Gyakran ismétlődő kérdések
az elektronikus aláírásról

Mi az elektronikus aláírás és mi a célja?

A jövő gazdaságában meghatározó szerepet kapnak a papíralapú iratokat, számlákat, megrendeléseket, dokumentumokat felváltó elektronikus iratok. Ezek elterjedése nemcsak papírtakarékosságot, hanem felgyorsuló iratkezelést, a megrendelések gyorsabb teljesítését, az üzleti élet hatékonyságának növelését eredményezi.
Az elektronikus aláírás ugyanazt a szerepet tölti be az elektronikus dokumentumok világában, mint a sajátkezű aláírás a papíralapú dokumentumok esetében. Az elektronikus aláírás olyan, a dokumentumokhoz csatolt digitális jelsorozat, amely a dokumentum tartalmából és az aláíró kizárólagos tulajdonában lévő, egyedi kulcsból (ez is digitális kód) bonyolult matematikai eljárással áll elő. Az érvényes aláírás a fogadó fél számára garancia a külső személyére nézve és arra, hogy a dokumentum az aláírás elhelyezése óta nem változott meg.

Miért kell a törvényi szabályozás?

A törvényi szabályozás célja, hogy megteremtse az elektronikus dokumentumok jogi elismerésének és felhasználásának jogi feltételeit. Az elektronikus aláírásról szóló törvény meghatározza azokat a feltételeket, amelyek teljesülése esetén az elektronikus aláírás egyenértékűnek tekintendő a sajátkezű aláírással. A törvény ezáltal biztosítja a hiteles elektronikus nyilatkozattétel, illetve adattovábbítás jogszabályi feltételeit.

Miről szól az elektronikus aláírás törvény?

A törvényi szabályozás három kérdéskörre terjed ki:
- biztosítja az elektronikus aláírás felhasználásának lehetőségét;
- meghatározza az elektronikus aláírással kapcsolatos szolgáltatások nyújtásának szabályait;
- szabályozza a szolgáltatásokkal kapcsolatos hatósági felügyeleti tevékenységet.

Mi az elektronikus aláírás szerepe a hétköznapi életben?

A polgárbarát közigazgatás kiépülésének és nemzetgazdaságunk versenyképességének egyik alapvető feltétele az információs társadalom nyújtotta lehetőségek hatékony alkalmazása. Egyre fontosabb szerepet kap mindennapi életünkben az elektronikus kereskedelem, az elektronikus okmányok, szerződések, beadványok használata. Az elektronikus aláírások használata lehetőséget nyújt arra, hogy egymást nem ismerő felek távközlő hálózatokon keresztül ügyeiket biztonságosan intézhessék. Különösen jelentős az elektronikus aláírások szerepe az

elektronikus banki műveletek és a közigazgatással kapcsolatos hivatalos ügyek intézésében.
Elektronikusan aláírható minden elektronikus dokumentum legyen az szöveg, hang, vagy akár kép. Egyedül a családjogi és öröklési ügyletek körében zárja majd ki a törvény felhasználásukat.

Mi a PKI?

A nyilvános kulcsú (PKI – Public Key Infrastructure) a nyílt távközlési hálózatokon (pl. Internet) napjainkban alkalmazott elektronikus aláírási rendszer.
Lényege, hogy az elektronikus aláírási funkciót két, egymást – matematikailag – kiegészítő kulccsal, egy un. aszimmetrikus kulcspárral valósítja meg. Az összetartozó kulcsok egyikével kódolt elektronikus adatsort csak a másik, hozzátartozó kulccsal lehet dekódolni. A felhasználó kizárólagos birtokában lévő, un. magánkulcs az elektronikus aláírás létrehozására (kódolás) használható. Az ehhez tartozó nyilvános kulcs az elektronikus aláírás ellenőrzésére (dekódolás) szolgál.
A nyilvános kulcsot egy hitelesítő szervezet által hitelesített és nyilvánosságra hozott tanúsítvány tartalmazza, ezáltal a nyilvános kulcshoz tartozó magánkulcs birtokosának, vagyis az üzenet küldőjének azonosítása a tanúsítvány alapján lehetséges.

Milyen fajta elektronikus aláírások vannak?

Az elektronikus aláírásról szóló törvény az elektronikus aláírások három típusát különbözteti meg. Ezek az „egyszerű” elektronikus aláírás, a fokozott biztonságú elektronikus aláírás és a minősített elektronikus aláírás.

