Nemzeti
Közszolgálati Egyetem

Az elektronikus közigazgatás alapjai

Budapest, 2014.

A tananyag az ÁROP-2.2.19-2013-2013-0001 Elektronikus képzési és távoktatási anyagok készítése című projekt keretében készült el.

Kiadja:
© NKE, 2014

Felelős kiadó:
Patyi András
rektor

Tartalom

I. AZ EURÓPAI UNIÓ INFORMÁCIÓS TÁRSADALOMMAL KAPCSOLATOS POLITIKÁI ÉS AZ ELEKTRONIKUS KÖZIGAZGATÁS

Az Európai Unió az 1990-es évek elején felismerte, hogy az informatika és az elektronikus hírközlés fejlődése e két terület önálló kezelését igényli. Az információs és kommunikációs technológiák (IKT) az ipari forradalomhoz hasonló változást generálnak. Az elektronikus adatfeldolgozó és hírközlési rendszerek teljesítményének növekedése és a digitális adattárolás valamint adatátvitel lehetőségeinek bővülése számos területet érintett, és egyre nyilvánvalóbb módon gyakorolt hatást a gazdaság működésére, az emberek mindennapjaira, a média világára és nem utolsó sorban az állami szervek munkájára. Társadalomtudományi kutatások és régóta formálódó elméletek szerint ez a komplex folyamat az „*információs társadalom*", egy globális kiterjedésű, informatika alapú társadalmi modell kialakulásához vezet. Erre a kihívásra az Európai Uniónak mihamarabb választ kellett adnia.

1.1. A Bangemann-jelentés

A felismerés már az 1980-as években is formálódott, de kinyilvánított társadalompolitikai szándékká csak később érett. 1993 decemberében az Európai Tanács felkért egy szakmai szakértői csoportot, hogy készítsen jelentést az információs társadalomról és fogalmazzon meg konkrét javaslatokat az információs fejlődés előmozdítására. Az „*Európa és a globális információs társadalom – Ajánlások az Európai Tanács számára*" című szakértői jelentés összeállítását az Európai Bizottság korábbi elnökhelyettese, Martin Bangemann irányította.

A Bangemann-jelentés az Európai Tanács aktívabb beavatkozását irányozta elő az európai vállalkozások nemzetközi versenyképességének megőrzéséhez, amihez szükség van a már megkezdett liberalizációs folyamat felgyorsítására, a már elérhető szolgáltatások működésének fenntartására és egységességének biztosítására. Alapelvként azt állapította meg, hogy az információs infrastruktúra kiépítése és működtetése elsősorban a privátszektor üzleti logikája alapján kell, hogy történjen, míg a szükséges szabályozási keret a tagállamok és az Unió intézményeinek összehangolt jogfejlesztő munkája nyomán alakul ki.

A Bangemann-jelentés tíz alkalmazási célterületet jelölt meg az informatikai és hírközlési technológiák alkalmazására és az eredmények elterjesztésére:

- távmunka,
- távtanulás,
- egyetemközi és kutatóközpontok közötti hálózatok,
- telematikus szolgáltatások a kis-és középvállalkozások számára,
- közúti közlekedési menedzsment rendszerek,
- és légi közlekedési ellenőrzés,
- egészségügyi hálózatok,
- a tendereztetési folyamatok számítógépesítése,
- egy egész Európát átfogó kormányzati hálózat, és végül
- városi információs szupersztráda kiépítése.

Az Európai Unió információs társadalommal kapcsolatos politikáinak ebben az első listájában már szerepel tehát az *elektronikus kormányzati* tevékenységgel kapcsolatos terület. A jelentést az Európai Tanács 1994. június 24-25-i korfui konferenciáján ismertették és elfogadták, ezzel új szakaszt nyitva a közösség információs társadalommal kapcsolatos politikáinak kidolgozásában.

A Bangemann-jelentést számos későbbi közösségi cselekvési terv követte, s ezek a stratégiai dokumentumok az információs társadalom fejlesztésében részt vevő szakterületek között rendre érintették az elektronikus közigazgatás, elektronikus kormányzat kérdéseit is.

1.2. Az eEurope 2002 akcióterv

Az „eEurope 2002 akcióterv" (Akcióterv) két vonatkozásban is meghatározza a fejlesztési folyamatokat az elektronikus közigazgatás területén. Egyfelől előirányozza, hogy az európai országok polgárai számára fontos közigazgatási szolgáltatások elektronikus úton elérhetővé váljanak. Ennek természetesen fontos eleme az ügyintézés egyszerűsítése és az információs társadalom kommunikációs infrastruktúrájának erősítése. Másik súlypontja pedig maga a közigazgatás hivatali apparátusának és munkaszervezésének átalakítása. Az elektronikus kormányzat ugyanis nemcsak az ügyfelek számára kínál szolgáltatásokat, hanem az igazgatási munkaszervezetek reakcióképességének és hatékonyságának javulását is eredményezheti.

A dokumentum szemlélete a „New Public Management" irányzat elveit tartja szem előtt, és tudatosan számol az üzleti igazgatásban kidolgozott szervezési és munkamódszereknek a közigazgatásban való meghonosításával, sőt ezen túlmenően a magánszektorral való együttműködéssel is. Stratégiai célként határozza meg a hivatalon belüli igazgatási és munkafolyamatok átalakítását, és az európai közösségi szintű közigazgatási szolgáltatások kialakítása érdekében a divergáló tagállami szabályozási környezet harmonizálását.

Az EU jogállami alapkövetelményként tekint az igazgatási szervezetrendszer átlátható működésére, s e törekvés erősítését azzal szolgálja az Akcióterv, hogy a közérdekű adatokhoz való hozzáférés javítását az egyik kiemelt célterületté teszi.

Az Akcióterv által meghatározott legfontosabb célfeladatok:

- alapvető közérdekű adatok elektronikus hozzáférhetővé tétele a digitális hálózaton keresztül;
- elektronikus hozzáférés az alapvető közigazgatási szolgáltatásokhoz;
- a közszféra intézményeinek kezelésében lévő adatok széles körű – akár piaci jellegű – újrahasznosítására vonatkozó koncepció kidolgozása;
- nyílt forráskódú szoftverek használatának támogatása a közszférában;
- az elektronikus kormányzattal és közigazgatással kapcsolatos tagállami és közösségi tapasztalatok megosztása;
- a Bizottság érdekeltségi körébe tartozó eljárások elektronikus környezetbe való átültetése;
- az elektronikus aláírás használatának támogatása.

1.3. Az eEurope 2005 akcióterv

Az előbbi cselekvési program céljainak szerves folytatása céljára dolgozták ki az eEurope 2005 akciótervet, amely egyéb területek fejlesztéspolitikai menetrendjének meghatározása mellett az elektronikus közigazgatási szolgáltatások terjesztését ugyancsak alapvető prioritásként kezeli. E tekintetben – általában 2005 év végi megvalósítási határidő megjelölésével – az alábbi területeket emeli ki:

- A tagállamokban minden közigazgatási szerv rendelkezzen szélessávú hálózati összeköttetéssel, melyben a nyílt forráskódú (az egyszerűség kedvéért: Linux alapú) szoftvereken alapuló megoldásoknak is teret biztosítanak.
- A tagállamok biztosítsák, hogy az alapvető közigazgatási szolgáltatások interaktívak és mindenki számára hozzáférhetőek legyenek.
- Elektronikus közbeszerzési szabályozás megalkotása és a gyakorlati megvalósításhoz és üzemeltetéshez szükséges informatikai rendszer kiépítése.
- Nyilvános, közösségi Internet-hozzáférés biztosítása minden európai polgár számára.
- Európát népszerűsítő elektronikus szolgáltatások indítása.
- A közszféra adatainak felhasználóbarát elérését lehetővé tevő szolgáltatások indítása és az erre vonatkozó szabályozás megalkotása.

1.4. i2010 eGovernment cselekvési terv

A 2006-ban elfogadott i2010 eGovernment cselekvési terv[1] abból a feltevésből indult ki, hogy szoros kapcsolat áll fenn a verseny- és innovációs képesség, valamint a közigazgatás minősége között, így a „jó kormányzás" megvalósítása elengedhetetlen a világgazdasági versenyben. Így az elektronikus közigazgatás minőségi javulása nagyban hozzájárulhat az Unió fejlesztési céljainak megvalósításához.

A cselekvési terv középpontjában öt fő célkitűzés áll, amelyek a következők:

- A hátramaradtak felzárkóztatása, azaz a társadalmi integráció felgyorsítása az elektronikus kormányzaton keresztül annak érdekében, hogy 2010-re minden polgár élvezhesse a megbízható, innovatív szolgáltatásokat és az azokhoz való könnyű hozzáférést.
- Az eredményesség és a hatékonyság elérése, azaz magas felhasználói elégedettség, átláthatóság, elszámoltathatóság megteremtése, valamint az adminisztratív terhek csökkentése.
- A polgárok és a vállalkozások javára nyújtott, nagy jelentőségű alapszolgáltatások (például közbeszerzés) elektronikus elérése és lebonyolítása.
- Lehetővé tenni a polgárok és a vállalkozások számára, hogy a közszolgáltatásokhoz 2010-re kényelmes, biztonságos és interoperábilis, hitelesített hozzáférést élvezhessenek egész Európában.
- A részvétel és a demokratikus döntéshozatal erősítése. Az elektronikus közigazgatás kiépítésével, megteremtésével az online közszolgáltatások révén leküzdhető a digitális megosztottság, megszüntethető a digitális kirekesztődés.

1.4.1 Alapvető elektronikus közszolgáltatások

A cselekvési tervben megfogalmazottak megvalósításának eredményeit a Bizottság három területen várta: a polgárok és vállalkozások tekintetében a közigazgatásban, valamint e kettő eredményeként a társadalom és a gazdaság egésze tekintetében. E várakozások teljesülésének előmozdítása érdekében az Európai Bizottság közzé is tette a közigazgatás által a polgárok és a vállalkozások számára elektronikus úton nyújtandó szolgáltatások körét; összesen 20 területet kiemelve. Ezek közül 12 szolgáltatást határozott meg a természetes személyek, és 8 további szolgáltatást a gazdálkodó szervezetek részére.

Természetes személyek számára nyújtott (nyújtandó) szolgáltatások:

- a jövedelemadóval kapcsolatos ügyintézés,
- a munkaügyi hatóságok álláskereső szolgáltatásai,
- a társadalombiztosítással kapcsolatos ügyintézés (a munkanélküliség, a családi pótlék, az orvosi kezelések költségei, illetve az ösztöndíjak területén),
- személyi okmányokkal kapcsolatos ügyintézés,
- gépjárművek adminisztrációja,
- építési engedélyek igénylése,
- rendőrségi bejelentések,
- könyvtári szolgáltatások,
- anyakönyvi ügyintézés,
- egyetemi és főiskolai beiratkozás,
- lakhelybejelentés,
- egyes egészségügyi szolgáltatások (pl. kórházakkal kapcsolatos információk beszerzése).

A gazdálkodó szervezetek számára nyújtott (nyújtandó) alapszolgáltatások:

- a munkavállalók járulékaival kapcsolatos ügyintézés,
- a társasági és a jövedéki adóval kapcsolatos ügyintézés,
- a cégnyilvántartáshoz kapcsolódó szolgáltatások,
- a statisztikai adatszolgáltatási kötelezettségek teljesítése,
- a vámügyintézés,
- a környezetvédelmi engedélyek beszerzése,
- a közbeszerzési eljárások lefolytatása.

1 i2010 eGovernment cselekvési terv: az elektronikus kormányzat létrehozásának felgyorsítása a társadalom egészének javára COM(2006) 173

Az elektronikus ügyintézés szintjei

Az e-ügyintézési szolgáltatási szintek kategorizálását az uniós stratégiai dokumentumok alapján egységesen használjuk.

