

## BIZALMI SZOLGÁLTATÁSOK ALAPVETŐ JOGI TUDNIVALÓI

Ez a dokumentum a Microsec zrt. (a továbbiakban: **Microsec**), mint az EU-ban nyilvántartott, eIDAS Rendelet (meghatározását lásd az 1. számú mellékletben) szerinti minősített bizalmi szolgáltató által nyújtott bizalmi szolgáltatásokkal kapcsolatos alapvető tudnivalókat ismerteti jogi szempontból.

### I. BIZALMI SZOLGÁLTATÁSOK

A Microsec legfőbb tevékenysége bizalmi szolgáltatások, azon belül minősített bizalmi szolgáltatások nyújtása. Ezek az eIDAS Rendelet alapján a következők:

1. elektronikus aláírás, elektronikus bélyegző tanúsítványok kibocsátása;
2. időbélyegzés;
3. weboldal-hitelesítő tanúsítványok létrehozása;
4. archiválás;
5. aláírások ellenőrzése (ilyet a Microsec nem nyújt bizalmi szolgáltatásként);
6. ajánlott elektronikus kézbesítési szolgáltatások (ilyet a Microsec nem nyújt bizalmi szolgáltatásként).

A minősített bizalmi szolgáltatásokat az EU-n belül egységesen szabályozzák, ez azt jelenti, hogy a Microsec, mint magyar bizalmi szolgáltató által nyújtott fenti szolgáltatásokat ugyanúgy el kell fogadni bármely más EU-tagállamban, mint Magyarországon.

A bizalmi szolgáltatások nyújtásának szabályait az EU-s szintű eIDAS Rendelet és számos magyar jogszabály részletesen meghatározza. Az összefoglaló melléklete tartalmazza a legfontosabb jogszabályokat, azonban a Microsec tevékenységére nem csak jogszabályok, hanem szabványok is irányadók. A szabványok nem jogszabályok, de kötelezőek a Microsec-re nézve, az auditok során ezek betartását is ellenőrzik. A minősített bizalmi szolgáltatások nyújtására elsősorban az Európai Távközlési Szabványügyi Intézet (ETSI) által kibocsátott szabványok irányadók.

A Microsec bizalmi szolgáltatásait a Nemzeti Média és Hírközlési Hatóság (NMHH) ellenőrzi és auditálja, ezenkívül a megfelelőség értékelést 2020-ig a német TÜViT végezte, 2020-tól a Hunguard végzi.

A bizalmi szolgáltatásra irányuló szerződésekre a jogszabályok, szabványok kötelező tartalmi elemeket írnak elő. A Microsec EHSZ (elektronikus hitelesítés szolgáltatás) üzletágának a Microsec honlapjáról, a <https://e-szigno.hu/letoltesek/dokumentumok-es-szabalyzatok/> címről letölthető ÁSZF-je, illetve minta szolgáltatási szerződése biztosítja az alkalmazandó jogszabályoknak és szabványoknak való megfelelést.

### II. A HITELESÍTÉS ÉS AZ ELEKTRONIKUS ALÁÍRÁS KÖZÖTTI KÜLÖNBSÉGEK

Az elektronikus dokumentum hitelessége több módon is biztosítható, ezek közül az egyik (de van, hogy az egyetlen lehetséges) módszer az elektronikus aláírás.

Az Eüt. Kormányrendeletben nevesített AVDH, azaz Azonosításra Visszavezetett Dokumentum Hitelesítés szolgáltatás is elektronikus dokumentum-hitelesítési lehetőséget biztosít a felhasználók (természetes személyek) számára anélkül, hogy saját aláírói tanúsítvánnyal vagy az AVDH rendszerben saját regisztrációval rendelkeznenek. Ebben az esetben a hitelesítést nem a nyilatkozattevő végzi, hanem a dokumentumot a NISZ Nemzeti Infokommunikációs Szolgáltató zrt. (a továbbiakban: NISZ zrt.) hitelesíti saját elektronikus bélyegzőjével és időbélyegzőjével, előtte elvégzi az ügyfél azonosítását (pl. Ügyfélkapu).