- „Egyszerű” elektronikus aláírás: ide tartozik mindenfajta, akár a technológiai biztonságot nélkülöző eljárás (pl. ha az aláíró egy elektronikus szöveg végére odaírja a nevét vagy más azonosítóját).
  A törvény kimondja, hogy az aláírás elfogadását megtagadni nem lehet kizárólag amiatt, hogy az elektronikus formában létezik.
- Fokozott biztonságú elektronikus aláírás: olyan elektronikus aláírás, amely az aláíróra és az aláírandó dokumentumra egyaránt jellemző elektronikus adatsor.
  Ha jogszabály írásban foglalást ír elő, a fokozott biztonságú elektronikus aláírással aláírt elektronikus irat e követelményeknek eleget tesz.
- Minősített elektronikus aláírás: olyan fokozott biztonságú elektronikus aláírás, amely biztonságos aláíró eszközzel készült, és amelynek hitelesítése céljából minősített tanúsítványt bocsátottak ki.
  A minősített elektronikus aláírással ellátott elektronikus dokumentum teljes bizonyító erejű magánokiratnak minősül.

Milyen tulajdonságai vannak a fokozott biztonságú aláírásnak?

A fokozott biztonságú elektronikus aláírás PKI-n alapul, ezért:

- alkalmas az ellenőrzés során alkalmazott eljáráson és a hozzá tartozó tanúsítványon keresztül az aláíró személyének azonosítására;
- egyedülállóan az aláíróhoz köthető;

- olyan aláíró eszközzel hozták létre, mely kizárólag az aláíró befolyása alatt áll;
- lehetővé teszi a dokumentum tartalmának az aláírás elhelyezését követő bármely megváltozásának kimutathatóságát;
- biztosítja az aláírás megtörténtének letagadhatatlanságát.

Hogyan lehet meggyőződni arról, hogy egy aláíró eszköz biztonságos?

Az aláírás létrehozó eszközök megfelelőségének tanúsítására erre specializálódott, a gyártótól független tanúsító szervezetek jogosultak. A kijelölt tanúsító szervezetekről és az általuk tanúsított aláírás-létrehozó eszközökről a Hírközlési Főfelügyelet nyilvántartást vezet és tesz közzé. Ha egy tanúsított eszköz szerepel a Hírközlési Főfelügyelete nyilvántartásában, akkor az ellenkező bizonyításáig feltételezni kell, hogy az aláírás-létrehozó eszköz biztonságos.

Kik az elektronikus aláírás készítés és ellenőrzés szereplői?

- Aláíró fél: az elektronikus dokumentumot aláíró fél, vagyis a feladó. Az aláírónak gondoskodnia kell az aláírás készítéshez használt magánkulcsának őrzéséről, valamint a tanúsítványban foglalt adatok megváltozása estén új tanúsítvány kibocsátását kell kezdeményeznie.
- Hitelesítés-szolgáltató: az aláíró személyazonosságát tanúsító fél. A hitelesítés-szolgáltató megfelelő azonosítás (regisztrálás) alapján elektronikus tanúsítványt bocsát ki. A tanúsítvány célja, hogy, igazolja a tanúsítványban szereplő nyilvános kulcshoz tartozó magánkulcs birtokosának személyazonosságát. A szolgáltató a kibocsátott tanúsítványokról nyilvántartást vezet, melyet az interneten publikál. A szolgáltató az elektronikus aláírással kapcsolatos egyéb szolgáltatásokat is nyújthat, melyek közül a legfontosabb az időbélyegzés.
- Fogadó fél: az aláírt dokumentumot fogadó fél, azaz a címzett, aki az aláírás érvényességét vizsgálja. Az aláírás érvényessége biztosítékot nyújt arról, hogy a dokumentumot a tanúsítványban szereplő aláíró fél küldte, és hogy a dokumentum tartalma nem változott meg az aláírás elhelyezése óta.

Hogyan juthatunk minősített tanúsítványhoz?

Minősített tanúsítványt kizárólag azok a szolgáltatók bocsáthatnak ki, amelyeket a Hírközlési Főfelügyelet minősített szolgáltatóként vett nyilvántartásba.
A minősített aláírásokhoz kapcsolódó jogbiztonság érdekében a Hírközlési Főfelügyeletet a hitelesítés-szolgáltatók minősített tanúsítvány kibocsátási szolgáltatását, annak megkezdése előtt, illetve egész tartama alatt folyamatosan, vizsgálja és ellenőrzi. A követelményeknek való megfelelőséget a minősített tanúsítványban fel kell tüntetni. A Hírközlési Főfelügyelet a minősített tanúsítványokat kibocsátó szolgáltatókról nyilvános jegyzéket tesz közzé.

Hogyan történik az elektronikus dokumentum aláírása és ellenőrzése?