Szolgáltatási szint	Szolgáltatási szint leírása
1. szint: Információ (tájékoztatás)	A közigazgatási szerv weboldalán csupán alapvető információkat (pl. elérhetőség), ügyleírásokat közöl, leírja, hogy milyen dokumentumok szükségesek az ügyintézéshez. (statikus weboldalak)
2. szint: Egyirányú kapcsolat	A közigazgatási szerv weboldaláról (Word, PDF stb.) dokumentumokat lehet letölteni az ügyintézéshez, de azokat nem lehet elektronikus formában visszaküldeni, csak hagyományos (postai levél) módon.
3. szint: Kétirányú interakció	A közigazgatási szerv honlapján a dokumentumokat ki lehet tölteni online, a kitöltés ellenőrzése is megtörténik ilyenkor, illetve a letöltött dokumentumokat azonosítási eljárás mellett vissza is lehet küldeni elektronikus formában (űrlapok visszaküldéséhez és fogadásához az elektronikus aláírás alkalmazására van szükség, ugyanakkor lakossági bejelentésekhez elegendő egyéb digitális azonosítás, pl.: regisztráció). Interaktivitást növelő szolgáltatások is segítik a felhasználók tájékozódását, például: kérdezés, visszacsatolás lehetősége, online segítségnyújtás, fórum. Az ügy indításához (intézéséhez, okmányok leadásához) személyes megjelenés nem szükséges, de az ügyhöz kapcsolódó közigazgatási irat (igazolvány, határozat stb.) átvétele, valamint a kapcsolódó illeték- vagy díjfizetés hagyományos úton történik.
4. szint: Tranzakció	Teljes körű elektronikus ügyintézés (ide értve a döntés közlését, a kézbesítést és a fizetést is), amely azt jelenti, hogy az elektronikusan visszaküldött dokumentumok (pl.: űrlapok) feldolgozása is automatikusan történik. Megvalósul a dokumentumok, ügymenetek elektronikus nyomon követése, lehetővé válik az illetékek, díjak elektronikus úton történő befizetése. Ennek feltétele egyrészt az elektronikus aláírás széles körű elterjedése, másrészt, hogy olyan integrált rendszer jöjjön létre, amely hatékonyan kapcsolja össze az önkormányzat front-office (kapcsolat az ügyféllel) és back-office (háttérben működő, az ügyintéző munkáját támogató) rendszereit.
5. szint: Perszonalizáció	A 4. szint kiegészítése az ügyfél maximális bevonásával. Személyre szabott, ügyfél-központú, automatizált és proaktív szolgáltatások

1.5. eGovernment 2011-2015 cselekvési terv

Az EU elektronikus közigazgatással és elektronikus kormányzattal kapcsolatos stratégiai tervei közül jelenleg az „*A 2011–2015 időszakra szóló európai elektronikus kormányzati cselekvési tervről az IKT az intelligens, fenntartható és innovatív kormányzat szolgálatában*”[2] című dokumentum a legfontosabb, mely egyúttal részét képezi a közösség információs társadalommal kapcsolatos politikáját 2020-ig meghatározó *európai digitális menetrendnek* is.[3]A program kiemelt célokat és ezek teljesüléséhez kulcsfeltételeket állapít meg.

1.5.1. A legfontosabb átfogó célterületek

- A felhasználók bevonása az interaktív elektronikus közszolgáltatások rendszerébe;
- a közszféra adatvagyonának üzleti célú további felhasználásának erősítése;
- a közigazgatási rendszer átláthatóságának javítása;
- akadálymentes közigazgatási szolgáltatások nyújtása a vállalkozások számára;
- EU-szerte a határok nélküli közigazgatási szolgáltatások megvalósítása, s ezáltal az egységes európai közigazgatási tér kialakítása;
- a közigazgatási szervezeten belül a hatékonyság növelése, az ügyfelek irányába pedig az adminisztratív terhek csökkentése.

2 COM(2010) 743
3 COM(2010) 245

1.5.2. A fenti célkitűzések teljesülésének előfeltételei

- *Interoperabilitás és nyílt hálózati architektúra alkalmazása*. Az interoperabilitás az összekapcsolt rendszerek és gépek képessége az adatok cseréjére, feldolgozására és megfelelő értelmezésére. Mivel az adatkezelésnek jogi, szervezeti és terminológiai szempontjai is vannak, nem csak műszaki kihívásról van szó.
- *Elektronikus személyazonosítási technológiák* fejlesztése és széles körű alkalmazása. Sok online szolgáltatás esetében különösen fontos a szolgáltatást használó személy vagy jogi személy hiteles beazonosítása. Az elektronikus személyazonosító (eID) technológiák és hitelesítési szolgáltatások (a magán- és a közszférában egyaránt) nélkülözhetetlenek az elektronikus úton végzett műveletek biztonsága szempontjából. A program előirányozza a tagállami elektronikus személyazonosítási megoldások kölcsönös elismerését lehetővé tevő páneurópai keretrendszer létrehozását, amely által a polgárok és a vállalkozások Európa bármely országában elektronikus úton tudják személyazonosságukat igazolni.
- *Elektronikus hitelesítés, biztonságos dokumentumkezelés.* Az elektronikus dokumentumok közigazgatási célú felhasználása megkívánja azok hiteles kezelésének biztosítását. Az együttműködésre képes elektronikus közszolgáltatások biztosítása érdekében pedig biztosítani kell a páneurópai hitelesítési rendszer kidolgozását. A koncepciónak tiszteletben kell tartania az adatok és a magánélet védelmére vonatkozó rendelkezéseket. E munka során figyelembe kell venni az elektronikus aláírásra és az elektronikus azonosításra vonatkozó, meglévő cselekvési tervben és az elektronikus aláírásról szóló irányelvben foglaltakat.

2. Az elektronikus közigazgatással kapcsolatos törekvések Magyarországon

2.1. A 2006 évi OECD jelentés

Az OECD 2006 decemberében elkészítette és közzétette az elektronikus közigazgatás magyarországi helyzetéről szóló jelentését.[4]A dokumentum a legfontosabb eredmények között említi, hogy az EU által meghatározott 20 alapvető elektronikus szolgáltatás Magyarországon megvalósult. Valójában a vizsgálat időpontjában nem lehetett még kijelenteni azt, hogy az említett szolgáltatások közül mindegyik az elvárt szinten áll a kitűzött teljesítési határidőre. A pontosság érdekében meg kell jegyezni, hogy az elvárásokat megfogalmazó EU is több szolgáltatási szintet jelölt meg, az egyszerű tájékoztató szolgáltatástól egészen a teljesen interaktív ügyintézési lehetőségek megvalósításáig.

Az Ügyfélkapu használata ebben az időben már terjedőben volt, s a dokumentum ezt is érdemként említi. A regisztrált felhasználók száma 2005 végén elérte a 150 ezer főt. Abszolút számban ez igen jelentős, de ezzel együtt is csak a hazai lakosság mintegy 1,5%-át teszi ki, ami nem tekinthető jó eredménynek. Az Ügyfélkapun elérhető szolgáltatások zöme pedig a vizsgálat idején nem volt – és bár helyzet azóta is sokat javult, valójában a mai napig sem – olyan, amely kiküszöbölné a személyes megjelenés szükségességét az ügyintézésben.

A jelentés hiányosságként értékelte, hogy Magyarországnak 2006 végéig nem volt az elektronikus közigazgatás kiépítésével kapcsolatos komplex célkitűzési és intézkedési csomagja.

2.2. Az E-közigazgatás 2010 Stratégia

Az OECD jelentésére reagálva a Kormány 2008-ban az *E-közigazgatás 2010 Stratégia* megalkotásával olyan jövőképet kívánt kialakítani, ami egységes keretet ad az elkövetkezendő évek fejlesztéseinek. A stratégia nem titkolt célja az is, hogy a közigazgatási fejlesztések a jövőben egységes elvek alapján, egységes keretrendszerben valósuljanak meg.

A dokumentum tartalma lényegében követi azokat az iránymutatásokat, amelyeket az EU stratégiai programjai kialakítottak. A program rámutat, hogy az online közigazgatás sikere az állampolgárok és a vállalkozások részvételén és a hagyományos ügyintézésen túlmutató, ügyfélbarát elektronikus közigazgatási szolgáltatások kiépítésén múlik.

4 Az OECD 2006. decemberi országtanulmányának végkövetkeztetései a magyarországi elektronikus kormányzásról, Magyar Közigazgatás, 2006. december, pp. 705-712.

2.3. Magyary Program 12.0 és a Digitális Megújulás Cselekvési Terv

A Magyary Zoltán Közigazgatás-fejlesztési Program 12.0 (MP 12.0) az e-közigazgatást a közigazgatás-fejlesztés eszközeként kezelte. A Digitális Megújulás Cselekvési Terv pedig az információs társadalom stratégiájaként nem ágazati, hanem horizontális célokat fogalmazott meg.

Az MP 12.0 az ügyviteli folyamatok és a inkább közigazgatás belső folyamatai oldaláról, a DMCST pedig inkább infrastrukturális oldalról közelítette meg az e-közigazgatás tágabb témakörét.

Történeti oka volt, hogy két külön dokumentum is érintette az e-közigazgatással. A 2010-ben kezdődő kormányzati ciklusban a közigazgatási informatikát két részre bontották, e-közigazgatásra és az infrastrukturális területre, ezeket pedig külön minisztériumok irányították.f

A Magyary Program részeként a Közigazgatási és Igazságügyi Minisztérium 2011-ben végrehajtotta a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény (röviden Ket.) reformját, megteremtve az elektronikus ügyintézés szükséges eljárási elemeit, garanciáit. A Ket. végrehajtási rendeletei az elektronikus úton nyújtott szolgáltatások részletszabályait hivatottak megalkotni, új irányt szabva és tartalmat adva az interoperabilitási törekvéseknek. További fontosabb eredmények:

- Adatvagyon törvény[5] végrehajtása; kiszervezett feladatok visszavétele.
- Az információbiztonság[6], az adatvédelem[7] és az interoperabilitás[8] törvényi szabályozása.

A Digitális Megújulás Cselekvési Terv négy fő területre koncentrált stratégiájában:

- Az állampolgárok esélyegyenlőségének biztosítása
- A vállalkozások versenyképességének növelése
- A modern közigazgatási informatika tényleges megteremtése
- Az informatikai infrastruktúra fejlesztése

A terv egyik legfontosabb pillére a fentiek alapján egyértelműen az infokommunikációs infrastruktúra.

2.4. Nemzeti Infokommunikációs Stratégia (NIS) 2014

Magyarország Nemzeti Infokommunikációs Stratégiáját a 1069/2014. (II. 19.) Korm. határozatban tették közzé.

A NIS jellemzően nem csak e-közigazgatási, hanem információs társadalmi kihívásokra (is) ad választ.

A Stratégia megalapozza a 2014-2020 közötti infokommunikációs célú fejlesztéseket, amelyeket döntően a Gazdaságfejlesztési és Innovációs Operatív Program Infokommunikációs fejlesztések prioritása finanszíroz több száz milliárd forint összegben.

5 2010. évi CLVII. törvény a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről
6 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
7 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
8 2013. évi CCXX. törvény az állami és önkormányzati nyilvántartások együttműködésének általános szabályairól

3. A magyar elektronikus közigazgatási rendszer szervezeti keretei

Az EU stratégiai dokumentumai és azok hazai adaptációja alapján a jelenlegi magyar elektronikus közigazgatási rendszer gerincét a *Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala* (KEKKH) és a *Nemzeti Infokommunikációs Szolgáltató Zrt.* (NISZ Zrt.) jelenti.

3.1. Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala

3.1.1. A KEKKH jogállása

2007. január 1. napjával a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala a Központi Adatfeldolgozó, Nyilvántartó és Választási Hivatal tevékenységi körének és szervezeti kereteinek,a Távközlési Szolgálat, valamint a Kormányzati és Frekvenciagazdálkodási Hivatalfeladataival történő kibővülésével jött létre.,

A KEKKH – közjogi jogállását tekintve – központi hivatal, amelyet a közigazgatási informatikáért (e-közigazgatásért) való felelőssége körében a közigazgatási és igazságügyi miniszter irányít. A KEKKH – költségvetési jogállását tekintve – önállóan gazdálkodó, az előirányzatok felett teljes jogkörrel rendelkező költségvetési szerv.

3.1.2. A KEKKH feladat és hatásköre

3.1.2.1. *A személyiadat- és lakcímnyilvántartáshoz kapcsolódó ügyek*

A KEKKH

- az elektronikus anyakönyvi rendszer adatkezelő szerve;
- gondoskodik a személyi azonosító képzéséről;
- kezeli a nyilvántartás adatállományát és biztosítja a nyilvántartásban kezelt adatok helyességét;
- a törvényben meghatározott feltételek fennállása esetében adatszolgáltatást teljesít a nyilvántartásból;
- ellátja a személyi adat- és lakcímnyilvántartás, valamint a személyazonosító igazolvány kiadásával és nyilvántartásával kapcsolatos hatósági feladatokat;
- működteti a nyilvántartás informatikai rendszerét;
- adatfeldolgozót bízhat meg egyes adatfeldolgozási műveletek, technikai feladatok elvégzésével.

3.1.2..2 Útlevélügyek

A KEKKH

- első fokon jár el a magánútlevéllel, az ideiglenes magánútlevéllel, a szolgálati és a hajós szolgálati útlevéllel, valamint a határátlépési igazolvánnyal összefüggő hatósági ügyben;
- a hatáskörébe tartozó úti okmányok soron kívüli, sürgősségi, valamint azonnali eljárás keretében történő kiállítására vonatkozó kérelmek átvételére és az ilyen eljárásban kiállított úti okmányok kiadására ügyfélszolgálati irodát tart fenn. Az úti okmányokkal és a külföldre utazásra felhasznált személyazonosító igazolványokkal összefüggő feladatok ellátásában közreműködő szervekkel és a konzuli tisztviselőkkel való kapcsolattartásra ügyeleti szolgálatot működtet;
- végzi az útlevelek megszemélyesítését és a biometrikus azonosítót tartalmazó tároló elem adatokkal történő feltöltését;
- ellátja a nemzeti dokumentum-aláíró hatósági és az országos aláíró hitelesítő hatósági feladatokat;
- ellátja az országos ellenőrzőhitelesítő hatósági, valamint a nemzeti dokumentumellenőrző-hitelesítő hatósági feladatokat.

