

ELEKTRONIKUS ALÁÍRÁS

Szerzők:

Roskó Tibor
Debreceni Egyetem

Első szerző e-mail címe:
r.tibor92@gmail.com

Lektorok:

Adamkó Attila
Debreceni Egyetem

Fekete Roland
Sz-Sz-B MRFK KHSZ

Mező Ferenc
Eszterházy Károly Egyetem

Nemes Magdolna
Debreceni Egyetem

Roskó, Tibor (2017): Elektronikus aláírás Különleges Bánásmód, III. évf. 2017/2. szám, 29-38. DOI 10.18458/KB.2017.2.29

Absztrakt

Elsődleges célunk egy olyan bevezető tanulmány elkészítése volt, mely közérthető formában mutatja be az elektronikus aláírás kialakulásának folyamatát, egészen a papír alapú aláírás kialakulásának kezdeti történetétől indulva. A főbb mérföldköveket felölelő tanulmányukban megismerhetővé válik mind a papír, mind az elektronikus úton alkalmazott aláírás történelmi és jogszabályi háttere. Ezen írásunk egyfajta bevezető az Electra Signature projektünk keretében elkészített tanulmányunkhoz, melyben az elektronikus aláírás létrehozására kidolgozott egy lehetséges módszerünket ismertetjük.

Napjainkban nagy aktualitással bír az elektronikus ügyintézés lehetősége, mely nagy segítséget jelenthet a különleges bánásmódot igénylő személyek és az őket segítő állampolgárok részére is. Elsődlegesen, az esetlegesen mozgásukban korlátozott személyek részére lehet nagy segítség az otthonról, interneten keresztül megvalósítható ügyintézés. Az esélyegyenlőség megteremtése napjainkban kiemelt fontosságú, így az e-ügyintézés már csak ebből a szempontból is egy rendkívül hatékony megoldás.

Kulcsszavak: elektronikus aláírás, elektronikus ügyintézés, IoT, esélyegyenlőség

Diszciplína: Informatikai tudományok

Abstract

We decided to describe the birth process of the electronic signature in a pure, easy understandable format from the starts of paper signature. The history and laws of both hand written and electronic signature can be met from the main milestones in our paper. We would have liked to create an introduction about e-signature for our other paper of Electra Signature project. This project builds up a possible solution to create e-signature.

Nowadays, the chance of electronic official administration is very actual theme because it also can help to the special needed people and their helpers, not only general citizens. Mostly, it can help to disabled people to make official administration easier, more comfortable at home via internet. This opportunity highlights how we can help them to live a complete life in the electronic official administration environments too.

Keywords: electronic signature, electronic official administration services, IoT, equal opportunities

Disciplines: Computer Science

BEVEZETÉS

Kutatásunk keretében több algoritmus kidolgozását szerveztük projektekké, melyek a szemantikus Web irányelveit szem előtt tartva egy olyan e-ügyintézési platform kidolgozását tehetik lehetővé, mely révén a szeparált rendszerek együttműködve növelhetik az adatkezelés hatékonyságát. Ezek közül az Electra Signature, Ügyfélkapu kormányzati autentikációra épülő elektronikus aláíró megoldásunkat emelnénk ki, mely lehetőséget teremt az elektronikus ügyintézés hatékonyságának előremozdításában, kooperáció kialakításában a már meglévő rendszerekkel.

E tanulmányunkban az elektronikus aláírás ma ismert formájának kialakulásához vezető utat szeretnénk ismertetni, mely cikksorozatunk első részeként egyfajta bevezetőként szolgálhat az általunk kidolgozott, Electra Signature rendszert bemutató további két tanulmányunknak. Ezekből a rendszer által biztosított egyedi szolgáltatások, a rendszer bevezetésének előkészítése, üzemeltetésének biztosítása, valamint a különleges bánásmódot igénylő hallgatók segítségének lehetősége lesz részletesen megismerhető.

Az aláírás, legyen az hagyományos papír alapon vagy elektronikus úton létrehozott, törvényileg szigorúan szabályozott, személyhez kötött azonosító eszköz. Hasonlóan az ujjlenyomathoz, ez is, bármennyire meglepően is hangzik, teljesen egyedi jegyekkel rendelkezik, segítségével, szinte kétséget kizáróan azonosítható a tulajdonosa. Ezen elemző eljárásról bővebben a következő fejezetben olvashat, informálódhat az olvasó. A jogszabályi kereteket szintén mindkét formára vonatkozóan tanulmányoztuk és egy fejezetben meg is osztjuk, közérthető formában, az érdeklődőkkel.

A következetesség kialakításához a kezdetekig nyúltunk vissza, így a bevezetőt követően először az aláírás kialakulásának történelmi hátterét ismerhetik meg, ezt követően a már említett egyedi jegyeket vizsgáló módszerek, majd az aláírásban részt vevők szerepe ismerhető meg.

