

Digitális Állampolgárság Program (DÁP) – alapjaiban változik az elektronikus ügyintézés





A [Digitális Állampolgárság Program](#) nem magyar találmány, hanem egy uniós kötelezettség teljesítésének a megvalósulása, tekintettel arra, hogy az EU deklarált célja az, hogy 2030-ra az uniós állampolgárok 80%-a elektronikusan intézze ügyeit. Ennek oka az, hogy az elektronikus ügyintézés gyors, egyszerű, energiatakarékos, valamint papír- és környezetkímélő.

eIDAS és eIDAS2

A belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről szóló, [AZ EURÓPAI PARLAMENT ÉS A TANÁCS 910/2014/EU RENDELETE](#) (a rendelet angol címének kezdőbetűiből alkotott rövidítéssel az „eIDAS” rendelet) 2024-es módosítása hívta elő az új kötelezettségeket Magyarország számára is.

A rendelet eddig is rendelkezett az elektronikus okiratok létrehozásának és kezelésének legalapvetőbb feltételeiről, így az elektronikus

- azonosításról,
- aláírásról (illetve azok fajtáiról, létrehozásáról és ellenőrzéséről),
- okiratok igazolt elküldéséről (kézbesítés), és
- hosszú távú megőrzéséről (archiválás).

A rendelet korábbi szövege is lehetővé tette már, hogy az egyes tagállamok azonosítási rendszereket vezessenek be – ilyen Magyarországon pl. a [Központi Azonosítási Ügynök \(KAÜ\)](#), az elektronikus személyi igazolvány ([eSzemélyi](#)), és hamarosan

a [DÁP](#) is –, és amennyiben az adott tagállam azt a Bizottság számára bejelenti, úgy azt a többi tagállamnak is el kellett fogadnia, illetve lehetővé tenni, hogy az adott azonosítási rendszert használja a tagállami állampolgár más tagállamban történő elektronikus ügyintézése során.

Ez elméletben azt jelentené, hogy ha pl. Németországban szeretnénk elektronikusan ügyet intézni, akkor a német államnak lehetővé kellene tennie, hogy a magyar állampolgárok a német állami szolgáltatásokat a KAÜ-n keresztül elérjék. Ez azonban sajnos nem működött eddig a gyakorlatban, már csak azért sem, mert Magyarország nem jelentette be sem a KAÜ-t, sem az eSzemélyit, mint nemzeti azonosító rendszert a Bizottság felé (eddig).

Ez alapvetően változik meg az eIDAS idei módosításával, ami kötelezővé teszi, hogy minden tagállam 2026. májusáig legalább egy, ún. **európai digitális személyiadat-tárcát** biztosítson az állampolgárai számára, ami alkalmas arra, hogy abban a) személyazonosító adatok (és azokhoz társított ún. elektronikus attribútumtanúsítványok – erről később részletesen értekezünk majd egy külön cikkben) kerüljenek hitelesen tárolásra, igazolásra és megosztásra, ha a felhasználó úgy kívánja;

- b) álnevek generálása és azok titkosított, helyi szintű tárolása történjen a tárcán belül;
- c) egy másik személy tárcájának (illetve az abban tárolt adatok) biztonságos hitelesítése, valamint a személyazonosító adatok és az elektronikus attribútumtanúsítványok biztonságos módon történő fogadása és megosztása legyen lehetséges két tárca között;
- d) hozzáférése legyen a tárcán keresztül végrehajtott összes tranzakció naplójához, amely lehetővé teszi a felhasználó számára, hogy:
 - megtekintse azon igénybe vevő felek naprakész listáját, amelyekkel a felhasználó kapcsolatot létesített, és adott esetben az összes kicserélt adatot;
 - könnyen kérelmezhesse az igénybe vevő féltől a személyes adatok törlését;
 - könnyen bejelenthesse az igénybe vevő felet az illetékes nemzeti adatvédelmi hatóságnak, ha állítólagosan jogellenes vagy gyanús adatigénylés érkezik;
- e) minősített elektronikus aláírással történő aláírás vagy minősített elektronikus bélyegzővel történő bélyegzés;
- f) a felhasználói adatok, az elektronikus attribútumtanúsítványok és a konfigurációk letöltése a műszakilag megvalósítható mértékben;
- g) az adathordozhatóságra vonatkozó felhasználói jogok gyakorlása megvalósulhasson.