Az eljárás hátrányai:

- az ügyfél azonosítása egyfaktoros (felhasználónév – jelszó, mely azonban akár a számítógép böngészőjében el is menthető) ezért felmerülhet a kérdés, hogy a dokumentum egyáltalán mennyiben köthető egyértelműen a felhasználó személyéhez,
- szerepkört nem tud igazolni, így cégképviselőre történő használata vitatott (a szolgáltató nem ajánlja), míg az elektronikus aláírás tanúsítványában feltüntethető mind a titulus (pl.

osztályvezető), mind a szervezet, mely adatokat a bizalmi szolgáltató közhiteles nyilvántartásban ellenőrizni köteles,

- több nyilatkozattevő esetén szükséges a dokumentum valamennyi nyilatkozattevő általi hitelesítése, az AVDH azonban nem tudja PDF formátumban kezelni a többes aláírást,
- az AVDH hitelesítéshez a magyar jog teljes bizonyító erőt rendel, azonban ez csak Magyarországon érvényes, az EU más tagállamában nem.

### III. AZ ELEKTRONIKUS ALÁÍRÁS / BÉLYEGZŐ

Elektronikus aláírást természetes személy (ember) tud létrehozni, míg az elektronikus bélyegző egy jogi személyhez (szervezethez) kapcsolható. Az elektronikus bélyegző igazolja, hogy a dokumentumot a jogi személy bocsátotta ki, biztosítva a dokumentum eredetének és sértetlenségének bizonyosságát. Bélyegző esetén a tanúsítvány alanya a szervezet, de a képviselőjében eljáró magánszemélyt ilyenkor is azonosítani kell.

Az eIDAS szerint az elektronikus aláírással / bélyegzővel ellátott okiratokat a bírósági eljárásokban kötelező bizonyítékként elfogadni, a minősített elektronikus aláírást pedig a saját kezű aláírással azonosnak kell elfogadni az EU egész területén.

#### 1. Az elektronikus aláírással / bélyegzővel ellátott okiratok típusai

Az elektronikus aláírással/bélyegzővel ellátott okiratok típusai között alapvetően annak alapján teszünk különbséget, hogy a létrehozásukhoz szükséges tanúsítvány kibocsátásakor (i) személyesen azonosítottuk-e az ügyfelet; (ii) milyen eszközre bocsátottuk ki a tanúsítványt. Ezek a körülmények azt is meghatározzák, hogy az adott aláíráshoz/bélyegzőhöz a jog milyen „joghatást” rendel. Ez azt jelenti, hogy minden elektronikus aláírással / bélyegzővel ellátott okirat felhasználható bizonyítékként, csak egyes típusú elektronikus aláírással / bélyegzővel ellátott okiratok „nagyobb”, mint másoké.

Elnevezés	Személyes vagy videós azonosítás van?	Milyen eszközre van kibocsátva?	Joghatás
<b>Fokozott biztonságú</b>	NEM, csak igazolványmásolatot küld be az ügyfél.	A tanúsítvány „NEM MINŐSÍTETT” eszközre is kibocsátható, így pl. lehet szoftveres vagy mobiltelefonra kibocsátott tanúsítvány.	<u>Nincs teljes bizonyító ereje</u> , a „meg nem hamisítottág vélelme” kapcsolódik hozzá. Az eIDAS alapján alkalmas az aláíró azonosítására és kizárólag az aláíróhoz köthető.
<b>Minősített tanúsítványon alapuló fokozott biztonságú</b>	IGEN, ettől lesz „minősített” a tanúsítvány.	A tanúsítványt „NEM MINŐSÍTETT” eszközre bocsátják ki. Mivel az aláírást létrehozó eszköz nem minősített, így csak „fokozott biztonságú aláírás” hozható vele létre.	<u>Teljes bizonyító erő</u> Magyarországon a Pp. 325. § alapján.
<b>Minősített</b>	IGEN, ettől lesz „minősített” a tanúsítvány.	A tanúsítványt „MINŐSÍTETT” eszközre bocsátják ki, így pl. aláíró kártyára (tokenre).	<u>Teljes bizonyító erő</u> a Pp. 325. § alapján, és az eIDAS alapján az egész EU-ban.

