2023

ICDL modultankönyv

ECDL elektronikus hitelesség, elektronikus aláírás

dr. Erdősi Péter Máté

Neumann Társaság

Szerző: dr. Erdősi Péter Máté

Nyelvi lektor: Rákosi Szilvia

ICDL szakmai lektor: dr. Keszthelyi András, intézetigazgató, Óbudai Egyetem, Szervezési és Vezetési Intézet

A kiadást a Magyar Elektronikus Aláírás Szövetség Egyesület és az Időérték Kft. támogatta.

Kiadó: Neumann János Számítógép-tudományi Társaság

Felelős kiadó: dr. Beck György, elnök, Neumann János Számítógép-tudományi Társaság

ISBN: 978-615-5036-25-5

Jogi nyilatkozat

A kiadvány gondos szakmai előkészítéssel, az ICDL program jogtulajdonosa, az ICDL-F előírásai alapján készült. Ezzel együtt az NJSZT, mint kiadó, az esetlegesen előforduló hibákért és az azokból eredő bármilyen következményekért nem tehető felelőssé. A változtatás jogát az NJSZT fenntartja

Támogatók:

MELASZ
Magyar Elektronikus Aláírás Szövetség

https://melasz.hu

Időérték Kft.

Tartalomjegyzék

1 Előszó

Ez a tankönyv az ICDL Foundation által támogatott Elektronikus Hitelesség, Elektronikus Aláírás modulhoz készült. Az informatika, a digitális világ fejlődésével és annak a mindennapokban való térnyerésével egyre fontosabb kérdéssé vált a hitelesség biztosítása a legtöbb elektronikus folyamatban, és egyre inkább elektronikus folyamatok vesznek minket körül. Az Európai Unió 1999-ben szabályozta először, és 2014-ben másodszor az elektronikus hitelesség európai közösségi alkalmazásának kérdéseit, de ennek széles körű elterjedése az európai társadalmakban – számos sikeres és eredménytelen kezdeményezést követően – a közelmúltig váratott magára. Az utóbbi évek eseményei azonban megmutatták, hogy hitelesség nélkül csak egy bizonyos szintig lehetséges bármilyen elektronikus folyamatot hosszú távon fenntartani. Ennek oka a biztonság hiánya vagy nem megfelelő szintű kialakítása és az ebből adódó törvényszerű bizalmatlanság. Az elektronikus folyamatok fejlődésének, továbbfejlesztésének irányai ismertek, de mára ennek korlátjává vált sok esetben a hitelesség hiánya vagy alacsony szintje. Emiatt és a fejlődési kényszerek miatt válik indokolttá az elektronikus hitelesség széles körben való megismerése és ehhez kapcsolódóan a gyakorlatban való használati tudásának igazolása. A közeljövő munkaerőpiacán vélhetően nagyobb esélylyel próbálkozik az, aki távolról is tud hitelesen elektronikusan kommunikálni, illetőleg ismeri és képes használni az elektronikus hitelesség különböző formáit is. Nem elhanyagolható a magyar közigazgatás digitalizációjának folyamatos fejlődése sem. Egyre inkább kötelezve lesznek az érintettek az elektronikus csatornák használatára, egyrészről a hatékonyság, másrészről a fenntarthatóság miatt. A digitális ökoszisztémának az elektronikus hitelesség, elektronikus aláírás mára nagyon fontos részévé vált, ennek megismerése alapvető fontosságú a digitális készségekkel rendelkező digitális polgár számára.

Ehhez azonban olyan háttérrendszert kellett létrehozni, mely a társadalom minden tagja számára egyforma eséllyel biztosítja a tudás megszerzésének lehetőségét, legyen életpályájának bármelyik szakaszán, és rendelkezzen bármilyen ismerethátterrel. Ezt a hátteret biztosította az ICDL Foundation az elektronikus aláírásról szóló támogatott modul akkreditálásával, mely a Neumann János Számítógéptudományi Társaság (NJSZT) mint modulgazda és a Magyar Elektronikus Aláírás Szövetség (MELASZ) szakmai támogatásával jöhetett létre.

A tankönyv célja az, hogy tartalmazza mindazon elméleti és gyakorlati tudnivalókat az ICDL Elektronikus Hitelesség, Elektronikus Aláírás támogatott modulból vizsgázni kívánók számára, melyekkel a sikeres vizsgára felkészülhetnek. A modul ismeretanyagának elsajátítása során – az elektronikus hitelesség jellegéből adódóan – előny az alapfokú számítógépes ismeret megléte (internethasználat, levelezés, szövegszerkesztés, táblázatkezelés stb.), mivel a tananyag ezek ismeretét feltételezi, és ezeket egészíti ki az elektronikus hitelesség elemeivel. A vizsgán az elméleti kérdéseket és a gyakorlati megoldásokat is számítógép segítségével kell majd előállítani, ezért a tanár segítségével történő felkészülés mindenképpen előnyös lehet a sikeres vizsgához. A könyv felépítése azonban olyan, hogy gyakorlottabb felhasználók otthon is el tudják sajátítani az elektronikus aláírást elmélettel és gyakorlattal együtt.

Az egyes fejezetek azt az ismeretanyagot tartalmazzák, melyek az elektronikus aláírás mindennapi használatához feltétlenül szükségesek – ideértve annak eldöntési képességét is, hogy egy adott szituációban a kommunikáció melyik formája mellett lehet és kell dönteni, azaz lehetséges-e választani a papír, az elektronikus és az elektronikusan aláírt kommuni-

káció között. Minden fejezet végén gyakorló kérdések segítenek a lényeg kiemelésében és a tudás elsajátításának ellenőrzésében.

2022-ben műszaki és társadalmi értelemben már széles körben lehetséges az elektronikus hitelességet megvalósító szolgáltatások igénybevétele, hiszen több éve léteznek minősített és nem minősített tanúsítványok, illetve időbélyegek kibocsátása, szakosodott minősített bizalmi szolgáltatók, és ezek hatósági felügyelete. Ezek a kialakult és működő intézmények a mindennapokban teszik használhatóvá az elektronikus hitelességet, és garanciát jelentenek a folyamatosan ellenőrzött működésre.

Az alábbi rövid felsorolás a teljesség igénye nélkül tartalmazza azokat az előnyöket, amelyeket egyéni és társadalmi szinten lehet biztosítani a hiteles elektronikus kommunikációval – a mai európai közszolgáltatásokat is igénybe véve:

1. gyors és hiteles (azonnali) kommunikáció,
2. sorban állás nélküli (akadálymentesített) ügyintézés,
3. papíralapú ügyintézéshez felhasznált erőforrások és energia csökkentése (fenntarthatóság),
4. távmunka, otthoni munkavégzés,
5. ügyintézés, munkavégzés helyszínére való utazáshoz szükséges üzemanyag csökkentése (szmoghelyzetek csökkentése).

Ezeket az előnyöket realizáló tudáshoz és a mindennapokban is használható gyakorlathoz kívánja hozzásegíteni ez a könyv az Olvasót.

A könyvben szereplő fogalmak alkalmasak a tárgyban kialakult miszticizmus és zavarosság megszüntetésére, mivel minden fejezet pontos, jól megfogalmazott definíciókat tartalmaz és használ. A könyv kiadójának szándéka az, hogy ezt a területet tudományos igénnyel, de ugyanakkor közérthető módon építse be napjaink társadalmába.

A vizsga platformfüggetlen módon is lebonyolítható, mivel minden platformra léteznek már olyan szoftverek, amelyekkel a vizsgafeladatok – egyszerűbben vagy bonyolultabb módon – megoldhatóak.

Az alábbi táblázatban összefoglaltuk azokat a platformokat és alkalmazásokat, amelyeken a gyakorlás lehetséges és ajánlható.

Alkalmazások Operációs rendszer	Irodai csomagok	Böngészők	Aláíró programok, csomagok
Windows	MS Office 365 OpenOffice, Outlook	Chrome, Firefox	KEAASZ, PGP, OpenSSL
Linux	OpenOffice, Evolution	Firefox	KEAASZ, GnuPG, OpenSSL
Mac OS X	Office for Mac MS Office 365 OpenOffice	Firefox	GnuPG OpenSSL

1. táblázat: Lehetséges vizsgaplatformok és alkalmazások

Az elektronikus levelezéssel kapcsolatos ismeretek alulreprezentáltsága szándékos, ezeknek az ismereteknek a használatát az ICDL Online alapismeretek modul segít elsajátítani.

A mai könyvpiacon számos elektronikus aláírással kapcsolatos elméleti és gyakorlati könyvvel lehet találkozni. Egyesek komoly matematikai fejtegetéseket is tartalmaznak – ez egye-

temi szinten és tudományos publikációknál figyelhető meg, mások részletesen ismertetik a rövid elméleti bevezető után egy-egy adott szoftver működését, használatát. Az ICDL vizsga jellegét tekintve alapvetően gyakorlatias, számítógép-használati jogosítványt ad a birtokosának, ezért ennek a könyvnek az a kimondott célkitűzése, hogy olyan elméleti és gyakorlati ismereteket adjon át, amelyekkel bármelyik platformon tetszőleges alkalmazás használata elsajátítható a vizsgára felkészülni kívánó olvasó számára. Elméleti háttér nélkül csak megértés nélküli mechanikus folyamatvégzést („gombok nyomogatását") lehet elsajátítani, hiszen a „Miért van ez így?" kérdésre a válasz nem adható meg az ehhez szükséges háttérismeretek nélkül. Emiatt a könyv elméleti részeket is tartalmaz, de csak annyit és olyan részletességgel, melyek a gyakorlati összefüggések megértéséhez szükségesek. A könyv ezért olyan gyakorlati ismereteket ad, amelyek nemcsak egyetlen alkalmazás használatát tanítják meg a vizsgára készülőnek, hanem minden aláírás-készítő programnál alkalmazhatóak. De a könyvnek nem célja az összes aláírás-készítő szoftver működésének részletes ismertetése – célkitűzési, terjedelmi és szoftverváltozási okokból –, hanem csak olyan részletességű gyakorlati ismeretanyagot tartalmaz, melyekkel a szoftverek értő működtetése – a sikeres vizsgára való felkészülés – megvalósítható. Megjegyezzük, hogy a vizsgát követően ez a tudás a mindennapi életben könnyen és egyszerűen alkalmazható.

A kiadó az ICDL vizsgákhoz sikeres felkészülést, és sok pozitív élményt kíván az elektronikus ügyintézés, elektronikus hitelesség, elektronikus aláírás mindennapos alkalmazásában!

Dr. Beck György

elnök

NJSZT

2 Információ és információs társadalom

2.1 Az információ fontossága

„*Valamikor az információ szolgálta az embert s nem az ember az információt. Arra volt hivatott, hogy segítse az embert s nem pedig arra, hogy kiszolgáltatottá tegye. Az értelmezésénél szakadt be alattunk a jég*” – írja az információ világának egyik vezetője, a Literator kiadó főszerkesztője, a Sorbán Attila által írt „Békák a szőnyegen” című könyv előszavában. A gondolatsort tovább fűzi azzal a gondolatkísérlettel, hogy ha egy ember egy rögzített pillanatban a világ minden jelen lévő információját birtokolná, minden újságot elolvasna, minden hírműsort meghallgatna, minden portált megnézne – megérti-e ebből az az ember, hogy ő maga merre tart ebben a világban, és egyáltalán szerepe van-e benne.

A fenti bekezdésben több olyan kifejezés is van, amelyik magától értetődőnek látszik, de mélyebb boncolgatásakor kiderül, hogy egyáltalán nem az. A „minden jelen lévő információ” fogalmával kapcsolatban fel lehet tenni azt a kérdést, hogy **hol** van jelen az információ. További kérdést lehet feltenni a megértéssel kapcsolatban, tulajdonképpen mikor lehet azt mondani, hogy „valaki **megért** valamit”? És lehet-e a megértés fogalmát használni akkor, ha az információbevitelt nem követi semmilyen cselekvés, **hatás**? Ezek a kérdésfeltevések indokolják az információ és az információs társadalom kapcsolatának alaposabb vizsgálatát.

Bárány-Horváth Attila az információelmélet alapelvei és az evolúció kapcsolatának kutatójaként így írt az információ fogalmának használatáról 1998-ban:

„... 1948-ban két alapvető információnális munka jelent meg: Norbert Wiener megveti a kibernetika, míg Claude E. Shannon a matematikai információelmélet (valójában kommunikációelmélet) alapjait. Ennek ellenére (bizonyos értelemben éppen ez okból) századunk (a XX.) leghomályosabb és legvitatottabb fogalmaként híresült el az információ. Wiener sejtéseket fogalmaz meg: »Az információ az információ, nem anyag és nem energia« (’Information is information, not matter or energy’), méghozzá formailag minősíthetetlenül (egy kirívó tautológiát két tagadás követ anélkül, hogy valamit is állítana). Ezzel elszabadul a pokol: sok száz azoknak a száma, akik megkísérlik vérmérsékletük, szakmájuk, érdeklődési körük, tágabb vagy szűkebb látóhatáruk, tudományfilozófiai felfogásuk stb. vetületében behatárolni az információ fogalmát. Hiányos féligazságok, egymásnak ellentmondó meghatározások kavalkádja sorjázik, melyek a beavatottakat is zavarba ejtik. Mi több, a disszonancia inflálódik.”

2.1.1 Az információ fogalomrendszere

Az **információ** fogalmának használata meglehetősen széles körű. Magyarázatok alakultak ki az információ kvalitatív (minőségi) és kvantitatív (mennyiségi) rendszereiről. A nem megfelelő szóhasználat értelmezési zavarokat is okoz sok esetben, ha nem azonos rendszerben vagy eltérő jelentéssel használják azt. Az információ szónak kialakult a hétköznapi, a tudományterületenkénti, a társadalmi (jogszabályi), és számos más egyéb helyen történő alkalmazása. Az információ fogalmának használata tehát sok területen magától értetődő, és régóta létező jelenség. Intuitív módon összekapcsolódnak az információhoz tartozó fogalmak (jel, jelentés, megértés, átvitel, bit, adat stb.), és sokszor a használatukkal sincsen semmi probléma, ha a kommunikációs partner is hasonló módon értelmezi azokat. A szabatos kifejezésmódhoz ennek ellenére ajánlatos a fogalmak és a kapcsolódó elméletek átfogó ismere-

te. Ezért ez a fejezet röviden áttekinti az információhoz kapcsolódó kutatásokat, elméleteket, fogalmakat és az eddig megismert eredményeket.

Az információ filozófiai megközelítéséhez felidézzük Bertrand Russel gondolatait:

„Az egymással harcban álló fanatizmusok zűrzavarában a kevés összetartó erő egyike a tudományos igazmondás lehet, melyen azt értem, hogy nézeteinket a lehető legszemélytelenebb, a helyi és egyéni előítéletektől leginkább mentes megfigyelésekre és következtetésekre alapozzuk. Hogy (Rousseau) szorgalmazta ennek az erénynek a filozófiába való beiktatását és hogy olyan hathatós módszert alkotott meg (logikai analízis), amely ezt lehetővé is teszi, az annak a filozófiának a fő érdeme, amelyhez magam is tartozom. Az e módszer által megkövetelt körültekintő igazságkeresés kiterjeszthető az emberi cselekvés egész szférájára, s ez talán csökkenti a fanatizmust s növeli az együttérzést és a kölcsönös megértést. Azzal, hogy elutasítja a dogmatikus jogköveteléseket, ez a filozófia nem mond le arról, hogy bizonyos életideált sugalljon és inspiráljon."

Az információ minőségi létezését érdekes módon a mennyiségi vizsgálatok elhatárolása igazolta azzal az állításával, hogy az információ az átvitelekor jel segítségével továbbítódik. Ebből azonban az is következik, hogy az információ létezik, jel nélkül is van értelme erről beszélni. Különböző észlelhető jelenségek és folyamatok veszik körül az embert, olyanok, amelyek az emberrel való kölcsönhatásban, felhasználásuk és különböző értelmezésük kapcsán lesznek információvá. Az egyik legfontosabb kulcsszó tehát az értelmezés.

Az információ megjelenési formája az **információs alakzat**, mely lehet ismeret, tudás, bölcsesség, készség, jártasság, tapasztalat, emlékezet, hagyomány, vélemény, meggyőződés, hit, világkép, nyelv, pletyka, rémhír. Az információs alakzatok közül a világkép kiemelt, azon az alapon, hogy az összes többi **transzformálódik**, a világkép kivételével.

Halassy Bálint fogalmilag szétválasztotta az adatot az információtól, és ez utóbbit emberközpontúan értelmezte. Definíciója szerint az **adat** értelmezhető (észlelhető, érzékelhető, felfogható és megérthető) ismeretet jelöl, míg az **információ** nem más, mint új ismeretté értelmezett adat.

Az információt az információelmélet atyjaként elhíresült Claude E. Shannon információelmélete tette mérhetővé 1948-ban. Ez az elmélet a híradástechnika (kommunikáció) új fejezetét nyitotta meg, mely a kommunikáció általános törvényszerűségeivel foglalkozik. Megállapításai azonban kizárólag olyan jelenségekre vonatkoznak, amelyek a távközlés különböző fizikai megvalósításaival függenek össze. Az információelméletben az információ szó nem a lélektani fogalmat írja le, hanem **fizikai rendszerek** objektív tulajdonságait tárgyalja annak érdekében, hogy jobb minőségű és hatékonyabb **távközlési** berendezéseket lehessen létrehozni. Ez ennek az elméletnek az erőssége és egyben a gyengesége is. Az információelméletből nem származtak még olyan új távközlési rendszerek, amelyek lényegesen eltérnének az eddigi rendszerektől.

A híradástechnikai rendszerek **statisztikai** jelleggel foglalkoznak az információval. Egy távközlési csatorna nem arra készül, hogy egy **meghatározott** közlést vigyen át egyik pontból a másikba, hanem a feladata a lehetséges közlések összességéből véletlenül kiválasztott **bármelyik** közlésnek az átvitele. A feladathoz mindig hozzátartozik az átviteli hibák legnagyobb megengedett gyakoriságának rögzítése is (azaz zajos csatorna is megengedett).

Az információelmélet az információ szót tehát speciális értelemben használja, nem engedi meg összekeverni a szó szokványos értelmével. Példa erre, hogy egy **képtelenség** és egy **nagy jelentéstartalmú üzenet** információtartalma lehet teljesen egyenértékű, mivel a jelentés műszaki értelemben közömbös. A kommunikációs csatornának teljesen mindegy, hogy melyiket kell átvinnie. Ebből következik, hogy az információ kommunikációs értelemben nem igazán arra vonatkozik, hogy „mit mondanak”, hanem hogy „mit mondHATnak”, más szóval az információ fogalma ebben az elméletben nem egyedi üzenetekre vonatkozik (mint a jelentés), hanem sokkal inkább az összes üzenet halmazára és a belőlük való választási szabadságra. Az információ további fontos kommunikációelméleti tulajdonsága, hogy jellemzi egy adott fajtájú információforrás által produkálható üzenethalmaz statikus szerkezetét, ez különösen a hibajavításban és a kódfejtésben fontos, ez a tulajdonság teremti meg a kódfejtés lehetőségét, statisztikai módszerek felhasználásával, így válik lehetővé a hiányzó információ pótlása, emlékezet nélküli és emlékezettel bíró információforrás rendszerek esetében is, ahol a múltbeli értékek az üzenetet teljes mértékben meghatározzák.

Az információ egysége a bit, értéke 0 vagy 1, két kimenetelű eseményhez tartozó valószínűség alapján. Az információ értékének további paradox furcsasága, hogy a maximális információmennyiséget hordozó üzenet **érdektelen**, mivel nem lehet megérteni. Itt minden jel egy külön világ, ha egy is hiányzik, egy egész világ tűnik el. Vagyis, ha maximális az információtartalom, ez tulajdonképpen nem jelent (érthető) információt, a figyelem ezt visszautasítja, mint reménytelen esetet. Következésképpen a **redundancia** a kommunikációban nagyon fontos szerepet tölt be a megértés szempontjából.

Az információs társadalom legnagyobb kérdése a kommunikációelmélet felé az, hogy a megtermelt információt hogyan lehet a kommunikációs csatornákon **eljuttatni** az információs társadalom minden tagja számára. Az aktuális és a jövőbeli várható helyzet az, hogy egyre növekvő mennyiségű információt kell eljuttatni, egyre több ember számára.

2.1.1.1 Archiválás az információrendszerekben

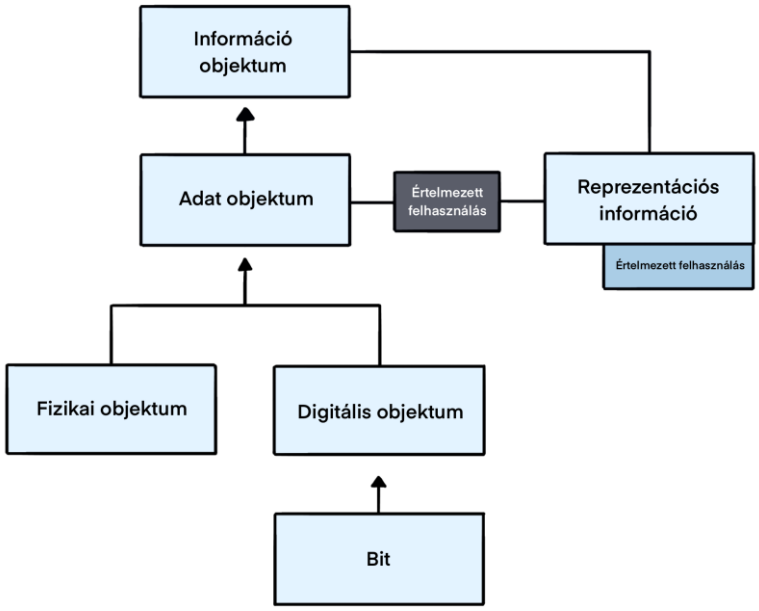
Az információ **megőrzési** igénye további eredményekkel gazdagította az információval kapcsolatos területeket a gyakorlat szintjén is. Megközelítési módja szerint nemcsak a fizikai, hanem a digitális formában létező információk megőrzésére is módszert ad, felismerve a hosszú távú megőrzés problémáit.

Az egyiptomi kőtábla példát alapul véve az információtartalmat a kőtábla hosszú ideig őrizte még azután is, hogy újra megtalálták és emberi szemek elé került. Tartalmának elolvasása és megértése számos megoldandó feladat elé állította a tudósokat. Ezeket a tapasztalatokat az archiválás tudománya feldolgozta, és ma már szabványok tartalmazzák az archiválás gyakorlati követelmény- és fogalomrendszerét, ami természetesen nem nélkülözheti az információval kapcsolatos fogalmakat sem.

Archiválási szempontból **információnak** nevezik a tudás bármelyik olyan formáját, amit továbbítani lehet. Az információt a továbbítás során az adat reprezentálja. Példa erre egy olyan bitsorozat, mely egy számot jelent, azzal az értelmezési információval, hogy ez egy adott tárgy hőmérsékletét jelenti Celsius-fokban megadva.

A nyílt archiválási információrendszerek olyan modellek, melyek **információobjektumok**at őriznek meg **hosszú távon**.

Az alábbi ábra szemlélteti egy szabványos információobjektum struktúráját:



1. Információs objektum az archiválási rendszerekben

Az archiválás során a hosszú táv azt jelenti, hogy a megvalósítás megfelelőségét – a megőrizhetőséget – nem befolyásolhatja egy esetleges technológiaváltás, új média megjelenése, új adatformátumok kialakulása vagy a felhasználói közösség megváltozása sem. Éppen ezért a hosszú táv pontos értéke nem meghatározható, a távoli jövőre is kiterjedhet. Az archiválás során az archiválási rendszer olyan információcsomagokat őriz meg – ilyen például egy archiválásszolgáltató –, amely minden időpillanatban és minden esetben tartalmazza a benne tárolt információs objektumok elolvasásához és értelmezéséhez szükséges információkat.

2.1.1.2 Az információ fogalma a biztonságtechnikában

Egyetemi kurzusokon – hasonlóan az információtörténeti megközelítéshez – olyan megfogalmazások fordulnak elő, mely szerint az **információ** alatt azokat az ismereteket kell érteni, amelyek ahhoz szükségesek, hogy egy vezető által irányított szervezet a társadalmilag elvárt módon működjön. Ezek az ismeretek a vezető fejében képződnek, és ezek az ismeretek **adat**ként jutnak el a beosztottakhoz. A beosztottak által termelt adatból ismét információ lesz a vezető fejében. Ebben az esetben az információ új ismeretté **értelmezett adat**, csak az emberben keletkezik, aki a **megismerést** létre tudja hozni. Az informatika ilyen értelmezésben az információk megszerzésével, tárolásával és feldolgozásával összefüggő **ismeretek** összessége. Szükség van a klasszikus információ fogalmának bevezetésére is, ami a jelek, jelsorozatok tartalmi jelentését foglalja itt magában, és új ismeretet tartalmaz, határozatlanságot szüntet meg. Az **adat** értelmezhető, de nem értelmezett ismeretként jelenik meg.

Informatikai értelmezésben a számítógépprogramok általában információs táblákkal dolgoznak. Az esetek többségében egy ilyen tábla nem egyszerűen numerikus értékek (bináris számok) amorf halmaza, mivel az egyes adatelemek között fontos **strukturális kapcsolatok** állnak fenn. Ahhoz, hogy egy számítógépet megfelelően lehessen használni, fontos, hogy jól ismertek legyenek az adatok között fennálló strukturális összefüggések, és elsajátítottak le-

gyenek azok a technikák, amelyekkel az ilyen struktúrákat egy számítógépen belül ábrázolni és kezelni lehet.

Az információtechnológiai szabványokban megjelenő **adat** definíciója nem más, mint tények, elképzelések, utasítások emberi vagy technikai eszközökkel történő formalizált ábrázolása ismertetés, feldolgozás, illetve távközlés céljára (ahogyan azt a mai ISO 27000 információbiztonsági szabványcsalád elődje, a British Standard 7799 megfogalmazta). Lényeges elem a **formalizált** ábrázolás, mert az adattal már humán értelemben csak abban az esetben foglalkozik, amikor az agyból az adat már kikerült (beszéd, jelzés, mozdulat).

Jól összhangban van a fentiekkel az információ biztonságáról Brüsszelben 1997. március 6-án kelt NATO megállapodás megerősítéséről és kihirdetéséről szóló 2000. évi IV. törvény 1. sz. függelékének a) pontjában leírt katonai célú információ definíciója: *„Az információ olyan ismeretanyagot jelent, amelyet bármilyen formában továbbítani lehet."* Tetten érhető ebben a megismerés, a formalizálás és a gépi továbbítástól való függetlenség megjelenése is.

2.1.1.3 Hétköznapi információ

Az információ fogalmát a magyar értelmező kéziszótár rövid, tömör formában így határozza meg: „1. Tájékoztatás, felvilágosítás, 2. Értesülés, adat." A hétköznapi értelemben ezek szerint akkor tekintünk egy információt a gyakorlatban jelen lévőnek, ha az megérkezett valakihez, és az meg is értette azt.

Többen vizsgálták, mennyi információ **keletkezett** a világban az adott évben. Ez például 2004-ben 1-2 exabájt (10^{18} bájt, milliárd gigabájt) volt, amelynek kb. 3 ezreléke volt a nyomtatott információ. Ez a szám 2011-re közel 300 exabájtra nőtt, 2021 decemberében pedig ott tartottunk, hogy csak a mobilhálózatok havi adatforgalma volt 84 exabájt, ami éves szinten már több mint 1 000 exabájtot jelent. Ezekben a mondatokban az információ „tárolt bit" értelemben használatos, mivel ezeket az információkat egyrészről tárolják, másrészről digitális eszközökön jelenítik meg, harmadrészt kereséskor csak digitális eszközök segítségével lesznek elérhetőek.

A magyar **jogszabályok** számtalan esetben tartalmazzák az információ szót. A legtöbb esetben általános értelemben vett tájékoztatást, adatkérést, adattárolást vagy adattovábbítást értettek alatta. Itt az információ és az adat fogalmak egymás szinonimájaként használatosak. Kivételes esetben foglalkoznak csak a jogszabályok az információ fogalmának valamilyen meghatározásával, speciális (védelmi) célból.

Ebben a könyvben az elektronikus hitelesség és az elektronikus aláírás szempontjából az információ fogalma azt jelenti, hogy az információ csak a jellel együtt jelenhet meg, a jel kódolása pedig bináris alapokon történik, mert az elektronikus aláírással vagy bélyegzéssel kapcsolatos műveletek kizárólag (a legáltalánosabb értelemben vett) számítógépekhez kapcsolható tevékenységek, és így információt csak **binárisan kódolt adat** (bitsorozat) megjelenési formájában lehetséges elektronikusan aláírni.

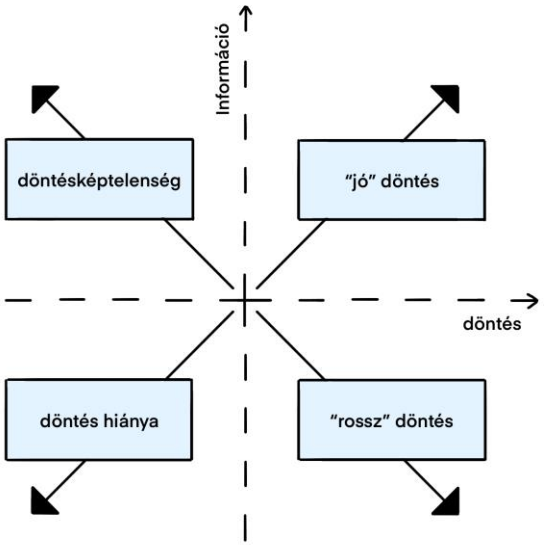
Gyakorló kérdések:

1. Van-e az információnak minden tudományterület által elfogadott definíciója?
2. Mi az információ alapegysége?
3. Mit tartalmaz a hosszú távon megőrizhető információs objektum?
4. Pontosan mit ír alá az elektronikus aláírás?

2.1.2 Az információ szerepe napjaink társadalmában

Az információval kapcsolatos műveletek végső célja valamilyen hatás elérése, általában nem öncélúan keresgetünk és fogyasztunk információt. Ebből az is adódik, hogy mindig van valamilyen célja az információ adott helyre való eljuttatásának, ellenkező esetben nem biztos, hogy az adott információ megjelenik az adott helyen. Sokszor az is lehet cél, hogy az adott helyen és időben az adott információ ne jelenhessen meg azért, hogy a hatás enélkül jöjjön létre. Ez felveti azt a kérdést, hogy akkor tehát nem mindenkinek ugyanaz a célja, nem igaz az, hogy mindenki ugyanazt a hatást szeretné elérni? A történelem során erre a kérdésre szinte minden társadalomban egyértelmű „nem” válasz volt adható. A válasz indoklása az adott **társadalom** folyamataiban található meg.

Amikor egy **döntés** megszületik, amikor egy tervet körvonalaznak, az embernek az a célja, hogy az adott problémára olyan választ adjon a jelenben, melynek helyessége, megfelelősége bebizonyosodik a jövőben, más szóval helyesen döntsön. Ehhez megfelelő információra van szükség. Amikor olyan döntés születik, melyre adott válasz a múltból már ismert, de a döntés pillanatában ez az ismert kimenet, következmény az adott döntéshozó információs terébe még nem került be, akkor az „információhiányos döntés” vagy esetleg a „nem megfelelő döntés” fogalma jelenik meg a kommunikációban. Ha ellenben a döntés előkészítése már sokadjára a sokadik információ begyűjtését jelenti, akkor „döntésképtelenség” jelenik meg a folyamatokban.



2. ábra: Információ és döntés

Nehéz pontosan számszerűsíteni azt, hogy egy helyes döntéshez mekkora mértékű információra van szükség, azaz mekkora bizonytalanságot kell megszüntetni ahhoz, hogy egy döntést helyesnek lehessen ítélni. A megítéléshez azonban mindig szükséges egy kis idő, vagyis a döntés következményeinek megvizsgálhatósága.

A társadalmi forma meghatározza azokat a folyamatokat, melyeket eredményesen lehet folytatni egy adott társadalomban, igaz ez a működtetett rendszerek **bonyolultsági** szintjére is. Kötetlenebb információáramlást biztosító társadalmak magasabb bonyolultságú rendszereket képesek működtetni. Elmondhatjuk, hogy számos országban elkezdődött az információs

társadalom kiépítése, ahol az információ termelése és fogyasztása kiemelt jelentőségű feladattá – sok esetben állami monopóliummá – vált. A továbbiakban néhány gondolatot járunk körül az információs társadalomról, a téma rendszerezett ismertetése nélkül. A fő cél az, hogy az információ és az információs társadalom kapcsolata megfoghatóvá váljon.

Az információs társadalom kezdeteinek meghatározására a szakirodalom a Japán Számítógép-alkalmazások Fejlesztési Intézete által 1972-ben kidolgozott, „Az információs társadalom terve – nemzeti cél a 2000. év felé közeledve” című tanulmányát említi meg, mint legfontosabb forrást. A tanulmány célja az volt, hogy modellként szolgáljon a japán **információs társadalom** megvalósításához.

A **modell** részeit az alábbiakban írták le (az egyes pontok részletes ismertetése nélkül felsorolva):

1. közigazgatás adatbank,
2. számítógépesített város,
3. körzeti távvezérelt orvosi rendszer,
4. számítógép-központú oktatás egy kísérleti iskolai körzetben,
5. egy nagy kiterjedésű körzet környezetvédelmi rendszere,
6. tanácsadó testület (think-tank center),
7. vezetési információs rendszer bevezetése a kisvállalatoknál,
8. munkaerő-átképző központ,
9. számítógépes béketestület.

Ehhez hasonló projektek indultak el Kanadában (TELIDON – videotextrendszer) – és Svédországban is (TERESE – társadalmi jólét kialakítása, fenntartása az információ elosztásán keresztül) az 1970–80-as években. A mai magyar társadalomban is fellelhetőek a fent felsoroltak közül részelemek, tehát joggal nevezhetjük napjaink magyarországi társadalmát legalább részben információs társadalomnak, vagy még pontosabban, átmenetben lévő információs társadalomnak.

Az információs társadalom koncepciója a következő **két feltételezésre** épült:

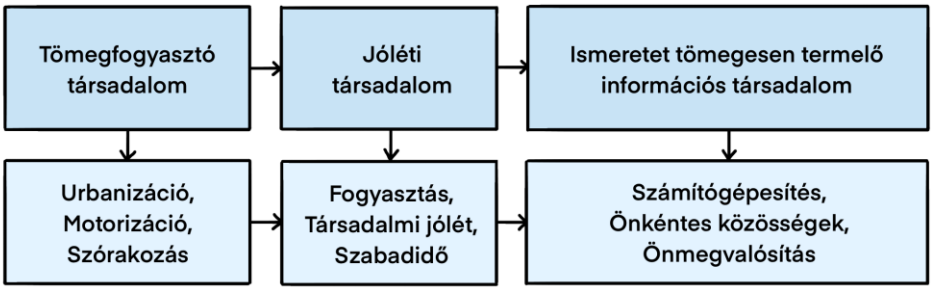
1. Az új típusú emberi társadalom teljes mértékben **különbözik** az ipari társadalomtól, mert hajtóereje az információs javak termelése, nem pedig az anyagiaké. Korábban az innovációk csak akkor voltak életképesek, ha az anyagi termelőerőre jelentett pozitív hatásuk kimutatható és alátámasztható volt, míg az innováció az információs társadalomban új keretben jelenik meg, annak alapvető természetét meghatározó számítógépes kommunikációs technikák rendszerén keresztül, elszakadva az anyagi termelőerőtől.
2. Az ipari társadalom fejlődése az a társadalmi modell, amelyből **megjósolható** az információs társadalom átfogó felépítése.

Az információs társadalomban a nemzeti cél az összjólét helyett az összelégedettség. Az információs piac hátterében a problémamegoldási lehetőségek bővülése áll, szemben az anyagi javak felhalmozásával. Filozófiai különbségek is felfedezhetőek a két társadalmi berendezkedés között: az ipari társadalom szellemiségét a reneszánsz testvéri szeretet jellem-

zi, míg az információs társadalom szellemisége a globalizáció: az ember és természet harmonikus együttélése, etikailag szigorú önfegyelem és társadalmi közreműködés jellemzi.

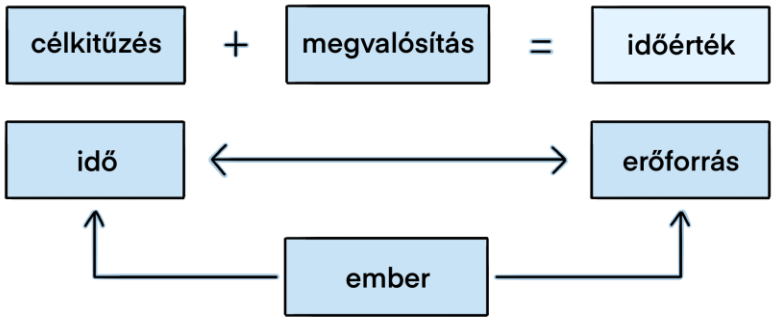
Egy ipari társadalom akkor alakul át teljes mértékben információs társadalommá, ha az adott társadalomban megvalósul az, hogy nincs környezetszennyezés, szimbiózisban él a természettel, erőforrás-takarékosság jellemzi, globális információs hálózata van, a termelés közös, a felhasználás megosztott. Ezek a célkitűzések nagyon magas szintűek.

Az átalakulás fázisait az alábbi ábra szemlélteti:



3. ábra: A társadalmi átalakulások

Az információs társadalomban az anyagi értékek helyébe az **időérték** lép. Időérték az, amit az eljövendő idő alatt az ember az erőforrások céltudatos felhasználása révén hoz létre. Az időérték helyettesíti a hagyományos anyagi értéket, vagyis az anyagi javak helyébe az időérték lép. A szabadidő fogalma is megváltozik – kibővül, nemcsak a szórakozásra fordított időt kell ez alatt a továbbiakban érteni, hanem azt az időt nevezi az információs társadalom szabadidőnek, amivel az egyén szabadon rendelkezik (pl. szórakozásra, önképzésre, öntevékenységre, pihenésre fordított idő).



4. ábra: Az időérték előállítási folyamata

Az időérték szerkezete ennek megfelelően hármas struktúrát vesz fel:

1. alany,
2. információs cél,
3. folyamat.

A gazdasági-társadalmi folyamatok szereplői számára az információ más-más szerepet tölt be, és máshol helyezkedhet el az információs célrendszerben. Különösen igaz ez az állami, a piaci és a privát szektor információhoz való hozzáállását elemezve. Ez legjobban a védendő információk bizalmasságában követhető nyomon. A legkevésbé védett, azaz a legkiszol-

gáltatottabb helyzetben a civil szereplők vannak, és a legnagyobb hegemóniával az állami szektor rendelkezik. A magánszektor a piac változásainak követésére szakosodik, kevésbé fókuszálva a társadalmilag fontos, de nem jövedelmező feladatokra, információkra. Az információs kiszolgáltatottság oktatással csökkenthető.

Az információs társadalomban az **oktatási rendszer**nek is meg kell változnia, az egyén sokkal hangsúlyosabb elemévé válik az oktatásnak, de mindezt annak kell alárendelni, hogy az egyén a társadalomban történő önmegvalósításához kapja meg a megfelelő eszközöket.

Ennek érdekében az oktatásban az információs társadalom azt preferálja, hogy az oktatás kiemelése történjen meg a formális iskolai kötöttségek közül, legyen bevezetve a személyes jellegű oktatás és az egyéni tanulás rendszere, jöjjenek létre a tudást teremtő oktatások, illetve egész életen át tartó oktatás valósuljon meg.

Az ezredfordulóig a graduális iskolák oktatás alatt az információk kiválasztását és átadását értették, kevés tekintettel arra, hogy a diákok milyen információs térrel rendelkeznek, tömegképzést valósítottak meg, tehetséggondozással együtt. Ennek a helyzetnek az információs csatornák növekedése vetett véget, mert ma már a diákoknak nem az iskola az elsődleges **információforrása**, hanem – sok esetben – az internet. Ma már sokkal több információhoz lehet a digitális világban hozzáférni. A digitális világ információmennyisége az ezredforduló után az első évtizedben exabájtban volt mérhető, ez a második évtizedre zettabájtos méreteket öltött. Ezek nagyon nagy számok, hiszen 1 zettabájt 10^{21} bájtnak felel meg. Összehasonlításképpen 2021 áprilisában a legnagyobb kapacitású háttértároló, amit lehetett kapni, 100 terrabájtos volt (100 x 10^{12} bájt).

Az adatok tárolása tehát nem kérdéses, de az információtartalma, hitelessége, pontossága sok esetben megkérdőjelezhető, erre egyre több példát láthatunk-hallhatunk a mindennapi életben is (pl. fake news, álhírek). A nem hiteles információ hitelesként történő fogyasztása zavarokat okozhat a döntési rendszerekben, és veszélyeztetheti az adott alany információs céljainak elérését is, végeredményben az időértéket csökkenti. Különösen fontos ez a dezinformációs időszakokban.

Emiatt az iskolák oktatási stratégiája is megváltozott az információs társadalomban, hozzáidomult a társadalmi folyamatokhoz és elvárásokhoz, és célkitűzésének megfelelően képessé teszi a diákokat a tudatos információfogyasztásra, -kezelésre és -feldolgozásra azért, hogy a jövő társadalmában a megfelelő döntéseket a megfelelő információk birtokában legyenek képesek meghozni – más szóval, hogy a megfelelő időértékek születhessenek meg, az adott **pillanatban** és az adott **pillanatra** egyaránt.

Gyakorló kérdések:

1. Melyek az információs társadalom legfőbb jellemzői?
2. Mi az időérték és milyen a szerkezete?
3. Hogyan változik az oktatás az információs társadalomban?
4. Hol és mikor jött létre az információs társadalom fogalma?

2.1.3 Információforrások a digitális univerzumban

„Az ismereteinket tartalmazó könyvek természetéről széles körben elterjedt egy helytelen felfogás. Úgy vélik, hogy ezek a könyvek olyanok, amelyeknek tartalmát a fejünkbe kell préselni. Azt gondolom, ennek az ellenkezője közelebb áll az igazsághoz. A könyvek azért vannak, hogy megtartsák magukban a tudást, mialatt mi a fejünket valami jobbra használjuk. Az ismeretanyag számára a könyv biztosabb otthont is nyújt.” (Szent-Györgyi Albert: Az élet jellege, 1973.)

Az ismeretek lassan gyarapodtak évezredeken keresztül, lassan változtak ennek megfelelően a termelési eszközök, eljárások, módszerek. Egy ember élete folyamán a változás olyan kicsi volt, hogy alig lehetett észre venni. Bármilyen mesterséget folytatott valaki, fiatalkorától öregkoráig megélhetett a tanulóévei alatt elsajátított tudásból.

Újítások, találmányok, felfedezések mindig születtek, de lassan terjedtek el. Példa erre, hogy hiába készítette el Fulton a gőzhajóját, sok tengerész kortársa vitorlás hajón tanult meg hajózni, és ott is fejezte be pályafutását. Az autó megjelenése után is a lovaskocsik még nagyon sokáig fennmaradtak, és még ma is léteznek. És mind a mai napig vannak olyanok, akik nem tanultak meg például autót vezetni. Ez a példa azonban nincs teljesen összhangban a műszaki információ terjedésével, de van hasonlóság benne.

A tudósoknak, kutatóknak korábban nem okozott nehézséget lépést tartani a tudományáguk fejlődésével, mivel a tudás megszerzése érdekében alig néhány folyóiratot és könyvet kellett elolvasniuk, és ez alig-alig csökkentette a kutatásra fordított idejét. A tudományos-műszaki forradalom azonban felforgatta ezt a kényelmes rendet. Az új ismeretek gyorsan szaporodnak és avulnak, és az innovációkkal szemben is alapvető követelmény, hogy rövid idő alatt alkalmazhatóak legyenek. Az iparban napjainkban alkalmazott eljárások, előállított termékek jelentős hányadát pár évvel korábban még nem is ismerték.

Ma már senki sem számíthat arra, hogy az iskolában elsajátított ismeretek élete végéig biztosítják a megélhetését. Az is előfordulhat – és már elő is fordult többször, hogy valakinek a tanult szakmája gyakorlatilag eltűnik vagy jelentős mértékben átalakul (pl. vájár, textilszövő, gőzmozdony-vezető). Az elektronikai ipar ötven év alatt jutott el a jelfogóktól és a ferritmemóriáktól – jelentős műszaki átalakulásokon keresztül – a nanotechnológiával gyártott félvezető tranzisztorlapkákig és a nagy kapacitású állandó memóriákig.

A mai, gyorsan változó világban az ember társadalomban elfoglalt helyének megőrzéséhez az aktuális információkhoz való hozzájutás és ennek megfelelő értelmezése szükséges. Az információ megőrzésénél leírtak szerint az értelmezéshez szükséges ismeretek is információk, tehát gyakorlatilag csak egyetlen eszközre van szükség a társadalmi pozíció megőrzéséhez, az információs folyamat eredményeként az időérték előállításához, a termelési folyamatok fenntartásához: **aktuális, pontos és hiteles információra**. A gyakorlatban mindegy, hogy ez az információ papíralapon vagy elektronikusan van-e jelen. Az emberiség információtermelési kapacitása viszont ma úgy oszlik meg, hogy csupán néhány ezrelék körül van a nyomtatott információ mennyisége a digitálissal szemben, és sokak kimondott célja, hogy a papíralapú információk digitalizálását a lehető leghamarabb és a lehető legnagyobb mértékben megvalósítsák (erre példák a digitális könyvtárak, Google book, digitalizált szabványtárak létrejötte és terjedelmük növekedése).

Az emberiség által termelt információmennyiség gyarapodásának és az egyes szakmák bonyolultságának másik következménye az, hogy ma már egyetlen ember sem képes a szak-

mája műveléséhez szükséges információmennyiséget fejben tartani, de ez nem is szükséges. Az is gyakran problémát okoz, hogy a szakmai változásokkal való lépéstartást, a szakma fejlődésének egyéni követését hogyan tudják megoldani a szakterületek véges olvasási kapacitással rendelkező művelői. Erre azért is szükség van, mert a megtanult adatok nagy része néhány év alatt elavul, és az aktualizálás olykor létfontosságú lehet a folyamat szereplői számára.

Ma már nem lehetséges minden szükséges információt fejben tartani. Éppen ezért nagyon fontos kérdéssé válik az, hogy hogyan lehet az éppen szükséges szakmai információkhoz hozzáférni. Ehhez az emberi agynál megbízhatóbb tárolóeszköz és azoknak a módszereknek az ismerete szükséges, melyek segítségével a digitálisan tárolt információk előhívhatóak és felhasználhatóak a szakember számára az adott szituációban.

2.1.3.1 Digitális információforrások

A papíralapú információkhoz való hozzáférés korlátozott és véges, egy időben csak annyian tudják olvasni, ahány példányban rendelkezésre áll a világban az adott forrás. Az új források megjelenésekor pedig számottevő időnek kell eltelnie, míg az összes könyvtárba eljut az új irodalom, még a repülőgépek korában is. A digitális információforrásoknak nincsenek ilyen korlátjai, amennyiben a hozzáférés elektronikusan engedélyezett, azt bárhol és szinte bármennyien képesek olvasni az egyetlen digitális példány valós idejű sokszorosításával, és azok ideiglenes vagy tartós időtartamú helyi másolatának képzésével.

A digitális univerzumban az információ forrásait tehát azok az eszközök jelentik, amelyek digitális formában tárolt adatokat tartalmaznak, vagy digitális formában leírható és megjeleníthető jellemzőkkel rendelkeznek. A digitális világban az **információ begyűjtése** során az alábbiak egyike fog bekövetkezni:

1. elektronikus levél elolvasása,
2. hírportálok híreinek megtekintése,
3. internetes oldal célzott meglátogatása,
4. helyben tárolt fájlok megnyitása,
5. elektronikus könyvtárban tárolt dokumentum (könyv, folyóirat stb.) olvasása,
6. vállalati adatbázis használata,
7. kereső- vagy gyűjtőoldalak eredményeinek felhasználása,
8. távoli eszközökön, szolgáltatókon (felhőben) tárolt fájlok letöltése, vagy
9. valós idejű digitális kommunikáció másokkal (csevegés, telefonálás).

Tekintettel arra, hogy a digitális adatok mennyisége – a becslések szerint – több tízezerszerese a nem digitális adatok mennyiségének, a digitális források hitelességének megállapítása és fenntartása alapvető fontosságú az információ felhasználhatóságára nézve. Kiragadva és megvizsgálva a keresést, mint az egyik legnépszerűbb internetes szolgáltatások egyikét, alapvető tény, hogy a különböző keresők nyilvánvaló módon nem birtokolhatják az internet összes adatának (weboldal, fájl, flashanimáció) az indextábláját – a dinamikus tartalomelőállítások miatt ez nem is lehetséges, hanem a teljes halmazból egy adott, de egyre bővülő részhalmazzal dolgoznak. Különböző eredményeknek kell megszületni ugyanarra a keresési kérdésre akkor, ha az egyik kereső például 151 millió oldallal, másik 31 millió oldallal dolgo-

zik, míg a harmadik képes keresni e-mailekben is – nyilván csak azokon a helyeken, amit elér. Ebből következik, hogy fontos lehet a keresők közötti különbségeket ismerni az általuk szolgáltatott eredmények megbízhatóságának megítélésében. Attól függően lesz egy kereső „jó” vagy „rossz”, hogy az általa birtokolt információkból először is tud-e választ adni a feltett keresési kérdésünkre, másodszor a válasz minősége mennyire megfelelő, harmadszor a megfelelő válaszok mennyire vannak elöl a találati listában – a kérdések feltevésének bonyolultságán vagy egyszerűségén túlmenően. A keresőmotorok működése legtöbbször az internet pásztázásán és a legsikeresebb esetekben ezen túl az egyes oldalakra mutató hivatkozások elemzésén is alapul, így adva vissza egy olyan eredményt, ami a felhasználó számára a leginkább megfelelő lehet. Fontos megállapítás, hogy az interneten a csak lexikális (szövegszerű) szempontból történő keresés nem hozott értékelhető eredményt a felhasználók többsége számára, mert a keresett információt a rendszerek egy olyan nehezen áttekinthető struktúrájú adathalmazban adták vissza, mely feldolgozása meghaladta az egyes felhasználók időbeli lehetőségeit, még a megfelelő pontossággal megfogalmazott kérdések esetében is.

A digitális források elérhetőségét és változatlanságát sok esetben nem garantálja a szolgáltató, így, ha korábban felhasználtak egy adott forrás által szolgáltatott adatot, nem biztos, hogy az adat egy későbbi időpontban is rendelkezésre áll, vagy nem fog megváltozni – valamilyen okból, célszerű tehát a felhasznált digitális forrásanyag hitelességét legalább a felhasználói oldalon biztosítani (ezt töltöttük le). Emiatt – és az internet történeti kutathatóságának megteremtése miatt – kezdték el például az internet archiválása projektet, ami azt a célt tűzte ki maga elé, hogy bizonyos időközönként az általa elérhető internetet végigpásztázza, az oldalakat begyűjti – azaz lemásolja, és hosszú távon archiválja.

Digitális információforrások:

1. elektronikus könyvtárak és használatuk,
2. fizikai könyvtárak elektronikus katalógusai és használatuk,
3. internetes hírügynökségek adatbázisai és keresés bennük,
4. konferencia-honlapok és a publikációk közötti keresés,
5. vállalati honlapok és hozzáférhető dokumentumtárak és ezekben való keresés,
6. internetes keresők elérése, keresési kérdések megfogalmazása, válaszok értelmezése.

Példák ilyen forrásokra, a Magyar Elektronikus Könyvtár, az Országos Széchényi Könyvtár honlapja és katalógus-adatbázisai, a Magyar Távirati Iroda online hírkeresője, a Networkshop konferenciaoldala és cikkei, a Microsoft terméktámogató oldalai, a Symantec és a Cisco nyilvános publikációi, végül a Google és a Google Scholar keresők, vagy a tudományos adatkeresők és eredményközlők zárják a példák távolról sem teljes körű felsorolását.

Ekkora információmennyiségnél egyre fontosabb kérdésként merül fel a hitelesség. Nyilvánvaló módon a hitelesebb információk felhasználása célszerűbb, míg a nem hiteles információkról ki kell derülnie rövid időn belül, hogy nem hitelesek (például ilyen eszköz a **hoax**[1] adatbázis). Előfordul, hogy nem hiteles információt a tömegtájékoztatás is átvesz, és azt továbbítja.

[1] A hoax szó jelentése: „beugratás”, „megtévesztés”, „átverés”, „álhír” vagy „kacsa”.

Gyakorló kérdések:

1. Mi a digitális és nem digitális információmennyiség növekedésének hatása az egyén szakmai fejlődésére?
2. Melyek a digitális információforrások?
3. Mely források használhatók az álhírek kiszűrésére?

2.2 Hiteles és nem hiteles információ

Az elektronikus aláírás intézményét az elektronikusan tárolt és továbbított adatok eszmei, de materiálisra is átváltható értékének növekedése és a papíralapú aláírás elektronikus konverziójának – más szóval a hiteles kötelezettségvállalások elektronikus dokumentálásának – igénye termelte ki. Csak az veszi komolyan és képes tudatosan használni az elektronikus aláírást, aki tudatában van az adatok értékének és annak, hogy az értékes dolgokat védeni kell. A védelem azonban nem feltétlenül egyenlő a titkokban tartással – erre az aláírás nem is alkalmas, de kétségkívül annak egyik eleme lehet. Nyilvános adatok védelme is megvalósul a digitális univerzumban a honlapok tartalmának védetté nyilvánításával, anélkül, hogy az olvashatóságát korlátoznák.

A hagyományos aláírás akkor terjedt el, amikor a polgárosodás elérte azt a fokot, hogy gyakran kellett értéket képviselő dokumentumot jogi szempontból hitelesíteni, a kötelezettségek vállalásának tényét bíróság előtt érvényesíteni. A honlapok hitelességének biztosítása is egy bizonyos érték, a megbízható információ szolgáltatójának járó jó hírnév eszmei értékének védelmét jelenti.

Az elektronikus aláírás akkor kezdett elterjedni, amikor egyrészről az elektronikus dokumentumok papíralapra konvertálása már mennyiségi problémát jelentettek, másrészről az elektronikus dokumentumban foglalt kötelezettségek hiteles igazolásának igénye (ki nyilatkozott, mit nyilatkozott és mikor nyilatkozott) felmerült az érintett felek között. Mindezekből adódik, hogy értelmes és érdemes megkülönböztetni a hiteles információt a nem hiteles információktól.

2.2.1 A biztonsági követelmények és a hitelesség

Az információs célkitűzések elérése, az információs folyamatok megfelelő végrehajtása érdekében is – mint az üzleti célkitűzések során – az információknak ki kell elégíteniük bizonyos követelményeket, amelyeket információkra vonatkozó üzleti követelményeknek is nevezhetünk. A szakirodalom a szélesebb körű **minőségi**, pénzügyi-**megbízhatósági**, és **biztonsági** követelmények alapján az alábbi hét megkülönböztethető, egymást néhol minden bizonnyal átfedő információkritériumot határoz:

- **hatékonyság:** arra vonatkozik, hogy az információkat az erőforrások optimális (legtermékenyebb és leggazdaságosabb) kihasználásával biztosítsák,
- **hatásosság/eredményesség:** azzal foglalkozik, hogy az információk a folyamat szempontjából jelentőséggel bírnak, és hogy az információkat időben, helyes, ellentmondásmentes és használható módon biztosítják,
- **megfelelőség:** a folyamatokat érintő előírások, törvények, jogszabályok, szabályozások és szerződéses megállapodások – azaz kívülről előírt jogi, üzleti és egyéb köve-

telmények, illetve belső irányelvek – betartását jelenti, amelyeknek a folyamat a tárgyát képezi,

- **megbízhatóság:** a vezetés számára olyan időszerű és pontos információk biztosítása, amelyek a folyamat működtetéséhez, pénzügyi megbízhatóságához és irányításához szükségesek,
- **bizalmasság:** arra vonatkozik, hogy megakadályozza a bizalmas információk engedély nélküli megismerését, vagyis fontos információkhoz illetéktelenek ne férjenek hozzá,
- **sértetlenség:** az információknak a mikrokörnyezeti (szervezeti) értékek és elvárások szerinti pontosságára, általános értelemben vett változatlanságára és teljességére, valamint az információk érvényességére és hitelességére vonatkozik,
- **rendelkezésre állás:** azzal foglalkozik, hogy az információk akkor álljanak rendelkezésre, amikor azokra a folyamatnak szüksége van most és a jövőben is, továbbá a szükséges erőforrások és az erőforrások szolgáltatási képességeinek védelmére is vonatkozik. Nem terjed ki a szolgáltatások megbízhatóságára, azaz amikor a szolgáltatást nyújtó eszközök működnek, de a végeredmény nem az elvárt.