Mit jelent ez a gyakorlatban?

Ez azt jelenti, hogy a tagállamnak biztosítania kell egy mobileszközön elérhető rendszert, azaz egy alkalmazást a felhasználók számára, amiben minden adatukat, okiratukat és igazolásukat tárolhatják és megoszthatják harmadik

személyekkel, illetve ellenőrizhetik az adataik felhasználásának jogszerűségét és egyszerűen bejelenthetik, ha valamilyen visszaélést észlelnek.

Azaz a jövőben nem kell már semmilyen okmányunkat magunkkal vinnünk az Unión belül, hanem a mobiltelefonos alkalmazásunkkal igazolhatjuk magunkat pl. a rendőrség felé igazoltatás során, vagy pl. ha jelentkezni kívánunk (akár egy másik tagállamban) egy álláshirdetésre, akkor nem lesz szükségünk a diplománk közjegyzői hiteles másolatára, hanem azt egyszerűen elektronikusan – hitelesen – el tudjuk küldeni az állást hirdetőnek, akár a tárcába kért és megkapott hiteles elektronikus erkölcsi bizonyítványunkkal, valamint a tárcában elektronikusan aláírt önéletrajzunkkal együtt.

A fenti felsorolásból is látszik, hogy a rendelet különös hangsúlyt fektet a személyes adatok és az érintetti (felhasználói) jogok védelmére, és ezt még több helyen megismétli, illetve ezen túlmenően az alábbi garanciákat is tartalmazza:

1. A tárca használata nem kötelező, hanem önkéntes,
2. a felhasználó bármikor dönthet úgy, hogy nem kívánja többet használni a szolgáltatást, mely esetben vissza kell vonni a tárcát,
3. biztonsági incidens esetén fel kell függeszteni, vagy vissza kell vonni a tárcát,
4. a tárcának nyílt forráskódúnak kell lennie, azaz bárki megismerheti annak működését (kivételes esetben tartalmazhat zárt forráskódú elemeket, de ez esetben a tagállamnak azt külön indokolnia kell),
5. a tárca működtetése közben folyamatosan biztosítani kell a GDPR szerinti adatvédelmi és a NIS2 szerinti kiberbiztonsági követelményeket.



Az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvényt (Eüsztv.)

2024. szeptember 1-től váltó, a digitális államról és a [digitális szolgáltatások nyújtásának egyes szabályairól szóló 2023. évi CIII. törvény \(DÁPtv.\)](#) keretein belül megvalósításra kerülő [Digitális Állampolgár mobilalkalmazás](#) a fent bemutatott, eIDAS rendelet szerinti tárca-alkalmazást hivatott megvalósítani, ami lépésről lépésre fogja bevezetni az egyes kötelező szolgáltatásokat 2026-ig.

Sokan tartanak attól, hogy ez eszköz lehet az állam számára az állampolgárok megfigyelésére, azonban az általános jogállami fékek és ellensúlyok rendszerén túlmenően maga az eIDAS rendelet is tartalmaz biztosítékokat, valamint erre tagállami és uniós felügyeletet is biztosítani kell.

Ahogy arról a fentiekben már szót ejtettünk, az elektronikus ügyintézés alapvető rész-funkciói, vagy pillérei az azonosítás, hitelesítés (aláírás), kézbesítés, archiválás, fizetés.