Tanulmányunk második felében a tényleges e-aláírásról írunk részletesen, melyből közérthetően megismerhető a létrehozás és ellenőrzés folyamata, a biztonságot szavatoló tényezőikig.

Utolsó fejezetként egyfajta bevezetést szeretnénk az olvasó elé tárni a meglévő e-aláírást létrehozó alternatívák ismertetésével, mely összehasonlítja két eltérő szolgáltatást az általunk kidolgozott megoldással. Az Electra rendszer részletes megismerésére a következő tanulmányunkban lesz lehetőség, mely szintén a Különleges Bánásmód online folyóiratban fog megjelenni.

Ahogy már említettük, az elektronikus ügyintézés számos pozitívummal kapcsolódik a különleges bánásmódot igénylő személyek életvitelének segítéséhez, esélyegyenlőségük javításához. Leginkább megfogható előny a mozgásukban korlátozott személyek segítésében található azáltal, hogy otthonuk elhagyása nélkül is teljes körű ügyintézésre nyílnak

lehetőségük, mindezt az Ügyfélkapu által térítésmentesen elérve. E mellett segítők, gondozójuk is részesülhet e szolgáltatások előnyeiből, hiszen, ha például olyan hátrányos tényezőt veszünk figyelembe, hogy a gondozott személyt nem lehet huzamosabb ideig magára hagyni, akkor szintén az online elérhető ügyintézés jelenthet hatékony megoldást. Továbbá az Ügyfélkapu szerepet kaphat az e- és m-learning alapú oktatási rendszerekben (Mező és Psenáková, 2009, 2010) is, mely rendszerek részeként indirekt módon az esélyegyenlőség biztosításához szintén nagyban hozzájárulhat. A már említett cikksorozatunk részeként megjelenő utolsó, a rendszer bevezetését és üzemeltetését ismertető tanulmányunk záró fejezetében szeretnénk egy összefoglalót készíteni, mely bemutatja a hátrányosan érintett hallgatók és segítők által felmerült igényeket és az általunk kidolgozott rendszer, valamint az e-ügyintézés szerepét, ezen igények kiszolgálásában. E fejezetből megismerhetővé válik, milyen lehetőségeket nyithat meg az elektronikus ügyintézés a különleges bánásmódot igénylők részére, melynek kidolgozásához egy szakértőt is bevontunk.

Bízunk benne, hogy jelen tanulmányunk révén olyan személyekhez is eljuthat az e-ügyintézés lehetősége, akik eddig még nem ismerhették meg előnyeit, illetve magát a szolgáltatás működési mechanizmusát.

AZ ALÁÍRÁS

Az aláírás szerepe már ősidők óta jelentős, tekintve, hogy a Kr. e. 18. században Hammurapi törvényi rendelkezésben is kikötötte az okiratok használatát adás-vételek és egyéb ügyek bizonyíthatóságára. Ezen szerződések kéz írott aláírás helyett még pecsétekkel voltak hitelesítve, és elég korszerűen védték meg a hamisítások ellen. A dokumentum agyagtáblába vésett szövegét hitelesítés után egy újabb agyagréteggel fedték, majd erre az előzővel megegyező szöveg került és az "aláírók" pecsétjei. Ha valaki hamisításra gyanakodott, eltávolította a felső réteget és ellenőrizhette, történt-e módosítás az eredetihez képest. (Neumann, 2013).

A középkorban a pecsétek mellett kéz írott aláírást is alkalmaztak, a fennmaradt királyi okleveleken találhatunk sablonbélyegző által létrehozott királyi aláírásokat is. Ezen eljárás során a király aláírásának körvonalait pecsételte az okiratra, majd ezt egy írnok tintával kitöltötte. Ettől függetlenül a legelterjedtebb megoldás a ma is használt kézi szignó volt. (Neumann, 2013)

A 14. században virágzott a hamisítások készítése, melyeket többnyire papok valósítottak meg, mivel nagyrészt csak ők voltak írástudók. A valódiság ellenőrzésére a bíróságok korábbi dokumentumokkal történő összehasonlításokat végeztek. Csak a 19, 20. század idejére valósult meg a ma is használatos eljárás, melynek során írásszakértő bevonásával igyekeztek a hamisítványok kiszűrését elvégezni.

Az eljárás során írásmintákkal hasonlítják össze a kérdéses aláírást, mely első körben megbukhat a teszten, ha 100%-os egyezést mutat, tekintettel arra, hogy senki nem tudja pontosan ugyanúgy kétszer leírni a nevét. Apró eltérések már szabad szemmel, vagy nagyítóval is felfedezhetők. Amennyiben az első rostán átment a hamisítvány, további ellenőrzések következnek, például az írás egyenletessége, dinamikája vagy az egyedi hurkok, áthúzások. Alapvető tény, hogy ha másolunk egy aláírást a vonalvezetés lassú, precíz, ezáltal nem tűnik életszerűnek egy kézjegy. Természetesen ettől jóval összetettebb elemzések és többéves gyakorlat szükséges egy aláírás valódiságának bizonyítására. Ennek bemutatása és részletezése túlmutatna a tanulmány eredeti célkitűzésén.