Az információkritériumok közül csak az utolsó három a **biztonsági követelmény** (bizalmasság, sértetlenség, rendelkezésre állás). A biztonságon belül a **hitelesség** kialakításával a sértetlenség foglalkozik. Egyes szakmai megközelítések a hitelességet és a letagadhatatlanságot kiemelik a klasszikus biztonsági követelményekből, és ezáltal ezeket hangsúlyosabban és részletesebben tárgyalják, ami ezek fontosságára irányítja rá a figyelmünket. Akkor veszíti el egy adott információ a hitelességét, ha vagy a forrás megbízhatatlansága kiderül, vagy a hitelesség ellenőrzését nem lehetséges elvégezni, illetőleg az ellenőrzés hamis eredményt ad. Nem megfelelő, ha az információ egy korábbi ellenőrzés eredményét automatikusan megőrzi, mert lehetséges, hogy az időközben lényeges módosuláson ment át, és ezt csak a hitelességének megismételt ellenőrzése képes feltárni. Ilyenkor az eredeti állapotot csak akkor lehetséges visszaállítani, ha létezik az információ korábbi, hiteles változata.

A biztonsággal kapcsolatos internetes alapszabály az, hogy amikor valaki rákapcsolódott az internetre, akkor az internet is rákapcsolódott a gépére, vagyis a kapcsolat nem egyirányú, bármennyire is annak látszik, vagy hiszik. A kapcsolódás nem tesz különbséget alapesetben a személyes eszközök, adatok vagy védendő információk tekintetében, a kommunikációs csatorna létrejöttével az átvitel minden információ számára biztosított. Az internet fejlődésével és elterjedésével, illetve az internet segítségével történő vagyoni értékszerzés növekedésével egyre nagyobb valószínűséggel jelennek meg káros tartalmak, rosszindulatú programok, melyek fenyegetik a kapcsolódó eszközök és az adatok illegális felhasználásán keresztül a felhasználók biztonságát. A biztonságnak olyan, a felhasználó számára kedvező állapotnak kell lennie, amelynek megváltozása nem valószínű, de nem is lehet kizárni. Ebből következik, hogy ennek a kedvező állapotnak a megléte nem automatikus, annak fennmaradási valószínűségét csak tudatos **intézkedésekkel** lehet biztosítani. Ugyanis bármikor megjelenhetnek olyan fenyegetések, melyek ellen a még nincs kialakítva a védelem.

Biztonság a gyűjtőneve minden olyan intézkedésnek, amely megteremti az adatok, számítógépek, alkalmazói programok bizalmasságát az adatok korlátozott megismerhetőségén és az eszközök korlátozott elérhetőségén keresztül, majd sértetlenségét – a jogosulatlan változtatásokat kizárva, illetve észlelve, és végül a rendelkezésre állását, vagyis az eszköz akkor és ott működjön, amikor szükségünk van rá.

Az alábbi táblázatban található néhány, az internetezés közben előforduló, biztonság elleni fenyegetés, típusok szerint:

Bizalmasság	Sértetlenség	Rendelkezésre állás
Adatlopási kísérletek: – gépbetörés adatszerzés miatt – megtévesztéssel kicsalt adatok e-mailben: – hamis weboldal segítségével kicsalt adatok (leggyakrabban felhasználói azonosítók és jelszavak, de minden személyes adat halászata is ide tartozik)	A sértetlenség ellen irányuló tevékenység megjelenési formája lehet: – a jelszófájlok megváltoztatása jogosulatlan felhasználó hozzáadása céljából, vagy – már létező program vagy nyilatkozat megmódosítása a támadó szándéka szerinti működés céljából, továbbá – a gépben tárolt internetes címek átírása is előfordulhat, hogy az igazi weboldal helyett egy nem hiteles áloldalra látogasson a felhasználó	A támadási formák leggyakrabban: – vírus települése a számítógépre, mely a működést előbb-utóbb lehetetlenné teszi, ritkábban: – az internetkapcsolat „elárasztása”, aminek következtében az internet-hozzáférés lelassul vagy megszűnik – vagy az otthoni internet-előfizetés jogosulatlan használata az utcáról vagy a világ másik részéről (botnet részeként)

2. táblázat: Fenyegetések hatása a biztonságra

Az aktuális fenyegetésekről pontos információkat szolgáltatnak azok a felmérések, melyeket a szakértő cégek időről időre közzétesznek (pl. Symantec Threat Landscape, ’Biztonsági tájkép’). Ezzel kapcsolatban talán ma a leglényegesebb megállapítás az, hogy a leggyakoribb támadási formák szerint a támadások a felhasználók aktív, de nem tudatos közreműködésével (valamilyen tartalom letöltése vagy megnézése közben a háttérben) következnek be a megtámadott gépeken, és a nagyon sokszor zsarolóprogramokhoz vezetnek.

Ez ellen a felhasználói tevékenységek tudatosabbá válásával – a nem hiteles források információinak elutasításával vagy óvatos felhasználásával – lehet védekezni, ez az egyik alapja a jövő megfelelő kiberbiztonságának.

Gyakorló kérdések:

1. Melyek a biztonsági követelmények?
2. Melyik biztonsági követelmény foglalja magában a hitelességet?
3. Mikor válhat egy korábban hiteles információ nem hitelessé?

2.2.2 A hitelesség fogalomrendszere

A hitelesség fogalmának tárgyalásához alapvető fontosságú annak megértése, hogy mi a különbség a hitelesség, a hitelesítés és aközött, hogy valami hiteles. Ennek bemutatásához a számítógépes bejelentkezési folyamat szolgáljon példaként, hiszen a hétköznapokban a felhasználók hitelesítéseként a legtöbbször a felhasználói nevet és a hozzá tartozó jelszót kell megadni. . A teljes bejelentkezési folyamat ilyenkor az alábbiak szerint működik:

1. lépés: **azonosítás** (identification) – a rendszer használatához meg kell adni azt az azonosító jelet, felhasználói nevet, ami alapján a rendszer a továbbiakban azonosítani tudja az adott felhasználói fiókot, vagyis ami alapján elvégezhető egy személy (vagy más entitás) állított azonosságának megállapítása. Ennek előfeltétele, hogy a rendszerben létezzen ilyen fiók, tehát a megfelelő szabályok szerint az arra feljogosított tisztviselő (vagy a rendszer saját maga) korábban hozza létre az adott felhasználói fiókot (azaz a regisztráció megtörténjen),
2. lépés: **hitelesítés** (authentication) – az adott felhasználói fiók használatát a rendszer csak akkor engedélyezi, ha az azt használni szándékozó megadja a felhasználói névhez tarto-

zó helyes jelszót – vagy többfaktoros hitelesítés esetén egy eszközt vagy egy egyszeri kódot is, ezzel erősíti meg azt az állítását, hogy a megadott felhasználó fiók az övé,

3. lépés: **feljogosítás** (authorization) – a rendszer a hitelesített felhasználói fiókhoz tartozó erőforrásokat (processzor, tárhely, memória, egyéb eszközök – pl. CD-olvasó, USB-port) hozzárendeli a fiókhoz és használatra előkészíti őket, azaz engedélyezi az erőforrások igénybevételét a felhasználó számára.

Ezt a bejelentkezési folyamatot végigjárva lesz képes a felhasználó egy adott felhasználói fiók erőforrásainak segítségével bármilyen számítógépes tevékenység végrehajtására. A lépések során csak a második lépésben történik meg a felhasználó hitelességének a megállapítása, vagyis a hitelesítés.

A **hitelesség** a definíció szerint azt jelenti, hogy valaminek a forrása az, amit megjelöltek, és a tartalma az eredeti, míg a **hitelesítés** alatt az állított azonosság megerősítését kell érteni. Ennek megfelelően, az a megállapítás, hogy valami **hiteles**, azt jelenti, hogy a kibocsátónak állított forrás azonosságának ellenőrzése megtörtént, és a kibocsátott üzenet tartalmának eredetisége megerősítetté vált. A számítógépes bejelentkezési példára vetítve ez azt jelenti, hogy a felhasználó a hitelességét úgy tudja előállítani, hogy sikeres hitelesítési eljárásokon keresztül teszi hitelessé az általa ismert és a rendszer által elfogadott adatokkal a felhasználói fiókját.

Az elektronikus folyamatokban – hasonlóan a mindennapi élethez – az alábbiakról lehetséges **azonosságot állítani**:

- **személy:** ez a személy, akinek a neve X. Y., vagy felhasználói neve x. y.,
- **eszköz:** ez az eszköz a www.xy.hu nevű webszerver, ami az X. Y. cég birtokában vagy felügyelete alatt van,
- **tulajdonság:** ez az X. Y. a Z. cég ügyvezető igazgatójaként jogosult aláírásra.

Könnyen belátható, hogy a felhasználói név ismerete önmagában nem elégséges a hitelesség megállapításához, hiszen ezt az adatot sokan ismerhetik. A második lépésben szükséges helyes jelszót azonban már – normál esetben – sokkal kevesebben ismerhetik, egyénhez tartozó felhasználói fiókok esetében pedig csak az adott személy ismerheti. Természetesen az idő múlásával és a jelszó felhasználásának gyakoriságával arányosan fennáll a jelszó kompromittálódásának, más általi megismerhetőségének veszélye, de ezen a jelszó időnkénti biztonságos megváltoztatása segíthet.

Ha ismer valaki egy felhasználói nevet, és tudja hozzá a megfelelő jelszót, a használathoz ez még nem elegendő. Az is szükséges, hogy a – az operációs rendszer hozzáférés-védelmét kikényszerítő és felügyelő – bizalmas számítástechnikai bázis az előre rögzített szabályok mentén a fiókhoz hozzárendelje a használható számítástechnikai erőforrásokat (alkalmazások, rendszerprogramok, csatlakoztatott eszközök stb.). Más szóval, a felhasználói fiókoknak az erőforrások használatára történő feljogosításának meg kell valósulnia – de ez azonban automatikusan, és a felhasználó elől rejtetten történik.

Az azonosítás, a hitelesítés és a feljogosítás három lépésének mindegyike szükséges egy védett számítógépes rendszer erőforrásaihoz való hiteles hozzáférés megvalósítása esetén. A hitelesítés – láthatóan – nem az elsődleges eleme a bejelentkezésnek, de nélkülözhetetlen az ellenőrzött és számonkérhető erőforrás-használathoz.

A kibocsátó **forrás** eredetiségének megállapítása úgy történik, hogy a kibocsátó igazolja, elismeri az adott tartalom kibocsátását. Ez történhet kézi aláírással, amikor a kibocsátó és minden érintett fél az ellenkező bebizonyosodásáig elismeri a az aláírásra feljogosítottak körét, tekintve az általuk aláírtakat (ilyen például egy megbízólevél vagy egy jelszó közlése), és utólagos elismeréssel is, amikor utólagos vizsgálat során állítja ki a kibocsátást elismerő igazolást (ilyen például az APEH adótartozás-mentességi „nullás” igazolásának hitelesítési eljárása).

A kibocsátott **tartalom** eredetiségének igazolására a digitális aláírást vagy az üzenethitelesítő kódot alkalmazzák. Ezek olyan kriptográfiai eljárások, melyek segítségével egyrészről a tartalom sértetlensége bebizonyítható, másrészről azt a kibocsátó olyan módon végzi, mely a hozzá köthetőséget (eredetiséget) végig biztosítja. Az első eljárás során a tartalomból képzett egyedi kivonat megfelelő kriptográfiai titkosítását végzik el, míg a második eljárás alapjául a kriptográfiai titkosító kulcs birtoklásának megállapíthatósága (jogi vagy magán), személyhez köthetősége szolgál.

A **digitális aláírás** (digital signature, DS) – röviden – az aszimmetrikus kriptográfiai algoritmusokat használó elektronikus aláírás, amely az üzenet, az elektronikus dokumentum tartalma, és az aláírás készítőjének hitelesítésére szolgál. Lényeges tulajdonsága, hogy csak az aláíró birtokában lévő (titkos és bizalmas) adattal lehetséges aláírást készíteni, és az aláírást ellenőrizni bárki számára hozzáférhető nyilvános adattal lehet. A nyilvános adatból a titkosra nem lehet következtetést levonni. Az **üzenethitelesítő kód** (message authentication code, MAC) szimmetrikus kriptográfiai algoritmust alkalmazó elektronikus aláírás, amikor az üzenet ellenőrző összegét (MAC) vagy az üzenet és titok együttes kivonatát (hashed MAC, HMAC) rejtjelezik, azaz egy kriptográfiai ellenőrző összeget képeznek, és azt csatolják hitelesítés céljából az aláírandó adatokhoz. A szimmetrikus kriptográfiai algoritmusok alapvető tulajdonságából következik, hogy a letagadhatatlanság önmagában nem biztosítható vele, ugyanis a küldőnek és a fogadónak ugyanazt a kulcsot kell birtokolnia az üzenethez képezett hitelesítő kód elkészítéséhez és elolvasásához. Ezzel ellentétben az aszimmetrikus kriptográfiai algoritmusok során az aláírónak és a fogadónak különböző kulcsra van szüksége az aláírás készítéséhez és annak értelmezéséhez, így a *személy – titkos kulcs* közötti hozzárendelés kölcsönösen egyértelműen megvalósítható.

A hitelesség és a letagadhatatlanság szorosan összefüggő fogalmak. A letagadhatatlanság arra a kérdésre ad negatív választ, hogy képes-e az adott személyen kívül másvalaki is a sikeres hitelesítési eljárás végrehajtására. A letagadhatatlanság értelmezhető küldő és fogadó oldalon is. Ez a tulajdonság kritikus a kézi aláírások és a kézbesítések biztonságos elektronikus megfelelőjének kialakításakor.

A biztonsági intézkedéseket alkalmazhatjuk a hitelesítési eljárásokra is, az alábbiak szerint:

1. **megelőző** intézkedések: a hitelesség elvesztését megelőző intézkedések, amelyek egyrészről biztosítják a hitelesítési eljárásokhoz szükséges adatok rendelkezésre állását, másrészről megvédik az adott adatokat a jogosulatlan módosításoktól,
2. **feltáró**, detektáló intézkedések: biztosítják a hitelesség elvesztésének felismerését, a sértetlenség megszűnésének detektálásával a jogosulatlan módosítások felismerésével,
3. **javító** intézkedések: az eredeti hiteles állapot helyreállítására tett intézkedések összessége.

Fontos megállapítani, hogy a digitális aláírás önmagában **nem védi** meg az adatot a módosítástól, mivel csak hozzákapcsolódik vagy hozzákapcsolható, mint egy plusz információ. Ez nem akadályozza meg az adatok módosítását, ellenben az aláírás rendszeres ellenőrzése a hitelesség folyamatos fennállását igazolja. Az is nyilvánvaló, hogy az aláírás egy korábbi ellenőrzésének sikeres eredménye nem biztos, hogy igaz lesz most is, hiszen az aláírás korábbi megfelelőségéből az adat változatlansága még nem következik, csak ha az ismételt ellenőrzés is sikeres, akkor lehet hitelt érdemlő módon kijelenteni az adat sértetlenségét. Ezekre a hitelességet érintő intézkedések tervezésekor és üzemeltetésében tekintettel kell lenni.

Gyakorló kérdések:

1. Mi a különbség a „hitelesség”, a „hitelesítés” és a „valami hiteles” fogalmak jelentése között?
2. Mi a letagadhatatlanság lényege?
3. Alkalmas-e a digitális aláírás az utólagos módosítások megakadályozására?

2.2.3 A hiteles információ szükségessége

A biztonság alapvető szükséglet minden társadalomban és annak minden egyede számára. A biztonság és a hiteles információ szoros kapcsolatban van egymással. A kapcsolatot az egyén társadalmi pozíciójának stabilitása jelenti. A társadalmi rendszerek azok az eszközök, melyek a rendezettséget fenntartják az adott társadalomban.

A biztonság témakörébe tartozik az egyén társadalomban elfoglalt **pozíciójának** megőrzése is. Ehhez – az információs társadalomban – az aktuális információkhoz való hozzájutás és ennek megfelelő értelmezése alapvető fontosságú. Az értelmezéshez szükséges ismeretek is információk, tehát – megismételve a korábban már megtett egyik legfontosabb megállapítást – egyetlen eszközre van szükség a társadalmi pozíció megőrzéséhez: **aktuális, pontos és hiteles információra**. Ebben a megállapításban az is benne van, hogy az információk aktuálissága, pontossága és hitelessége megváltozhat azok életciklusa során – ez nyilvánvaló módon kihatással van a felhasználhatóságukra. Figyelemre méltó megállapítás ez, amely az információt, illetve annak birtoklását nem célként, hanem eszközként definiálja. A cél ekkor is az időérték hatékony és hatásos előállítása, a rendelkezésre álló eszközök, erőforrások segítségével, a társadalmilag hasznos követelmények (pl. környezetvédelem) mentén – ami nem feltétlenül egyezik meg az adott társadalomban hasznosnak vélt követelményekkel, a társadalmi berendezkedéstől az egyezőség vagy a különbözőség erősen függ.

Az információ hitelességét ellenőrizheti személy vagy gépi entitás is. Mindkét esetben meg lesznek vizsgálva az adott információk hitelességét igazoló bizonyítékok (forrás hitelessége és az adat hitelessége szempontjából), de az egyén elfogadásában vagy elutasításában kevésbé formális szempontok is szerepet játszhatnak („hitelesnek tűnik”, „nem hiszek az ellenőrzés eredményének”, „ha elutasítom, megakad a folyamat” stb.), így elképzelhető, hogy ugyanazon információ hitelességét eltérően fogja megítélni egy emberi és egy gépi intelligencia.

Az információs társadalom alapvető terméke az ismeret, ahol az ismereteket nagy tömegben számítógépes rendszerekben tárolják, továbbítják vagy dolgozzák fel további ismereteket előállítva. A számítógépes rendszerekben tárolt ismeretek, bináris adatok, programok, adatbázisok, alkalmazások hitelessége (eredete és teljessége) azonban nem automatikus, mivel

akár hiba, gondatlan vagy szándékos cselekedet eredményezheti a tárolt ismeretek jogosulatlan megváltozását. Ha az ismeret feltüntetett eredete vagy a tartalma – nem kívánt módon – megváltozik a rendszerben, és ha a rendszer üzemeltetője nem rendelkezik az ismeret korábbi hiteles példányával, vagy az ismeret pontosan egyező újra előállíthatósága nem biztosítható, ebben az esetben az adat, ismeret, információ részben vagy teljesen elveszettnek tekinthető mindhárom (gépi, emberi és reprezentációs) szinten. Ha a rendszer működtetője rendelkezik a sérült adat korábbi hiteles változatával, akkor annak egyszerű visszatöltésével az esemény javítható. Számítógépes rendszerben hitelességet biztosító intézkedések nélkül pedig a meglévő információ tartalma is megkérdőjelezhető, akár tömeges méretekben is, ami mindenképpen hátrányos lehet az információbirtokos egyén számára. A digitális világban tehát a hitelesség fontos tulajdonsága minden egyes adatnak, ismeretnek, információnak.

A hitelesség fogalomrendszerének tárgyalása azért fontos, mert a szó informatikai és a hétköznapi jelentése között eltérés áll fenn. Ha valakit vagy valamit hitelesnek tartunk a mindennapokban, ezzel valójában azt fejezzük ki, hogy szavahihető emberrel állunk szemben vagy azt a valamit igaznak gondoljuk. Információbiztonsági értelemben pedig a hitelesség azt jelenti, hogy az információ forrását bizonyítottan ismerjük, és a tartalom meg nem változása igazolttá vált előttünk. A kettő között átvitt értelemben van csak közös jellemvonás, mert ha valaki azt mondaná, hogy tegnap piros hó esett, akkor nem tartanánk szavahihetőnek, de ha igazolni tudjuk azt, hogy az a valaki volt az, aki tegnap pontosan ezt mondta, akkor ez a mondat hitelesnek számít információbiztonsági értelemben, függetlenül attól, hogy tegnap esett-e hó, és ha igen, milyen színű. Fontos tehát a hitelességet és az igazságértéket elválasztani egymástól a digitális világban. Az elektronikus hitelességnek ebből adódóan nem lehet a feladata az állítások igazságtartalmának vizsgálata vagy értékelése.

Gyakorló kérdések:

1. Mi jelenti a kapcsolatot az egyén társadalmi biztonsága és a hiteles információ között?
2. Lehet-e hiteles a nem hitelesített információ?
3. Mit jelent a hitelesség elvesztése, és mit lehet tenni ekkor?

3 Az elektronikus aláírás az európai információs társadalomban

3.1 Az elektronikus aláírás fogalmai

3.1.1 Az elektronikus aláírás fogalmának kialakulása

Az elektronikus aláírás kifejezés nem műszaki, hanem **jogi eredetű fogalom**. Az európai uniós elektronikus aláírási irányelv első, 1997-es tervezetében jelent meg. Ezt megelőzően – az 1970-es és az 1980-es években az elektronikus aláírás kifejezést a műszaki terminológiában lényegében nem használták, illetőleg digitalizált formában létező aláírást értettek rajta. Ekkor azonban még nem volt egyetlen egy működő gyakorlati megvalósítása sem az aláírásoknak, ezek elterjedése csak 1995-ben kezdődhetett meg, amikor Phil Zimmermann elkészítette és szabadon hozzáférhetővé tette az első Pretty Good Privacy (PGP) programcsomagot, amely az elektronikus levelek titkosítása mellett azok RSA-algoritmuson alapuló digitális aláírását is lehetővé tette. A program méltán vált az egész világon népszerűvé, hiszen jól megtervezett és egyszerűen megvalósított funkcionalitással rendelkezett.

A műszaki terminológiában a legelterjedtebb kifejezés a digitális aláírás elnevezés volt, emellett gyakran használták még a PKI (nyilvános kulcsú infrastruktúra) aláírás megnevezést is, amikor kifejezetten az ITU X.509-es ajánlásában meghatározott tanúsítványok használatán alapuló hitelesítési megoldásokra kívántak utalni. (Érdemes megjegyezni azt is, hogy sokan használták a digitális aláírás kifejezést az aláírásmintákat tartalmazó grafikus fájlok megjelölésére is. A témában nem túl jártas emberek gyakran ma is elsőként erre a megoldásra asszociálnak az elektronikus és digitális aláírás kifejezések hallatán.) Jogi megközelítésben a PKI aláírás kifejezés fogja jelölni a nyilvános kulcsú aláírásokat a továbbiakban.

3.1.1.1 Elektronikus aláírás szabályozásának a célja

Az uniós elektronikus aláírási irányelv megalkotói tudatosan választották a műszaki világ által használt kifejezésektől eltérő elektronikus aláírás megnevezést. Az új kifejezés használatának egyik oka az volt, hogy a szabályozás fogalomrendszere ne egy konkrét technológiai megoldásra utaljon, vagyis, hogy a jogi szabályozástechnológia semleges legyen.

Az új fogalom bevezetésének másik oka az volt, hogy a jogi szabályozás célját jobban szolgálta egy olyan elnevezés, amely nem rendelkezik határozott jelentéssel valamilyen más területen. Az elektronikus aláírás jogi szabályozására ugyanis azért volt szükség, hogy meghatározzák az elektronikus dokumentumok tekintetében a saját kezű aláírások szerepét betölteni képes megoldások és gyakorlatok körét. Az elektronikus aláírás jogi szabályozásának ugyanis nem egyes technológiák használatának a megtiltása vagy kötelezővé tétele a célja, hanem annak meghatározása, hogy milyen műszaki megoldások, milyen feltételek teljesülése esetén lesznek alkalmasak arra, hogy a papírdokumentumon elhelyezett saját kezű aláírással egyenértékű jogi hatást tulajdoníthassunk neki.

3.1.1.2 Az elektronikus aláírás fogalma és típusai

A szabályozási célkitűzésekkel összhangban az eIDAS[2] a következőképpen definiálta az **elektronikus aláírást**:

„olyan elektronikus adat, amelyet más elektronikus adatokhoz csatolnak, illetve logikailag hozzárendelnek, és amelyet az aláíró aláírásra használ”.

A definíció rendkívül tágan határozza meg az elektronikus aláírások körét. A rendelet szerint éppúgy elektronikus aláírásnak minősül egy e-mail végén elhelyezett szöveges aláírás vagy egy dokumentum végére beillesztett beszkennelt kézi aláírás képe, mint egy elektronikus dokumentum nyilvános kulcsú titkosítással kódolt lenyomata (PKI aláírás).

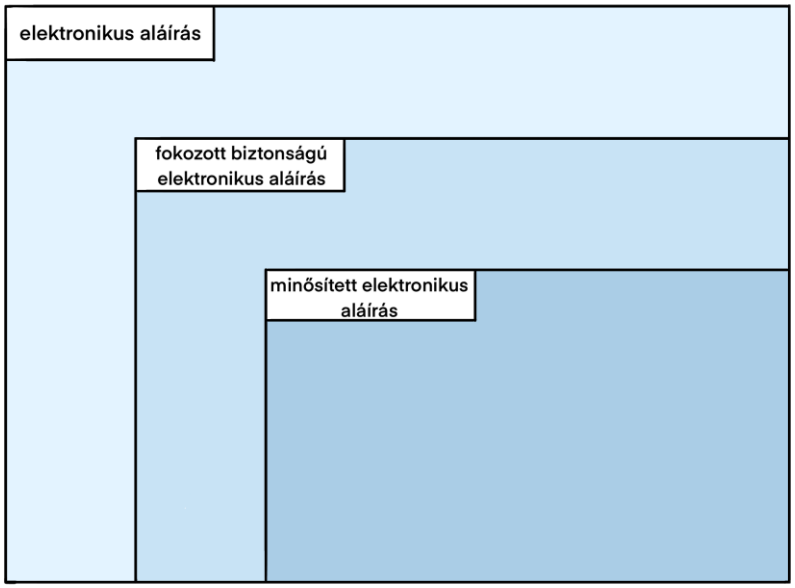
Természetesen egy e-mail végére írt „aláírás” (pl. Üdvözlettel: Kiss János) egyáltalán nem lesz alkalmas arra, hogy ugyanolyan szerepet töltsön be a joggyakorlat szempontjából, mint a papíralapú dokumentumokon elhelyezett saját kezű aláírás. Ezért az irányelv két további aláírástípust is definiált. Az egyik a **fokozott biztonságú** elektronikus aláírás, a másik pedig a **minősített elektronikus aláírás**.

A **fokozott biztonságú elektronikus aláírást** az különbözteti meg a „sima” elektronikus aláírásoktól, hogy olyan megoldást (technológiát vagy eljárást) kell alkalmazni a létrehozásakor, amely lehetővé teszi az aláíró személyének tényleges azonosítását. Konkrétan az irányelv négy követelményt fogalmaz meg a fokozott biztonságú aláírásokkal szemben:

1. kizárólag az aláíróhoz köthető;
2. alkalmas az aláíró azonosítására;
3. olyan, elektronikus aláírás létrehozásához használt adatok felhasználásával hozzák létre, amelyeket az aláíró nagy megbízhatósággal kizárólag saját maga használhat;
4. olyan módon kapcsolódik azokhoz az adatokhoz, amelyeket aláírtak vele, hogy az adatok minden későbbi változása nyomon követhető.

Mind a négy követelmény általános jellegű, vagyis a rendelet nem mondja meg konkrétan, hogy mely technológiák lesznek azok, amelyek alkalmasak arra, hogy segítségükkel fokozott biztonságú elektronikus aláírást készítsünk. Mindennek ellenére a megfogalmazásokból kitűnik, hogy az irányelv megalkotói igyekeztek olyan megfogalmazásokat kialakítani, amely lehetővé teszi, hogy a PKI aláírást használó műszaki megoldások mindenképpen fokozott biztonságú elektronikus aláírásnak minősülhessenek.

[2] Az Európai Parlament és a Tanács 910/2014/EU rendelete (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről



5. ábra: Az elektronikus aláírások típusai

A **minősített elektronikus aláírások** a fokozott biztonságú elektronikus aláírások közé tartoznak. Ahhoz, hogy egy fokozott biztonságú elektronikus aláírás minősített elektronikus aláírás legyen, nem további műszaki jellegű követelményeket kell teljesíteni, hanem két további feltételt. Az egyik feltétel az, hogy az aláírást az aláírónak egy biztonságos aláírás-létrehozó eszközzel hozza létre. A másik feltétel pedig az, hogy az aláírónak a saját személyazonosságát egy speciális, minősített tanúsítvánnyal kell igazolnia.

Magyarországon 2014-ig a jogi személyek és a természetes személyek aláírása nem különült el definíció szintjén, mindkét entitás képes volt elektronikus aláírást létrehozni. Az eIDAS rendelet hatályba lépését követően az Európai Unió megkülönbözteti a jogi személyek aláírását a természetes személyek aláírásától és külön szóval is illeti. Ez a fogalom az **elektronikus bélyegző**, létrehozója pedig kizárólag jogi személy lehet. Az elektronikus aláírás és bélyegző fogalmai közötti erőteljes hasonlóságot mutatja az, hogy egyrészről az eIDAS rendelet megismétli szinte szóról-szóra az elektronikus bélyegzők esetében az elektronikus aláírásra vonatkozó előírásokat, másrészről az elektronikus ügyintézésről szóló törvény (2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól, a továbbiakban: Eübszt.) kodifikációs fikcióval élve előírja, hogy – eltérő rendelkezés hiányában – bizonyos szabályok vonatkozásában az elektronikus bélyegzőt is elektronikus aláírásnak kell tekinteni. A bélyegzők is ugyanúgy lehetnek fokozott biztonságúak és minősítettek is.

3.1.1.3 A műszaki elektronikus aláírás fogalmai

3.1.1.3.1 Digitális aláírási standard

A Federal Information Processing Standard (FIPS) amerikai szövetségi dokumentumok közül a FIPS PUB 186-3 szabvány rögzíti a **Digitális Aláírás Szabvány** (Digital Signature Standard – DSS) tulajdonságait a szövetségi hivatalok számára. Az alapvető tulajdonságai nem térnek el jellemző módon az európai szabványoktól, a technológiai alapok természetesen közösek, a különbség a használt aláíró algoritmusban érhető tetten. A DSA algoritmus a

diszkrét logaritmus kiszámításának problémáján alapszik a prímszámok és a szorzás művelet által alkotott matematikai csoportban.

Ez a szabvány részletezi azokat az algoritmusokat, melyek az alkalmazások számára megfelelőek lesznek a digitális aláírás követelményeinek kielégítéséhez. A digitális aláírás a számítógépben egy bitsorozatot jelent. A digitális aláírás kiszámítása a szokásos szabályok és paraméterek használatával történik, hogy biztosítva legyen az aláíró személyazonossága, és az adatok sértetlensége igazolt legyen. A digitális aláírást tárolt, illetve elektronikusan továbbított adatok mellé is lehet generálni.

Az aláírás generálásához egy titkos kulcs használatos, ami létrehozza a digitális aláírást. Az ellenőrzéshez egy nyilvános kulcs használatos, ami a titkos kulcshoz tartozik, de nem egyezik meg azzal. Minden aláíró birtokol egy titkos és egy nyilvános kulcsból álló kulcspárt. A nyilvános kulcsot ismerhetik sokan, de a titkos kulcsot titokban kell tartani. Mindenki, aki ismeri a nyilvános kulcsot, képes ellenőrizni az aláírást a nyilvános kulcs segítségével. De kizárólag csak az a felhasználó képes elkészíteni a digitális aláírást, akinek a birtokában van a titkos kulcs.

A kivonatoló (hash) függvényt itt is az aláírás generálásának folyamatában használják, az aláírandó adatokra jellemző rövid, aláírható adat előállítása érdekében. Ezeket az adatokat gyakran az üzenet digitális kivonatának (message digest) hívják. Ez a kivonat lesz a bemenete a digitális aláírást végző algoritmusoknak, hogy létrehozzák a digitális aláírást. A hash-függvények leírását a 2008-ban kiadott Secure Hash Standard (SHS), FIPS 180-3 dokumentum tartalmazta, amelyet 2015 augusztusában a FIPS 180-4 váltott fel. A FIPS előírja, hogy a digitális algoritmusok olyan hash-függvényeket használjanak, amelyek az SHS-ben részletezettek és jóvá is hagyták azokat.

A digitális aláírás biztosítja az adatok tudatos ellenőrzését. Az ellenőrző ellenőrzi az aláírást az aláíráshoz tartozó nyilvános kulccsal, és ugyanazt a kivonatolást, lenyomatképzést (hash-függvényt) hajtja végre az üzeneten, mint az aláíró az aláírás elkészítésénél. Hasonló eljárásokat lehet alkalmazni mind az aláírás elkészítésénél, mind annak ellenőrzésénél, tárolt és küldött adatok esetében egyaránt.

A digitális aláírási rendszer biztonsága az aláírásra használt titkos kulcsok biztonságának fenntartásától függ. Ennek következtében az aláíróknak vigyázniuk kell arra, nehogy a titkos kulcsuk sokak által ismert legyen, kitudódjon. A FIPS-PUB 186-3 azonban nem terjed ki az aláíró személyes környezetének biztonságára, azaz arra, hogy az aláírási műveleteknek a személyes végrehajtása megfelelően biztonságos-e. Az aláírás készítőjének és ellenőrzőjének a felelőssége az, hogy gondoskodjon a műveletek végrehajtásának biztonsági környezetéről, ideértve a műveletek bármely részét, illetve a digitális aláírások tervezését és felépítését is.

3.1.1.3.2 XML digitális aláírás

XML digitális aláírás alatt az XML kódolással készült aszimmetrikus kriptográfiai eszközökkel készült aláírásokat értjük. Az RFC 3275 dokumentum rögzíti az **XML digitális aláírásokra** vonatkozó szintaxist, és feldolgozási szabályokat tartalmaz a digitális aláírások készítéséhez és megjelenítéséhez. Az XML-aláírások bármilyen XML-formátumú digitális tartalomhoz alkalmazhatóak. Egy XML-aláírás egy vagy több forrás alkotta tartalom esetében is alkalmazható. Beágyazott vagy beágyazódó aláírások létezhetnek ugyanazon XML-dokumentumban rögzített adatokhoz az XML-dokumentumon belül, az elkülönült aláírás (detached signature)

az aláírt elemeken kívüli formában létezik. Az XML specifikációja definiálja egy XML-aláírás elemeit, az elemek típusait, megfelelőségi követelményeket XML-séma definiálásával és prózai szöveggel. Ez a specifikáció továbbá tartalmaz még más szükséges adattípusokat is, mint például a hivatkozási adatok begyűjtésének módszerei, algoritmusok, kulcsok és kezelési információk.

Az XML-aláírás egy módszer az aláíró kulcs és a hivatkozott adatok összekapcsolására, de általában nem rögzítik, hogyan lesznek a kulcsok a személyekhez vagy intézményekhez rendelve, és a hivatkozott és aláírt adatok jelentésére nézve sem tartalmaznak utalásokat.

Az XML-névtér [XML-ns] URI (Uniform Resource Identifiers), amit kötelezően használnia kell minden (ehhez dátumozott) implementációnak, a következő: xmlns="http://www.w3.org/2000/09/xmldsig#"

Ez az URI specifikálja az XML-aláíráshoz használható erőforrásokat, algoritmusokat és szemantikát egyaránt.

Minden XML-digitális aláírás egy Signature elemmel valósítható meg, amely struktúrája az alábbi felépítést követi (ahol a „?" nulla vagy egy, a „+" egy vagy több, és a „*" jel nulla vagy több előfordulását jelenti az adott elemnek):

```
<ds:Signature ID?>
  <ds:SignedInfo>
    <ds:CanonicalizationMethod/>
    <ds:SignatureMethod/>
    (<ds:Reference>
      (<ds:Transforms>)?
      <ds:DigestMethod>
      <ds:DigestValue>
    </ds:Reference>)+
  </ds:SignedInfo>
  <ds:SignatureValue>
 (<ds:KeyInfo>)?
 (<ds:Object>)*
</ds:Signature>
```

`SignedInfo`: ez az elem az aláírt adat objektumokról tartalmaz információt.

```
<element name="SignedInfo" type="ds:SignedInfoType"/>
<complexType name="SignedInfoType">
  <sequence>
    <element ref="ds:CanonicalizationMethod"/>
    <element ref="ds:SignatureMethod"/>
    <element ref="ds:Reference" maxOccurs="unbounded"/>
  </sequence>
  <attribute name="Id" type="ID" use="optional"/>
</complexType>
```

`CanonicalizationMethod`: ez az elem adja meg azt az algoritmust, amit az aláírt adat objektum lenyomatolás előtti kanonizálására használtak.

```
<element name="CanonicalizationMethod"
      type="ds:CanonicalizationMethodType"/>
<complexType name="CanonicalizationMethodType" mixed="true">
  <sequence>
    <any namespace="##any" minOccurs="0" maxOccurs="unbounded"/>
  </sequence>
  <attribute name="Algorithm" type="anyURI" use="required"/>
</complexType>
```

`SignatureMethod`: ez az elem azokat az algoritmusokat tartalmazza, amely a kanonizált `SignedInfo` tartalmakat `SignatureValue` tartalommá alakítja. Ezek az algoritmusok lehetnek lenyomatoló eljárások, kulcsfüggő aláíró algoritmusok, valamint egyéb eljárások, mint például feltöltés. Az algoritmusok nevei aláírt attribútumok, ezáltal kivédhetőek az algoritmus cseréjén alapuló támadások. A különböző alkalmazások közötti kompatibilitás biztosítása érdekében meghatározott a kötelező-en alkalmazandó algoritmusok.

```
<element name="SignatureMethod"type="ds:SignatureMethodType"/>
<complexType name="SignatureMethodType" mixed="true">
  <sequence>
```

```
    <element name="HMACOutputLength" minOccurs="0"
        type="ds:HMACOutputLengthType"/>
    <any namespace="##other" minOccurs="0" maxOccurs="unbounded"/>
   </sequence>
  <attribute name="Algorithm" type="anyURI" use="required"/>
 </complexType>
```

`Reference`: minden ilyen elem egy adat objektumra hivatkozik (mely alá lesz írva).

Minden `Reference` elem tartalmazza egy lenyomatoló eljárás meghatározását (`DigestMethod`), valamint a meghatározott adat objektum ilyen algoritmussal készült lenyomatát (`DigestValue`), Base64 kódolással. Tartalmazhat még adatátalakítási leírást (Transforms) is, amellyel a lenyomatoló eljárás bemenő adata – lenyomatkészítés előtt – kialakítható.

```
 <element name="Reference" type="ds:ReferenceType"/>
 <complexType name="ReferenceType">
  <sequence>
   <element ref="ds:Transforms" minOccurs="0"/>
   <element ref="ds:DigestMethod"/>
   <element ref="ds:DigestValue"/>
  </sequence>
  <attribute name="Id" type="ID" use="optional"/>
  <attribute name="URI" type="anyURI" use="optional"/>
  <attribute name="Type" type="anyURI" use="optional"/>
 </complexType>
```

`SignatureValue`:ez az elem tartalmazza az aláírás eredményét, Base64 kódolással.

`KeyInfo`: ez az elem adja meg azt a kulcsot, amivel az aláírás érvényesítése (ellenőrzése) megtörténhet.

`Object`: ez az (opcionális, de többször is előfordulható) elem tetszőleges adatokat tartalmazhat.

A létrehozott XML elektronikus aláírás lehet:

1. elkülönített állomány az aláírt tartalomtól (detached signature),
2. a Signature elembe ágyazott aláírt XML-tartalom (enveloping signature), illetve
3. aláírt XML-tartalomba ágyazott (enveloped signature).

Ügyelni kell a Signature elem azonosítójának (ID) egyediségére, mert ha többszörösen létezik, vagy összekombinálódott egy másik elemmel (és annak ID-jével) ugyanazon XML-dokumentumon belül, akkor a nevek választásánál különösen nagy óvatosság ajánlott, hogy a tartalomban és a hozzárendelhetőségben ne legyen ütközés (ugyanazon ID-k és eltérő tartalom), mert ez könnyen vezethet az aláírás érvényességének elvesztéséhez.

3.1.1.3.3 PKI aláírás

A digitális aláírás technikáját a Publikus Kulcsú Infrastruktúrákban (PKI) és a Privilégium Menedzsment Infrastruktúrákban (PMI) használják arra, hogy az a szervezet, mely digitális tanúsítványokat bocsát ki, ezzel hitelesítse a tanúsítványban szereplő adatok összetartozását, összekötését. A PKI-rendszerekben a kibocsátott nyilvános kulcsú tanúsítvány igazolja a nyilvános kulcsnak és a tanúsítvány címzettjének összetartozását, a PMI rendszerekben a kibocsátott tulajdonságtanúsítvány (privilégiumtanúsítvány) pedig a tanúsítványbirtokos és a kibocsátott tulajdonság (privilégium) összetartozását hitelesíti.

A szabvány nem általános értelemben vett digitálisaláírás-szabvány, hanem rögzíti a tanúsítványtárak, PKI és PMI rendszerek aláírandó jelölt elemeit. Az aláírt információ fogadója egyrészről alkalmazza a megkapott információra az egyirányú kivonatolási függvényt újra, és összehasonlítja a kapott eredményt az aláírásból az aláíró nyilvános kulcsa segítségével kinyert értékkel.

A szabvány nem írja elő egyetlen kötelező kivonatoló függvény használatát, de szándéka szerint alkalmazható minden megfelelő kivonatoló függvényre, és alkalmazható minden olyan változás esetén, amit a kriptográfiai, matematikai technikák vagy számítási kapacitások jövőbeli változása okoz.

Az aláírt információk tartalmaznak arra nézve adatokat, hogy melyik kivonatoló vagy aláíró algoritmus lett felhasználva a digitális aláírás készítése során.

A PKI aláírások terminológiáját az X509 szabvány segítségével mutatja be ez a rész a továbbiakban. Valamely adatok kriptográfiai kódolásának eredményét az alábbi ASN.1 struktúrával lehet leírni:

ENCRYPTED { ToBeEnciphered } ::= BIT STRING (CONSTRAINED BY {
-- shall be the result of applying an encipherment procedure –
-- to the BER-encoded octets of a value of – ToBeEnciphered })
HASH {ToBeHashed} ::= SEQUENCE {
algorithmIdentifier AlgorithmIdentifier,
hashValue BIT STRING (CONSTRAINED BY {
-- shall be the result of applying a hashing procedure to the DER-encoded octets –
-- of a value of – ToBeHashed }) }
ENCRYPTED-HASH { ToBeSigned } ::= BIT STRING (CONSTRAINED BY {
-- shall be the result of applying a hashing procedure to the DER-encoded octets –
-- of a value of – ToBeSigned – and then applying an encipherment procedure to those octets -- })
SIGNATURE { ToBeSigned } ::= SEQUENCE {
algorithmIdentifier AlgorithmIdentifier,
encrypted ENCRYPTED-HASH { ToBeSigned }}

Ezen túl a szabvány, mint Nyilvános Kulcsú Tanúsítványok Keretrendszere foglalkozik a digitális aláírással, és alapvetően a tanúsítványokra fókuszál.

A PKI könyvtárséma definiálja azokat az elemeket, melyeket egy PKI Directory objektumként tartalmazhat:

1. **PKI user object class**: a PKI tanúsítvány tárgy/subject elemeinek definiálására szolgál,
1. **PKI CA object class**: a tanúsítványkibocsátóként működő szervezetek definiálására használják,
2. **CRL distribution points object class and name form:** a visszavonási lista közzétételi pontjának meghatározására szolgál,
3. **Delta CRL object class:** a különbségi (kibocsátás óta eltelt idő alatti eseményeket tartalmazó) visszavonási listákat tartalmazó elemek megjelölésére szolgál,
4. **Certificate Policy & CPS object class:** a hitelesítési rendek, hitelesítésszolgáltatási szabályzatok megjelölésére használt elem,
5. **PKI certificate path object class:** a PKI tanúsítvány-útvonal objektum tartalmazza a tanúsítvány elérhetőségi információit. Általában a pkiCA ojbektummal együtt alkalmazzák.

Az egyes osztályok ASN.1 kódolású leírását a szabvány az alábbiakban rögzíti:

pkiUser OBJECT-CLASS ::= {
SUBCLASS OF {top}
KIND auxiliary
MAY CONTAIN {userCertificate}
ID id-oc-pkiUser }

pkiCA OBJECT-CLASS ::= {
SUBCLASS OF {top}
KIND auxiliary
MAY CONTAIN {cACertificate |
certificateRevocationList |
authorityRevocationList |
crossCertificatePair }
ID id-oc-pkiCA }

cRLDistributionPoint OBJECT-CLASS ::= {
SUBCLASS OF { top }
KIND structural
MUST CONTAIN { commonName }
MAY CONTAIN { certificateRevocationList |
authorityRevocationList |

```
deltaRevocationList }
ID id-oc-cRLDistributionPoint }

cRLDistPtNameForm NAME-FORM ::= {
NAMES cRLDistributionPoint
WITH ATTRIBUTES { commonName}
ID id-nf-cRLDistPtNameForm }

deltaCRL OBJECT-CLASS ::= {
SUBCLASS OF {top}
KIND auxiliary
MAY CONTAIN {deltaRevocationList}
ID id-oc-deltaCRL }

cpCps OBJECT-CLASS ::= {
SUBCLASS OF {top}
KIND auxiliary
MAY CONTAIN {certificatePolicy |
certificationPracticeStmt}
ID id-oc-cpCps }

pkiCertPath OBJECT-CLASS ::= {
SUBCLASS OF {top}
KIND auxiliary
MAY CONTAIN { pkiPath }
ID id-oc-pkiCertPath }
```

Gyakorló kérdések:

1. Az elektronikus aláírás fogalom hol jelent meg először a társadalomban?
2. Mi a kapcsolat a kézi aláírás és az elektronikus aláírás között?
3. Hogyan osztályozza az irányelv az elektronikus aláírásokat?

3.1.2 Az elektronikus aláírás fogalomrendszere

Az elektronikus aláírással kapcsolatos kérdések megértéséhez – az elektronikus aláírás fogalmának ismerete mellett – további fogalmak ismerete is szükséges. Ezen fogalmak egy része **szabályozási** (jogi) eredetű, más része pedig a ma elérhető **műszaki** megoldásokhoz kapcsolódik. A jogi és műszaki fogalmak megkülönböztetésének jelentősége abban áll, hogy az egyes műszaki megoldásokhoz kapcsolódó fogalmaknak kizárólag az egyes technológiáknál van értelme. Az elektronikus aláírás jogi fogalomrendszere várhatóan sokkal hosszabb távon marad velünk, mint az egyes technológiákhoz kapcsolódó fogalmak. Emellett az a tendencia is megfigyelhető, hogy a jogi eredetű fogalmak használata lassan háttérbe szorítja a műszaki világ által eredetileg használt elnevezéseket, és ezért a műszaki eredetű fogalmakkal csak a konkrét alkalmazások esetében találkozunk.

Jogi eredetű fogalmak	Konkrét műszaki megoldásokhoz kapcsolódó fogalmak
Aláírás-létrehozó adat	PKI magánkulcs vagy PKI titkos kulcs
Aláírás-ellenőrző adat	PKI nyilvános kulcs
Tanúsítvány	ITU X.509-es tanúsítvány
Minősített tanúsítvány	Tanúsítvány-visszavonási lista
Bizalmi szolgáltatások	Valós idejű visszavonási állapot szolgáltatás
Tanúsítvány-kibocsátás elektronikus aláírásokhoz	Tanúsítványkibocsátó

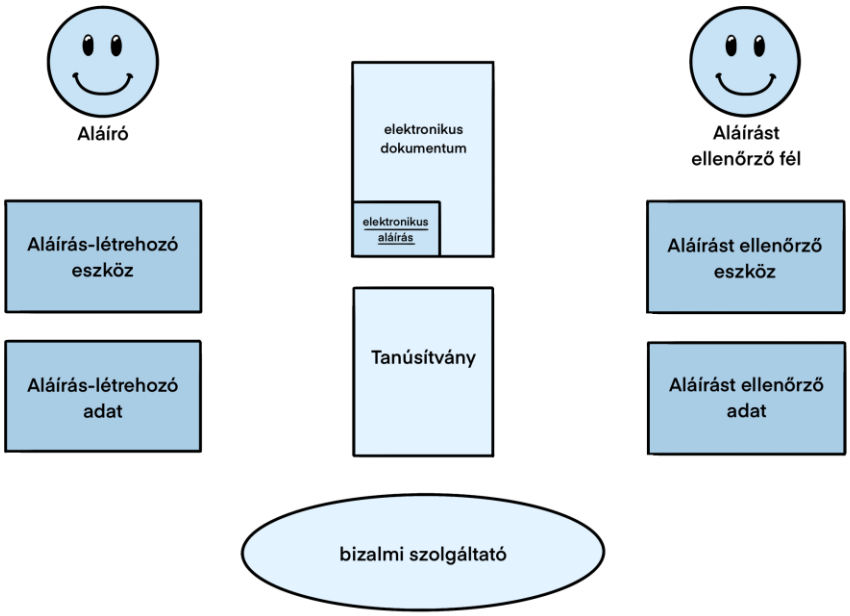
Jogi eredetű fogalmak	Konkrét műszaki megoldásokhoz kapcsolódó fogalmak
Elektronikus aláírási termék Biztonságos aláírás-létrehozó eszköz Aláíró	Aláíró hardver és szoftver Chipkártya Aláírási politika

3. táblázat: Jogi és műszaki eredetű fogalmak

A táblázat a fontosabb jogi és műszaki fogalmak összefoglaló bemutatását tartalmazza. A fejezet további részében pedig az egyes jogi eredetű fogalmakat, valamint a ma leginkább elterjedt műszaki eredetű fogalmakat ismertetjük.

3.1.2.1 Az elektronikus aláírással kapcsolatos jogi eredetű fogalmak

Az alábbi ábra a jogi fogalmakat az elektronikus aláírás használatának szempontjából betöltött szerepük szerint csoportosította:



6. ábra: Jogi elektronikus aláírási fogalmak

Szorosan az aláíróhoz kötődő fogalmak az aláírás-létrehozó adat és eszköz. Az aláírás-ellenőrző félhez értelemszerűen az aláírás-ellenőrző eszköz és adat fogalmak tartoznak. A tanúsítvány leginkább a hitelesítésszolgáltatóhoz és az aláírás-ellenőrzéshez kapcsolódó fogalom. Annak ellenére igaz ez, hogy a tanúsítvány nem vesz részt az aláírásban, de a tanúsítvány birtokosa az aláíró. Az elektronikusan aláírt elektronikus dokumentum nélkül az összes többi koncepció természetszerűleg értelmezhetetlen, ezért szerepel ez az ábrán. Hasonló ábra készíthető a bélyegzők tekintetében is.

3.1.2.1.1 Aláírás és bélyegzés létrehozója

Az elektronikus aláírási rendelet megfogalmazásában az **aláíró** azt a személyt jelöli, aki az aláíró eszközt birtokolja, és aki a saját nevében, illetve más személy vagy szervezet nevében jár el. Az aláíró az irányelv megfogalmazásában egyértelműen egy ember (jogi terminológiával: természetes személy), vagyis egy szervezet vagy egy gép (pl. egy szerver) nem

minősülhet jogi értelemben aláírónak, azaz elektronikus aláírás létrehozójának. Ennek a korlátozásnak az a következménye, hogy elektronikus aláírást jogi értelemben magánszemélyen kívül más nem hozhat létre. Szervezet nevében pedig elektronikus bélyegzőt lehet csak létrehozni.

A gyakorlatban léteznek olyan megoldások, amelyek emberi beavatkozás és közvetlen felügyelet nélkül hoznak létre digitális aláírásokat. Ilyen megoldásokat találunk például az elektronikus számlákat kibocsátó szolgáltatások esetében. Ezekben az esetekben az aláírók csak látszólag a gépek. Az aláíró eszközök ezekben az esetekben is konkrét személyhez kötődnek, az aláíró eszköz birtoklása azonban közvetett. Ez konkrétan azt jelenti, hogy az aláíró eszközt például egy szerverben helyezik el, amelyhez olyan tanúsítvány kapcsolódik, amelyet kizárólag a szervezet képviseletére feljogosított személy tud igényelni, és rendelkezhet a felhasználás módjáról.

3.1.2.1.2 Aláírás-létrehozó és -ellenőrző adat

Az **aláírás-létrehozó adat** olyan egyedi adat, amelyet az aláíró használ az elektronikus aláírás létrehozásához. Ahhoz, hogy egy adat aláírás-létrehozó adatnak minősüljön, az egyetlen lényegi követelmény az, hogy egyedi legyen. Az **aláírás-ellenőrző adat** olyan adat, amellyel az aláírás kriptográfiai érvényességét lehet ellenőrizni. Az **érvényesítési adat** olyan adat, amely elektronikus aláírás vagy elektronikus bélyegző érvényesítéséhez használt, ahol az **érvényesítés** alatt azt a folyamatot kell érteni, amelynek keretében ellenőrzik és igazolják, hogy az elektronikus aláírás vagy bélyegző érvényes.

Az aláírás-létrehozó és -ellenőrző adat megkülönböztetéséből nem következik az, hogy kizárólag a PKI megoldások segítségével lehetne elektronikus aláírást létrehozni. A különbségtétel nem zárja ki azt, hogy például szimmetrikus titkosítási megoldásokat vagy egyszerű aláíró kódokat használjanak elektronikus aláírás létrehozásához. Az egyetlen tartalmi követelmény lényegében az, hogy az aláírás-létrehozó adatnak egyedinek kell lennie. Az aláírás-ellenőrző adattal szemben még ilyen követelményt sem fogalmaz meg az elektronikus aláírási irányelv. Ebből adódóan egy elektronikus banki szolgáltatásnál alkalmazott egyszer használatos kód is aláírás-létrehozó adat lehet, és az egyszer használatos kódnak a tranzakciós adatokhoz történő csatolásával „sima” (azaz nem fokozott biztonságú) elektronikus aláírás hozható létre.

3.1.2.1.3 Bizalmi szolgáltatások és a tanúsítványok kibocsátása

Az eIDAS szabályokat tartalmaz a bizalmi szolgáltatásokra (angolul: trust service), valamint a szolgáltatók (angolul: trust service provider) által nyújtható különböző szolgáltatásokra, ideértve a tanúsítványok kibocsátását is. A bizalmi szolgáltatás egy általános kategória, amely magában foglal minden olyan szolgáltatást, amely az elektronikus aláírások, bélyegzők, webhitelesítő tanúsítványok és az aláírások vagy tanúsítványok megőrzéséhez kapcsolódhatnak. A tanúsítványok kibocsátását **hitelesítésszolgáltatás** néven nevesíti az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény a kormány által kötelezően biztosított szabályozott elektronikus ügyintézési szolgáltatásként definiált kormányzati hitelesítésszolgáltatás esetében. Ez írta elő a Kormányzati Hitelesítés Szolgáltató kötelező kialakítását.