Jelenleg ezeket a funkciókat a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló [2023. évi CIII. törvény \(DÁPtv.\)](#) átmeneti rendelkezései alapján még a már hatályon kívül helyezett, az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény (Eüsztv.), és annak még jelenleg is hatályos végrehajtási rendelete, az elektronikus ügyintézés részletszabályairól szóló 451/2016. (XII. 19.) Korm. rendelet szabályozza. Ezen rendelkezések alapján az

- az azonosítási funkciót a Központi Azonosítási Ügynök (**KAÜ**), és annak jelenleg még működő 5 fiókja: a DÁP eAzonosítás,

az emelt szintű kétfaktoros Ügyfélkapu+, a „sima” Ügyfélkapu, az elektronikus személyi igazolvány, a telefonos azonosítás és az arcképes azonosítás) valósítja meg,

- a hitelesítési funkciót az azonosításra visszavezetett dokumentumhitelesítés (**AVDH**),
- a kézbesítési funkciót az ún. Biztonságos Kézbesítési Szolgáltatás (BKSZ), ismertebb nevén az Ügyfélkapu és Cégkapu „tárhely” [a nehezebb érthetőség érdekében hívják még „Központi Ügyfél-regisztrációs Nyilvántartáshoz tartozó tárhely”-nek (**KÜNY-tárhely**) is],
- az archiválási funkciót a fenti BKSZ „Tartós tár”,
- a fizetési funkciót (amit egyébként nem szabályoz az eIDAS) pedig az Elektronikus Fizetési és Elszámolási Rendszer (**EFER**) biztosítja.

A fenti szolgáltatások azonban nem felelnek meg az eIDAS elvárásainak, így azokat le kell cserélni, de az eIDAS megfeleléségen kívül az alábbi problémák merülnek még fel:

Az azonosítás kapcsán felmerülő problémák

A telefonos azonosítás nem a legbiztonságosabb megoldás, de szerencsére nem is használták sokan, így az ezek miatt kivezetésre kerül. Szintén kivezetésre kerül a nehezen használható arcképes azonosítás, valamint az egyébként nagyon biztonságos, de szintén nehézkesen és ezért kevesek által használt eSzemélyi azonosítás. Ezek azonban keveseknek fognak hiányozni.



Ügyfélkapu+

Ugyanakkor **nagyon fontos, hogy 2025. január 15-én kivezetésre kerül a „sima” Ügyfélkapu is**, azaz eddig az időpontig mindenkinek, aki eddig ügyfélkapus bejelentkezést használt, döntenie kell, hogy bekapcsolja magának a jóval biztonságosabb, ún. kétlépcsős azonosítást biztosító **Ügyfélkapu+t („Ügyfélkapu plusz”)**, vagy regisztrál a Digitális Állampolgárság Programra.

Az átállás oka, hogy egyrészt az egyszerű felhasználónév és jelszó páros nem megbízható azonosítás, könnyen ellopható kamerás megfigyeléssel is akár, vagy ún. keylogger, azaz billentyűleütéseket rögzítő kémszoftverrel, illetve szándékosan, vagy akár véletlenül is lementhető a böngészőbe, nem beszélve arról, hogy ha valaki mindenhol ugyanazt a felhasználónév és jelszó párost használja, akkor az meglehetősen sebezhetővé teszi a feltörésekkel szemben, továbbá a rossz nyelvek szerint több tízezer Ügyfélkapu felhasználónév és jelszó páros vehető a darkweben.

Fentiekén túlmenően tapasztalat az is, hogy sokan megadják a felhasználónév és jelszó párosukat a könyvelőnek, mondván, hogy ő csak így tud bevallásokat benyújtani, ami egész egyszerűen nem igaz. A könyvelő részére meghatalmazást tudunk adni a [NAV ONYA rendszerben](#) az ÚJEGYKE nevű nyomtatvánnyal, vagy cégkapu-megbízotti státusz adható a <https://cegkapu.gov.hu> oldalon, vagy akár külön meghatalmazás a [Rendelkezési Nyilvántartásban](#), amit követően a könyvelő (de természetesen akár más megbízott, vagy adminisztrátor, ügyvédek esetében ügyvédasszisztens, vagy ügyvédjelölt is) a saját KAÜ bejelentkezési azonosítóival tud hozzáférni a szükséges felületekhez a megbízója/meghatalmazója nevében.

