Vágujhelyi Ferenc
elnök
Nemzeti Hírközlési és Informatikai Tanács

Kell-e bizalmi szolgáltató a fokozott biztonságú elektronikus aláíráshoz?

1. Bevezető (és előzetes következtetés)

Előfordul, hogy valamely ágazati jogszabály előírja, hogy az elektronikus formában létrejövő megállapodást rögzítő okiratot legalább fokozott biztonságú elektronikus aláírással kell ellátni. Az ilyen szabályozás célja általában az ügyletben résztvevő felek jogbiztonságának növelése. A cikk azt a kérdést elemzi, hogy ezen jogalkotói szándék elérhető-e akkor, ha nem azonos érdekérvényesítő képességgel rendelkező felek – például egy bank és ügyfele – esetén, a vélhetően *„erősebb”* fél azt ajánlja a vélhetően *„gyengébbnek”*, hogy a jogszabálynak minősített bizalmi szolgáltató által nyújtott garancia nélkül feleljenek meg. Kap-e ilyen esetben a gyakorlatban is érvényesíthető garanciát az ügyfél, vagy a megfelelés csupán formális, és a jogalkotói szándék kikerülése a cél?

Az Európai Unióban, így Magyarországon is az eIDAS[1] rendelet szabályozza az elektronikus hitelességet, így az elektronikus aláírást is. A rendelet szerint az elektronikus aláírás lehet fokozott biztonságú vagy minősített. A minősített elektronikus aláírásról a 25. cikk (2) bekezdése kimondja, hogy *„a minősített elektronikus aláírás a saját kezű aláírással azonos joghatású”*. Az aláírást támogató informatikai rendszert úgynevezett minősített bizalmi szolgáltató bocsátja rendelkezésre, amelynek személyére és működési feltételeire számos összetett szabály vonatkozik, és azt az illetékes állami hatóság még a szolgáltatás megkezdése előtt ellenőrzi. A fokozott biztonságú elektronikus aláírásra csak a négy logikai feltételt tartalmazó 26. cikk vonatkozik, hitelességi erejére pedig semmi. A bonyolult szabályok betartása természetesen nem az aláírást használó feladata és felelőssége, hanem az infrastruktúrát létrehozó bizalmi szolgáltatóé. A minősített aláírás esetében a rendelet több tucat oldalon taglalja az aláírás tanúsítványára, a létrehozó eszközökre, azok tanúsítására, hiteles adatbázisára, érvényesítésére, felfüggesztésére, megőrzésére, és a minősített bizalmi szolgáltatóra vonatkozó követelményeket, valamint azok ellenőrzését. A fokozott biztonságú aláírás esetén a rendelet nem írja elő a minősített bizalmi szolgáltató létét, sőt nem minősített bizalmi szolgáltatóét sem.

Mikor fontos, hogy ki a bizalmi szolgáltató? Nyilván akkor, ha az aláírás hitelességével kapcsolatban kétely merül fel. Valamelyik fél azt állítja, hogy ő nem azzal a tartalommal írta alá a dokumentumot, vagy egyáltalán nem írt alá semmit. Vita esetén a bíróság vagy a felek elsősorban az elektronikus aláíráshoz tartozó tanúsítványt kibocsátó bizalmi szolgáltatót keresik meg. Ha nincs bizalmi szolgáltató, nincs kit megkeresni! Ebben az esetben a hitelesség elismertetése esetleges, inkább valószínűtlen. Erre az esetre az eIDAS rendelet sem ad iránymutatást. Ha van bizalmi szolgáltató, de az nem minősített, akkor annak szándékos vagy gondatlan károkozását a 13. cikk (1) szerint annak kell bizonyítania, aki a kár megtérítését követeli. Ha az aláíró magánszemély, a szolgáltató megbízója pedig egy nagy bank, akkor ez inkább csak formális, nem pedig reális lehetőség. Ha a bizalmi szolgáltató minősített, akkor ugyanennek a joghelynek a következő bekezdése kimondja, hogy annak szándékosságát vagy gondatlanságát vélelmezni kell, azaz a bizonyítási teher megfordul. Gyakorlatilag ez jelent tényleges védelmet az informatikai biztonság és a kriptográfia terén járatlan aláírónak. A bizalmi szolgáltató garanciájához nincs szükség minősített elektronikus aláírás alkalmazására, csupán arra, hogy a fokozott biztonságú aláírás minősített tanúsítványon alapuljon. Ehhez ugyanis minősített bizalmi szolgáltatóra van szükség.

