70]
- az iratok visszakereshetőségét és megőrzését.

A BEDSZ fogadja mind az ügyfélkapus, mind az ügyfélkapu használatát nélkülöző, elektronikus aláírással ellátott dokumentumokat, mind pedig a hatóságok által, ügyfél részére továbbított válaszdokumentumokat.

A dokumentum-azonosítás a központi rendszeren keresztül nemcsak a BEDSZ által valósul meg, hanem azáltal is, hogy csak az általános nyomtatványkitöltővel és -tervezővel készített dokumentumok fogadására képes, amelyek azonban előzetesen felülvizsgáltak.

A BEDSZ front-office csatlakozási pontja az ügyfélkapu, back-office pontja a hivatali kapu.[71] A biztonságért való felelőssége a következőképpen alakul: gondoskodik a benyújtásra kerülő dokumentum sérülésmentességének, valamint formai követelményeknek való megfelelőségének ellenőrzéséről; amennyiben biztonsági kockázatot észlel, jogosult megtagadni a dokumentum befogadását, amelyről a küldemény benyújtóját haladéktalanul értesíti.[72]

A formátum[73] és a segédprogramok leszabályozása által – kivéve esetleg az ügyfélkapu mellőzésének esetét – szerintem az ügyfélkapun keresztül küldött dokumentumoknál a biztonsági kockázat nulla, hiszen a rendszer csak azt az űrlapot és kitöltést segítő programokat tudja értelmezni, amelyet előre közzétesz.

A biztonságos kapcsolat garantálása érdekében – a kapcsolódó jogszabályi környezetből is érezhetően – a hivatal a fontosabb iratainak továbbítása esetén, együttesen veszi igénybe a hivatali kaput, gerinchálózatot és az elektronikus aláírás kínálta informatikai lehetőségeket. Ezért a KR rendelet 36.§ (4) bekezdése ebből a szempontból helytelennek tűnik. Az említett jogszabályi hely azokat az eseteket tárgyalja, ha a hatóság dokumentumot kíván továbbítani olyan ügyfél számára, akinek az ügyfélkapuja időközben megszűnt. Azt jogilag helyesnek tartom, hogy a lakcím ismeretében a hagyományos közlési formát kell irány-

---

[69] Ket. 166.§ (1) bek.

[70] A Ket. módosítás ezt a kitételt kiveszi.

[71] NÉMETH, *i. m.* 107.

[72] KR rend. 33.§ (3) bek.

[73] Az elektronikus ügyintézési eljárásban alkalmazható dokumentumok részletes szabályairól szóló 12/2005. (X.27.) IHM rendelet.

adónak tekinteni.[74] Azzal azonban már nem értek egyet, hogy ennek hiányában az ismert e-mailcímre küldik el a dokumentumot, még akkor sem, ha az minősített elektronikus aláírással van ellátva. Egyrészt a küldési folyamat nehéz nyomon követhetősége, másrészt a visszaigazolás hiánya miatt. Utolsó érvként pedig megint a Ket. módosítás hozható fel: az ügyfél hatósággal való elektronikus kapcsolattartásának egyetlen formájaként az ügyfélkaput említi, ezért a hatóság ügyfél irányában történő kommunikációjánál is ezt az utat kell jogszerűnek tekinteni.

2.6. Elektronikus iratkezelés

A dokumentum-azonosításnál beszélni kell az iratkezelésről, amelyet a Keir. szabályoz. A szerv vezetője a szerv szervezeti és működési szabályzatában határozza meg az iratkezelés szervezeti rendjét, az iratkezelésre, valamint az azzal összefüggő tevékenységekre vonatkozó feladat- és hatásköröket.[75]

2.6.1. Az iratkezelés általános követelményei[76]

- a dokumentum azonosítható, fellelési helye, útja követhető, ellenőrizhető és visszakereshető legyen;
- tartalma csak az arra jogosult számára legyen megismerhető;
- kezeléséért fennálló személyi felelősség egyértelműen megállapítható legyen;
- szakszerű kezeléséhez, nyilvántartásához, kézbesítéséhez, védelméhez megfelelő feltételek biztosítva legyenek;
- a beérkezett iratok megváltoztathatatlansága biztosítva legyen;
- a rendszeres selejtezés elvégzésével az irattári iratanyag felesleges felhalmozódása megelőzhető, a maradandó értékű iratok megőrzése biztosított legyen;
- az ügyintézéshez, a döntések előkészítéséhez, a szervezet rendeltetésszerű működéséhez megfelelő támogatást biztosítson.[77]

---

[74] Ezt a megoldást támogatja a Keir. is: 58.§ (2) Amennyiben az elektronikus levél elküldése meghiúsul, az elektronikus irat papíralapú hiteles változatát hagyományos kézbesítési módszerrel kell megküldeni a címzettnek.