A személyes azonosításra szigorú szabályok vonatkoznak. Kötelező megnézni az illető igazolványát (személyi, útlevél, jogosítvány), kötelező a személy megadott adatait egyeztetni a belügyminisztériumi adatbázisokkal, továbbá kizárólag személyes lehet az azonosítás, nem történhet meghatalmazott vagy titkárnő útján.

A COVID-19 világjárványt megelőzően személyes azonosításra kizárólag a bizalmi szolgáltatónál, illetve közjegyzőnél történő személyes megjelenés útján volt lehetőség. Tekintettel azonban arra, hogy a járványhelyzet ezt sokszor kizárta vagy jelentősen megnehezítette és a korábbi, megfelelő garanciák maradéktalan biztosítása mellett elsődleges szemponttá lépett elő mind az elektronikus aláírást igénylő személyek, mind pedig a bizalmi szolgáltató, illetve a folyamatban részt vevő egyéb szervezetek munkavállalóinak egészségügyi biztonsága, így a jogalkotó is reagált a megfelelő jogi környezet kialakításával.

2020. december 4. napján lépett hatályba a Videoazonosítás kormányrendelet, mely a bizalmi szolgáltatások esetében a személyes jelenléttel egyenértékű biztosítékot nyújtó, nemzeti szinten elismert egyéb azonosítási módszerek között nevesíti a videotechnológiás azonosítást.

Az Eüt. kormányrendelet szerint a videotechnológiás azonosítás oly módon történik meg, hogy a bizalmi szolgáltató élő telekommunikációs kapcsolat során videofelvétel útján képmást készít az ügyfélről, majd összeveti az ügyfélről készített fényképet és az azonosításhoz felhasznált személyazonosság igazolására alkalmas okmányban szereplő képmást. Az azonosítás az E-ügyintézés Kormányrendelet alapján akkor megfelelő, ha a bizalmi szolgáltató által egyértelműen megállapítható, hogy az okmányban szereplő személy azonos a videofelvételen szereplő ügyféllel.

## **2. Az elektronikus aláírással / bélyegzővel ellátott okiratok bizonyító ereje**

Az alábbi táblázat a bizonyító erő szintje alapján mutatja be az egyes okirat fajtákat, valamint azt, hogy az adott okirat létrehozásához az elektronikus aláírások / bélyegzők közül melyik típust kell használni.