A fentiek alapján tehát kijelenthető, hogy amennyiben egy ágazati jogszabály egy szolgáltató és ügyfele – azaz nem *„egyenrangú felek”* – közötti elektronikus formátumú megállapodáshoz garanciális szándékkal legalább fokozott biztonságú elektronikus aláírás alkalmazását írja elő, a szándékolt garancia csak akkor valósul meg, ha az eIDAS szerinti minősített bizalmi szolgáltató tanúsítványán alapul az aláírás. Ha a jogalkotó szándéka viszont nem ez volt, akkor a jogszabályok szövegéből nem vezethető le ez a követelmény.

A továbbiakban ennek a fenti következtetés logikai hátterét mutatom be.

[1] 910/2014/EU Európai Parlament és a Tanács rendelete

2. Az elektronikus aláírás

2.1. Hitelesség aláírás nélkül

A modern informatika korai szakaszában az elektronikus hitelességet az adta, hogy az adat ellenőrzött és zárt rend szerint került be egy ellenőrzött és zárt elektronikus rendszerbe, és ott csak engedélyezett műveleteket hajtottak végre rajta. Az állami rendszerek jelentős része mind a mai napig így működik, bár az alapadatok beérkezése (például adóbevallás, ingatlan adás-vételi szerződés, nyugdíjjogosultság) esetenként hitelességi feltételhez kötött. Idővel egyes informatikai rendszerek használatához egy olyan tanúsítvány megszerzésére és rendszeres megújítására volt szükség, amely igazolta, hogy a jogszabályban előírt feltételeket kielégíti. Azután felmerült az igény arra, hogy egy elektronikus formában létező dokumentum hitelességét csupán a dokumentum és az aláírás vizsgálatából meg lehessen állapítani. A cél teljesítése nem triviális, mivel az elektronikus adat végső soron nullák és egyesek sorozatából áll (ezért minden dokumentum egy szám, amellyel számítást lehet végezni!), amely egyeseket és nullákat nem lehet egymástól megkülönböztetni, korlátlanul másolhatók és módosíthatók. A feladatot megoldó eljárást nevezzük elektronikus aláírásnak.

2.2. Az elektronikus aláírás, mint számítási feladat

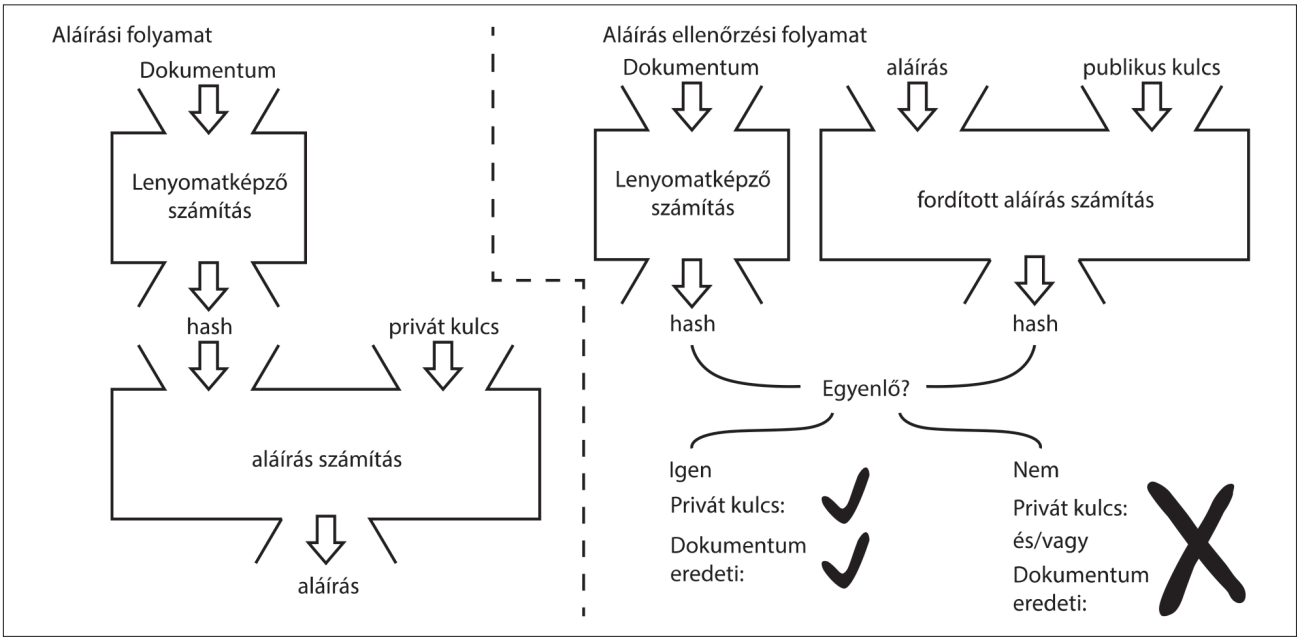
Az elektronikus aláírás két számítási eljárásból, az aláírásból és az ellenőrzésből áll. A gyakorlatban – kizárólag praktikus okokból – a dokumentumból számolt lenyomat (hash) értéket írjuk alá, mert a lenyomatképző (hash) függvényekről alapos okkal vélelmezzük, hogy annak előállítására gyakorlatilag csak az adott dokumentum birtokában van lehetőség. Az aláírás során a hash értékből kell kiszámolni az aláírást. Első követelményként azt szeretnénk, hogy erre csak az aláíró legyen képes, ezért a számítás során egy olyan adatra van szükség, amelyhez csak ő fér hozzá. Ezt a számot nevezzük privát kulcsnak. Az aláírás tehát az aláírt adattal (vagy hash értékével) és a privát kulccsal végzett számítás eredménye.