Az elektronikus aláírás térhódítása mellett is a mai napig legelterjedtebb hogy egy szerződést, nyilatkozatot papír alapon hozunk létre és ekképp hitelesítjük. Emiatt számos jogi háttér is tartozik egy saját kezű, papíron tett aláíráshoz. Ezek megismerése előtt néhány gondolat, miért is gyakori még a 21. század e-mail korában a papír megoldás. Legfőbb

érvünk, hogy gyors és olcsó megoldás, persze tudjuk, hogy személyes interakcióra van szükség és ugyan ez hogyan lehetne mégis gyorsabb, mint egy e-mail váltásban megkötött lakásbérleti szerződés. Elsőként ahhoz, hogy elektronikus úton intézzük a formai kivitelezést, szükséges egy minősített aláíró tanúsítvány igénylése, melyhez személyes megjelenés és személyazonosságunk igazolása elengedhetetlen. Ezt követően az aláírás létrehozásához szükséges eszközök, a tanúsítvánnyal együtt történő megvásárlása. Amennyiben nem rendszeresen kötünk e-szerződéseket, elsőre elég nagy járulékos költségekkel kell számolnunk és a másik nagy probléma az időbeliség. E szemszögből tényleg kijelenthetjük, egy papír alapú okirat gyorsabban és egyszerűbben kiállítható. Ettől viszont árnyaltabb képet kell alkotnunk, miért használ még mindenki papírt, hiszen ha szélesebb körben elterjedne az e-aláírás, biztosan kedvezőbb áron válna elérhetővé. Több tanulmányt is olvastunk e témában és arra a következtetésre jutottunk, hogy a legnagyobb probléma a közsféra által jelenik meg az e-ügyintézés elterjedésének előremozdításában. Saját tapasztalat tükrében az elektronikusan elindított ügyek kapcsán valahol biztosan felbukkan a papír, legtöbbször a hivatalok irányából. Emiatt gyakran terelődik teljesen hagyományos útra a további ügyintézés, ezzel gátat szabva az e-ügyintézés kultúrájának kialakulásban az emberek szemléletében.

A következőkben pedig tekintsük át, hogyan hozhatunk létre szabályosan egy papír alapú aláírást. (Németh,2013b)

A törvényi kereteket figyelembe véve legtöbb esetben magánokiratot készítünk, mely lehet egyszerű vagy teljes bizonyító erejű. Ettől egy magasabb szinten a közokirat fogalma értelmezett, azaz valamely hatóság vagy közjegyző által kiállított dokumentum, például egy személyi igazolvány. Esetünkben a magánokirat formai követelményeivel tudjuk megfogalmazni, mi számít szabályos, hiteles aláírásnak. A legegyszerűbb esetben egy nyomtatott levél, aláírással ellátva egyszerű magánokiratnak tekintendő, teljes bizonyító erejűnek akkor felel meg, ha kézzel íródott. Egyéb esetben lép be a tanúk vagy közjegyző szerepe. Legalább két tanú aláírása és a lakcímük feltüntetése révén biztosított, hogy a dokumentum aláírója előttük írta alá, vagy aláírását magáénak elismerve szóban nyilatkozott. Az ügyvédi ellenjegyzés és a tanúk aláírás által keletkezett bizonyító erejű esetek a Ptk. szerint szigorúan meghatározottak, emiatt egy példát szeretnénk bemutatni, amely az általunk fejlesztett rendszerben is kivitelezhető. (Hidasi, 2009)

Tegyük fel, hogy egy adásvételi szerződést készítünk, melyet két fél köt egymással: eladó és vevő. Az eladó és vevő aláírását követően két tanú, majd az ügyvéd hitelesíti. A lánc felépítése ezáltal: eladó, vevő aláírás -> tanúk aláírása -> ügyvédi ellenjegyzés/aláírás. Ezzel létrejött egy teljes bizonyító erejű magánokirat. (Hidasi, 2009)

A fentiekből világosan megállapítható a tanú szerepe egy dokumentum aláírásakor, papír alapú okirat esetén a tanú előtt kell, történjen az aláírás vagy az aláíró sajátjaként kell, elismerje a kézjegyet. Elektronikus folyamatban a tanú ellenőrzi az aláírás érvényességét, meggyőződik róla, hogy valóban a tulajdonosa helyezte el a szignót. A jog nem határozza meg, ki lehet tanú, viszont a dokumentum kikezdetlensége végett célszerű nem közeli családtagot felkérni, például egy adásvétel vagy végrendelet esetén. (Hidasi, 2009)