3.1.2.1.4 Tanúsítvány és minősített tanúsítvány

A **tanúsítvány** egy olyan elektronikus igazolás, amely az aláírás-ellenőrző adatnak az aláíróhoz való tartozását igazolja. Az irányelv szerint nem szükséges tanúsítvány ahhoz, hogy valaki elektronikus aláírást hozzon létre. A tanúsítvány kizárólag az elektronikus aláírás érvényességének (aláíróhoz való tartozásának) ellenőrzéséhez nyújt segítséget. Tanúsítványt jellemzően a hitelesítésszolgáltatók bocsátanak ki, akik megbízható harmadik félként tanúsítják, hogy az aláírás ellenőrző adatok mely személyekhez tartoznak.

A **minősített tanúsítvány** olyan tanúsítvány (igazolás), ami az eIDAS I. számú mellékletében felsorolt adatokat tartalmazza, és olyan bizalmi szolgáltató bocsátotta ki, amely az eIDAS szerint működik. Az eIDAS minősített bizalmi szolgáltatók számára előírt követelményeit teljesítő bizalmi szolgáltatók a **minősített bizalmi szolgáltatók**, akiknek erről akkreditált tanúsító szervezet által kiállított tanúsítvánnyal is kell rendelkezniük.

Az eIDAS I. számú melléklete szerint a minősített tanúsítványnak az alábbi adatokat kell tartalmaznia:

a) legalább automatizált feldolgozásra alkalmas formában utalnia kell arra, hogy a tanúsítványt elektronikus aláírás minősített tanúsítványaként bocsátották ki;

b) a minősített tanúsítványt kibocsátó minősített bizalmi szolgáltatót egyértelműen azonosító adatok, beleértve legalább azt a tagállamot, amelyben az érintett szolgáltató letelepedett, valamint

- jogi személy esetében a hivatalos nyilvántartásban szereplő megnevezést és adott esetben nyilvántartási számot,
- természetes személy esetében a személy nevét;

c) legalább az aláíró neve vagy pedig egy álnév;. álnév használata esetén ezt egyértelműen jelezni kell;

d) az elektronikus aláírás érvényesítéséhez használt adat, amely megfelel az elektronikus aláírás létrehozásához használt adatnak;

e) a tanúsítvány érvényességi idejének kezdete és vége;

f) a tanúsítvány azonosító kódja, amelynek a minősített bizalmi szolgáltatóhoz tartozó egyedi kódnak kell lennie;

g) a minősített bizalmi szolgáltató fokozott biztonságú elektronikus aláírása vagy fokozott biztonságú elektronikus bélyegzője;

h) az a helyszín, ahol a g) pontban említett, a fokozott biztonságú elektronikus aláírásra vagy fokozott biztonságú elektronikus bélyegzőre vonatkozó tanúsítvány ingyenesen hozzáférhető;

i) azoknak a szolgáltatásoknak a helye, amelyek segítségével felvilágosítás kérhető a minősített tanúsítvány érvényességi állapotáról;

j) amennyiben az elektronikus aláírás érvényesítéséhez használt adathoz kapcsolódó, elektronikus aláírás létrehozásához használt adat minősített elektronikus aláírást létrehozó eszközön található, ennek megfelelő feltüntetése, legalább automatizált feldolgozásra alkalmas formában.

3.1.2.1.5 Termék és biztonságos aláírás-létrehozó eszköz

Termék alatt az eIDAS olyan hardver- vagy szoftvereszközt, illetve ezek megfelelő részét érti, amelyet bizalmi szolgáltatások nyújtásában való felhasználásra szántak.

Az **aláírás-létrehozó eszközök** körében az eIDAS külön definiálja a minősített aláírás-létrehozó eszközöket. Ennek jelentősége abban áll, hogy a minősített elektronikus aláírások létrehozásának feltételeként szabja azt, hogy az elektronikus aláírást minősített aláírás-létrehozó eszközzel készítse az aláíró. Egy aláírás-létrehozó eszköz akkor tekinthető **minősített aláírás-létrehozó eszköznek**, ha teljesíti az eIDAS II. számú mellékletében meghatározott követelményeket. A legfontosabb követelmény az, hogy a minősített elektronikus aláírást létrehozó eszközöknek megfelelő technikai és eljárási megoldások segítségével garantálniuk kell legalább azt, hogy:

a) az elektronikus aláírás létrehozásához használt adat bizalmassága ésszerű mértékben biztosítva legyen;

b) az elektronikus aláírás létrehozásához használt adat gyakorlatilag csak egyszer jöhessen létre;

c) az elektronikus aláírás létrehozásához használt adatok kikövetkeztethetősége ésszerű mértékig kizárható legyen, az elektronikus aláírás pedig megbízhatóan védve legyen a jelenleg rendelkezésre álló technológiákkal elkövetett hamisítás ellen;

d) az elektronikus aláírás létrehozásához használt adatot a jogszerűen aláíró személy megbízható védelemmel tudja ellátni a mások általi felhasználás ellen.

A minősített aláírás-létrehozó eszközök esetében a fenti követelményeknek való megfelelőséget egy **terméktanúsító szervezetnek** kell tanúsítania. Ez azt jelenti, hogy a minősített aláírás-létrehozó eszközök esetében nem elegendő csak a követelmények teljesítése, hanem szükséges a követelmények teljesülésének a gyártótól független szervezet általi vizsgálata és a vizsgálat eredményéről történő **terméktanúsítvány** kiállítása is.

Gyakorló kérdések:

1. Melyek a jogi és a műszaki eredetű elektronikus aláírási fogalmak?
2. Jogi értelemben mit neveznek aláírónak és mit zárnak ki ebből a körből?
3. Mi az aláírás-létrehozó adat és egy egyszer használatos kód között a hasonlóság?

3.2 Az EU céljai és az elektronikus aláírás jogi szabályozásának helyzete

3.2.1 Az európai e-programok (eEurope) és nemzeti kihatásaik

3.2.1.1 Elektronikus aláírás és az Európai Unió

Az elektronikus aláírással kapcsolatos európai uniós törekvések viszonylag hamar, már az 1994-es **Bangemann Report**ban is megjelentek. Az elektronikus aláírás szabályozására az uniós szakpolitikusok a téma megjelenésétől kezdve úgy tekintettek, mint az uniós tagállamok modernizációjának egyik szabályozási eszközére.

1993 decemberében Brüsszelben az Európa Tanács – látván az USA és Japán közötti versenyfutást – jelentést kért az információs társadalom közösségi fejlesztésének lehetőségei-

ről, amit 1994-ben Korfun meg is vitatott. A jelentést vezető szakértők csoportja készítette el, a csoport vezetője az akkori ipari, informatikai és telekommunikációs európai biztos Martin Bangemann volt. A jelentésben feltárták a globális piacot akkor jellemző tényeket, és sürgették az Európai Uniót olyan piaci mechanizmusok és motivációs tényezők kialakítására, melyek átvezetik a közösséget az **információs korba**, továbbá a kapcsolódó akciótervben európai és tagállami szinten is olyan javaslatokat fogalmaztak meg, melyek *„lebontják a fennálló, kollektív hátrányokat eredményező elsáncolt pozíciókat”*. A Bangemann Report hangsúlyosan használta az „**Európai információs társadalom kialakítása**” fogalmat, és rávilágított arra, hogy az információs társadalmi verseny már globálisan is elindult. Az akcióterv számos javaslatot fogalmaz meg a magán- és a közszféra partnerségén alapulva, amelyek átvihetik Európát az információs társadalomba.

Az Európai Bizottság 1997-ben kezdte meg az **elektronikus aláírási irányelv** kidolgozását. Az irányelv célja az információs és kommunikációs technológiák használatának Unión belüli elterjedését segítő szabályozás kialakítása volt. Természetesen senki nem gondolta, hogy a különböző technológiák, így az elektronikus aláírás használatának az elterjedése a szabályozás eredményeként fog megvalósulni. A szabályozás célja kifejezetten az elektronikus aláírás használatának elterjedését nehezítő szabályozási akadályok (pl. eltérő vagy egymásnak ellentmondó tagállami szabályozások) létrejöttének a megakadályozása volt. 2014-ben felülvizsgálták az addigi szabályozást, és a tapasztalatok alapján létrejött az **eIDAS**, amely minden tagállamban törvényi szinten érvényesült.

Az uniós elektronikus aláírás szabályozás két részre bontható. Azon túlmenően, hogy az aláírásokat a bizalmi szolgáltatások között szabályozták, a szabályozás egyik része az elektronikus aláírások **mibenlétével** foglalkozik, a másik része pedig az elektronikus aláírással aláírt elektronikus dokumentumok **használatához** kötődik. Az előbbi témakör általánosságban magára az aláírásokra és bélyegzőkre vonatkozik, az elektronikus aláírás használatával kapcsolatos szabályozás azonban sok különböző ágazati jogi szabályozásban található, és kivétel nélkül egy-egy konkrét témakörhöz kötődik.

3.2.1.2 Az elektronikus aláírás használatával kapcsolatos uniós szabályozás

Az elektronikus aláírási irányelv megjelenése óta számos **uniós szabályozásban** jelent meg direkt vagy indirekt hivatkozás az elektronikus aláírásra. Ezek a hivatkozások kivétel nélkül az elektronikus aláírás használatához kapcsolódnak.

A legfontosabb ilyen uniós szabályozások az alábbi témaköröket érintik:

1. elektronikus számla,
2. közbeszerzés,
3. elektronikus és digitalizált dokumentumok használata.

3.2.1.2.1 Elektronikus számla

A hozzáadottérték-adóval kapcsolatos 2001/115/EK irányelv és később az ezt felváltó 2006/112/EK irányelv egyaránt megköveteli a tagállamoktól, hogy biztosítsanak lehetőséget az **elektronikus számlák** használatára. Az irányelv azt a követelményt fogalmazza meg az elektronikus számlákkal szemben, hogy olyan technológiával állítsák elő, amely a számla tartalmának integritását (későbbi megváltoztatásának felismerhetőségét) biztosítani tudja. Az irányelv kimondja továbbá, hogy az integritás biztosítására alkalmas műszaki megoldásnak

kell tekinteni a fokozott biztonságú elektronikus aláírás használatát. Az irányelv lehetővé teszi a tagállamok számára azt is, hogy a fokozott biztonságú elektronikus aláírás helyett a minősített elektronikus aláírás használatát követeljék meg az elektronikus számlák esetében.

Fontos további előírása az irányelvnek továbbá, hogy (a 234. cikk alapján) a tagállamok a területükön termékértékesítést vagy szolgáltatás nyújtást végző adóalanyok számára nem írhatnak elő a számlák elektronikus úton való továbbítására vagy rendelkezésre bocsátására szolgáló rendszer alkalmazásával kapcsolatos további kötelezettségeket vagy alaki követelményeket.

3.2.1.2.2 Közbeszerzési irányelvek

A közbeszerzési irányelvek az **elektronikus közbeszerzés** kapcsán érintik az elektronikus aláírás használatának kérdését. Az irányelvek nem határozzák meg, hogy pontosan milyen elektronikus aláírást kell használni a tagállami elektronikus közbeszerzések során, ugyanakkor előírják, hogy az elektronikus aláírás használatát érintő közbeszerzési szabályoknak konzisztensnek kell lenniük a tagállami szabályozással. Az elektronikus közbeszerzési rendszereket legkésőbb 2010-ig kellett megvalósítaniuk a tagállamoknak.

A magyar elektronikus közbeszerzési törvény megengedi, sőt kötelezően elő is írja azt, hogy a közbeszerzéssel kapcsolatos eljárási cselekmények elektronikusan is gyakorolhatók legyenek. Értelmezi továbbá az „írásbeli, írásban” fogalmakat is, külön a közbeszerzések számára. Az írásbeliség itt *„a közbeszerzési eljárás során tett nyilatkozatok, illetve eljárási cselekmények tekintetében bármely, szavakból vagy számjegyekből álló kifejezés, amely olvasható, reprodukálható, majd közölhető, ideértve az elektronikus úton továbbított és tárolt adatokat is”* lehet, ez számít a közbeszerzés szempontjából írásbelinek, írásban megtett kötelezettségvállalásnak.

3.2.1.2.3 Elektronikus és digitalizált dokumentumokkal kapcsolatos határozat

Az Európai Bizottság 2004/563-as határozata a Bizottság belső eljárási szabályzatát tartalmazza. A határozat kimondja, hogy az elektronikus dokumentumok használata esetén a Bizottság elektronikus aláírást fog használni az elektronikus dokumentumok érvényességének a biztosítására.

A határozatot Brüsszelben, 2004. július 7-én hozták. Az alábbi rendelkezéseit érdemes kiemelni és modellértékűnek tekinteni:

„Szükség van olyan rendelkezések elfogadására, amelyek a Bizottság vonatkozásában meghatározzák az elektronikus és digitalizált dokumentumok vagy elektronikus úton továbbított dokumentumok érvényességi feltételeit, amennyiben ezeket a feltételeket máshol nem határozták meg, valamint azok megőrzésének feltételeit is, biztosítva a dokumentumok és az azokat kísérő metaadatok mindenkori teljességét és olvashatóságát a szükséges megőrzési idő teljes tartamára. (…)

Abban az esetben, ha egy alkalmazandó közösségi vagy nemzeti rendelkezés értelmében egy dokumentum aláírt eredeti példányára is szükség van, egy, a Bizottság által elkészített vagy átvett elektronikus dokumentum akkor tesz eleget ennek a követelménynek, ha a kérdéses dokumentumot olyan fokozott biztonságú elektronikus aláírással látták el, amely egy minősített tanúsítványon alapul, és egy biztonságos aláírás-létrehozó eszközzel hoztak létre,

vagy amelyet olyan elektronikus aláírással láttak el, amely hasonló biztosítékokkal szolgál az aláíráshoz rendelt funkcionalitások tekintetében.

Abban az esetben, ha egy alkalmazandó közösségi vagy nemzeti rendelkezés szükségessé teszi, hogy egy dokumentumot írásban készítsenek el, az aláírt eredeti példányra azonban nem tart igényt, egy, a Bizottság által elkészített vagy átvett elektronikus dokumentum akkor tesz eleget ennek a követelménynek, ha a dokumentumot előállító személyt megfelelően azonosították, és a dokumentumot olyan feltételek mellett készítették el, amelyek biztosítékkal szolgálnak tartalmának és az azt kísérő metaadatoknak a teljességére nézve, és azt a meghatározott feltételek szerint megőrizték."

Ezeket az elveket az iratkezelésről és az irattárról szóló 2021/2121 EU Bizottsági Határozat (2020. július 6.) maradéktalanul átvette, továbbá az eIDAS vélelmeit is beépítette. Lényeges elem, hogy a Bizottság irattári anyagait elektronikus formában kell létrehozni, és azokat a hivatalos elektronikus adattárakban kell tárolni. Ez biztosítja, hogy a kezelt iratokat (adatokat és információkat) a lehető legszélesebb körben hozzáférhetővé lehessen tenni, és meg lehessen osztani a Bizottságon belül, kivéve, ha a hozzáférést jogi kötelem korlátozza.

Gyakorló kérdések:

1. Hány részre bontható az uniós elektronikus aláírási szabályozás és mik ezek?
2. Lehet-e elektronikus úton közbeszerzést végezni?
3. Melyek az uniós szabályozás legfontosabb témakörei, amelyek alkalmazzák az elektronikus aláírásokat?

3.2.2 Az elektronikus aláírás fontosabb uniós szabályozásai

3.2.2.1 Az eIDAS rendelkezései

Az elektronikus aláírás legelső európai uniós szabályozása az 1999/93/EK irányelvben volt megtalálható. Az irányelvet – többéves előkészítő munkát követően – 1999. december 13-án fogadták el. Az uniós irányelvekről fontos tudni, hogy előírásaik nem személyeknek vagy szervezeteknek szólnak, hanem az Európai Unió tagállamait kötelezik meghatározott tartalmú szabályozás kialakítására. Az elektronikus aláírási irányelv számos kérdéskörben írt elő követelményeket az elektronikus aláírással kapcsolatos nemzeti szabályozások tekintetében, amelyet a 2001. évi XXXV törvény ültetett át a magyar gyakorlatba, és ez volt hatályban 2016. június 30-ig.

Időközben felvetődött a szabályozás felülvizsgálatának igénye. A 2013-ban elkezdődött átalakítás vezetett az eIDAS megjelenéséhez. Az eIDAS két fő fejezete szabályozta az elektronikus azonosítás és a bizalmi szolgáltatások működését az egész EU-ban határon átnyúló módon, valamint kimondta, hogy egyetlen egy elektronikus dokumentum joghatása és bírósági eljárásokban bizonyítékként való elfogadhatósága sem tagadható meg kizárólag amiatt, hogy az elektronikus formátumú. Az eIDAS megjelenését követően számos uniós végrehajtási rendelet látott napvilágot, példának okáért az alábbiak:

- A Bizottság (EU) 2015/296 végrehajtási határozata (2015. február 24.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról szóló 910/2014/EU európai parlamenti és tanácsi rendelet 12. cikkének (7) bekezdése értelmében vett, a tagállamok által az elektronikus azonosítás te-

rületén folytatandó együttműködésre vonatkozó eljárási szabályok megállapításáról EGT-vonatkozású szöveg

- A Bizottság (EU) 2016/650 végrehajtási határozata (2016. április 25.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról szóló 910/2014/EU európai parlamenti és tanácsi rendelet 30. cikkének (3) bekezdése és 39. cikkének (2) bekezdése alapján a minősített aláírást és bélyegzőt létrehozó eszközök biztonsági értékelésére vonatkozó szabványok megállapításáról (EGT-vonatkozású szöveg) C/2016/2303
- A Bizottság (EU) 2015/806 végrehajtási rendelete (2015. május 22.) a minősített bizalmi szolgáltatások uniós bizalmi jegyének formájára vonatkozó előírások megállapításáról (EGT-vonatkozású szöveg) C/2015/3364
- A Bizottság (EU) 2015/1501 végrehajtási rendelete (2015. szeptember 8.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról szóló 910/2014/EU európai parlamenti és tanácsi rendelet 12. cikkének (8) bekezdése szerinti átjárhatósági keretről (EGT-vonatkozású szöveg)
- A Bizottság (EU) 2015/1502 végrehajtási rendelete (2015. szeptember 8.) az elektronikus azonosító eszközök biztonsági szintjeire vonatkozó minimális technikai specifikációknak és eljárásoknak a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról szóló 910/2014/EU európai parlamenti és tanácsi rendelet 8. cikkének (3) bekezdése szerint történő megállapításáról (EGT-vonatkozású szöveg)

Az elektronikus ügyintézés legfontosabb hazai normatív dokumentuma a 2015. évi CCXXII. törvény lett, amely kiegészítette és részletezte az eIDAS által leírtakat.

3.2.2.2 Nemzetközi aspektusok

Az eIDAS megalkotásának egyik célja az elektronikus aláírással kapcsolatos szolgáltatások és az elektronikus aláírási termékek egységes, uniós belső piacának a megteremtése. A nem uniós elektronikus aláírással kapcsolatos szolgáltatások Unión belüli elismerésének kérdését azonban önmagában nem érinti az elektronikus aláírással kapcsolatos szabályozás uniós (belső) egységesítése. Ezért külön foglalkozik a rendelet azzal a kérdéssel, hogy nem uniós országok (**harmadik országok**) szolgáltatóinak elismerése miként történhet meg.

A harmadik országban letelepedett bizalmi szolgáltatók által nyújtott bizalmi szolgáltatásokat abban az esetben kell jogilag egyenértékűnek elismerni az Unióban letelepedett minősített bizalmi szolgáltatók által nyújtott minősített bizalmi szolgáltatásokkal, ha a harmadik országból származó bizalmi szolgáltatásokat az Unió és a szóban forgó harmadik ország vagy valamely nemzetközi szervezet által megkötött megállapodásban elismerték.

Természetesen nemcsak a harmadik országok szolgáltatóinak Unión belüli elismerése lehet kérdés, hanem az uniós szolgáltatóknak az Unión kívüli működése is nehézségekbe ütközhet. Az EU-s bizalmi szolgáltatások **globális elismerése** még hiányzik, de az EU komoly erőfeszítéseket tesz ennek érdekében.

3.2.2.3 Személyes adatok védelme

A bizalmi szolgáltatók, különösen a tanúsítványkibocsátó szolgáltatók az aláírók személyes adatait szükségszerűen kezelik. A rendelet ezért megköveteli a **GDPR** (az Európai Parlament és a Tanács [EU] 2016/679 Rendelete [2016. április 27.] a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről [általános adatvédelmi rendelet]) rendelkezéseinek a betartását. Ennek eredményeként a szolgáltatók kizárólag közvetlenül az aláírótól vagy az aláíró engedélye alapján gyűjthetnek adatokat, és jogszabályi felhatalmazás alapján tárolhatják azt, Magyarországon a tanúsítványok lejáratát követő 10 évig. A szolgáltatók az aláíró adatait kizárólag a tanúsítványkibocsátás és -menedzsment céljából kezelhetik.

Nem a személyes adatok kezeléshez kapcsolódó kérdés, de a magánélet védelme szempontjából általában véve fontos az a rendelkezés is, amely szerint a tagállamoknak biztosítaniuk kell az aláírók számára azt a lehetőséget, hogy a tanúsítványok tulajdonosaiként esetleg ne a saját nevüket, hanem egy álnevet tüntessenek fel. Ily módon nem tilos az álnevek elektronikus tranzakciók során való használata, ennek során pedig az álnevek nemzeti jog szerinti joghatása sem sérül.

3.2.2.4 Elektronikus aláírás-létrehozó eszközök tanúsítása

Az eIDAS külön rendelkezik a minősített aláírás- és bélyegző-létrehozó eszközökről. Nem volt cél, hogy a rendelet kiterjedjen annak a rendszerkörnyezetnek az egészére, amelyben az ilyen eszközök üzemelnek, ezért a minősített aláírást és bélyegzőt létrehozó eszközök tanúsítását azon hardver-eszközökre és szoftverekre korlátozták, amelyek a legszűkebb értelemben véve az aláírás létrehozásához használatos adatok kezelésére és védelmére szolgálnak.

A tagállamok által kijelölt megfelelő állami vagy magánszerveknek tanúsítaniuk kell, hogy a minősített elektronikus aláírást létrehozó eszközök megfelelnek a rendelet II. mellékletben meghatározott követelményeknek. A terméktanúsító szervezetek elsősorban üzleti vállalkozások lehetnek, viszont nem kizárt, hogy terméktanúsítási tevékenységet állami hatóság is végezzen. Ez utóbbi esetben a hatóságot ugyanúgy kell kezelni, mintha egy üzleti vállalkozás lenne. Semmiképpen sem megengedett ugyanakkor az, hogy az a hatóság foglalkozzon terméktanúsítással, amely hatóság a hitelesítési szolgáltatást nyújtók felügyeletét ellátja.

A terméktanúsítók által kiállított megfelelőségi igazolásokat szintén tanúsítványnak hívják, ennek a tanúsítványnak az elnevezésén kívül azonban semmi köze sincs a bizalmi szolgáltatók által kiállított aláírási vagy bélyegzési célú tanúsítványokhoz.

Az értelmezési problémák elkerülése érdekében jelen könyv az *eszköztanúsítvány* fogalmat használja, amikor *egy terméktanúsító szervezet által kiadott tanúsítványát* kell említeni.

Gyakorló kérdések:

1. Mi az eIDAS két fő kérdésköre?
2. Milyen jogi elismerésre kötelezettek az uniós tagállamok?
3. Mi a garanciája a minősített elektronikus aláírást létrehozó eszközök magasabb biztonsági szintjének?

3.2.3 Az elektronikus aláírás nemzeti szabályozása Magyarországon

A **magyar elektronikus aláírási szabályozás** az uniós szabályozást egészíti ki, és határoz meg részletszabályokat az általános, és EU-ban érvényes szabályok mellett.

Az elektronikus aláírásokra és bélyegzőkre vonatkozó legfontosabb magyar jogszabály az elektronikus ügyintézésről és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény (Eübszt.). A törvény részletezi az elektronikus ügyintézésre vonatkozó előírások mellett a bizalmi szolgáltatókra vonatkozó követelményeket is.

Az első rész bevezető rendelkezései definiálják a fogalmakat, sokszor visszautalnak az eIDAS rendelet definícióira (pl. 1. § 2., 7., 10., 13., 20), biztosítva a két törvényi szintű jogszabály közötti konzisztenciát. A második rész az elektronikus ügyintézést biztosító szervezetek és az ügyfelek elektronikus kapcsolatának általános szabályait rögzíti. A VI. fejezet írja le a szabályozott elektronikus ügyintézési szolgáltatások (SZEÜSZ) nyújtásának szabályait, ideértve a Kormány által kötelezően biztosított szabályozott elektronikus ügyintézési szolgáltatásokat, a VII. fejezet pedig a központi szabályozott elektronikus ügyintézési szolgáltatásokat (KEÜSZ) részletezi. 2019-ben megjelent a központi állami szolgáltatás (KASZ) fogalma is. Az elektronikus ügyintézés felügyeletéről a IX. fejezet tartalmaz előírásokat. A harmadik részben az informatikai együttműködés alapelveit és követelményeit fekteti le a jogalkotó. Az 55. § alapján csak olyan informatikai fejlesztés valósulhat meg, amelyik képes a szabályozott és központi elektronikus ügyintézési szolgáltatásokkal való együttműködésre. A papíralapú dokumentumok teljes kiküszöbölését segíti, hogy az együttműködő szerv a csak papíralapon létező dokumentumokról elektronikus másolatot készíthet vagy készíttethet (59. § (3)). A XII. fejezetben az elsődleges információforrások kizárólagos használatának igénye jelenik meg. Ha közhiteles – vagy a törvény által elsődlegesnek tekinthető – adatforrás tartalmazza az ügyintézéshez szükséges adatokat, akkor azokat az elektronikusan együttműködő szerv köteles elektronikus úton ezekből az adatforrásokból azokat beszerezni, amivel az egyszeri adatszolgáltatás elve (’once-only’ principle) automatizált eszközökkel teljesíthető.

A törvény a bizalmi szolgáltatások nyújtásának feltételeit tárgyalja a XVI. fejezettől kezdődően. A szolgáltatókra, a tanúsítványokra és az ellenőrzésre vonatkozó szabályok között alapvető fontosságú jogi vélelmeket is megfogalmaz az elektronikus dokumentumokkal kapcsolatosan:

- minősített aláírással, bélyegzővel vagy időbélyegzővel ellátott dokumentum tartalmát változatlannak kell vélelmezni, amennyiben az aláírások ellenőrzése pozitív (97. § (1)),
- minősített bizalmi szolgáltató által megőrzött dokumentumok esetében vélelmezni kell (az ellenkező bebizonyosodásáig) azt, hogy az aláírás időpontjában az aláírás, bélyegző vagy időbélyegző érvényes volt (100. §).

Ezt ki kell egészíteni a papíralapú és az elektronikus dokumentumok átjárhatóságát biztosító vélelmekkel, amely szerint amennyiben az eredeti dokumentumról készült vagy készíttetett hiteles másolat bizonyító ereje megegyezik az eredeti dokumentum bizonyító erejével (12. §).

A törvény végrehajtásához és az itt definiált szolgáltatások működtetéséhez számos további részletszabály jelent meg, amelyeket az Elektronikus Ügyintézési Felügyelet a honlapján összegyűjtött és hozzáférhetővé tett a nyilvánosság számára (https://euf.gov.hu/kapcsolodo-

jogszabalyok-szeusz). Az elektronikus ügyintézésre vonatkozó legfontosabb szabályokat kiadásuk időrendi sorrendjében a következő jogszabályhelyek tartalmazzák:

- 414/2015. (XII. 23.) Kormányrendelet a személyazonosító igazolvány kiadása és az egységes arcképmás- és aláírás-felvételezés szabályairól,
- 137/2016. (VI. 13.) Kormányrendelet az elektronikus ügyintézési szolgáltatások nyújtására felhasználható elektronikus aláíráshoz és bélyegzőhöz kapcsolódó követelményekről,
- 24/2016. (VI. 30.) BM rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről, és a
- 451/2016. (XII.19.) Kormányrendelet az elektronikus ügyintézés részletszabályairól.

A jogszabályok időnként változnak, érdemes a frissítésekre olykor-olykor rákeresni.

3.2.3.1 Bizalmi szolgáltatások

A bizalmi szolgáltatásokat az eIDAS többé-kevésbé definiálja rendszerint díjazás ellenében nyújtott, az alábbiakból álló elektronikus szolgáltatásokként:

a) elektronikus aláírások, elektronikus bélyegzők vagy elektronikus időbélyegzők, ajánlott elektronikus kézbesítési szolgáltatások, valamint az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok létrehozása, ellenőrzése és érvényesítése; vagy

b) weboldal-hitelesítő tanúsítványok létrehozása, ellenőrzése és érvényesítése; vagy

c) elektronikus aláírások, bélyegzők vagy az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok megőrzése.

Fontos tudni, hogy elektronikus aláírás *létrehozása* sosem lehet bizalmi szolgáltatás. Mivel ez azt jelentené, hogy a tulajdonoson kívül más is hozzáférhet az aláírás-létrehozó adathoz így azt „*kompromittálódottnak*” kellene tekinteni, ami annak azonnali érvénytelenségét vonná maga után. Emiatt a távoli aláírások úgy lettek kialakítva, hogy a kulcsokat menedzselő minősített bizalmi szolgáltató a tulajdonos aktív közreműködése nélkül nem férhet hozzá az aláírás-létrehozó adathoz, vagyis önállóan nem használhatja aláírások létrehozására. Nem véletlen, hogy a terméktanúsításra vonatkozó szabályokat akkor is be kell tartani, ha az eszköz egy kulcsot képes tárolni, és akkor is, ha többmillió ügyfél kulcsát kell tárolnia. A biztonsági követelmények mindkét esetben ugyanazok és azok betartását minden esetben egy akkreditált tanúsító szervezet vizsgálja be és tanúsítja.

3.2.3.2 Az eszköztanúsítás szabályai

Az eIDAS a 30. cikkében rendelkezik a minősített elektronikus aláírást létrehozó eszközök, a 39. cikkében pedig a minősített elektronikus bélyegzőt létrehozó eszközök tanúsításáról. Ennek értelmében a tagállamok által kijelölt megfelelő állami vagy magánszerveknek kell azt tanúsítaniuk, hogy a minősített elektronikus aláírást vagy bélyegzőt létrehozó eszközök megfelelnek a rendeletben előírt biztonsági követelményeknek. A tagállamok tájékoztatják az Európai Bizottságot az általuk kijelölt állami vagy magánszerv nevéről és címéről, és a Bizottság ezt az információt a tagállamok rendelkezésére bocsátja. A tanúsításnak olyan biztonságértékelési eljáráson kell alapulnia, amelyet információtechnológiai termékek biztonságának értékelésére vonatkozó elfogadott szabványok egyikének megfelelően hajtottak végre. A tanúsítás meglétét az állami felügyelő hatóságok ellenőrzik.

Gyakorló kérdések:

1. Melyik nemzeti jogszabály foglalkozik a bizalmi szolgáltatásokkal?
2. Melyek a bizalmi szolgáltatások?
3. Milyen célt szolgál a minősített elektronikus aláírás- vagy bélyegző-létrehozó eszközök kötelező terméktanúsítása?

3.3 Az elektronikus aláírás működése

Az elektronikus aláírás jogi fogalom, a szabályozás során jött létre, technológiafüggetlen módon. Különbözik a digitális aláírástól, nem lesz annak szinonimája, mivel nem minden egyes elektronikus aláírás lesz digitális aláírás, és az ellenkező irányból megközelítve, nem minden digitális aláírás lesz elektronikus aláírás. Például a biometrikus aláírás, amelyet egy digitális aláírópadon digitális tollal készítünk, az elektronikus aláírás lesz, de távolról sem nevezhető digitális aláírásnak. Továbbá egy elektronikus bélyegző digitális aláírást tartalmazhat, azonban nem lehetséges elektronikus aláírásnak nevezni ezt, hiszen nem magánszemély állította elő. A két halmaznak tehát – elektronikus aláírások és digitális aláírások – van közös metszete, de vannak aláírások a metszeten kívül is, így a valóságban ténylegesen különböznek egymástól. Az elektronikus bélyegzőkre hasonló kijelentés fogalmazható meg, lesz a bélyegzőknek és a digitális aláírásoknak metszete, de lesznek olyan digitális aláírások, amelyek nem nevezhetők elektronikus bélyegzőknek.

3.3.1 A digitális és a nem digitális aláírások közötti különbségek

3.3.1.1 A digitális aláírás készítése

A digitális aláírások azok az eszközök, melyekkel az adatok jogosulatlan módosításai felderíthetőek, és használható az aláíró azonosítására is – egyszóval a hitelesítés módszeréül szolgálnak. Az aláírt adatok fogadója a digitális aláírást olyan eszközül használhatja, mely harmadik felek felé demonstrálja az aláírás tényét és annak az állított aláíró általi megtörténtét. Ez gyakorlatilag a letagadhatatlanságot jelenti, mivel az aláíró az aláírás tényét nehezen tudja letagadni egy későbbi időpontban, különösen akkor, ha az aláírás-létrehozó adat egyetlen egy példányban létezik, és az aláíró azt személyesen vette át, és őrzi azt.

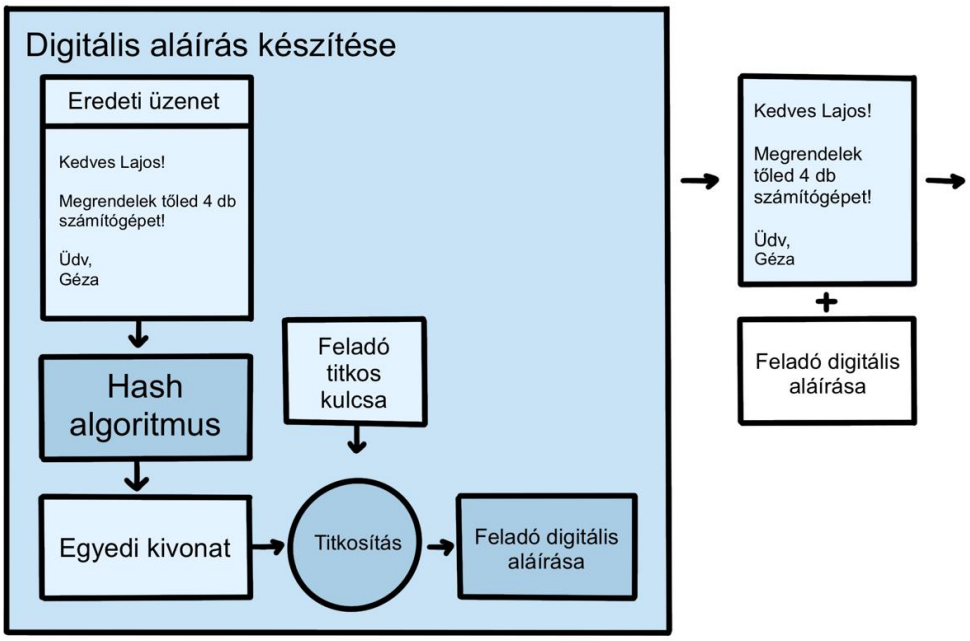
Az aláírás **elkészítésének** és fogadó oldali ellenőrzésének lépései az alábbiak:

1. az aláírandó adatokból elkészül annak fix (általában 160-512 bit) hosszúságú kivonata[3],
2. a kivonatot az aláíró algoritmus és a titkos kulcs segítségével rejtjelezi az alkalmazás, és ez lesz a digitális aláírás,
3. az aláírás kezdeti ellenőrzése automatikusan megtörténik,
4. a digitális aláírás az adatokhoz csatolva eljut a fogadóhoz.

A digitális aláírás abban különbözik a nyilvános kulcsú titkosítástól, hogy itt a titkos kulccsal történik az üzenet aláírása, a nyilvános kulccsal pedig az aláírás ellenőrzése – titkosításnál pontosan fordítva.

[3] Itt a FIPS 180-4 által leírt SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 és SHA-512/256 kivonatoló algoritmusokra gondolunk elsősorban. Ronald Rivest több Message Digest (MD) hash algoritmust írt le korábban, ezeknek 128 bit volt a kimenete (MD2 1989, MD4 1990, MD5 1991).

Az aláírás elkészítése úgy történik, hogy először is az aláíró a nyílt szövegből egy kivonatkészítő egyirányú függvénnyel (hash function) elkészíti az üzenet kivonatát. Ha a kivonat mérete nem megfelelő (kisebb, mint az aláírást végző algoritmus mérete), akkor az üzenetet egy **feltöltő** (padding) **algoritmus** segítségével kiegészítik a megfelelő méretre (nem minden aláíró algoritmus igényli ezt a beavatkozást). Ezt a lenyomatot kódolja a magánkulcsával, ez a kódolt bináris adat lesz a digitális aláírás. Az aláíró elküldi az eredeti kódolatlan üzenetet és az üzenetből készített kódolt lenyomatot a fogadó félnek vagy feleknek.



7. ábra: A digitális aláírás készítése

3.3.1.2 A digitális aláírás ellenőrzése

Az aláírás ellenőrzésénél alapvetően két ellenőrzési formát különböztetünk meg. A **kezdeti ellenőrzést** és az **utólagos ellenőrzést**. A kezdeti ellenőrzést az aláíró végzi, és az aláírást követően minél hamarabb el kell végezni annak érdekében, hogy azokat az információkat be lehessen gyűjteni, amelyek a hosszú távú ellenőrzés során érvényessé teszik az aláírást. Az utólagos ellenőrzést az elfogadó fél végzi, és az aláírás létrehozása után akár évekkel később is el lehet végezni. Itt nincs szükség más adatokra, mint amit az aláírás kezdeti ellenőrzése során már begyűjtöttünk – esetleg kiegészítve az aktualizált változatukkal.

Az aláírás készítésének utolsó lépéseként a küldő a digitális aláírást az adatokhoz csatolva eljuttatja azt a fogadóhoz, aki az alábbi módon, utólagosan **ellenőrzi**:

1. a fogadói oldalon a fogadó a fogadott üzenetből újra elkészíti a kivonatot,
2. a digitális aláírásból a nyilvános kulcs segítségével visszaállítja az eredeti kivonatot,
3. a fogadó az új kivonatot és az eredeti kivonatot összehasonlítja, és ha egyezik, akkor az aláírás rendben van, ha nem egyezik, akkor pedig az aláírás elfogadását – alapesetben – meg kell tagadni.

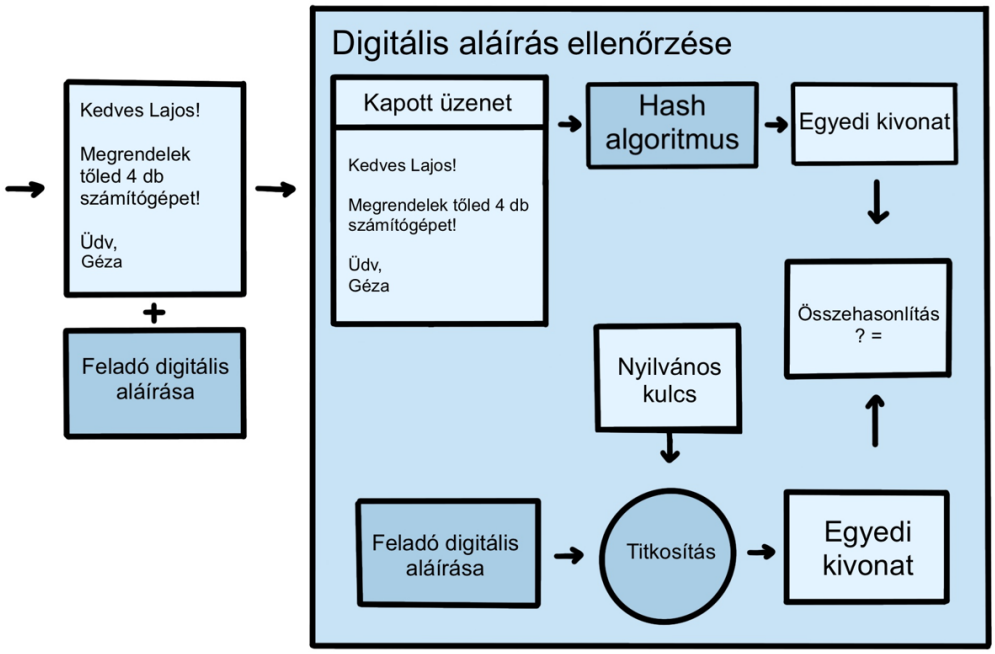
A digitális aláírás **sikeres ellenőrzéséből** az alábbiak következnek:

- az aláírt adatok ugyanazok, amit a küldő elküldött, menet közben nem változtak,
- az adatok aláírását a nyilvános kulcshoz tartozó titkos kulccsal végezték, és
- amennyiben a nyilvános kulcshoz létezik tanúsítvány, és tanúsítványban szereplő névhez tartozó személyt megbízható módon kapcsolták, akkor az a fizikai személy is ismert, aki aláírta az adatokat.

A digitális aláírás ellenőrzésének **sikertelensége** esetén az alábbiak lehetnek – a teljesség igénye nélkül – az okok:

1. az adatok a küldés során megváltoztak,
2. az ellenőrzéskor más kulcsot vagy algoritmust használtak,
3. a tanúsítványt nem tette a fogadó még megbízhatóvá a saját rendszerében,
4. a tanúsítvány lejárt,
5. a nyilvános kulcshoz tartozó tanúsítvány hibás.

Az ellenőrzés sikertelensége okán kapott hibaüzenet behatárolhatja a hiba pontos okát, ami segít az aláírás ellenőrzésének későbbi sikeres megvalósításában. A megfontolt és körültekintő eljárás indokolt, mivel az érvénytelen aláírás elfogadásából adódó minden következmény az elfogadót terheli.



8. ábra: A digitális aláírás ellenőrzése

Az aláírás ellenőrzése végződhet az ellenőrzésre vonatkozóan nem sikeres (sikertelen vagy nem végrehajtható) eredménnyel, aminek tehát sokféle lehetséges oka lehet. Ebben az esetben az üzenet újra küldése vagy más csatornán történő ellenőrzése lehet a megoldás. Fontos, hogy az ilyen üzenet elfogadásából származó összes felelősség az elfogadót terheli.

3.3.1.3 A megbízható harmadik fél

A digitális aláírás biztosítja az üzenet sértetlenségének és eredetének a megállapíthatóságát. Azonban mindaddig nem biztosítja az aláíró azonosságát, amíg azt egy megbízható harmadik fél nem igazolja, hogy az aláírás-létrehozó adat kinek lett odaadva. A minősített elektronikus aláírás egyik nagyon fontos tulajdonsága a letagadhatatlanság. Ez különösen abban az esetben fontos, ha az adott dokumentumban valamilyen kötelezettségvállalás is szerepel. A minősített elektronikus aláírással ellátott dokumentum biztosít afelől, hogy az aláíró személy ne tudja letagadni a dokumentum aláírását és a dokumentumban szereplő kötelezettség felvállalását, illetve a kötelezettséget utólag ne tudja másra áthárítani. Ennek szigorú feltételei léteznek. Az egyik ilyen a *megbízható tanúsítvány*, ami biztosítja *az aláíró kulcs feletti kizárólagos rendelkezést*. A tanúsítvány egy megbízható fél igazolása arról, hogy az aláíró kulcs az adott személy birtokában van. A magánkulcs biztonságáról azonban a kulcs tulajdonosának kell gondoskodnia. Az aláíró kulcs tárolható a számítógépen, de ezzel különböző veszélyeknek van kitéve. Ezek elhárítása érdekében alkalmazzák a minősített aláírás-létrehozó eszközöket (MALE), amik általában intelligens kártyák, smartkártyák (chipkártyák, SIM-kártyák) – távoli aláírás esetében hardveres biztonsági modulok – vagy kriptotokenek. Ezeken tárolva a magánkulcsot csupán arra kell vigyázni, hogy az eszköz – különösen a hozzáférési jelszóval együtt – ne kerüljön illetéktelen felhasználó kezébe. Fontos itt megjegyezni, hogy a minősített aláírás-létrehozó eszközök jellemzően egyetlen egy példányt tartalmaznak az aláírás-létrehozó adatból, és mivel nem lehet azt belőlük kinyerni, a használata egyértelműen ahhoz a személyhez köthető, akinek az eszközt biztonságos úton átadták.

Gyakorló kérdések:

1. Mi a különbség a digitális és az elektronikus aláírás között?
2. Hogyan működik a digitális aláírás?
3. Milyen következtetéseket lehet levonni a digitális aláírás ellenőrzésének eredményéből?

3.3.2 A digitális aláírási séma

A digitális **aláírási sémát**, mint gyűjtő fogalmat használják a digitális aláírások témakörében. Létezésüket az indokolja, hogy egy aláírás elkészítése során több algoritmusra is szükség van, és ezek variálhatóak, így az egységes használat érdekében fontos volt ezek sémába szervezése. Ebben a könyvben a digitális aláírási séma fogalmát a digitális aláírás folyamatában részt vevő algoritmusok együttes elnevezéseként használjuk, az ETSI TS 102 176-1 szerinti értelmezésben.

Az aláírási séma a következő elemekből tevődik össze:

- kulcsgeneráló algoritmus,
- ellenőrző, aláíró algoritmus,
- feltöltő algoritmus (padding function),
- kivonat készítő eljárás (hash function).

Sok helyen a séma csupán a kulcsgeneráló, az aláíró és az ellenőrző algoritmust tartalmazza. Ha az aláírási sémát kiegészítjük a feltöltő (padding) és a kivonatkészítő (hash) algoritmusokkal is, akkor az **aláírási készlet** (signature suit) fogalmát kapjuk meg. Az algoritmusok egymáshoz való különböző társításának nincs gyakorlati akadálya, ezért többféle aláírási

séma létezik. Ezek ismerete azért fontos, mert az elektronikus aláírás készítője a tanúsítvány igénylésekor saját maga választhatja ki, hogy milyen konfigurációt, algoritmusokat kíván használni. Különböző felhasználási célterületekhez más-más séma működhet, és a különböző eljárások nem feltétlenül kompatibilisek egymással az eltérő algoritmusok miatt. A leggyakrabban használt sémákat azonban minden elterjedt program képes azonosítani, így például a kormányzati aláíró és aláírás-ellenőrző programot (KEAASZ) is.

3.3.2.1 Kulcsgenerálás, gyakran használt algoritmusok és jellemzőik

Ebben a fejezetben röviden bemutatjuk a leggyakrabban használt kriptográfiai algoritmusokat és jellemzőiket. A megfelelő tulajdonsággal bíró kriptográfiai algoritmusok adják annak a tudományosan (matematikailag) bizonyított hátterét, hogy miért lehet megbízni az adott kriptográfiai művelet eredményében. A lista természetesen nem teljes, hiszen folyamatosan jelennek meg újabb algoritmusok, és várhatóak is újabbak – különös tekintettel a kvantumszámítógépekre.

1 **RSA kulcspár:** az RSA algoritmus az egész számok faktorizációjának (prímfelbontásának) matematikai problémáján alapszik. A kulcsok előállításához két véletlen és egymástól teljesen független prímszámot kell generálni, ezekből lesznek megképezve a kriptográfiai kulcsok, amelyek matematikai értelemben egymás párjai lesznek az adott műveletsorozatban. Akkor jó a kulcspár, ha a kulcstér elegendően nagy, az egyik kulcs nem számítható ki a másikból, és belátható időn belül nem is lehet kitalálni a titkos kulcsok értékét. Ha egy ilyen kulcsot valaki aláírás-létrehozó adatként birtokol egy minősített aláírás-létrehozó eszközön, akkor elméletileg csak egyetlen egy ilyen kriptográfiai kulcs létezhet az egész világon[4]. Ezzel a kulccsal a letagadhatatlanság biztosítható, hiszen nincs másnak esélye a használatra.

2 **DSA kulcspár:** a DSA algoritmus a diszkrét logaritmus kiszámításának problémáján alapszik a prímszámok és a szorzás művelet által alkotott matematikai csoportban. (Diszkrét logaritmus az logaritmus, ahol a logaritmus számításakor egész számokat használunk alapként, kitevőként és eredményként is.) A prímszámokon túl itt véletlen egész számokat is alkalmaznak a visszafejthetőség megnehezítésére.

3 **ECDSA és ECGDSA:** ezeknek a függvényeknek a segítségével történő aláírás a diszkrét logaritmus matematikai problémájának alkalmazása elliptikus görbék (EC) pontjaira. A paraméterek megválasztásának bemutatását, a kulcsok működését és a kulcsok előállításához szükséges lépéseket az ETSI TS 102 176-1 V2.1.1 (2011-07) megnevezésű szabvány tartalmazza.

3.3.2.2 Aláíráshoz és ellenőrzéshez használt eljárások

A műszaki világban a digitális aláírások készítéséhez és ellenőrzéséhez számos algoritmust használnak, amelyeknek változó a piaci elterjedése. A leggyakrabban használt algoritmusokat az alábbi táblázat mutatja be. Az algoritmusok elterjedése a számítási kapacitások növekedésével együtt folyamatosan változik.

[4] Mivel a világ összes hitelesítésszolgáltatói tanúsítványtárának az összehasonlítása nem megvalósítható a gyakorlatban, az egyes szolgáltatókat meglehetősen nagy kulcstér előírásával, és a már kiadott kulcsok újra felhasználásának tiltásával kötelezik az egyediség biztosítására. Továbbá ha a szolgáltató a felhasználó nevében előzetesen hozza létre az aláírás-létrehozó adatot (titkos kulcsot), garanciákat kell arra nézve is nyújtania, hogy nem őriz meg és nem ad át titkos kulcsokat a tulajdonos tudta és engedélye nélkül senkinek sem.

Aláíró algoritmus rövid neve	Kulcs- és paraméter-előállítási algoritmusok	Normatív hivatkozás
rsa	rsagen1	RFC 3447
dsa	dsagen1	FIPS Publication 186-2, ISO/IEC 14888-3:2006
ecdsa-Fp	ecgen1	ANSI X9.62
ecdsa-F2m	ecgen2	ANSI X9.62
ecgdsa-Fp	ecgen1	ISO/IEC 15946-2 (2002)
ecgdsa-F2m	ecgen2	ISO/IEC 15946-2 (2002)

4. táblázat: Aláíró és ellenőrző algoritmusok

3.3.2.3 Kivonatoló függvények és jellemzőik

Egy kriptográfiai lenyomatképző, kivonatképző vagy idegen szóval 'hash' függvénynek a következő elvárásokat kell teljesíteni ahhoz, hogy biztonságosnak legyen minősíthető:

- egy adott elektronikus dokumentum lenyomatának ismeretében gyakorlatilag nem lehetséges a lenyomatból a dokumentumot visszaállítani (**egyirányúság**),
- egy adott elektronikus dokumentum és az ebből a dokumentumból készült lenyomat ismeretében gyakorlatilag nem lehetséges olyan másik elektronikus dokumentumot előállítani, amely az eredetitől eltér, azonban a belőle származtatott lenyomat azonos volna a már ismert lenyomattal, azaz gyakorlatilag lehetetlen két olyan, egymástól értelmesen különböző elektronikus dokumentumot előállítani, amelyek lenyomata azonos (**ütközésmentesség**),
- ha az eredeti dokumentum egy bitje megváltozik, a hash-értéknek egytől több bitben kell megváltoznia (**lavinahatás**).

A következő táblázat az elfogadott kivonatoló függvényeket sorolja fel az ETSI TS 119 312 V1.4.3 (2023-08) alapján.

A kivonatképző függvény neve	A függvényre vonatkozó normatívák	Kivonat hossza (bit)
SHA-224	FIPS Publication 180-4	224
SHA-256	FIPS Publication 180-4	256
SHA-384	FIPS Publication 180-4	384
SHA-512	FIPS Publication 180-4	512
SHA-512/256	FIPS Publication 180-4	512/256
SHA3-256	FIPS Publication 202	256
SHA3-384	FIPS Publication 202	384
SHA3-512	FIPS Publication 202	512

5. táblázat: Kivonatoló (hash) algoritmusok

3.3.2.4 Teljes felépített sémák

Az algoritmusoknak az elektronikus aláírások biztonságát esetlegesen kedvezőtlenül befolyásoló egymásra gyakorolt hatásai miatt a biztonságos elektronikus aláírás céljára használható kriptográfiai algoritmuskészlet komponensei és paraméterei szabványosítottak, és a szabványok szerint kizárólag a táblázatokban megadott kombinációkban alkalmazhatók. Néhány példa elfogadott sémákra:

1) Séma neve: sha256 – with rsa
   a) hash: sha-256
   b) aláíró algoritmus: rsa

2) Séma neve: sha3-with-ecdsa
   a) hash: SHA3-256, SHA3-384, vagy SHA3-512
   b) aláíró algoritmus: EC-DSA

Gyakorló kérdések:

1. Mit tartalmaz a digitális aláírási séma?
2. Melyek a leggyakrabban használt algoritmusok?
3. Mik a jellemzői a kivonatoló (hash) függvényeknek?

4 Publikus Kulcsú Infrastruktúra, PKI

4.1 Kriptográfiai alapismeretek

A **p**ublikus (nyilvános) **k**ulcsú **i**nfrastruktúra (**PKI**) megértéséhez először a történelmi múltba kell visszamenni, mégpedig a kriptográfia, a titkosítás technikájának történelmébe.

Régen az üzeneteket a háborúban és egyéb hétköznapi esetben úgynevezett **egykulcsos titkosítással** titkosították. Ez azt jelentette, hogy az információ titkosításához (kódolás) és megfejtéséhez (dekódolás) egy kulcsot használtak. Ennek az volt a következménye, ha a kulcs, a kódolási eljárás illetéktelen kézbe kerül(t), akkor azt más is el tudta olvasni, sőt a kódolási eljárás ismeretében hamis üzenetet tudott létrehozni.

Ilyen egykulcsos eljárás például, hogy mindkét fél (a küldő és a címzett) egy adott könyvből dolgozott, és a küldő a betűk helyett az adott könyv oldalszámát, a sor számát és balról jobbra a betűszámot adta meg. Természetesen a modern informatikai környezetben is sokszor használunk még egykulcsos titkosítást, mert nagy előnye, hogy gyors, így nagy adattömeg esetében (pl. mozgókép) is ez a javasolt módszer. Nagy hátránya – mint minden kulcsmegosztás nélküli kriptográfiai védelemnek, hogy ha a teljes megfejtő kulcs illetéktelenek kezébe kerül, akkor az üzenet (minden olyan üzenet, amit ezzel a kulccsal titkosítottak) megfejthető, és hamis üzenet állítható elő.

A matematika előrehaladásával kifejlődtek olyan eljárások, melyek lehetővé tették az egy kulcspár = két kulcs létrehozását a titkosítási folyamathoz, kialakult a **kétkulcsos titkosítás**.

A két kulcsot az alábbiak jellemzik:

- az első kulcshoz mindig ugyanaz a második kulcs hozható létre,
- a második kulcsból nem hozható létre az első kulcs,
- ha elég nagy a kulcs (sok bitből áll), akkor a nyers feltörés módszerével (brute force, amikor is egyesével végigpróbálják az összes lehetséges megoldást) belátható időn belül nagy valószínűséggel nem jutnak eredményre a támadók.