3.1.2.3. Bűnügyi nyilvántartások vezetése, adatszolgáltatás és hatósági erkölcsi bizonyítvány kiállítása

A KEKKH kezeli a jogszabályban meghatározott különböző bűnügyi nyilvántartásokat. Ezek a következők:
- a bűntettesek,
- a kényszerintézkedés alatt állók,
- a büntetőeljárás alatt állók,
- a daktiloszkópiai és fénykép, valamint
- a DNS-profilok nyilvántartása.

Ezekből az arra jogosultak
- a bíróság,
- az ügyészség,
- a nyomozó hatóságok,
- az idegenrendészeti ügyekben eljáró szervek

részére adatszolgáltatást teljesít.

E nyilvántartások alapján az érintett természetes személy kérésére hatósági erkölcsi bizonyítványt állít ki.

3.1.2.4. Választási informatikai feladatok

A választás informatikai rendszerét – állami feladatként – szintén a KEKKH működteti. Az informatikai rendszer a KEKKH számítóközpontjára és a vele hálózati kapcsolatban lévő számítógépes munkaállomásokra épül.

Az informatikai rendszert kell alkalmazni
- a szavazókörök kialakításához és aktualizálásához, a szavazókör kijelöléséhez, jelentéséhez,
- a névjegyzék és az értesítő elkészítéséhez szükséges adatállományoknak a helyi választási irodák részére történő biztosításához, a névjegyzék összeállításához, elkészítéséhez,
- a névjegyzék továbbvezetéséhez, a névjegyzék közszemlére, illetve szavazókörbe kerülő példányának elkészítéséhez,
- a választójogosultság megállapításához, illetve ellenőrzéséhez,
- a választójoggal nem rendelkező nagykorú polgárok adatait tartalmazó jegyzék kezeléséhez,
- a választópolgárnak a névjegyzék elkészítése után bekövetkezett lakcímváltoztatásával kapcsolatos feladatok teljesítéséhez,
- az igazolás kiadásához,
- a jelölő szervezetek, listák és jelöltek adatainak nyilvántartásához,
- az ajánlószelvények ellenőrzéséhez,
- a választás előzetes tájékoztató adatait tartalmazó, országosan összesített tájékoztató adatok előállításához.

A KEKKH vezeti a választójoggal nem rendelkező személyek központi nyilvántartását, és a választásokhoz, továbbá az országos népszavazás-kezdeményezést és a népi kezdeményezést aláírók adatainak hitelesítéséhez hivatalból, egyéb esetben írásos kérelem alapján adatszolgáltatást teljesíti az arra jogosultak (pl. választási bizottságok, választási irodák, az érintett választópolgár, bíróságok) részére.

3.1.2.5. A közúti közlekedési igazgatási feladatok

E körben a KEKKH egyebek mellett:
- megküldi a vezetői engedélyt a kérelmező részére,
- kiállítja, és postai úton továbbítja a jogosult részére a törzskönyvet,
- engedélyezi az egyénileg kiválasztott és az egyedileg előállított rendszámtábla legyártását és használatát,
- kiadja a muzeális jellegű járműveken használható OT betűjelű rendszámtáblát,
- ellátja járműkísérő lappal a gépjármű-forgalmazókat.

3.1.2.6. Okmányokkal, hatósági igazolványokkal kapcsolatos további első fokú hatósági feladatok

- A személyazonosító igazolvány, valamint a személyi azonosítóról és a lakcímről szóló hatósági igazolvány ügyében első fokú hatóságként jár el az illetékes jegyzővel együtt.
- Vezeti az egyéni vállalkozók nyilvántartását.
- Eljár a „Magyar igazolvány” és a „Magyar hozzátartozói igazolvány” kiadásával, cseréjével, visszavonásával és nyilvántartásával összefüggő hatósági ügyben.

3.1.2.7. Informatikai biztonsági és rejtjelezési feladatok

A KEKKH a telekommunikációs és hálózat-fenntartási feladatai körében elvégzi

- a működtetési körébe utalt rejtjelező végpontok műszaki-technikai üzemvitelét, kulcsellátását,
- a saját rejtjelfelügyelettel nem rendelkező szervezetek számára ellátja a rejtjelező eszközök használatához szükséges kiképzési, vizsgáztatási feladatokat.

3.1.2.8. Irányítási és felügyeleti feladatok

- A KEKKH felel fővárosi és megyei kormányhivatal járási hivatalainak szervezeti egységeiként működő okmányirodák feladatainak ellátásáért. E feladatai ellátásán túl szakmai irányítást gyakorol az okmányirodák ügyfélszolgálati tevékenysége, működése felett, amelynek keretében ellátja különösen az ügyfélszolgálati működés fejlesztésére, elemzésére, monitoringjára vonatkozó feladatokat.
- A KEKKH szakmai irányítást gyakorol a fővárosi és megyei kormányhivatalok törzshivatala és szakigazgatási szerveinek, valamint a fővárosi és megyei kormányhivatal járási hivatalainak törzshivatala és szakigazgatási szervei informatikai tevékenysége felett, ennek keretében gondoskodik az informatikai üzemeltetés feltételeinek meghatározásáról, valamint egyetértési jogot gyakorol az informatikai tárgyú szerződések megkötése során.
- A KEKKH e szakmai irányítása keretében a fővárosi és megyei kormányhivatalok szakigazgatási szervei által használt szakrendszerek esetében együttműködik a szakrendszereket üzemeltető szakmai irányító szervvel.

3.2. NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.

3.2.1. A NISZ és jogelődei története

A NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. (rövid nevén NISZ Zrt.) jogelődei révén fél évszázados múltra tekint vissza. Elődei, az 1964-ben alapított Konjunktúra- és Piackutató Intézet (KOPINT) és az 1968-ban létrehozott Datorg Külkereskedelmi Adatfeldolgozó és Szervező Rt., melyeknek összevonásával 1987-ben jött létre a KOPINT-DATORG Konjunktúra-, Piackutató és Informatikai Intézet. 2005 júliusától a társaság egyedüli tulajdonosa a magyar állam lett, azóta zártkörűen működő részvénytársaságként működik. 2007 óta a vállalat fő tevékenysége teljes körű infokommunikációs szolgáltatások nyújtása. 2008-ban a tulajdonosi jogokat a Magyar Nemzeti Vagyonkezelő Zrt. vette át, a társaság neve 2011-től NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.

Legnagyobb megrendelői államigazgatási szervek és országos hatáskörű intézmények, de gazdálkodó szervezetek, vállalkozások és magánszemélyek is igénybe veszik egyes szolgáltatásait. A NISZ Zrt. stratégiai feladatai között első helyen a

- kormányzati informatikai infrastruktúra működtetése,
- e-közigazgatási megoldások támogatása, valamint
- kormányzati szintű alap és emelt szintű informatikai szolgáltatások állnak.

A szolgáltatások kiterjesztésének érdekében NISZ Zrt. 2012-ben felvásárolta a Pro-M Zrt.-t, majd 2013-ban az IdomSoft Zrt.-t.

A NISZ elektronikus közigazgatási szolgáltatásai

3.2.2.1. A Központi Rendszer

A NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. által üzemeltetett Központi Rendszer a hazai elektronikus kormányzati szolgáltatások centrális hálózata.

3.2.2.2. A Kormányzati Portál

A Kormányzati Portál (www.magyarorszag.hu) az elektronikus kormányzati szolgáltatások centruma, melynek főbb profilja:

- az ügyfélkapu működtetése, kapcsolódó ügyfélszolgálat támogatása;
- köz- és államigazgatási információk gyűjtőhelye;
- e-szolgáltatások gyűjteménye;
- állampolgári közszereplést biztosító, személyes azonosításon alapuló fórum;
- hivatali kapu működtetése, teljes körű infokommunikációs szolgáltatások nyújtása az állami intézmények számára (hivatali kapu).

3.2.2.3. Az ügyfélkapu

Ügyfélkapu a magyar kormányzat elektronikus ügyfélbeléptető és azonosító rendszere. Segítségével a felhasználók biztonságosan és hitelesen léphetnek kapcsolatba a hatóságokkal, közigazgatási szervekkel és ügyeiket elektronikusan intézhetik. A portál felhasználóinak száma meghaladja az egymilliót, a Magyarországon nyújtott elektronikus kormányzati szolgáltatások túlnyomó része már elérhető ezen a rendszeren keresztül.

3.2.2.4. A hivatali kapu

A hatóságok egymás közötti és állampolgárokkal történő hiteles elektronikus kommunikációjának megteremtése kiemelt jelentőségű feladat a kormányzat és az egész közigazgatás számára. E feladat megvalósítására a Központi Rendszer kínál megoldást.

4. Az e-közigazgatás aktuális trendjei Magyarországon

4.1. Az elektronikus aláírás közigazgatási használatának elterjedéséről

Az elektronikus aláírás közigazgatási, hivatali célú használata eddig alacsony mértékű volt. Csak elszórtan, illetve jellemzően jól automatizálható eljárásokban fordult elő (pl. hivatalos lapok – Közlöny, Értesítő – kiadása). Ennek több oka is volt, amelyek közül a szolgáltatás költségigényét kell megemlíteni, vagy a papír alapú ügyintézés bürokratikus szemlélet beragadását.

A Kormány az elektronikus aláírás közigazgatási használatának elterjedése, elterjesztése érdekében egyrészt az Eat. felhatalmazása alapján a 78/2010. (III. 25.) Korm. rendeletben meghatározta az elektronikus aláírás közigazgatási használatához kapcsolódó követelményeket és az elektronikus kapcsolattartás egyes szabályait.

A Kormány másrészt felismerte, hogy igény van kormányzati szolgáltatóra a piaci helyett. Az új tanúsítványok a tervek szerint olcsóbbak, egységesebbek és szélesebb körben alkalmazhatóak. Az állam a piaci szolgáltatások igénybe vételétől függetleníteni kívánva magát saját, kormányzati hitelesítés-szolgáltatást valósít meg. A kormányzati hitelesítés-szolgáltatás (GOV CA) SZEÜSZ-t tervezetten a NISZ Zrt. fogja nyújtani.

A NISZ Zrt. a piaci szolgáltatók kvázi konkurenciájaként azért jelent meg, hogy a jellemzően állami szervezetek és intézményeik számára az Eat-ban meghatározott szolgáltatások közül a következőket nyújtsa:

a) elektronikus aláírás hitelesítés-szolgáltatás,
b) aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése,
c) időbélyegzés szolgáltatás. Erre a NISZ Zrt-t a Ket. végrehajtási rendelete jelöli ki [84/2012. (IV. 21.) Korm. rendelet az egyes, az elektronikus ügyintézéshez kapcsolódó szervezetek kijelöléséről].

4.2. Szabályozott elektronikus ügyintézési szolgáltatások alkalmazásának elterjedése

Háttér

Az e-közigazgatás érdemi megjelenése a 2001-es kormányzati portálhoz köthető. Ekkor még csak tájékoztatásról, űrlapletöltésről, ügyindításról beszélhettünk. Az érdemi ügyintézés feltételrendszerét a Ket. tette lehetővé, 2005. november 1-től. A Ket. logikája szembe ment a korábbi, papír alapú ügyintézési gondolkodásával, és az elektronikus ügyintézést próbálta bevezetni. 2009 szeptemberéig az elektronikus aláírással próbálták az ügyintézés jogi relevanciáját biztosítani, de ez a kísérlet kudarcba fulladt, az elektronikus aláírás nem terjedt el, a kormányzati szándék ellenére.

Az ügyfélkapu egyenlővé tette a rajta keresztül elektronikusan igénybe vett szolgáltatásokat a papír alapú ügyintézéssel. A 2009. évi szabályozások[9] alapvetően egy centralizált modellt kívántak érvényesíteni az elektronikus közszolgáltatások tekintetében. A Központi Elektronikus Szolgáltató Rendszer és a hozzá kapcsolódó „ügynet-modell" az Elektronikus Kormányzati Gerinchálózaton (EKG), és kapcsolódó centrális szolgáltatások központi üzemeltetésén alapult

Szemléletváltás

A Ket. 2011. évi módosítása jelentősen módosította az elektronikus ügyintézésre vonatkozó szabályokat, és markáns szemléletváltást hozott az elektronikus ügyintézés szabályozásában és a fejlesztési irányok meghatározásában.

Az informatikai rendszer helyett az informatikai megoldással biztosítandó szolgáltatást helyezte a középpontba.

A Ket. és a 2012-ben kihirdetett végrehajtási rendeletei eljárás-centrikus (és lehetőség szerint technológia-független) szabályozást hoztak (szemben a korábbi modellel, amely az informatikai megoldáshoz kívánta igazítani a folyamatokat). A program- és technológia független, illetve decentralizált modellel új logikát szabtak az elektronikus ügyintézésnek, és a kapcsolódó szolgáltatásoknak. Megalkották a szabályozott elektronikus ügyintézési szolgáltatások (SZEÜSZ) rendszerét, amelyek olyan elektronikus szolgáltatások, amelyek működését az állam maga kívánja szabályozni, és ezek egy részét maga szolgáltatja.