Végezetül néhány szó a bélyegzőről, mely elektronikus formában is elérhető az eIDAS rendelet szerint jogi személy és szervezet számára. Ez hasonlóan működik, mint a hagyományos bélyegző, mely cégszerű aláírás esetén az aláírási címpéldányon megadott módon érvényes, például ügyvezető aláírása és bélyegző együttesen. Ettől eltérően kézzel is leírható a bélyegző tartalma, amennyiben a címpéldányon nem lett kikötve a bélyegző kötelező alkalmazása. (Németh, 2013a)

ELEKTRONIKUS ALÁÍRÁS JOGSZABÁLYI KERETE

2015. 12. 23-tól hatályba lépett a 2015. évi CCXXII. törvény, mely az eIDAS (2014. július 23-i 910/2014/EU európai parlamenti és tanácsi rendelet) rendeleten alapulva fogalmazza meg a nemzetközileg is elfogadott elektronikus ügyintézés, aláírás szabályait. Ezzel a 2001. évi XXXV. és 2011. évi XXXV. törvények hatályon kívül helyeződtek, a tényleges elektronikus aláírás létrehozásának lépései, folyamata az eIDAS-ban érhetők el.

eIDAS: elektronikus azonosításról és bizalmi szolgáltatásokról szóló rendelet

Az általunk implementált rendszer alapját a 26. cikkben szereplő követelményeknek való megfelelés biztosítja:

"26. cikk: A fokozott biztonságú elektronikus aláírásra vonatkozó követelmények

A fokozott biztonságú elektronikus aláírásnak az alábbi követelményeknek kell megfelelnie:

- a) kizárólag az aláíróhoz köthető;
- b) alkalmas az aláíró azonosítására;
- c) olyan, elektronikus aláírás létrehozásához használt adatok felhasználásával hozzák létre, amelyeket az aláíró nagy megbízhatósággal kizárólag saját maga használhat;
- d) olyan módon kapcsolódik azokhoz az adatokhoz, amelyeket aláírtak vele, hogy az adatok minden későbbi változása nyomon követhető."

Ennek értelmében, ha biztosított egy olyan azonosítási rendszer, amely kétséget kizáróan képes azonosítani egy személyt, valamint az általa hitelesíteni kívánt dokumentum későbbi sértetlenségét/módosíthatatlanságát felügyelő szolgáltatás, létrehozható elektronikusan hitelesített irat.

Az elektronikus hitelesítés szolgáltatás nyújtása során a másik meghatározó jelentőséggel bíró tényező az aláírás elhelyezésének időpontja, melyre a rendelet 42. cikkében meghatározott követelményeknek megfelelő időbélyeg szolgáltatást megoldást. Az itt megfogalmazott feltételek lényege, hogy a nemzetközi világidőhöz kötött, pontos forrásból származó időadat kerüljön felhasználásra. Az időbélyeg tartalmazza a pontos dátumot és az időt másodpercre pontosan, ez rendszerint egy int típusú számsorral kerül ábrázolásra, mely az 1970. 01. 01. 00:00:00 GMT óta eltelt másodpercek száma. Ilyen formában a dokumentum ellenőrzése során hibamentesen jeleníthető meg az aláírás időpontja a különböző időzónákban.

A magyar jogrendben érvényes 2015. évi CCXXII. tv. XX. fejezet 58/97-99. §-ai a fent ismertetett szabályokat fogalmazzák meg.

Az EU rendeletben pontosan rögzítve lett a felelősség kérdése is, melyet a 13. cikk részletez, legfontosabb bekezdése a szolgáltatás igénybevétele előtti tájékoztatás biztosítása a szolgáltató részéről:

"Amennyiben a bizalmi szolgáltatók előzetesen megfelelően tájékoztatják az ügyfeleiket az általuk nyújtott szolgáltatások igénybevételére vonatkozó korlátozásokról, és amennyiben ezek a korlátozások harmadik felek számára felismerhetők, a bizalmi szolgáltatók nem felelősek a szolgáltatások igénybevételéből eredő, a jelzett korlátozásokat meghaladó károkért."

ELEKTRONIKUS ALÁÍRÁS

Bár 2001-től törvényi szinten is elérhető az elektronikus aláírás Magyarországon, mégis számos félreértés van mai napig a használata körül, főként az elektronikus ügyintézés folyamatában. Legnagyobb megosztó kérdés az elektronikus számlázással kapcsolatos, hivatalosan, NAV állásfoglalás szerint nem kötelező elektronikus aláírással ellátni egy e-számlát, annak kiadását követő sértetlenségét és származását számos más módon is biztosítani lehet. Ettől függetlenül a legbiztosabb módszer ténylegesen az e-aláírással történő hitelesítés. Másik fő hiányosság az elektronikus irat kezelésében ismerhető fel: sokan kinyomtatják, ezzel

pedig érvényét veszti maga az aláírás, illetve az az irány is, hogy e-ügyintézés folytassunk. Természetesen van lehetőség konverziókra a papír és elektronikus változatok között. A papír alapú okirat digitalizálást követően e-aláírással, az elektronikus, nyomtatást követően kézzel írt aláírással hitelesíthető. (DigitDoc,b)