Okirat fajtája	Hogyan lehet ilyet előállítani?	Bizonyító erő
<b>Közokirat</b>	Csak bíróság, hatóság vagy közjegyző állíthatja ki, ügykörén belül.  <u>Elektronikus közokirat</u> : minősített vagy minősített tanúsítványon alapuló fokozott biztonságú elektronikus aláírás / bélyegző + ha jogszabály előírja, időbélyegző	gyakorlatilag „kétségbe vonhatatlanul” bizonyítja az okiratban foglaltakat
<b>Teljes bizonyító erejű magánokirat</b>	Bárki előállíthat ilyet, számos módon. Papíron: <ul style="list-style-type: none"> <li>• az aláírókon kívül két tanú is aláírta</li> <li>• az okiratot előállító személy azt végig saját kézzel írta és aláírta</li> <li>• „cégszerűen” aláírták</li> <li>• az aláírást ügyvéd ellenjegyezte</li> </ul> Elektronikusan: <ul style="list-style-type: none"> <li>• minősített vagy minősített tanúsítványon alapuló fokozott biztonságú elektronikus aláírás / bélyegző + ha jogszabály előírja, időbélyegző</li> <li>• AVDH</li> <li>• „biometrikus” aláírás</li> </ul>	teljes bizonyító erővel bizonyítja, hogy az okirat aláírója az abban foglalt nyilatkozatot: megtette, elfogadta, magára kötelezőnek ismerte el.  (ellenbizonyítás lehetséges, ha hibás az aláírás / érvénytelen a tanúsítvány, stb.)
<b>Magánokirat, aminek „meg nem hamisított” voltát vélelmezni kell</b>	Fokozott biztonságú aláírás / bélyegző használatával nem hozható létre teljes bizonyító erejű magánokirat, de egy olyan „vélelmet” társít hozzá a jog, hogy az okirat, amit ilyen aláírással / bélyegzővel láttak el, „nem hamisított”.	<u>feltételezhető</u> , hogy az írta alá, akinek az elektronikus aláírása azon szerepel, és a dokumentum tartalma az elektronikus aláírást kibocsátó személy jognyilatkozata,  (ellenbizonyítás lehetséges, ld. fent)
<b>Egyszerű magánokirat</b>	Papíralapú dokumentum, ami nem felel meg a teljes bizonyító erejű magánokiratra vonatkozó feltételeknek.	<u>a jogszabály nem társít hozzá semmilyen bizonyító erőt</u> , a bíróság / hatóság minden esetben egyedileg mérlegeli, hogy elfogadja-e bizonyítékként.

Érdemi bizonyító erőt a jog a minősített, illetve a minősített tanúsítványon alapuló fokozott biztonságú aláírásokhoz kapcsol. Emiatt, ha a jogszabályok elektronikus aláírás használatát írják elő valamilyen eljárásban (pl. cégeljárás), általában megkövetelik a teljes bizonyító erőt képviselő minősített, vagy minősített tanúsítványon alapuló fokozott biztonságú e-aláírás használatát.

Az elektronikus aláírás használata mellett szól, hogy ha egy papíralapú dokumentumot saját kezűleg aláírunk (de nincs rajta két tanú aláírása, nem hitelesíti közjegyző, ügyvéd stb.) akkor az a fentiek szerint csak egy „egyszerű magánokirat”, aminek önmagában alacsony, illetve nem garantált a bizonyító ereje. Ezzel szemben, ha minősített aláírással látunk el egy elektronikus okiratot, arról más közreműködő személyek (tanúk, ügyvéd) hitelesítése nélkül is feltételezi a jog, hogy az ténylegesen a mi nyilatkozatunk.

### **3. Az elektronikus aláírás / bélyegző fő felhasználási területei**

A jogszabályok bizonyos esetekben kötelezően előírják, más esetekben lehetővé teszik az elektronikus aláírás / bélyegző használatát. Az EÜT. alapján a közigazgatásban széles körben biztosítani kellene az állami szervezetek az elektronikus ügyintézés lehetőségét, ez azonban a gyakorlatban nem valósul meg teljes körűen.

Az útmutató 2. számú mellékletében található táblázat bemutatja az elektronikus aláírás felhasználásának főbb eseteit, megjelölve, hogy jogszabály alapján kötelező-e az e-aláírás használata, vagy csak lehetőségéről van szó.

Azon dokumentumok, nyilatkozatok esetén, melyet jogszabályi előírás alapján kötelező írásba foglalni (így különösen: munkaszerződések, ingatlan-ügyletek, adatfeldolgozási szerződés) legalább fokozott biztonságú elektronikus aláírás használata kötelező, az e-mail, illetve a .pdf dokumentum önmagában nem felel meg az írásbeliség kritériumainak.

#### IV. AZ ELEKTRONIKUS IDŐBÉLYEGZŐ

Az elektronikus időbélyegző azt igazolja, hogy az időbélyegzett elektronikus adatok az időbélyegzés időpontjában léteztek.

Minősített elektronikus időbélyegző esetében vélelmezni kell az időbélyegző által feltüntetett dátum és időpont pontosságát, valamint az adatok sértetlenségét. Tehát ha minősített aláírást és időbélyegzőt használunk, nem csak azt tudjuk utóbb igazolni, hogy megtettük az elektronikus okiratba foglalt nyilatkozatot, hanem azt is, hogy azt *pontosan mikor* tettük meg.