[75] Keir. 3.§ (3) bek.

[76] BUDAI Balázs Benjámin, SZAKOLYI András, *Interaktív önkormányzat*, Budapest, Magyar Mediprint Szakkiadó, 2005, 54.

Az ügyiratokból és a nem iktatással nyilvántartott egyéb irategyüttesekből tárgyi alapon irattári tételeket alakítanak ki. Ezeken belül meg kell határozni a selejtezhető és nem selejtezhető iratokat. Ez utóbbi esetben a kapcsolódó határidőket és az őrzés helyét, módját is ki kell dolgozni. Irattári tervet kell kialakítani rendszerezéssel és a tételek csoportosításával.

Az iratokat az e célra rendszeresített papíralapú vagy elektronikus iktatókönyvben, iktatószámon kell nyilvántartani (iktatni). Az iratok iktatásával és az iratforgalom dokumentálásával biztosítani kell, hogy az ügyintézés folyamata, és az iratok szervezeten belüli útja pontosan követhető és ellenőrizhető, az iratok holléte pedig naprakészen megállapítható legyen.[78]
Az iratkezelési szabályzat az átvételre való jogosultságot és az ezzel kapcsolatos feladatokat foglalja össze. Az átvétel papír alapú iratok esetében aláírással és az átvétel dátumának feltüntetésével történik. Ezt követi az érkeztetés,[79] majd az iktatás a beérkezés napján, de legfeljebb az azt követő munkanapon (főszám, alszám, kiadás éve, egyedi azonosító). Ehhez meghatározott adatokat tartalmazó iktatókönyvet kell rendszeresíteni, amelyet évente nyitnak meg és az utolsó munkanapon zárnak le.

Az iratkezelő az érkezett iratot köteles az illetékes szervezeti egység vezetőjének vagy a vezető megbízottjának átadni, aki kijelöli az ügyintézést végző személyt (szignálás).[80]

A hatóság által küldendő iratokat csak a szervezeti és működési szabályzatban, ügyrendben meghatározott, kiadmányozási joggal rendelkező személy írhatja alá.

A szervezeti egység iratkezelőjének ellenőriznie kell, hogy a hitelesített iratokon végrehajtottak-e minden kiadói utasítást, és a mellékleteket csatolták-e (expediálás). Az elektronikus irat elküldése időpontját dokumentálni kell.

2.6.2. Az elektronikus iratokkal szemben támasztott követelmények:

- biztosítani kell a papíralapú és az elektronikus iratot egyaránt tartalmazó ügyiratok egységének megőrzését, kezelhetőségét és használhatóságát;

---

[77] Keir. 6.§; *e-közigazgatás, e-önkormányzatok: Informatikai lehetőségek a helyi közigazgatásban*, szerk. TAKÁCS Emőke, ZÁSZLÓS Angéla, Budapest, Municipium Magyarország Alapítvány, 2003, 105.

[78] Keir. 14.§ (1), (4) bek.

[79] Keir. 34.§ (2) A küldeménynek a fogadó félhez történő beérkezése időpontjában nyilvántartásban kell rögzíteni minimálisan a küldemény sorszámát, küldőjét, az érkeztetés dátumát és könyvelt postai küldeménynél a küldemény postai azonosítóját.

[80] Keir. 51.§ (1) bek.