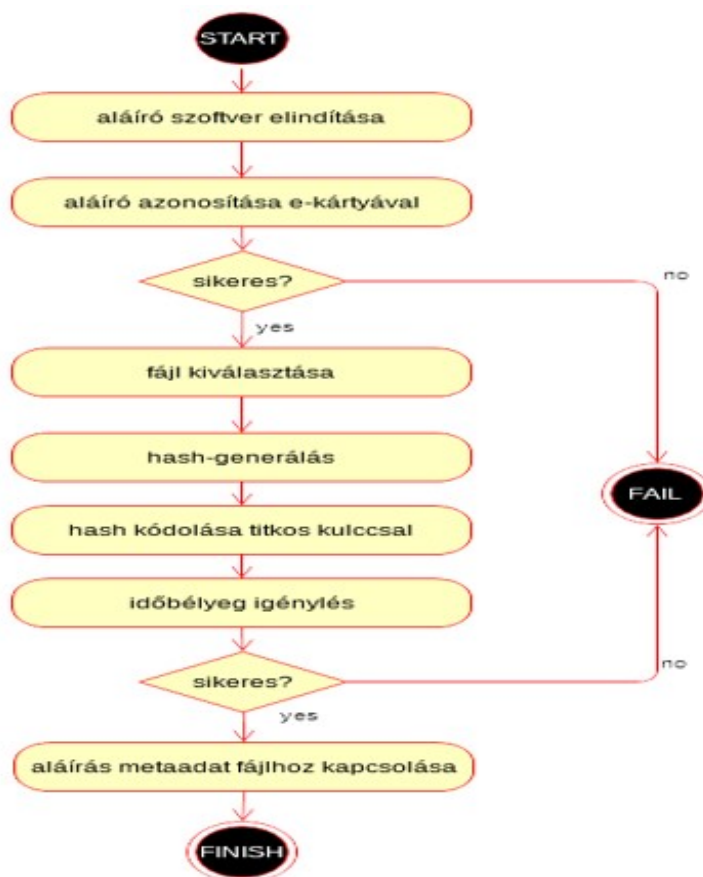
E fejezetben az elektronikus aláírás fajtáit, létrehozásának folyamatát és annak joghatását kívánjuk ismertetni.

Definíció szerint egy kriptográfiai eljárással létrehozott, joghatást kiváltó, a hagyományos kézzel írott aláírással egyenértékű dokumentum hitelesítés, melynek során az aláírás metaadatai a fájlhoz elválaszthatatlanul kapcsolódva kerülnek rögzítésre.

Típus szerint megkülönböztetünk fokozott biztonságú és minősített elektronikus aláírást. Az első egy alacsonyabb biztonsági szintet nyújtó megoldás. Az aláírási folyamatban nem feltétlen történik meg a személyazonosság alapos ellenőrzése, például e-kártya alkalmazásával. Ettől magasabb szinten a minősített esetben minősített tanúsítványra épülve készül el az aláírás, rendszerint aláíró kártyás azonosítással. E megoldással teljes bizonyító erejű magánokirat hozható létre.

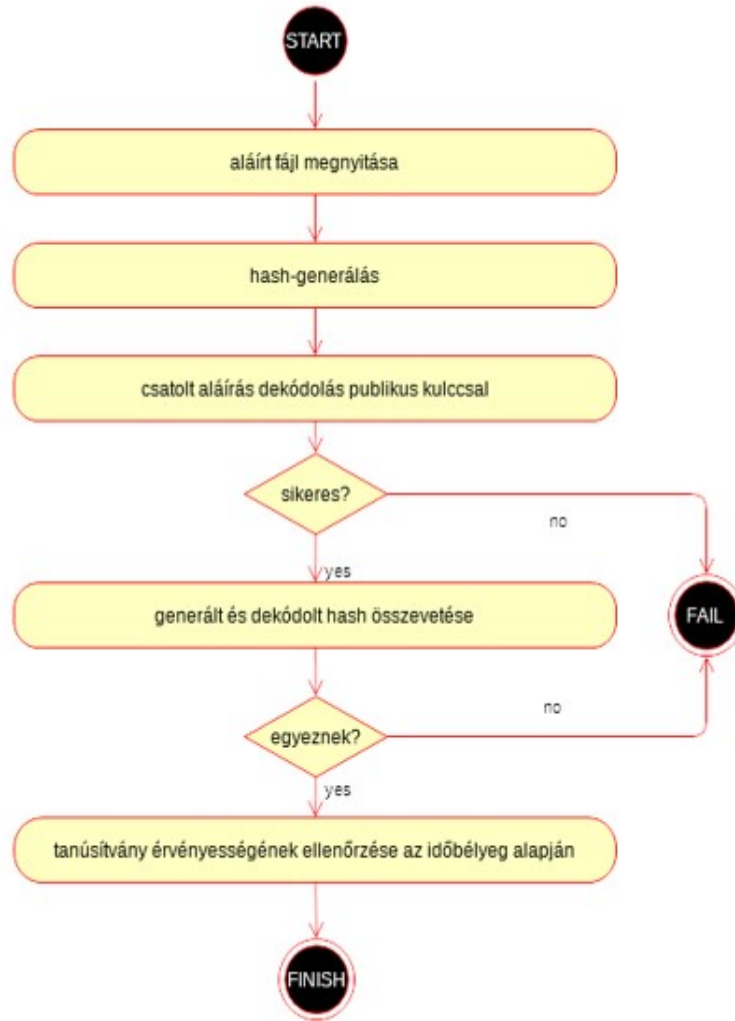
Az aláírás létrehozása PKI alapon történik az igényelt tanúsítvány használatával. Első lépésként az elmentett fájlról egy hash-t képez sha-256 algoritmussal, mely két problémát is lekezel: mely dokumentumhoz rendelték az aláírást, változott-e az aláírás után. Ezt követően a lenyomatot az aláíró tanúsítvány titkos kulcsával kódolja. A létrejött kriptográfiai stringet átadja az időbélyeg szolgáltató felé, aki a saját tanúsítványával aláírt időbélyeget küldi vissza válaszként. Az így előállt formulát csatolja elválaszthatatlanul az aláírandó fájlhoz. A folyamatot az 1. ábra szemlélteti.