2.3. Az elektronikus aláírás ellenőrzése

A számként létező aláírás érvényességét úgy ellenőrizhetjük, hogy az aláíráson elvégzünk egy számítást. Ha ennek eredménye az eredeti aláírt értéket adja, úgy az aláírás érvényes. A feladat tehát az aláírási számítás megfordításának, azaz inverzének megtalálása. Tehát az aláírásból kell kiszámolni a hash értéket. Vannak-e ilyen függvények? Igen, vannak, de ennek részletezésétől itt eltekintek. Az ellentétes irányú aláírás-ellenőrző függvény praktikus, ha nem alapul aláírónként, azaz privát kulcsonként más-más számítási eljáráson, hanem mindig ugyanazt az algoritmust, a privát kulcshoz tartozó szám-paraméterrel használjuk, így megfordítva az aláíró számítást. Ezt a paramétert, azaz számot nevezzük nyilvános kulcsnak. A privát és a nyilvános kulcs tehát olyan értelemben összetartozik, hogy két számítást egymás ellentettjévé tesz. A használt számítási módszer az aláírandó adatból és a privát kulcsból aláírást számol, az aláírásból és a nyilvános kulcsból pedig aláírt adatot.

Az aláírás ellenőrzése tehát a következőképpen történik. Az ellenőrzést végző a dokumentum birtokában kiszámolja a hash értéket, majd az aláírás és a nyilvános kulcs birtokában végrehajtja az aláírás inverz műveletét. Ha a két számítás azonos eredményt ad, az aláírást a nyilvános kulcshoz tartozó privát kulccsal hajtották végre azon a dokumentumon, amelyet mi is birtoklunk. Ha az eredmény más, akkor vagy nem a nyilvános kulcshoz tartozó privát kulcsot használta az aláíró, vagy a dokumentum azóta megváltozott, vagy mindkettő.

Amit itt számítási eljárásnak nevezünk az maga a rejtjelezési módszer, amellyel szemben számos feltételt kell támasz-



tani. Egyik elsőre látszik: a nyilvános kulcs ismeretében ne lehessen kiszámítani a privát kulcsot!

Az itt vázolt módszer a nyilvános kulcsú infrastruktúrán (PKI-n) alapuló elektronikus aláírás. A jogi szabályozást megteremtő eIDAS rendelet az alkalmazott technológiát tekintve semleges kívánt maradni, de a gyakorlatban más módszert nem alkalmaznak. PKI infrastruktúrát több kriptográfiai (rejtjelezési) eljárásra is lehet építeni.