A mindennapokban ez a matematikai felfedezés használható a titkosításra és a sértetlenség igazolására is. A titkosítás során, amikor egy nem nyilvános (titkos) üzenetet szeretne kapni egy felhasználó, meg kell kérnie az üzenet küldőjét, hogy a fogadó fél nyilvános kulcsával rejtjelezze az üzenetet, majd így küldje azt el. Ahhoz, hogy valaki tudjon egy ilyen **titkosított üzenetet** értelmezni, először is rendelkeznie kell egy kulcspárral, majd a privát (vagy titkos) kulcsot biztonságos módon el kell tárolnia, hiszen azzal tudja megfejteni a neki érkező üzenetet. A kulcspár másik elemét meg el kell küldenie vagy hozzáférhetővé kell tennie azok számára, akiktől a titkos üzenetet várja. Ha a küldő a nyilvános kulccsal titkosította az üzenetet, akkor azt csak a titkos kulcs segítségével lehetséges elolvasni. Ha a titkos kulcs őrzése megfelelően biztonságos, akkor ez egyenértékű azzal a megállapítással, hogy a titkos üzenetet csak a példában adott felhasználónk volt képes elolvasni, mindenki más számára a titkos üzenet csak egy értelmetlen zagyvalék lesz.

Amikor az a cél, hogy egy elektronikus dokumentum **sértetlenségét**, azaz a tartalom változatlanságát és a forrás eredetiségét együttesen bizonyítsuk, a kétkulcsos technológiát szintén alkalmazhatjuk. Ez egy olyan eljárás, amelyben az aláíró, a titkos kulcs birtokosa, az aláírás során a titkos kulccsal rejtjelezi az üzenetnek a kivonatát, és elnevezi ezt **digitális alá-**

írásnak, az ellenőrző (fogadó) pedig a nyilvános kulccsal tudja ellenőrizni ezt az aláírást. Fontos, hogy ne keverjük össze az aláírást a titkosítással, míg az aláírás során a tulajdonos a titkos kulcsot használja, addig a titkosításnál a partnerek a nyilvános kulcsot használják az üzenet előállításához. Ennek megfelelően a fogadó oldalon az aláírás ellenőrzéséhez a nyilvános kulcsra, míg a titkos üzenet elolvasásához a titkos kulcsra van szükség.

Tekintettel arra, hogy a nyilvános kulcs önmagában csak egy számsor, információt a számsor birtokosáról nem tartalmaz, ezért további elemre, elemekre van szükség ahhoz, hogy tudni lehessen, kihez tartozik az a nyilvános kulcs. Erre jött létre a **tanúsítvány**. A tanúsítványban szereplő adatokat – a sértetlenségük megőrzéséhez ugyanezt a technológiát alkalmazva – digitálisan aláírják.

A tanúsítvány a következő főbb részekre tagolódik:

- a felhasználó nyilvános kulcsa,
- a felhasználó adatai,
- a tanúsítványkiállító adatai,
- a tanúsítványkiállító nyilvános kulcsa,
- tanúsítványhoz kapcsolódó egyéb információk (pl. sorszáma, érvényesség időtartama, a tanúsítvány felhasználási köre stb.).

A tanúsítvány tehát a nyilvános kulcsot (egy egyedi számsort) köti össze fizikai birtokosának hiteles adataival, feldolgozható, szabványos formában. A tanúsítvány kiadását a **tanúsítványkibocsátó** (Certificate Authority, CA) végzi. A magyar szóhasználatban a **hitelesítésszolgáltató** szervezetet is szokás CA-nak nevezni, de itt nemcsak a tanúsítvány kibocsátásának folyamatát végző egységet, hanem az ehhez kapcsolódó összes tevékenységet (regisztráció, tanúsítványkibocsátás, tárolás, visszavonás, felfüggesztés, adatok megőrzését) végző szervezetet is jelentheti. A könyv terminológiájában szükséges különbséget tenni a tanúsítványkibocsátási funkció és a tanúsítványkibocsátási (hitelesítés)szolgáltatás között, mégpedig oly módon, hogy az előbbi valódi része az utóbbinak. A fenti különbségtétel jogosságát igazolja a regisztrációs szervezet (Registration Authority) külön említése és feladatainak tárgyalása is a vonatkozó szakirodalomban. Azaz léteznek olyan szervezetek, amelyek kizárólag az ügyfelek azonosításával foglalkoznak, és nem ők bocsátják ki a tanúsítványokat az ügyfelek részére.

A PKI alapja az erős központosítottság. A központi folyamat, ami köré minden más szerveződik, a tanúsítványkiadás, amikor is a digitális tanúsítványba a nyilvános kulcs és a tulajdonos adatai bekerülnek, és azt a kibocsátó az aláírásával hitelesíti. A tanúsítványokat kibocsátó bizalmi szolgáltató (**hitelesítésszolgáltató)** az a kitüntetett szervezet (szervezeti egység, magán- vagy jogi személy), amely a PKI elemeit működtetve a szükséges fizikai, szervezési és humán hátteret kialakítva a PKI elemek funkcióit felhasználva végzi **a bizalmi szolgáltatásait** – beleértve a tanúsítványkiadást is – az adott helyen, időben és módon[5].

[5] A centralizált szolgáltatások felvetik azt a kérdést is, mennyire lehet megbízni egy hitelesítésszolgáltatóban, ha az senki által sem felügyelt, vagy állami felügyelet alatt álló profitorientált szervezet, amelyet akkreditált tanúsító szervezet tanúsított, ez utóbbi a műszaki feltételek teljesítését hivatott igazolni. A bizalmi kérdés mellett itt a joghatás is megjelenik. Ha valaki nem bízna meg az állam által felügyelt minősített bizalmi szolgáltatásokban, azokkal ettől függetlenül még teljes bizonyító erejű magánokira-

A tanúsítvány összeköti a fizikai személy által birtokolt privát kulcshoz tartozó nyilvános kulcsot, azaz az ezek által képviselt elektronikus „virtuális” világot a „való” világgal azáltal, hogy a hitelesítésszolgáltató a nyilvános kulcson elhelyezett aláírásával igazolja a nyilvános kulcshoz csatolt „való” világ (jelen esetben a kérelmező fizikai) adatainak hitelességét. Egy nyilvános körben kibocsátott tanúsítvány aláírása ezért egy komoly **kötelezettségvállalás** is, melyet a hitelesítésszolgáltató tesz meg és nyilvánít ki a felhasználói közösség, leginkább az elfogadók felé. A kötelezettségvállalás lényege, hogy a tanúsítványban szereplő adatokat a hitelesítésszolgáltató egyrészről megbízható módon állította elő, másrészről a fizikai személy adatait – az előírt módon – ellenőrizte és megfelelően hitelesnek találta. A hitelesítésszolgáltatónak emiatt tehát nemcsak a tanúsítvány kiadását (mivel az csak az egyik részfolyamat), hanem az összes kapcsolódó folyamatot is biztonságos módon kell végeznie, kiemelve a felhasználók azonosítását és adatainak magas szintű ellenőrzését.

A hitelesítésszolgáltató azért lesz **hiteles szereplő** a közösség számára, mert a felhasználói közösség megbízik benne. Ez igaz az első komoly incidensig, más szóval az első csalódásig, utána csak kérdőjelekkel és fenntartásokkal működhet, ha egyáltalán működőképes egy bizalomra épülő szolgáltatás súlyos incidenst követően.

A bizalom alapja alapvetően az, hogy

- a hitelesítésszolgáltató biztonságos eljárást alkalmaz annak ellenőrzésére, hogy a titkos kulcs az igénylőnél van (a nyilvános kulcshoz a tanúsítványt tényleg az kéri, aki arra jogosult),
- a tanúsítványban szereplő adatok hitelesek, azt a hitelesítésszolgáltató körültekintően ellenőrizte (személyes adatokat, a bemutatott okmányokat, szervezeti okmányokat, esetleg meghatalmazásokat stb.),
- a hitelesítésszolgáltatásokhoz tartozó informatikai rendszert nagy biztonsággal üzemelteti (nagyfokú rendelkezésre állás, mentés, naplózás stb.),
- folyamatos szolgáltatást nyújt a tanúsítványok felfüggesztéséhez, visszavonásához, publikálásához,
- szervezeti felépítése lehetővé teszi a rendszer megfelelő működését (szabályzatok, megfelelő képzettségű és számú munkatárs, pénzügyi garanciák stb.),
- a fentiek meglétét, megfelelőségét független, akkreditált szervezetek folyamatosan ellenőrzik, tanúsítják.

Magyarországon a Nemzeti Média- és Hírközlési Hatóság (NMHH) az az európai felügyeleti szervezet, amely az eIDAS hatálya alá tartozó bizalmi szolgáltatásokat nyújtó bizalmi szolgáltatókat felügyeli, azaz működésüket nyilvántartásba veszi, és azt folyamatosan ellenőrzi.

Nemzetközi szinten az egyik legismertebb auditszervezet a Chartered Professional Accountant (CPA) Canada és az általa felügyelt WebTrust metódus, amely a bizalmi szolgáltatók által működtetett rendszerek szakmai követelményeknek való megfelelőségi vizsgálatához ad támpontot. Az általa felhatalmazott könyvvizsgálók által bevizsgált szolgáltatókat nemzetközi szinten is elfogadják, ezért jogosultak a népszerű böngészőkbe (pl. Firefox, MS Edge, Opera) a nyilvános kulcsaikat mint megbízható hitelesítésszolgáltatók kulcsait a megfelelő

tok hozhatók létre. Nyilvánvaló módon egy nem kontrollált szolgáltatáshoz nem lesz teljes bizonyító erő hozzárendelve a jogrendszerben.

kulcstárba elhelyezni. Ezek a garanciális követelmények csökkentik a csalások bekövetkezését, és növelik a megbízható működést. Ennek következményeként elegendő, ha egy felhasználó hiteles forrásból rendelkezik a hitelesítésszolgáltatók nyilvános kulcsaival, mert ekkor az azokkal aláírt tetszőleges tanúsítványt egyszerű módon tudja ellenőrizni. Ezeknek a tanúsítványoknak a számítógépes rendszerekben történő alapértelmezett elfogadása további következményeket is jelent:

- a felhasználó a továbbiakban **automatikusan** megbízik a bevizsgált hitelesítésszolgáltatókban, hogy csak olyan tanúsítványokat adnak és adtak ki, amelyekben valós adatok szerepelnek,
- a felhasználó a bevizsgált hitelesítésszolgáltatók által kibocsátott **minden** (személyes, eszköz és szervezeti) tanúsítványban automatikusan megbízik,
- a felhasználónak vagy a vállalatának a számítógépes rendszere telepítésekor – mivel a bevizsgált szervezetek tanúsítványainak feltöltése automatikus – a fentiekről **nincs is tudomása**.

Gyakorló kérdések:

1. Mi a különbség az egykulcsos és a kétkulcsos titkosítás között?
2. Mi a különbség a kétkulcsos titkosítás és a digitális aláírás között?
3. Mi a tanúsítvány-kibocsátókba vetett bizalom alapja?

4.2 A PKI elemei

A következő részben átfogó jelleggel ismertetjük a korábban már érintőlegesen említett, a technológia biztonságos működtetésében részt vevő elemeket, folyamatokat és szereplőket.

4.2.1 Publikus kulcsú infrastruktúra

A PKI egy olyan keretrendszer, amely tartalmazza a szükséges protokollokat a bizalmi szolgáltatások nyújtásához, és amely eszközöket biztosít a kulcsok generálására, a tanúsítványokhoz való hozzájutáshoz, valamint az ellenőrzés és a visszavonás megvalósítására, illetve szabályozására is.

Mivel a PKI a bizalomra épül, ezért a nyilvános kulcsok **tárolásának** két lehetséges technológiai formája van:

- **decentralizált:** a nyilvános kulcsok tárolását egy viszonylag laza együttműködés határozza meg, nincs kijelölt, elsődleges tárolóhely;
- **centralizált:** azaz a nyilvános kulcsok tárolását egy központi szervezet (hitelesítésszolgáltató) végzi, a nyilvános kulcshoz tartozó adatokat hitelesíti.

Decentralizált rendszerre példa a már említett PGP[6], melynek jellemzője, hogy a nyilvános kulcsokat nem egy központi hely (tanúsítványkibocsátó) hitelesíti, hanem egymás kulcsait hitelesíthetik a PGP-felhasználók. A hitelesítés módja a kulcs további aláírása. Egy PGP-kulcsot akárhány más kulccsal alá lehet írni, amiket újabb kulcsok hitelesíthetnek és így tovább. Ilyen módon egy „bizalmi háló” alakul ki. A PGP-kulcsokhoz e-mail címek tartoznak,

[6] PGP: Pretty Good Privacy, Philip Zimmermann fejlesztette ki 1995-ben, a felhasználók személyes adatainak védelmére alkalmazta a nyilvános kulcsú titkosítást, hitelesítést.

mint a kulcs birtokosainak egyedi azonosítói. Arra azonban, hogy valaki, aki kovacs@valahollakik.hu-nak mondja magát, valóban Kovácsnak hívják-e és van köze a Valahollakik tulajdonsághoz Magyarországon, nincs közvetlen biztosíték, más szóval a tulajdonos fizikai, személyi adatainak ellenőrzése nem közvetlen módon valósul meg ebben a rendszerben.

Centralizált rendszerre példa az összes magyarországi minősített bizalmi szolgáltató.

4.2.2 Hierarchikus felépítés

A tanúsítványkibocsátók **hierarchikus** felépítése a centralizált működési módból és a központok közötti kapcsolatok jellegéből következik. Alapvető igény, hogy egy olyan szervezet adja ki a tanúsítványokat, amelyikben mindenki megbízik. A felhasználók számában jelentős különbségek lehetnek, lehet nagyon kevés, és lehet nagyon sok felhasználó is, ezen kívül az igények is eltérnek, sőt a tanúsítványtípusok is különbözőek, ezért a felhasználók köre és a hierarchia felépítése szempontjából többféle megoldás alakult ki a gyakorlatban.

Felhasználói kör szerint az alább megadott csoportosítás végezhető el a szolgáltatók körében.

1) Saját belső szolgáltató

Amikor egy vagy több szervezet munkatársai, eszközei csak ezen a körön belül kiadott tanúsítványokat akarják használni – akár határokon átnyúlóan is, akkor a szervezet felállíthat saját, zárt hitelesítésszolgáltatót. Ebben az esetben a tanúsítványok hitelességét a szervezeti egység létrehozott szabályzata határozza meg, és ez írja le a kibocsátás menetét és azt, hogy hol és hogyan használhatók a tanúsítványok.

Például saját hitelesítésszolgáltatót állíthat fel egy nagyobb multinacionális cég (optimálisan több száz vagy ezer főre) az egymás közötti belső levelezés hitelességének biztosításához, vagy az informatikai rendszerbe való távoli bejelentkezéshez. Figyelemmel kell arra lenni, hogy ez a kommunikáció a szervezeten kívül a legtöbb esetben nem bír jogi vélelemmel.

2) Nyilvános szolgáltató

Amikor minden fél a PKI technológiát kívánja használni, de jogi, anyagi, kényelmi, bizalmi okból a zárt belső megoldás nem jön szóba, akkor egy nyilvános bizalmi szolgáltatót kell választani. A nyilvános bizalmi szolgáltatók esetében a szolgáltató egy független harmadik fél. Mindenki számára azonos feltételeket, azonos színvonalú szolgáltatást nyújt, és a bizalmat a legtöbbször egy független körülmény (jogszabály, ellenőrzés, audit) alapozza meg. Egy bizalmi szolgáltató akár többféle tanúsítványt is kibocsájthat. Erre példa minden olyan hitelesítésszolgáltató, amelyiknek van egy vagy több minősített, és egy vagy több nem minősített tanúsítványkibocsátási funkciója is.

4.2.2.1 Fastruktúra

A PKI rendszerben a végfelhasználói és szolgáltatói tanúsítványokat kibocsátó rendszerek struktúrába szerveződnek, amelyek közül a fastruktúra a legegyszerűbb. Itt egy legfelső szintű kibocsátó alatt helyezkednek el a köztes kibocsátók, amelyek ellátják a végfelhasználókat tanúsítványokkal.

Problémát jelenthet, ha egy kibocsátó adja ki az összes tanúsítványt, ugyanis, ha valamilyen technikai probléma kapcsán a kibocsátói kulcs(pár) megsérül vagy kompromittálódik, akkor az összes kiadott és még érvényes tanúsítványt vissza kell vonni, és újakat kell kiadni (az azonosítás újbóli elvégzésével).

Másrészről az is probléma, hogy ha két felhasználó két különböző fastruktúrában kapott tanúsítványt, hogyan biztosítható az átjárás a két struktúra között? Erre az a megoldás jött létre a gyakorlatban, hogy a szolgáltatók egymás nyilvános kulcsait is **hitelesíthetik**, erre a célra szintén tanúsítványokat adhatnak ki. Ez egyben azt is jelenti, hogy ha ismert egy hitelesítésszolgáltató nyilvános kulcsa, akkor annak alapján az általa hitelesített hitelesítésszolgáltatókét is le lehet ellenőrizni, ezekkel pedig azokét, akik számára ők bocsátottak ki tanúsítványt és így tovább. Ennek megfelelően új, összetett hitelesítési láncok, bizalmi útvonalak alakulhatnak ki közöttük. Ennek az az előnye, hogy a kereszthitelesítéssel mindkét struktúrában elfogadható hitelesnek a másik struktúrában kibocsátott összes érvényes tanúsítvány további művelet nélkül, mivel, ha egy láncolatban lévő szolgáltatót elfogadtak, mint megbízható szolgáltatót, ezzel automatikusan az ezalatt kibocsátott vagy a jövőben kiadott szolgáltatói és végfelhasználói tanúsítványokat is megbízhatónak fogadta el a felhasználó.

Az egymást (és a felhasználókat) hitelesítő szolgáltatók közötti hitelesítési kapcsolatok révén egy **hierarchikus hálózat** jön létre. Ebben a különböző hitelesítésszolgáltatóknak más-más szerepköre lehet: vannak hitelesítésszolgáltatók, amelyek csak hitelesítésszolgáltatók számára adnak ki tanúsítványokat; vannak, amelyek kizárólag a felhasználók számára, és akadnak, amelyek vegyesen. Vannak kitüntetett, „a hierarchia csúcsán álló” hitelesítésszolgáltatók, ezeket hívják magyarul **legfelső** vagy **gyökér-hitelesítésszolgáltatónak,** angolul **Root-CA**-knak. Az ilyen szolgáltatók nyilvános kulcsának hiteles beszerzése tehát a legpraktikusabb (és egyben a legnagyobb feladat). A gyakorlatban ezt úgy oldják meg, hogy az aláírt dokumentumokat kezelő szoftver (pl. MS Edge, Google Chrome vagy Firefox) telepítőcsomagjában már eleve elhelyezik néhány legfelső szintű szolgáltató (és esetenként több más tanúsítványkibocsátó) nyilvános kulcsát tartalmazó aláírt tanúsítványát is. Ezek segítségével a később beszerzett – és ezek által kibocsátott – tanúsítványok már ellenőrizhetők lesznek.

4.2.3 Egy PKI-rendszer felépítése

Az eddigiekből már látható, hogy a PKI-rendszerek funkciói igen különbözőek is lehetnek. továbbá két PKI-rendszer nem lesz teljes mértékben azonos, mivel a megvalósítás során számos különböző funkcionalitásból lehet választani a vonatkozó szabványok szerint, a rendszer céljának megfelelően. A választható funkciókat az alábbiak szerint lehet összefoglalni:

1. elektronikus aláírás készítése és ellenőrzése,
2. elektronikus bélyegző készítése és ellenőrzése,
3. tanúsítványok kibocsátása,
4. regisztrációs szolgáltatások,
5. visszavonási lista szolgáltatása,
6. online tanúsítvány státusinformáció-szolgáltatók,
7. tanúsítványok tárolását végző szolgáltatások,

8. időbélyeg-szolgáltatások,
9. időjel-szolgáltatások,
10. nyilvános szabályzatok, és aláírási politika kibocsátása.

Ki kell térnünk itt az eltérő szóhasználatra, amely az Európai Unió és a világ többi része között fennáll. Kezdetben a tanúsítványokat kiállító szervezetek megjelölésére a hitelesítésszolgáltató (certificate authority) kifejezés volt használatos, ezt a fogalmat használták az amerikai szabványosító szervezetek. Azonban ahogy bővültek a kapcsolódó szolgáltatások, az EU a vonatkozó szabályozásában elkezdte a bizalmi szolgáltató (trust service provider) megnevezést alkalmazni, amelybe beleérti a tanúsítványokat kibocsátó szolgáltatókat is, az időbélyegzést, a megbízható kézbesítést vagy az aláírások ellenőrzését végző szolgáltatók mellett. A hitelesítésszolgáltató tehát a tanúsítványokat kibocsátó bizalmi szolgáltató fogalmának feleltethető meg.

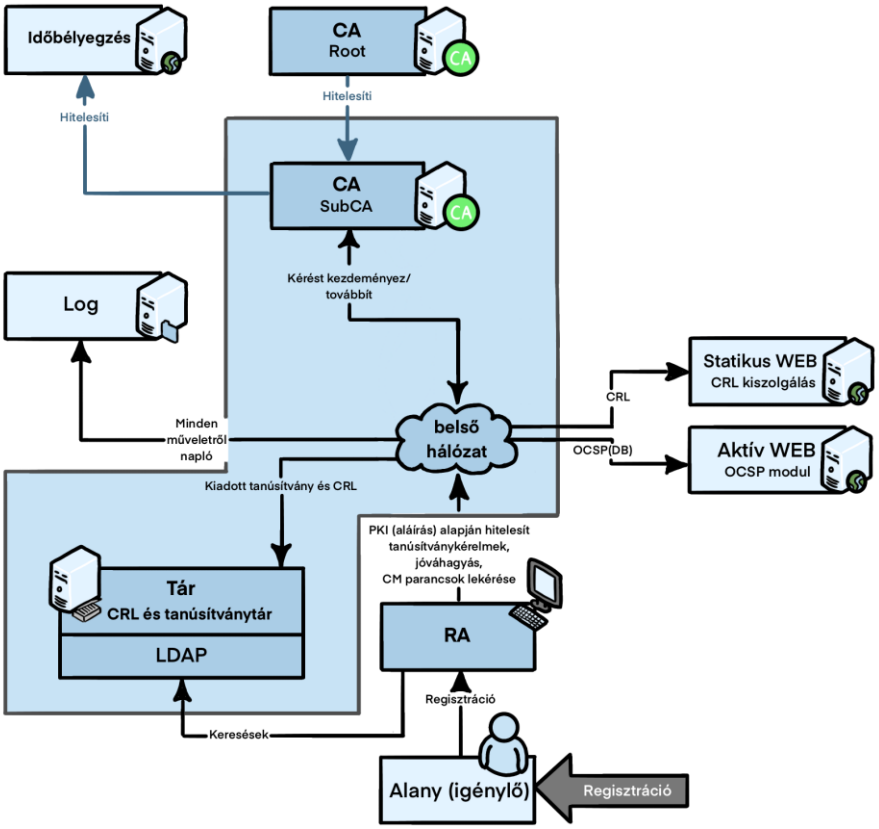
A funkciókhoz tartozó funkcionális egységeket az alábbi módon lehetséges elkülöníteni:

- **Gyökértanúsítvány-kibocsátó** (**root CA**)**:** legfelső szintű szolgáltató, a szolgáltatói hierarchia legfőbb kulcsát tárolja, és legfontosabb tulajdonsága, hogy a hitelességét saját maga igazolja. A tanúsítványkibocsátóktól független módon működik, jellemzően csak a tanúsítványkibocsátók felülhitelesítésekor és az időszakos tanúsítvány-visszavonási lista kiadásakor kapcsolják be, de az adatok átvitele ebben az esetben sem a hálózaton keresztül történik. Folyamatos működtetése is elképzelhető, attól függően, milyen gyakorisággal kell felülhitelesítenie vagy tanúsítvány-visszavonási listát kibocsátania.
- **Hitelesítésszolgáltató (certificate authority, CA):** tanúsítványok kibocsátását végző szervezet, a szervezési és műszaki folyamataival és eszközeivel együtt.
- **Időbélyeg-kibocsátó (time stamping authority, TSA)**: az időbélyegek kibocsátását végző szolgáltató, a kibocsátás során az atomórához szinkronizált időjelet kapcsolja össze az időbélyegzésre elküldött dokumentummal, saját szolgáltatói digitális aláírásának felhasználásával.
- **Tanúsítvány-kibocsátó (subordinate CA):** a végfelhasználói és szolgáltatói tanúsítványokat kiállító, a root CA-tól különböző műszaki egységek. Az egységeket sok esetben az egyes tanúsítványtípusok és felhasználói csoportok szerint elkülönítetten alakítják ki. Jellemzően az aláíró, bélyegző, titkosító és autentikációs tanúsítványokat egy hitelesítésszolgáltatói szervezeten belül más-más tanúsítvány-kibocsátó adja ki. Emellett kialakíthatóak további alrendszerek, mint például a tesztrendszer vagy egy nagyobb szervezet munkatársai számára kitelepített láncolt CA-rendszer. Ezek mindegyike tanúsítvány-kibocsátónak tekinthető. Nagyon fontos, hogy mindegyik tanúsítvány-kibocsátóhoz egy vagy több külön szabályzat tartozik, ami az adott tanúsítvány kibocsátását, felhasználását és ellenőrzését definiálja.
- **Regisztrációs hatóság (registration authority, RA):** a tanúsítványigénylő azonosításáért és hitelesítéséért felelős szervezeti egység, funkció. A regisztrációs hatóság veszi fel a tanúsítványban szereplő adatokat, azonosítja a felhasználót, sok esetben személyesen ő adja át az elkészült tanúsítványt és az aláírás-létrehozó eszközt is az igénylőnek. Amely országban ez jogszabályban megengedett, video-azonosítással is ki lehet bocsátani tanúsítványokat.

- **Biztonságos hardver modul (hardware security module, HSM):** olyan tanúsított kriptográfiai eszköz, amely tárolja és védi a CA-hoz és az adott szolgáltatáshoz, alrendszerhez tartozó privát kulcsot úgy, hogy azt ne lehessen illetéktelen módon felhasználni.
- **Minősített aláírás-létrehozó eszköz, MALE (qualified signature creation device, QSCD):** az eIDAS mellékletében rögzített feltételeknek tanúsítottan megfelelő aláírás-készítő fizikai eszköz (jellemzően chipkártya, SIM-kártya, USB-token vagy távoli HSM modul), amely tárolja és védi a felhasználói titkos kulcsokat, megfelelő hozzáférés-védelmet biztosítva.
- **Minősített bélyegző-létrehozó eszköz, MBLE (qualified seal creation device, QSCD):** az eIDAS mellékletében rögzített feltételeknek tanúsítottan megfelelő bélyegző-készítő fizikai eszköz (jellemzően chipkártya, SIM-kártya, USB-token vagy távoli HSM modul), amely tárolja és védi a felhasználói titkos kulcsokat, megfelelő hozzáférés-védelmet biztosítva. Funkcionális értelemben megegyezik a MALE eszközzel.

4.2.4 A PKI-rendszerek műszaki elemei

A hitelesítésszolgáltatások mindegyike műszaki alapon működik, tehát minden rendszerelemhez hardver- és szoftvereszközök tartoznak. Egy hitelesítésszolgáltató teljes körű PKI-rendszerének felépítése látható a kapcsolódó szolgáltatásokkal az alábbi ábrán:



9. ábra: Egy PKI-rendszer elemei

Egy PKI-rendszerben az alábbi fő elemek lehetnek tehát:

1. **Gyökértanúsítvány-kibocsátó (Root CA)**
2. **CA (certificate authority) – tanúsítvány-kibocsátó:** a tanúsítványokat kibocsátó, a gyökértanúsítvány-kibocsátótól különböző műszaki egység. Kiadhat további szolgáltatói vagy végfelhasználói tanúsítványokat egyaránt. Kibocsátás után publikálja a kiadott tanúsítványokat a tanúsítványtárban.
3. **RA (registration authority) – regisztrációs modul:** a regisztrációs modul végzi a felhasználói tanúsítványt igénylő adatainak a rögzítését, a munkafolyamat támogatását.
4. **Tanúsítványtár (repository):** a kiadott tanúsítványokra vonatkozó információk adatbázisa. Itt van nyilvántartva a tanúsítvány és az érvényessége (kiadott, felfüggesztett, visszavont).
5. **CRL (certificate revocation list) – visszavonási lista:** a visszavont tanúsítványok fájlalapú adatbázisa, publikálása rendszeres időközönként megtörténik, de eseti kibocsátás is elképzelhető.
6. **OCSP (online certificate status protocol) – valós idejű tanúsítvány-visszavonási állapot szolgáltatás:** a tanúsítvány állapotának 7/24 módon elérhető online lekérdezését biztosító modul.
7. **TSA (time stamp authority) – időbélyeg-szolgáltatás:** a bejövő időbélyegzés-kérés feldolgozását és időbélyeg-válasz küldését biztosító modul.
8. **LOG (log module) – naplózómodul**, mely biztosítja, hogy minden tevékenységről a megfelelő szintű naplóbejegyzés történjen, azért, hogy bármilyen esetben nyomon követhető legyen, hogy ki (melyik felhasználó vagy modul) mikor, milyen adattal mit végzett.

Gyakorló kérdések:

1. Mi az a PKI?
2. Milyen struktúrába szerveződhetnek a tanúsítványkibocsátók?
3. Milyen elemei lehetnek egy PKI-rendszernek?

5 Digitális tanúsítványok

5.1 A tanúsítványok fogalmi rendszerei

A **tanúsítvány** olyan dokumentum, amely egy hiteles állítást tartalmaz valaminek az igazolására, megerősítésére. Ilyen tanúsítványokra alapul a hivatalos ügyintézés évszázadok óta. Ma tanúsítványnak számít a személyi igazolvány, a lakcímigazoló kártya, az útlevél, a jogosítvány, a tb-kártya és egyéb hivatalos okmányok, amelyek tanúsítják a fizikai és jogi személyek létezését és összekapcsolhatóságát, a lakcímét vagy egy vállalkozás székhelyét/telephelyeit, a magánszemély állampolgárságát, valamint autóvezetési vagy autótulajdonosi jogait.

Ezek mind tanúsítványok, azaz olyan dokumentumok, amelyek állítást tartalmaznak valaminek az igazolására, és az hitelesíti azokat, aki erre jogszabály vagy más megegyezés alapján fel van jogosítva (legjobb példa erre egy közhiteles nyilvántartásokon alapuló igazolvány). De tanúsítvány az érettségi bizonyítvány és a diploma is. Ezek azt állítják, hogy az alanya elvégzett valamilyen iskolát vagy tanfolyamot, amit az iskola pecsétje és az iskolaigazgató aláírása is igazol, hitelesít. Ezek az igazolások lehetnek papíralapúak, vagy digitálisak. A digitális igazolásokra jó példa az OpenBadges szabvány[7] alapján kibocsátott tanúsítvány, amely megköveteli az igazolások aláírását JSON Web Signature (JWS)[8] használatával. Azokat a tanúsítványokat nevezték először digitális tanúsítványoknak, amelyek egy kulcspár nyilvános kulcsát tartalmazzák, és elektronikus aláírási, bélyegzési, webhitelesítési vagy más célokra bocsátottak ki. Ezeknek a célja nem valamilyen tanfolyam elvégzésének vagy képesség megszerzésének az igazolása, hanem a titkos kulcs birtoklásának magán- vagy jogi személyhez, esetleg egy eszközhöz (pl. webszerver) kötése.

5.1.1 A digitális tanúsítvány fogalomrendszere

5.1.1.1 Tanúsítvány az elektronikus világban

Az elektronikus világban a digitális igazolás olyan elektronikus iratként definiálható, amelyet egy hozzá csatolt digitális aláírással hitelesít egy olyan intézmény, amelyben a tanúsítványt felhasználók közössége megbízik (jogszabály vagy megegyezés alapján). Ezt az intézményt szokták nevezni megbízható harmadik félnek (trusted third party), vagy amerikai szóhasználattal élve hitelesítésszolgáltatónak. Európai szóhasználatban az eIDAS óta a bizalmi szolgáltató fogalma terjedt el. Bizalmi szolgáltató azonban csak olyan intézmény lehet az EU-ban, amelyet nyilvántartásba is vettek.

Habár a digitális igazolás fogalmába belefér az időbélyegző, a visszavonási lista és akár egy elektronikus személyi igazolvány is, a digitális tanúsítvány alatt azonban a következő fejezetekben kizárólag a nyilvános kulcsú tanúsítványt fogjuk érteni.

Az elektronikus aláírás egyik alapvető célja a kiállító és a tartalom hitelességének biztosítása. Ezt a nyilvános kulcsú kriptográfia tudja is biztosítani, de nem önmagában, hanem számos kiegészítő infrastrukturális elemmel együtt. Például, ha látunk egy titkos kulccsal hitelesített dokumentumot, és meg akarunk bizonyosodni arról, hogy ki és mit hitelesített, a következő kérdést kellene feltennünk: hogyan biztosított, hogy az aláírás ellenőrzésére használt

[7] https://openbadges.org/build és https://www.imsglobal.org/spec/ob/v2p1/
[8] RFC 7515 JSON Web Signature (JWS) (https://www.rfc-editor.org/rfc/rfc7515)

nyilvános kulcs valóban ahhoz tartozik, aki ezt állítja magáról? Erről meg lehet győződni akár személyes találkozással és a nyilvános kulcsok kicserélésével, valamint úgy is, hogy egy elektronikus kulcscsere után szóban – ellenőrzött hívással és kommunikációs partnerrel – bájtról bájtra egyeztetik a kulcs lenyomatát.

Ilyen esetekre a kérdés/válasz módszerek is jó megoldási lehetőséget nyújtanak, vagyis ennek gyakorlati módja az lehet, hogy a küldő egy olyan általa ismert véletlenszerű adat kódolását kéri a partnerétől, amelyet a küldő aláír digitálisan a saját titkos kulcsával. A partner ezt a saját titkos kulcsával titkosítva visszaküldi, és ezt a küldő a partner nyilvános kulcsával vissza tudja fejteni, és ezután azt is le tudja ellenőrizni, hogy az őáltala aláírt véletlenszerű adat szerepel-e a visszafejtett üzenetben. (Szerencsére a kulcselosztás és hitelesítés problémájára van ennél egyszerűbb, biztonságosabb és automatikusabb módszer is, ami ráadásul még akkor is működik, ha a kommunikációs partnerünket korábban nem is ismertük. A megoldás alapelve igen egyszerű. Mivel a digitális aláírás biztosítja a hitelességet, megfelelő módon – például nyilvános bizalmi szolgáltató által – alá kell írni a nyilvános kulcsot is.)

5.1.1.2 A hitelesítésszolgáltató

A tanúsítványokat tehát egy megbízható harmadik félnek kell aláírnia, akiben megbízik a felhasználói közösség. Az egyik bizalmi modell szerint ez a megbízható harmadik fél a hitelesítésszolgáltató, aki a saját aláírásával bizonyítja a nyilvános kulcs adott személyhez tartozását (valamint gondoskodik az így létrehozott tanúsítványok nyilvánosságra hozataláról, szükség szerinti visszavonásáról). A bizalom webje modellben a kulcsokat a tulajdonosa írja alá, és teszi közzé a közösség számára. A közösség tagjai pedig bizalmat szavaznak a kulcs és a közzétevő közötti kapcsolatnak. Ebben a bizalmi modellben nem szükséges megbízható harmadik félnek jelen lennie.

A továbbiakban a megbízható harmadik feleken alapuló bizalmi modellt vesszük alapul, mivel ez a modell terjedt el leginkább a közigazgatásban és az üzleti világban is.

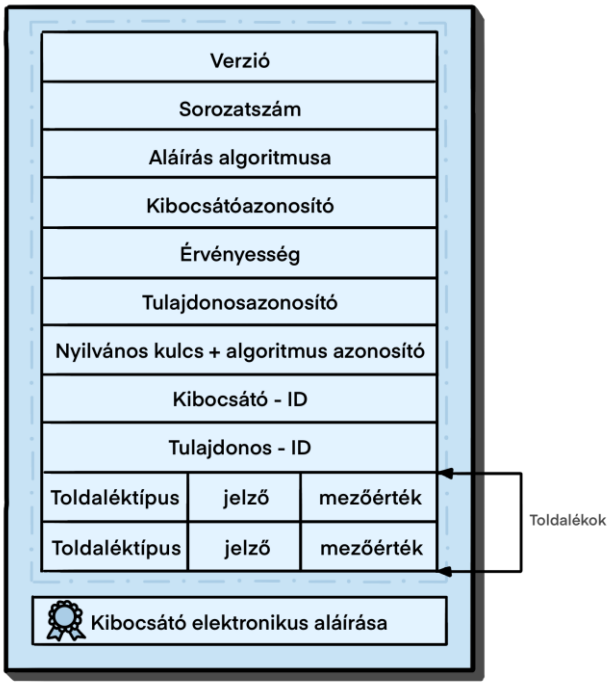
A tanúsítvány egyik legfontosabb eleme a hitelesítésszolgáltató által aláírt nyilvános kulcs. Magában a tanúsítványban továbbá fel van még tüntetve, hogy az kinek – mely személynek – a nyilvános kulcsát tartalmazza. Így lesz a tanúsítvány annak az állításnak az igazolása, hogy a nyilvános kulcs és a feltüntetett személy összetartoznak. A tulajdonos neve mellett érdemes lehet feltüntetni egyéb hasznos információkat is: ki adta ki, milyen algoritmussal készült a nyilvános kulcs (lehetővé téve a közösség tagjai számára, hogy különböző algoritmusokat is felhasználjanak, és hogy azonos algoritmussal ellenőrizzék), meddig érvényes stb. Így lesz a tanúsítvány egy olyan elektronikus irat, amely nemcsak egy szimpla állítást, de annak attribútumait is tartalmazza. Mint ahogy az előbb említett diploma esetében szintén fel van tüntetve a kiadó tanintézet neve, a kiadás dátuma, az elért eredmény és még sok minden más is.

5.1.1.3 Az X.509 szabvány

Az X.509 az ITU[9] által kibocsátott szabvány, mely a tanúsítvány és tanúsítvány-visszavonási lista szerkezetére, felépítésére, tartalmára, kezelésére és még sok más, ezzel összefüggő dologra ad előírásokat. A tanúsítványok kezelésében ez a szabvány világszerte általánosan elfogadott és egyeduralkodó.

[9] ITU: International Telecommunication Union, Nemzetközi Telekommunikációs Egyesülés.

Az X.509-es szabvány 3-as verziója szerint a tanúsítvány a következőképpen néz ki:



10. ábra: Az X.509.V3 tanúsítvány felépítése

A mezők jelentése a következő:

Verzió	A tanúsítvány a szabvány mely verziója alapján készült (v1, v2, v3)
Sorozatszám	A tanúsítvány egyedi sorszáma (tanúsítványkibocsátón belül)
Aláírás algoritmusa	A kibocsátó által a tanúsítvány aláírására használt algoritmus azonosítója
Kibocsátóazonosító	A tanúsítványt kibocsátó tanúsítványkibocsátó egyedi (X.500) neve
Érvényesség	A tanúsítvány érvényességének kezdő és végdátuma
Tulajdonosazonosító	A tanúsítvány tulajdonosának egyedi (X.500) neve
Nyilvános kulcs	A tanúsítvány által hitelesített nyilvános kulcs és annak algoritmusazonosítója
Kibocsátó-ID	A kibocsátó egyedi azonosítója
Tulajdonos-ID	A tanúsítvány tulajdonosának egyedi azonosítója
Toldalék típusa	A toldalék típusának egyedi objektumazonosítója
Toldalékjelző	Kritikus / Nem kritikus
Toldalék értéke	A toldalék értéke a típusnak megfelelően

6. táblázat: Az X.509 tanúsítványok mezőinek jelentése

A „Verzió”-tól a „Nyilvános kulcs”-ig terjedő mezők kötelezően kitöltendőek. A „Kibocsátó-ID” és a „Tulajdonos-ID” mezők opcionális felhasználásúak. Ezek a mezők azt a célt szolgálják, hogy a kötelező részbe foglalt azonosítókat egyértelművé tegyék abban az esetben, ha ugyanazt a nevet újra kiosztanák, továbbá azt, hogy a használt névformátumtól eltérő névkonvenciónak megfelelő nevet is fel lehessen tüntetni azonosítóként. A toldalék (kiterjesztés) mezők, melyekből több is követheti egymást, lehetőséget biztosítanak arra, hogy bármely kibocsátó olyan adatot foglaljon a tanúsítványba, ami neki tetszik. Megjegyezzük, hogy toldalékmezők szabadon felvehetők a tanúsítványokba, azonban szabványos háttér nélkül ezek ismertsége és felhasználhatósága korlátozott lehet csak.

5.1.2 A tanúsítványok érvényességi ideje és állapota

5.1.2.1 Tanúsítványok és kulcsok érvényességi ideje

A tanúsítványoknak és a kulcsoknak **érvényességi ideje** és **érvényességi állapota** van, ami a felhasználás műszaki és jogi értelemben vett **korlátozását** is jelenti. Műszaki értelemben a korlátozás azt jelenti, hogy a tanúsítványokat és kulcsokat kezelő alkalmazások a felhasználást az érvényességi időn kívül, illetve érvénytelen állapot esetén alapesetben nem teszik lehetővé. Matematikai értelemben a felhasználás természetesen nincs korlátozva, az algoritmus bárhol és bármikor működik. A kérdés az, hogy a létrehozott eredményt mire lehetséges felhasználni. A jogi értelem ezért arra utal, hogy ha nem helyesen, azaz annak érvényességi korlátozásait figyelmen kívül hagyva járunk el a kulcsunkkal és a tanúsítványunkkal, akkor az így létrehozott aláírás matematikailag rendben lesz ugyan, de jogilag érvénytelen lesz, mivel nem fűződnek hozzá azok a jogi vélelmek, amelyek az előírt feltételek betartásával készített aláírásokat, bélyegzőket, időbélyegzőket megilletik. Az érvényességi idők és állapotok értelmezése emiatt nemcsak az aláírók, de az aláírásokat ellenőrzők számára is kiemelten fontos, ezért érdemes áttekinteni az ezzel kapcsolatos kérdéseket.

Az aláírásra vagy bélyegzésre és rejtjelezésre használatos kulcsokat nem szabad a végtelenségig használni. Ennek egyrészt az az oka, hogy a technika fejlődése véges időn belül elavulttá tesz korábban még biztonságos megoldásokat, másrészt túl hosszú felhasználás esetén a kriptoanalízis (feltörés) veszélye is jelentősen megnő.

Ezért a kulcsok élettartamát be szokták határolni, aminek több előnye is van:

- lehet csökkenteni a kriptoanalízis fejlődésével járó kompromittálódási veszélyeket,
- a kulcsok algoritmusa, erőssége változtatható a kriptográfia eredményeinek megfelelően,
- az esetlegesen kompromittálódott kulcsokkal okozható veszteségek csökkenthetők,
- a tanúsítvány-visszavonási lista mérete csökkenthető, javul ezzel a működés biztonsága.

A kulcsok élettartama és a kapcsolódó tanúsítvány érvényességi ideje lehet különböző, de a titkos kulcs nem lehet hosszabb ideig érvényes, mint a tanúsítvány. Alapesetben a kulcs érvényessége megegyezik a tanúsítvány érvényességi idejével. A tanúsítványban ennek megfelelően feltüntetik az érvényesség kezdeti és végdátumát, ezeken kívüli időpontban a tanúsítvány nem tekinthető érvényesnek. A kezdeti dátum általában a kiadás dátuma, a végdátum pedig a lejárat dátuma, amelyet jogszabály vagy a szolgáltató által kiadott szabályzat határoz meg. Érdekes, hogy az eIDAS nem korlátozza a tanúsítványok élettartamát, pusztán az ilyen jellegű korlátozás lehetőségét engedi meg a szolgáltatók számára, a felelősségük korlátozása kapcsán. Emiatt a tanúsítványok élettartamát leggyakrabban a nemzeti jogrend szabályozza. Ez típusonként és országonként is eltérhet. Például 2022-ben Magyarországon a minősített tanúsítványok maximális érvényességi ideje 3 év, Észtországban 5 év. A tanúsítványkibocsátók saját szolgáltatói tanúsítványai ettől eltérően akár húsz-harminc évig is érvényesek lehetnek.

A tanúsítvány érvényességi ideje egyfelől azt jelenti, hogy a hitelesítésszolgáltató aláírása addig érvényes a tanúsítványon, utána már nem igazolja a benne foglalt adatok valódiságát, sértetlenségét, összetartozását, másfelől a titkos kulcs legkésőbbi felhasználhatósági idejét is jelenti. A kulcs érvényességi ideje ettől rövidebb is lehet, de ekkor ezt külön fel kell tüntetni a tanúsítványban. A nyilvános kulcs érvényességét nem célszerű korlátozni, hiszen előfor-

dulhat, hogy egy aláírást vagy időbélyeget a kapcsolódó tanúsítvány lejáratát követően kell ellenőrizni, ez pedig csak a nyilvános kulccsal tehető meg. Az ellenőrzéskor természetesen ebben az esetben is tekintettel kell lenni a kriptográfiai háttérre .

5.1.2.2 Tanúsítványok visszavonása

Bár a tanúsítványoknak előre behatárolt érvényességi időtartama van, szükség lehet arra is, hogy ezen időtartamon belül visszavonják egy tanúsítvány érvényességét. Például, ha már valamilyen ok miatt már nem igaz a benne foglalt állítás, vagy esetleg valaki elvesztette a tanúsítványát, vagy netán ellopták tőle.

Érdekmúlás esetén a papíralapú tanúsítványnál megoldható az eredeti példány megsemmisítése, de az érvénytelenítés további igazolást igényel. Az elektronikus világban a megsemmisítés már nem járható út, hiszen egyrészről nincs „eredeti” példány, másrészről bárhol lehet másolata a tanúsítványnak. Ekkor csak az érvénytelenítés lehet a megoldás. Ha a hitelesítésszolgáltató tanúsítványtárat működtet, ahol az addig kiadott tanúsítványai fellelhetők, akkor vezethet egy nyilvántartást azokról a tanúsítványokról is, amelyeket időközben visszavontak, azaz már nem érvényesek. A nyilvántartás nyilvánosan elérhető a nyilvános szolgáltatók esetében, így abban bárki ellenőrizheti az éppen használt tanúsítvány aktuális állapotát, érvényességét. Az ebben szereplő információ határozza meg a tanúsítvány állapotát: ha a tanúsítvány szerepel a tanúsítvány-visszavonási listában, akkor a tanúsítvány állapota érvénytelen, ha pedig nem, akkor érvényes.

A tanúsítványok világában nem lehet kulcsot külön visszavonni, csak tanúsítványt lehet érvényteleníteni. Ezért a tanúsítvány állapotának érvénytelenségét úgy kell érteni, mintha mind a tanúsítvány, mind a magánkulcs érvényességi ideje a visszavonás pillanatában véget ért volna (a visszavonás időpontját a lista tartalmazza). A PGP-világban lehetőség van a kulcsok érvénytelenítésére, egy speciális visszavonási állítás közösségen belüli elterjesztésével.

A felhasználónak a tanúsítvány érvényességi idejének lejáratát követően, illetve visszavonás után az aláíró/bélyegző magánkulcsát érdemes megsemmisítenie. A nyilvános kulcs ezt követően is használható ellenőrzési célokra.

5.1.2.3 Tanúsítványok felfüggesztése

A tanúsítvány visszavonása végleges, irreverzibilis cselekedet, a nyilvánosan működő bizalmi szolgáltatóknál azt nem lehet visszaállítani. Ha mégis szükség lenne egy rá, akkor újat kell kérni. Létezik nem végleges visszavonási lehetőség olyan esetekre, amikor a tulajdonos bizonytalan az aláírás-létrehozó adatának hollétét illetően, de lehetséges, hogy egyszerűen csak feledékeny volt, nem történt semmilyen biztonságot veszélyeztető incidens, vagy a használati jogosultság ideiglenesen, átmeneti jelleggel – rövid időre – megszűnik, de tudjuk, hogy az átmeneti időtartam után a használat továbbra is szükséges lesz. Erre a célra szolgál a felfüggesztés intézménye, amit nem minden szolgáltató támogat. Ha egy tanúsítványt felfüggesztenek, annak a gyakorlati hatása ugyanaz, mint a visszavonásnak – a gyakorlatban érvénytelenítve lesz, de átmeneti jelzéssel.

A tanúsítvány legfeljebb az érvényességének lejártáig lehet felfüggesztett állapotban. Ha a tanúsítvány még nem járt le a visszaállítás idején, akkor a tanúsítványt újra érvénybe lehet helyezni a tulajdonos kérése alapján, a kérés jogosságának ellenőrzése után.

5.1.3 A tanúsítványok típusai

A tanúsítványokat egy vagy több jól meghatározott célra bocsátják ki. Több tanúsítványtípust is ismerünk, ilyenek az aláíró, bélyegző, időbélyegző, webhitelesítő, autentikációs, email hitelesítő tanúsítványok, hogy csak a leggyakoribb típusokat említsük. Továbbá használunk minősített és nem minősített tanúsítványokat is. Vagyis a gyakorlatban különböző **típusú** tanúsítványok jöttek létre.

5.1.3.1 Tanúsítványtípusok

A tanúsítványok típusának beállítását a kibocsátás során végzik el, ott jelölik meg ezeket a használati célokat, az igénylésnek megfelelően. A típust befolyásolhatja az, hogy magánszemély vagy jogi személy lesz-e a tulajdonosa, avagy személyes használatú lesz, vagy automata fogja azt használni. A felhasználási területek is befolyásolják a tanúsítványok típusait, külön típusok jöttek létre aláírásra, bélyegzésre, időbélyegzésre, weboldal hitelesítésére, szoftverkód aláírására vagy email hitelesítésére. A tanúsítvány típusát és a felhasználás célját megjelölik a tanúsítványban is, az erre a célra szolgáló kulcshasználati mezőkben. Az erre vonatkozó részletes szabályozást az RFC 5280 megjelölésű dokumentum foglalja keretbe[10].

A tanúsítványokat megkülönböztethetjük biztonsági szint szerint is. Ezt a megkülönböztetést használják leginkább a jogszabályokban. Az eIDAS definícióit alapul véve:

1. elektronikus aláírás tanúsítványa: olyan elektronikus igazolás, amely az elektronikus aláírást érvényesítő adatokat egy természetes személyhez kapcsolja, és legalább az érintett személy nevét vagy álnevét igazolja;
2. elektronikus aláírás minősített tanúsítványa: olyan, elektronikus aláírás céljára használt tanúsítvány, amelyet minősített bizalmi szolgáltató bocsát ki; és amely megfelel az eIDAS I. mellékletben megállapított követelményeknek;
3. elektronikus bélyegző tanúsítványa: olyan elektronikus tanúsítvány, amely az elektronikus bélyegzőt érvényesítő adatokat egy jogi személyhez kapcsolja, és igazolja az érintett jogi személy nevét;
4. elektronikus bélyegző minősített tanúsítványa: elektronikus bélyegző olyan tanúsítványa, amelyet minősített bizalmi szolgáltató bocsát ki; és amely megfelel az eIDAS III. mellékletben megállapított követelményeknek;
5. „weboldal-hitelesítő tanúsítvány”: olyan igazolás, amely lehetővé teszi a weboldal hitelesítését és a weboldalt ahhoz a természetes vagy jogi személyhez kapcsolja, akinek vagy amelynek részére a tanúsítványt kiállították;
6. „minősített weboldal-hitelesítő tanúsítvány”: olyan weboldal-hitelesítő tanúsítvány, amelyet minősített bizalmi szolgáltató bocsát ki, és amely megfelel az eIDAS IV. mellékletben megállapított követelményeknek.

Az eIDAS emelt szintű követelményeket határozott meg a minősített tanúsítványok kibocsátóival szemben , így joggal mondhatjuk, hogy azok biztonsági szintje is emelt szintű, szemben a nem minősített tanúsítványokkal. Ezt a jogalkotó is felismerte, és a jogrendekben a minősített tanúsítványokhoz magasabb szintű garanciákat kapcsolt, sok esetben ennek

[10] Lásd https://www.rfc-editor.org/rfc/rfc5280 4.2.1.3 és 4.2.1.12 fejezeteket.

használatát preferálva. Megemlítjük, hogy az aláírásoknak is van hasonló osztályozása, és van is kapcsolat a tanúsítványok és az aláírások osztályai között, azonban a hasonlóságok ellenére sem szabad ezeket összekeverni.

5.1.4 A tanúsítványok struktúrája és hierarchiája

A nyilvános kulcsokat a tanúsítványok segítségével lehet szétosztani. A nyilvános kulcs tanúsítvány formában a partnereknek közvetlen elküldhető, akár első, elektronikusan aláírt üzenetváltás alkalmával is, még akkor is, ha a kommunikációs csatorna nem biztonságos.

A tanúsítványt a kibocsátó aláírása hitelesíti. A hitelességről az aláírás ellenőrzésével lehet megbizonyosodni, amihez a kibocsátó nyilvános kulcsa szükséges. Ez egy másik tanúsítványban, a szolgáltatói tanúsítványban található meg. Előfordulhat az is, hogy ezt a tanúsítványt egy másik szolgáltatói tanúsítvány hitelesíti, így a tanúsítványok különböző hosszúságú láncolata jön létre a végfelhasználói tanúsítványtól a közbülső kibocsátón vagy kibocsátókon keresztül, a legfelső szintű tanúsítványig. A legfelső szinten álló tanúsítványt gyökértanúsítványnak nevezzük. A legrövidebb lánc három elemű, mert gyökértanúsítvánnyal nem szokás végfelhasználói tanúsítványt hitelesíteni, ezért legalább egy köztes kibocsátóra is szükség van.

Azonban nem lenne célszerű megoldás, hogy egyetlen egy kibocsátó adná ki típustól függetlenül az összes végfelhasználói tanúsítványt, mivel a különböző tanúsítványokra különböző követelmények vonatkoznak. Emiatt egy szolgáltatón belül több különböző köztes kibocsátó is megjelenhet, amelyek összességét nevezzük a szolgáltató PKI struktúrájának. Ez a struktúra többféle modellt is megvalósíthat. A leggyakoribb a hierarchikus, egyirányú fastruktúra, amelyben minden levélnek pontosan csak egy szülője van, és a hierarchia tetején egyetlen egy szülő, a gyökértanúsítvány-kibocsátó áll. A levelek száma elvileg nem korlátos, egy szülőnek tetszőleges – de véges – számú levele lehet. A legfelső szintű kibocsátó felelős a közvetlen alatta lévő köztes tanúsítványkibocsátók és visszavonási állapotuk hitelesítéséért. A köztes kibocsátók felelősek a végfelhasználói tanúsítványok kibocsátásáért és állapotuk hitelesítéséért. Ez a háromszintű fastruktúrát leképező hierarchia. A köztes kibocsátók kiadhatnak újabb és újabb kibocsátói tanúsítványokat is, amivel a szintek száma bővíthető, a funkcionalitás azonban az előbb felsoroltakat tartalmazza.

Két különböző fastruktúrának különböző legfelső szintű kibocsátóval kell rendelkeznie, azonban a köztes kibocsátók között már lehetnek átfedések. Erre a legjobb példa a magyar Közigazgatási Gyökér Hitelesítés-Szolgáltató (KGYHSZ), amely a magyar közigazgatásban használható tanúsítványokat kibocsátó szolgáltatók szolgáltatói tanúsítványát felülhitelesítő szervezet. Ez azt jelenti, hogy a magyar közigazgatásban akkor lesz használható egy tanúsítvány, ha a láncolatnak a tetején a KGYHSZ áll, mint legfelső szintű kibocsátó.

Egy másik modellben egymás hitelesítését is elvégezhetik az egyes kibocsátók, amivel azt érik el, hogy a másik kibocsátó által kiadott tanúsítványokban a felhasználói közösség ugyanolyan módon megbízhat, mint a saját kibocsátású tanúsítványokban, hiszen mindkét struktúrában létrehozható egy olyan tanúsítványláncolat, amely visszavezethető az adott struktúrában megbízható kibocsátóra. Ezt a módszert kereszthitelesítésnek nevezik, a modellt pedig híd (bridge) kibocsátói modellnek, mivel az egyes struktúrák így hidalják át az egymás között lévő bizalmi szakadékot.