1.ábra. Az elektronikus aláírás folyamata.



Egy dokumentum ellenőrzése során az előbbi folyamat fordítottja történik: ismét elkészül a dokumentum hash lenyomata, a fájlhoz kapcsolt lenyomatot pedig az aláíró nyilvános kulcsával dekódolja, amennyiben nem egyezik a két lenyomat, az aláírás érvénytelen vagy a dokumentum megváltozott a hitelesítést követően. E folyamat a 2. ábrán látható.

2.ábra. Az elektronikus aláírás folyamatának ellenőrzése.



A fent bemutatott ábrák a minősített aláíró tanúsítványon alapulnak, mely titkos kulcsa e-kártyán keresztül érhető el a megvásárolt kártyaolvasó eszköz és aláíró szoftver segítségével.

Az előző fejezetben részletezett jogszabályokra tekintettel mind a fokozott, mind a minősített elektronikus aláírás a hagyományos aláírással egyenértékű joghatással bír. Minősített aláírással teljes bizonyító erejű okirat állítható elő, mely a bírósági perek során egyenértékű a papír alapon létrehozott változattal.

MEGLÉVŐ ALTERNATÍVÁK ELEKTRONIKUS ALÁÍRÁS LÉTREHOZÁSÁHOZ

A tradicionális tanúsítványon alapuló elektronikus aláírás mellett számos eltérő technológiát alkalmazó megoldás is megtalálható. Ezek egy része még tanúsítvány segítségével biztosítja a megfelelőséget, rendszerint egy központi tanúsítvánnyal írják alá a dokumentumot a folyamat

végén. Két szolgáltatást szeretnénk bemutatni e téren: DigitDoc biometrikus aláírás (DigitDoc (a)) és NISZ AVDH (Ferencz, A., 2015).

Az első alkalmazás már jóval a tényleges joghatással bíró eIDAS bevezetése előtt létezett és elterjedt használatban volt, főképp a csomagszállítás területén. A hagyományos aláíráshoz minden tekintetben közel álló technológia egy háttérszoftver segítségével metainformációként rögzíti az aláírás paramétereit, melyet a fájlhoz csatol. Az eljárás során két megoldásból választhatunk: e-pad vagy e-toll. Az e-pad használatával maga az aláíró felület érzel, míg a toll esetén külső eszköz nélkül, okostelefon vagy tablet révén is elvégezhető az aláírás. Minden esetben az aláírás képen túl tárolásra kerül egy biometrikus profil, mely rendszerint az írás sebességét, a tollra ható nyomatókot, szüneteket tartalmazza. Ez egy aláírástárból vagy kétes esetben mintából összehasonlíthatóvá teszi az elhelyezett szignót. Hasonlóan egy papír alapú aláírás vizsgálatához.

Az eljárás során PDF dokumentumokat leszünk képesek hitelesíteni, melyekhez az ISO/IEC (19794-7:2007) szabvány által meghatározott aláírás konténerben készül el a profil és csatolódik elválaszthatatlanul. A jogszabályi kereteket bemutató fejezetben ismertetett rendelet révén e szolgáltatással egy teljes bizonyító erejű okirat hozható létre, amennyiben csatolunk minden aláírás mellé egy hiteles időbélyeget is. Tekintettel arra, hogy az aláírást követően nem lehet észrevétlen módosítást végrehajtani, teljesül az e-aláírás rendelet egy része, viszont az időpont megállapításához szükséges még időbélyegző alkalmazása, mely nem része a szolgáltatásnak.