A SZEÜSZ rendszer a közigazgatás egységes, összehangolt rendszerként történő működését célozza. Az e-közigazgatás alapvető működéshez szükséges szolgáltatások tartoznak ide, amelyek csak központilag meghatározott szabályok alapján nyújthatók. A szabályozás megteremti a kapcsolattartási csatornák körének szélesítésének lehetőségét, az ügyfelek azonosítási módjait bővíti, szabályrendszere meghatározza az egyes szereplők és informatikai rendszereik együttműködését.

A cél jól definiált funkciókkal rendelkező szolgáltatásokat nyújtani az e-kormányzati alkalmazásokhoz. A szolgáltatások igénybevételével az egyes alkalmazásoknál elkerülhető a funkciók ismételt kifejlesztése és megvalósítása (ez minimum költséghatékonyságot eredményez, de ugyanakkor a szakmai és technikai széttartó megoldások felszámolását is).

A szolgáltató szempontjából két féle szolgáltatás létezik:

a) államilag kötelezően nyújtandó,

b) piaci szereplő által is nyújtható.

A Ket. X. fejezete alapján az alábbi szabályozott elektronikus ügyintézési szolgáltatásokat a Kormány köteles nyújtani:

a) az ügyfél ügyintézési rendelkezésének nyilvántartása,

b) az ügyfél időszaki értesítése az elektronikus ügyintézési cselekményekről,

c) összerendelési nyilvántartás szolgáltatás,

d) azonosítási szolgáltatás természetes személy ügyfelek részére,

e) biztonságos kézbesítési szolgáltatás,

f) elektronikus dokumentumtárolási szolgáltatás,

g) a hatóság nyilatkozattételével kapcsolatos elektronikus igazolás szolgáltatása,

h) elektronikus fizetési és elszámolási rendszer,

i) iratérvényességi nyilvántartás,

j) kormányzati hitelesítés-szolgáltatás,

k) kormányzati elektronikus aláírás ellenőrzési szolgáltatás,

l) központi azonosítási ügynök,

9 2009. *évi* LX. törvény az elektronikus közszolgáltatásról, illetve a végrehajtási rendeletei

m) ÁNYK űrlapbenyújtás támogatási szolgáltatás,
n) azonosításra visszavezetett dokumentumhitelesítés,
o) elektronikus irat hiteles papír alapú irattá alakítása,
p) papír alapú irat átalakítása hiteles elektronikus irattá,
q) iratkezelő rendszerek közötti iratáthelyezés szolgáltatás,
r) központi érkeztetési ügynök,
s) központi kézbesítési ügynök.

Ez a felsorolás nem taxatív, mivel a törvény felhatalmazása alapján kiadott kormányrendelet további, állam által kötelezően nyújtandó szolgáltatást is meghatározhat.

4.3. Interoperabilitás (IOP)

A modulszerűen felépülő e-közigazgatási megoldások csak abban az esetben tölthetik be küldetésüket, ha biztosított az egyes modulok zavartalan, tökéletesen illeszkedő együttműködése.

Interoperabilitás feltételeinek megteremtéséhez elengedhetetlen az állami nyilvántartások egységesítése, a redundancia (adatok többszörös nyilvántartásának) csökkentése, együttműködési képesség növelése (adatátadás és –fogadás, valamint egyértelmű feldolgozásának, vagyis az egyező módon értelmezés képessége), és etalon közhiteles adatbázisok kialakítása, a technikai és tartalmi feltételek megfogalmazása.

A különbözőségek kialakulása szinte már törvényszerű volt, hiszen az informatikai igények az egyes szervezeteknél eltérő időben jelentkeztek (más fejlettségi szint, más technológiai lehetőségek és megoldások), más szervezeteknél, nem összehangoltan, ugyanarra vagy hasonló a problémára más megoldással reagálva. A rosszul vagy nem megfelelően kommunikált igények alapján a informatikai megoldásokat szállítók rossz vagy a saját magának kényelmes megoldást választotta, ami nem ritkán vezetett a szállítófüggőség kialakulásához is.

Az együttműködést a leghatékonyabban szabványok megalkotásával lehet elérni, amelyek rögzítik a minél magasabb szinten történő együttműködés feltételeit.

Az interoperabilitás mind az uniós, mind a hazai e-közigazgatási feladatrendszerben kiemelt prioritású terület, hiszen ez garantálja a szabványosságot és az átjárhatóságot mind államon belül, mind tagállamok adminisztrációi és szolgáltatásai között.

Az eEurope 2005-ben fogalmazódik meg először az Európai Interoperabilitási Keretrendszer (EIF) felállítása, mely ajánlásokat és irányelveket rögzít az e-kormányzati alkalmazásokhoz. [10] [11]

Az interoperabilitás öt szintje az EIF-ben: politikai, jogi, szervezeti, szemantikai, technikai.

Az interoperabilitás a 2014-2020-as uniós költségvetési tervezés során az e-közigazgatási prioritások meghatározásának egyik hívószava is.

Az Európai Unió egyik fő célkitűzése az interoperabilitás, az alapvető elektronikus szolgáltatások határokon átnyúlása, a kölcsönös tájékoztatás. Jelen tananyag készítésekor 11 uniós tagország már képes személyazonosító elektronikus adatokat cserélni egymással, míg akadnak olyan országok is, amelyek fizetési meghagyások és elektronikus számlák cseréjére is képesek.

A magyar jogalkotó az állami és önkormányzati nyilvántartások együttműködésének általános szabályairól szóló 2013. évi CCXX. törvénnyel megalkotta az interoperabilitási keretszabályozást. A törvény kialakítja a nyilvántartók és nyilvántartások közötti interoperabilitás szabályozásához szükséges **egységes fogalomrendszert**, meghatározza a nyilvántartók interoperabilitáshoz kapcsolódó **kötelezettségeit és jogosultságait**, kialakítja a nyilvántartók és a nyilvántartások interoperabilitási szempontú **felügyeletének rendszerét**, létrehozza a nyilvántartások interoperabilitási célú nyilvántartását, a **nyilvántartások regiszterét** és s**tandardizált fogalmak** jegyzékét.

A trendek, tervek szerint a 2014-es év során a döntéshozó kijelöli az elsődleges nyilvántartásokat, majd 2015-ben technikailag is felkészül a napi adatmódosítások kezelésére. 2015 folyamán összekapcsolódnának a közigazgatási nyilvántartások. Ennek eredményeképpen a rendszer 1-2 napos átfutási idővel képes lesz szinkronizálni az adatmódosításokat. Képzeljük egy, hogy milyen jelentős teher manapság egy címváltozás bejelentése az érintett hatóságokhoz, és hogy ez kiváltható azzal, hogy tényleg elegendő ezt egyetlen ügyintézési ponton bejelenteni.

10 EIS – European Interoperability Strategy (Európai Interoperabilitási Stratégia)**:** a kölcsönösen elfogadott, koherens és koordinált interoperabilitási (IOP) kezdeményezések.

11 EIF – European Interoperability Framework (Európai Interoperabilitási Keretrendszer)**:** a közszolgáltatások koncepcionális modellje**;** az IOP öt szintje: politikai, **jogi, szervezeti, szemantikai,** technikai **szintek.**

4.4. ÁROP-2.2.18 „Neten a hivatal” projekt

A „Neten a hivatal” projekt célja egyrészt az e-közigazgatási szolgáltatások ismertségének és használatának növelése a lakosság és a vállalkozások körében, másrészt a közigazgatásban dolgozók e-közigazgatási ismereteinek bővítése. http://netenahivatal.gov.hu/

5. Az elektronikus aláírás

5.1. Az elektronikus aláírás technikai háttere

5.1.1. Bevezetés

Napjaink információs forradalma és a nyomában kiépülő információs társadalom alapvető technológiája az automatizált adatfeldolgozás és az elektronikus adatátvitel. E technológia hallatlan mértékben megnöveli az emberek közötti távolsági kommunikáció hatókörét és kiterjeszti alkalmazásának területét. Mind több írásbeli és verbális üzenetváltás zajlik a világban igen nagy földrajzi távolságban lévő helyek között, s tartalmukat tekintve ezek az üzenetek is nagyon sokfélék. Természetesen nagy súlyt képviselnek közöttük az olyan üzenetek, melyeket egymást jól ismerő felek váltanak, de emellett egyre növekszik az egymással baráti, rokoni vagy egyéb személyes kapcsolatban nem álló felek közötti üzleti vagy igazgatási célú üzenetváltások mennyisége is. Mivel a távközlési eszközök és rendszerek használata egyre nagyobb mértékben beépül a magánélet, a gazdasági kapcsolatok és az igazgatási ügyek intézésének gyakorlatába, természetesen egyre nagyobb az igény az iránt, hogy ez a kommunikáció biztonságos, esetenként akár hiteles és illetéktelen beavatkozástól mindenképpen mentes legyen.

Természetesen az írásbeliség több ezer éves története során az emberiség folyamatosan törekedett arra, hogy a rendelkezésére álló technológia mindenkori szintjén megvalósítsa a távollevő felek közötti hiteles és biztonságos kommunikációt. Az erre szolgáló megoldások jól ismertek: viaszpecsét, bélyegző, saját kezű aláírás illetve ennek tanúkkal történő igazolása, közjegyzői hitelesítés, rejtjelezés és még számos más eszköz.

Korunkban azonban nyilvánvalóan új technológia és – ne habozzunk kimondani – gyökeresen új típusú írásbeliség van kialakulóban, amely természetesen igényli a bizalom megteremtésének és fenntartásának új megoldásait is. Ennek a változásnak a hordereje talán csak az írás és hagyományos írásbeliség több ezer vagy a könyvnyomtatás ötszáz évvel ezelőtti feltalálásával mérhető össze. Az előző technikák esetében a hitelesítési megoldások létrehozására és finomítására kellően hosszú idő állt rendelkezésre. A hiteles elektronikus dokumentumok és hiteles elektronikus kommunikáció eszközeinek és eljárásainak kidolgozása útján azonban még csak az első lépéseket tettük meg. A továbbiakban ennek a folyamatnak az eddig elért eredményeiről lesz szó, különös tekintettel a joghatás kiváltására irányuló dokumentumok hitelesítésének problémájára.

5.1.2. Hiteles okiratokkal kapcsolatos követelmények

A jogrendszer – különösen a magánjog – egyik alapvető rendeltetése az *ügyleti forgalom biztonságának* garantálása. Ez gyakorlatilag elképzelhetetlen megbízható eljárásjogi intézmények, többek között a gyakorlati igényeket jól szolgáló bizonyítási rendszer nélkül. A kereskedelmi tranzakciók egyik lényeges alaki jellegzetessége az írásbeliség, ami a szerződések írásba foglalásától a számviteli műveletek bizonylatokkal történő dokumentálásáig terjed. Ezek a jogi tényeket tartalmazó okiratok valamint a pénzügyi bizonylatok a hagyományos kereskedelmi tevékenység elterjedése során alakultak ki és váltak általánosan alkalmazott bizonyítási eszközökké.

Ideális esetben az okiratok felhasználása az egyéb eszközökön alapuló, gyakran kétes kimenetelű, lassú, nehézkes és költséges bizonyítás lefolytatását – amely tanúk meghallgatásával, szemletárgyak megtekintésével, helyszíni vizsgálatokkal, esetleg szakértői vélemény beszerzésével jár – elkerülhetővé teszi. A gyakorlat a hagyományos okiratok vonatkozásában is olyan kezelési módszer kialakítására törekedett és törekszik ma is, amelynek keretében az irat valamely tény fennállását – vagy éppen fenn nem állását – gyorsan és egyszerűen képes igazolni. E rendeltetésüknek az okiratok akkor tudnak megfelelni, ha kezelésük és felhasználásuk során két feltétel teljesül:

- *Technikai biztonság*: A technológia és az írásbeliség adott fejlettségi szintjét tekintve az okirat maradandó eszközzel és kellően biztonságos technológiával készült. Olyan eszközök felhasználásával, melyek a gyakorlat számára elfogadható áron és megfelelő valószínűséggel biztosítják az illetéktelen beavatkozás kizárását vagy

legalább azok felismerhetőségét. A technikai biztonság mindig arányossági kérdés is. Mérlegelni kell a biztonság megteremtésének költségeit és az elérni kívánt biztonsági szintet. Valójában sohasem beszélhetünk teljes biztonságról. csak a költségek és elvárások arányában definiálható *optimális biztonság* létezik.

- *Valódiság vélelme*: A fenti, kellően erős technikai védelemmel ellátott dokumentum tartalmát úgy kell tekinteni, hogy az helyesen és pontosan fejezi ki a ténybeli valóságot. Ez a vélelem mindaddig fennáll, amíg törvényes eljárás keretében az ellenkezője be nem bizonyosodik.