5.1.5 A tanúsítványok elfogadhatósága

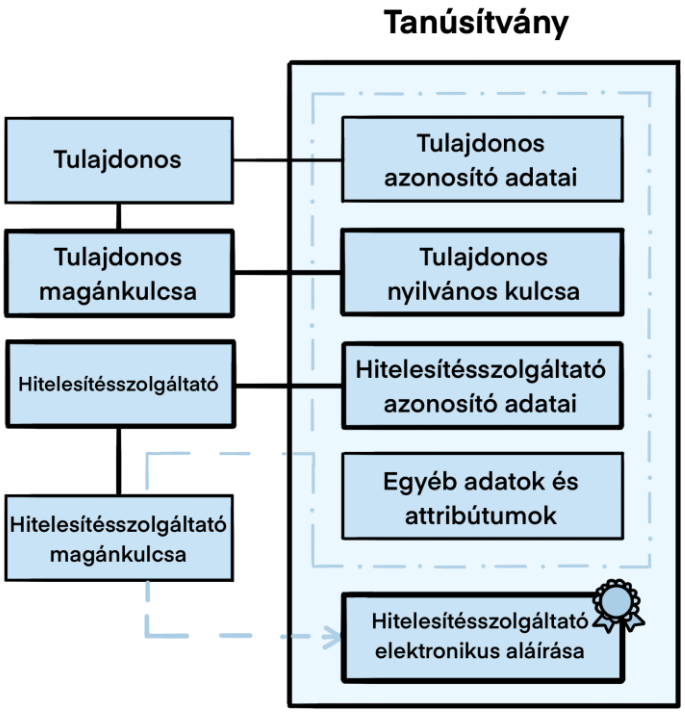
5.1.5.1 A tanúsítási lánc

A tanúsítványok kibocsátóinak aláírásával hitelesített végfelhasználói és kibocsátói tanúsítványok sorozatát, **tanúsítási láncnak** nevezzük. A felhasználó tanúsítványa akkor tekinthető érvényesnek, ha a tanúsítási láncban minden egyes tanúsítvány érvényes. Az aláírás pedig akkor lesz érvényes, ha az aláíró tanúsítási lánca az aláírás időpontjában érvényes volt. Ennek ellenőrzéséhez az ellenőrzést végzőnek a lánc összes tanúsítványával rendelkeznie kell. Az ellenőrzés során a tanúsítványok aláírásainak érvényességét, és a legfelső szintű kibocsátó aláírásának megbízhatóságát igazoljuk. A lánc legfelső elemét – a legfelső szintű kibocsátót – szokták bizalmi pontnak is nevezni, mivel, ha egy ilyen tanúsítványban megbízunk, azzal együtt megbíztunk a hierarchiában szereplő összes kibocsátó minden egyes kibocsátott tanúsítványában is alapértelmezésben.

5.1.5.2 A tanúsítványok ellenőrzése

A tanúsítványok ellenőrzése során a legalapvetőbb információkat az alkalmazások maguktól is ellenőrzik. Legfontosabb automatikus ellenőrzés, hogy a tanúsítvány aláírása érvényes-e. A felhasználás során további ellenőrzéseket is végeznek a szoftvereink, például e-mail esetében összehasonlítják a levél küldőjének e-mail címét a tanúsítványban feltüntetettel, weboldal esetében az oldal címét a tanúsítványban szereplővel, továbbá ellenőrzik, hogy a tanúsítvány érvényességi ideje nem járt-e le, és hogy a tanúsítvány kibocsátójának és a kibocsátói hierarchiának minden szolgáltatói tanúsítványa a felhasználó által megbízhatónak minősített szolgáltatók listájában megtalálható-e.

A tanúsítványok adatainak ellenőrzését a tanúsítvány-megjelenítő funkció segítségével végezhetjük el, amelynek során a tanúsítvány összes adata megjelenik számunkra.



11. ábra: A tanúsítvány adatainak megjelenítése

Különösen érdemes odafigyelni a tanúsítványban a kibocsátói szabályzatra, és a típusjelzésre való utalásra (a szabályzat tartalma külön tekinthető meg). Ezek az információk a tanúsítvány típusát és a mögöttes biztonsági szintjét határozzák meg. Az egyébként teljesen hasonló módon megjelenő tanúsítványok csak ezen apró attribútumukban különböztethetőek meg, de ez az apróság lényeges használati különbséget is jelenthet.

Hasznos tudni még, hogy a tanúsítvány ellenőrzése nem egyezik meg az aláírás ellenőrzésével, de az aláírás ellenőrzésekor minden tanúsítványt illik ellenőrizni. Bár az aláírás alapszintű ellenőrzését (azaz az aláírásnak az aláíró tanúsítványban szereplő nyilvános kulccsal való elolvashatóságát, a tanúsítványlánc érvényességének és az aláírt információ sértetlenségének ellenőrzését) az alkalmazások automatikusan elvégzik, az aláírás is tartalmazhat olyan attribútumokat, amelyek ellenőrzése emberi közreműködést igényelhet.

Gyakorló kérdések:

1. Mi a tanúsítvány és mi a tartalma?
2. Hogyan kell ellenőrizni egy tanúsítványt vagy tanúsítványláncot?
3. Milyen biztonsági szintjei vannak a tanúsítványoknak?

5.2 A tanúsítványok használata

5.2.1 Tanúsítványok igénylése

A tanúsítványok igénylését az őket kibocsátó szolgáltatóknál kell kezdeményezni. A tanúsítványt kibocsátó szolgáltató működhet üzleti és nonprofit alapon is (pl. egy kormányzati, vállalati vagy egyetemi belső hitelesítésszolgáltató).

5.2.1.1 Állampolgári tanúsítvány igénylése

2013-ban év végén elkezdte működését a 83/2012. Kormányrendelet 74. § által leírt hitelesítésszolgáltató SZEÜSZ, vagyis elindult a Kormányzati Hitelesítés Szolgáltató Magyarországon és megkezdte az új személyazonosító igazolványba integráltan az állampolgári jogon járó tanúsítványok kiosztását. Ezt a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény 2015-ben történt változása tette lehetővé, amely megnevezte az elektronikus tároló elemeket, mint a személyazonosító igazolvány szerves részeit, és beemelte a minősített elektronikus aláírás készítését az igazolvány funkciói közé[11]. Ezt követően vált lehetővé magyar személyazonosító igazolvánnyal minősített elektronikus aláírás készítése. Ennek jelentőségét az eIDAS rendelet adja meg, amely szerint a minősített elektronikus aláírás a kézi aláírással azonos joghatású, továbbá minden tagállamban el kell fogadni a minősített elektronikus aláírást minősítettként, függetlenül annak létrehozási helyétől[12].

[11] Lásd Nytv. 29. § (1) Az állandó személyazonosító igazolvány alkalmas a polgár elektronikus úton történő közhiteles azonosítására, e törvényben megjelölt kivételekkel – a polgár kérelmére – minősített elektronikus aláírás létrehozására, valamint a polgár törvényben megjelölt esetekben gyakorolhatja vele a külföldre utazás jogát.

[12] Lásd AZ EURÓPAI PARLAMENT ÉS A TANÁCS 910/2014/EU RENDELETE (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről (eIDAS) 25. cikk: Az elektronikus aláírás joghatása
(1) Az elektronikus aláírás joghatása és bírósági eljárásokban bizonyítékként való elfogadhatósága nem tagadható meg kizárólag amiatt, hogy az elektronikus formátumú, illetve nem felel meg a minősített elektronikus aláírásra vonatkozó követelményeknek.
(2) A minősített elektronikus aláírás a saját kezű aláírással azonos joghatású.

Ahhoz, hogy aláírásra is tudjuk használni az eSzemélyi igazolványunkat, a megfelelő tároló elemnek tartalmaznia kell azt az aláírás-létrehozó adatot, amelyet minden állampolgári minősített aláíráshoz innentől kezdve használni fogunk. Tekintettel arra, hogy ezt az adatot az igazolvány kiállításakor nem adják oda automatikusan, hanem csak kérelemre, első lépésként kérni kell a minősített aláírásra feljogosító adatok elhelyezését az eSzemélyi elektronikus tároló elemében[13]. Szerencsére 14. életévét betöltött állampolgár már saját jogon kérelmezheti az igazolvány kiadását[14] Magyarországon.

A személyazonosító igazolvány kiadását részletesen a személyazonosító igazolvány kiadása és az egységes arcképmás- és aláírás-felvételezés szabályairól szóló 414/2015. (XII. 23.) Korm. rendelet írja le. Ennek értelmében igazolványt kormányhivatalban, kormányablakban lehet igényelni. Vagyis akinek még nincsen személyazonosító igazolványa (mert például idáig csak útlevele volt, és azzal tudta magát igazolni), annak el kell mennie egy kormányablakba[15] személyazonosító igazolványt igényelni.

Az aláírás igényléséhez és biztonságos használatához javasolt:

1. az igénylő mindenképpen jelezze, hogy elektronikus aláírást is szeretne a személyazonosító igazolványára kapni,

2. az igénylő jelezze, hogy szeretné, ha a tanúsítványában feltüntetnék az email címét, és

3. az igénylő jelezze, hogy szeretné a tanúsítványát a Kormányzati Hitelesítés Szolgáltató tanúsítványtárában közzétenni.

Az igénylés végeztével a kormányablak kinyomtatja és aláírattatja az igénylési lapot az igénylővel, odaadja az eID és eSZIG borítékot, és 8 munkanapon belül elkészíti az új igazolványt.

Amennyiben már van személyazonosító igazolványunk, de még nem került rá az elektronikus aláírási lehetőség, akkor ennek igénylését utólag is meg lehet tenni a kormányablakokban[16].

Ekkor egy szolgáltatási szerződést kell kötni a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.-vel, akik kijelölt üzemeltetői a Kormányzati Hitelesítés Szolgáltatónak, amely alapján a NISZ elkészíti a tanúsítványt és lehetővé teszi annak későbbi használatát.

---

(3) A valamely tagállamban kibocsátott minősített tanúsítványon alapuló minősített elektronikus aláírást az összes többi tagállamban el kell ismerni minősített elektronikus aláírásként.

[13] Lásd Nytv. 52. § (8) A tároló elemmel rendelkező személyazonosító igazolvány – amennyiben a polgár kérelmére elektronikus aláírási funkcióval is rendelkezik – a tároló elem biztonságos aláírás-létrehozó eszközként történő tanúsításáig minősített tanúsítványon alapuló fokozott biztonságú elektronikus aláírás létrehozására alkalmas.

[14] Lásd Nytv. 29. § (13) A cselekvőképtelen kiskorú polgár részére a személyazonosító igazolványt – a (13a) bekezdésben meghatározott kivétellel – a törvényes képviselő kérelmére kell kiadni. A korlátozottan cselekvőképes kiskorú és a cselekvőképességében részlegesen korlátozott nagykorú jogosultat a személyazonosító igazolvány kiadása ügyében megilleti az eljárási képesség.

[15] Az aktuális kormányablakok listáját itt lehet megnézni: https://kormanyablak.hu/hu/kormanyablakok

[16] Lásd 414/2015. Korm.R. 15. Az e-aláírási funkcióval és időbélyegzéssel kapcsolatos szolgáltatási szerződés 51. § (1) Az e-aláírási funkcióval és az időbélyegzés szolgáltatással kapcsolatos szolgáltatási szerződés a járási hivatalnál, a kijelölt kormányhivatalnál és a nyilvántartást kezelő szervnél köthető meg.
(2) Az e-aláírási funkcióval és az időbélyegzés szolgáltatással kapcsolatos szolgáltatási szerződés a) – a (3) bekezdésben foglalt kivételekkel – az állandó személyazonosító igazolvány kiadására irányuló kérelem előterjesztésével egyidejűleg, valamint
b) tároló elemmel ellátott érvényes állandó személyazonosító igazolvány birtokában
személyesen köthető meg.

5.2.1.2 Tanúsítványigénylés piaci szolgáltatótól

A tanúsítvány kibocsátásának első mozzanataként az igénylőnek meg kell igényelnie a tanúsítványát egy erre rendszeresített tanúsítványigénylő formanyomtatvány (űrlap) segítségével. A formanyomtatvány lehet papíralapú vagy elektronikus, ennek megfelelően az igénylés történhet papíron vagy elektronikus úton (jellemzően webes űrlap kitöltésével).

Az űrlapon kell megadni az igénylő és a felhasználó adatait – ha különböznek egymástól. Az adatok két csoportra bonthatók, a tanúsítványban megjelenő adatokra és a regisztráció során jogszabály vagy belső előírás szerint megadni szükséges adatokra. Ha a kulcspárt a felhasználó gyártotta le – esetenként ez megengedett opció, akkor az igényléshez csatolnia kell saját nyilvános kulcsát, és a magánkulcs tulajdonlását is bizonyítania szükséges – leginkább a kérelemnek az adott magánkulccsal való digitális aláírásával.

A szerződéskötés előtt az ügyfélnek tájékoztatást kell kapnia a felhasználás különböző kondícióiról, a szerződéses feltételekről, saját jogairól és kötelezettségeiről és mindenfajta egyéb lényeges körülményről. A szerződéssel jogi értelemben egy szolgáltató–ügyfél kapcsolat jön létre a két fél között.

A szerződéskötéshez és a szolgálatás megfelelő nyújtásához szükséges adatok felvételét és ellenőrzését együttesen regisztrációnak nevezzük. A regisztráció során megadott adatokat ellenőrizni szükséges. Az eIDAS rendelkezése szerint minősített tanúsítvány kibocsátásakor a minősített bizalmi szolgáltató megfelelő eszközökkel és a nemzeti jogszabályokkal összhangban ellenőrzi annak a természetes vagy jogi személynek az azonosságát, és – adott esetben – egyedi jellemzőit, akinek vagy amelynek a részére a minősített tanúsítványt kibocsátották.

A nagyobb biztonságot garantáló tanúsítványok esetében több személyes adatot is rögzítenek a felhasználóról, amelyeket ellenőriznek is. Ilyen esetekben a személyi igazolvány, az útlevél vagy egyéb azonosító okmányok és dokumentumok bemutatása kötelező. Az ellenőrzés során az okmányban szereplő fénykép és aláírás ellenőrzését (igénylővel való összevetését) is el szokták végezni, így a személyes megjelenés vagy az azzal egyenértékű azonosítás nem kerülhető el. A szolgáltató a felvett adatokat és a bemutatott okmányokat különböző hatósági nyilvántartásokban is ellenőrizheti (például lakcímnyilvántartás, okmánynyilvántartás stb.). Ha egy szervezet nevében kérünk tanúsítványt, ekkor a személyes identitáson túl a szervezet azonosságát is igazolni kell (például alapító okirat), ezen kívül egy hiteles dokumentum is szükséges arról, hogy a szervezet hozzájárul a tanúsítvány igényléséhez.

5.2.2 Tanúsítványok telepítése

A tanúsítványokat telepíteni szükséges azokba a rendszerekbe, ahol használni szeretnénk őket. Az aláírások készítésekor, és az aláírások ellenőrzésekor is csak telepített, hozzáférhető tanúsítványt tudunk használni. Bár főként az utóbbi esetben van rájuk szükség, az aláírás során is felmerülhet a kezelésük, különösen, ha az aláíró több különböző titkos kulccsal rendelkezik, illetve az aláírás során a tanúsítványt hozzá kell csatolni az aláíráshoz. A tanúsítványok egyrészről segítenek a megfelelő kulcs kiválasztásában, másrészről az elfogadhatósághoz szükséges további információkat is tartalmaznak (például az is a tanúsítványban van jelezve, hogy a tanúsítvány minősített, és a kulcs minősített eszközön található).

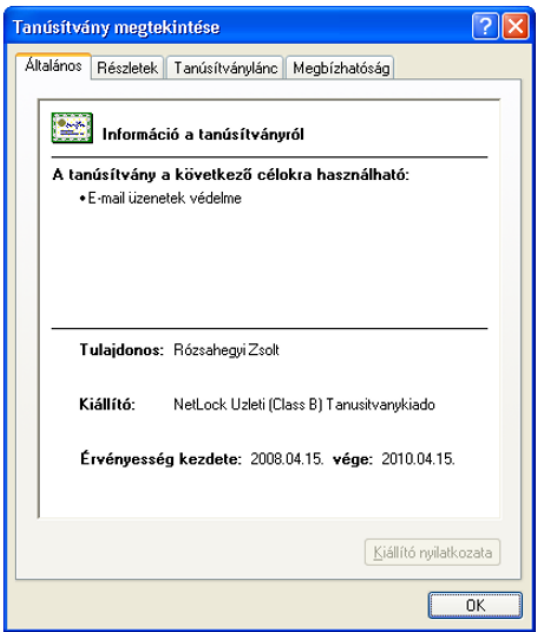
A tanúsítványok telepítése során különbséget kell tenni a titkos kulccsal rendelkező tanúsítványok, és az ilyennel nem rendelkező tanúsítványok között. Az előbbiek lesznek a saját

tárolónkban, az utóbbiak pedig a más emberek vagy szolgáltatók tárolójában (a telepítő erre kiemelten figyel). A tanúsítványokat úgy kell telepíteni, hogy a tanúsítvány importáló varázslóra (Windows rendszerekben) kétszer rákattintunk, és néhány egyszerű kérdés után a program a megfelelő tárolóba helyezi az importálni kívánt tanúsítványt. A tanúsítványok exportálását hasonló módon el tudjuk végezni. A tanúsítványok és kulcsok törölhetők is, ami a lejárt és visszavont tanúsítványok esetében lehet szükséges.

5.2.3 Tanúsítványok használata

A saját – nem minősített – és a mások tanúsítványainak menedzselése között az a különbség, hogy a titkos kulcsokkal való műveletekre értelemszerűen csak a saját tanúsítványok esetében van lehetőség (és van értelme), míg mások tanúsítványainál csak és kizárólag a nyilvános kulcsokkal lehetséges műveleteket végezni. Érthető, mivel, ha hozzá lehetne férni mások titkos kulcsaihoz, ez egyben annak kompromittálódását is jelentené, és azokat rögtön vissza kellene vonni. Minősített tanúsítványok biztonságos aláírás-létrehozó eszközön kezelhetők, ami azt jelenti, hogy a titkos kulcs az eszközt semmilyen módon nem hagyhatja el – még a tulajdonos kedvéért sem. Ez esetben a tulajdonos is csak engedélyt ad a PIN-kódjával a titkos kulcsának használatára a biztonságos eszközön, annak megismerése és kimásolása nélkül, mivel ez még a kulcs tulajdonosa számára sincs megengedve és lehetővé téve. A tanúsítványok tartalmának megjelenítését a Windows egy több megjelenítési lappal rendelkező ablakban végzi. Az első fül alatt (főoldalon) a legfontosabb információk kivonata található:

- a tanúsítvány felhasználási célja,
- a tanúsítvány tulajdonosának és kiállítójának neve, és
- a tanúsítvány érvényessége.



1. ábra: A tanúsítvány főbb adatainak megjelenítése

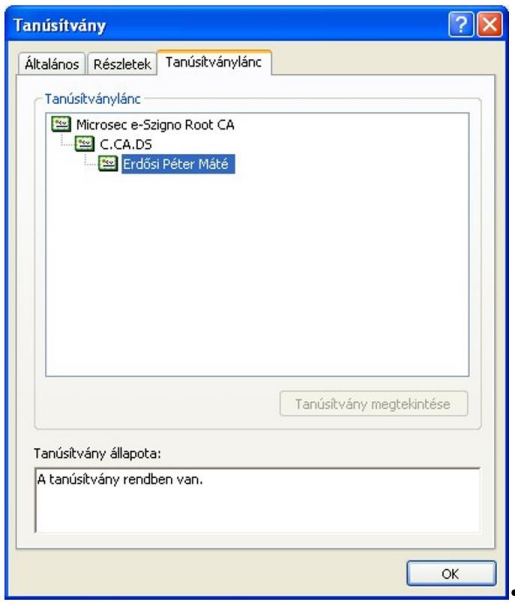
A bal felső sarokban található tanúsítvány szimbólum kinézete szerint különböző jelentést hordoz. Különleges jelzés nélküli formában az egyszerű pecsétszimbólum azt jelzi, hogy a tanúsítvánnyal nincs probléma. Egy piros körben megjelenő fehér kereszt feltűnése arra utal,

hogy a tanúsítvány nem érvényes (mert pl. lejárt), vagy mert a kibocsátó szervezet nincs benne a megbízható hitelesítőszervezetek listájában. A kis sárga háromszögben feltűnő felkiáltójel pedig azt jelenti, hogy a Windows nem képes a tanúsítvány ellenőrzésére (mert például nem rendelkezik a kibocsátó egység tanúsítványával). Az állapotokra vonatkozó szöveges információ is megjelenik a szimbólum alatt (a felhasználási cél helyett).

A főlapon a **Kiállító nyilatkozata / Issuer Statement** gomb automatikusan megjeleníti a szolgáltató által megjeleníteni kívánt információt, jellemzően a vonatkozó szabályzatot, amelyre majd a „Hozzáférés a kiállítói információkhoz” toldalék fog pontosan rámutatni.

A második fül („Részletek”) alatt a tanúsítvány mezőinek tételes tartalma jelenik meg. Ha a tanúsítvány tulajdonosának vagy kibocsátójának neve nem volt egyértelmű, akkor itt a teljes adattartalom megtekinthető. Ugyanígy részletesebb (óra és perc) adatokkal van feltüntetve az érvényességi idő is, valamint itt lehet megtudni a használt algoritmusok típusát és a kulcs jellemzőit is.

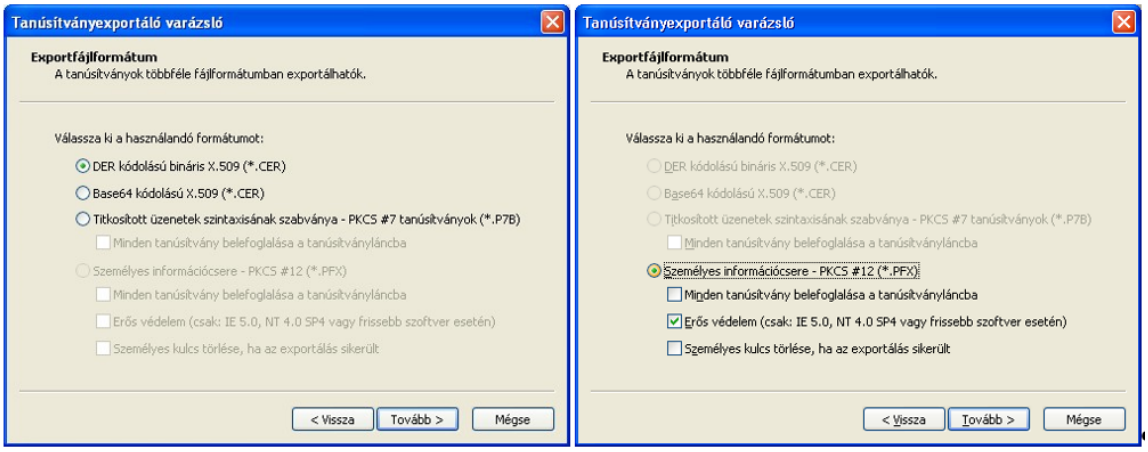
A harmadik lap („Tanúsítványlánc”) a tanúsítási lánc felépítését mutatja és a tanúsítvány állapotát jelzi (a lánc azon tanúsítványának állapotát, amin állunk). Ha a tanúsítvány lejárt vagy más probléma van vele, **A tanúsítvány rendben van.** / **This certificate is OK**. szöveg nem jelenik meg. A tanúsítási lánc valamely tanúsítványtagján állva annak részletes adatait is megtekinthetjük a **Tanúsítvány megtekintése / View Certificate** gomb segítségével.



2. ábra: A tanúsítási lánc megjelenítése

A második oldalon található **Másolás fájlba / Copy To File** gomb segítségével a tanúsítvány különböző formátumú állományokba exportálható.

Exportálásnál megadható, hogy a magánkulcs is exportálódjon-e a tanúsítvánnyal együtt (amennyiben az rendelkezésre áll, a kriptográfiai szolgáltató támogatja a kulcsexportot, az export nincs letiltva és van hozzáférési jogunk). Ennek hatására a varázsló különböző tanúsítványtárolási formátumokat ajánl fel. A formátumtól függően lehet választani a teljes lánc és a tanúsítvány önmagában történő exportálása között. Amennyiben a magánkulcsot is exportálják, beállítható annak erősebb védelmi szintje és az, hogy ezek után a magánkulcs törlődjön-e a védett tárból.



3. ábra: Tanúsítványexportálási formátumok

Gyakorló kérdések:

1. Hogyan lehet hozzájutni tanúsítványokhoz?
2. Hogyan lehet megállapítani, hogy milyen tanúsítványok vannak egy adott rendszerben?
3. Mely esetekben lehetséges a titkos kulcsot is exportálni?

5.3 Digitális tanúsítványok a mai rendszerekben

5.3.1 Tanúsítványtárolók a rendszerekben

A tanúsítványokat és az aláírásokat kezelő **szoftverek**, így például az operációs rendszerek, böngészők, irodai és az aláíró alkalmazások vagy saját tanúsítványtárolóval rendelkeznek, vagy ennek hiányában egy másik alkalmazás (tipikusan az operációs rendszer vagy az ide beépülő kriptográfiai funkció) tanúsítványtárolóját alkalmazzák. Az alkalmazás tanúsítványtárában a saját tanúsítványaink, elfogadott partnereink tanúsítványai, az általunk elfogadott hitelesítésszolgáltatók (gyökér- és kibocsátó) tanúsítványai, a megbízhatatlannak minősített tanúsítványok, a szoftverhitelesítők tanúsítványai, visszavonási listák és tanúsítványbizalmi listák kapnak helyet.

A tanúsítványtárba több módon kerülhetnek be a tanúsítványok és egyéb adatok (pl. visszavonási listák):

- saját tanúsítványaink az igénylés során, illetve azt követően;
- partnereink és szolgáltatók tanúsítványai az elektronikus aláírások elfogadásakor hozott döntéseink során;
- az alkalmazások szállítója is tanúsítványokkal együtt adhatja a szoftverét, amit az új szoftververziók, javítókészletek kibocsátásával frissíthet is; valamint
- a Microsoft a negyedéves frissítés kapcsán is bővítheti az addigi tanúsítványok körét a rendszerben.

Tekintettel arra, hogy a bekerülést megelőző biztonsági vizsgálatok szintje különböző is lehet, azt kell mondanunk, hogy az így bekerülő tanúsítványok megbízhatósági szintje is lehet különböző.

5.3.1.1 Windows tanúsítványtár

A Windows saját **tanúsítványtárral** (Certificate Store) rendelkezik. Ez a nyilvántartás már az újonnan telepített operációs rendszerek esetében is tartalmaz tanúsítványokat, például a Microsoft által megbízhatónak tartott szolgáltatók tanúsítványát (köztük a magyar bizalmi szolgáltatók gyökértanúsítványait is). A nyilvántartás később saját, partnereink és az általunk megbízhatónak tekintett szolgáltatók tanúsítványaival gyarapodik, ahol a tanúsítványokat az interneten keresztül töltjük le, vagy más módon importáljuk őket.

A tanúsítványtár a következő fontosabb logikai egységekre tagozódik:

- **Személyes (Personal):** ez a saját tanúsítványok könyvtára, ahol olyan tanúsítványok tárolódnak, melyek magánkulcsával is rendelkezünk. Tipikusan saját részre vagy a felügyeletünk alatt álló számítógépek és alkalmazások részére kibocsátott tanúsítványok. Az itt tárolt tanúsítványok mellett a hozzájuk tartozó magánkulcsra és kriptográfiai szolgáltatóra is van utalás.
- **Más személyek (Other People):** olyan végfelhasználói tanúsítványok listája, amelyek hitelesítésszolgáltató által aláírtak, és ezért implicit megbízhatóak, valamint nem rendelkezünk hozzájuk titkos kulccsal (például itt vannak levelezőpartnereink tanúsítványai, miután telepítettük őket).
- **Közbenső szintű hitelesítésszolgáltatók (Intermediate Certification Authorities):** tanúsítványokat kibocsátó szolgáltatói tanúsítványok tárolási helye.
- **Megbízható legfelső szintű hitelesítésszolgáltatók (Trusted Root Certification Authorities):** megbízhatónak minősített hitelesítésszolgáltatók gyökértanúsítványai.
- **Megbízható gyártók (Trusted Publishers):** a megbízhatónak minősített szoftverhitelesítők tanúsítványai.
- **Nem megbízható közzétevők (Untrusted Certificates):** megbízhatatlannak minősített tanúsítványok (általunk vagy a Microsoft által).

A Windows minden felhasználónak vagy szolgáltatásnak biztosítja a saját tároló létesítésének lehetőségét, de lehet közös tárolót is használni többfelhasználós környezetben. Ez a megkülönböztetés a tárolók rendszergazdai kezelésekor lehet fontos, amikor a rendszer minden egyes felhasználójának a tárolójáról gondoskodni szükséges.

5.3.1.2 A tanúsítványtár és a védett tár biztonsága

A megbízhatónak minősített szolgáltatói tanúsítványok listájának sértetlensége biztonsági szempontból ugyanannyira **kritikus**, mint magánkulcsunk védelme. Ha a jogosultakon – jellemzően a rendszergazdákon és a felhasználókon – kívül bárki képes tanúsítvány elhelyezésére a listában, akkor azzal olyan aláírások elfogadására vehetik rá az aláírások elfogadóját, amit egyébként nem tenne. Méghozzá úgy, hogy ez észrevétlen marad mindaddig, míg a listát felül nem vizsgálják, illetve amíg be nem következik valamilyen probléma a visszaélés miatt. A magánkulcsokat a Windows egy védett tárban (protected store) tárolja. A védelem itt egy rejtjeles tárolási formát jelent, amiről a CryptoAPI gondoskodik.

Hálózatos környezetben a magánkulcsok és a tanúsítványok részei a felhasználói profilnak, és amikor a felhasználó először jelentkezik be egy hálózati gépre, átmásolódnak oda a profilgazda szerverről. Ugyanígy a menet közben szerzett kulcsok és tanúsítványok a profil ré-

szeként kijelentkezéskor a profilgazda gépre is felmásolódnak. Ez a kényelem okozhat biztonsági problémát, ha a felhasználók a magánkulcsukat számos gépen otthagyják, ami megkönnyíti azok rosszhiszemű megszerzését, különösen, ha a gép kikerül a védett környezetből, például javítási vagy selejtezési okokból.

Linux rendszereken a Mozilla Network Security Services (NSS) szolgáltatásai védik a titkos kulcsokat. Itt csak az tudja a titkos kulcsokat is tartalmazó tanúsítványokat telepíteni, exportálni vagy törölni, aki ismeri a tanúsítványokhoz tartozó jelszavakon kívül az NSS mesterjelszavát is – amit nyilvánvaló módon megfelelően erősre kell választani a kialakításakor. A mesterjelszónak a rendelkezésre állására is szükséges gondolni, mivel ennek hiányában a titkos kulcsokat már nem lehetséges menedzselni.

Gyakorló kérdések:

1. Hogyan állapíthatóak meg egy tanúsítvány fizikai paraméterei?
2. Mit kell tenni a tanúsítványok biztonsága érdekében?
3. Milyen funkciókat biztosít egy tanúsítványmenedzsment-alkalmazás?

5.3.2 A személyes tanúsítványok kiválasztása, használata és ellenőrzése

5.3.2.1 Választás a tanúsítványok közül

Amennyiben a felhasználó egyetlen egy tanúsítvánnyal rendelkezik, annak felhasználása nagyrészt teljesen automatikus tud lenni, mivel az azt kezelő alkalmazások számára nem kérdés, hogy mely tanúsítványt kell felhasználni az aláírás során. Ugyanez igaz lehet még akkor is, ha a felhasználónak több különböző célú tanúsítványa van, pl. egy aláíró és egy titkosító. Az alkalmazások a tanúsítványban megjelölt célnak megfelelően ki tudják **választani** a használni kívánt tanúsítványt. Az aláírás persze nem a tanúsítvánnyal, hanem az ahhoz tartozó magánkulccsal jön létre, de a magánkulcsot a tanúsítványban szereplő nyilvános kulcs azonosítja.

Amennyiben azonban a felhasználó **több aláíró vagy bélyegző tanúsítvánnyal** is rendelkezik (pl. egy minősített céges bélyegző és egy minősített személyes aláíró tanúsítványa is van), akkor az aláírás során neki kell kiválasztania az alkalmazni kívánt tanúsítványt. Ezt minden egyes aláírás alkalmával meg kell tennie, hacsak az alkalmazásban valamilyen módon nem konfigurálható a felhasználási móddal összefüggésben a szükséges tanúsítvány automatikus használata. A tanúsítványok kiválasztása során kellő gondossággal kell eljárni. Fontosabb megkülönböztető adatok lehetnek a tulajdonosok, a kibocsátók, a tanúsítvány minősítettsége, a céges vagy privát használatot pedig megkülönbözteti az e-mail cím. A tanúsítvány kiválasztásakor a megkülönböztető adatokat kell megvizsgálni, és ezek szerint kiválasztani a megfelelő tanúsítványt.

5.3.2.2 Eljárás kompromittálódás esetén

Ha valaki a kulcshordozója (a kártya vagy a számítógép) eltűnését észleli, azonnal **fel kell függesztenie** a tanúsítvány használatát, és kezdeményeznie kell a tanúsítvány felfüggesztését vagy visszavonását a kibocsátó szolgáltatónál. Ugyanígy kell tennie, ha megalapozottan vélelmezhető a magánkulcshoz való jogtalan hozzáférés. Ilyen esetekben nem szabad tovább megbízni az eddig alkalmazott védelmi megoldásokban (bármilyen körültekintően lettek is megvalósítva), és az aktivizáló adat (PIN-kód) által nyújtott védelemben.

Amennyiben a magánkulcs használatát meg kell szüntetnünk, érdemes a tanúsítványt felfüggeszteni, illetve visszavonatni, és ezek mellett a magánkulcsot is hozzáférhetetlenné tenni (pl. biztos helyre zárni vagy megsemmisíteni). Nem szabad a számítógép háttértárolóján hagyni a magánkulcsot, ha a gépet eladják vagy kölcsönadják, hanem a kulcsot tartalmazó fájlokat biztonságos törlést alkalmazva javasolt törölni.

5.3.2.3 Fizikai tanúsítványformátumok

Az X.509 szabvány **nem szabályozza** a tanúsítvány fizikai (bájt szintű) tárolását. Az egyes mezők kódolására a DER (Distinguished Encoding Rules) kódolást írja elő, de emellett azonban széles körben elterjedtek más kódolási módszerek is. Ilyen például a Base64, melyet az elektronikus levelezés kapcsán fejlesztettek ki bináris csatolt állományok kódolására, így implementációja minden internetes applikációban megtalálható. Az adott formátum könnyen felismerhető. Elegendő egy szövegszerkesztővel szövegként megnyitni a tanúsítványt. Ha nem látunk szöveget, akkor egy DER, ha pedig a „BEGIN CERTIFICATE" szöveget látjuk, akkor az egy PEM tanúsítvány lesz Base64 kódolással. Elterjedt a használata az RSA Laboratories által kifejlesztett két formátumnak is, a PKCS #7-nek (Cryptographic Message Syntax Standard) és a PKCS #12-nek (Personal Information Exchange). Az előbbi lehetővé teszi egy állományban több tanúsítvány összefogását is (egymástól független tanúsítványokat vagy egy tanúsítási lánc tagjait), és a tanúsítványok mellett különböző attribútumok tárolását is meg tudja oldani. Az utóbbi képes a tanúsítvány mellett a magánkulcs tárolására is, valamint szintén magába tudja foglalni egy tanúsítási lánc minden tanúsítványát. E két tárolási forma így tulajdonképpen nem csak tanúsítványkódolási forma, de tanúsítványtárformátum is.

A különböző tanúsítványformátumok eltérő kiterjesztésű állományok formájában öltenek testet. A DER és Base64 kódolású tanúsítványok DER, CER vagy CRT kiterjesztést kapnak, a PKCS #7 kódolásúak P7B, P7C vagy SPC, a titkos kulcsot is tartalmazó PKCS #12 kódolásúak P12 vagy PFX kiterjesztést. Ezeket a formátumokat a Windows mind ismeri és kezeli, exportálhatóak a belső tanúsítványtárból, illetve importálhatóak oda. A visszavonási listák szintén előfordulhatnak PKCS #7 formátumú tárakban és CRL kiterjesztésű PEM állományokban.

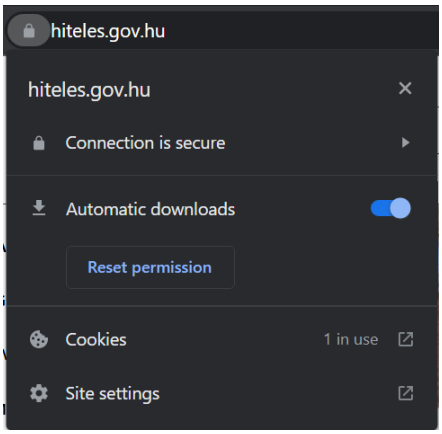
Gyakorló kérdések:

1. Hogyan kell kiválasztani a személyes tanúsítványokat?
2. Mit kell tenni a tanúsítvány kompromittálódása esetén?
3. Milyen különböző tanúsítványkódolási formátumok léteznek?

5.3.3 A tanúsítványok ellenőrzése

5.3.3.1 Webszerver-tanúsítványok

A dokumentumok hitelesítésén és az elektronikus levelezésen kívül még máshol is lehet tanúsítványokkal találkozni. Az internetes böngészés során számos alkalommal találkozunk a **webszerver-tanúsítványokkal** (SSL/TLS tanúsítványoknak is nevezik a webszerver által alkalmazott biztonságos kommunikációs protokollra utalva). Ha meglátogatunk egy weboldalt, és a címsorban a webhely neve előtt **https://** előtagot, ez előtt pedig egy lakat ikont látunk, akkor az a weboldal tanúsítvánnyal védett lesz. A lakatra kattintva megjelennek a weboldal adatai, és megnézhető itt a szerver tanúsítványa is.



4. ábra: Biztonságos webszerver-tanúsítvány

A webszerverek tanúsítványainak az ellenőrzésekor három fontos dologra kell odafigyelni. Az első a tanúsítvány érvényessége. Mivel lejárt és érvénytelen tanúsítvánnyal is lehetséges kommunikációt kezdeményezni, a felhasználón múlik annak megítélése, hogy megbízik-e az ilyen kommunikációban, vagy inkább óvatos lesz, ha ilyet lát. A második fontos elem a kibocsátó megbízhatósága. Amennyiben a kibocsátó szerepel a böngésző tanúsítványtárában, akkor jobban megbízhatunk benne, míg, ha nem, nem árt az óvatosság ekkor sem. A harmadik lényeges eleme a webszerverek tanúsítványainak a védeni kívánt weboldalak feltüntetése. A tanúsítvány alanyait egyrészről a „Tulajdonos” (Subject) mező, másrészről a „Tulajdonos alternatív neve” (Subject Alternative Name) mező tartalmazza. Ha a weboldal URL-címe nem szerepel ezekben a mezőkben, akkor azt a tanúsítványt nem annak a weboldalnak a védelmére állították ki, amelyiket éppen meglátogattuk, az óvatos megközelítésmód ebben az esetben is erősen ajánlott. Figyelem, ebben az esetben a „www.valami.hu” és a „valami.hu” domain nevek különbözőknek számítanak!

5.3.3.2 Szoftvertanúsítványok

További találkozási lehetőség a **szoftvertanúsítványok** esete. Ilyen leginkább akkor látható, ha egy alkalmazás letöltése után elindítjuk azt. Amennyiben a telepítőcsomag rendelkezik digitális aláírással, akkor a futás engedélyezése során megtekinthető a csomag kibocsátójának az aláírása is. Ma már szinte minden professzionális alkalmazást ilyen aláírással ellátva bocsátanak ki, és ha a kibocsátó tanúsítványát már megbízhatónak elfogadtuk, akkor az ellenőrzés teljes mértékben a háttérben fog megvalósulni. A beállításoktól függően a szoftverek indításakor megjelenhet egy Biztonsági figyelmeztetés (Security Warning) ablak is, ami nem feltétlen valamely veszélyre hívja fel a figyelmet, hanem annak ellenőrzését kínálja fel, hogy a gépre éppen települni szándékozó programhoz a gyártója adta-e a nevét. A képernyőn ilyenkor látható a letöltendő alkalmazás neve, a gyártó szervezet neve, és hogy milyen jogosultságokat kér az alkalmazás (pl. Full Permissions). A szervezet nevére kattintva megjelenik az alkalmazás aláírására kibocsátott tanúsítvány. A telepítésre vonatkozó pozitív döntésünket követően a telepítés elindul.

Gyakorló kérdések:

1. Milyen ellenőrzést tesz lehetővé egy tanúsítvány egy webhelyen?
2. Lehetnek-e hibás tanúsítványok?
3. Hogyan biztosítják a tanúsítványok egy szoftver integritását?

5.4 Visszavonási listák, a visszavonási állapot ellenőrzése

A nyilvános kulcsú rendszerek működésének egyik alapfeltétele, hogy a privát, titkos kulcsok szigorúan titokban maradjanak; azokat kizárólag jogos tulajdonosa használja. Azonban a tanúsítványok használati szándéka megváltozhat, az aláíró kötelezettségvállalásait korlátozhatják, és minden szándék ellenére mégis előfordulhat, hogy a privát kulcs vagy az őt hordozó eszköz illetéktelen kezekbe kerül (pl. a privát kulcsot tároló chipkártyát a tulajdonosa elhagyja, vagy a szoftveres tanúsítványt adathordozóval együtt értékesítik). Ilyenkor – az észlelést követő legrövidebb időn belül (azonnal) – le kell tiltani a kulcspár használatát, hiszen ettől kezdve a tulajdonos nem vállalhat felelősséget a használatáért (mivel a használata már nem kizárólag hozzá köthető).

Ennek során a tanúsítvány birtokosa az esetet bejelenti a hitelesítésszolgáltatónak, egyben kéri, hogy a kulcspárhoz kötődő tanúsítványt vonja vissza. Egy kulcspár visszavonásának módszere az, hogy a nyilvános kulcsot felveszik egy úgynevezett visszavonási listára. Adott hitelesítésszolgáltató által kiadott tanúsítványok közül az – adott időpontban – visszavont és felfüggesztett tanúsítványokat tartalmazó, kibocsátó által aláírt lista a **visszavonási lista** (certificate revocation list – CRL). A visszavonási lista legfontosabb funkciója az, hogy a nem megbízható módon keletkezett aláírásokat fel tudjuk ismerni, azaz bármely aláírást, amely a visszavonás időpontja után keletkezet ne tekinthessük érvényesnek. Fontos azonban biztosítani, hogy a visszavonást megelőzően készített aláírások érvényesek maradjanak.

A tanúsítvány lejárat előtti **érvénytelenségét** három tényező okozhatja, amelyek után a visszavonást kezdeményezni szükséges:

- a tanúsítványlánc bármely eleméhez tartozó aláíró adat bizalmasságának sérülése,
- az alkalmazott aláírási algoritmus vagy kulcshossz gyengesége,
- szervezeti okok, mint például megváltozott szervezeti egység vagy szereplő lett a tanúsítvány új birtokosa.

A lejárat után a tanúsítvány szintén elveszti az érvényességét.

5.4.1 A visszavonási lista és funkciói

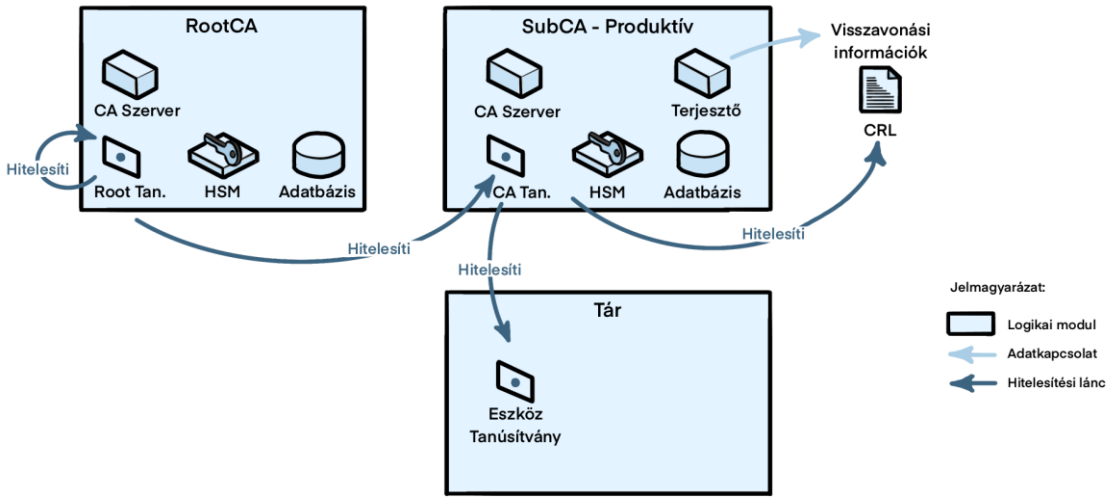
Az aktuális visszavonási listákat (CRL) a szolgáltató előre meghatározott időközönként hozza nyilvánosságra, a következő CRL megjelenésének időpontját az előző CRL tartalmazza.

Két CRL publikálása között eltelt idő lehet:

- **Változó:** ekkor a szolgáltató eseményvezérelten bocsátja ki CRL-t, és így minden esetben, amikor változik egy – általa kibocsátott – tanúsítvány állapota, új CRL-t bocsát ki. Ekkor az elérhető legfrissebb CRL mindig az aktuális információt fogja tartalmazni.
- **Fix:** ekkor periodikus kibocsátású lesz a CRL, amikor egy tanúsítvány megváltozott állapota a következő CRL kibocsátáskor lesz észlelhető a nyilvánosság számára.

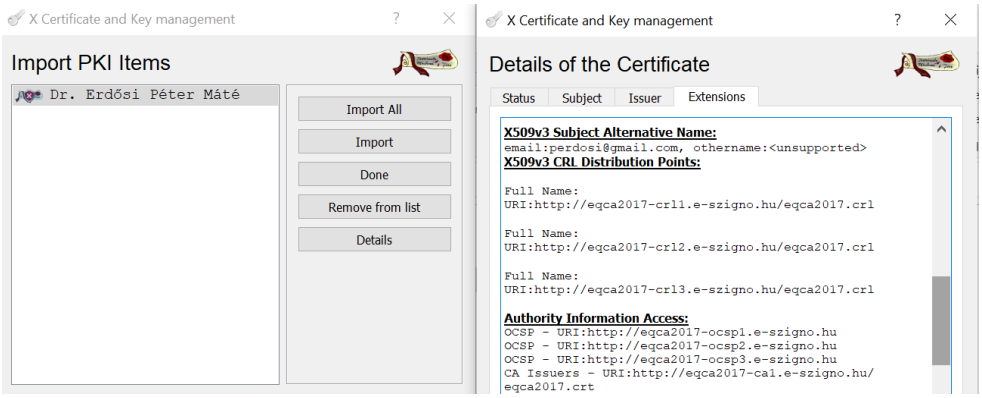
A végfelhasználói tanúsítvány esetében a visszavonási listákat jellemzően 24 óránként frissítik. A szolgáltatói tanúsítványok állapota ettől ritkábban szokott megváltozni, ezért a szolgáltatói visszavonási listák kibocsátási időköze ettől jóval nagyobb lehet, több hónap is elfogadható ebben az esetben.

Ennek következménye, hogy a tanúsítvány érvényességére vonatkozóan bizonyosságot csak a teljes láncolatra vonatkozó, az aláírást követően legelőször kiadott CRL-ek begyűjtése után tudunk mondani. Ez a legtöbb ügyviteli, üzleti folyamatban nem kivárható, ezért általában az első, a tanúsítvány birtokosára vonatkozó CRL után a legtöbb ügyviteli folyamatot a felek folytatják, vagy az online állapotot preferálják.



5. ábra: CRL publikálása

A **CRL feltalálási helyére** vonatkozó információ benne van a tanúsítványban, ezek megnevezése és helye a tanúsítvány megtekintésekor kinyerhető belőle (a keresett link végén .crl kiterjesztés található).



6. ábra: A CRL helye a tanúsítványban

A CRL-t az adott kibocsátó a saját aláírásával látja el, ennek révén a **CRL hitelessége** ellenőrizhető. Teljesen akkor lehetünk biztosak a tanúsítvány érvényességében, ha a CRL aláíró tanúsítványt és annak láncolatának érvényességét is ellenőriztük.

5.4.2 A visszavonási listák beszerzése

A visszavonási listára vonatkozó információ

- egyrészről szerepel a tanúsítványban,

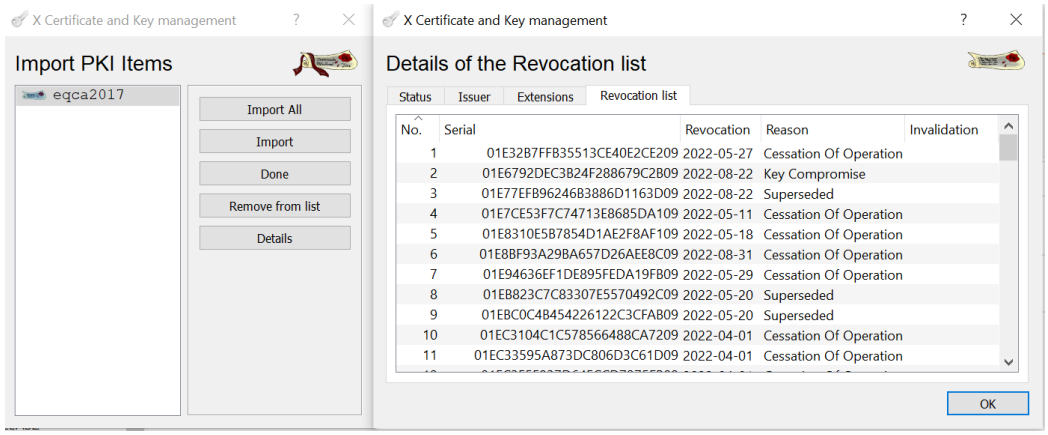
- másrészt minden szolgáltatónak kötelessége a visszavonási listát (listákat) a saját honlapján jól elérhető helyen közzétenni.

5.4.2.1 A visszavonási listák manuális beszerzése a szolgáltatók honlapjairól

A tanúsítvány kiállítójának honlapjáról általában közvetlenül elérhető az adott tanúsítványtípushoz tartozó visszavonási lista, amelyre kattintva az fájlként letölthető, elmenthető.

A visszavonási lista manuális megnyitáskor az általános részben (fülön) láthatók a legfontosabb információk:

- a kiállító,
- a hatályba lépés dátuma,
- a következő frissítés dátuma,
- az aláírás algoritmusa,
- a visszavonási lista sorszáma.



7. ábra: A CRL-ben az adott tanúsítványra vonatkozó információk

A Visszavont tanúsítványok listája ablakon láthatjuk a visszavont tanúsítványra vonatkozóan:

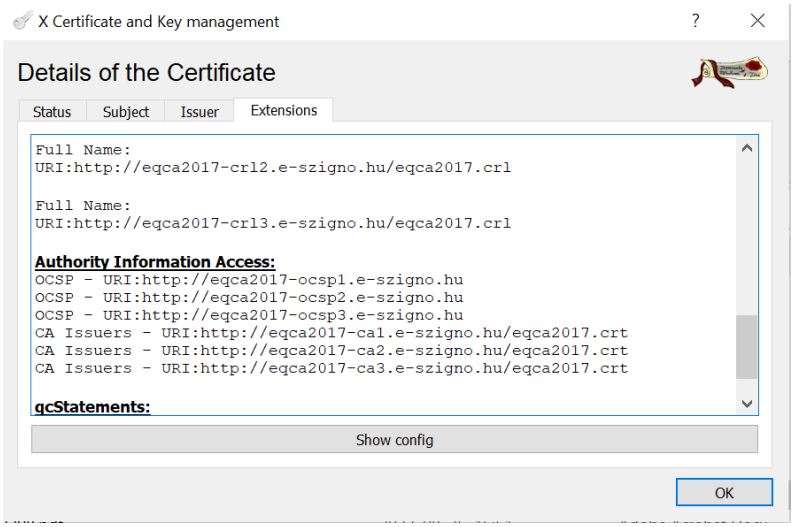
- a tanúsítvány sorszámát (hexadecimális szám formában),
- a visszavonás idejét dátum, óra, másodperc formátumban,
- valamint a visszavonás okát (opcionálisan).

5.4.3 Az online tanúsítványállapot protokoll és használata

Az online tanúsítványállapot protokoll (on-line certificate status protocol: OCSP) lehetővé teszi, hogy csak egyetlen egy adott tanúsítványra vonatkozóan kérdezzük le a szolgáltató adatbázisából az adott tanúsítvány érvényességi adatait, szemben a CRL listával, amely minden visszavont tanúsítványt megmutat.

Az OCSP általában a tanúsítványkibocsátó szolgáltató különálló szolgáltatásaként valósul meg. Az állapotellenőrzés egy kívülről induló kérés, amelyet a tanúsítvány ellenőrzője indít a tanúsítványt kibocsátó szolgáltató felé. Az OCSP-kérésben a legfontosabb információ – amit az ellenőrzéshez elküldenek a szolgáltatónak – a tanúsítvány sorszáma (hexadecimális szám formájában). A válaszadó szolgáltatás a tanúsítványállapot-adatbázisból kiveszi a

megfelelő értéket, és azt aláírásával ellátva visszaküldi a kérdezőnek. A tanúsítványnak tartalmaznia kell az OCSP-szolgáltatás elérhetőségéhez szükséges információt.



8. ábra: Az OCSP elérhetőségére vonatkozó információ egy tanúsítványban

Az OCSP-válasz a következő értékeket tartalmazhatja:

- **Jó (good),** ami, azt jelenti, hogy a tanúsítvány nincs visszavonva. Ez egy állapotjelző, azaz akkor is ez lehet a válasz, ha egy a tanúsítvány már lejárt, mivel az érvényességi idő és a visszavonási állapot ellenőrzése két független ellenőrzést jelent.
- **Visszavonva (revoked),** ami azt jelenti, hogy a tanúsítványt korábban kibocsátották, és már vissza is vonták véglegesen vagy ideiglenesen (felfüggesztés). A válasz tartalmazza a visszavonás pontos idejét is.
- **Ismeretlen (unknown),** ami azt jelenti, hogy az OCSP rendszer nem tud a tanúsítvány állapotára vonatkozó kérdéssel mit kezdeni (mert lehet, hogy nem jó szolgáltatást kérdeztünk meg, vagy nem áll rendelkezésre minden szükséges adat).

Az OCSP-választ a hitelesítésszolgáltató elektronikusan aláírja. A választ kérő és feldolgozó rendszernek ezt az aláírást és érvényességét ugyanúgy ellenőriznie kell, mint bármely más aláírást. Mivel az OCSP egy speciális gépi üzenet, ezért manuálisan nem készíthető el. A szolgáltatók a legtöbb esetben egy webes felületet biztosítanak egy adott tanúsítvány állapotának lekérdezéséhez.

Gyakorló kérdések:

1. Mikor adják ki a visszavonási listát?
2. Milyen adatok szerepelnek a visszavonási listában?
3. Mikor használják az OCSP-t?

6 Az elektronikus aláírások osztályozása és készítése

Az elektronikus aláírási formátumok tetszőleges elektronikus tartalom (adatobjektum) elektronikus aláírására használhatók, azok formátumára való tekintet nélkül. Az adatok lenyomata egyéb információkkal együtt egy külön elemben tárolódik, és ennek az elemnek a lenyomata lesz valójában az elektronikus aláírás bemenete. Az egyéb információktól függ az, hogy az adott aláírás melyik dimenzió mentén, melyik osztályba fog tartozni, ami a használatát befolyásoló lényeges elemként jelenik meg a mindennapi gyakorlatban. Ezekre a – néha csak apró – különbségekre a készítés során is oda kell figyelni.