A rendszer bármely érintőképernyős eszközzel használható, valamint nem kizárólag aláírás céljára vethető be. Az út a papírintes iroda felé kezdeményezés előmozdítására rendkívül előnyös megoldásnak tekinthető. Használatával kihagyható a papír bármilyen munkafolyamatból azáltal, hogy a dokumentumba bármilyen megjegyzés kézzel beírható, kézírás formában jelenik meg, hasonlóan, mintha papírra írtunk volna. A fejlesztő elsősorban orvosi leletek jegyzetelésére tér ki, de emellett bárhol megállja a helyét.

Rendelkezésre áll többplatformos szoftver is, mellyel menedzselhetők a dokumentum létrehozásának munkafolyamatai. Offline eszköz használatára is lehetőség nyílik, ekkor a kapcsolattal nem rendelkező applikációban elvégzett események szinkronizálhatók a központi rendszerrel egy későbbi időpontban is.

Összességében, egy hatékony megoldásra tehetünk szert a DigitDoc rendszerével, viszont kiegészítő szolgáltatások igénybevétele is szükséges a ténylegesen hiteles, archiválható okiratok létrehozásához.

A másik megoldás a Nemzeti Infokommunikációs Szolgáltató Zrt által kifejlesztett Azonosításra Visszavezetett Dokumentumhitelesítés szolgáltatás. Ennek alapját az általunk is használt Ügyfélkapu személyhitelesítő funkciója adja, ettől függetlenül nem vetélytársként, hanem kooperatív megoldásként tekintünk az AVDH-ra. Azért is, mert az elvégezhető művelet nem a mi általunk megvalósítani kívánt procedúrát testesíti meg, hanem egy elkészült dokumentum letagadhatatlanságát, vagyis az aláíró által történt hitelesség megalapozottságát. Emiatt ténylegesen nem is e-aláírás szolgáltatásnak tekinthető, hanem ahogy a nevében is megjelenik, a dokumentum hitelességét hivatott szavatolni azáltal, hogy a dokumentum kiállítója önmagát Ügyfélkapu fiókkal vagy tanúsítvánnyal azonosítja, majd ezt követően a NISZ írja alá elektronikusan a fájlt. A folyamat során egy igazolást csatolnak a PDF fájlhoz, mint elválaszthatatlan mellékletet, ezen igazolás tartalmazza az aláírást igénylő Ügyfélkapu e-mail címét és viselt nevét. Ennek tükrében felmerült az Electra rendszerrel történő integráció lehetőségének bevezetése is, ezzel is növelve a dokumentum hitelességét, melyet az Electra-ban írtak alá Ügyfélkapu azonosítással. Az aláírókat tartalmazó metaadat hozzáadását

követően történne meg az AVDH hitelesítés, majd ezt követően íródna alá a metaadatban rögzített felek által.

Visszatérve az AVDH-ra, ez egy nonprofit, a kormány által biztosított szolgáltatás Ügyfélkapuval vagy tanúsítvánnyal rendelkezők részére. Azáltal, hogy elektronikus aláírással és időbélyeggel is ellátja a beküldött fájlt egy teljes bizonyító erejű magánokirat keletkezik, mely szavatolja a dokumentumban foglaltak hitelességét és megakadályozza a későbbi módosítások észrevétlenségét.

Összegezve, az AVDH használatával lehetőség nyílik papír alapon készült okiratok elektronikus archiválására, vagy elektronikus úton előállított dokumentumok hitelesítésére.

ÖSSZEFOGLALÁS

A rövid bevezetést követően feltártuk az aláírás kialakulásának történelmi hátterét, mely az ókortól egészen napjainkig végigkísérte a kialakulás folyamatát. Törekedtünk a valós forrásokon alapuló tényeket, főbb állomásokat megemlíteni, melyek hozzájárultak az aláírás ma ismert formaiságának kialakulásához. Egy másik irány mentén bemutattuk a jogi szabályozásokat, miket fontos betartani a szabályos okiratok létrehozásánál, ezzel biztosítva minden érintett részére egyfajta biztonságot, mely egy esetleges vita során kivédi a kérdéses dokumentum megdöntését, a benne foglaltak megkérdőjelezésének lehetőségét.

Ezt követően az elektronikus aláírás mikéntjét ismertettük, szintén több szemszögből: felépítés, működés és joghatás. Itt is szem előtt tartottuk az aktuális információk megosztását, valamint a részletes jogi oldalról vett értékek, követelmények ismertetését. Ez a pont még a kéz írott aláírásnál felvázoltaktól is lényegesebb, ha valamely része a jogszabályoknak nincs megfelelően megvalósítva, könnyen kikezdzhető vagy érvénytelen okiratot állíthatunk elő. Ezen felül a megoldás friss bevezetése, elfogadás miatt még nem kiforrott a jogi szabályozás sem, ezért körültekintően, mindig az aktuális paragrafusok elemzését követően kell létrehozni egy e-dokumentumot.