A hagyományos okiratok körében az aláírás vált mára a hitelesítés elsődleges eszközévé, amit a többi alkalmazott eszköz csak kiegészít és megerősít. Az aláírás általánosan elfogadott céljai az alábbiak:

- *Azonosíthatóság:* az aláíró személyének és magának az okiratnak az egyediesítése.
- *Hitelesség:* annak igazolása, hogy az okirat valóban attól származik, akit kibocsátójaként a szöveg megnevez.
- *Sértetlenség:* az irat tartalmi integritásának bizonyítása. Védelmet jelent az aláírás elhelyezését követően eszközölt módosítások ellen.
- *Letagadhatatlanság:* a nyilatkozattétel tényének rögzítése, megerősítése.

Az elektronikus kereskedelem és az elektronikus közigazgatás egyre szélesebb körben terjedő szolgáltatásainak köszönhetően gyorsan felmerült az igény a hiteles elektronikus okiratok alkalmazása iránt annak érdekében, hogy ebben a körben is teljesülhessen az ügyleti forgalom biztonságának követelménye, azaz lehetővé váljon a hiteles elektronikus nyilatkozattétel. Korábban az elektronikus okiratok esetében gyakorlatilag nem lehetett a fenti feltételeket kielégíteni. Speciális megoldások nélkül az elektronikus iratok világából minduntalan vissza kellett térnünk a hagyományos hitelesítés eszközeihez és megoldásaihoz. A gyakorlatban ez azt jelentette, hogy azokat az elektronikus úton létrehozott dokumentumokat, amelyek joghatás kiváltására irányultak ki kellett nyomtatni és ezután a hagyományos módszerekkel – aláírással, bélyegzővel – hitelesíteni és a továbbiakban is manuális módszerekkel feldolgozni. Ez nemcsak felesleges párhuzamosságot okoz a dokumentumkezelésben, hanem a papír nélküli iroda és az ettől remélt gyorsabb és hatékonyabb ügyintézés kialakítását is kizárja.

A ma rendelkezésünkre álló hitelesítési technológia az elektronikus aláírás. Az elektronikus aláírás lehetővé teszi, hogy az elektronikus iratok teljes kezelési ciklusuk során megmaradjanak elektronikus formában. Az elektronikus aláírás a kapcsolódó eljárásokkal együtt alkalmas arra, hogy biztosítsa az aláíró egyértelmű azonosíthatóságát, az aláírás tényének letagadhatatlanságát, továbbá azt, hogy az elektronikus úton aláírt elektronikus irat tartalma nem változott meg azóta, hogy az a személy, akihez az elektronikus aláírás tartozik, az aláírást „elhelyezte" az iraton. Azon technológia biztonságosságának, amellyel az elektronikus aláírást előállítják, és hozzáfűzik az irathoz, jogi relevanciája is van. Ennek ellenére a szabályozás legfelső szintjének az alkalmazott technológiától függetlennek kell lennie, mivel az alkalmazott technológiák gyorsan változnak. A jogi szabályozás kidolgozásakor azonban mégsem lehet teljesen figyelmen kívül hagyni a jelenleg elfogadott technikai megoldásokból eredő követelményeket. Az elvileg rendelkezésre álló műszaki illetve matematikai megoldások közül az ún. *nyilvános kulcsú eljárásokra* alapozott elektronikus aláírás terjedt el.

5.1.3. Rejtjelezés és elektronikus aláírás

A nyilvános kulcsú hitelesítési eljárások a kriptográfián, azaz a rejtett tartalmú üzenetváltások technológiáján alapulnak. A rejtjelezés célja az, hogy a bizalmas üzenetet úgy juttassuk célba, hogy annak tartalmához csak a címzett férhessen hozzá, és a *címzett* meggyőződhessen a *feladó* kilétéről. Ugyanakkor a rejtjelezés során feltételezni kell azt is, hogy a címzetten, és a feladón kívül létezik egy harmadik személy, a *lehallgató*, aki

- megpróbál illetéktelenül hozzáférni az üzenet tartalmához, és/vagy
- a feladó nevében hamis üzenetet próbál küldeni a címzettnek.

A rejtjelezést a diplomáciai, a védelmi, katonai, a bizalmas természetű üzleti és a magáncélú kommunikációban egyaránt régóta – valójában több ezer éve – alkalmazzák. E hosszú idő alatt a kriptográfiai algoritmusoknak két nagy osztálya alakult ki, a *szimmetrikus és az aszimmetrikus eljárások*.

5.1.3.1. Szimmetrikus rejtjelezés

A szimmetrikus eljárások lényegi elemét képezi az a körülmény, hogy a feladó és a címzett ismernek valamilyen titkos információt, mindketten ugyanazt, amelyet a lehallgató nem ismer. Ennek a titkos információnak a birtokában képes a feladó a *rejtjelezett üzenetet létrehozni a nyílt szövegből*, a címzett pedig dekódolni tudja azt. A lehallgató, a titkos információ hiányában sem megfejteni nem tudja a rejtjelezett szöveget, sem arra nem képes, hogy maga hozzon létre és küldjön hamis tartalmú rejtjelezett üzenetet. Ennek alapján a címzett biztos lehet benne, hogy az üzenet valóban az

általa ismert feladótól származik. A titkos információ általában a rejtjelezéshez használt algoritmus egyik paramétere, a *kódoló/dekódoló kulcs*.

Bár a szimmetrikus kulcsú rejtjelezésre hosszú évszázadok során nagyon jó módszereket dolgoztak ki, vannak kétségtelen hátrányai is. Az első számú gyakorlati problémát az jelenti, hogy a titkos kulcsban meg kell állapodnia a címzettnek és a feladónak. Ez egy olyan kommunikációs művelet, amelyet kellően biztonságos módon lebonyolítani, s ennek a megszervezése gyakran komoly nehézségeket támaszt. A titkos kulcsot olyan módon kell a feladónak és a címzettnek egymással megosztani, hogy eközben a lehallgató ne tudja azt megszerezni. Ehhez olyan kommunikációs csatornát kell használniuk, amely biztonságos, nem lehallgatható. Ennek a csatornának a használata azonban valamilyen értelemben korlátozott – nagyon drága vagy nagyon lassú – ellenkező esetben ugyanis nem kellene rejtjelezést használni, hanem ezen a csatornán lehetne az üzenetet küldeni.

Ugyancsak a kulcskezeléssel kapcsolatos probléma, hogy a rejtjelezett üzenetváltásban résztvevő minden kommunikáló párnak – minden egyes feladónak minden egyes címzettel – külön-külön meg kell egyeznie egy, vagy több titkos kulcsban. Ez már viszonylag kis számú pár esetén is sok bizalmasan megőrzendő kulcsot, következésképpen komoly szervezési és adminisztrációs feladatot jelent. Szabatosan kifejtve ugyanis n partner esetén, ha mindenki mindenkivel kommunikálni fog, akkor $n(n-1)/2$ kulcsban kell megegyezni. azaz ha $n=10$, akkor a szükséges kulcsok száma $10*9/2=45$.

További igen lényeges problémája a szimmetrikus kulcsú rejtjelezési algoritmusoknak, hogy bármelyik ismert és gyakorlatban alkalmazott megoldásnál kellően hosszú, vagy elegendően nagyszámú üzenet alapján a kulcs – elsősorban statisztikai alapon – megfejthető, s a továbbiakban ennek felhasználása már nem biztonságos. Emiatt a kulcsokat gyakran cserélni kell, ami tovább fokozza a kulcskezeléssel kapcsolatos adminisztrációs és szervezési nehézségeket és az ebben rejlő biztonsági kockázatokat is.

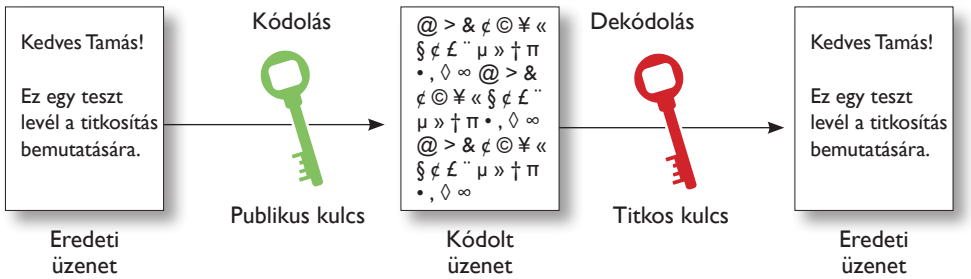
A fenti problémák az aszimmetrikus rejtjelezési módszerekkel lényegesen mérsékelhetők.

5.1.3.2. Aszimmetrikus rejtjelezés

Az aszimmetrikus rejtjelezés története sokkal rövidebb, mint az előző módszeré. Az algoritmust elsőként James H. *Ellis*, Clifford *Cocks* és Malcolm *Williamson*, a *Government Communications Headquarters* (GCHQ) munkatársai dolgozták ki az 1970-es évek elején, eredményeiket azonban 1997-ig nem ismerhette meg a világ, s így az nem is hasznosulhatott. Az eljárás felfedezésének pillanatától államtitkot képezett, ugyanis a GCHQ a brit titkosszolgálatok egyike. A sors furcsa fintora, hogy ezúttal az elsőség nem garantálta a felfedezők számára a szakmai dicsőséget és a világhírt.

A titokban tartott eljárást újra fel kellett fedezni. Ez a néhány évvel későbbi eredmény *Diffie-Hellmann kulcscsere eljárásként* vált ismertté, miután 1976-ban két amerikai matematikus, Whitfield Diffie és Martin Hellman már civil felhasználásra szánt módszerként nyilvánosságra hozta. Ez az első gyakorlatban is alkalmazható megoldás olyan biztonságos rejtjelkulcs megosztási rendszerre, amelyet nyilvános célú – tehát lehallgatás ellen nem védett – kommunikációs csatornán keresztül valósítanak meg.

Az eljárás a kódolás, vagyis a rejtjel létrehozásának műveletét elválasztja a dekódolástól, és olyan algoritmust használ, ahol a kódoláshoz használt kulcs nemcsak, hogy nem azonos a dekódoláshoz használt kulccsal, hanem a kulcsok nem is határozhatók meg egymásból. Egy ilyen algoritmussal a kódoló kulcsot nyilvánossá téve bárki rejtjelezett üzenetet tud küldeni a címzettnek, akihez az a nyilvános kulcs tartozik, de dekódolni csak a címzett tudja, amennyiben a privát kulcsot csak ő maga ismeri.



1. ábra Kétkulcsos kriptográfia alkalmazása rejtjelezett üzenetváltásra

A kulcskezelés adminisztrációja is átalakul és egyszerűsödik egy ilyen rendszerben. Ezt a módszert használva ugyanis létrehozható egy olyan nyilvánosan hozzáférhető kódkönyv, amiben mindenkinek szerepel a nyilvános kulcsa, és így a kódkönyvben szereplők bármelyikének tud bárki levelet küldeni anélkül, hogy előtte a partnerrel saját titkos kulcsban megállapodtak volna. Természetesen a kódkönyvnek megbízhatónak kell lennie.

A Diffie-Hellmann eljárás csak a kulcskezelés logikai sémáját képezi. A kívánt tulajdonságokkal rendelkező kulcsokat előállító szabatos és megbízható matematikai eljárást csak két évvel később, 1978-ban publikálták. Az *RSA algoritmus*, amely az új eredményt bejelentő három amerikai matematikus, Ronald *Rivest*, Ron *Shamir* és Len *Adleman* nevének kezdőbetűit őrzi, valójában CliffordCocks módszerének általánosítása.

5.1.4. Elektronikus aláírás PKI technológiával

A ma használt elektronikus aláírási rendszerek az aszimmetrikus rejtjelezési technológián alapulnak. A felhasználás célja azonban meghatározó a felhasználás módja tekintetében is. Az elektronikus aláírásnak az a feladata, hogy a dokumentumot hitelesítse, nem pedig az, hogy illetéktelenek számára hozzáférhetetlenné tegye. Az eltérő célok pedig azt eredményezik, hogy ugyanazt az apparátust más módon használjuk fel. A legfontosabb különbség az aláírási folyamat eredményén azonnal észlelhető is: az elektronikus aláírással ellátott dokumentum továbbra is nyílt hozzáférésű marad, tartalmaz azonban egy olyan adategységet, amely biztosítja és tanúsítja a hitelességét, a sértetlenségét és a letagadhatatlanságát.

Az aláírási rendszerben is jelen van az aszimmetrikus rejtjelezést lehetővé tevő kulcspár, de a rendszernek számos további eleme is van, melyek a hitelességet szolgálják. A technológia megfelelő működését különböző eljárásrendek és szervezetek biztosítják, amelyeket együttesen *nyilvános kulcsú infrastruktúrának* (*Public Key Infrastructure*.**PKI**) nevezünk.

A PKI főbb elemei:

- az aláíró és az aláírást ellenőrző felek,
- a rendszert működtető megbízható harmadik fél (TrustedThirdParty, **TTP**), azaz a *hitelesítés-szolgáltató*,
- a már ismert kriptográfiai nyilvános/titkos *kulcspár*,
- a kulcspár és az aláíró összetartozását bizonyító *tanúsítvány*.