Az elektronikus időbélyegző használata azért is fontos, mert az elektronikus aláírás / bélyegző létrehozásához szükséges tanúsítvány érvényességi ideje Magyarországon 3 év. A tanúsítvány lejárt, visszavonása esetén a már nem érvényes tanúsítvánnyal korábban készített aláírásokat az aláíró programok érvénytelennek mutatják, ha azonban a dokumentum az elektronikus aláírás / bélyegző használatával egyidejűleg időbélyegzővel is el lett látva, akkor az aláírások érvényessége nem vész el.

Bizonyos, jogszabályban meghatározott esetekben az időbélyegző használata kötelező, így például hiteles másolatkészítés, azaz papíralapú dokumentum digitalizálása esetén.

#### V. A TANÚSÍTVÁNYOK TARTALMA

Elektronikus aláírás / bélyegző, illetve elektronikus időbélyegző létrehozásához szükséges egy PKI (Public Key Infrastructure) technológiával létrehozott tanúsítvány. A tanúsítványokban közös, hogy két kulcs kapcsolódik hozzájuk: egy nyilvános kulcs és egy magánkulcs.

A tanúsítvány maga tartalmaz egy nyilvános kulcsot, a nyilvános kulcshoz tartozó magánkulcs birtokosának (a tanúsítvány alanyának) nevét és adatait, valamint a tanúsítványt kiállító bizalmi szolgáltató elektronikus aláírását. A tanúsítványban foglalt adatok alapvetően nyilvánosak, így a Microsec által kibocsátott tanúsítványok adatai elérhetők a Microsec online tanúsítványtárában. A tanúsítványhoz tartozó magánkulcs mindig titkos, alapvetően az alany kezelésében áll, kivéve, ha az alany megbízza a bizalmi szolgáltatót, hogy a magánkulcsát helyette kezelje (ez az ún. tárolt kulcsú aláírás szolgáltatás).

#### VI. TANÚSÍTVÁNYOK TÍPUSAI FELHASZNÁLÁSI CÉL SZERINT

A tanúsítványoknak számos felhasználási célja is lehet, nem csak aláírás, pl.:

- **Aláíró / bélyegző tanúsítvány:** arra szolgál, hogy elektronikus okiratokat egy adott személyhez kapcsoljon
- **Titkosító tanúsítvány:** segítségével titkosított üzenet, dokumentum küldhető, amelyet kizárólag a titkosító tanúsítványban szereplő nyilvános kulcshoz tartozó magánkulcs birtokosa képes visszafejteni;
- **Autentikációs tanúsítvány:** Az autentikációs tanúsítványok birtokosaival mások biztonságos (titkosított és hitelesített) kapcsolatot létesíthetnek. A webszerverek számára kiállított TSL (régii nevén SSL) tanúsítványok is autentikációra szolgálnak.

A tanúsítványok tartalmazzák magukról, hogy milyen célra lettek kibocsátva, amit a programok tudnak ellenőrizni, és pl. nem engedik, hogy titkosító tanúsítvánnyal írjunk alá.

#### VII. ARCHIVÁLÁS

Az eIDAS Rendelet az elektronikus aláírások, bélyegzők vagy az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok megőrzését definiálja minősített archiválás szolgáltatásként. A gyakorlatban ritka, hogy valaki csak az aláírást szeretné archiválni, általában az egész dokumentum archiválásra kerül.

Az archiválás szolgáltatás során az archívumba beküldött elektronikus dokumentumokat az ügyfél által kért ideig, akár 50 évig megőrizzük és biztosítjuk a dokumentumok (i) adattartalmának változatlanóságát (ii) illetéktelenek számára történő hozzáférhetetlenségét (iii) és a dokumentumokon elhelyezett elektronikus aláírások érvényességének megőrzését.