- az irat megnyitása nélkül is azonosíthatónak kell lennie;
- elektronikus iktatókönyv vezetése;
- az átvétel az automatikus érkeztetőszámot is tartalmazó visszaigazolással történik (átvételi nyugta);
- az átvétel időpontja folyamatos működésű rendszerek esetén az átvételi nyugtában szereplő időpont;
- nem folyamatos működésű rendszernél a határidő megtartottnak minősül, ha üzemzavar idejére esik, ekkor a visszaigazolás az ezt követő első munkanapon történik meg,[81]
- itt is megjelenik a biztonsági kockázat, ebben az esetben az átvételt meg kell tagadni;
- iktatás előtt megnyithatóság (olvashatóság) szempontjából ellenőrizni kell[82] – három napos tájékoztatási kötelezettség;
- az érkeztetőszámot a 193/2005. (IX.22.) Kormány rendelet szabályainak megfelelően kell képezni;
- az elektronikus aláírás ellenőrzése;
- az elektronikus iratot gépi adathordozón (hajlékony lemez, CD ROM stb.) átvenni vagy elküldeni csak papíralapú kísérőlappal lehet,[83]
- az iktatókönyv lezárását és hozzáférhetetlenségét informatikai módszerekkel kell biztosítani;
- az iktatókönyv lezárása időbélyeg elhelyezésével történik;
- tájékoztatási kötelezettség,[84]
- automatikus iktatásra is lehetőség van;
- elektronikus levélben iratot csak akkor lehet küldeni, ha a címzett a kérelmet elektronikusan küldte be, vagy azt – az elektronikus levélcíme megadása mellett – kifejezetten kéri;
- az elektronikusan tárolt adatok, iratok utólagos olvashatóságát, használatát a selejtezési idő lejáratáig vagy levéltárba adásáig biztosítani kell;
- elektronikus iratok esetében a jogosult felhasználók naplózás mellett tekinthetik meg az iratot.

---

[81] Keir. 22.§ (1)-(2) bek.

[82] Keir. 31.§ (1) bek.

[83] Keir. 36.§

[84] Iktatási számáról, az eljárás megindításának napjáról, az ügyintézési határidőről, az ügyintézőről és hivatali elérhetőségéről (Keir. 45.§ (1) bek.)

Ezeken túlmenően a 195/2005. (IX.22.) Korm. rendelet is meghatároz a dokumentálással kapcsolatos követelményeket az elektronikus ügyintézést lehetővé tevő informatikai célrendszer esetén:

- a rendszer felépítésére vonatkozó rendszerleírások, modellek megléte;
- tárolt és feldolgozott adatok tárolási szerkezetének és szintaktikai feldolgozási szabályainak kidolgozása;
- az adatokhoz történő hozzáférési rend meghatározása;
- a működtetésre vonatkozó utasítások, előírások biztosítása.[85]

Elektronikus iratkezelés esetén többletkövetelményeket határoz meg a közokiratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény (továbbiakban: Ltv.), amely szerint a közfeladatot ellátó szerv kizárólag olyan iratkezelési szoftvert alkalmazhat, amely a külön jogszabályban meghatározott követelményeknek megfelel és tanúsítvánnyal rendelkezik.[86] A köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény módosításáról szóló 2005. évi CXLIX. törvény azonban ezt a rendelkezést fokozatosan kívánta bevezetni:

a) a társadalombiztosítási nyugellátásról szóló 1997. évi LXXXI. törvény 79. §-ának (1) bekezdésében meghatározott törzsszámhoz kapcsolódó iratok kezelése tekintetében 2015. január 1-jétől,

b) a bevezetésre kerülő iratkezelési szoftverek tekintetében 2007. január 1-jétől,

c) a már alkalmazásban lévő iratkezelési szoftvereket illetően pedig 2009. január 1-jétől kell alkalmazni.

A közfeladatot ellátó szerveknél alkalmazható iratkezelési szoftverekkel szemben támasztott követelményekről szóló 24/2006. (IV. 29.) BM-IHM-NKÖM együttes rendelet egyértelműen meghatározza az iratkezelő szoftverrel szemben támasztott követelményeket, összefoglalja az elvárt biztonsági-, funkcionális-, közigazgatási-, valamint az elektronikus megoldásokkal kapcsolatos feltételeket.

A szoftverek tanúsításának három formája van. A szűkített tanúsítvány ugyan igazolja a szűken vett iratkezelési szabályoknak való megfelelést, ugyanakkor nem rendelkezik elektronikus dokumentumkezeléssel és elektronikus aláírási modullal. Az ezekkel tanúsítottan rendelkező szoftverek tanúsítványa a teljeskörű, a kibővítetten tanúsított szoftverek a kormányzati portállal a gerinchálózaton keresztül való kapcsolattartásra is képesek.