3. A fenti számítások hogyan eredményeznek jogi hitelességet?

A hagyományos, papír alapú aláírás vizsgálatánál a cél az aláírás és az aláíró személy közötti kapcsolat bizonyítása. Ott kézzel fogható, szemmel látható tulajdonságokat vizsgálnak hitelesítéskor. Milyen tulajdonsága legyen egy fokozott biztonságot adó elektronikus aláírásnak? A jogszabályt egy kicsit a fenti példára átfogalmazva:

1. Kizárólag az aláíró személyéhez kötődjön. Ezt úgy tudjuk biztosítani, ha a privát kulcshoz csak az fér hozzá, akinek az aláírást tulajdonítjuk.
2. Legyen alkalmas az aláíró azonosítására. Az ellenőrzést végző számára derüljön ki, hogy a nyilvános kulcs kinek a privát kulcsához tartozik.
3. Más nagy valószínűséggel ne legyen képes létrehozni az adott kulcspárt.
4. Kötődjön a dokumentumhoz. Az aláíró egy dokumentum ismeretében ne legyen képes egy másikat konstruálni (kiszámolni), amelynek ugyanaz az aláírási értéke.

A fentiekből következik, hogy az aláírás letagadhatatlan, mivel csak az képes egy dokumentumot aláírni, aki rendelkezik magával a dokumentummal és a privát kulccsal. Más az aláírás kiszámítására nem képes. Ha valaki a dokumentumot, az aláírást és a nyilvános kulcsot közzéteszi, nem tudja letagadni, hogy az aláírást maga számolta ki, mivel erre más nem volt képes, feltéve, hogy az bizonyított, hogy a nyilvános kulcshoz tartozó privát kulcsról valaki igazolja, hogy az övé.

A privát és a nyilvános kulcs két szám. Hogyan biztosítható az, hogy az valakihez kötődjön? Ha valakivel személyesen találkozom és átadok neki egy papírt, amelyre rá van írva a nyilvános kulcsom egy olyan nyilatkozattal együtt, hogy a kulcs használatát a saját kezű aláírásommal egyenértékűnek ismerem el, akkor a hagyományos hitelesség segítségével létrehoztam a kapcsolatot az ezen kulcs privát párjával készült aláírás és köztem. Ha partnerem a papírról számítógépbe írja ezt a kulcsot, az aláírásom ellenőrzéséhez szükséges számításokat el tudja végezni. Mindezt közjegyző előtt is megtehetjük. Megjegyzem, hogy a privát kulcsot az itt leírt példában is csak én ismerem, általam vagy az én birtokomban lévő eszközzel került előállításra. A probléma az, hogy mindenkinek, aki ezzel a kulccsal aláírt dokumentumra akar jogvitában hivatkozni, szüksége van egy ilyen aláírt papírra vagy hitelesített másolatára. Ez jelentős akadályt gördítene a gyakorlati alkalmazás elé, ezért más megoldást használnak, mely az eIDAS rendeletnek is megfelel.

4. Bizalmi szolgáltatók

Ennek a problémának a megoldására jöttek létre a bizalmi szolgáltatók. Az ő feladatuk az, hogy egy aláírás nyilvános kulcsa és az aláíró személye közötti kapcsolatot – akár a fenti nyilatkozathoz hasonló módszerrel – megállapítsák, majd erről saját elektronikus aláírásukkal egy nyilatkozatot tegyenek közzé. Mivel ez is egy elektronikus aláírás, ezt is hitelesíteni kellene egy újabb bizalmi szolgáltatónak, aki még nem szerepelt a hitelesítési láncban. Ez azonban nem mehet a végtelenségig. Kell egy úgynevezett gyökértanúsító, akinek az aláírásában a jog erejénél fogva meg kell bízni. Ők egy minősítő eljárást követően egy állami hatóságtól (Magyarországon az NMHH-tól) kapják meg ezt a felhatalmazást, ezért őket minősített bizalmi szolgáltatónak nevezzük. Megjegyzem, hogy nem hierarchikus rendszerek is léteznek. Ebben bárki, aki „biztos abban", hogy egy nyilvános kulcs egy általa ismert személyhez tartozik, aláírja a kulcsot és közzéteszi. Így mindenki, aki benne megbízik, már abban az aláírásban is megbízhat (bizalmi hálózat). Mivel az gyakorlatilag nem ellenőrizhető, hogy ki, kit, hogyan vesz rá nyilvános kulcsának hitelesítésére, a módszer mögé nehéz lenne jogi szabályzást alkotni.