Az **Ügyfélkapu+** viszonylag egyszerűen és gyorsan bekapcsolható bárki által, aki már rendelkezik Ügyfélkapu hozzáféréssel. Ehhez az [Ügyfélkapu oldalán](#) bejelentkezve az „Ügyfélkapu+ igénylés” menüpontot választva tudunk eljutni. Az Ügyfélkapu+ bekapcsolásához szükségünk lesz egy okostelefonra, amire már előtelepítettük – választásunk szerint – vagy a Google Authenticator, vagy a Microsoft Authenticator applikációt (telepítésnél nagyon figyeljünk oda, mert kihasználva a figyelmetlenségünket, sok fejlesztő ajánlja a saját, nem megbízható termékét, ezért jól nézzük meg, hogy pontosan mi a szoftver neve.

A Google Authenticator

- [hivatalos elérhetősége Androidon](#)
 - [iOS-en,](#)
- a Microsoft Authenticator
- [hivatalos elérhetősége Androidon](#)
 - [iOS-en.](#)

Az Ügyfélkapu+ aktiválása során a felület ad egy QR-kódot, amit a mobiltelefonra előtelepített autentikációs alkalmazással le kell olvasnunk, majd a telefon 30 másodpercenként kódokat dob fel. Ezt a kódot kell beírni az Ügyfélkapu+ aktiválási folyamat következő lépéseként a számítógépen, amivel a folyamat befejeződik. Ekkor kapunk egy törlőkódot, amit jól tároljunk el egy biztonságos helyen, mert ha kizárnánk magunkat az Ügyfélkapu+-ból, akkor ezzel tudunk újat beállítani.

Nagyon fontos, hogy mind a számítógép, mind a telefon órája pontosan legyen beállítva, mert ennek hiányában nem fogjuk tudni használni a rendszert!

Az Ügyfélkapu+ sikeres aktiválását követően a „sima” Ügyfélkapu többé nem használható, minden bejelentkezési felületen az Ügyfélkapu+ opciót kell választanunk, és a megszokott felhasználónév, valamint jelszó páros megadása után még be kell írni a telefonunk által feldobott kódot is, csak így tudunk bejelentkezni.

DÁP mobilapplikáció

Ettől jóval egyszerűbb bejelentkezési megoldást biztosít a [DÁP applikáció](#), mivel ott vagy az alkalmazásban kell jóváhagynunk a bejelentkezést, ha mobileszközről kívánunk belépni, vagy pusztán egy QR-kód mobiltelefonos leolvasásával, ha számítógépen (vagyis semmilyen kódot nem kell begépelnünk).

Fontos azonban tisztában lenni azzal, hogy aki aktiválja a DÁP regisztrációját, az ugyan még 2025. december 31-ig használhatja az Ügyfélkapu+ bejelentkezési módszert, de többé már nem térhet vissza rá még akkor sem, ha inaktíválja a DÁP regisztrációját.

A DÁP regisztrációt az alkalmazás letöltését követően kormányablakban tudjuk elvégezni, vagy akinek olyan személyi igazolványa van, aminek a bal felső sarkában található egy uniós zászló, és ismeri az igényléskor – zöld szélű borítékban – kapott PIN kódját, az a mobiltelefonon is tud regisztrálni az alkalmazás segítségével.

Ez a bejelentkezés jóval biztonságosabb, mint bármelyik másik, mivel itt minden esetben egyrészt a telefonunkat is fel kell oldani, valamint a DÁP applikációt is vagy egy általunk megadott PIN-kóddal, vagy a telefonon bekapcsolt biometrikus azonosítással (ujjlenyomat vagy arckép), és ezt követően tudjuk jóváhagyni a bejelentkezést. Vagyis a tudtunk és engedélyünk nélkül más bizonyosan nem tud bejelentkezni.