---

[85] 195/2005. (IX.22.) Korm.rend. 8.§ (1) bek.

[86] 9.§ (2) bek., illetve a tanúsító szervezeteket a közfeladatot ellátó szerveknél alkalmazható iratkezelési szoftverek megfelelőségét tanúsító szervezetek kijelölésének részletes szabályairól szóló 16/2006. (IV.6.) BM rendelet határozza meg

3. Összegzés

Az elektronikus dokumentum-azonosítás az én értelmezésemben jelenti egyrészt a dokumentum keletkezésekor a tulajdonos azonosítását, kiváltva ezzel a személyes jelenlét szükségességét; másrészt pedig a dokumentum-kezelés során biztosítja a visszakereshetőséget, a felelősség megállapíthatóságát, az éppen aktuális állapotot, a tárolás módját és helyét. A dokumentum-azonosítás jogszabályi háttere kellően részletes, de hiányolom belőle back office (hatóság) oldalon egy egységes rendszer kifejlesztését, szabványosítását és országos szinten (hatósági ügyekben első- és másodfokon egyaránt) történő bevezetését. Ez nemcsak egy keretrendszer informatikai kialakítását igényli, hanem az informatika, a jog és a szervezés együttesének megteremtését, tehát egy tudásalapú, workflow-jellegű[87] rendszer kiépítését, amely munkamozzanat szintig lebontja a folyamatokat, az eljárási lépésekhez kapcsolódóan jogi helpeket és formanyomtatvány-sablonokat ajánl és azonnali reagálásra képes bármikor végezhető tevékenységek beillesztésével. Emellett képes kezelni az ügyintézési és belső eljárási határidőket, mulasztás esetén a felettes szerv, munkáltató felé jelzéssel él és mindig rögzíti az eljáráshoz tartozó dokumentumok változását, fellelhetőségét. További elvárás, hogy a szakrendszerek összekapcsolására, az átjárhatóság biztosítására[88] és a papíralapú, hagyományos és elektronikus eljárás párhuzamosságának felszámolására is képes legyen.

A dokumentum-azonosítás tekintetében részletesen elemeztem az elektronikus aláírás jogintézményét. Ezt a részt kellően megalapozottnak találom, használata elterjedőben van számos területen (cégbejegyzés, kereskedelem, biztonságos üzleti kapcsolattartás, stb.). Azonban a közigazgatásban számos nehézségbe ütközik alkalmazása. Egyrészt az elektronikus ügyintézés kiforratlansága, a hiányos, vagy egymásnak ellentmondó jogszabályi háttér, másrészt a mögöttes infrastruktúra kiépítetlensége és nem utolsó sorban a nagyfokú bizalmatlanság, bizonytalanság, tudatlanság az internettel kapcsolatban is akadályt képez. Ennek tudható be az is, hogy a Ket-ből októbertől mintegy teljesen eltűnik az elektronikus ügyintézés fejezete. Pozitív változásnak tudható be, hogy önálló szabályozást nyerve, elektronikus közszolgáltatásként definiálva jelenik meg, a központi rendszert erősítve, azonban nem tartom helyesnek, hogy az elektronikus aláírásról mintegy elfeledkeztek a jogalkotók. Bár – a tanulmányban is hangsúlyozom – külön rendelet még lehetőséget biztosít alkalmazására, azonban a Ket-ben az elektronikus kapcsolattartás

---

[87] TÉCSY Zoltán, *Közigazgatási portalógia: Az Internet szerepe a közigazgatásban* = E-Government Tanulmányok II., Budapest, E-Government Alapítvány, 2005, 131-134.

[88] Interoperabilitás. Vö. TÉCSY, *i. m.*, 128.

formája már egyértelműen a központi rendszer biztosította ügyfélkapu és hivatali kapu közötti kommunikáció. Az elektronikus aláírással való ügyindítás visszahelyezését azért tartom szükségesnek, mert pl. a cégkapu megjelenésével lehetőség nyílik a jogi személyek, társaságok önálló ügyindítására is, amelyek feltehetően élnének ezzel az azonosítási formával – a cégkapu hiányában is ez az ügyfélkör szerintem egyéb területen is gyakran használja az elektronikus aláírást, miért ne tenné itt is.