Ennek érdekében az archívumot használó ügyfélnek rendelkeznie kell (i) elektronikus aláírói vagy bélyegző tanúsítvánnyal az archívumba beküldött dokumentumok aláírásához, (ii) autentikációs tanúsítvánnyal az archívumba való belépéshez (iii) titkosító tanúsítvánnyal, hogy az archívumban elhelyezett dokumentumokhoz csak ő férhessen hozzá.

#### **MELLÉKLETEK**

1. számú Melléklet - A legfontosabb alkalmazandó jogszabályok listája
2. számú Melléklet - Az elektronikus aláírás / bélyegző fő felhasználási területei

## **1. számú Melléklet - A legfontosabb alkalmazandó jogszabályok listája**

Jogszabály rövid neve	Jogszabály teljes neve	Mit szabályoz, ami a Microsec számára releváns?
<b>eIDAS Rendelet</b>	electronic IDentification, Authentication and trust Services rendelet – Az Európai Parlament és a Tanács 910/2014/EU rendelete a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról	<ol style="list-style-type: none"> <li><u>elektronikus azonosítás</u> <ul style="list-style-type: none"> <li>kormányzati e-ügyintézéshez szükséges e-azonosítási rendszerekre vonatkozó követelmények</li> </ul> </li> <li><u>bizalmi szolgáltatások, azon belül: minősített bizalmi szolgáltatások</u> <ul style="list-style-type: none"> <li>elektronikus aláírás, bélyegző, időbélyegző – kapcsolódó tanúsítványok</li> <li>weboldal-hitelesítő tanúsítványok</li> <li>archiválás</li> </ul> </li> </ol>
<b>Eüt.</b>	2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól	<ol style="list-style-type: none"> <li><u>elektronikus ügyintézés a közigazgatásban</u> <ul style="list-style-type: none"> <li>kötelező e-ügyintézés esetei, közig. szerv / ügyfél jogai és kötelességei</li> <li>szabályozott elektronikus ügyintézési szolgáltatások (SZEÜSZ) – van olyan, amit a Microsec is nyújthat</li> <li>központi elektronikus ügyintézési szolgáltatások (KEÜSZ) – csak a NISZ, a kormányzati szolgáltató nyújthatja</li> </ul> </li> <li><u>bizalmi szolgáltatások (eIDAS által nem szabályozott, tagállami szabályok)</u> <ul style="list-style-type: none"> <li>szolgáltatási szerződés az ügyféllel</li> <li>tanúsítványok felfüggesztése, visszavonása</li> <li>a bizalmi szolgáltató felügyelete, ellenőrzése</li> </ul> </li> </ol>
<b>Pp.</b>	2016. évi CXXX. törvény a polgári perrendtartásról	az okiratok bizonyító erejét: a közokirat, teljes bizonyító erejű magánokirat fogalmát, a „meg nem hamisítottság” vélelmét
<b>Üttv.</b>	2017. évi LXXVIII. törvény az ügyvédi tevékenységről	az elektronikus aláírás használatát az ügyvédi tevékenység során, az elektronikus ellenjegyzés szabályait
<b>Ctv.</b>	2006. évi V. törvény a cégnyilvánosságról, a bírósági cégeljárásról és a végelszámolásról	<ol style="list-style-type: none"> <li><u>elektronikus cégnyilvántartás</u> <ul style="list-style-type: none"> <li>elektronikus cégkivonat, cégmásolat, cégbizonyítvány lekérése, csoportos lekérdezés, kötelező adatszolgáltatás</li> </ul> </li> <li><u>elektronikus cégeljárás</u></li> </ol>
<b>Eüt. kormányrendelet</b>	451/2016. (XII. 19.) Korm. rendelet az elektronikus ügyintézés részletszabályairól	Az Eüt. végrehajtási rendelete, részletesebben tárgyalja a közigazgatási e-ügyintézt és a SZEÜSZ, KEÜSZ nyújtására vonatkozó szabályokat. Ami a Microsec-nek releváns:  <u>papíralapú dokumentumról hiteles elektronikus másolatkészítés szabályai</u>