5.1.4.1. Az aláíró és az aláírást ellenőrző felek

Az egymással elektronikus úton kommunikáló és dokumentumokat cserélő felek természetesen alapvető elemei az elektronikus aláírási rendszernek. Aláíró fél az, aki a kulcspárral rendelkezik, akinek javára elektronikus tanúsítvány került kiállításra s kriptográfiai privát kulcsának felhasználásával készíti el az elektronikus úton létrehozott dokumentumhoz tartozó elektronikus aláírást. Az elektronikus aláírással ellátott dokumentum címzettje ellenőrzi az aláírás, ezen keresztül pedig a kapott dokumentum hitelességét, az aláíró személyazonosságát. Az ellenőrzés elvégzéséhez az aláíró nyilvános kulcsát használhatja fel.

5.1.4.2. A hitelesítés-szolgáltató

A *hitelesítés-szolgáltató* olyan, a tanúsítvány kibocsátásra specializálódott szervezet, amely arra vállalkozik, hogy egy adott földrajzi területen – tipikusan egy országban – működő aláírókat az adott terület jogi, közigazgatási, gazdasági rendszerének ismeretében felépített eljárásrend alkalmazásával hitelt érdemlően azonosítsa, és ezek alapján igazolja akár az egész világ felé létezésüket és adataik valódiságát.

A hitelesítés-szolgáltató köteles az aláírók nyilvános kulcsait nyilvánosan kezelni és kérelemre rendelkezésre bocsátani, az aláíró ügyfelekről és a kiadott kulcsokról megbízható, magas szintű technikai védelemmel ellátott nyilvántartást vezetni, s a kulcsot az aláíró kérésére, valamint bíróság, vagy más erre jogosult szerv határozata alapján érvényteleníteni, és a visszavont, érvénytelenített kulcsokról ugyancsak nyilvántartást vezetni.

A rendszerben kiemelt jelentőségű a hitelesítés-szolgáltató magánkulcsának védelme, mivel ezzel az eszközzel fogja a szolgáltató az általa kibocsátott tanúsítványokat hitelesíteni, azaz elektronikusan aláírni azokat. A hitelesítés-szolgáltató létezését önmaga igazolja önmaga számára kibocsátott tanúsítvánnyal. Az ehhez az úgynevezett *főtanúsítványhoz* kapcsolódó bizalmat a szervezet – a pénzintézetekhez hasonlóan – hagyományos üzletpolitikai eszközökkel teremti meg. Ezek közül a legfontosabbak a következők:

- átlátható, stabil, erős pénzügyi hátterű működés,
- büntetlen előéletű, magas szakmai felkészültségű vezetők és munkatársak,
- minőségvédelmi auditok elvégeztetése, ezek eredményének nyilvánosságra hozatala,

- bekerülés a nemzetközi hitelesítés-szolgáltatói listára,
- felelősségbiztosítás,
- pénzügyi garancia nyújtása a tanúsítványokkal történő esetleges visszaélésből eredő kár megtérítésére.

5.1.4.3. A kulcspár

Az elektronikus aláírásnál alkalmazott kriptográfiai magánkulcsok és nyilvános kulcsok olyan digitális jelsorozatok, amelyek megfelelő számítógép-programokkal kezelhetőek. A magánkulcsot az aláírónak titokban kell tartania, megfelelő intézkedésekkel védenie kell az illetéktelen felhasználás, eltulajdonítás ellen. Ha a magánkulcs titkossága megszűnik, akkor az eljárás garanciái (aláírt irat hitelessége, az aláíró azonosítása) megszűnnek. A megfelelően gondos kezelés a kulcstulajdonos felelőssége éppúgy, mint a bankkártyák esetében. A kulcs sokféle fizikai adathordozón tárolható. az aláíró számítógépén található rejtjelezett adatállományban, flash-memórián, önálló vagy mobiltelefonba épített chipkártyán. A nyilvános kulcs bárki által hozzáférhető, sőt kívánatos, hogy minél szélesebb körben megismerhető legyen (pl. a hitelesítés-szolgáltatónál vagy címtár-szolgáltatónál), ugyanis az aláíró a nyilvános kulcshoz kapcsolt adatok alapján azonosítható.

A kulcspár létrehozásakor megbízható matematikai algoritmusok biztosítják azt, hogy a nyilvános kulcs ismeretében gyakorlatilag nem lehet visszafejteni a hozzá tartozó magánkulcsot, illetve az aláírást nem lehet a nyilvános kulcs ismeretében hamisítani. A nyilvános kulcs ismeretében egy aláírásról gyakorlatilag egyértelműen megállapítható, hogy a hozzá tartozó magánkulcs felhasználásával készült-e vagy sem.

5.1.4.4. A tanúsítvány

A rendszer működésének egyik sarokköve, hogy megbízható harmadik fél vállaljon garanciát az egész külvilág felé arra, hogy adott kulcspár adott aláíróhoz tartozik. Erre szolgál a *tanúsítvány*, egy olyan elektronikus dokumentum, amely tartalmazza az aláíró szokásos azonosító adatait – név, lakcím illetve székhely, különböző nyilvántartási azonosító számok – és az aláírás ellenőrzéséhez használható nyilvános kulcsát. A tanúsítványban szereplő azonosító adatokat a hitelesítés-szolgáltató – hagyományos okiratok alapján – ellenőrzi, majd az ennek alapján összeállított elektronikus dokumentumot saját elektronikus aláírásával hitelesíti.

A hitelesítés-szolgáltató működésének és a hiteles tanúsítványnak köszönhetően az elektronikus úton aláírt iratok cseréje során nincs szükség a küldő és címzett személyes találkozására. Az elektronikus tanúsítvány hitelesíti az aláíró személyét és az elektronikus úton aláírt üzenetet, iratot, a címzett pedig egyértelműen meggyőződhet azok hitelességéről.

5.1.5. Az elektronikus aláírás működése

A nyilvános kulcsú eljárásokra alapozott elektronikus aláírás fő tulajdonságai:

- egy adott elektronikus aláírásnak kizárólag egy tulajdonosa lehet,
- lehetővé teszi az aláíró személyének egyértelmű meghatározását,
- az aláírónak kizárólagos lehetősége van aláírásának készítésére,
- egyértelműen megállapítható az elektronikus úton aláírt elektronikus irat bármely, az aláírást követő véletlen vagy szándékos módosulása,
- további technológiai elemek, illetve szolgáltatások alkalmazásával az aláírás hiteles időpontja is csatolható az elektronikus úton aláírt irathoz.

Az elektronikus aláírás működése két lépésben valósul meg. Az első az aláírás létrehozása, a második pedig az aláírás ellenőrzése.

5.1.5.1. Az elektronikus aláírás létrehozása

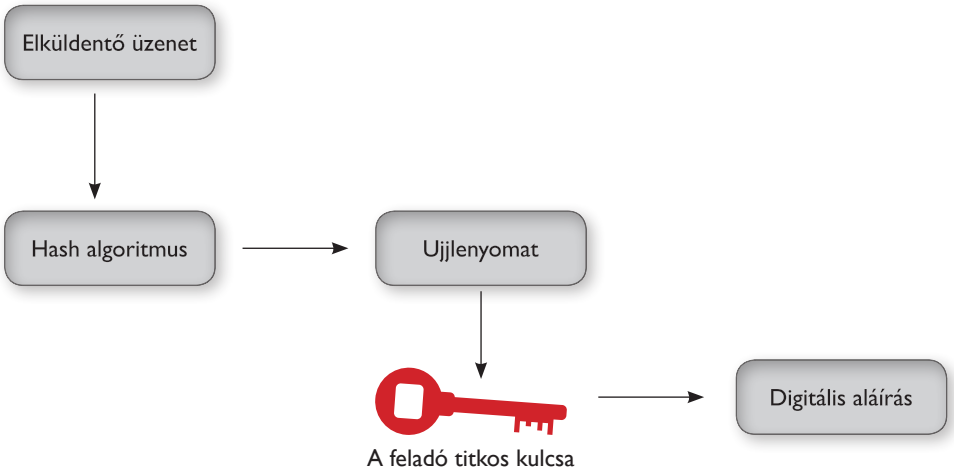
Az aláírás hitelesítő szerepe csak akkor valósulhat meg, ha a címzett kétséget kizáróan meggyőződhet arról, hogy az eredeti dokumentum jutott-e el hozzá, vagy annak egy módosult, manipulált változata. Problémát okoz, hogy külön védekezés nélkül a digitálisan tárolt adatoknál a változtatás nem hagy nyomot. A megoldást egy *digitális lenyomat* készítése és csatolása adhatja meg. A lenyomatkészítés az egyirányú hash-függvényen alapul.

5.1.5.2. Lenyomat képzése hash-eljárással

A hash-függvény lényegileg egy olyan matematikai transzformáció, amely egy tetszőleges méretű – de véges – dokumentumból olyan fix hosszúságú bitsorozatot (digitális lenyomatot) állít elő, amely egyértelműen jellemző az adott szövegre. Eszerint tehát egy adott dokumentum lenyomata – valahányszor csak végrehajtjuk a transzformációt – mindig bitről bitre ugyanaz lesz. A lenyomat igen rövid, előre meghatározott hosszúságú bitsorozat. A jelenleg elterjedt szabványos eljárások – az alkalmazott algoritmustól függően – tipikusan 128 vagy 160 bites lenyomatokat eredményeznek. Ebből következik, hogy az egymástól különböző lenyomatot produkáló dokumentumok száma 2^{128} illetve 2^{160} lehet, ami a gyakorlat számára megnyugtató nagyságrend. E szerint ugyanis annak valószínűsége, hogy két dokumentum esetén a transzformáció azonos eredményt, azonos lenyomatot ad, $1:2^{128}$, illetve $1:2^{160}$.

A hash-transzformáció fő tulajdonságai az egyirányúság, az ütközésmentesség és az ún. lavinahatás:

- *Egyirányúság:* A lenyomatból az eredeti dokumentum nem állítható vissza és annak tartalmára sem lehet következtetni. Gyakorlatilag kizárt egy adott lenyomathoz olyan dokumentumot létrehozni illetve hozzárendelni, amelyik a transzformáció végrehajtásakor ugyanazt a lenyomatot produkálja.
- *Ütközésmentesség:* Gyakorlatilag lehetetlen két olyan dokumentumot konstruálni, amelyek azonos lenyomatot eredményeznek.
- *Lavinahatás:* Ha egy bitet megváltoztatunk a dokumentumban, akkor a lenyomat képe a bitek körülbelül felében különbözni fog.



2. ábra Kétkulcsos kriptográfia alkalmazása elektronikus aláírás létrehozására

5.1.5.1.1. A lenyomat rejtjelezése

A dokumentumból képzett szabványos hosszúságú digitális lenyomatot a következő lépésben az aláíró saját kriptográfiai magánkulcsával kódolja. Az ennek eredményeként előállt rejtjelezett adathalmaz maga az elektronikus aláírás, amely az irathoz csatolva kerül továbbításra, vagy tárolásra. Ugyancsak tárolásra illetve továbbításra kerülhet – az aláíró tanúsítványának részeként – az aláírás ellenőrzésére szolgáló nyilvános kulcs is.

5.1.5.2. Az aláírás ellenőrzése

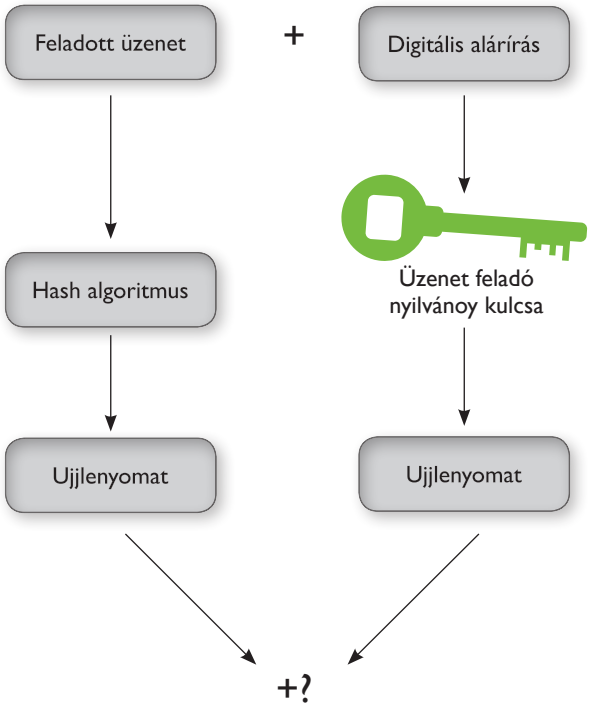
Az elektronikus aláírás ellenőrzését tipikusan az üzenet címzettje, a dokumentum jogosult felhasználója végzi. A címzett az ellenőrzés során – esetenként a hitelesítés-szolgáltató segítségével – meggyőződhet az elektronikus úton aláírt irat hitelességéről, és az aláíró személyéről. Az aláírás ellenőrzését, csakúgy, mint az aláírás létrehozását, e feladatra specializált számítógép-programok végzik el. Mind az aláíró, mind a címzett csak kezdeményezi a műveletek elvégzését, a számítási műveleteket a szoftver végzi el, majd a folyamat végén közérthető, felhasználóbarát formában közli az eredményt.