Az aláíró fél a dokumentumból meghatározott eljárással készített ujjlenyomatot (sűrítményt) a magánkulcsával kódolja. Mivel a magán aláírói kulcs és a dokumentum egyedi, a kapott digitális adatsor is egyedi. Ezt a későbbi ellenőrzésre felhasználható adatsort csatolják a dokumentumhoz elektronikus aláírásként. A dokumentumhoz a tartalom érvényességének igazolására időbélyegző is csatolható. Az időbélyegző maga is elektronikus aláírás, mely tanúsítja egy elektronikus dokumentum adott időpontbeli, adott tartalommal bíró létezését.
A fogadó fél az aláíró nyilvános kulcsával dekódolja dokumentumhoz csatolt elektronikus aláírást. Ezt az adatsort összehasonlítja az általa a dokumentum fogadáskor azonos eljárás útján készített ujjlenyomattal. Ha a két adatsor egyezik, akkor biztos lehet, hogy a dokumentum tartalma annak aláírása óta nem változott. Ezen eljárás mellett a hitelesítés-szolgáltató nyilvántartásában – jellemzően távközlő hálózaton keresztül – ellenőrzi az aláíró fél személyazonosságát és a tanúsítvány érvényességét.
A hiteles, aláírt elektronikus dokumentum megőrzéséről (pl. egy későbbi jogvita esetére) az aláíró és fogadó feleknek kell gondoskodniuk.

Kötelező lesz-e használni az elektronikus aláírást?

Az ügyfél részéről nem. A Törvény a jogbiztonság védelmében előírja, hogy jogszabály sem teheti kötelezővé az elektronikus dokumentum és elektronikus aláírás felhasználását.
Az államigazgatási és bírósági eljárásokban a nem elektronikus dokumentumokat mellőzve csak kifejezetten az adott eljárás-típusra vonatkozó megengedő jogszabályi rendelkezés alapján lehet eljárni. Ez a szabály a közigazgatási szervekre nézve kötelezettséget szab, az ügyfélnek pedig jogot ad elektronikus dokumentum használatára.

Mennyibe kerül egy elektronikus aláírás?

Az elektronikus aláírás költsége jellemzően két részből tevődik össze:
- az elektronikus aláíró eszköz és illesztő egység beszerzése egyszeri kiadást jelent. Az ár praktikusan § Ft-tól (nem „biztonságos” aláíró eszköz) kb. 25 eFt-ig terjedhet (intelligens kártya és kártyaolvasó);
- az elektronikus aláírás tanúsítása, illetve annak fenntartása a tanúsítvány típusától, biztonsági fokozatától függően évi 1-2 eFt-tól kb. 10 eFt-ig terjed.
  Az egyes tranzakciók aláírásáért többnyire külön már nem kell fizetni.

Más országban elfogadható-e az elektronikus aláírás?

Külföldi hitelesítés-szolgáltató által kibocsátott tanúsítványon alapuló elektronikus aláíráshoz a belföldivel azonos jogkövetkezmények fűződnek, ha nemzetközi szerződés így rendelkezik, vagy ha egy belföldi hitelesítés-szolgáltató felelősséget vállal a külföldi által kibocsátott tanúsítványért.
Magyarország EU csatlakozásával egyidejűleg életbe lép az az egységes és kölcsönös előírás, amely alapján a más országbeli hitelesítés-szolgáltató

tanúsítványához azonos jogkövetkezmények fűződnek, ha a szolgáltató székhelye, illetve lakóhelye az EU valamely tagállamában van.

Hamisítható-e az elektronikus aláírás?

A nyilvános kulcsú rendszerrel készített elektronikus aláírás alapvető tulajdonsága, hogy gyakorlatilag lehetetlen egy adott dokumentumhoz valakit megszemélyesítő aláírást előállítani – kivéve természetesen az adott személy magánkulcsával. Tehát a jogosulatlan megszemélyesítés (hamisítás) elleni védelem sarokpontja a magánkulcshoz való illetéktelen hozzáférés kizárása az alábbi módokon:

- a magánkulcs az aláíró kizárólagos tulajdonába kerül, arról semmilyen másolat sem készülhet a hitelesítés-szolgáltatónál;
- a magánkulcs csak alkalmi engedélyezés (pl. PIN kód, és/vagy biometrikus azonosítás stb.) után használható;
- a biztonságos aláíró eszköz meggátolja a magán aláírói kulcs kiolvasását;
- amennyiben a magánkulcs kitudódik (illetéktelen kézbe kerül), a hozzátartozó tanúsítványt azonnal vissza kell vonni, ettől kezdve a kulccsal készített minden aláírás érvénytelen.
  Fenyegetettséget jelenthet még a nem biztonságos informatikai környezet, amelyben aláírnak vagy aláírást ellenőriznek. (Pl. akkor, ha rosszindulatú program kerülhet az aláíró vagy ellenőrző számítógépébe.)

Mikortól lehet használni az elektronikus aláírást?

Elektronikus aláírás már ma is használható Magyarországon (működik is elektronikus aláírás hitelesítés-szolgáltató). A Törvény hatályba lépése után azonban jogi érvényessége már nem tagadható meg és bírósági eljárásokban bizonyítékként el kell fogadni. Minősített elektronikus aláírás minősített szolgáltató által kibocsátott minősített tanúsítványokon kell alapuljon. Ilyen aláírás készítésének feltétele, hogy legyen legalább egy hazai szolgáltató, amely a Hírközlési Főfelügyelet erre vonatkozó nyilvántartásában szerepel.