6.1 Az elektronikus aláírások osztályozása

Az elektronikus aláírásokat az alábbi fontosabb dimenziók mentén lehet osztályozni a gyakorlati felhasználás megkülönböztethetősége érdekében:

1. számosság és egymáshoz viszonyított elhelyezkedés,
2. szabványos tartalom, bonyolultság,
3. joghatás, jogi vélelem.

Ezek a dimenziók egymásban is létrehozhatnak különböző osztályozási rendszereket, például van értelme a szabványos aláírásokon belül elkülöníteni a kézírással egyenértékű aláírásokat az írásbeliséget kielégítő aláírásoktól, habár a szabványos aláírások a minősített és a nem minősített tanúsítványok használata között szintaxisban nem tesznek különbséget, a tanúsítványnak ezen tulajdonsága az aláírásoknál szemantikai szinten jelentkezik.

6.1.1 Egyszeres és többszörös aláírások és tulajdonságaik

Ezeknek az alkalmazásoknak a segítségével az egyszerű és a párhuzamos digitális aláírások mellett létrehozhatóak a szekvenciális aláírások is, amikor az aláírások egymás után, mintegy egymásba becsomagolva helyezkednek el, és ellenőrzésüknél is csak kívülről befelé lehet haladni. A párhuzamos aláírások elkészítésénél akár egyszerre több ember is aláírhatja a dokumentumot, de ezzel az aláírások nem épülnek egymásba, az aláírások egymás mellett léteznek és kezelhetőek, ellenőrzésük tetszőleges sorrendben elvégezhető. Vegyes aláírás lehet a különböző szerződések ellenjegyzése, ami egy párhuzamos aláírásból, illetve egy következő szinten történő, szekvenciális aláírásból áll.

6.1.1.1 Az egyszeres aláírás tulajdonságai

Miután elkészült a dokumentumhoz az elektronikus aláírás, azt valamilyen módon hozzá kell csatolni a dokumentumhoz. Amennyiben egyetlen aláírás csatolása a feladat, azt az következő módokon lehetséges a dokumentumhoz rögzíteni:

1. különálló aláírás (*detached signature*): az aláírás a dokumentumtól, az aláírandó információktól teljesen külön van kezelve, nem függ annak mozgatásától vagy tárolásától, egyedül annak tartalmától,
2. beágyazódó aláírás (*enveloping signature*): az aláírásba ágyazódnak bele az aláírandó információk, tartalmazási értelemben alacsonyabb szinten, az aláírásnak a része lesz az aláírandó tartalom,

3. beágyazott aláírás (*enveloped signature*): az aláírás beágyazódik egy magasabb szintű aláírt egységbe, belefoglalódik annak tartalmába.

Azt, hogy mikor melyiket alkalmazzák, függ az aláírás céljától és a kötelezettségvállalásban elfoglalt helyétől is. Az aláírásoknak ez a felosztása nem függ az aláírás kódolási eljárásától.

6.1.1.2 A többszörös aláírás fajtái

A mindennapi életben gyakran előfordul, hogy egy dokumentumot több személynek kell aláírnia, hitelesítenie. Erre a hétköznapi gyakorlatnak és szervezeti, működési hierarchiának megfelelően kétfajta többszörös aláírás formátum használatos.

Párhuzamos aláírás

Egy már meglévő (egyszeres vagy többszörös) aláíráshoz egy újabb független aláírás adódik hozzá. A párhuzamos aláírás azt jelenti, hogy az újonnan hozzáadott aláírás a meglévőkkel egyenrangú aláírás, és nem függ a korábbiaktól semmilyen módon. A párhuzamos aláírás az aláírásába belefoglalhat nulla, egy vagy több, az aláírt XML-dokumentumban jelen levő tetszőleges elemet.

A párhuzamos aláírás hétköznapi felhasználására egy példa, amikor egy pénzügyi beszámolóba az egyes üzleti területek munkatársai a saját területük eredményét tartalmazó kimutatásokat csatolják és azt aláírják, mindenki a sajátját.

Ellenjegyző aláírás

Egy már meglévő (egyszeres vagy többszörös) aláíráshoz egy újabb aláírás adódik hozzá. Az ellenjegyző aláírás azt jelenti, hogy az újonnan hozzáadott aláírás a meglévők felett álló, attól függő módon arra rárakódó, a meglévő tartalmat vagy annak egy részét hitelesítő aláírás. Az ellenjegyző aláírás egy referenciát tartalmaz, amely az aláírt adatok elemére mutat.

Az ellenjegyző aláírásra példa a cégbírósági eljárásban a cég társasági szerződésének ügyvédi aláírása, amit az ügyfelek aláírása után helyez el a dokumentumon az ügyvéd, a korábbi aláírásoktól függő, azokat hitelesítő ellenjegyző módon.

Vegyes aláírás

Már meglévő többszörös aláírásokhoz egy újabb, ellenkező hierarchiájú (párhuzamos vagy ellenjegyző) aláírás adódik hozzá. Ebben az esetben megmarad a korábbi aláírások érvényessége, struktúrája, de az új aláírásnak is meg kell felelni az aláírásra jellemző (párhuzamos/ellenjegyző) követelményeknek. Egy dokumentumban technikailag bármennyi és bármilyen hierarchiai kapcsolatot kifejező aláírás lehet.

A vegyes aláírásra példa a cégbírósági eljárás, ahol a cég tulajdonosai a társasági szerződést aláírják (párhuzamos aláírással), amelyet az ügyvéd még ellenjegyző aláírással lát el.

Gyakorló kérdések:

1. Melyek a többszörös aláírás fajtái?
2. Mi a különbség az egyszeres és a többszörös aláírás között?
3. Mit jelent a vegyes aláírás?

6.1.2 Szabványos aláírások és tulajdonságaik

Az információ archiválási igényeinél tehát megjelentek az értelmezési információk is, amelyek nélkül a tárolt adat nem értelmezhető. Ezek láthatóságán és megismerhetőségén túl követelménnyé vált hosszú távon ezek megőrzése is. Ha egy információs struktúra elemeinek értelmezési tartománya széles, akkor sok értelmezési információt kell hozzá megőrizni. Ebből az is adódik, hogy az értelmezési információk leírása több helyet fog felemészteni, ha számos paramétert kell megvizsgálni és értelmezni annak elfogadásáig. Az elektronikus aláírás – célja miatt – rengeteg részletes információt tartalmaz a kötelezettségekről, az aláíróról és annak hitelességéről, ami bonyolulttá teszi az aláírás, mint információs struktúra számítógépes kezelését, feldolgozását. Szükségessé vált tehát az aláírások megjelenési formáinak szabványosítása.

A paraméterek szabványosításánál két paramétertípussal lehet találkozni: egyrészről a paraméter létezését minden aláírásban azonos megnevezéssel kötelezően előíró szabály, másrészről a paraméter értékére csak egy bizonyos értékeket tartalmazó, előre felsorolt tartalmú listából kiválasztást engedélyező szabály írja le a szabványos aláírások kötelező és választható tartalmát. A szabványosítás kiterjedt a rövid és a hosszú távon érvényes aláírásokra egyaránt.

Legelsőként az RFC 3126 szabályzat (később az RFC 5126) fogalmazott meg formátumfüggetlen műszaki követelményeket a hosszú távon érvényes elektronikus aláírásokkal szemben, ezeket később az ETSI is átvette és kiterjesztette a fokozott biztonságú aláírások készítésére és ellenőrzésére (ETSI EN 319 102-1). Az ETSI szabványok külön részletezték a különböző formátumokra (CMS[17], XML[18] és PDF[19]) érvényes specifikus követelményeket is, létrehozva a CAdES, XAdES és PAdES aláírásokat, majd később a fokozott biztonságú aláírással ellátott XML-alapú konténereket (ASiC) is[20].

Az aláírások típusainak kialakulását nagymértékben befolyásolta az, hogy milyen időtávon mennyire kell az aláírásban részt vállaló komponensek (tanúsítványok, visszavonási információk) érvényességéről és a létrejöttének időpontjáról meggyőződni. Nyilvánvaló módon, ha hosszabb időtávon kell egy aláírás érvényességéről meggyőződni, több információ begyűjtése és megőrzése szükséges hozzá.

Nagyon fontos megállapítás továbbá, hogy mind a CAdES, mind a XAdES, mind pedig a PAdES formátumú elektronikus aláírások – és bélyegzők – kielégítik az eIDAS által az „advanced”, vagyis „fokozott biztonságú” elektronikus aláírásokkal – és bélyegzőkkel – szemben támasztott követelményeket.

Emlékezzünk arra, hogy az eIDAS három aláírás- és bélyegzőfajtát különböztet meg különböző joghatások kiváltására alkalmasságuk szempontjából:

1. **normál aláírás / bélyegző**: amelynek nincsenek követelményei a definíció kielégítésén túl, a meg nem tagadhatóság vonatkozik rá,
2. **fokozott biztonságú aláírás / bélyegző:** amelynek komolyabb követelményei vannak, és így alkalmas az írásbeliség követelményének kielégítésére (AdES). A követelmények az alábbiak:

[17] Lásd ETSI EN 319 122-1 és ETSI EN 319 122-2
[18] Lásd ETSI EN 319 132-1 és ETSI EN 319 132-2
[19] Lásd ETSI EN 319 142-1 és ETSI EN 319 142-2

a) alkalmas az aláíró / bélyegző azonosítására,

b) egyedülállóan az aláíróhoz /bélyegzőhöz köthető,

c) olyan eszközökkel hozták létre, amelyek nagy megbízhatósággal kizárólag az aláíró / bélyegző befolyása alatt állnak,

d) és a dokumentum tartalmához olyan módon kapcsolódik, hogy minden – az aláírás elhelyezését követően a dokumentumon tett – módosítás érzékelhető,

3. **minősített aláírás:** olyan fokozott biztonságú aláírás, amelyet biztonságos aláírás-létrehozó eszközzel készítettek, és amelyhez minősített tanúsítványt bocsátottak ki, ezért alkalmas a kézírással egyenértékű jogok biztosítására.

4. **minősített bélyegző:** olyan, fokozott biztonságú elektronikus bélyegző, amelyet minősített elektronikus bélyegzőt létrehozó eszközzel állítottak elő, és amely elektronikus bélyegző minősített tanúsítványán alapul, így esetében vélelmezhető a hozzájuk kapcsolódó adatok sértetlensége és a bélyegzőnek megfelelő eredet.

Ebből következik, hogy egyrészről, ahol a jogszabályok legalább fokozott biztonságú aláírásokat kötnek ki, ott a szabványos aláírások vagy bélyegzők és az azokat előállító alkalmazások biztonsággal használhatóak, másrészről a minősített aláírásokhoz vagy bélyegzőkhöz az aláírás- vagy bélyegző-létrehozó eszközön túl a tanúsítvány kibocsátóját is megfelelően kell megválasztani az előírásoknak való megfeleléshez. Másszóval a minősített aláírások és bélyegzők is az alábbi szabványos aláírások valamely formáját veszik fel, egy speciális – minősített – tanúsítványelemmel és tanúsított eszközzel kibővülve.

6.1.2.1 Normál aláírások

A normál aláírások halmazába az alap- és az explicit politika alapján előállított elektronikus aláírások tartoznak.

1. **Alap aláírások:**

   a. **AdES-BES (BES: Basic Electronic Signature, alap elektronikus aláírás):** azt a minimumszintet írja le, amit egy fokozott biztonságú aláírásnak kötelezően tartalmaznia kell. Az alapszintű aláírás három komponensből tevődik össze, mégpedig az aláíró dokumentuma, aláírt attribútumok és a digitális aláírás.

   b. **AdES-EPES (Explicit Policy based Electronic Signature – explicit politika alapján készült aláírás):** kifejezett, explicit aláírási politika alapján készült aláírás. Az aláírási politika olyan dokumentum, mely rögzíti az adott érintett felek (aláíró, ellenőrző) számára azokat az explicit tulajdonságokat, eljárásokat, melyeket megkövetelnek egymástól az aláírás készítése és ellenőrzése során ahhoz, hogy az aláírás érvényessé, elfogadhatóvá váljon. Ez az aláírás egy adattal – az aláírási politika azonosítójával – tartalmaz többet, mint az előző aláírás-típus.

Az alapaláírás tehát ott használható, ahol az aláírás érvényességének megállapítása az aláírást követő rövid időn belül megtörténik, és az érvényesség utólagos, újbóli ellenőrzése – hosszú távon – nem követelmény. Tipikusan ilyen lehet az elektronikus ügyintézések során

[20] Lásd ETSI EN 319 162-1 és ETSI EN 319 162-2

egy beküldött aláírt ügyféldokumentum, melynél csupán azt kell a fogadónak megállapítania, hogy valóban az ügyféltől érkezett-e és sértetlenül, mert a további feldolgozásban a hitelességet a fogadó a saját eljárásaival biztosítja, és ennek feladatait így nem hárítja a küldőre.

6.1.2.2 Érvényességi adatokkal ellátott aláírások

Az elektronikus aláírások érvényességének megállapításához további adatok lehetnek szükségesek, melyeket **érvényességi adatoknak** neveznek, és amelyek a következőkből állnak:

1. nyilvános kulcsú tanúsítványok (aláíró vagy tulajdonság),
2. visszavonási állapotinformáció minden tanúsítványhoz,
3. megbízható időbélyeg az aláíráshoz vagy számonkérhető pontosságú időjel,
4. az aláírási politika részletes előírásai az elektronikus aláírás ellenőrzéséhez (opcionális).

Az érvényességi adatokat szolgáltathatja mind az aláíró, mind az ellenőrző, de együtt is lehetnek felelősek az összes szükséges érvényességi adat összegyűjtéséért és előállításáért.

6.1.2.2.1 Időponttal ellátott aláírások

Az időponttal ellátott aláírások lesznek az **AdES-T (Electronic Signature with Time, időponttal ellátott aláírás)** aláírások. Ha az alapaláírást kiegészítjük időbélyeggel vagy időjellel, akkor jutunk ehhez a formához. A megbízható időponttal ellátott előírások alapvető fontosságúak az érvényesség hosszú távon fenntartható megítélhetőségében. Az aláírás elkészítési időpontjának megbízható jelölése teremt lehetőséget arra, hogy az aláírás érvényességének későbbi megállapításakor ne az aktuális állapotból, hanem az aláírás elkészítéséhez tartozó állapotból lehessen kiindulni.

Megbízható időt két módon lehet kapcsolni az alapaláírásokhoz:

1. időbélyeg segítségével vagy
2. megbízható időjel csatolásával.

Az időponttal ellátott aláírások tartalma az AdES-BES/EPES aláíráson **felül** csak egy olyan **időponttal** bővül, mely lehet

1. **időbélyeg**ek esetében signature-time-stamp attribútum vagy
2. a BES/EPES aláírásokon **időjel** (ebben az esetben az időjel pontossága a megbízható harmadik fél, az időjel-szolgáltató felelőssége).

6.1.2.2.2 Komplex aláírások

Komplex aláírásnak nevezzük az **AdES-C (ES with Complete validation references – elektronikus aláírás teljes érvényességi hivatkozásokkal)** formátumú aláírást. Ebben az aláírásban az aláírás ellenőrzéséhez szükséges összes tanúsítvány- és visszavonási információ, hivatkozás referenciáját hozzácsatolják az aláíráshoz. A referencia azt jelenti, hogy az érvényességi adat nem jelenik meg az aláírásban, csak az elérhetőségi helye, amelynek felkeresésével és az ott található információk ellenőrzésével az aláírás érvényessége megállapíthatóvá válik. Tartalma (az AdES-T aláíráson túlmenően) csak a teljes tanúsítvány- és visszavonási referenciákkal – de nem az adatokkal – egészül ki.

A komplex aláírást csak akkor lehet létrehozni, amikor minden olyan adat és annak referenciája előállt, amely az érvényesség megállapításához szükséges. Addig nem lehetséges elkészíteni a komplex aláírást, amíg minden érvényességi adat elő nem áll.

6.1.2.2.3 Kiterjesztett aláírások

A komplex aláírásokat ki lehet terjeszteni további aláíratlan attribútumokkal, melyek az aláírás érvényességének megállapítását nagyon hosszú időtartamig teszik lehetővé, illetve az érvényesség megállapíthatóságát ebben az esetben nem veszélyezteti számos olyan katasztrófaesemény sem – jellemzően a titkos kulcsok aláírást követő kompromittálódása vagy cseréje, mely az érvényesség korábbi időpontra vonatkozó megállapítását lehetetlenné teszik. Az ilyen adatokkal kiterjesztett komplex aláírásokat kiterjesztett vagy kiterjesztett tartalmú aláírásoknak nevezik. A kiterjesztett aláírások (a komplex aláíráson túlmenően) kiegészülnek minden tanúsítványadattal és visszavonási információval (tanúsítványláncok, visszavonási listák mind az aláíró, mind a tanúsítványkibocsátó és annak legfelső szintű kibocsátója tekintetében).

Ha fennáll a veszély, hogy a szolgáltatói aláíró kulcs kompromittálódott, szükségessé válhat elhelyezni további időbélyegzőt a kiterjesztett aláíráson annak bizonyítására, hogy az aláírás valamely érvényesítési adat kompromittálódása előtt keletkezett, illetve az érvényességi adatok is megbízhatóak voltak az adott időpontot megelőzően. A kiterjesztett időbélyeget kétféleképpen lehet elhelyezni az aláíráson:

1. a teljes aláíráson (attribútumokon, digitális aláíráson és referenciákon együttesen) elhelyezett időbélyeg,
2. vagy csak a tanúsítvány- és visszavonási referenciákon van időbélyeg.

Ha ezeket az aláírásokat kiegészítjük az összes releváns érvényesítési adattal, a hosszú kiterjesztett aláíráshoz jutunk (**AdES-X Long**). Első esetben a teljes aláíráson (attribútumokon, digitális aláíráson és referenciákon együttesen) elhelyezett időbélyeg után illesztik be az érvényesítési adatokat, míg a második esetben a tanúsítvány- és visszavonási referenciák időbélyegzését követően írják bele az aláírásba az érvényesítési adatokat.

6.1.2.2.4 Archív aláírások

Mielőtt a használt kriptográfiai algoritmusok meggyengülnének, és a kriptográfiai funkciók sebezhetővé válnának, vagy az időbélyegzést támogató tanúsítványok elavulnának, az aláírt adatokat, a komplex aláírásokat (AdES-C) és a további információkat tartalmazó aláírásokat (AdES-X) időbélyegzéssel kell ellátni – amennyiben lehetséges, erősebb algoritmussal, mint az eredetit. Ezeket a hozzáadott információkat és időbélyeget **AdES-A (Archival Electronic Signature, archív elektronikus aláírásnak)** néven ismerjük. A felülbélyegzési eljárást periodikusan meg kell ismételni, amikor a gyengülés veszélye fennáll. Egy archív aláírás többszörösen beágyazott időbélyegeket is tartalmazhat, attól függően, hogy hányszor történt meg a felülbélyegzése.

Az archív aláírás készítése láthatóan a legbonyolultabb eljárás, és nem feltétlenül egyszeri művelet. A kriptoanalízis (rejtjelfejtés) fejlődésével egyes algoritmusok biztonsági szintje megváltozhat, elavulhat. Ekkor továbbra is meg kell őrizni az archív aláírás érvényességét, annak megállapíthatóságát, ami ezt követően csak akkor biztosítható, ha az aláírás hitelességét a kor műszaki színvonalán elfogadott algoritmusokkal újra és újra biztosítják. Erre a

hosszú távú megőrzéskor gondolni szükséges, és a megfelelő folyamatokat ki kell alakítani ehhez.

6.1.2.3 PDF alapú aláírások

A Portable Document Format (PDF), más szóval az ISO 32000-1 szabvány szerinti formátumban elkészített dokumentumok elterjedése általánosnak mondható az egész világon. Az ingyenesen és szabadon elérhető PDF-megjelenítők eredményeként az olvashatóságnak sem platform, sem szoftver nem szab gátat. Megjelent tehát az igény a PDF-dokumentumok szabványos elektronikus aláírására is. Az ISO 32000-1 szabvány a digitális aláírásokkal kapcsolatban három tevékenységet támogat:

1. dokumentum azonnali aláírása,
2. aláírási mező létrehozása jövőbeli aláírások számára, és
3. aláírások érvényességének ellenőrzése.

Az ETSI frissítette a 2009 júliusában kibocsátott TS 102 778 szabványcsaládot a PDF-alapú fejlett vagy magyar terminológiában fokozott biztonságú aláírások (PAdES: PDF Advanced Electronic Signature) készítésének további egységesítése érdekében. Az új szabványcsalád két részből áll:

1. ETSI EN 319 142-1 PAdES digitális aláírások; 1. rész: Építőelemek és alapszintű PAdES aláírások
2. ETSI EN 319 142-2 PAdES digitális aláírások; 2. rész: További PAdES aláírási profilok

Két dolgot érdemes itt megjegyezni: az egyik az, hogy a PAdES aláírások is megfelelnek az eIDAS-nak, azaz fokozott biztonságú aláírások ebben a formában is létrehozhatók, másrészről ugyanazokat az elemeket lehet használni PDF alapú dokumentumok esetében is, amelyeket korábban a CMS vagy XML kódolású aláírások már használtak.

A dokumentumok formátuma tehát már nem akadálya az elektronikus aláírás elhelyezésének, az ismert és elterjedt formátumok esetében.

Gyakorló kérdések:

1. Hogyan osztályozza a szabvány az aláírásokat? Miért bővebbek a kiterjesztett aláírások?
2. Milyen tartalommal rendelkezik az archív aláírás?
3. Milyen plusz adatinformáció van az AdES-A típusú aláírásban az AdES-C típusú aláíráshoz képest?

6.1.3 A normál, a fokozott biztonságú és a minősített aláírás joghatásai

A jogi vélelmek olyan feltételezések, amit egy bírósági vagy hatósági eljárásban igaznak kell tekinteni. A jogi vélelmeknek két típusa van: az egyik a megdönthető vélelem, a másik pedig a megdönthetetlen vélelem. A megdönthetetlen vélelmek esetében az ellenkező bizonyításának nincs helye, ezzel szemben a megdönthető vélelmek esetében van lehetőség a vélelemben megfogalmazott állítás ellenkezőjének bizonyítására. Az elektronikus aláírással kapcsolatos szabályozás területén csak megdönthető vélelmekkel találkozunk. (A vélelmek szerepe a jogéletben rendkívül jelentős, lényegében egy jogi vélelem a bírósági és hatósági eljá-

rásban egy tény bizonyításának terhét jelenti, és ezáltal a jogi eljárásban részt vevő ellenérdekű felek álláspontja közül az egyikük számára védett helyzetet hoz létre.)

Az elektronikus aláírások joghatásával kapcsolatosan az eIDAS rendelet a 25. cikkben három előírást fogalmazott meg, amelyek minden tagállamra kötelező érvényűek az Európai Unióban:

1) Az elektronikus aláírás joghatása és bírósági eljárásokban bizonyítékként való elfogadhatósága nem tagadható meg kizárólag amiatt, hogy az elektronikus formátumú, illetve nem felel meg a minősített elektronikus aláírásra vonatkozó követelményeknek.

(2) A minősített elektronikus aláírás a saját kezű aláírással azonos joghatású.

(3) A valamely tagállamban kibocsátott minősített tanúsítványon alapuló minősített elektronikus aláírást az összes többi tagállamban el kell ismerni minősített elektronikus aláírásként.

Az elektronikus bélyegző joghatása kicsit eltérően, de azért igen hasonlóan alakul az eIDAS 35. cikkében:

(1) Az elektronikus bélyegző joghatása és bírósági eljárásokban bizonyítékként való elfogadhatósága nem tagadható meg kizárólag amiatt, hogy az elektronikus formában létezik, illetve nem felel meg a minősített elektronikus bélyegzőkre vonatkozó követelményeknek.

(2) A minősített elektronikus bélyegzők esetében vélelmezni kell a hozzájuk kapcsolódó adatok sértetlenségét és a bélyegzőnek megfelelő eredetét.

(3) A valamely tagállamban kibocsátott minősített tanúsítványon alapuló minősített elektronikus bélyegzőt valamennyi tagállamban el kell ismerni minősített elektronikus bélyegzőként.

Az elektronikus ügyintézésről szóló törvény implementációja során az elektronikus aláírások joghatásával kapcsolatos eIDAS követelményeket, illetve azok működéséhez szükséges elemeket tovább részletezte és egészítette ki a magyar szabályozás. Jogi vélelmeket fogalmazott meg az elektronikus ügyintézésről szóló törvény (Eübszt.) a minősített elektronikus aláírással, a minősített időbélyegzés, az aláírás-létrehozó adat elhelyezése és az archiválási szolgáltatásokkal kapcsolatosan. Fontos előírása, hogy az aláírást és a bélyegzőket egyenértékűnek kell tekinteni, ha más rendelkezés nincs kimondva:

99. § (2) Ahol valamely jogszabály elektronikus aláírást vagy elektronikusan aláírt dokumentumot említ, azon kifejezett eltérő rendelkezés hiányában elektronikus bélyegzőt vagy elektronikus bélyegzővel ellátott dokumentumot is érteni kell.

További vélelmeket fogalmazott meg a minősített elektronikus aláírással aláírt elektronikus dokumentumok tekintetében a 2016. évi CXXX. törvény a polgári perrendtartásról (Pp.) a bizonyítási eszközként történő felhasználás tekintetében. A jogi vélelmek mellett az elektronikus aláírások joghatásával kapcsolatosan a polgári törvénykönyv (Ptk.), valamint - az elektronikus aláírással aláírt elektronikus dokumentumok bizonyítási eszközként történő felhasználásának tekintetében -különböző egyéb eljárási jogszabályok fogalmaznak meg további előírásokat.

Például a Pp. 325. § [A teljes bizonyító erejű magánokirat] fejezete kimondja, hogy

(1) Teljes bizonyító erejű a magánokirat, ha

a) a kiállító az okiratot saját kezűleg írta és aláírta,

b) két tanú igazolja, hogy az okirat aláírója a részben vagy egészben nem általa írt okiratot előttük írta alá, vagy aláírását előttük saját kezű aláírásának ismerte el; igazolásként az okiratot mindkét tanú aláírja, továbbá az okiraton a tanúk nevét és – ha törvény eltérően nem rendelkezik – lakóhelyét, ennek hiányában tartózkodási helyét olvashatóan is fel kell tüntetni,

c) az okirat aláírójának aláírását vagy kézjegyét az okiraton bíró vagy közjegyző hitelesíti,

d) az okiratot a jogi személy képviseletére jogosult személy a rá vonatkozó szabályok szerint megfelelően aláírja,

e) ügyvéd vagy kamarai jogtanácsos az általa készített okirat szabályszerű ellenjegyzésével bizonyítja, hogy az okirat aláírója a más által írt okiratot előtte írta alá vagy aláírását előtte saját kezű aláírásának ismerte el,

f) az elektronikus okiraton az aláíró a minősített vagy minősített tanúsítványon alapuló fokozott biztonságú elektronikus aláírását vagy bélyegzőjét helyezte el, és – amennyiben jogszabály úgy rendelkezik – azon időbélyegzőt helyez el,

g) az elektronikus okiratot az aláíró a Kormány rendeletében meghatározott azonosításra visszavezetett dokumentumhitelesítés-szolgáltatással hitelesíti, vagy

h) olyan, törvényben vagy kormányrendeletben meghatározott szolgáltatás keretében jött létre, ahol a szolgáltató az okiratot a kiállító azonosításán keresztül a kiállító személyéhez rendeli és a személyhez rendelést a kiállító saját kezű aláírására egyértelműen visszavezethető adattal együtt vagy az alapján hitelesen igazolja; továbbá a szolgáltató az egyértelmű személyhez rendelésről kiállított igazolást elektronikus dokumentumba kapcsolt, elválaszthatatlan záradékba foglalja és azt az okirattal együtt legalább fokozott biztonságú elektronikus bélyegzővel és legalább fokozott biztonságú időbélyegzővel látja el.

Ha tehát valamelyik említett módszernek megfelelő módon állítottuk elő az okiratot, annak teljes bizonyító ereje van, ami azt jelenti, hogy az ellenkező bebizonyításáig ezt kell érvényesnek tekinteni. Tekintettel arra, hogy a felsorolt módozatok közül több is elérhető manapság, a teljes bizonyító erejű elektronikus okiratok előállításának most már nincs sem jogi, sem technológiai akadálya.

A Ptk. az írásbeliséget így határozza meg:

6:7. § [Írásbeli alakhoz kötött jognyilatkozat]

(1) Ha a jognyilatkozatot írásban kell megtenni, az akkor érvényes, ha legalább a lényeges tartalmát írásba foglalták.

(2) Ha e törvény eltérően nem rendelkezik, a jognyilatkozat akkor minősül írásba foglaltnak, ha jognyilatkozatát a nyilatkozó fél aláírta.

(3) Írásba foglaltnak kell tekinteni a jognyilatkozatot akkor is, ha annak közlésére a jognyilatkozatban foglalt tartalom változatlan visszaidézésére, a nyilatkozattevő személyének és a nyilatkozat megtétele időpontjának azonosítására alkalmas formában kerül sor.

(3a) Ha jogszabály eltérően nem rendelkezik, az ingatlannal kapcsolatos, valamint az öröklési jogi, családjogi, társasági jogi, illetve pénzügyi szolgáltatási jogviszonnyal összefüggésben elektronikus úton tett jognyilatkozat kizárólag akkor minősül írásba foglaltnak, ha annak tart-

alma írásjegyekkel rögzített és eleget tesz az elektronikus okirat létrehozására irányadó jogszabályi követelményeknek.

Nem lehet nem felfedezni a hasonlóságot a fokozott biztonságú elektronikus aláírás eIDAS rendeletben meghatározott követelményei (26. cikk) és az itt leírtak között:

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.

Megismételjük a legfontosabb megállapítást a normál elektronikus aláírásokról: „Az elektronikus aláírás joghatása és bírósági eljárásokban bizonyítékként való elfogadhatósága nem tagadható meg kizárólag amiatt, hogy az elektronikus formátumú, illetve nem felel meg a minősített elektronikus aláírásra vonatkozó követelményeknek.” Ehhez még hozzá lehet fűzni azt, hogy az elektronikus aláírás olyan adat, amelyet az aláíró aláírásra használ, de csak akkor lesz fokozott biztonságú az aláírás, ha további követelmények is teljesülnek az előbb felsoroltak szerint.

A törvény indoklásából és más jogászi véleményekből is kiderül, hogy habár a korábbi elektronikus aláírásra vonatkozó törvény hatályon kívül helyezése következtében a fokozott biztonságú aláírás és az írásbeliség explicit kapcsolata a magyar jogrendből kikerült, de implicit módon mégis benne maradt, , mivel továbbra is általánosan elfogadott az , hogy a fokozott biztonságú aláírással teljesíthetők a Ptk. írásbeliség számára megfogalmazott követelményei.

Tekintettel arra, hogy a fokozott biztonságú aláírás is olyan normál elektronikus aláírás, amelyik teljesít még további követelményeket, természetesen a normál aláírásokhoz fűződő jogi vélelem ugyanúgy megilleti, mint azokat az aláírásokat, amelyek nem érik el a nem fokozott biztonságú aláírások szintjét.

A fokozott biztonságú elektronikus bélyegzőkre vonatkozó követelmények kicsit eltérnek az aláírásra vonatkozó követelményektől, mivel a fokozott biztonságú elektronikus bélyegző készítője jogi személy, emiatt a fokozott biztonságú elektronikus bélyegzők számára az alábbi követelmények teljesítése a követelmény:

a) kizárólag a bélyegző létrehozójához kötött;

b) alkalmas a bélyegző létrehozójának azonosítására;

c) olyan, elektronikus bélyegző létrehozásához használt adatok felhasználásával hozzák létre, amelyeket a bélyegző létrehozója nagy megbízhatósággal kizárólag saját maga elektronikus bélyegző létrehozására használhat;

d) olyan módon kapcsolódik azokhoz az adatokhoz, amelyekre vonatkozik, hogy az adatok minden későbbi változása nyomon követhető.

A bélyegzőkhöz fűződő jogi vélelmek is igen hasonlítanak az aláírásokra vonatkozó vélelmekhez. Sok változás tehát nem lelhető fel a bélyegzőkhöz és az aláírásokhoz fűződő jogi vélelmek között, ami érthető is, mivel ez a megkülönböztetés 2016 előtt nem is létezett.

6.1.4 Minősített aláírások és bélyegzők jogi elismerése

Az Európai Unió egységesen szabályozta a minősített aláírások és bélyegzők joghatását az eIDAS rendeletben (Az Európai Parlament és a Tanács 910/2014/EU rendelete (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről. Minden tagállamban – így Magyarországon is – tehát egységesen kötelező az elektronikus aláírások és elektronikus bélyegzők, valamint időbélyegzők joghatásait figyelembe venni a már említettek szerint.

A „minősített elektronikus aláírás” fogalma számos nemzeti jogszabályunkban szerepel ma már, néhány példa:

- 2019. évi LXXX. törvény a szakképzésről: 11. § (2)-(3) A képzési és kimeneti követelményeket – a Kormány adott ágazatért felelős tagjának egyetértésével – a szakképzésért felelős miniszter hivatalos kiadványként az általa vezetett minisztérium honlapján (a továbbiakban: honlap) teszi közzé. A képzési és kimeneti követelmények normatív rendelkezést nem tartalmazhatnak és azok tartalma jogszabállyal és közjogi szervezetszabályozó eszközzel nem lehet ellentétes. A képzési és kimeneti követelmények a honlapról nem távolíthatók el, archiválásukra a digitális archiválás szabályait kell alkalmazni. A közzétett képzési és kimeneti követelményeket a szakképzésért felelős miniszter minősített elektronikus aláírásával és olyan szolgáltató által kiadott időbélyegzővel kell ellátni, amely e szolgáltatást minősített szolgáltatóként nyújtja. A képzési és kimeneti követelményekben a közzététel időpontját és az alkalmazás kezdő dátumát fel kell tüntetni. A közzététel időpontja nem lehet korábbi, mint az időbélyegzőben szereplő naptári nap.
- 2014. évi XL. törvény, 32/A. § (7)-(8) A pénzügyi intézmény kivonatához csatolt tájékoztatóban nyilatkozni kell a szabályozás rendszeréről, struktúrájáról, a szabályozási szintekről és azok egymáshoz való viszonyáról. A pénzügyi intézmény kivonatát és a (7) bekezdés szerinti tájékoztatót szerkeszthető elektronikus formában – minősített elektronikus aláírással ellátva a) elektronikus levélben és b) elektronikus adathordozón is be kell nyújtani.
- És egy negatív (kizárásos) példa: 2015. évi XLII. törvény, 6. § (4)-(5) A jognyilatkozat akkor is írásbelinek tekinthető, ha annak közlésére a jognyilatkozatban foglalt információ változatlan visszaidézésére, a nyilatkozattevő személyének és a jognyilatkozat megtétele időpontjának azonosítására alkalmas elektronikus dokumentumban (a továbbiakban: elektronikus dokumentum) kerül sor. A nyilatkozattevő személyének (4) bekezdés szerinti azonosításához nem szükséges a nyilatkozattevő elektronikus aláírása vagy minősített elektronikus aláírása.

Megállapíthatjuk tehát, hogy a magyar jogrend is számos helyen említi a minősített elektronikus aláírást/bélyegzőt, ennek elterjedése folyamatosan növekszik, és ez az egyetlen olyan aláírás/bélyegző, amelyet az egész Európai Unió területén egyöntetűen el kell fogadni.

6.1.4.1.1 Bizalmi szolgáltatást nyújtók felelőssége

Tekintettel arra, hogy a tanúsítványkibocsátók bizalmi szolgáltatásokat nyújtanak, az eIDAS **emelt szintű felelősséget** ír elő a szolgáltatók számára. A rendelet felelősségi szabályainak a lényege az, hogy a szolgáltatóknak gondoskodniuk kell arról, hogy amennyiben a tevékenységük eredményeként valakit kár ér, akkor a károsult kártalanítása gyorsan megtörténhessen. Nagyon fontos rendelkezés az is, hogy a minősített bizalmi szolgáltató szándékosságát vagy gondatlanságát kell vélelmezni, kivéve, ha a minősített bizalmi szolgáltató bizonyítja, hogy a kár nem az ő szándékos vagy gondatlan működése miatt következett be. Természetesen komoly műszaki háttér szükséges ahhoz, hogy a szolgáltató képes legyen bebizonyítani azt, hogy a bekövetkezett kár ellenére minden tőle telhetőt megtett annak érdekében, hogy elkerülhesse az ilyen eseteket.

A rendelet ezeknek az emelt szintű felelősségi szabályoknak a betartását kizárólag a **minősített tanúsítványt** kibocsátó szolgáltatókra vonatkozóan követeli meg. A szolgáltatóknak ez az emelt szintű felelőssége leginkább a minősített tanúsítványban szereplő adatok valótlanságából, vagy az aláírás-létrehozó adat rossz helyre való továbbításából eredő károkért áll fenn. Továbbá a szabályozás lehetőséget biztosít a szolgáltatók számára, hogy a felelősségük mértékét korlátozzák vagy felelősségüket bizonyos felhasználási cél esetére kizárják. A szolgáltatói felelősség korlátozásának érvényességi feltétele az, hogy a szolgáltató a minősített tanúsítványban feltüntesse a kár mértékére vagy a felhasználási célra vonatkozó felelősségkorlátozást.

Gyakorló kérdések:

1. Mit kell biztosítani az eIDAS szerint a tagállamokban az elektronikus aláírás jogi elismerésében?
2. Melyek a minősített bizalmi szolgáltatókkal kapcsolatos garanciális elvárások?
3. Melyek az aláírásokkal kapcsolatos követelmények és mik a feltételeik?

6.2 Az elektronikus aláírások és bélyegzők készítése

Egy elektronikus aláírás vagy bélyegző elkészítése a gyakorlatban azt jelenti, hogy valamely kiválasztott algoritmuskészlettel és ismert kulcsokkal jól meghatározott eljárásrendet követve létrejön egy vagy több olyan adat, amit egy másikhoz csatolnak hitelesítés céljából. A mai gyakorlatban az esetek nagy részében – amikor összefoglaló néven elektronikus aláírást vagy bélyegzőt használnak – ez digitális aláírást jelent. Ennek értelmében az elektronikus aláíráson és bélyegzőn belül megkülönböztetett és a leggyakrabban használt nyilvános kulcsokon alapuló digitális aláírás folyamatait ismertetjük ebben a fejezetben. Attól függően lesz a digitális aláírásból elektronikus aláírás vagy elektronikus bélyegző, hogy az aláíráshoz tartozó nyilvános kulcsot aláírási célú vagy bélyegzési célú tanúsítványba foglalták-e bele. Ezzel egyúttal be is mutattuk a digitális aláírások és az elektronikus aláírások közötti különbséget, ami indokolja a kettő megkülönböztetését, azaz nem egyenértékű használatát. A nem digitális aláírások készítésének részletes bemutatásától eltekintünk.

6.2.1 Az aláírás létrehozásra képes alkalmazások típusai

A digitális aláírások készítésére több program áll rendelkezésre. Ezeket aláírási szempontból két fő részre lehet osztani. Az egyik csoportot azok az alkalmazások alkotják, amelyeknek nem az aláírás elkészítése a fő céljuk, mégis tartalmaznak olyan lehetőségeket, hogy az

adott programon belül el lehessen végezni az aláírást. Az aláírást elkészítő programok másik fajtája dedikált alkalmazásként célirányosan foglalkozik az aláírások elkészítésével, valamely adott célú, elektronikus dokumentum feldolgozási folyamatának részeként.

6.2.1.1 Alkalmazások aláírási funkcióval

Digitális aláírás létrehozható a legtöbb levelezőprogramban (pl. MS Outlook, Lotus Notes, Evolution), szövegszerkesztőben (pl. LibreOffice Writer, MS Word), táblázat-kezelőben (pl. LibreOffice Calc, MS Excel), illetve az irodai programcsomagokban fellelhető további alkalmazásokban – mint például a prezentációkészítő alkalmazásokban. Ezek a programok képesek létrehozni és ellenőrizni bizonyos típusú aláírásokat, de összetettebb műveletek elvégzésére vagy bonyolultabb aláírások készítésére nem alkalmasak. Ezek a programok a legtöbb esetben nem csinálnak kezdeti ellenőrzést az aláírás érvényességének ellenőrzése érdekében, de a tanúsítvány érvényességét általában ellenőrzik. Néha nem érvényes tanúsítvánnyal is lehet aláírást készíteni, ha az ellenőrzés következményeként az alkalmazás a felhasználó figyelmeztetése után hajlandó tovább folytatni az aláírás-készítési folyamatot. Nyilván a nem érvényes tanúsítvánnyal készített aláírás minden bizonyítható következményét is az aláíró fél viseli, ezért nincs minden esetben műszakilag korlátozva egy lejárt tanúsítvány használata. Az összetettebb feladatok elvégzése érdekében számos aláírási feladatra specifikálódott program jött létre.

6.2.1.2 Aláírás-készítő alkalmazások

A programfejlesztő cégek számos aláírás-készítő programot fejlesztettek, amelyek különböző kinézetűek, felhasználói felületűek és felépítésűek lehetnek. Azok, amelyek kereskedelmi forgalomba kerülnek vagy a felhasználók széles körét célozzák meg, legtöbb esetben már grafikus felülettel rendelkeznek. Természetesen léteznek parancssorból használható programváltozatok is, de ezek inkább az informatikában jártasabb felhasználók, rendszergazdák, esetleg fejlesztők számára lehet fontos. A különböző alkalmazások kezelőfelülete eltérhet egymástól, de egyformán alkalmasak az elektronikus aláírás és az azzal kapcsolatos egyéb műveletek elvégzésére. Meg kell említeni, hogy az Európai Unió létrehozta a digitális aláírási szolgáltatáscsomagját (Digital Signature Service – DSS[21]), amely szabadon hozzáférhető és felhasználható az érdeklődők számára.

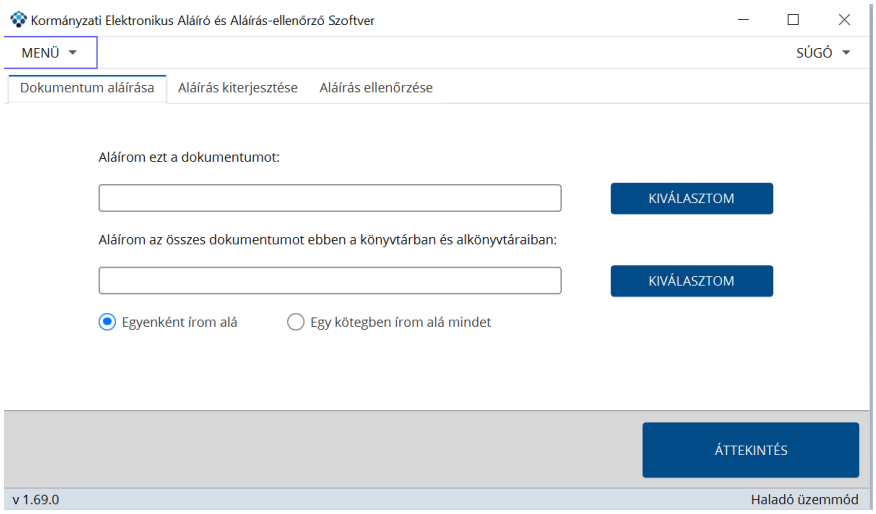
Az egyedi dokumentum egyszeri aláírása mellett lehetőség van az aláírandó dokumentumok különböző rendszerezésére is. Így akár egy egész mappát is lehetséges aláírni, de a mappa elemei külön-külön is aláírhatók. Az aláíró alkalmazások is kezelhetnek dokumentumsémákat, azaz dokumentumkezelési értelemben vett dokumentumstruktúrákat. Ilyen sémák lehetnek az elektronikus cégeljárás, elektronikus beszámoló vagy ezeken kívül elektronikus tértivevény készítése és ellenőrzése is. Az aláírás-típusokat figyelembe véve az elérhető, megvásárolható dedikált alkalmazások java része képes az ismert, szabványos aláírásformátumok előállítására (AdES-BES, AdES-EPES, AdES-T, AdES-C, AdES-X-Long valamint AdES-A), aláírások elkészítésére. Az aláírások készítésére és ellenőrzésére egy programot, vagy két külön szolgáltatást is használhatunk, a fejlesztők, szolgáltatók honlapjairól letölthetők, kipróbálási céllal tesztelhetők vagy teljes funkcionalitásukban használhatók – a gyártó filozófiai megközelítésének függvényében.

[21] Lásd https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Digital+Signature+Service+-++DSS

6.2.1.3 Elektronikus aláírás elkészítése, ellenőrzése

Az aláírás-készítése és adott esetben az ellenőrzése az a funkció, amelyet a legtöbb dedikált aláíró program képes végrehajtani. Az aláírás készítésére vonatkozóan azonban különböző lehetőségeket kínálhatnak fel. A legegyszerűbb esetben egy kiválasztott dokumentumot ír a program alá, ami formálisan a következő lépéseket tartalmazza:

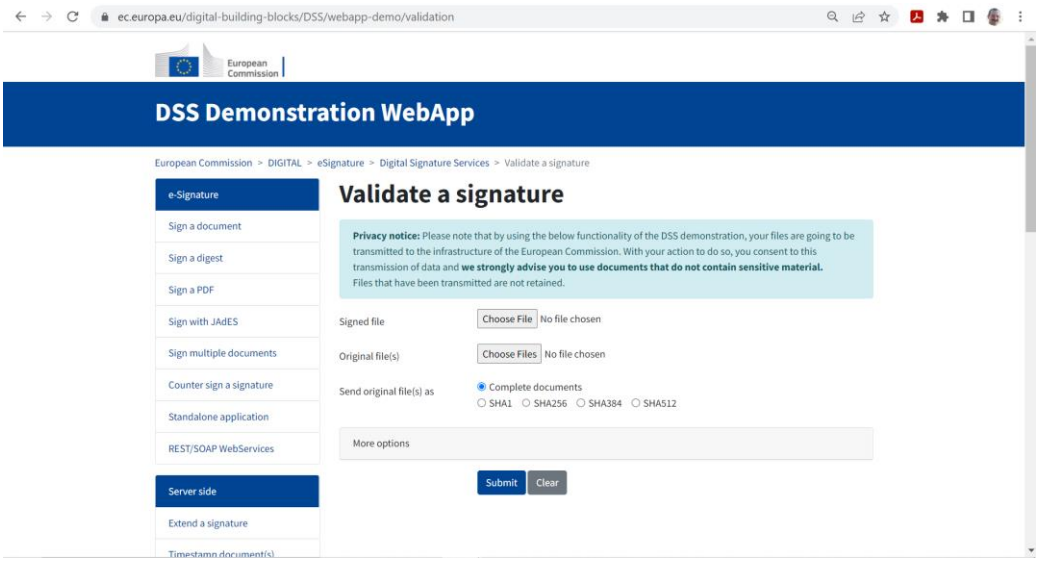
1. A kérdéses dokumentum kijelölése, megnyitása, beillesztése.
2. A dokumentum megjelenik egy kezelőfelületen. A programok általában ikonokkal jelölik a főbb funkciókat (aláírás, ellenőrzés, időbélyeg stb.).
3. A következő lépés az aláírás elkészítése. Mielőtt az alkalmazás elkészítené az aláírást, felajánlja a dokumentum megtekintését, esetleges változtatását.
4. Ezután megjelenik egy tanúsítványtár, itt ki kell választani a használni kívánt tanúsítványt.
5. A program ellenőrzi a tanúsítvány érvényességét. Ha rendben van, elkészíti az aláírást.
6. Az aláírás tulajdonságainak megtekintése is biztosítva van a legtöbb esetben.



9. ábra: A kormányzati aláíró program kinézete

Természetesen nem csak egyetlen dokumentum aláírását lehet egyszerre elvégezni. Létrehozható egy e-dosszié vagy elektronikus mappa, ami több különböző típusú dokumentumot is tartalmazhat. Lehetőség van a teljes mappa vagy a mappa tartalmát alkotó dokumentumok külön-külön történő aláírására is. Az aláírásokat ellenőrizni is lehet, és felhasználás, elfogadás előtt érdemes is. A funkció célja az aktában lévő egyes dokumentumokon (vagy egyetlen dokumentumon) lévő aláírások hitelességének ellenőrzése. Az ellenőrzéshez ki kell jelölni egy aláírást, majd rá kell kattintani az aláírás ellenőrzése funkcióra. Egyes programok soronként lehetővé teszik az ellenőrzés végig követését, mások az eredményt közlik csak a felhasználóval. Ha az ellenőrzés eredménye negatív, hibaüzenettel figyelmeztet a program, ellenkező esetben az aláírás megfelelőségéről szóló ablak jelenik meg a képernyőn. Az aláírások ellenőrzését el tudják végezni az erre a célra kijelölt elektronikus szolgáltatók is, mint amilyen a Kormányzati Elektronikus Aláírás-Ellenőrzés Szolgáltatás (KEAESZ)[22] vagy EU DSS Validáció[23] szolgáltatások.

[22] Lásd https://keaesz.gov.hu/keaesz/validate.html
[23] Lásd https://ec.europa.eu/digital-building-blocks/DSS/webapp-demo/validation



10. ábra: Az EU DSS validációs szolgáltatása

Az aláírás ellenőrzéséhez szükséges a visszavonási állapotok lekérdezése vagy online (OCSP), vagy listaalapon (CRL), ezért offline módon általában nem lehetséges aláírás érvényességét ellenőrizni, ha az aktuális visszavonási állapotok nem érhetők el.

Gyakorló kérdések:

1. Melyek az aláírás létrehozására képes programok típusai?
2. Mi a különbség egy aláíró program és egy aláírásra képes alkalmazás között?
3. Hogyan lehet egy aláírás érvényességéről meggyőződni?

6.2.2 Aláírási politika

6.2.2.1 Az aláírási politika elméletben

Aláírási politika alatt azt a szabályrendszert értjük, amely biztosítja az egyes aláírások érvényességének technikai konzisztenciáját bármely környezetben, ideértve az aláírások készítését és ellenőrzését is. Másszóval az aláírási politika megelőzi azt, hogy ugyanazon aláírást egyik ellenőrzésénél érvényesnek, másik ellenőrzésnél érvénytelennek találjanak ugyanazon érvényességi adatok birtokában csak azért, mert az ellenőrzési eljárások nem konzisztensek – pl. eltérő algoritmust használnak a készítéshez és az ellenőrzéshez, vagy eltérő aláírástípusként akarják értelmezni és ellenőrizni, vagy más-más időzónában a relatív (helyi) időket akarják használni az érvényesség megállapításához. Teljesen nyilvánvaló, hogy egy aláírás érvényessége csak akkor lehet konzisztens **az egész világra** kiterjedően, ha minden egyes helyen és időben ugyanazon érvényességi adatokat gyűjtik be hozzá, és ugyanazon szabályok mentén állapítják meg az érvényességét, ennek hiányában az ellenőrzéskor különböző eredményeket kaphatnak az aláírás elfogadói. Az aláírási politika definícióját és felépítését az alábbi ETSI-standardok tárgyalják részleteiben.

További információkat tartalmaznak a következő dokumentumok:

- ETSI TR 102 038: XML-formátumok az aláírási politikákhoz,
- ETSI TR 102 041: Jelentés az aláírási politikákról,

- ETSI TR 102 045: Aláírási politika kiterjesztett üzleti modellekhez,
- ETSI TR 102 272: ASN.1 formátumok aláírási politikákhoz,
- ETSI TS 101 733: CMS fejlett elektronikus aláírások (CAdES) (4.2, 5.8.1 fejezetek és C.1, C.3.1. függelékek),
- IETF RFC 3125: Elektronikus aláírási politikák.

Az explicit aláírási politikának egyedi azonosítóval kell rendelkeznie az egész világon, amit az aláíró az aláíráshoz csatol az aláírás készítésének részeként. Az aláírási politikának szükséges lehet az emberi olvasható formában való közzététele is, amit hozzáférhetővé kell tenni, hogy kielégíthetőek legyenek az éppen alkalmazott jogszabályi és szerződéses követelmények. Továbbá az elektronikus aláírás automatikus feldolgozhatóságához annak számítógéppel feldolgozható formáját is szükséges rendelkezésre bocsátani.

Az ETSI-dokumentum szerint egy aláírási politikának az alábbiakat kell tartalmaznia:

- szabályokat, melyek egy részleges aláírás technikai ellenőrzéséhez alkalmazhatóak,
- szabályokat, melyek az aláírásra vonatkozó hitelesítési rend tartalmának elfogadásából adódnak (pl. a titkos aláíró kulcs bizalmasságának biztosítása),
- szabályokat, melyek az aláíró által használt környezetre vonatkoznak (pl. elfogadott kártyaolvasó használata a chipkártyával kapcsolatban).

Az aláírás technikai érvényesítésére vonatkozó legfontosabb szabályoknak tartalmazniuk kell az elfogadott gyökér hitelesítésszolgáltatók kulcsait, elfogadható tanúsítványszabályzatokat (hitelesítési rendek, szolgáltatási szabályzatok – ha léteznek), a kötelezően használandó tanúsítványkiterjesztéseket és ezek értékeit – ha vannak ilyenek, a tanúsítványlánc minden eleméhez az érvényességhez szükséges visszavonási státust, az elfogadható időbélyeg-szolgáltatók listáját (ha időbélyegeket is használni kell az aláíráshoz), a számonkérhetőséget biztosító, időjellel ellátott naplóadatokat őrző elfogadott szervezeteket (ha időjel is szükséges), az attribútumtanúsítványokat kibocsátó elfogadható szervezeteket (ha egyáltalán vannak ilyenek a kontextusban) annyira, amennyire a szabályok az elektronikus aláírás elemeit meghatározzák, amelyeket egyrészről az aláírónak kell szolgáltatnia, másrészről az ellenőrző fél számára szükséges biztosítani a hosszú távú érvényesség megállapításához.

6.2.2.2 Az aláírási politika a gyakorlatban

Működő elektronikus aláírási politikára több példát is lehet találni. Hazai viszonylatban a Pénzügyi Szervezetek Állami Felügyeleténél (PSZÁF), az elektronikus közzétételek oldalon jött létre az első, széles körben használatos Elektronikus Aláírási Szabályzat (EASZ) Magyarországon. A szabályzat az alábbi fő fejezetekből áll (részletezve az aláírással kapcsolatos rendelkezéseket):

1. Általános rendelkezések
2. Az elektronikus aláírással kapcsolatos érvényesítési rendelkezések
    a) Az aláíró tanúsítványra vonatkozó megkötések
    b) Az érvényesítő adatokra vonatkozó szabályok
    c) Az aláírás létrehozójára vonatkozó szabályok

d) A kötelezettségvállalás elfogadott típusai

e) A hitelesítésszolgáltatók használatára vonatkozó szabályok

f) Az időbélyegzésre vonatkozó megkötések

g) Az aláírás elfogadójára vonatkozó szabályok

h) A végfelhasználói tanúsítványokra vonatkozó kivárási idő

i) A használható aláíró algoritmusokra vonatkozó szabályok

j) Az elektronikusan aláírt adatszolgáltatás értelmezése, ellenőrzése

3. Az adatszolgáltatásra/bejelentésre kötelezett bejelentkezési kötelezettsége

4. Vitás esetek rendezése

Érdemes kiemelni és közelről megvizsgálni a kötelezettségvállalásra vonatkozó részletet:

„A kötelezettségvállalás azt jeleníti meg, hogy az aláíró milyen szándékkal hozta létre az aláírást. A küldemény csomag esetén a kötelezettségvállalás típusa kötelezően 'Proof of Origin'.