Aláírás ellenőrzésének lépései:

1. A program – a hash-függvény alkalmazásával – ismét létrehozza a dokumentum digitális lenyomatát.
2. A szoftver a dokumentumhoz csatolt digitális aláírást a nyilvános kulcs felhasználásával dekódolja, amelyből szintén egy digitális lenyomat képződik.
3. Az így előállított két digitális lenyomatot a rendszer bitről bitre összehasonlítja. Ha a lenyomatok azonosak, igen nagy valószínűséggel állítható, hogy az elektronikus úton aláírt irat tartalma nem változott továbbítása illetve tárolása során és az adott nyilvános kulcshoz tartozó magánkulccsal készült a digitális aláírás.

A fenti lépések mellőzhetetlenek az aláírás érvényességének megállapításához. A további két ellenőrzési lépésre csak akkor kerül sor, ha az aláíró személyazonosságát vagy a tanúsítvány érvényességét illetően kétség merül fel.

1. Az aláíró személyét azonosító adatokat a nyilvános kulcs ismeretében a hitelesítés-szolgáltató kérelemre megadja és tanúsítja, és azt is igazolja, hogy az adott kulcs érvényes-e vagy sem (lejárt, ellopták stb.).
2. Az aláíró tanúsítványának hitelessége szintén ellenőrizhető az azt kiállító hitelesítés-szolgáltató aláírásának a közismert, könnyen hozzáférhető nyilvános kulcsa alapján.



3. ábra Kétkulcsos kriptográfia alkalmazása elektronikus aláírás ellenőrzésére

5.1.6. Az elektronikus aláírás és a rejtjelezés felhasználási területei

Az elektronikus aláírásnak és a digitális rejtjelezési technikának számos alkalmazási területe van. Ezek köre egyre bővül, így e helyen csak néhány fontos és jellemző területet emelünk ki:[12]

- Elektronikus levelezés biztonságossá tétele az üzenet aláírásával és rejtjelezésével.
- Biztonságos internetes szolgáltatások, elsősorban elektronikus kereskedelmi illetve elektronikus közigazgatási szolgáltatások nyújtása a szolgáltató és az igénybe vevő megbízható azonosításával és a szolgáltatott adatok hitelességének, sérthetetlenségének, letagadhatatlanságának és bizalmasságának biztosításával.
- Zárt internet-közösségek létrehozása (orvosi konzílium, ügyvédi fórum, valamely előfizetett szolgáltatás) a felhasználók megbízható azonosításával és a kommunikáció bizalmassá tételével.
- Zárt kommunikációs csoportok kialakítása bármilyen kommunikációs felületen (mobiltelefon, Internet, LAN, WAN hálózatok) a csoport tagjainak azonosításával és az adatforgalom aláírásával, titkosításával.

12 Almási János: Elektronikus aláírás és társai. Sans Serif, Budapest. 2002. 65-66. o.

- Biztonságos elektronikus fizetési módszerek kialakítása a felhasználó azonosításával és a készpénz-helyettesítő fizetési eszköz (tipikusan kártya) adatainak titkosításával, akár Interneten, akár mobiltelefonon keresztül.
- Elektronikus pénztárca és elektronikus pénz megoldások kis összegű vásárlások (micropayment) céljára a „pénz"-kibocsátó általi elektronikus aláírással.
- Biztonságos archiválás és adatbázis-kezelés, az eltárolt információ elektronikus aláírásával és/vagy titkosításával.
- Felhasználók biztonságos azonosítása és beléptetése informatikai eszközök által védett rendszerekbe vagy helyiségekbe.
- Szoftverek származásának igazolása és sértetlenségének biztosítása a programkód aláírásával.
- Adatbázis vagy egyéb digitálisan tárolt tartalom – esetleg audiovizuális tartalom (fotó, hang- vagy videofelvétel) – létezésének, származásának igazolása és sértetlenségének biztosítása a fájl aláírásával.
- Különböző elektronikus okiratokkal kapcsolatos szolgáltatások.

5.2. Az elektronikus aláírás szabályozása

Az elektronikus aláírás szabályozási kereteit egyrészt az elektronikus aláírásról szóló 2001. évi XXXV. törvény (Eat.), másrészt a polgári perrendtartásról szóló 1952. évi III. törvény (Pp.) vonatkozó szakaszai alkotják.

5.2.1. Alapfogalmak

Az Eat. több alapvető fogalom-meghatározást tartalmaz.

A törvény értelmében *elektronikus dokumentum*: elektronikus eszköz útján értelmezhető adategyüttes – azaznemcsak írott dokumentum, hanem állókép, mozgókép, hangfelvétel, stb. is lehet elektronikus dokumentum (természetesen digitális formátum esetén), sőt, akár szoftver is, így ezek elektronikus aláírása is elképzelhető.

Az *elektronikus aláírás* a törvény szerint az elektronikusan aláírt elektronikus dokumentumhoz azonosítás céljából logikailag hozzárendelt vagy azzal elválaszthatatlanul összekapcsolt elektronikus adat.

Az *aláírás-létrehozó adat*: olyan egyedi adat (jellemzően kriptográfiai magánkulcs), melyet az aláíró az elektronikus aláírás létrehozásához használ.

Aláírás-ellenőrző adat: olyan egyedi adat (jellemzően kriptográfiai nyilvános kulcs), melyet az elektronikusan aláírt elektronikus dokumentumot megismerő személy az elektronikus aláírás ellenőrzésére használ.

Aláírás-létrehozó eszköz: olyan hardver, illetve szoftver eszköz, melynek segítségével az aláíró az aláírás-létrehozó adatok felhasználásával az elektronikus aláírást létrehozza.

Aláíró: az a természetes személy, aki az aláírás-létrehozó eszközt birtokolja és a saját vagy más személy nevében aláírásra jogosult.

5.2.2. Az elektronikus aláírás típusai

A törvény három különböző biztonsági szintű elektronikus aláírást különböztet meg: (1) az egyszerű elektronikus aláírást, (2) a fokozott biztonságú elektronikus aláírást és (3) a minősített elektronikus aláírást.

1. *Egyszerű elektronikus aláírás*, amelyhez különösebb joghatások nem kapcsolódnak. Ilyen pl. az email vagy a dokumentum végére begépelt név.

   Ez nem alkalmas arra, hogy a dokumentum szerzőjének személyéről vagy a dokumentum tartalmáról hiteles információt szolgáltasson.

2. *Fokozott biztonságú elektronikus aláírás*: olyan elektronikus aláírás, amely
   a) alkalmas az aláíró azonosítására,
   b) egyedülállóan az aláíróhoz köthető,
   c) olyan eszközökkel hozták létre, amelyek kizárólag az aláíró befolyása alatt állnak, és
   d) a dokumentum tartalmához olyan módon kapcsolódik, hogy minden – az aláírás elhelyezését követően a dokumentumon tett – módosítás érzékelhető.

A törvény tehát funkcionális követelményeket támaszt az aláírással szemben, és nem szól e követelmények technikai, eljárási és szervezeti megvalósításáról. Mindazok a technikai, eljárási és szervezeti megoldások felhasználhatók, amelyek kielégítik a fokozott biztonságú elektronikus aláírással szembeni követelményeket. Az első részben vázolt technikai folyamatok eredményeként létrejövő elektronikus aláírás ezeket a követelményeket teljesíti.

3. *Minősített elektronikus aláírás*: olyan – fokozott biztonságú – elektronikus aláírás, amelyet az aláíró biztonságos aláírás-létrehozó eszközzel hozott létre, és amelynek hitelesítése céljából minősített tanúsítványt bocsátottak ki.

A minősített elektronikus aláírás esetében tehát nem az aláírás funkciói, hanem annak biztonsági feltételei változnak.(A funkciók ugyanazok, hiszen ez a fokozott biztonságú elektronikus aláírás egyik fajtája).

5.2.3. Az elektronikus aláírás joghatása

Az elektronikus aláírás egyes típusaihoz fűződő jogkövetkezmények a biztonsági szintjüktől függően változnak. Mivel az elektronikus aláírás önmagában csak egy értelmezhetetlen számsor, ezért az elektronikus aláírással ellátott dokumentum kinyomtatott változatához természetesen nem fűződnek az elektronikus változatra vonatkozó jogkövetkezmények.

5.2.3.1. **Közös szabályok**

Az azonosítás biztonságától függetlenül nem lehet az elektronikus aláírás, illetve az elektronikus dokumentum elfogadását megtagadni, jognyilatkozat tételére, illetve joghatás kiváltására való alkalmasságát kétségbe vonni kizárólag amiatt, hogy az aláírás, illetve a dokumentum elektronikus formában létezik. Különösen nem tagadható meg az ilyen aláírás és dokumentum bizonyítási eszközként történő alkalmazása, amivel kapcsolatban az eljáró bíróságnak vagy hatóságnak egyébként is szabad mérlegelési lehetősége van. E rendelkezésével az Eat. megteremti az *elektronikus írásbeliség* törvényi alapját.

Személyes jellegük miatt az öröklési jogi és családjogi jogviszonyokban nem lehet a hagyományos (írott) dokumentumokat mellőzve, kizárólag elektronikus aláírást felhasználni.

Szintén korlátozott az elektronikus dokumentumok és aláírások felhasználásának lehetősége a bírósági eljárásokban és a hatósági jogviszonyokban, de a közigazgatásban egyre inkább nő az elektronikus ügyintézés lehetősége.

5.2.3.2. A fokozott biztonságú elektronikus aláírás joghatásai

Az Eat. a fokozott biztonságú elektronikus aláíráshoz azt a jogkövetkezményt fűzi, hogy az ilyen aláírással ellátott elektronikus irat írásba foglalt iratnak minősül, alkalmazásával elektronikus úton is érvényesen megtehetők az írásbeli alakhoz kötött nyilatkozatok.

5.2.3.3. A minősített elektronikus aláírás jogkövetkezményei

Kimondja a törvény, hogy ha az elektronikus dokumentumon minősített elektronikus aláírás szerepel – és az aláírás ellenőrzésének eredményéből más nem következik –, vélelmezni kell, hogy a dokumentum tartalma az aláírás óta nem változott. Az Eat. tehát ebben az esetben felállítja a hamisítatlanság vélelmét.

A minősített elektronikus aláírással ellátott elektronikus dokumentum a Pp. szerint teljes bizonyító erejű magánokiratnak minősül, azaz az ellenkező bebizonyításáig teljes bizonyítékul szolgál arra, hogy kiállítója az abban foglalt nyilatkozatot megtette, illetőleg elfogadta, vagy magára kötelezőnek ismerte el. A magánokirat valódiságát csak akkor kell bizonyítani, ha azt az ellenfél kétségbe vonja, vagy a valódiság bizonyítását a bíróság szükségesnek találja.

Ugyancsak teljes bizonyító erejű magánokirat az elektronikus ügyvédi ellenjegyzéssel ellátott elektronikus okirat.

5.3. A hitelesítés-szolgáltató szerepe és jogállása, a tanúsítvány

5.3.1. Hitelesítés

A hitelesítés az az eljárás, amelynek során a hitelesítő a kriptográfiai kulcspárt – vagy egyéb aláírás-létrehozó és -ellenőrző eszközt – biztonságosan hozzárendeli egy meghatározott és azonosított személyhez. A hozzárendelésről kiállított igazolás a tanúsítvány. Elektronikus aláírás esetén a hitelesítést az ún. hitelesítés-szolgáltató végzi.

Hitelesítésre a saját kezű aláírás vonatkozásában is szükség van: léteznie kell egy olyan dokumentumnak, amely a saját kezű aláírást külső fél által hitelesítetten az aláíróhoz, annak arcképéhez rendeli. A személyi okmány egyrészt az arckép feltüntetésével azonosítja az okmány tulajdonosát, másrészt az okmányon szereplő aláírást is hozzárendeli az okmány tulajdonosához. Az azonosítás és a hozzárendelés hitelességét, harmadik személy általi kétségbe vonhatatlanságát az okmány (igazolvány) kiállítójának egyértelmű megbízhatósága adja. (Más esetben pl.: az aláírásnak tanúk,

közjegyző vagy ügyvéd általi hitelesítése során a tanúk, a közjegyző vagy az ügyvéd aláírása bizonyítja azt, hogy az aláírás valóban az aláírótól származik).

Az elektronikus aláírás hitelesítésével kapcsolatban egységesen az a szabályozási megoldás alakult ki, hogy a hitelesítés nem (állami) hatósági feladat, hanem piaci szolgáltatás, a hitelesítők nem közigazgatási szervek, hanem vállalkozások. A hitelesítés-szolgáltató „megbízható harmadik félként" bekapcsolódik a felek közötti jogviszonyba: az aláíró által fizetett díj ellenében tanúsítja az aláíró személyazonosságát, és ezért felelősséggel tartozik.