<b>Bizalmi Rendelet</b>	24/2016. (VI. 30.) BM rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről	<ul style="list-style-type: none"><li>• bizalmi munkakörök meghatározása</li><li>• tanúsítvány kibocsátásra vonatkozó részletes követelmények</li><li>• archiválásra vonatkozó részletes követelmények</li><li>• szolgáltató kötelező felelősségbiztosítása (min. 3M HUF / káresemény)</li><li>• szolgáltatási szabályzatok kötelező tartalma</li></ul>
<b>Digitális Archiválás Rendelet</b>	1/2018. (VI. 29.) ITM rendelet a digitális archiválás szabályairól	hogyan lehet teljesíteni az elektronikus iratok megőrzésére vonatkozó kötelezettséget
<b>Videoazonosítás kormányrendelet</b>	541/2020. (XII. 2.) Korm. rendelet a bizalmi szolgáltatások esetében a személyes jelenléttel egyenértékű biztosítékot nyújtó, nemzeti szinten elismert egyéb azonosítási módszerekről	a videotechnológias azonosítás szabályait, melyek betartásával történő videotechnológias azonosítást a személyes jelenléttel egyenértékű azonosításnak kell tekinteni, ily módon tehát minősített aláírás tanúsítvány bocsátható ki

## 2. számú melléklet - Az elektronikus aláírás / bélyegző fő felhasználási területei

Eljárás neve	Hogyan használják az e-aláírást az eljárásban?	Kötelező-e az e-aláírás használata?
<b>Cégeljárás</b>	Cégeljárásban a jogi képviselő kötelező, így az adott céget képviselő ügyvéd / jogtanácsos a cégbíróság felé benyújtandó cégalapítási / változásbejegyzési / egyéb kérelmet elektronikusan írja alá és küldi be, és így veszi át a cégbíróság végzéseit is.	IGEN
<b>Fizetési meghagyásos eljárás (FMH)</b>	Jogi személyek (pl. cégek) csak elektronikus úton adhatnak be FMH kérelmet. 3 millió Ft alatti követelést kötelező ilyen úton érvényesíteni. A kérelmet a közjegyző bírálja el, aki elektronikusan kommunikál a kérelem előterjesztőjével.	IGEN, jogi személyek számára.
<b>Peres eljárás</b>	2018. január 1-től csak elektronikus úton pereskedhetnek a gazdálkodó szervezetek (pl. cégek), az állami szervek, illetve mindenki, aki jogi képviselővel (ügyvéd, jogtanácsos) jár el.	IGEN, de AVDH-val vagy „biometrikus aláírással” helyettesíthető.
<b>Bejelentés a Hitelezési Nyilvántartásba</b>	A hitelbiztosítéki nyilvántartás elsősorban azt tartalmazza, hogy milyen vagyontárgyakat terhel zálogjog vagy más biztosíték. A nyilvántartást a közjegyzői kamara vezeti, azonban nem csak közjegyzők tehetnek bejelentést a nyilvántartásba, hanem jogi képviselők, illetve a zálogjog (biztosíték) jogosultja vagy kötelezettje is.	IGEN
<b>JÜB rendszer használata</b>	Az ügyvédek, jogtanácsosok, közjegyzők, felszámolók, végrehajtók bizonyos esetekben kötelesek magánszemélyeket azonosítani. Ezt a személyi adat- és lakcímnnyilvántartáson keresztül teszik, amit a Jogügyletek Biztonságát Erősítő Adatszolgáltatási Keretrendszeren keresztül érnek el. Az adatlekérdezési kérelmet elektronikusan alá kell írni.	IGEN
<b>VIEKR rendszer használata</b>	A Magyar Bírósági Végrehajtói Kar (MBVK) Végrehajtási Iratok Elektronikus Kézbiztosítási Rendszerét a pénzügyintézetek kötelesek használni az adós vagyonának felkutatása iránti végrehajtói intézkedések fogadása és végrehajtói megkeresések megválaszolása során. A rendszerbe továbbá önkéntes alapon csatlakozhat bármely, a végrehajtókkal hivatalos kapcsolatban álló fél, pl. ügyvéd, adós, hitelező stb. A rendszerben megküldött megkereséseket, hivatalos értesítéseket elektronikusan alá kell írni.	IGEN
<b>Elektronikus Közbeszerzési Rendszer használata</b>	A közbeszerzési eljárásban az eljárási cselekmények elektronikusan is gyakorolhatók, nyilatkozat elektronikusan is tehető (legalább fokozott biztonságú e-aláírás használatával).	NEM