A kötelezettségvállalással az aláíró vállalja a felelősséget, hogy az aláírt dokumentum tartalmát ismeri és ő készítette. Ezt a kötelezettségvállalási típust kötelező elhelyezni valamennyi olyan aláírói dokumentumban, amelyet a KAP szoftver felhasználásával írnak alá.

PROOF_OF_ORIGIN: OID: 1.2.840.113549.1.9.16.6.1

Description: "Elismerem, hogy a dokumentumot en keszitettem es azt elkuldtem.

A tartalmat jovahagyom." (Ékezetek nélkül!)"

Látható, hogy a kötelezettségvállalás és az aláírás ténye között fennálló szándékot is lehet formálisan, külön szabályzatban rögzíteni – ez az aláírási politika egyik fontos feladata. Minden aláírási politika tartalma hasonlóan rögzíti az aláírások készítésével és ellenőrzésével kapcsolatos tudnivalókat a felhasználói kör számára elérhető formában.

További példaként egyszerűsége és elterjedtsége okán álljon itt a PGP aláírási politikája is. Az aláírások típusainak ismertetésénél utalni kell a PGP-világ filozófiájára is, ami a „sok ismerős személy állít valamit, attól lesz megbízható" elvet követi. Nem fogadja el alapértelmezésben azt a rendszert, melyben egy állami hatóság kinevezi magát megbízhatónak, és ezt minden résztvevőnek kötelező elfogadnia.

Az OpenPGP szabvány négy aláírástípust különböztet meg, melyeket 0x10-től 0x13-ig számoz meg, és amely megkülönböztetés a használt tanúsítványokon alapul:

- **0x10: nem kategorizált:** ez a típus a tanúsítványok kategorizálása előtti időkből származik, és azt a célt szolgálta, hogy azt az aláírást jelölje, amely kategorizálását a fogadó nem tudja vagy nem akarja elvégezni,
- **0x11, nagyon alkalmi tanúsítvány:** ez az aláírás olyan kulcs alapján készült, melynek birtokosát az elfogadó személyesen nem ismeri, csak egy harmadik fél által szolgáltatott bizonyítékok alapján, közvetve ítéli megbízhatónak, és az aláíró azonosítását is csak ilyen módon lehetséges elvégezni. A feltüntetett e-mail cím feltételezhetően a kulcsbirtokoshoz tartozik,

- **0x12, személyes ismerős:** ez az aláírás olyan kulcs alapján készült, mely személyes ismerőshöz tartozik, és a kulcs és a személy összetartozása régóta ismert, ezért a kulcsbirtokos személyazonossága és e-mail címe bizonyos az elfogadó számára,
- **0x13, különlegesen megbízható kulcsbirtokos:** eddig még nem használt elvi kategória, akkor használható elvileg, ha kiterjedt kutatás igazolná a kulcsbirtokos minden azonosító adatát – gyakorlatilag ez megegyezik a saját tanúsítvány által igazolt adatok megbízhatóságával.

Az aláírási politikák különösen fontos szerepe az, hogy biztosítják, hogy valamely aláírás megtörténte után nem lehetséges olyan pillanat, amelyben nem dönthető el az aláírás érvényessége vagy érvénytelensége. Ez a garanciája a hitelesség folyamatos, hosszú távú fenntartásának és fenntarthatóságának.

Gyakorló kérdések:

1. Mi az aláírási politika célja és szerepe?
2. Mit kell tartalmaznia egy aláírási politikának?
3. Hogyan lehet működő példákat találni aláírási politikákra?

6.2.3 Aláírások létrehozása irodai alkalmazásokban

6.2.3.1 Aláírások szövegszerkesztőkben

A digitális aláírási funkció a legtöbb ismert **szövegszerkesztőben** (MS Word, LibreOffice Writer stb.) benne van, általuk ismert szolgáltatás. A használatuk során lehet digitális aláírásokat készíteni az adott dokumentumhoz kapcsolódóan, de az aláírásokat tekintve korlátozott funkcionalitással. A szabványos aláírás-típusok közül a szövegszerkesztők a gyakorlatban az alapszintű aláírástípusokat ismerik, több-kevesebb kiterjesztésekkel. Ilyen kiterjesztés például az aláírás célja vagy az aláíráshoz tartozó gépidő belefoglalása az aláírásba – aminek pontossága és hitelessége függ az adott rendszer menedzselésétől.

A Microsoft két – megjelenésében különböző – lehetőséget biztosít az Office-dokumentumok aláírására. A következők egyikét lehet választani:

- látható digitális aláírási sorok adhatók a dokumentumhoz a szükséges digitális aláírások befogadására,
- láthatatlan digitális aláírások adhatók a dokumentumhoz.

Mindkét aláírás digitális aláírás, de azzal a különbséggel, hogy a látható aláírás megjelenik a szövegben, és képi forma is társítható hozzá (például a beszkennelt kézi aláírás), míg a láthatatlan digitális aláírás nem jelenik meg a szövegben, de a tartalma és érvényessége ugyanúgy ellenőrizhető. A látható aláírás folyamata a digitális aláírás elkészítése előtt kiegészül az aláíró adatainak (név, beosztás, e-mail, képfájl) megadásával, azaz a látható adatok beállításával, és csak ezek után ad lehetőséget a (láthatatlan) digitális aláírás elkészítésére.

A szövegszerkesztőben tett digitális aláírások készítéséhez is szükség van tehát aláíró tanúsítványra. A megkapott tanúsítványt fel kell ismertetni az adott rendszerrel, használat előtt például telepíteni kell az adott tanúsítványkezelő rendszer tanúsítványtárába.

A dokumentum aláírásának lépéseit az alábbi elvi lépések gyakorlati megvalósításán keresztül mutatjuk be:

1. a szövegszerkesztőben létre kell hozni egy üres dokumentumot és tetszőleges szöveg, kép, ábra, tartalom beírásával (pl: „saját dokumentum, elektronikusan aláírva”),
2. valamilyen névvel a dokumentumot el kell menteni,
3. következik az aláírási funkciót tartalmazó menüpont kiválasztása:
    a) MS Word Fájl menü / Információ / Dokumentumvédelem / Digitális aláírás hozzáadása,
    b) LibreOffice Writer: Fájl menü / Digitális aláírások / Digitális aláírások… menüpont,
4. klikkelés a „Digitális aláírások” menüpontra,
5. ezután hozzá kell adni az aláírásra használni kívánt tanúsítványt:
    a) MS Word: Módosítás gomb után (ha az alapértelmezett tanúsítvány nem megfelelő),
    b) LibreOffice Writer: Dokumentum aláírása gomb,
6. az aláírás létrehozása az „Aláírás” gombra kattintással megtörténik.

A sikeres aláírást az állapotsorban feltűnő kis pecsét alakú ikon jelzi. Ha a felhasználó erre az ikonra kattint, megnézheti, hogy kitől származik az elektronikus aláírás.

Az OpenOffice és a Word is lehetőséget biztosít párhuzamos aláírás (egymás után több független aláírás) elkészítésére, de szekvenciálisat – egymástól függő aláírást – egyik szövegszerkesztő segítségével sem lehet csinálni. Ez azért fontos, mert amíg a szerződő felek megállapodhatnak írásban Word dokumentum segítségével, addig hitelesíteni az aláírásukat ezzel nem tudja ezt a közjegyző, ehhez más aláíró eszközre lesz szüksége. Továbbá láthatjuk, hogy az aláírás típusa XAdES-EPES, azaz alapszintű aláírást tud csak létrehozni alapesetben a szövegszerkesztő, bonyolultabb aláírásokat jellemzően nem lehet ezekkel létrehozni. Ha ilyet szeretnénk, akkor dedikált aláíró programra lesz szükségünk.

Az aláírt dokumentumok tartalmának módosítása során az aláírásokat a szövegszerkesztők többféle módon kezelik. A Word nem engedi az aláírt tartalom módosítását, csak az aláírás törlése után. Ha a szövegszerkesztőből indítva más néven elmentjük az aláírt fájlt, az aláírás érvénytelenné válik és törlődik. A LibreOffice Writer a tartalom módosításával jelzi, hogy az aláírás érvénytelenné vált, és végérvényessé a módosított tartalom mentésével válik ez a változtatás, ami maga után vonja az aláírás törlését is. Ha a „Mentés másként” funkciót használjuk, ekkor szintén törlődni fog a dokumentum elektronikus aláírása az újonnan létrejövő LibreOffice dokumentumból. Azaz az aláírt dokumentum módosítását javasolt elkerülni az aláírás használhatóságának megőrzése érdekében.

6.2.3.2 Aláírások táblázatkezelőkben

A digitális aláírási funkció a legtöbb ismert **táblázatkezelőben** (MS Excel, LibreOffice Calc stb.) is benne van, általuk szintén ismert szolgáltatás. A szövegszerkesztésnél leírtakhoz hasonlóan működik az aláírás a táblázatkezelőkben is, ugyanazt az aláírási funkciót lehet használni itt is, mint a szövegszerkesztőknél.

A táblázat aláírásának **lépései**:

1. A táblázatkezelőben létre kell hozni egy új táblázatot tetszőleges adatokkal.

2. Valamilyen névvel a dokumentumot el kell menteni.
3. Következik az aláírási funkciót tartalmazó menüpont kiválasztása:
    a) MS Word Fájl menü / Információ / Füzetvédelem / Digitális aláírás hozzáadása,
    b) LibreOffice Calc: Fájl menü / Digitális aláírások / Digitális aláírások… menüpont,
4. Klikkelés a „Digitális aláírások” menüpontra.
5. Ezután hozzá kell adni az aláírásra használni kívánt tanúsítványt
    a) MS Excel: Módosítás gomb után (ha az alapértelmezett tanúsítvány nem megfelelő),
    b) LibreOffice Calc: Dokumentum aláírása gomb,
6. Az aláírás létrehozásához az „Aláírás” gombra klikkelve létrejön az aláírás.

A sikeres aláírást az állapotsorban feltűnő kis pecsét alakú ikon jelzi. Ha a felhasználó erre az ikonra kattint, megnézheti, hogy kitől származik az elektronikus aláírás. Szintén igaz, hogy a LibreOffice és az MS Office táblázatkezelője is lehetőséget biztosít párhuzamos aláírás elkészítésére, de szekvenciális aláírást egyikkel sem lehet csinálni.

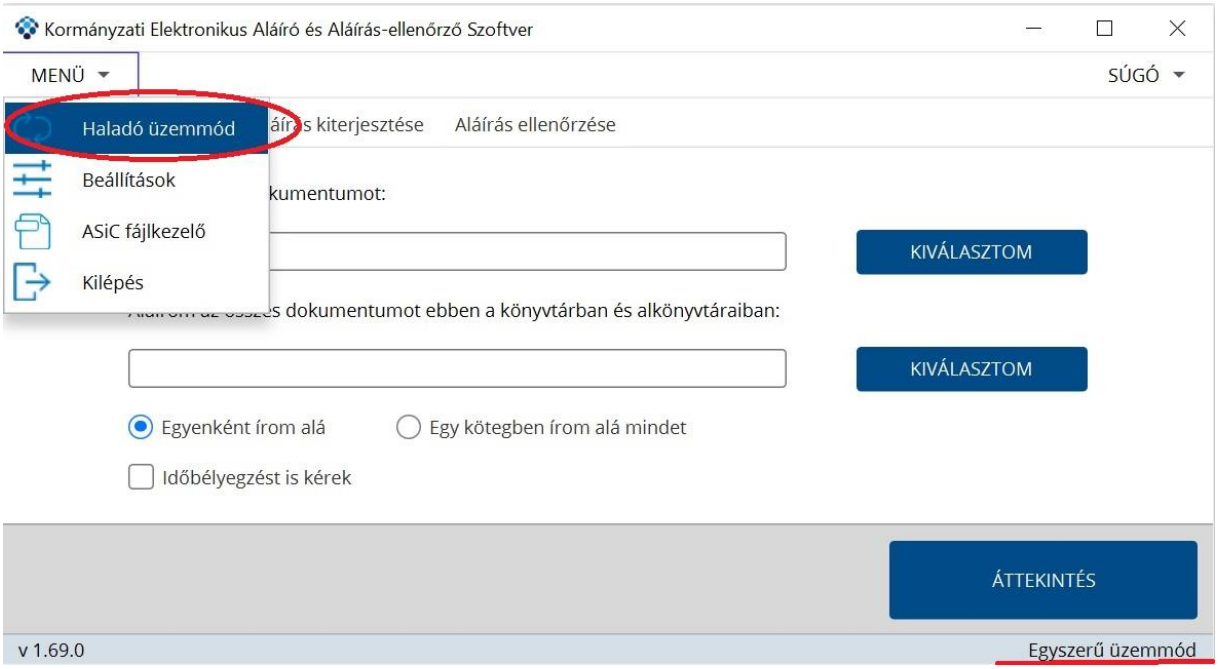
6.2.4 Aláírás készítése a Kormányzati Elektronikus Aláíró és Aláírás-ellenőrző (KEAASZ) szoftverrel

A magyar kormány minden állampolgár számára ingyenesen és szabadon letölthető módon rendelkezésre bocsátotta a Kormányzati Elektronikus Aláíró és Aláírás-ellenőrző (KEAASZ) szoftvert[24]. Letöltés után egyszerű módon telepíthető az alkalmazás, amivel tetszőleges fájlt alá lehet írni. A program a PDF-dokumentumokat PAdES-aláírással látja el, a többi állományt belehelyezi egy ASiC konténerbe, és ez írja alá. Alapesetben alap aláírást fog készíteni a program minden dokumentumhoz. Az aláíró alkalmazás alapbeállításait módosítani szükséges ahhoz, hogy a dokumentumokon időbélyegzett aláírás jöjjön létre. Ennek ismerete és használata javasolható mindenki számára. Ehhez négy konfigurációs pontot kell ellenőrizni és beállítani:

1. a KEAASZ készítsen PDF aláírást időbélyeggel együtt,
2. az állampolgári tanúsítványunkat használja az aláíráshoz,
3. a Kormányzati Hitelesítés Szolgáltató által kibocsátott minősített időbélyeg kerüljön rá az aláírásra, és
4. a PDF aláírás a szövegben láthatatlan legyen.

A beállítások elvégzéséhez nem az egyszerű, hanem a haladó beállítási módot szükséges használni. Az éppen aktuális beállítási módozatot a jobb alsó sarokban találhatjuk. A menüben (jobb felső sarok) lehet a másik módot kiválasztani, itt állítsuk az üzemmódot „Haladó üzemmód”-ra!

[24] Lásd https://eszemelyi.hu/letoltesek/#alairo-szoftver



11. ábra: KEAASZ haladó üzemmód beállítása

Alapesetben a program a dokumentumokat időbélyeg nélküli, alap aláírással látja el. Ekkor az aláírás idejének a számítógépek megbízhatatlan óráit veszi figyelembe a szoftver, ami nem lesz minden kétséget kizáró módon hiteles idő, ezért ha időbélyeggel ellátott aláírást szeretnénk létrehozni, akkor azt a beállításokban át kell állítani.

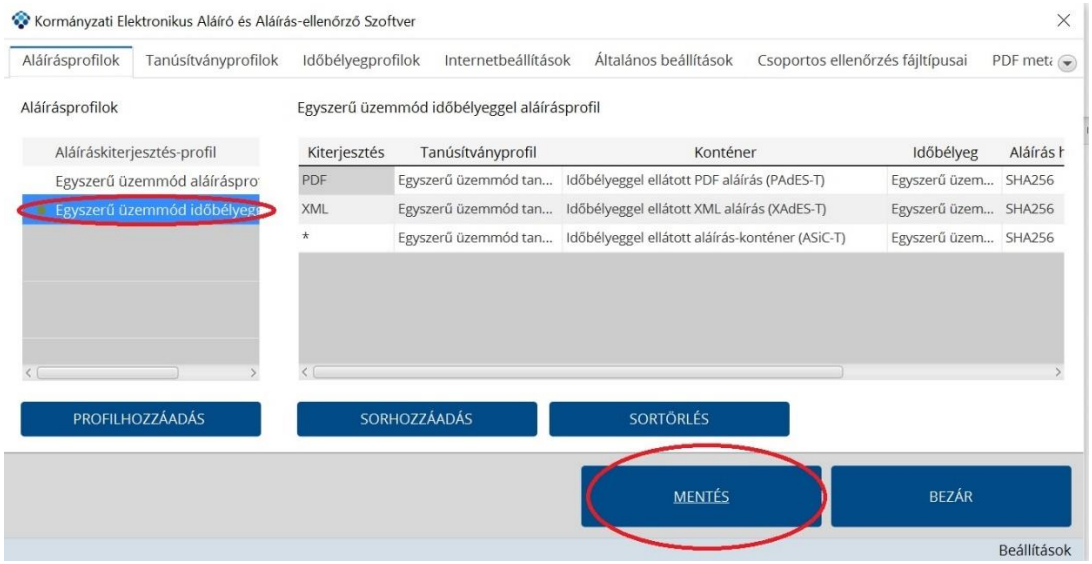
A menüben a beállításokra kattintva feltűnik a nyolc konfigurációs fület tartalmazó felület, ahol a legelső az „Aláírásprofilok”. Itt három profilt lehet látni:

1. Aláíráskiterjesztés-profil
2. Egyszerű üzemmód aláírásprofil
3. Egyszerű üzemmód időbélyeggel aláírásprofil

A zöld pont jelzi az éppen aktuális profilt. Amennyiben ez nem az „Egyszerű üzemmód időbélyeggel aláírásprofil” mellett van, úgy tegyük a következőket.

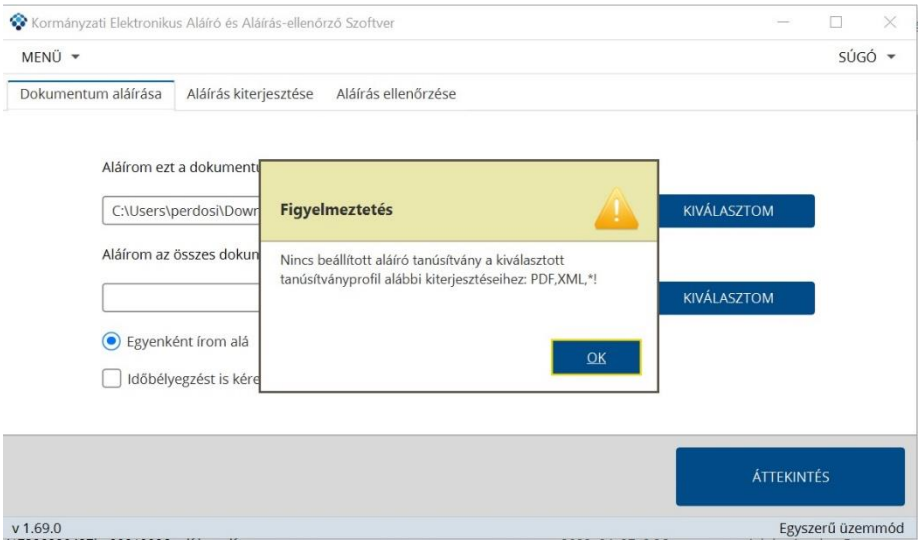
Kattintsunk az „Egyszerű üzemmód időbélyeggel aláírásprofil”-ra, így az kékké válik. Az egér jobb gombjával kattintsunk bele ebbe a kék sorba, és a megjelenő két lehetőség közül válasszuk a „Beállítás alapértelmezettként (Haladó üzemmód)” opciót. Ezt követően a zöld pontnak az újonnan kiválasztott üzemmód mellett kell lennie.

Kattintsunk a „Mentés” gombra, mert enélkül a változás nem lesz érvényesíthető. (Megjegyzés: minden fülön minden változtatás után a „Mentés” gomb érvényesíti a változásokat!)



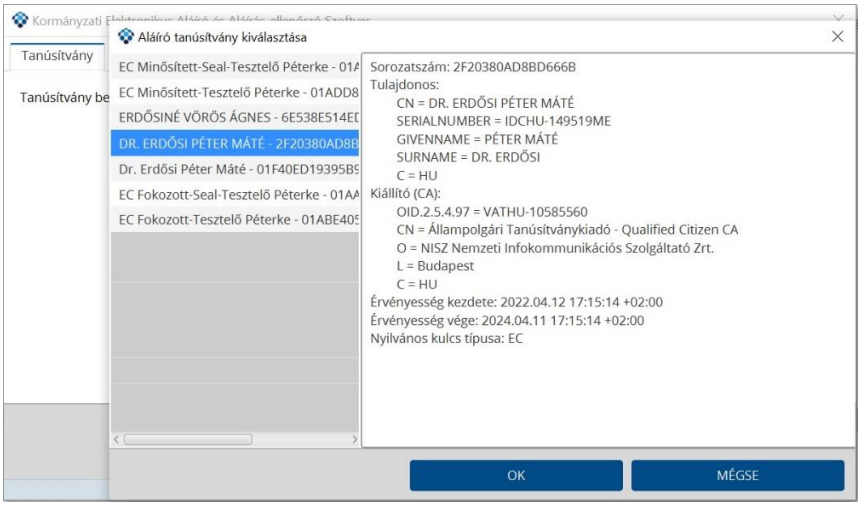
12. ábra: KEAASZ egyszerű üzemmód beállítása

Az aláírás megkezdése előtt ki kell választanunk az aláírásra használt tanúsítványt. A program az indítást követően azonnal rákérdez arra, hogy melyik tanúsítványt szeretnénk használni az aláírásokhoz. Ha itt nem választunk tanúsítványt, az aláírás megkezdésekor hibaüzenetet kapunk.



13. ábra: KEAASZ tanúsítvány hiánya üzenet

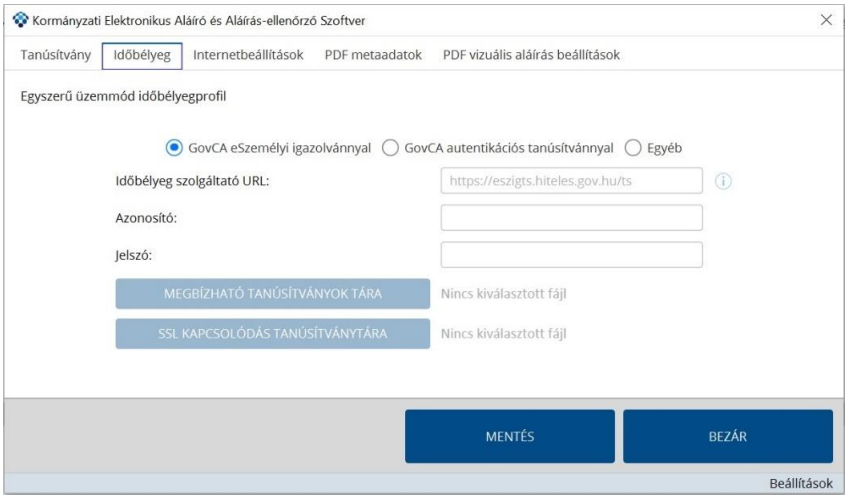
Az aláíró tanúsítvány kiválasztását a Menüben a Beállítások fülre kattintva megjelentő Tanúsítvány beállítási oldalon tudjuk elvégezni. Ha rákattintunk a „Tanúsítványkiválasztás” gombra, a szoftver kilistázza a gépünkön található – és a hozzákapcsolódó olvasóban lévő aláírásra használható tanúsítványokat. Ezek közül – ha több is van, válasszuk ki az állampolgári tanúsítványunkat (névre szóló és nagybetűs írásmóddal jelzett).



14. ábra: KEAASZ tanúsítvány kiválasztása

Az „OK” gombbal véglegesítve a választást a „Mentés” gombbal érvényesítjük azt. Ezzel a program felkészült a kiválasztott tanúsítvány segítségével történő aláírásra.

A NISZ Kormányzati Hitelesítés Szolgáltató minden állampolgári tanúsítvánnyal rendelkező ügyfélnek[25] ingyen biztosít minősített időbélyegzési lehetőséget[26], ezt a következő módon kell beállítani a KEAASZ-ban. A Menü legördülő menüjében a Beállításokat kiválasztva az „Időbélyeg” fülre navigáljunk el. A NISZ Kormányzati Hitelesítés Szolgáltató ingyenes minősített időbélyeg-szolgáltatását akkor érhetjük el, ha a „GovCA eSzemélyi igazolvánnyal” opció van kiválasztva. Ha nem ez lenne, válasszuk ki, majd a „Mentés” gombbal érvényesítsük a változtatást.



15. ábra: KEAASZ időbélyeg-szolgáltató beállítása

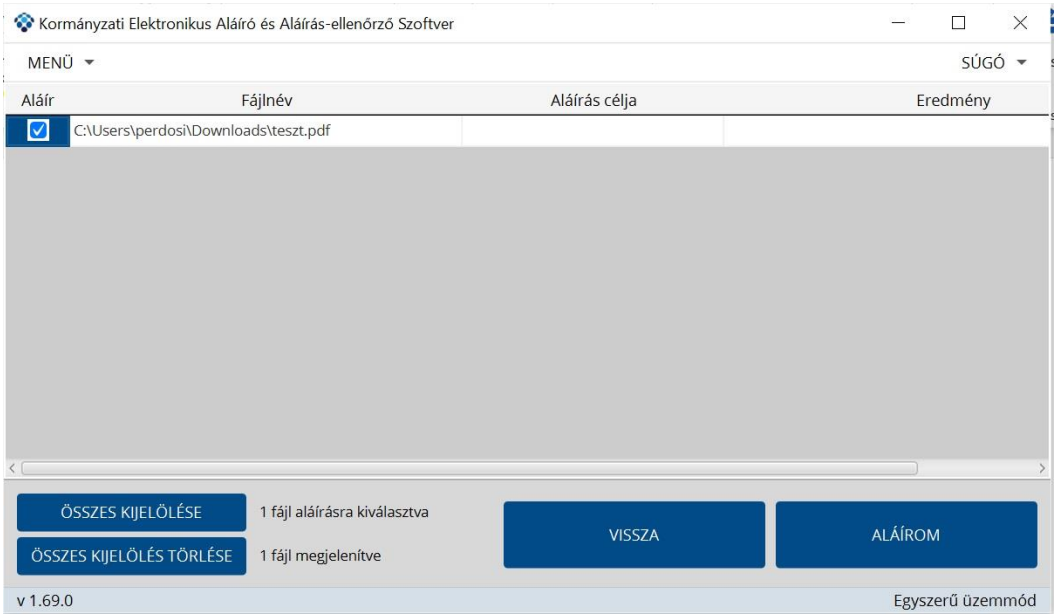
[25] Lásd 84/2012. (IV. 21.) Korm. rendelet egyes, az elektronikus ügyintézéshez kapcsolódó szervezetek kijelöléséről 7/C. § A Kormány a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló törvény szerinti, a személyazonosító igazolványhoz tartozó elektronikus aláírás hitelesítési és az ehhez kapcsolódóan nyújtott időbélyegzés szolgáltatás szolgáltatójaként a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.-t jelöli ki. Az állampolgárnak Szolgáltatási Szerződést kell kötnie a kijelölt szolgáltatóval az időbélyegzés igénybevételéhez.

[26] Lásd NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. Időbélyegzés Bizalmi Szolgáltatási Szabályzat (IBSZ), 9.1.1 Időbélyegzők díja: Szolgáltató az eSzemélyi tulajdonosok (állampolgárok) számára kiadott időbélyegzőkért díjat nem számít fel.

Az eSzemélyivel rendelkező ügyfelek esetében a NISZ az időbélyegzőt azt követően bocsátja ki, hogy meggyőződött arról, hogy a kérelmező birtokolja azt az eSzemélyit, amellyel kapcsolatban a szerződéses jogviszony létrejött. Emiatt a NISZ megköveteli, hogy az időbélyegző-kérést a beküldés előtt az eSzemélyin tárolt minősített tanúsítványához tartozó magánkulccsal írja alá a kérelmező. Az időbélyeg-kérelem elfogadása vagy visszautasítása a kérésen elhelyezett elektronikus aláírás ellenőrzését és a jogosultság ellenőrzését követően automatikusan történik, mivel a NISZ tudja, kikkel kötött már szolgáltatási szerződést, azaz kik jogosultak az időbélyegzés használatára. Akiknek már van állampolgári tanúsítványuk, ők természetesen jogosultak ingyenesen időbélyeget is kérni.

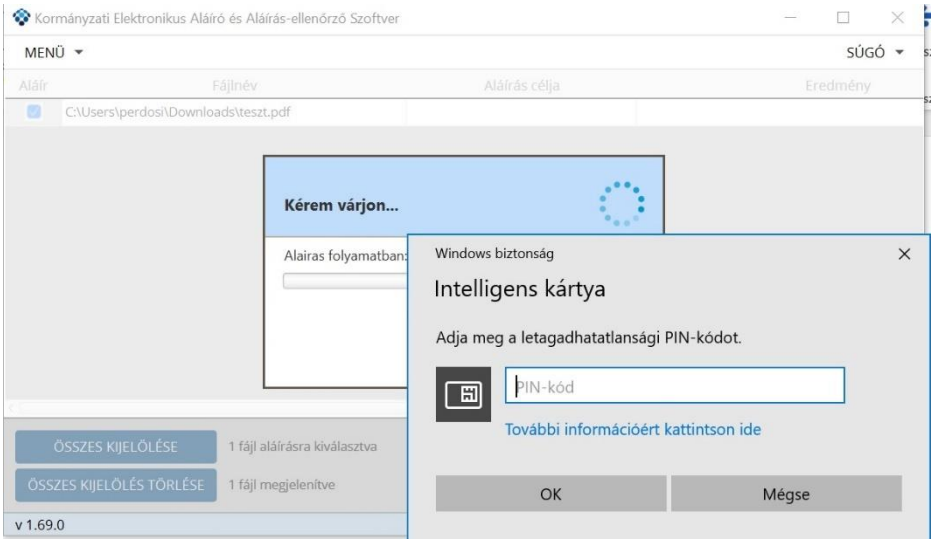
Végül a PDF-en elhelyezni kívánt aláírást kell beállítanunk. Első megközelítésben a láthatatlan aláírásnak a beállítását javasoljuk az aláírás elkészítése előtt. Ehhez a Menü legördülő menüjében a Beállításokat kiválasztva a „PDF vizuális aláírás beállítások” fülre navigáljunk el, és ellenőrizzük le, hogy a „látható szöveg az aláíráson” és a „látható kép az aláíráson” jelölő négyzetek üresek legyenek, vagy kattintsuk ki őket. Ne feledkezzünk el a „Mentés”-sel a változtatásokat érvényesíteni. A „Bezár” gombbal térhetünk vissza az aláírási funkciókhoz.

Az aláírás készítéséhez a főoldalon a „Dokumentum aláírása” fülön tallózzuk be az aláírni kívánt dokumentumot. Lehetőség lenne kötegelt aláírások létrehozására is, azonban nekünk egy PDF dokumentum aláírásához az „Egyenként írom alá” opciót kell kiválasztani. Az „Időbélyegzést is kérek” jelölőnégyzet maradjon üresen, hiszen az alapértelmezett aláírás-profil – ha beállítottuk – már tartalmazza az időbélyeget. A fájl kiválasztása és betallózása után az „Áttekintés” gombra kattintva láthatóvá válik az aláírni kívánt dokumentumok – esetünkben egy PDF – listája.



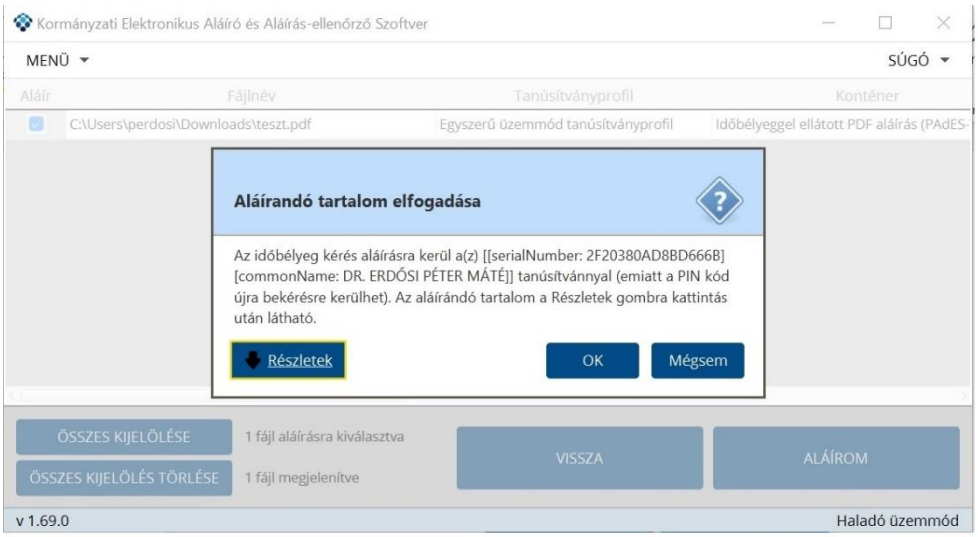
16. ábra: KEAASZ dokumentum aláírása

Az aláírás az „Aláírom” gombra kattintva indul el. Ha minden kapcsolat rendben van, és az eSzemélyi is alkalmas minősített elektronikus aláírás készítésére, a program ekkor elkészíti a PDF dokumentum kivonatát, elkéri az aláíráshoz szükséges hétjegyű PIN-kódot, elküldi a kártyának a kivonatot aláírásra, majd beilleszti az aláírást a PDF dokumentumba.



17. ábra: KEAASZ PIN-kód megadása minősített aláíráshoz

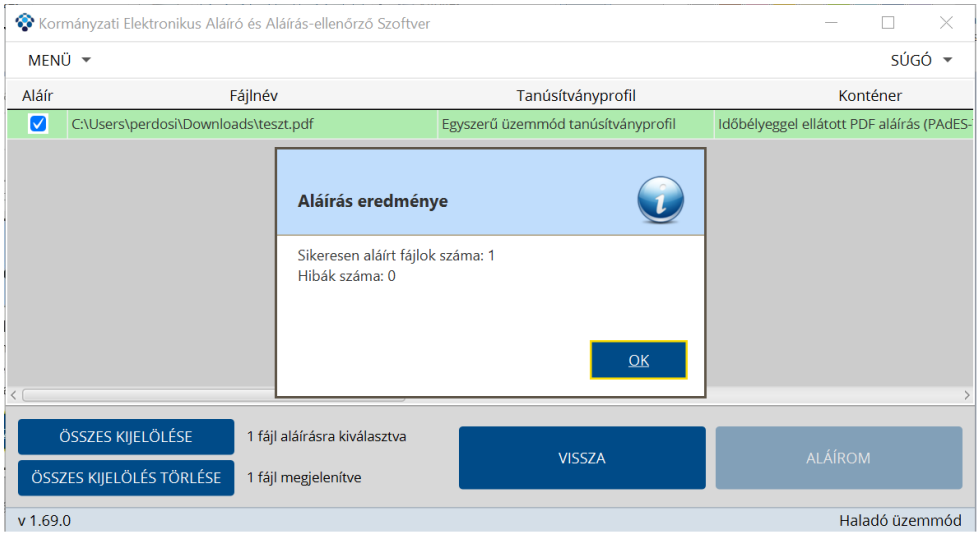
Ezt követően kerül sor az időbélyeg kérésére.



18. ábra: KEAASZ Időbélyeg kérése aláíráshoz

Ehhez újra meg kell adnunk az aláíráshoz szükséges hétjegyű PIN-kódot, hogy a NISZ tudja ellenőrizni a jogosultságunkat az ingyenes minősített időbélyeghez.

Sikeres aláírás esetében a program zöld színnel jelzi a problémamentes eredményt, megmutatva a sikeres aláírások és a hibák számát is (ez utóbbinak nullának kell lennie jó esetben). A soron végig lehet görgetni, amivel az aláírt PDF dokumentum minden lényeges tulajdonságát meg lehet tekinteni. Ebből a legfontosabb az „Időbélyeggel ellátott PDF aláírás” megjegyzés. Ha nem sikerült időbélyeget tenni a dokumentumra, akkor itt „Egyszerű PDF aláírás (PAdES-B) lenne csupán.



19. ábra: KEAASZ Időbélyeg kérése aláíráshoz

6.2.5 Azonosításra Visszavezetett Dokumentumhitelesítés (AVDH)

Az azonosításra visszavezetett dokumentum-hitelesítés szolgáltatás (továbbiakban: AVDH) az ügyfélkapuval rendelkező állampolgárok részére nyújt megoldást arra nézve, hogy biztonságosan tudják intézni hivatalos ügyeiket a közigazgatásban. Az AVDH gyors bekapcsolódási lehetőséget biztosít az elektronikus ügyintézésbe minden olyan felhasználó részére, akik nem rendelkeznek elektronikus aláírással, vagy adott esetben nem kívánják használni az elektronikus aláírásukat, de az eljárás megköveteli a teljes bizonyító erejű magánokirat kiállítását. Így bárki, aki rendelkezik „ügyfélkapuval”, vagyis a Központi Azonosítási Ügynök (KAÜ) tudja őket hitelesíteni, teljeskörűen részt tud venni az elektronikus ügyintézésben az AVDH szolgáltatás igénybevételével.

Az AVDH az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény 38. § (1) bekezdés d) pontjában nevesített központi szabályozott elektronikus ügyintézési szolgáltatás (KEÜSZ). Az AVDH-val a polgári perrendtartásról szóló törvény (Pp.) 325. § (1) bekezdés g) pontja alapján teljes bizonyító erejű magánokirat, a 451/2019. Korm.R. (Eüvhr.) 12. § (1) bekezdés d) pont és a 113. § (4) bekezdés alapján közokirat hozható létre. Az AVDH keretében a NISZ a felhasználó által rendelkezésre bocsátott nyilatkozatot az általa igazolt személyhez rendeli, majd a személyhez rendelést hitelesen igazolja. A Szolgáltató a személyhez rendelésről kiállított igazolást elektronikus dokumentumba, vagy az igazolást az elektronikus dokumentumhoz kapcsolt záradékba foglalja és azt a rendelkezésre bocsátott nyilatkozattal együtt külön jogszabályban meghatározott elektronikus bélyegzővel és időbélyegzővel hitelesíti. Az igazolás vagy záradék tartalmazza:

a) a nyilatkozattevő nevét és a rendelkezésére álló további igazolt azonosító adatok közül a nyilatkozattevő által megjelölt és a Szolgáltató által az azonosítási szolgáltatónál, a központi azonosítási ügynök, a rendelkezési nyilvántartás vagy az összerendelési nyilvántartás igénybevételével lekérdezett adatokat (születési név, születési idő, születési hely, anyja neve), valamint

b) a nyilatkozat további azonosító adatait.

Fontos még tudni, hogy az AVDH nem kezel külön felhasználókat, és ideiglenesen tárolja csak az oda feltöltött adatokat, azaz nem archiválja. Az ügyfelek számára minden AVDH

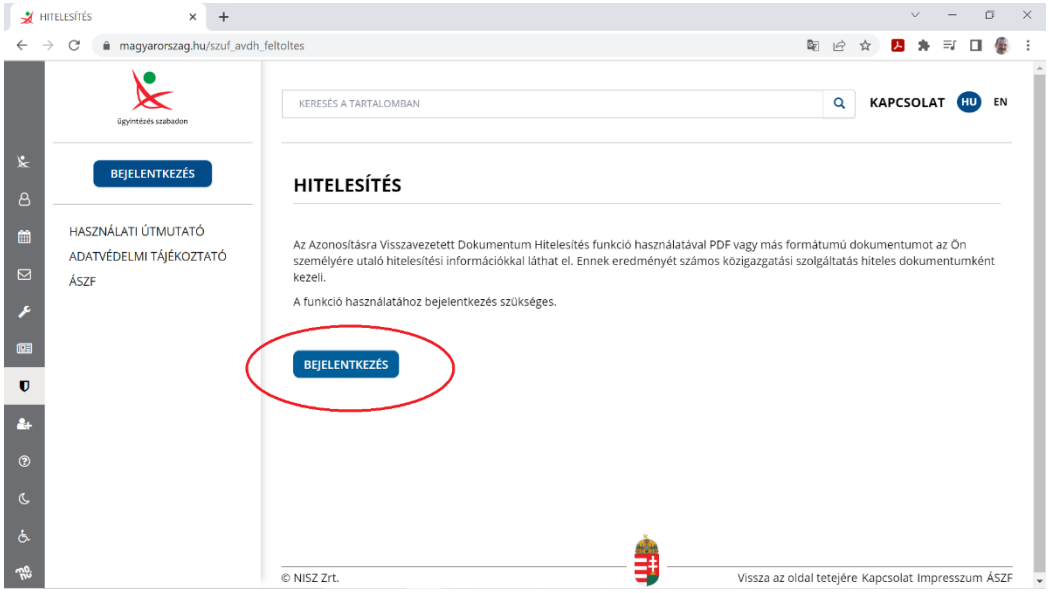
folyamat a háttérben, láthatatlan módon zajlik. Az AVDH-t a felhasználók webes felületen érhetik el.

Fontos különbség az állampolgári minősített elektronikus aláíráshoz képest, hogy a dokumentumhitelesítés során a dokumentum itt nem lesz aláírva a felhasználó által, hanem a sikeres azonosítást követően a NISZ minősített tanúsítványon alapuló fokozott biztonságú bélyegzője és egy minősített időbélyegző hitelesíti a felhasználó állítását, azaz a feltöltött dokumentumot. Ez a megoldás tehát nem alkalmazható ott, ahol követelmény a dokumentumon az aláírás feltüntetése, mivel az AVDH alapértelmezésben nem tartalmazza a felhasználó aláírását. Ugyanakkor a magyar jogrend szerint az AVDH ugyanolyan teljes bizonyító erővel rendelkezik, mint a minősített aláírás.

6.2.5.1 Az AVDH hitelesítés lépései

Egy AVDH hitelesített dokumentum előállításához első lépésként egy böngészővel a következő weboldalt kell megnyitni:

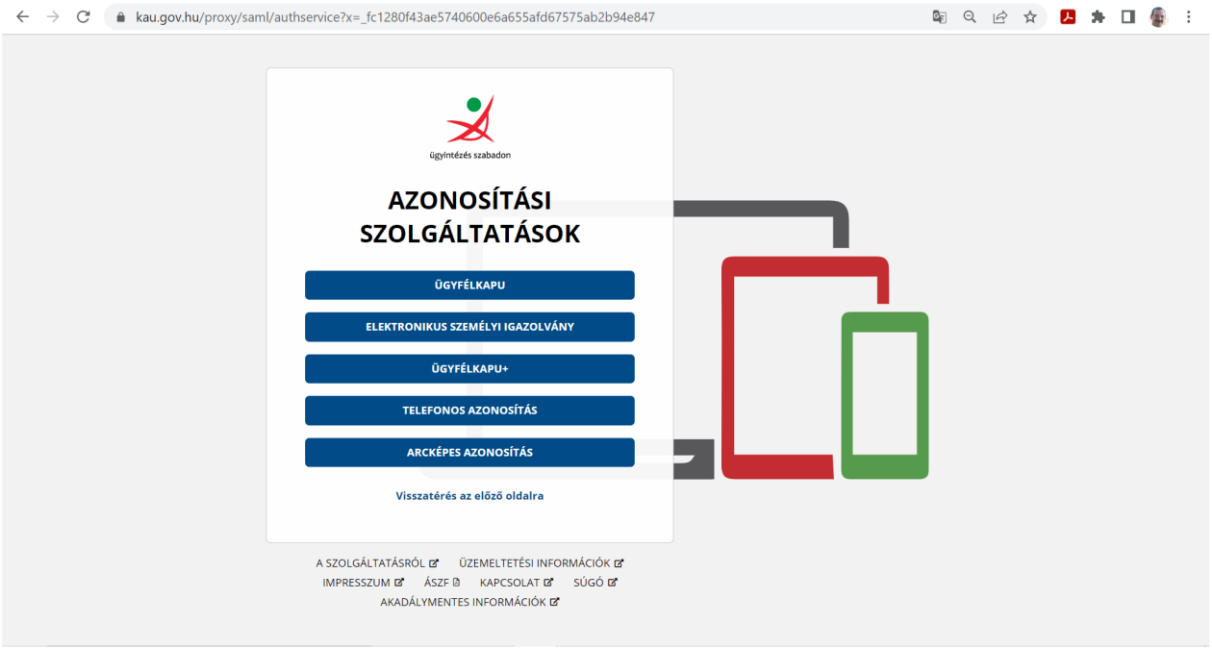
- https://magyarorszag.hu/szuf_avdh_feltoltes



20. ábra: Bejelentkezés AVDH használatához

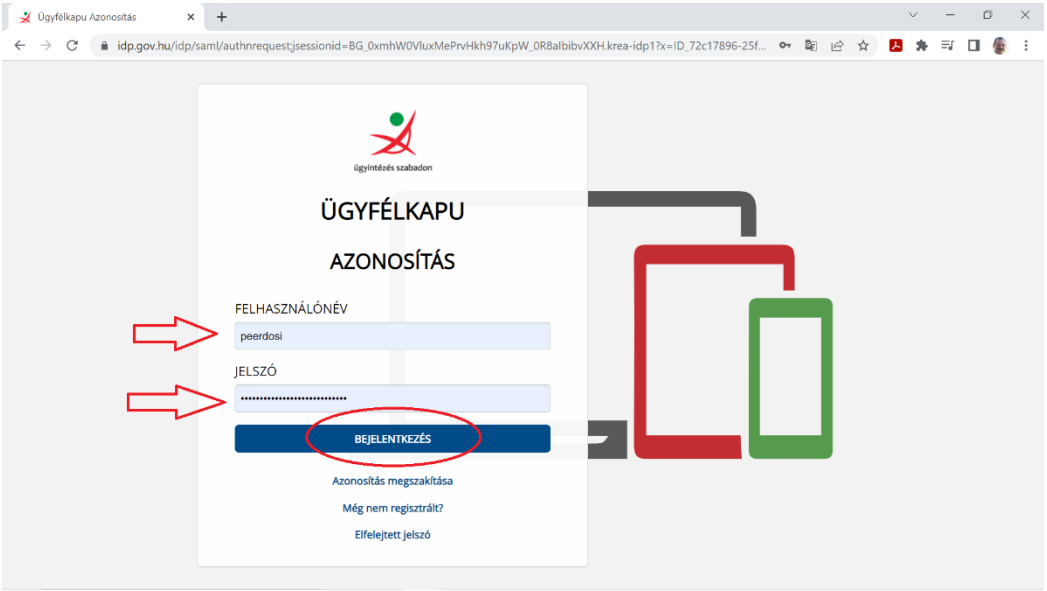
A szolgáltatás használatához először be kell jelentkezni a Központi Azonosítási Ügynökön (KAÜ) keresztül, a bejelentkezés gombra kattintva.

A megjelenő azonosítási módszerek közül ki kell választanunk az általunk használni kívánt módszert (leggyakrabban az ügyfélkapus felhasználói név és jelszó megadását választják az ügyfelek).



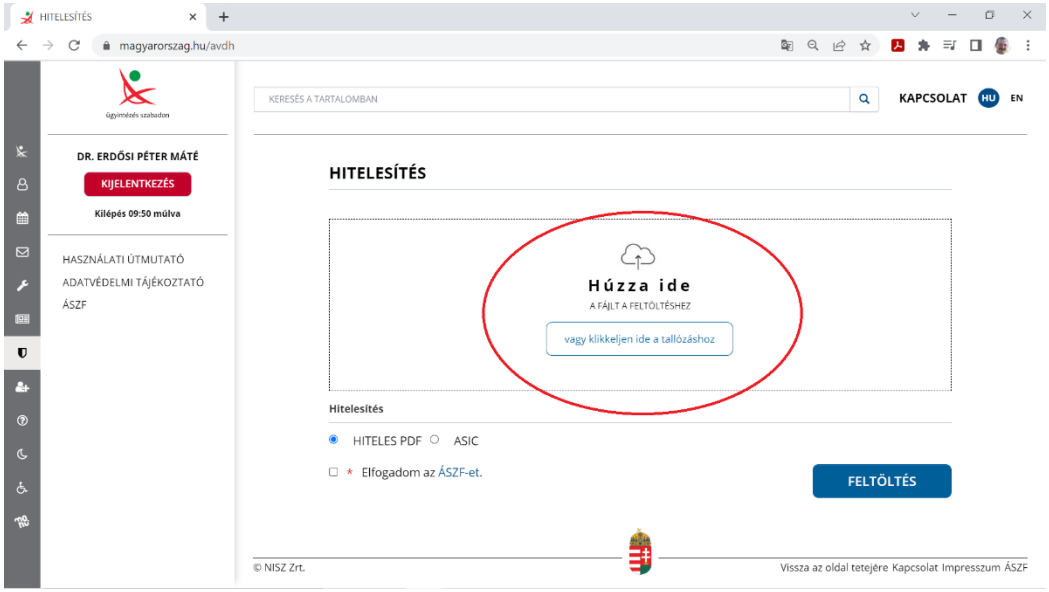
21. ábra: KAÜ bejelentkezési képernyő

Ezt követően meg kell adni a hitelesítéshez szükséges adatokat.



22. ábra: KAÜ bejelentkezési adatok

Amennyiben sikeres volt a bejelentkezési adatok megadása, a fájlok feltöltését lehetővé tévő képernyőnek kell megjelennie ezután.



23. ábra: Dokumentum tallózása AVDH hitelesítéshez

A feltöltött dokumentum formátuma egy egyszerű PDF vagy esetleg ASiC lehet. A PDF dokumentum hitelesített változatát szintén PDF formátumban kapjuk vissza.

A hitelesített dokumentum a következő három lépésben állítható elő:

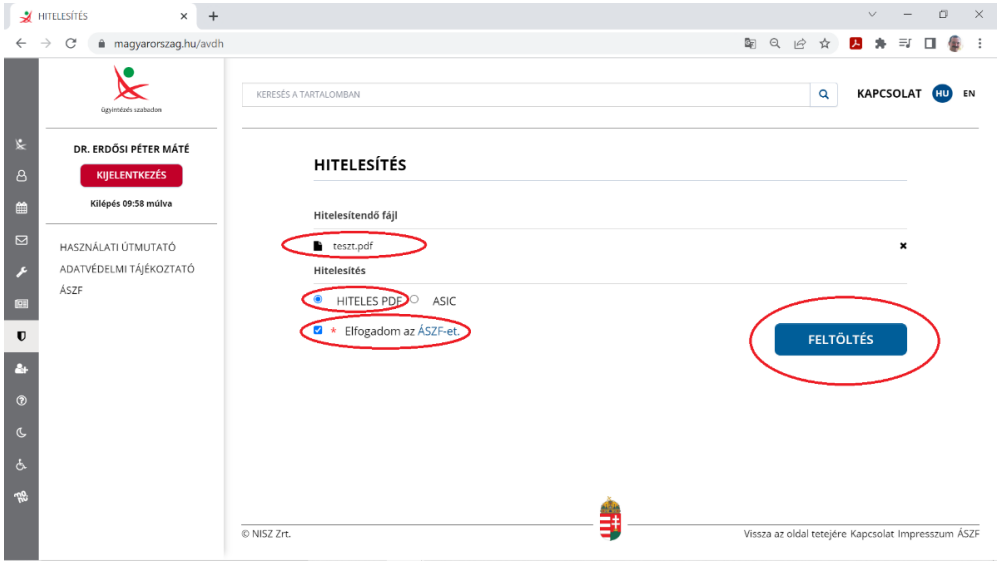
1) Fájl kiválasztása: a kiválasztás kétféleképpen történhet.

a. Tallózás: A hitelesíteni kívánt fájl kiválasztásához kattintson a "Fájl kiválasztása" mezőbe. Ekkor a felugró tallózóablakban a saját gépéről kiválaszthatja azt a fájl, amelynek a hitelesítését el szeretné végezni

b. Fogd-és-vidd: A hitelesíteni kívánt fájt az intézőben egérrel megragadjuk, és bedobjuk a „Húzza ide” feliratú ablakba a weboldalon.

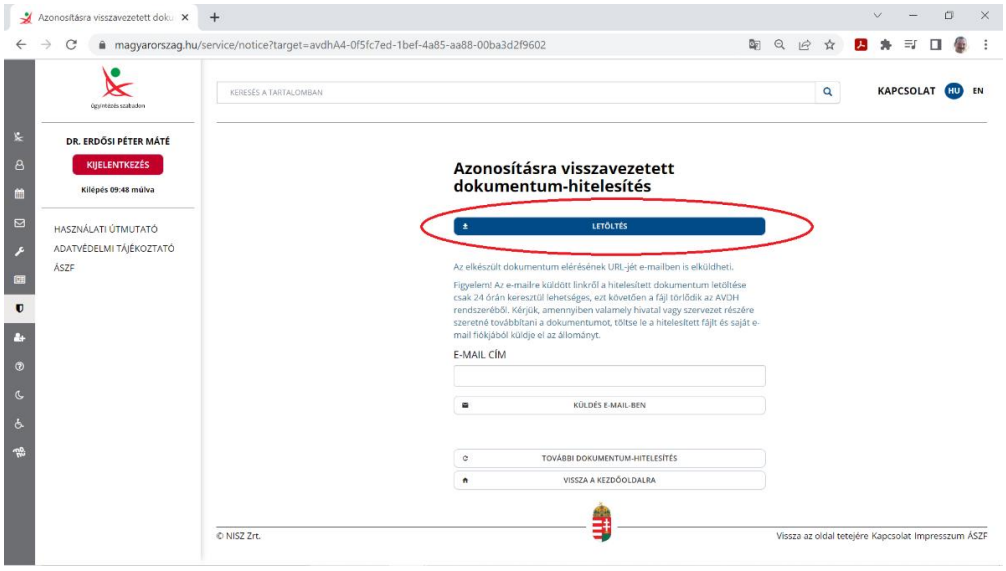
2) Hitelesítés kiválasztása: A hitelesítés típusának kiválasztásakor csak és kizárólag a „Hiteles PDF" típusú eljárást kérjük használni.

3) ÁSZF: A jelölőnégyzet kipipálásával el kell fogadni az Általános Szolgáltatási feltételeket, majd el kell küldeni a dokumentumot a rendszernek hitelesítésre a „Feltöltés” gomb megnyomásával.



24. ábra: Dokumentum feltöltése AVDH hitelesítésre

Ezt követően az AVDH szolgáltatás hitelesíti a dokumentumot, és az a felhasználó számára elérhetővé válik: a hitelesített dokumentum a felhasználói gép „Downloads” vagy „Letöltések” mappájába kerül letöltésre.



25. ábra: Dokumentum letöltése AVDH hitelesítés után

Itt kell látnunk a letöltés befejezését követően egy hasonló elnevezésű (avdh-val kezdődő fájlnévvel rendelkező) PDF dokumentumot:

- avdhA4-0f5fc7ed-1bef-4a85-aa88-00ba3d2f9602.pdf

A dokumentum letöltése után azt felhasználhatjuk a kívánt célra.

Gyakorló kérdések:

1. Milyen dokumentumokat lehetséges aláírással ellátni?
2. Hogyan készíthető el egy aláírás irodai programcsomag segítségével?
3. Mi a különbség a KEAASZ és az AVDH aláírás között?

7 Kormányzati és hivatali ügyintézés elektronikusan

7.1 Az elektronikus aláírás és a kormányzás kapcsolata

7.1.1 E-kormányzás az EU-ban

AZ EU 2000-ben elfogadta az eEurope 2002 akciótervét, amelynek egyik meghatározó eleme egy szolgáltatási lista volt. Ez nevesítette és konkretizálta először azokat a szolgáltatásokat, amelyeknek elektronikus úton történő elérhetőségét a tagállamoknak biztosítaniuk kellett. A kiválasztottak között tizenkét olyan közigazgatási, közszolgáltatási ügytípus volt, amelyet a polgárok gyakran igénybe vesznek, továbbá nyolc olyan ügytípust is kiválasztottak, amelyeket a vállalkozásoknak kell gyakorta intézniük. Ez a húsz ügytípus alkotta az alapvető közszolgáltatások közösségi listáját (a CLBPS-t). Ezeknek a szolgáltatásoknak az akcióterv szerint 2002 végére minden tagállamban működniük kellett.