A hitelesítés során a hitelesítés-szolgáltató azonosítja az igénylő személyét (gyakorlatilag személyes megjelenés útján, személyazonosító igazolvánnyal azonosítja) és ez alapján tanúsítványt bocsát ki. A hitelesítés-szolgáltató felelős azért, hogy a tanúsítvány a valóságnak megfelelő adatokat tartalmazzon.

5.3.2. A tanúsítvány

5.3.2.1. A tanúsítvány fogalma

A tanúsítvány a hitelesítés-szolgáltató által kibocsátott igazolás, amely az aláírás-ellenőrző adatot (nyilvános kulcsot) egy meghatározott személyhez kapcsolja, és igazolja e személy személyazonosságát vagy valamely más tény fennállását, ideértve a hatósági (hivatali) jelleget is.

A tanúsítvány gyakorlatilag a hitelesítés-szolgáltató elektronikus aláírásával aláírt elektronikus dokumentum, amely tartalmazza az aláíró aláírás-ellenőrző adatát (nyilvános kulcsát) és egyéb – az aláíróra, a hitelesítés-szolgáltatóra és a felhasználás feltételeire vonatkozó – információkat.

A tanúsítvány kiállítható az aláíró által meghatározott álnévre is. Ebben az esetben a tanúsítvány azt igazolja, hogy az aláírás az álnév tulajdonosától származik (tényleges személyazonosságot ez esetben nem igazol). A tanúsítvány kiállítható továbbá olyan céllal is, hogy az az aláírót más személy vagy szervezet *képviseletében* történő aláírásra jogosítsa fel.

5.3.2.2. Érvényességi idő

Biztonsági okokból mindenképpen célszerű korlátozni a tanúsítvány érvényességi idejét. A jogalkotó ilyen általános korlátozást a minősített tanúsítványokkal kapcsolatban állapít meg, amelyek érvényességi ideje nem haladhatja meg az aláírás-ellenőrző adathoz kapcsolható aláírás-létrehozó eszközzel összefüggésben meghatározott érvényességi időt.

5.3.2.3. A tanúsítvány közzététele

A hitelesítés-szolgáltató kötelessége a tanúsítványokkal kapcsolatos adatok nyilvántartása, a nyilvántartás folyamatos karbantartása, a változások átvezetése, valamint a nyilvántartásnak közcélú távközlő hálózatok segítségével bárki számára hozzáférhető és folyamatosan elérhető módon közzététele. Igen jelentős érdek fűződik ahhoz, hogy a tanúsítványok aktuális állapota folyamatosan hozzáférhető legyen. E nélkül az aláíróval kapcsolatba kerülő fél nem tudhatja, hogy az alkalmazott elektronikus aláírás valóban érvényes-e, azaz nem került-e sor a felfüggesztésére vagy visszavonására, illetve alkalmas-e az adott jogügyeletben történő felhasználásra.

5.3.2.4. A tanúsítvány visszavonása

Az elektronikus aláírás csak akkor töltheti be a funkcióját, ha a tanúsítványban szereplő adatok folyamatosan megfelelnek a valóságnak. Ha ezzel kapcsolatban kételyek merülnek fel, akkor a hitelesítés-szolgáltató köteles a tanúsítvány érvényességét felfüggeszteni vagy visszavonni, és ezt a nyilvántartásában haladéktalanul közzétenni.

A hitelesítés-szolgáltató felfüggeszti a tanúsítvány érvényességét vagy visszavonja a tanúsítványttovábbá akkor, ha ezt az aláíró, illetve a képviselt személy kéri, vagy ha a Nemzeti Média- és Hírközlési Hatóság (NMHH) jogerős és végrehajtható határozatában így rendelkezik.

5.3.3. A hitelesítés-szolgáltató jogállása

5.3.3.1. *Szolgáltatási jogosultság*

Mivel a hitelesítés-szolgáltatást végző vállalkozásokra a jogalkotó igen komoly bizalmi feladatot ruház, ezért velük szemben egyúttal átfogó, a szolgáltatás biztonsági szintje szerint differenciált szervezeti és működési szabályokat állapít meg.

Fokozott biztonságú elektronikus aláírással kapcsolatos szolgáltatásokat a meghatározott pénzügyi követelmények teljesítése esetén bármely belföldi lakóhelyű vagy belföldön tartózkodási hellyel rendelkező természetes személy, illetve belföldi székhelyű (telephelyű) jogi személy vagy jogi személyiség nélküli szervezet nyújthat. A szolgáltatásnyújtás bejelentési kötelezettséghez kötött, amit a szolgáltató legkésőbb a szolgáltatás elindítása előtt 30 nappal az NMHH felé köteles teljesíteni .

A minősített szolgáltatások nyújtása a nagyfokú személyi, szakmai, műszaki és pénzügyi megbízhatóságnak az NMHH által lefolytatott minősítési eljárás során történő igazolásához kötött. Minősített szolgáltatást az a szolgáltató végezhet, amelyik

- igazolja, hogy a természetes személy, illetőleg a jogi személy vagy jogi személyiséggel nem rendelkező szervezet vezető tisztségviselője, illetőleg vezetője és alkalmazottai büntetlen előéletűek;
- igazolja, hogy a természetes személy, a jogi személy vagy jogi személyiséggel nem rendelkező szervezet vezető tisztségviselője, illetőleg vezetője vagy alkalmazottja a jogszabályban meghatározott szakképesítéssel rendelkezik;
- rendelkezik a tevékenység biztonságos folytatásához szükséges pénzügyi háttérrel és felelősségbiztosítással;
- biztosítja a tevékenység végzéséhez szükséges, az Eat. mellékleteiben és más jogszabályokban meghatározott szervezeti, biztonsági, eljárási, tájékoztatási követelményeket.

Amennyiben a minősítés során bebizonyosodik, hogy a szolgáltató megfelel a jogszabályokban foglalt követelményeknek, az NMHH a hitelesítés-szolgáltatót mint minősített tanúsítvány kibocsátására jogosult hitelesítés-szolgáltatót nyilvántartásba veszi. A szolgáltató köteles a működésében bekövetkező változásokat bejelenteni, és változással érintett körülményekre vonatkozóan a minősítést újra el kell végezni.

5.3.3.2. A hitelesítés-szolgáltató felelőssége

A minősített szolgáltatást nyújtó hitelesítés-szolgáltató mint megbízható harmadik fél felelősséget vállal az elektronikus aláírás és az időbélyegző felhasználásával kapcsolatos körülményekért. Felelőssége fennáll a vele szerződéses kapcsolatban lévő ügyfelével – az aláíróval – szemben, a szerződésszegésért viselt felelősség polgári jogi szabályai szerint.

A törvényben foglalt kötelezettségek megszegése esetén fennáll a felelősség a szolgáltatóval szerződéses jogviszonyban nem álló harmadik személlyel szemben is azokkal a jogügyletekkel kapcsolatban, amelyekben az általa kibocsátott tanúsítványt használták fel. Ez olyan többletgaranciát jelent, ami egyrészt növeli az elektronikus aláírás megbízhatóságát, másrészt biztosítja az aláírással kapcsolatban esetlegesen felmerülő károk megtérülését.

A szolgáltató felelőssége fennáll különösen akkor, ha a kárt

- a nem tanúsított aláírási termék felhasználása okozta;
- az igénylő nem megfelelő tájékoztatása okozta;
- az aláíró személyének, illetve képviseleti jogosultságának nem a törvényben foglaltak szerinti azonosítása okozta;
- az okozta, hogy a tanúsítványban foglalt adatok neki felróható okból nem felelnek meg a valóságnak;
- az okozta, hogy a hitelesítés-szolgáltatótól származó aláírás-létrehozó adat és aláírás-ellenőrző adat nem egyedi;
- az adatkezelési és adatvédelmi szabályok megszegése okozta.

A szolgáltató

- felelőssége kizárólag a minősített szolgáltatásokkal – minősített elektronikus aláírással vagy minősített időbélyegzővel –, illetve az ezekkel ellátott elektronikus dokumentumokkal okozott kárért áll fenn, és
- mentesül a szolgáltató a felelősség alól – mind az aláíróval, mind harmadik személlyel szemben –, ha a kárt az okozta, hogy az aláíró nem tett eleget a törvényben foglalt tájékoztatási kötelezettségeinek.

5.3.3.3. Állami felügyelet

A hitelesítés-szolgáltatás olyan bizalmi jellegű szolgáltatás, amelyre vonatkozóan szükség van állami felügyeletre. A felügyeleti szervek folyamatosan ellenőrzik a szolgáltatás-nyújtás követelményeinek teljesülését.

Az Eat. szerint a felügyeleti feladatokat a Nemzeti Média- és Hírközlési Hatóság látja el, ennek keretében

- nyilvántartásba veszi a fokozott biztonságú, illetve a minősített szolgáltatásokat nyújtó szolgáltatókat, valamint az elektronikus aláírási termékek tanúsításra jogosult személyeket (szervezeteket);
- a minősítést megelőzően, a bejelentéssel egyidejűleg, illetve azt követően, valamint a szolgáltatók működésének időtartama alatt a törvényben meghatározott eljárásban folyamatosan vizsgálja, illetőleg ellenőrzi, hogy a szolgáltatók megfelelnek-e az e törvény, a felhatalmazása alapján kiadott jogszabályok, a szolgáltatási szabályzat, illetve az általános szerződési feltételek előírásainak;
- a szolgáltatóval szembeni követelmények nem teljesítése esetén a törvény szerinti intézkedéseket és szankciókat alkalmazza.

Az NMHH felügyeleti tevékenysége során a törvényben meghatározott intézkedéseket tehet és bírságolhat. A jogsértés súlyára, gyakoriságára, az okozható vagy okozott kár mértékére, a szolgáltató minősített szolgáltatókénti működésére, valamint a korábbi intézkedésekre figyelemmel a következő intézkedéseket teheti, akár együttesen is:

- felhívhatja a szolgáltató figyelmét az a vele szemben meghatározott követelmények betartására;
- megtilthatja meghatározott technológiák, illetőleg eljárások alkalmazását;
- elrendelheti a korábban kiadott minősített tanúsítványok visszavonását, ha valószínűsíthető, hogy a minősített tanúsítvány valótlan adatot tartalmaz, vagy meghamisították, illetőleg ha a hitelesítés-szolgáltató által a minősített tanúsítványok aláírásához használt aláírás-létrehozó eszköz nem biztonságos;
- 100.000 forinttól 10.000.000 forintig terjedő bírságot szabhat ki;
- törölheti a szolgáltatót a minősített hitelesítés-szolgáltatók nyilvántartásából, ha a nyilvántartásba vételt meg kellett volna tagadni, vagy ha e törvény, illetőleg a felhatalmazása alapján kiadott jogszabályokban foglalt követelmények teljesítése más módon nem biztosítható.

5.3.4. Az elektronikus aláíráshoz kapcsolódó szolgáltatások

5.3.4.1. A hitelesítés szolgáltatás

Ennek keretében a hitelesítés-szolgáltató

- azonosítja az igénylő személyét,
- kulcspárt generál az igénylő számára,
- tanúsítványt bocsát ki (fogadja a tanúsítványokkal kapcsolatos változások adatait),
- nyilvánosságra hozza a tanúsítványhoz tartozó szabályzatokat,
- nyilvánosságra hozza az aláírás-ellenőrző adatokat (a nyilvános kulcsot),
- nyilvánosságra hozza a tanúsítvány aktuális állapotára (különösen esetleges visszavonására) vonatkozó információkat.

5.3.4.2. Időbélyegzés szolgáltatás

Egyes esetekben nem csak a dokumentum változatlansága, a küldő fél azonosított személye, hanem a dokumentum keletkezésének vagy módosulásának időpontja is fontos lehet. Erre alkalmas az időbélyegző-szolgáltatás.

A törvény szerint az időbélyegző elektronikusan aláírt elektronikus dokumentumhoz végérvényesen hozzárendelt vagy azzal logikailag összekapcsolt olyan adat, amely igazolja, hogy az elektronikusan aláírt elektronikus dokumentum az időbélyegző elhelyezésének időpontjában változatlan formában létezett.

Az időbélyegző tehát nem tartalmaz információt az aláíró személyére vonatkozóan, hanem az adott dokumentum adott időpontbeli tartalmát igazolja.

5.3.4.3. Aláírás-létrehozó adatnak az aláírás-létrehozó eszközön történő elhelyezése

Az Eat. az elektronikus aláíráshoz kapcsolódó szolgáltatásként határozza meg az aláírás-létrehozó adat elhelyezését az aláírás-létrehozó eszközön.

5.3.4.4. Elektronikus archiválás szolgáltatás

A hitelesítés-szolgáltatók archiválási szolgáltatást is nyújthatnak, amely elektronikus dokumentumok hosszabb távú hiteles megőrzésére szolgál.