Mikor hitelesítsen a bizalmi szolgáltató? Ehhez az aláíró személyének megállapítása sajnos kevés. Az eIDAS 26. cikkében megfogalmazott négy feltétel, köztük a *„kizárólagos személyhez kötődés"*, a más általi hozzáférhetetlenség biztosítása csak egy sor műszaki és eljárási feltétel teljesülése esetén garantált. Elvileg lehetséges lenne, hogy létrehozok egy PKI rendszert, abban generálok saját kulcspárt, majd a nyilvános részt odaadom a bizalmi szolgáltatónak hitelesítésre. Ő a hitelesítést megtagadja, ha előtte nem győződött meg arról, hogy a saját rendszerem megfelel-e a szigorú műszaki feltételeknek, az annak használata során követett eljárásom és dokumentációs rendszerem pedig logikailag és fizikailag biztonságos-e. Ehelyett tőle tudok elektronikus aláírást létrehozó eszköz vásárolni, amely létrehozza a kulcspáromat, amelynek nyilvános tagját már hitelesíteni fogja.

5. A minősített és a nem minősített bizalmi szolgáltató közti különbség

Az eIDAS nem köti minősített bizalmi szolgáltató – sőt még csak bizalmi szolgáltató – közreműködéséhez sem a fokozott biztonságú elektronikus aláírás érvényességét. Például két cég vezetői dönthetnek úgy, hogy egymás PKI rendszerét hitelesnek fogadják el. Erről köthetnek szerződést. Ebben az esetben viszont amennyiben az aláírások érvényességével kapcsolatban kétely merül fel, a bizonyítási teher azé, aki azt megfogalmazza. Én például nem szívesen fogadnám el egy olyan rendszer biztonságát, amely az ellenérdekű fél kontrollja alatt áll.

A minősített bizalmi szolgáltatóról a felügyeleti hatóság előzetesen megállapította, hogy a jogszabályi feltételeknek megfelelően működik. A nem minősített bizalmi szolgáltatókat előzetesen nem kötelező ellenőrizni. Ügyfelük bizal-

mára építve működnek. *„A felügyeleti szervnek csak akkor kell eljárnia, ha arról értesült (például az adott nem minősített bizalmi szolgáltatótól, más felügyeleti szervtől, felhasználótól, üzleti partnertől vagy saját vizsgálata alapján), hogy valamely nem minősített bizalmi szolgáltató nem tartja be a rendelet követelményeit"* [eIDAS preambulum (36)]). A 13. cikk (1) szerint ráadásul *„[a] nem minősített bizalmi szolgáltató szándékosságát vagy gondatlanságát annak a természetes vagy jogi személynek kell bizonyítania, aki/amely állítása szerint az első albekezdésben em*lített kár megtérítését követeli*"*. Lássuk be, hogy egy magánszemély erre gyakorlatilag képtelen. Amennyiben tehát egy ágazati jogszabály egy szolgáltató (például egy bank) magánszemély ügyfelének védelmében kötelezővé teszi legalább fokozott biztonságú elektronikus aláírás alkalmazását, úgy az alkalmazott aláírókulcsnak minősített bizalmi szolgáltató által kibocsátott tanúsítványon kell alapulnia. E nélkül a szabályozási cél, azaz az ügyfél védelme egyszerűen nem teljesül.

Gondoljunk bele, hogy az elektronikus aláírás célja egy nyilatkozat kibocsátó általi hitelesítése. Ha feltétlen, mindig fennálló bizalmat feltételeznénk az ügylet résztvevői között, akkor nem lenne szükség elektronikus aláírásra. Ha a jogszabály mégis előírja a legalább fokozott biztonságú aláírás használatát, azt azért teszi, hogy példánkban mind a banknak, mind a bank ügyfelének bizonyító erejű elektronikus dokumentum legyen a birtokában a megállapodás tartalmáról. Milyen garanciát ad egy olyan aláírással ellátott dokumentum, amelynek birtokában az ügyfélnek magának kell bizonyítania, hogy egy bonyolult kriptográfiai rendszer biztonságosan működik-e? Ahol igazságügyi informatikai szakértőt kell igénybe vennie, aki a PKI rendszer alapos vizsgálata után mond arról valamit, hogy a felek aláírása hiteles-e? Ez gyakorlatilag semmi védelmet nem ad a megfelelő anyagi eszközökkel, tudással és érdekérvényesítő képességgel alig rendelkező magánszemély ügyfélnek. A példában említett ágazati szabály megalkotójának nyilvánvalóan nem ez volt a szabályozási célja.