A hitelesítés kapcsán felmerülő problémák

A jelenleg széles körben alkalmazott **AVDH 2024. december 31. napjával megszüntetésre kerül**. Ehelyett biztosít (a törvény szerint 2024. szeptember 1. napjától, azonban jelenleg még nem működik, így csak) majd ún. eAláírási funkciót a DÁP keretrendszer és maga az applikáció is. Ez már az eIDAS szerinti ún. minősített elektronikus aláírás lesz majd, ami minden EU tagállamban egyenértékű a kézi aláírással, azonosításra is alkalmas (az aláírás ún. tanúsítványán keresztül), és a magyar jog szerint teljes bizonyító erejű magánokirat létrehozására alkalmas, valamint ügyvéd által ellenjegyezhető. Ennek megfelelően

célgépjárársban és ingatlan-nyilvántartási eljárásban is használható lesz, fontos korlátozás azonban, hogy kizárólag magánszemélyként, azaz üzleti célra és jogi személy képviseletében nem lesz használható.

Az eAláírás előnye az AVDH-val szemben, hogy míg az AVDH tartalmazza az ún. 4T (természetes) személyazonosító adatainkat (így a születési név, születési hely és idő, valamint édesanyánk születési neve), addig az eAláírás tanúsítványa kizárólag a nevünket, esetleg az e-mail címünket és a tanúsítvány azonosítóját fogja tartalmazni. Ezzel kiküszöbölhető például az a probléma, hogy a jogi képviselő személyes adatai utaznak a képviselt ügyfél nevében elektronikusan benyújtott iratokkal. De fentiekén túlmenően, míg az AVDH külföldön nem használható, addig az eAláírás minden más EU tagállamban is azonos hatályú hitelesítést jelent.

A kézbesítés tekintetében felmerülő problémák

A BKSZ legnagyobb problémája jelenleg az, hogy azon keresztül kizárólag az állam és hatóságai tudják a kapcsolatot tartani az állampolgárokkal, vagy a gazdálkodó szervezetekkel, de nincs lehetőség arra, hogy állampolgár állampolgárnak, gazdálkodó szervezet gazdálkodó szervezetnek, vagy állampolgár gazdálkodó szervezetnek (és viszont) tudjon hitelesen elektronikusan küldeményt kézbesíttetni.

Ezen túlmenően a BKSZ nem az eIDAS szerinti ún. minősített ajánlott kézbesítési szolgáltatás, ami minden tagállamban kézbesítési fikciót keletkeztetne. Ennek megfelelően szükséges lesz lecserélni a BKSZ-t egy eIDAS-nak megfelelő, és mindenki számára egységesen elérhető, bárki számára kézbesítésre alkalmas felületre, ez lesz az ún. ePosta szolgáltatás. Fontos hangsúlyozni, hogy az eIDAS módosítása alapján ezeket a szolgáltatásokat összekapcsolhatóvá kell tenni, mivel lehetőséget kell biztosítani arra, hogy az egyes – különböző tagállami – digitális személyiadat-tárcák között az állampolgárok bármilyen adatot megoszthassanak. Ez azt is jelenti, hogy ezeket a – hiteles („tértivevényes”) – elektronikus kézbesítési szolgáltatásokat ugyanúgy össze kell kapcsolni majd, mint ahogy az egyes tagállami postaszolgáltatások összekapcsolásra kerültek már jóval korábban, és természetesen számunkra az, hogy a postán feladott küldeményünk minden probléma nélkül megérkezzen bármelyik másik tagállamban élő/működő címzett számára.

Az archiválás tekintetében felmerülő problémák

Az elektronikus okirataink hosszú távú megőrzéséről nekünk kell gondoskodnunk. Ennek [az eIDAS rendelet és a jelenleg hatályos [1/2018 \(VI. 29.\) ITM rendelet](#) rendelkezései alapján] háromféleképpen tehetünk eleget:

1. Az eIDAS szerinti minősített archívum szolgáltatás igénybevételevel, mely esetben az elektronikus okiratainkat



átadjuk egy minősített bizalmi szolgáltatónak és így ez a szolgáltató köteles gondoskodni az elektronikus okirat hosszú távú olvashatóságáról és hitelességének biztosításáról. Az eIDAS módosítása alapján az ilyen szolgáltatással eltárolt okiratokhoz az a vélelem kapcsolódik, hogy azok a megőrzés időszaka alatt sértetlenek és hitelesek.