Eljárás neve	Hogyan használják az e-alírást az eljárásban?	Kötelező-e az e-alírást használata?
<b>Ingtalan-nyilvántartási eljárások</b>	A kérelemre induló olyan ingatlan-nyilvántartási eljárásokban, amelyekben a jogváltás bejegyzésének alapjául közjegyző által készített okirat, illetve ügyvéd vagy kamarai jogtanácsos által ellenjegyzett magánokirat szolgál, a jogi képviselő kötelező. A Földhivatalok befogadják az elektronikusan aláírt és benyújtott ingatlan-nyilvántartási kérelmet, amennyiben a mellékletek is eredeti elektronikusan aláírt dokumentumok. Az erről szóló jogi tájékoztatónk az alábbi linket olvasható: <a href="https://www.microsec.hu/hu/pki-blog/elektronikus-okiratok-alapjan-jar-el-foldhivatal">https://www.microsec.hu/hu/pki-blog/elektronikus-okiratok-alapjan-jar-el-foldhivatal</a>	NEM
<b>Elektronikus bizonylatolás, számlázás</b>	Elektronikus számla csak akkor bocsátható ki, ha a számla és az abban foglalt adattartalom sértetlensége, valamint eredetiségének hitelessége és olvashatósága biztosított. Ezt legbiztonságosabban úgy lehet elérni, ha a számlát a kibocsátó szervezet elektronikusan aláírással látja el, a kibocsátás időpontját pedig időbélyegzéssel igazolja. Elektronikus számla esetén a teljes megőrzési idő alatt (8 év) garantálni kell az eredet hitelességét, az adattartalom sértetlenségét és az olvashatóságot, a PKI technológia mindháromat garantálja.	NEM
<b>Szerződéskötés, ajánlatok, teljesítés igazolás, meghatalmazás, egyéb céges dokumentumok</b>	Amennyiben mindkét fél rendelkezik e-alírással, az elektronikus formában (pl. pdf) létező dokumentumot mindketten aláírhatják e-alírással, így nem szükséges minden oldalt szignózni, és elérhető a teljes bizonyító erejű magánokirati forma. Hibrid szerződéskötés lehetősége: szerződéskötés e-alírással akkor is lehetséges, ha csak az egyik fél rendelkezik elektronikusan aláírással. Az erről szóló jogi tájékoztatónk az alábbi linken olvasható: <a href="https://www.microsec.hu/hu/pki-blog/szerzodeskotés-e-alairással">https://www.microsec.hu/hu/pki-blog/szerzodeskotés-e-alairással</a>	NEM
<b>Munkaügyi iratok, M30-as nyomtatvány aláírása</b>	A munkaügyi dokumentumok akár nagy számban egyszerre is aláírhatóak.	NEM
<b>Hiteles elektronikus másolat készítése (digitalizálás)</b>	Papíralapú dokumentumról történő digitalizálás során a másolat készítője elkészíti az elektronikus másolatot, megállapítja a papíralapú dokumentum és az elektronikus másolat képi vagy tartalmi megfelelését, majd ellátja az elektronikus másolatot hitelesítési záradékkal és elektronikusan aláírással vagy bélyegzővel, és ha az időpont feltüntetése szükséges, elektronikusan időbélyegzővel	IGEN