6. …és ha nincs bizalmi szolgáltató?

Első példámban bizalmi szolgáltató közreműködése nélkül, a polgári jog alapján létrejött, papír alapú megállapodás szerint ismerték el kötelező erejűnek aláírásukat a felek. Az ilyen megállapodás mögött is lehet az eIDAS fokozott biztonságú aláírását kielégítő rendszer. A probléma az, hogy egyrészt az ügyfélnek nyilvánvalóan nincs ilyen saját rendszere, másrészt az ügyfél általában képtelen megállapítani, hogy a bank rendszere ilyen-e. A bank ilyenkor nyilván saját vagy (nem bizalmi szolgáltató) megbízottja rendszerének használatát írja elő. Ez teljes nonszensz! A felek közötti majdani esetleges viták eldöntéséhez bizonyítékot szolgáltató rendszer az egyik fél kizárólagos kontrollja alatt van. A helyzetet fokozza, ha a privát kulcs nem az ügyfél rendszerében keletkezik. Ez egyébként valószínű, hiszen az ügyfélnek csak akkor van ilyen *„rendszere"*, ha például egy aláíró smart card-ot kap a banktól. E nélkül a bank vagy nem minősített megbízottjának kontrollja alatt marad a privát kulcs. Ilyenkor logikai értelemben az aláírás olyan, mintha semmilyen biztonságot nem nyújtana: az ellenérdekű fél ugyanúgy használhatja, mint az, akinek szánták.

7. Következtetés

Amennyiben tehát egy jogszabály nem bízza a felekre az elektronikus hitelesség kérdését, hanem legalább fokozott biztonságú elektronikus aláírás használatát írja elő egy elektronikus okiraton, hogy az a kívánt joghatás kiváltására alkalmas legyen, nyilvánvalóan azért teszi, hogy a jogügyletben védje a felek érdekeit. Ezt úgy éri el, hogy a feleknek olyan elektronikus dokumentumot ad a *„kezébe"*, amelynek segítségével bíróság előtt képesek bizonyítani azt, hogy mi a megállapodás tartalma. Ha ehhez további bizonyítási eszközökre van szükségük, például műszaki körülmények vizsgálatára, akkor a jogszabály nem éri el célját. Ezért az ilyen értelmezés nyilvánvalóan ellentétes a jogalkotói szándékkal. A minősített bizalmi szolgáltató nélküli aláírás a kívánt garancia megteremtésére nem képes.

8. Kiegészítés: az elektronikus aláírás és a polgári perrendtartás

Előfordul, hogy a polgári perrendtartásról szóló 2016. évi CXXX. törvény (Pp.) 325. § (7) bekezdését általában hivatkozzák az elektronikus aláírásokkal kapcsolatban felmerülő kétség esetén. Véleményem szerint az ilyen érvelés nem megalapozott, legfeljebb példaként használható. A Pp. az elektronikus aláírásra vonatkozó szabályokat általánosan nem, kizárólag a közokiratra (a 323. §-ban) és a teljes bizonyító erejű magánokiratra (a 325. §-ban) vonatkozóan tartalmazza. Az általános értelmezés hibás voltát mutatja az is, hogy abban az értelmezésben a (7) bekezdés hiányossá válik, mivel bizalmi szolgáltató hiánya esetén az aláírással vagy az okirat hamisítatlanságával kapcsolatos kérdésekben – a jogszabály rendelkezésével ellentétben – nincs bizalmi szolgáltató, akihez a bíróság fordulhat. Ha azonban a (7) bekezdést kizárólag a szakasz címében is meghatározott teljes bizonyító erejű magánokiratra alkalmazzuk, a rendelkezés nem hiányos. Ez az okirati fajta ugyanis háromféleképpen hozható létre elektronikus formában: minősített vagy minősített tanúsítványon alapuló elektronikus aláírással, azonosításra visszavezethető dokumentum hitelesítéssel, valamint törvényben vagy kormányrendeletben meghatározott szolgáltatással. Az első esetben az eIDAS szerint szükséges a minősített bizalmi szolgáltató közreműködése, a két utóbbi esetben pedig a szolgáltatást a Kormány a NISZ Zrt.-n keresztül biztosítja AVDH és e-Papír néven, azaz a hitelességet hazai jogszabály felhatalmazása alapján ez a szolgáltató garantálja.