2. Mi magunk gondoskodunk az elektronikus okiratok biztonságos megőrzéséről, ennek keretében az olvashatóság, sértetlenség és a hitelesség biztosításáról. Ez technikailag úgy történik, hogy a legutolsó időbélyeg érvényességi idejének lejárta előtt újabb időbélyeggel felüldőbélyegezzük az okiratainkat. Ez viszonylag egyszerűen algoritmizálható folyamat, és már vannak a piacon ezt biztosító szoftveres megoldások.
3. Megbízunk egy piaci – de nem bizalmi – szolgáltatót, hogy a fenti követelményeknek megfelelő őrzést és felülhitelesítést biztosítsa.

Amennyiben külső szereplőt bízunk meg ezzel, úgy fontos megfelelően megvizsgálni az üzleti (üggyvédi) titkok biztosítását is.

A magánszemélyek és gazdálkodó szervezetek számára a részükre az állam és hatóságai által küldött hiteles okiratok hosszú távú megőrzésére állami megoldásként jelenleg kizárólag a BKSZ „Tartós tár” áll rendelkezésre, ami csak az oda érkező küldemények eltárolását teszi lehetővé, és magánszemélyként legfeljebb 30Mb, míg gazdálkodó szervezet (Cégek) tárhelyén legfeljebb 300Mb mennyiségű irat tárolható el, ami borzasztóan kevés.

Az ígéret szerint az ezt felváltó eDokumentumtár eIDAS-megfelelő archívum-szolgáltatás lesz, ahová nem csak az ePostán érkező hiteles okiratainkat tudjuk eltárolni, hanem bármilyen, általunk oda feltöltött iratot.

A fizetés tekintetében felmerülő problémák

A fizetés tekintetében nyilván fontos biztosítani, hogy az egyes eljárási költségeket az elektronikus ügyintézés folyamatában, annak megszakítása nélkül biztonságosan és ügyfélbarát módon meg tudjuk valósítani (hiszen nyilván nem lenne ügyfélbarát, ha a számítógép elől felállva a postára kellene mennünk, hogy ott „sárga” csekk befizessük az ügyintézés díját és utána ezt a csekk beszkennelésével igazoljuk vissza). Ezt hivatott biztosítani majd az EFER-t leváltó eFizetés, ami az ígéret szerint az összes jelenleg használatos elektronikus fizetési megoldást (bankkártya, azonnali átutalás, qvik) biztosítani fogja.

Ugyanakkor fontos kihangsúlyozni, hogy az eAzonosítási, eAláírási, ePosta, eDokumentumtár és eFizetési szolgáltatás kizárólag a DÁP-ra regisztráltak és regisztrációjukat aktiválók számára, a DÁP keret-alkalmazásban lesz elérhető; azok számára, akik maradnak az Ügyfélkapu+ azonosítási megoldás mellett, azok ezeket a szolgáltatásokat nem fogják tudni élvezni.

Alábbi táblázatban összefoglaltam az egyes ügyintézési szolgáltatásokat a könnyebb áttekinthetőség érdekében:

| Offline | eIDAS | Eüsztv/Vhr. | DÁP | |
|--------------------------------|-------------------------|------------------|-----------------|-----------------|
| Személyes azonosítás okmánnyal | Elektronikus azonosítás | KAÜ (5 fiók) | KAÜ eAzonosítás | KAÜ Ügyfélkapu+ |
| Kézi aláírás | Hitelesítés (aláírás) | AVDH | eAláírás | ? |
| Posta | Kézbesítés | BKSZ („Tárhely”) | ePosta | ? |
| Irattár | Archiválás | BKSZ Tartós Tár | eDokumentumtár | ? |
| „Sárga” csekk/illetékbélyeg | | EFER | eFizetés | ? |

Szerző: dr. Kósa Ferenc ügyvéd,
a VI. Wolters Kluwer Jogászdíj Közönségdíjasa,
a Magyar Elektronikus Aláírás Szövetség Egyesület elnöke