Az utolsó fejezetben az elérhető e-ügyintézés támogató megoldásokat mutattuk be, egyfajta alternatívaként az általunk fejlesztett rendszer mellett. Itt két elérhető szolgáltatást vizsgáltunk meg részleteiben: DigitDoc biometrikus aláírás és NISZ AVDH. Az első rendszer tanúsítvány alkalmazása nélkül biztosít lehetőséget e-aláírás létrehozására, viszont a hitelesség végett tanúsított időbélyeggel kell ellátni az aláírt dokumentumot, mely nem része az alapszolgáltatásnak. A második alternatíva az Ügyfélkapura épülő dokumentum hitelesítés, mely egy elektronikus dokumentum tartalmát hitelesíti egy központi -NISZ által biztosított- e-aláírással. Ezzel lehetőség nyílik egy papír alapon megkötött szerződés digitalizált változatának hitelesítésére, vagy egy megrendelés elektronikus úton történő hiteles benyújtására.

IRODALOM

2015. évi CCXXII. tv.. (Letöltés: 2016.10.05.). (Web: http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1500222.TV).
2015. évi CCXXII. tv (b). 2017-től érvényes változások. (Letöltés: 2016.10.05.). (Web: http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1500222.TV×hift=20170101).
- DigitDoc (a). Biometrikus aláírás. (Letöltés: 2016.10.05.). (Web: <https://digitdoc.hu/megoldasaink/biometrikus-kezi-alairas/ismerteto>).
- DigitDoc (b). Hogyan működik az e-aláírás. (Letöltés: 2016.10.05.). (Web: <http://www.digitdoc.hu/hatteranyagok/digitalis-hitelesites/hogyan-mukodik>).
- Dr. Hidasi. (2009). Ellenjegyzés vagy tanú. (Letöltés: 2016.10.05.). (Web: http://www.hidasi.hu/index.php?option=com_content&view=article&id=183&catid=20&la

- ng=hu).
- Dr. Németh, G. (2013a). Aláírás, bélyegző használat. (Letöltés: 2016.10.05.). (Web: <http://blog.drnemethlaw.hu/belyegzo-es-stemplinyomkodas-kek-tinta-vagy-nyomtatott-betuk-mitol-eros-egy-okirat-es-mi-az-ami-nem-szamit-az-alairaskor/>).
- Dr. Németh, G. (2013b). Hibák a szerződésben. (Letöltés: 2016.10.05.). (Web: <https://e-szigno.hu/hitelesites-szolgaltatas/tanusitvanyok/tanusitvany-fajtak.html>).
- eIDAS 910/2014/EU rendelet. (Letöltés: 2016.10.05.). (Web: <http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A32014R0910>).
- Ferencz, A.. (2015). AVDH tájékoztató. NISZ Zrt. (Letöltés: 2016.10.05.). (Web: http://hiteles.gov.hu/letoltes/11/PKI_tajekoztato_v1_1_signed.pdf).
- Mező, F. és Psenáková, I. (2009). A képességfejlesztés lehetőségei az e-learning és m-learning révén. In: Ildikó Psenáková, Ferenc Mező, Ildikó Viczayová (szerk.): Teória a prax II. Nitra: Univerzita Konstantina Filozofa v Nitre. pp. 119-129.
- Mező, F. és Psenáková, I. (2010). Measuring and development of cognitive abilities of Guilford's SoI-Theory by E- and M-learning. In: Zuzana Nagyová-Lehocká (szerk.): Collection of Psychological Studies. Nitra: Constantine the Philosopher University in Nitra, Faculty of Central European Studies. pp. 27-31.
- Neumann, T.. (2013). Királyi aláírás és pecsét használat a Jagelló korban. (Letöltés: 2016.10.05.). (Web: http://www.academia.edu/5479928/Kir%C3%A1lyi_al%C3%A1%C3%ADr%C3%A1s_%C3%A9s_pecs%C3%A9t_haszn%C3%A1lat_a_Jagell%C3%B3_kor_elej%C3%A9n_Royal_Signature_and_the_Usage_of_Royal_Seals_in_the_Beginning_of_the_Jagiellon_Era).

FÜGGELÉK

Rövidítések feloldása

1. GMT: Greenwich Mean Time
2. ISO/IEC: International Organization for Standardization / International Electrotechnical Commission
3. NAV: Nemzeti Adó- és Vámhivatal
4. NISZ AVDH: Nemzeti Infokommunikációs Szolgáltató Zrt. Azonosításra Visszavezetett Dokumentum Hitelesítés
5. PDF/a: Portable Document Format / archivable
6. PKI: Public Key Infrastructure
7. Ptk.: Polgári törvénykönyv
8. sha-256: Secure Hash Algorithm 2 (256 bites változat)