A listában meghatározott 20 ügytípus szétválasztását a polgárok (CIT) és az üzleti szféra (BUS) számára a következőképpen tették meg:

Szolgáltatás	Leírás
Vállalkozóknak nyújtott (BUS) szolgáltatások	
BUS 1/a	Munkavállalók és foglalkoztatók számára nyújtott szolgáltatások (munkáltatók bejelentési kötelezettségének elősegítése, munkavállalók számára betekintési lehetőség a róluk benyújtott információkba)
BUS 1/b	Munkáltatók bejelentése nyugdíjbiztosítási adatokról
BUS 2	Társaságiadó-bevallás, -értesítés
BUS 3	ÁFA-bevallás, -értesítés
BUS 4	Korlátolt felelősségű társaságok és részvénytársaságok bejegyzése, változásbejegyzése
BUS 5	Adatközlés a statisztikai hivataloknak
BUS 6	Vámáru-nyilatkozatok benyújtása, kezelése
BUS 7	Környezetvédelemmel összefüggő engedélyek megszerzése
BUS 8	Közbeszerzési eljárás
Állampolgároknak nyújtott (CIT) szolgáltatások	
CIT 1	Jövedelemadó-bevallás, értesítés a kivetett adóról
CIT 2/a	Álláskeresés interneten keresztül az ÁFSZ állásajánlataiban
CIT 2/b	Állásbejelentés interneten keresztül az ÁFSZ állásadatbázisába

Szolgáltatás	Leírás
CIT 3/a	Munkanélküli járadék igénylése
CIT 3/b	Munkavállalók gyermekei után járó pótlékok igénylése
CIT 3/c	Kötelező egészségbiztosítás ellátásai
CIT 3/d	Tanulói ösztöndíj megpályázása
CIT 4/a	Útlevéligénylés és útlevéllel kapcsolatos egyéb ügyintézés
CIT 4/b	Gépjárművezetői engedély ügyintézése, illetőleg vezetési jogosultság megszerzése
CIT 5	Járművek nyilvántartásával kapcsolatos ügyintézés, járműigazgatás (új, használt és importált gépjármű forgalomba helyezése, műszaki vizsgáztatása, járműigazgatási ügyek)
CIT 6	Építési engedély iránti kérelem
CIT 7	Rendőrségi online bejelentések, feljelentések
CIT 8	Közkönyvtári katalógusok hozzáférhetősége, keresési lehetőségek elérése 1954-ig
CIT 9/a	Születési anyakönyvi kivonat ügyintézése: kérvényezés, kiadás
CIT 9/b	Házassági anyakönyvi kivonat ügyintézése: kérvényezés, kiadás
CIT 10	Felvételi jelentkezés (középiskolákba, felsőoktatási intézményekbe)
CIT 11	Lakcímváltozás bejelentése (lakcímigazolvány-pótlás, -csere)
CIT 12	Egészségüggyel összefüggő szolgáltatások (pl. interaktív tanácsadás kórházi szolgáltatások elérhetőségéről, kórházi bejelentkezések)

7. táblázat: Az alapvető közszolgáltatások európai közös listája

A gyakran citált „20-as” vagy „12+8-as lista” a leggyakoribb ügyeket tartalmazza, amelyek a kormányportálon keresztül elérhetők, a leírások mindenki számára, az ügyek pedig annak a többmillió polgárnak a számára, akik rendelkeznek KAÜ (ügyfélkapu, ügyfélkapu+, eID, telefonos vagy videós) azonosítási lehetőséggel.

Teljesen elektronikus ügyintézés pedig csak teljesen elektronikusan történő aláírással képzelhető el, ahogyan azt a 910/2014 EU rendelet megfogalmazta és szabályozta.

7.1.1.1 Elektronikus cégeljárás

A Polgári törvénykönyvről szóló 1959. évi IV. törvény (Ptk.) 29. § (1) bekezdése alapján a jogi személy létrejöttének és megszüntetésének feltételeit a jogszabály a jogi személy egyes fajtáihoz képest állapítja meg. A Ptk. 29. § (4) bekezdése kimondja továbbá, hogy ha jogszabály a jogi személy létrejöttét nyilvántartásba vételhez köti, a bejegyzett körülmények megváltoztatása harmadik személyek irányában csak akkor hatályos, ha a változást a nyilvántartásba bevezették. A cégekre vonatkozó cégadatok nyilvántartását, továbbá a nyilvántartás-

ban bekövetkezett változások bejegyzésének módját és rendjét a cégnyilvánosságról, a bírósági cégeljárásról és a végelszámolásról szóló 2006. évi V. törvényt (Ctv.) határozza meg.

A gazdasági társaságokról szóló 2006. évi IV. törvény (Gt.) 26. § (1) bekezdése alapján a gazdasági társaság alapításának, a társasági szerződés módosításának, a cégjegyzékbe bejegyzett jogoknak, tényeknek és adatoknak, illetve ezek változásának, valamint törvényben előírt más adatoknak a cégbírósági – elektronikus úton történő – bejelentése a vezető tisztségviselők kötelezettsége. Az **elektronikus cégeljárással** kapcsolatos feladatokat az Igazságügyi és Rendészeti Minisztérium szervezeti egységeként működő Céginformációs és az Elektronikus Cégeljárásban Közreműködő Szolgálat (Céginformációs Szolgálat vagy Cégszolgálat) látja el.

A Cégszolgálat feladatai körébe alapvetően három szolgáltatás sorolható:

1. elektronikus úton történő bejegyzési (változásbejegyzési) eljárás;
2. elektronikus úton nyújtott céginformáció;
3. beszámoló közzététele, letétbe helyezése elektronikus úton az Online Beszámoló és űrlapkitöltő Rendszer (OBR) segítségével.

Az elektronikus cégeljárás törvényi hátterét, valamint **az elektronikus cégeljárás** kizárólagossá tételét a Ctv.-t módosító 2007. évi LXI. törvény tette lehetővé. A Ctv. 36. § (1) bekezdésének első mondata alapján 2008. július 1-jétől a cégbejegyzési (változásbejegyzési) eljárás – ide nem értve a jogorvoslati eljárást – **kizárólag elektronikus eljárás formájában** lehetséges. A Ctv. 32. § (4) bekezdése szerint a cégbejegyzési (változásbejegyzési) eljárás kérelemre történik, amelynek során a jogi képviselet kötelező [Ctv. 33. § (2)]. Ügyvéd vagy kamarai jogtanácsos jogi képviselő esetén az ügyvédi tevékenységről szóló törvényben meghatározott elektronikus aláírás és elektronikus bélyegző is használható.

7.1.1.2 Közjegyzők és elektronikus ügyintézés

A közjegyzőkről szóló 1991. évi XLI. törvény (Kjtv.) 111. § (3) bekezdése szerint a **közjegyzői okirat, ennek hiteles kiadmánya és hiteles másolata** – ha törvény eltérően nem rendelkezik – elektronikus úton is elkészíthető. A Kjtv. 137.§ (3) bekezdése alapján a másolatok hitelesítésére vonatkozó szabályokat kell megfelelően alkalmazni az okiratról, illetve az elektronikus úton vezetett adatbázisból a közjegyző felügyelete mellett, elektronikus úton előállított másolat és kivonat hitelesítésére, továbbá az elektronikus okiratról készített papíralapú másolat és kivonat hitelesítésére. A közjegyző az elektronikus úton készített másolatot és kivonatot minősített elektronikus aláírással látja el.

Nem kell hitelesítési záradékkal ellátni az elektronikus okiratról készített kiadmányt és másolatot, ha az sérülésmentes papíralapú okiratról készült és tartalmazza a teljes okiratot, továbbá a közjegyző elektronikus aláírását és az időbélyegzőt.

A Kjtv. 171/A.§-a rendelkezik a közjegyzők által vezetett elektronikus letéti tárról, amely alapján a fél kérelmére **a közjegyző az elektronikus letéti tárban** helyezi el a kérelemben megjelölt okirat elektronikus hiteles másolatát. Az elektronikus letéti tárban az elektronikus okiratot három évig kell őrizni. Az őrzési idő a lejáratot megelőzően külön kérelemre - legfeljebb hároméves időtartammal - többször meghosszabbítható, a hosszabbításra irányuló kérelem hiányában az elektronikus másolatot törölni kell. A letéti tárból csak a letevő fél vagy meghatalmazottja részére adható ki papíralapú vagy elektronikus másolat, amelyet azonban bár-

mely közjegyző kiadhat, nemcsak az, aki az okiratot készítette. A Kjtv. 21/A § alapján a közjegyző (és a közjegyzőhelyettes) hivatali elektronikus aláírása a Magyar Országos Közjegyzői Kamara által részükre rendszeresített minősített elektronikus aláírás. A közjegyző (és a közjegyzőhelyettes) minősített elektronikus aláírásával látja el a hatáskörébe tartozó ügyben általa készített elektronikus közokiratot.

Hivatali elektronikus aláírásként olyan minősített elektronikus aláírás használható,

1. amelyhez tartozó tanúsítványban a hitelesítésszolgáltató feltüntette annak a tényét is, hogy az aláíró közjegyző vagy közjegyzőhelyettes, és
2. a hitelesítésszolgáltató biztosítja, hogy a tanúsítvánnyal kapcsolatos érvényes visszavonási kérelem alapján a módosított visszavonási állapotot legfeljebb három percen belül közzéteszi a nyilvántartásában, és a tanúsítvány ellenőrzését kérő felhasználóknak a tanúsítvány visszavonási állapotáról folyamatos tájékoztatást ad.

Megjegyzendő továbbá, hogy a fizetési meghagyásos eljárásról szóló 2009. évi L. törvény alapján a fizetési meghagyásos ügyek a bíróságoktól közjegyzői hatáskörbe kerültek. Az ügyeket – nemperes szakaszban – teljes egészében elektronikusan és automatikusan intézi a Magyar Országos Közjegyzői Kamara[27] rendszere. Ez jelentősen meggyorsította a végrehajtásokat, ami javította a nem fizetők fizetési hajlandóságát.

7.1.1.3 Önkormányzati elektronikus ügyintézés

Az állam 2012-ben az Önkormányzati ASP (Application Service Provider, alkalmazásszolgáltató) központ felállítását tűzte ki célul. A projekt két lépcsőben valósult meg, első lépcsőben a központi régióban az önkormányzatok belső működése támogatásának és az elektronikus ügyintézési szolgáltatások nyújtásának megvalósítására fókuszált. A fejlesztés hosszú távú célja az volt, hogy a csatlakozó önkormányzatok számára megteremtse egy azonos eljárási alapokon nyugvó, költséghatékony informatikai rendszer használatának lehetőségét. Az alkalmazásszolgáltató (ASP) központon keresztül olyan hardver- és szoftver infrastruktúra, arra épülő keret- és szolgáltatási rendszer jött létre, amely által az önkormányzatok képesek az alábbi területeket digitálisan működtetni:

- gazdálkodási rendszer
- ingatlanvagyon-kataszter rendszer
- önkormányzati adórendszer
- iratkezelő rendszer
- önkormányzati portál rendszer
- ipari és kereskedelmi rendszer

Az Önkormányzati ASP-1 projekt keretében 2015. június végéig 55 önkormányzatot csatlakoztattak a rendszerhez, akik már akkor igénybe vehették az alkalmazásszolgáltatást. Ezt követően a KIFÜ felkérést kapott a Széchenyi 2020 program keretében induló KÖFOP 1.2.2 - ASP 2.0 projekt konzorcium vezetői és projektgazdai szerepére, a belügy-, a nemzetgazdasági- és a nemzeti fejlesztési miniszterektől. Az ASP 2.0 projekt célkitűzései a következők voltak:

- az önkormányzati ASP szolgáltatásrendszer országos kiterjesztése,

[27] A Magyar Közjegyzői Kamara honlapja elérhető itt: http://www.mokk.hu

- a további önkormányzati csatlakoztatások központi támogatása,
- az elektronikus közigazgatási szolgáltatások fejlesztése és bevezetése,
- a szakrendszerek bővítése és továbbfejlesztése,
- az ASP szakrendszerekre, mint adatforrásokra épülő adattárház megvalósítása,
- a kapcsolódó hálózat és infrastruktúra bővítése.

A fejlesztések lezárulásával a Kormány az önkormányzati ASP rendszert a Magyar Államkincstár útján működteti. A működés szabályait az önkormányzati ASP rendszerről szóló 257/2016. (VIII.31.) Korm. rendelet rögzíti. Ez teremtette meg az elektronikus önkormányzati ügyintézés központi hátterét.

Az ügyfelek az itt kialakított szolgáltatásokat az E-önkormányzat portálon vehetik igénybe, mert ez a portál lett az önkormányzati ASP rendszerben az elektronikus önkormányzati ügyintézés helyszíne. Az önkormányzati ASP rendszert igénybe vevő települések – természetes személy és jogi személy – ügyfelei számára az E-önkormányzat portálon keresztül biztosítják ügyfeleik számára az elektronikus ügyintézéshez szükséges szolgáltatásokat. A portál bárki számára elérhető (https://ohp-20.asp.lgov.hu/nyitolap), egyes funkciók szabadon használhatók, más funkciók azonban bejelentkezéshez kötöttek. Az online ügyintézéshez szükséges a Központi Azonosítási Ügynökön (KAÜ) keresztüli azonosítás, az alábbi elektronikus azonosítási szolgáltatások egyikén keresztül:

- Ügyfélkapus azonosítás (Ügyfélkapu)
- Elektronikus személyazonosító igazolvány (eSzemélyi, annak is az eID része, ami minden eSzemélyi kötelező eleme)
- Ügyfélkapu+ (kétfaktoros Ügyfélkapu)
- Telefonos Azonosítás (RKTA)
- Arcképes azonosítás.

Nem természetes személy nevében (pl. cég, civil szervezet) történő ügyintézés esetén az eljáró személynek szintén KAÜ-azonosítással kell bejelentkeznie, és szerepkör-váltással kezdeti meg a jogi személy képviseletében az ügyek intézését.

Ezen túlmenően az egyes hivatalok további saját fejlesztéseket tehetnek elérhetővé az ügyfeleik számára, ilyen volt például a budaörsi „Elektronikus Adó Ügyintézési- és Számlaegyenleg Lekérdezés” szolgáltatás, amely a helyi adószámlákhoz biztosított hozzáférést a helyi adó fizetésére kötelezett polgárok számára[28].

A helyi adószámla lekérdezése így pár kattintással megtehető és egy részletes PDF dokumentumot visszakapva eredményül pontosan láthatók a befizetését és a hátralékok is. Azaz az ASP egyszerűen használható kiváló eszközt biztosít a központosított ügyintézés bevezetéséhez is minden egyes önkormányzat számára.

Gyakorló kérdések:

1. Milyen működő példák vannak az e-közigazgatásra Magyarországon?
2. Mely működő közigazgatási példákban kötelező az elektronikus aláírás használata?
3. Milyen szabványos aláírásokat fogadnak el az egyes eljárások?

[28] Lásd pl. https://budaors.eado.hu/Content/Kezdolap.aspx.

7.1.2 A hitelesség fontossága internetes vásárláskor

7.1.2.1 Távollévők közötti kötött szerződések

A Polgári törvénykönyvről szóló 2013. évi V. törvény (Új Ptk.) tartalmazza az általános törvényi rendelkezéseket a szerződések jogára vonatkozóan, így az **elektronikus úton kötött szerződéseket** illetően is. A Ptk. rendelkezéseit többször módosították annak érdekében, hogy a fogyasztók védelmét előmozdító európai uniós szabályozásnak megfelelő rendelkezéseket adaptálják a magyar jogba. Emellett a távollévők között kötött szerződések esetén a fogyasztók védelméről szóló 1997/7/EK irányelvet a távollévők között kötött szerződésekre vonatkozó előírásokat is magában foglaló, a fogyasztó és a vállalkozás közötti szerződések részletes szabályairól szóló 45/2014. (II. 26.) Kormányrendelet (rendelet) képezte le.

A Ptk. 6:4. §-a alapján a szerződésekre vonatkozó általános rendelkezések szerint szerződést, jognyilatkozatot akár szóban, akár írásban is lehet tenni, illetve ezt az akaratot ráutaló magatartással is kifejezésre lehet juttatni. A 6:82. § előírja az elektronikus úton történő szerződéskötések esetében azt is, hogy elektronikus úton történő szerződéskötés esetén az elektronikus utat biztosító fél köteles a szerződéskötésre vonatkozó jognyilatkozatának megtételét megelőzően a másik felet tájékoztatni

a) a szerződéskötés technikai lépéseiről;

b) arról, hogy a megkötendő szerződés írásba foglalt szerződésnek minősül-e, az elektronikus utat biztosító fél rögzíti-e a szerződést, továbbá, hogy a szerződés utóbb hozzáférhető lesz-e;

c) azokról az eszközökről, amelyek az adatok elektronikus rögzítése során felmerülő hibák azonosítását és kijavítását a szerződési jognyilatkozat megtételét megelőzően biztosítják;

d) a szerződés nyelvéről; és

e) ha ilyen létezik, arról a szolgáltatási tevékenységre vonatkozó magatartási kódexről és annak elektronikus hozzáférhetőségéről, amelyet az elektronikus utat biztosító fél magára nézve kötelezőnek ismer el.

Az elektronikus utat biztosító fél köteles az általános szerződési feltételeit olyan módon hozzáférhetővé tenni, amely lehetővé teszi a másik fél számára, hogy tárolja és előhívja azokat.

A szerződések részletes szabályairól szóló kormányrendelet részletesen szabályozza a 8. fejezetben a szerződéskötésre vonatkozó formai követelményeket távollévők között kötött szerződések esetén. Ha a távollevők közötti, elektronikus úton kötött szerződés a fogyasztó számára fizetési kötelezettséget keletkeztet, a vállalkozás köteles gondoskodni arról, hogy a fogyasztó a szerződési nyilatkozatának megtételekor kifejezetten tudomásul vegye, hogy nyilatkozata fizetési kötelezettséget von maga után. Ha a nyilatkozat megtétele gomb vagy hasonló funkció aktiválásával jár, a gombot vagy a hasonló funkciót könnyen olvasható módon fizetési kötelezettséggel járó megrendelés vagy ennek megfelelő, egyértelműen megfogalmazott felirattal kell ellátni, amely jelzi, hogy a szerződési nyilatkozat megtétele a vállalkozás javára teljesítendő fizetési kötelezettséget von maga után. Ha a vállalkozás nem tesz eleget ennek a kötelezettségének, a szerződés semmis, vagyis a fogyasztó érdekére hivatkozva, nem jön létre.

Speciális szabályok vonatkoznak tehát a pénzügyi szolgáltatások távértékesítésére irányuló, távollévők között kötött szerződésekre, összhangban a fogyasztói pénzügyi szolgáltatások

távértékesítéssel történő forgalmazásáról szóló 2002/65/EK irányelv rendelkezéseinek megfelelően. A 2005. évi XXV. törvény alapján távértékesítés keretében kötött pénzügyi ágazati szolgáltatási szerződés a pénzügyi távértékesítési törvényben meghatározott pénzügyi ágazati szolgáltatásokra irányuló szerződés (önkéntes kölcsönös biztosító pénztári tagság esetében a pénztár által elfogadott belépési nyilatkozat), amelyet szolgáltató és fogyasztó köt egymással szervezett távértékesítés keretében olyan módon, hogy a szerződés megkötése érdekében a szolgáltató kizárólag távközlő eszközt alkalmaz. A pénzügyi távértékesítési törvény 2. § (1) g) pontja alapján távközlő eszköz **bármely eszköz,** amely alkalmas a felek távollétében – szerződés megkötése érdekében – szerződési nyilatkozat megtételére.

A szolgáltató a fogyasztónak a szerződéskötésre irányuló jognyilatkozatát megelőzően – tekintettel a szolgáltatás és a távközlő eszköz jellegére, a fogyasztók védelme érdekében – kellő időben köteles tájékoztatni a fogyasztót a pénzügyi távértékesítési törvény 3. §-ban foglaltakról, így többek között a szolgáltató adataival, elérhetőségével, a szerződés fontosabb rendelkezéseivel kapcsolatos, illetve a szerződés tárgyát érintő bármely lényeges kérdésről.

A távközlő eszköz útján megkötött pénzügyi ágazati szolgáltatásokra irányuló szerződéstől a fogyasztó a szerződéstől a szerződéskötés napjától számított **tizennégy napon belül indokolás nélkül elállhat**. Az önkéntes kölcsönös biztosító pénztári tagság esetében, a pénztár által elfogadott belépési nyilatkozat tekintetében az elállási jog gyakorlására nyitva álló határidő a belépési nyilatkozat pénztár általi elfogadása napjától számított harminc nap, míg a biztosítási szerződés esetében elállás helyett a fogyasztó a szerződést a szerződéskötés napjától számított tizennégy napon belül indokolás nélkül azonnali hatállyal felmondhatja. Életbiztosítási szerződés esetében pedig a felmondási jog gyakorlására nyitva álló határidő attól a naptól számított harminc nap, amikor a szolgáltató a fogyasztót a szerződés létrejöttéről tájékoztatja.

A fogyasztókkal szembeni kereskedelmi gyakorlatra, így különösen a fogyasztók tájékoztatására vonatkozó rendelkezések megsértése esetén az adott szolgáltatás felügyeletére felhatalmazott szervezetek (a fogyasztóvédelmi hatóság, a Magyar Nemzeti Bank, a Gazdasági Versenyhivatal, vagy az élelmiszerlánc-felügyeleti hatóság) a fogyasztókkal szembeni tisztességtelen kereskedelmi gyakorlat tilalmáról szóló 2008. évi XLVII. törvényben meghatározott szabályok szerint járnak el.

7.1.2.2 Webáruházak

Interneten történő vásárlás esetében kétfajta **webáruházat**[29] érdemes megkülönböztetni. Az első esetben az elektronikus kereskedelmi szolgáltatás tárgya egy olyan termék, amely fizikai módon megfogható és átruházható, így ebben az esetben lehetőség van hagyományos fizetési eszközök használata révén kiegyenlíteni a termék vételárát. A második esetben olyan termékek megvásárlásáról van szó, amely esetben a fizetés módja kizárólag elektronikus úton, közvetlenül a vásárlást követően meg kell történnie, tipikusan letölthető szellemi javak, pl. zeneszámok, filmek letöltése és megvásárlása. Természetesen az elektronikus fizetési eszközök alkalmazása mindkét típusú termék esetében alkalmazható.

[29] Az e-boltokról részletes összefoglaló található a következő honlapon: http://www.xn--klker-kva.hu/wp-content/uploads/2013/03/Hogyan_nyissunk_e_boltot.pdf

7.1.2.2.1 Tájékoztatási kötelezettség

A webáruházak működésével kapcsolatban egyrészt az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény (Elkertv.) megfelelő rendelkezései irányadóak. Másrészt mivel az elektronikus úton (Elkertv. 2.§ b) pont) megkötött fogyasztói szerződések távollevők között kötendő szerződésnek minősülnek, ezért a korábban már említett fogyasztók és ügyfelek közötti szerződésekről szóló kormányrendelet rendelkezéseire is figyelemmel kell lenni és a két törvény rendelkezései egyaránt alkalmazandóak. A 2001. évi CVIII. törvény alapján a webáruház működtetője, illetve amennyiben nem ugyanarról a személyről van szó, a kereskedő részére tájékoztatási kötelezettséget állapít meg annak érdekében, hogy a fogyasztók a szükséges információk birtokában vegyék igénybe a szóban forgó szolgáltatást, vagyis jelen esetben a webáruházon keresztül történő vásárlást. Az Elkertv. 4.§-a megszabja, melyek azok az adatok, amelyeket a szolgáltató köteles elektronikus úton közvetlenül és folyamatosan, könnyen hozzáférhető módon, magyar nyelven közzétenni:

a) a szolgáltató nevét,

b) a szolgáltató székhelyét, telephelyét, ennek hiányában lakcímét,

c) a szolgáltató elérhetőségére vonatkozó adatokat, különösen az igénybe vevőkkel való kapcsolattartásra szolgáló, rendszeresen használt elektronikus levelezési címét,

d) ha a szolgáltató létrejöttét vagy tevékenysége gyakorlásának megkezdését jogszabály nyilvántartásba való bejegyzéshez köti, a szolgáltatót a nyilvántartásba bejegyző bíróság vagy hatóság megnevezését, és a szolgáltató nyilvántartásba vételi számát,

e) ha a szolgáltató tevékenységének gyakorlása jogszabály alapján engedélyköteles, ezt a tényt az engedélyező hatóság megnevezésével és elérhetőségi adataival, valamint az engedély számával együtt,

f) ha a szolgáltató az általános forgalmi adó alanya, a szolgáltató adószámát;

g) a szabályozott szakmák gyakorlásának körében:

ga) annak a szakmai érdek-képviseleti szervnek (kamarának) a megnevezését, amelynek a szolgáltató akár kötelező előírás alapján, akár önkéntesen tagja;

gb) a természetes személy szolgáltató szakképzettségének, illetve szakmai, tudományos fokozatának, valamint annak a tagállamnak a megjelölését, ahol ezt a szakképzettséget, illetve fokozatot megszerezte;

gc) hivatkozást a szabályozott szakma gyakorlásának a szolgáltató letelepedési helye szerinti államban alkalmazandó szakmai szabályaira, és az azokhoz való hozzáférés módjára,

h) a szolgáltató részére a tárhelyet biztosító, a 2. § l) pont lc) alpontjában meghatározott szolgáltató székhelyét, telephelyét, az elérhetőségére vonatkozó adatokat, különösen az igénybe vevőkkel való kapcsolattartásra szolgáló, rendszeresen használt elektronikus levelezési címét, kivéve, ha a szolgáltató részére nyújtott tárhelyszolgáltatás jellegéből adódóan ezek az adatok egyébként is megismerhetőek.

Az Elkertv. 5.§-a külön szabályokat állapít meg az elektronikus úton történő szerződéskötésre vonatkozóan. A szolgáltató a szolgáltatásra vonatkozó általános szerződési feltételeket köteles oly módon hozzáférhetővé tenni, amely lehetővé teszi az igénybe vevő számára,

hogy tárolja és előhívja azokat. Az általános szerződési feltételek elérhetősége mellett a szolgáltató a szolgáltatást igénybe vevő megrendelésének elküldését megelőzően köteles egyértelmű tájékoztatást adni:

a. azokról a technikai lépésekről, amelyeket a szerződés elektronikus úton való megkötéséhez meg kell tenni,

b. arról, hogy a megkötendő szerződés írásba foglalt szerződésnek minősül-e, a szolgáltató iktatja-e a szerződést, illetve, hogy az iktatott szerződés utóbb hozzáférhető lesz-e,

c. az adatbeviteli hibáknak a szerződéses nyilatkozat elküldését megelőzően történő azonosításához és kijavításához biztosított eszközökről,

d. a szerződéskötés lehetséges nyelveiről,

e. arról a – szolgáltatási tevékenységére vonatkozó – magatartási kódexről, amelynek az adott szolgáltatás tekintetében aláveti magát, amennyiben van ilyen; továbbá arról, hogy ez a magatartási kódex elektronikus úton hol hozzáférhető.

Az Elkertv. 5.§-ban írt tájékoztatási kötelezettség szabályától a szerződéskötő felek csak abban az esetben térhetnek el közös megegyezéssel, amennyiben a szolgáltató fogyasztónak nem minősülő igénybe vevővel, tehát pl. gazdálkodó szervezettel köt szerződést. A szerződéskötés módjára tekintettel mondja ki a törvény, hogy a szolgáltató köteles megfelelő, hatékony és hozzáférhető technikai eszközökkel biztosítani, hogy az igénybe vevő az adatbeviteli hibák azonosítását és kijavítását megrendelésének elektronikus úton való elküldése előtt el tudja végezni. Ilyen lehetőség hiányában az igénybe vevő megrendelése nem minősül szerződéses nyilatkozatnak. A szolgáltató köteles az igénybe vevő megrendelésének megérkezését az igénybe vevő felé elektronikus úton haladéktalanul visszaigazolni. Amennyiben a visszaigazolás az igénybe vevő megrendelésének elküldésétől számított, a szolgáltatás jellegétől függő elvárható határidőn belül, de legkésőbb 48 órán belül az igénybe vevőhöz nem érkezik meg, az igénybe vevő mentesül az ajánlati kötöttség vagy szerződéses kötelezettség alól (Elkertv. 6.§ (1)-(2) bekezdései).

7.1.2.2.2 Adatvédelem

Figyelemmel arra, hogy a webáruház esetében a szolgáltató szükségszerűen kezeli és tárolja a szolgáltatásával összefüggésben a szolgáltatás igénybe vevőinek személyes adatait, ezért az Elkertv. 13/A. §-a külön rendelkezéseket tartalmaz az adatvédelemmel kapcsolatban. Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 5.§ (1) b) pontja alapján személyes adatot kezelni (így az adatkezelés céljának és az adatkezelés korlátainak meghatározásával) a felhasználó hozzájárulásán túl törvény vagy – törvény felhatalmazása alapján, az abban meghatározott körben – helyi önkormányzat rendelete írhatja elő. Erre tekintettel az Elkertv. 13/A.§-a a fentiekben említett törvényen alapuló adatkezelési célt határoz meg. Így a szolgáltató a szolgáltatás nyújtására irányuló szerződés létrehozása, tartalmának meghatározása, módosítása, teljesítésének figyelemmel kísérése, az abból származó díjak számlázása, valamint az azzal kapcsolatos követelések érvényesítése céljából kezelheti az igénybe vevő azonosításához szükséges természetes személyazonosító adatokat és lakcímet. A szolgáltató a szolgáltatás nyújtására irányuló szerződésből származó díjak számlázása céljából kezelheti a természetes személyazonosító adatokat, lakcímet, valamint a szolgáltatás igénybevételének időpontjára, időtartamára és

helyére vonatkozó adatokat a szolgáltatás nyújtása céljából kezelheti azon személyes adatokat, amelyek a szolgáltatás nyújtásához technikailag elengedhetetlenül szükségesek. A szolgáltatónak úgy kell megválasztania és minden esetben oly módon kell üzemeltetnie a szolgáltatás nyújtása során alkalmazott eszközöket, hogy személyes adatok kezelésére csak akkor kerüljön sor, ha ez a szolgáltatás nyújtásához és az e törvényben meghatározott egyéb célok teljesüléséhez feltétlenül szükséges, azonban ebben az esetben is csak a szükséges mértékben és ideig.

7.1.2.2.3 Elállási jog

A távollévők között kötött szerződésekről szóló kormányrendelet különös szabályokat állapít meg az elektronikus úton kötött szerződésektől történő elállási és felmondási jogokkal kapcsolatban. Ennek megfelelően a kormányrendelet szerint a fogyasztókat részletesen, írásban tájékoztatni kell az őket megillető elállási jogról minden internetes kereskedelmi forma esetében, ellenkező esetben az elállási határidő tizenkét hónappal meghosszabbodik (21. § (1)). Az elállási jog gyakorlása során azonban a fogyasztót is terhelik kötelezettségek, ezekre tekintettel kell az elállást megvalósítani.

A felek eltérő megállapodása hiányában azonban a fogyasztó nem gyakorolhatja az általános szabályok szerint őt megillető elállási jogát a kormányrendelet 29. § (1) pontban meghatározott esetekben. Így például olyan termék értékesítése esetében, amely a fogyasztó személyéhez kötött, illetve amelyet a fogyasztó utasításai alapján vagy kifejezett kérésére állítottak elő, vagy amely természeténél fogva nem szolgáltatható vissza vagy gyorsan romlandó, lezárt csomagolású hang-, illetve képfelvétel, valamint számítógépi szoftver példányára vonatkozó szerződés esetében, ha a csomagolást a fogyasztó felbontotta, hírlap, folyóirat és időszaki lap értékesítésére vonatkozó szerződés esetében – az előfizetési szerződések kivételével; illetve szerencsejáték-szerződés esetében.

7.1.2.2.4 Fizetési módok

Az elektronikus fizetési módok közül a bankkártyás fizetések használata az egyik legelterjedtebb megoldás a webes alapú áruházak körében, melyek a legkisebb kockázatot jelenthetik a fizetés biztonságát illetően. Ebben az esetben a bankkártya használatához szükséges egy vPOS elfogadóhely létesítése, ahol a bankkártyakibocsátó társaság rendszerében elfogadó bankként részt vevő bank elfogadja a bankkártyával történő fizetést. Nem minden bankkártya alkalmas internetes tranzakciók rendezésére, egyre több helyen használnak webkártyát, amelyet kifejezetten online vásárlásra történő használatra fejlesztettek ki. A vásárlás lebonyolítását megelőzően a webkártyát – amelyhez elkülönült kártyaszám tartozik – csak annyi pénzzel szükséges és érdemes feltölteni, amennyit az online vásárláskor el kívánunk költeni. A webkártyával bonyolított vásárláskor kiküszöbölhető, hogy a bankkártyaszámmal esetleg visszaéljenek. A webkártya mellett a dombornyomású kártyák alkalmasak internetes felületen történő fizetésre.

Gyakorló kérdések:

1. Hogyan alkalmazható a távollévők között kötött szerződésben az elektronikus aláírás?
2. Van-e összefüggés az elektronikus aláírás és az elektronikus pénz között?
3. Milyen jogi eszközök védik a fogyasztókat az internetes vásárláskor?

7.1.3 A hitelesség fontossága az e-bankolásban

Az elektronikus úton történő **fizetési módoknak** különböző formái közül megemlíthető a bankkártyával történő tranzakciók (internet banking), az elektronikus felületen (webshop) közvetlenül történő internetes fizetés, a „bevásárlókocsis" szolgáltatások útján történő fizetés, az elektronikus pénz, az elektronikus mikrofizetési megoldások használatával történő fizetést.

Az elektronikus fizetési megoldásokra vonatkozóan a hitelintézetekről és a pénzügyi vállalkozásokról 2013. évi CCXXXVII. törvény (Hpt.) rendelkezései, és a pénzforgalom lebonyolításáról szóló 35/2017. (XII. 14.) MNB rendelet rendelkezései irányadóak.

Az elektronikus fizetési eszközök esetében a fizetési infrastruktúra alapvetően háromféle lehet:

- a fizetőhöz, illetve a fizető bankszámlájához vagy elektronikus pénztárcájához kötődő: ide tartozik pl. a házibank, irodai bank, telebank, mobilbank, valamint a fizetés elektronikus pénzzel;
- a jogosulthoz, jogosult bankszámlájához vagy elektronikus pénztárcájához kötődő: ide sorolható a POS-rendszer, vPOS vagyis internetes bankkártyás vagy virtuális bankkártyás fizetési megoldás, ATM-rendszer és az emelt díjas szolgáltatások;
- az összetett fizetési struktúra, amely az előző két struktúra elemeit egyaránt alkalmazza: ide tartozik pl. a fizetés banki regisztrációval, mobil fizetési rendszer, az MPP és a SeMoPS (Security Mobile Payment Service).

Minden esetben szükséges a tranzakciók sértetlenségéről gondoskodni a továbbítás során, megakadályozva annak módosítását. A jogosultságot a tranzakciók ügyfél általi hitelesítésével biztosítják a pénzintézetek (pl. egyszer használatos token, hitelesítő applikáció alkalmazása) a tranzakció benyújtásakor, amely az ügyfél aktív közreműködését igényi és legalább kettő faktoron alapul. Ilyen megerősítés lehet a minősített elektronikus aláírás is (pl. SmartID alkalmazása az észt bankrendszerben).

Gyakorló kérdések:

1. Melyek az elektronikus fizetési módok Magyarországon?
2. Hogyan használható az e-bankolásban az elektronikus aláírás?
3. Hogyan biztosítható a számítógép biztonsága e-banking használata esetében?

7.2 Az e-adózás és e-számla

7.2.1 Az e-adózás fő funkciói és fontossága

Az állami adóhatóság (Nemzeti Adó- és Vámhivatal – NAV) mint az egyik legtöbb adattal foglalkozó szervezet, mindig is kiemelt, úttörő szerepet játszott az elektronikus közigazgatási szolgáltatások elterjesztésében. Ennek egyik legjelentősebb példája az **elektronikus adóbevallás és adatszolgáltatás**.

Egyre többen igényelték Magyarországon az elektronikus bevallási lehetőséget, ennek feltételeit az Art. 175. § (13) bekezdése tartalmazza, mely szerint 2005. április 1-jétől bármely adózó benyújthatja adóbevallását, adatszolgáltatását elektronikus úton is. Az adóügyek dön-

tő többsége ma már személyes jelenlét nélkül is intézhető, mert a Nemzeti Adó és Vámhivatal (NAV) kialakította a kapcsolattartás elektronikus csatornáit. Vannak, akiknek kötelező ezeket a csatornákat használni (pl. egyéni vállalkozók, gazdálkodó szervezetek), és vannak, akik eldönthetik, hogy a kapcsolattartásnak ezt a formáját szeretnék-e alkalmazni. Aki elektronikus kapcsolattartásra kötelezett, az papíralapon nem küldhet kérelmeket, egyéb iratokat a NAV-hoz. Az ilyen formában érkezett kérelmek hatálytalannak minősülnek, azaz azokat úgy kell tekinteni, mintha az ügyfél be sem adta volna.

Bárkinek van lehetősége az elektronikus ügyintézésre és kapcsolattartásra, aminek azonban fontos szabályai vannak az adatbiztonság, az ügyfelek egyértelmű azonosítása és egyéb tényezők miatt. Ezek a szabályok elérhetők a NAV honlapján[30].

Az elektronikus adózás legfontosabb felülete a NAV e-BEV portálja[31]. Az e-BEV portál számos funkciót biztosít a felhasználók számára, a bevallások benyújtásán át az összes ránk vonatkozó adat lekérdezéséig.

Többek között lehetőség van lekérdezni az adóteljesítményünket, amelynek kiszámítási módját jogszabály írja elő, így az nem a megjelenített adóelemek összege, hanem a jogszabályban megfogalmazott feltételeknek - az adóigazgatási eljárás részletszabályairól szóló 465/2017. (XII. 28.) Kormányrendelet VII. fejezet. 46. pont. - megfelelő számítási módszer eredményeként kapott érték.

További érdekes lekérdezési lehetőség a keresetkimutatás lekérdezése. Ez a funkció a banki kölcsön igénylési folyamat ügyintézési terheinek csökkentése miatt került bevezetésre. A menüpont segítségével az adózó a NAV nyilvántartása alapján keresetkimutatás tud lekérni, és ha elfogadhatónak találja, közvetlenül tovább tudja küldeni az általa kiválasztott pénzintézetnek. A NAV közvetlenül a banknak küldi az igazolást így ez hivatalos papírnak tekintendő.

Még egy fontos lekérdezési lehetőséget kell megemlítenünk: a biztosítotti bejelentések lekérdezését. A biztosítotti adatok lekérdezhetők a biztosítottak részére, amellyel a munkavállaló ellenőrizheti, hogy a munkáltatója ténylegesen bejelentette-e a munkaviszonyát – beadta-e a vonatkozó bevallásokat és milyen tartalommal – az előírtaknak megfelelően, és így a társadalombiztosítási jogosultsága érvényesen fennáll. A lekérdezés feladata tehát, hogy biztosítsa a foglalkoztatott számára a munkáltató (kifizető) által benyújtott bejelentésekben szereplő adatok lekérdezését. A portálon tehát minden olyan adat megtekinthető és lekérdezhető, amely az adózóval összefüggésben az adóhatóságnál megjelenik, és lehetőség van ezek pontosítására, adott esetben helyesbítésére, az elektronikus felületet használva, a hét és nap bármely órájában, mivel a rendszer 7/24 üzemmódban működik.

Gyakorló kérdések:

1. Hogyan működik az e-adózás folyamata?
2. Milyen szerepe van az e-adózásban a NAV e-BEV portáljának?
3. Melyek a legfontosabb funkciói a NAV e-BEV portálnak?

[30] Lásd https://nav.gov.hu/pfile/file?path=/ugyfeliranytu/nezzen-utana/inf_fuz/2021/32._informacios_fuzet_-_Az_elektronikus_ugyintezes_es_kapcsolattartas_altalanos_szabalyai_adougyekben

[31] Lásd https://ebev.nav.gov.hu/

7.2.2 E-számlázás és a magyar szabályozás

Számla minden olyan okirat, ami megfelel az az általános forgalmi adóról szóló 2007. évi CXXVII. törvény (ÁFA tv.) X. fejezetében meghatározott feltételeknek. A számlával egy tekintet alá esik minden olyan okirat, amely kétséget kizáróan az adott számlára hivatkozva, annak adattartalmát módosítja (és megfelel az ÁFA tv. 170. §-ában meghatározott feltételeknek). Az EU más tagállamában nyilvántartásba vett adóalany esetében számla a termékértékesítéséről, szolgáltatásnyújtásról kibocsátott olyan okirat, amely megfelel a Héa-irányelv 226-231. és 238-240. cikkével harmonizáló azon előírásoknak, amelyek abban tagállamban alkalmazandóak, amelyben az adóalanyt nyilvántartásba vették. (Héa-irányelv alatt a 2006/112/EK tanácsi irányelvet kell érteni.)

Az ÁFA tv. előírása alapján a számla kibocsátásának időpontjától a számla megőrzésére vonatkozó időszak végéig biztosítani kell a számla eredetének hitelességét, adattartalma sértetlenségét és olvashatóságát.

Az „eredet hitelessége” a terméket értékesítő, a szolgáltatást nyújtó, illetve a számlát kibocsátó azonosságának biztosítását jelenti.

Az „adattartalom sértetlensége” azt jelenti, hogy a számlának az ÁFA tv. szerinti tartalmát nem változtatták meg.

A számla olvashatósága pedig azt jelenti, hogy a számlának az ember számára – alapos vizsgálat, illetve magyarázat nélkül – olvashatónak kell lennie.

Az e kötelezettségekhez kapcsolódó keretszabály értelmében az eredet hitelességére, az adattartalom sértetlenségére és az olvashatóságra vonatkozó követelményeknek mindig meg kell felelni és bármely olyan üzleti ellenőrzési eljárással eleget lehet tenni, amely a számla és a termékértékesítés/szolgáltatásnyújtás között megbízható üzleti kapcsolatot biztosít. Az eredet hitelességére és az adattartalom sértetlenségére vonatkozó feltételt a számlakibocsátónak és a számlabefogadónak is teljesítenie kell, amely feltételek fennállását a felek egymástól függetlenül (is) biztosíthatják. Amennyiben azonban a számla minősített aláírással és időbélyegzővel van ellátva, akkor a kibocsátó feladata a helyes elkészítés, a fogadó feladata pedig a változatlan megőrzés, ebben az esetben a fogadónak már nem kell „egyéb eljárással” biztosítania az üzleti kapcsolatot a számla és a kiszámlázott tevékenység között.

Az ÁFA tv-ben megjelölt üzleti ellenőrzési eljárás megnevezés mindazonáltal széles körű fogalmat takar. Üzleti ellenőrzési eljárásnak kell minden olyan eljárást tekinteni, amelyet az adóalany a számlának a saját pénzügyi követelésével, illetve kötelezettségével történő összevetése érdekében alkalmaz. Az üzleti ellenőrzési eljárás fontos eleme, hogy a számlát az üzleti és számviteli folyamaton belül ellenőrzik (nem pedig független, önálló dokumentumként kezelik). Az adóalany az általa választott/kidolgozott üzleti ellenőrzési eljárás során, a saját érdekében kibocsátóként és befogadóként is elsődlegesen azt ellenőrzi, hogy a számla lényegében megfelelő-e, vagyis, hogy a számlában feltüntetett ügylet ténylegesen a feltüntetett mennyiségben és minőségben teljesült-e. Továbbá befogadóként vizsgálja, hogy a számla kibocsátójának fizetési igénye jogos-e, a számla kibocsátója által megadott bankszámlaszám megfelelő-e annak biztosítására, hogy ténylegesen csak azokat a számlákat egyenlítse ki, amelyek kiegyenlítésére kötelezett. Ez utóbbi esetben az elektronikus számlák elektronikus aláírása mellőzhető, viszont ebben az esetben a befogadónak további intézkedéseket kell tennie a hitelesség biztosítására a megőrzési idő végéig.

A számla tehát papíralapon és elektronikus úton is kibocsátható. Az ÁFA tv-ben meghatározott fogalomnak megfelelően elektronikus számlának minősül minden olyan, az ÁFA tv-ben előírt adatokat tartalmazó számla, amelyet elektronikus formában bocsátottak ki és fogadtak be, más megkötés gyakorlatilag nincs. Egyes kiemelt területek – például európai elektronikus közbeszerzés – meghatároznak olyan elektronikus számlaformátumokat, amelyeket minden szereplőnek kötelessége támogatni, de az általános kötelezettségeket a számlarendelet tartalmazza.

A számlákra vonatkozó általános szabályokat az elektronikus számlákra is alkalmazni kell. Mivel az elektronikus számla fogadásának, illetve az eredet hitelessége, az adattartalom sértetlensége és az olvashatóság biztosításának a termék beszerzője/szolgáltatás igénybe vevője részéről technikai feltételei vannak, az elektronikus számlázáshoz elengedhetetlen a felek együttműködése. Ezért az ÁFA tv. az elektronikus számla kibocsátásának feltételeként előírja a számlabefogadó beleegyezését (ami nem csak formális lehet, vagyis megvalósulhat pl. a kapott számlán szereplő ellenérték kifizetésével, hallgatólagos beleegyezés révén is), illetve elektronikus adatcsere (EDI) rendszer alkalmazása esetén a felek előzetes írásbeli megállapodását.

Áfával számítottan (azaz bruttó) 900.000 forintos értékhatár alatt mentesül a számlaadási kötelezettség alól az adóalany, ha a terméket megvásárló, a szolgáltatást igénybe vevő olyan nem adóalany személy, aki az ügylet ellenértékét – a teljesítés napjáig – készpénzzel, készpénz-helyettesítő fizetési eszközzel, vagy pénzhelyettesítő eszközzel, esetleg többcélú utalvánnyal megtéríti, és számla kibocsátását nem kéri. Ezekben az esetekben az adóalany köteles a termék beszerzője, szolgáltatás igénybe vevője részére nyugtát kibocsátani. Nyugta helyett az adóalany számlát is kibocsáthat, ez természetesen nem tilos. A nyugta lehet papíralapú vagy elektronikus, és kizárólag magyar nyelven állítható ki.

A nyugta kötelező adattartalma (ÁFA-törvény 173. §) a következő:

- a nyugta kibocsátásának kelte (vagy az az időpont vagy időszak, amikor a nyugtában megjelölt szolgáltatás igénybe vehető),
- a nyugta sorszáma, amely a nyugtát kétséget kizáróan azonosítja,
- a nyugta kibocsátójának adószáma, valamint neve és címe, illetve
- a termék értékesítésének, szolgáltatás nyújtásának adót is tartalmazó ellenértéke.

Természetesen a nyugta kibocsátásának időpontjától a nyugta megőrzésére vonatkozó időszak végéig szintén biztosítani kell a nyugta eredetének hitelességét, adattartalma sértetlenségét és olvashatóságát. Érdekességként megemlítjük, hogy a NAV készített egy ingyenesen használható online számlakészítő megoldást is (https://onlineszamla.nav.gov.hu/ - a zöld oldal).

7.2.2.1 Az elektronikus számla megőrzése

A hatályos szabályok szerint minden személy, szervezet, aki adótörvényben szabályozott jogot gyakorol, illetőleg akire az adótörvény kötelezettséget állapít meg, köteles az adómegállapítás hiánytalan és helyes volta ellenőrizhetőségének érdekében az általa vagy nevében kibocsátott, valamint a birtokában levő vagy egyéb módon rendelkezésére álló okiratot legalább az adó megállapításához való jog elévüléséig megőrizni. A megőrzési kötelezettség papíralapú okirat esetében a kibocsátásra kötelezett részéről a másodlati példányra, a befogadó részéről az okirat eredeti példányára, vagy – ha azt a törvény nem zárja ki – eredeti

példány hiányában annak hiteles másolatára vonatkozik. A megőrzési kötelezettség teljesíthető a papíralapon kibocsátott okirat elektronikus formában történő megőrzésével is. Elektronikus okirat kizárólag elektronikus formában őrizhető meg. A kötelezettség teljesítését nem befolyásolja az elektronikus okirat formátumának a 168/A. §-ban foglalt követelményeknek megfelelő megváltoztatása. A megőrzési kötelezettség elektronikus formában történő teljesítése esetén az adóalanynak elektronikusan kell megőriznie a számla eredetének hitelességét, adattartalma sértetlenségét biztosító adatokat is. Fontos szabályokat tartalmaz ehhez a számla és a nyugta adóigazgatási azonosításáról, valamint az elektronikus formában megőrzött számlák adóhatósági ellenőrzéséről szóló 23/2014. (VI. 30.) NGM rendelet és a digitális archiválás szabályairól szóló 1/2018. (VI. 29.) ITM rendelet is. Az aláírt bizonylatokkal kapcsolatos fontos rendelkezés, hogy ha a legalább fokozott biztonságú elektronikus aláírással ellátott dokumentum megőrzéséről a megőrzésre kötelezett nem bizalmi szolgáltató útján gondoskodik, akkor az utólagos módosítás és sérülés elleni védelem érdekében köteles az elektronikus aláírás érvényességét ellenőrizni, és a megőrzési kötelezettség időtartama alatt köteles gondoskodni az elektronikus aláírás érvényességének fenntartásáról.

Gyakorló kérdések:

1. Melyek az e-számla főbb jellemzői?
2. Mi a követelmény az e-számla hitelességének biztosításához?
3. Meddig kell megőrizni az e-számlákat?

8 Irodalomjegyzék

8.1 Könyvek, kiadványok, folyóiratok

[1] Almási János: Az elektronikus aláírás és társai, Sans Serif, 2002, ISBN: 963 2027 44 2

[2] Almási János, Balázs László, Erdősi Péter Máté, Kovács Árpád, Rátai Balázs, Schvéger Judit: Elektronikus hitelesség, elektronikus alírás, 2010, ISBN: 978 963 06 8727 0

[3] Az információs társadalom dimenziói, Információ és Társadalom Sorozat, szerk. Balogh Gábor, Gondolat-Infónia, Budapest, 2006, ISBN: 963 9610 41 00, ISSN: 1786-0024

[4] Balogh Zsolt György: Az elektronikus aláírás technikai alapjai és szabályozási keretei. BALOGH Zsolt György, JÓZSA Zoltán, SIKET Judit: Közigazgatási eljárásjogi ismeretek. Szegedi Tudományegyetem Állam- és Jogtudományi Kar, 2014. p. 137-159.

[5] Bárány-Horváth Attila: A „megfoghatatlan" információ – az empíria és az új paradigma mezsgyéjén; Korunk – kultúra, haza, nagyvilág, Harmadik Folyam, IX/4 szám, 1998. április, 61-76. old.

[6] Bertrand Russel: A nyugati filozófia története, Göncöl Kiadó, 1994. ISBN: 963 7875 56 5

[7] Budai Balázs Benjámin: *Az e-közigazgatás elmélete (Második, átdolgozott kiadás).* Budapest, Akadémiai Kiadó, 2014. ISBN 978 963 05 9498 1

[8] Claude E. Shannon–Warren Weaver: A kommunikáció matematikai elmélete – az információelmélet születése és távlatai, Budapest, 1986, OMIKK, ISBN: 963 592 508 5

[9] Csató István: A kibernetika – Az információ forradalma, Kossuth Könyvkiadó, 1972. 2. javított kiadás, PL-78-K-7174

[10] Donald E. Knuth: A számítógépprogramozás művészete – 1. Alapvető algoritmusok, 2. kiadás, Műszaki Könyvkiadó, Budapest, 1994. ISBN: 963 16 0075 0

[11] Fülöp Géza: Az információ nyomában – Bevezetés a szakirodalom-kutatásba, Kriterion Könyvkiadó, Bukarest, 1978; 894 511-95

[12] Halassy Béla: Az adatbázistervezés alapjai és titkai. Avagy az út az adattól az adatbázison át az információig. IDG Magyarországi Lapkiadó, 1994.

[13] Holy Péter: Információs rendszerek szervezése I., főiskolai jegyzet, ZMNE Egyetemi Kiadó, Budapest, 2002

[14] Horányi Özséb: Jel, jelentés, információ, kép; General Press Kiadó, 2006, ISBN: 963 9598 90 9

[15] Információs társadalom, mint a megfigyelések társadalma, Budapest, 2004, Aristotelész Kiadó, ISBN: 963 86670 0 1

[16] KESZTHELYI, András: Az IKT okozta paradigmaváltás. Multidiszciplináris Kihívások Sokszínű Válaszok, 2018 (3), Budapest, BGE KVIK, 2018. p. 24-36.

[17] Kóródi Albert: Bevezetés az információelméletbe (kézirat), 1954, Felsőoktatási Jegyzetellátó Vállalat, Budapest

[18] Sorbán Attila: Békák a szőnyegen – Apokrif feljegyzések az információ társadalmának összeomlása utáni időkből, Literator Könyvkiadó, Nagyvárad, 1999, ISBN: 973 9360 10 6

[19] Yoneji Masuda: Az információs társadalom, mint posztindusztriális társadalom, OMIKK, 1988, ISBN: 963 592 761 4

[20] Z. Karvalics László: Bevezetés az információtörténelembe, Gondolat-Infónia, Budapest, 2004, ISBN: 963 9567 32 9

8.2 Szabványok, keretrendszerek

[21] ISO17421: Open Archival Information System

[22] Consultative Committee for Space Data Systems: Reference Model for an Open Archival Information System (OAIS), CCDSD 650.0-B-1, January 2002, http://www.ccsds.org/

[23] CobiT: Control Objectives for Information and Related Technology, version 4.1, ISACF, 2007., http://www.cobit.org

[24] XML Signature Syntax and Processing (Second Edition), W3C Recommendation, 10 June 2008

[25] A Request for Comments „de facto” szabványok gyűjteménye, 2022, http://www.faqs.org/rfcs

[26] X.509: Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, Approved: 2008-11.

[27] International Telecommunication Union (ITU) X.800 Recommendation; Data Communication Networks: Open Systems Interconnection (OSI); Security, Structure and Applications; Security Architecture for Open Systems Interconnection for CCITT Applications, 1991, Geneva

[28] FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION (FIPS PUB) 186-4: Digital Signature Standard (DSS), National Institute of Standards and Technology, Gaithersburg, MD 20899-8900, Issued July, 2013

[29] ISO 32000-1: Document management - Portable document format - Part 1: PDF 1.7

[30] ETSI EN 319 122-1 V1.2.1 (2021-10) Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures

[31] ETSI EN 319 132-1 V1.2.1 (2022-02) Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures

[32] ETSI EN 319 142-1 V1.1.1 (2016-04) Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures

[33] ETSI EN 319 162-1 V1.1.1 (2016-04) Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers

[34] ETSI TR 102 038 V1.1.1 (2002-04) TC Security - Electronic Signatures and Infrastructures (ESI); XML format for signature policies

[35] ETSI TR 102 041 V1.1.1 (2002-02) Signature Policies Report

[36] ETSI TR 102 045 V1.1.1 (2003-03) Electronic Signatures and Infrastructures (ESI); Signature policy for extended business model

[37] ETSI TR 102 272 V1.1.1 (2003-12) Electronic Signatures and Infrastructures (ESI); ASN.1 format for signature policies

[38] ETSI TS 101 733 V2.2.1 (2013-04) Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)

[39] ETSI TS 102 176-1 V2.1.1 (2011-07) Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms

[40] ETSI TS 119 312 V1.4.3 (2023-08) Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

[41] NIST FIPS 180-4. Secure Hash Standard (SHS) Date Published: August 2015. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf