

Tájékoztató

elektronikus aláírás – időbélyegzés - titkosítás

A NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. az elektronikus aláíráshoz kapcsolódó hitelesítésszolgáltatásait azért fejlesztette ki, hogy független harmadik félként megteremtse ügyfelei és azok partnerei számára a biztonságos és hiteles elektronikus kommunikáció legfontosabb feltételeit.

Kormányzati hitelesítés szolgáltatóként az általunk kibocsátott tanúsítványban igazoljuk a szolgáltatásokat igénybe vevők személyazonosságát, elektronikus aláírásuk hitelességét. A szolgáltatási szabályzatainkban rögzített azonosítás-hitelesítési eljárást követően, az általunk kiadott tanúsítványok megfelelnek a magyar jogszabályoknak, a nemzetközi szabványoknak és ajánlásoknak, valamint az Európai Unió 1999/93/EK irányelvének.

Szolgáltatásainkat a Nemzeti Média- és Hírközlési Hatóság rendszeresen ellenőrzi.

Fogalmak, szolgáltatásaink rövid ismertetése:

Elektronikus aláírás: elektronikus dokumentumhoz azonosítás céljából logikailag hozzárendelt vagy azzal elválaszthatatlanul összekapcsolt elektronikus adat.

Elektronikus dokumentum: elektronikus eszköz útján értelmezhető adategyüttes.

Aláíró: az a természetes személy, aki az aláírás-létrehozó eszközt birtokolja és a saját vagy más személy nevében aláírásra jogosult, valamint az a jogi személy vagy közhiteles nyilvántartásban szereplő jogi személyiség nélküli szervezet, amely az aláírás-létrehozó eszközt birtokolja, és akinek a nevében az őt képviselő természetes személy az elektronikus aláírást az elektronikus dokumentumon elhelyezi, valamint aki meghatározza, hogy a nevében jogszabályban meghatározott feltételeknek megfelelő informatikai eszköz elektronikus aláírást elektronikusan dokumentumon elhelyezzen.

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

Alany: a hitelesítés-szolgáltató által kibocsátott tanúsítványban azonosított természetes személy, jogi személy, közhiteles nyilvántartásban szereplő jogi személyiség nélküli szervezet, aki vagy amely a tanúsítványban szereplő nyilvános kulcsnak megfelelő magánkulcsot birtokolja.

Érintett fél: az érintett fél (aláírás ellenőrző) olyan természetes vagy jogi személy, aki vagy amely, az aláírt *elektronikus dokumentum* fogadója, és egy adott tanúsítványon alapuló *elektronikus aláírásra* hagyatkozva jár el az aláírás hitelességének ellenőrzésekor.

A **PKI technológia** (Public Key Infrastructure, magyarul: Nyilvános Kulcsú Infrastruktúra) alkalmazása lehetővé teszi, hogy minden elektronikusan aláírt dokumentum vagy üzenet olvasója ellenőrizni tudja az üzenetet küldő személy azonosságát és az üzenet sértetlenségét. Az *elektronikus aláírás* az *aláíró* (alany) magánkulcsával készül és kizárólag annak párjával, a nyilvános kulccsal lehet ellenőrizni az aláírás eredetiségét, az aláírt *elektronikus dokumentum* sértetlenségét.

Ha az aláírt üzenetben vagy dokumentumon bármilyen változtatás történik, akkor az elektronikus aláírás nem fejthető vissza.

A **titkosítás** során a feladó az általa elkészített üzenethez vagy dokumentumhoz a címzett nyilvános kulcsát kapcsolja, vagyis a kódolás a nyilvános kulccsal történik. A címzett a hozzá

eljuttatott dokumentumot vagy üzenetet kizárólag a nyilvános kulcs párjával, azaz a saját tulajdonában lévő magánkulcsával tudja dekódolni, vagyis elolvasni.

Lényeges tudni, hogy a törvény a titkosítást csak az erre készült titkosító kulcspárral engedélyezi. Ezért a titkosítás önálló szolgáltatásként, a hozzá kapcsolódó szabályozási rendszerben működik.

Az **időbélyegzés-szolgáltatás** keretében hiteles időpontot, időbélyeget rendelünk az elektronikus üzenethez vagy dokumentumhoz. Az elektronikus üzenethez vagy dokumentumhoz rendelt igazolás másodperc pontossággal tartalmazza a bélyegzés időpontját, és biztosítja, hogy a dokumentumon minden, az igazolást követő módosítás érzékelhető legyen.

Összességben elmondható, hogy a kormányzati hitelesítés szolgáltatások igénybevételével megvalósul a biztonságos elektronikus kommunikáció, az ügyvitel felgyorsul és ennek köszönhetően a felhasználók jelentős időmegtakarítást nyerhetnek. A hitelesítés-szolgáltatások mellett biztosítani tudjuk a szükséges eszközöket és szoftvereket is.

A tényleges felhasználás megkönnyítésére munkatársaink rendelkezésére állnak, hogy személyes tanácsadással segítsék a választását és a használatbavételt.

Mindazokat az ismereteket, melyek a szolgáltatásban részt vevők számára elengedhetetlenül fontosak, a **Szolgáltatási Szabályzatainkban** (HSZSZ-F, HSZSZM, HSZSZ-T), az **Általános Szerződési Feltételeinkben** (ÁSZF) valamint az **Időbélyegzés Szolgáltatási Rend** (ISZR) c. dokumentumokban adjuk meg, melyekhez a szolgáltatások internetes honlapján, a <http://hiteles.gov.hu> weboldalon keresztül férhet hozzá. Ezekben ismertetjük a különböző előírásokat, jogszabályi hivatkozásokat, a tanúsítványok kezelésének módját, a hitelesség és biztonság mértékét és az erre vonatkozó technikai, üzleti és pénzügyi garanciákat, jogi felelősségvállalásokat, biztonsági előírásokat.

Jelen tájékoztatónkkal néhány fontos ismeretre szeretnénk felhívni szíves figyelmét, remélve, hogy sikerül megnyerni bizalmát, és felkeltjük érdeklődését szolgáltatásaink iránt.

Hogyan kell elektronikusan aláírni?

Maga az elektronikus aláírás azt jelenti, hogy Ön a **magánkulcsával** aláíráslétrehozó adat) az **elektronikus dokumentumához hitelesítés céljából hozzárendel egy olyan elektronikus adatsort** (elektronikusan kódolja, azaz "aláírja" a dokumentumot), mely a dokumentum elválaszthatatlan részévé válva minden kétséget kizáróan bizonyítja annak eredetét, hitelességét, sértetlenségét, és azonosítja Önt, mint aláíró személyt, illetve biztosítja az aláírás letagadhatatlanságát.

Az aláírás létrehozásához a magánkulcsot kizárólag Ön tudja aktivizálni a rendelkezésére álló PIN kóddal. Éppen ezért nagyon fontos, mind a chipkártya, mind a PIN kód biztonságos őrzése. **Ez, akárcsak a személyi igazolvány, a bankkártya és más személyes azonosságunkat jelző eszköz megőrzése komoly felelősséget ró Önre, mint felhasználóra, hiszen a magánkulcs és a PIN kód biztonságos használata csak addig garantált, amíg azok nem kerülnek illetéktelen kézbe.**

Saját érdekében kérjük, haladéktalanul tájékoztassa társaságunkat, ha az aláíráslétrehozó eszköze vagy PIN kódja elveszett, vagy illetéktelen személyhez került, illetve bármi más rendellenességet észlel.

Az aláírás és a dokumentum hitelességének, sértetlenségének ellenőrzése a címzett (érintett fél) feladata. Az ellenőrzéshez az üzenettel egyidejűleg a címzett rendelkezésére áll az aláíró fél nyilvános kulcsa, mellyel dekódolhatja az aláírást, és tanúsítványa, mellyel azonosíthatja az aláírót.

Cégünk a **tanúsítványban** „igazolja” (hitelesíti) az Ön személyazonosságát, és garantálja a címzett számára az Ön személyének, magánkulcsának és nyilvános kulcsának egymáshoz tartozását. Az aláírás elfogadásához a címzettnek indokolt ellenőrizni a tanúsítvány érvényességét a tanúsítványtárunkban. A kiadott előfizetői tanúsítványok adatai a kiadásuk után azonnal átkerülnek a tanúsítványtárunkba. Az érvénytelen tanúsítványok a mindenkori állapotot tükröző visszavonási listában vannak feltüntetve. A tanúsítványtár és a visszavont (tehát érvénytelen) tanúsítványok listája Internetes honlapunkon keresztül érhető el, a <http://hiteles.gov.hu> weboldalon.

Milyen tanúsítványok vannak, mi szükséges a tanúsítvány igényléséhez és a személyazonosság hitelesítéshez?

Előfizetői tanúsítványok

Fokozott biztonságú – aláírói – tanúsítványok

Minősített – aláírói – tanúsítványok

Titkosító tanúsítványok

A kétféle aláírói tanúsítvány technológiai háttere megegyezik, közöttük az eltérő biztonsági követelmények és joghatások adják a különbséget.

A fokozott biztonságú elektronikus aláírás olyan elektronikus aláírás, amit cégünk tanúsít, és amely alkalmas az aláíró azonosítására, használatával biztosítható a dokumentum hitelessége és sértetlensége. Mivel ez esetben az előírt biztonsági követelmények kevésbé szigorúak, a joghatása is enyhébb. Ez gyakorlatilag azt jelenti, hogy a fokozott biztonságú elektronikus aláírás esetében az érvényesség és a valódiság bizonyítása az aláírót és a hitelesítés-szolgáltatót terheli.

A minősített elektronikus aláírás olyan elektronikus aláírás, amely biztonságos aláíráslétrehozó eszközzel készült és ennek hitelesítése céljából minősített tanúsítvány került kibocsátásra. A minősített tanúsítvánnyal hitelesített elektronikus dokumentum teljes bizonyító erejű magánokiratnak minősül. Ebből következően annak kell bizonyítani az érvényesség és valódiság esetlegesen hamis voltát, aki azt kétségbe vonja.

Minősített tanúsítványon alapuló fokozott biztonságú aláírás

Mind a fokozott biztonságú, mind a minősített elektronikus aláíráshoz szükséges tanúsítvány személyesen vagy minősített elektronikus aláírással hitelesítve elektronikus úton igényelhető a közzétett érvényes szolgáltatási díjak megfizetésével, a hitelesítés szolgáltató és a felhasználó között létrejött szerződés keretében a hivatalos dokumentációkban leírt felelősségvállalások, kötelezettségek mellett.

Attól függően, hogy Ön milyen célra kívánja felhasználni elektronikus aláírását, az alábbi tanúsítványok közül választhat:

Gépi elektronikus aláírás

Személyes tanúsítvány (fokozott biztonságú és minősített)

Természetes személy igényelheti személyesen, a saját nevében, mint előfizető és aláíró egyben. Az azonosítás-hitelesítéshez szükséges: személy-azonosító igazolvány bemutatása személyesen.

Szervezeti személy vagy Munkatársi tanúsítvány (fokozott biztonságú és minősített)

Természetes személy igényelheti személyesen, egy adott szervezet alkalmazottjaként (munkatársaként), illetve tisztségviselőjeként.

Ez a tanúsítvány többek között azt is tanúsítja, hogy egy természetes személy valamely szervezet tagja, emellett hitelesíti a szervezetben betöltött funkcióját is.

Az azonosítás-hitelesítéshez szükséges: 30 napnál nem régebbi cégkivonat vagy alapító okirat, aláírási címpéldány, az aláíró személy személyazonosító igazolványának bemutatása személyesen.

Szervezeti tanúsítvány

Authentikációs tanúsítvány

Természetes személy igényelheti személyesen, egy adott szervezet alkalmazottjaként (munkatársaként), illetve tisztségviselőjeként.

Időbélyegzés szolgáltatásunk igénybevételének egyik feltétele egy autentikációs tanúsítvány megléte, mellyel bejelentkezhet időbélyeg szerverünkre. Az autentikációs tanúsítvány másik felhasználási területe valamely távoli szerver elérése tanúsítvány használatával (felhasználónév és jelszó helyett).

Web szerver SSL tanúsítvány

Természetes személy vagy szervezet igényelheti az IP címmel rendelkező informatikai eszköze (Web szerver, WAP szerver, stb.) részére.

A web szerver SSL tanúsítvány igénylése esetén a személy, illetve a szervezet azonosítása mellett szükséges az eszköz birtoklásáról és azonosításáról szóló nyilatkozat is.

Felhívjuk figyelmét, hogy a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. szolgáltatói tanúsítványai alapértelmezetten nem szerepelnek az elterjedt böngészőkben, ill a Windows tanúsítványtárban, ezért azokat kézzel kell telepíteni. Ennek megkönnyítésére létrehoztunk egy szolgáltatói tanúsítványokat telepítő alkalmazást, mely a Windows tanúsítványtárba (ezáltal az Internet Explorerbe) néhány másodperc alatt telepíti az összes szolgáltatói tanúsítványt – ez honlapunkról elérhető. Ezt követően már megbízhatóként tünteti fel a böngésző az általunk kiadott tanúsítványokat.

Milyen események fordulhatnak elő a tanúsítvánnyal kapcsolatban a kibocsátástól a visszavonásig?

A tanúsítvány kibocsátása

Az előfizető által kért tanúsítványt, a megrendelést és a regisztrációt követően, az Előfizetői Szerződésben foglaltaknak megfelelően aláírás-létrehozó eszközön bocsátjuk rendelkezésre.

Tanúsítványok megújítása (frissítés, aktualizálás)

Az előfizetői tanúsítványok érvényességi ideje általában: 1 év. A tanúsítvány lejártá előtt 30 nappal az előfizetőt e-mailben értesítjük a frissítés szükségességéről, egyúttal az érvényességi idő egy évre történő meghosszabbításának lehetőségére is felhívjuk a figyelmet. A tanúsítványok meghosszabbítására csak azok érvényességi idején belül van lehetőség.

Tanúsítvány felfüggesztés és visszavonás

A tanúsítvány tulajdonosának az aláíró eszköze vagy a PIN-kódja elvesztése, ellopása, nyilvánosságra kerülése, vagy mindezek gyanúja esetén, a visszaélések elkerülése érdekében haladéktalanul gondoskodnia kell a tanúsítvány felfüggesztéséről vagy visszavonásáról.

Felfüggesztés

A felfüggesztést kérheti az előfizető, az aláíró, vagy egyéb harmadik fél a HSZSZnek megfelelően, amennyiben a tanúsítvány biztonságos használatával kapcsolatban probléma merül fel.

A felfüggesztést telefonon kell kérni az erre a célra megadott felfüggesztési jelszó közlésével. Ilyen esetben az éjjel-nappal hívható Helpdesk Irodánkhoz kell fordulni. A tanúsítvány legfeljebb 5 naptári napig lehet felfüggesztett állapotban (ez átmeneti érvénytelenítést is jelent), ezt követően - kérelem esetén - újraérvényesítjük, illetve ennek elmaradása esetén visszavonjuk a tanúsítványt.

Visszavonás

A visszavonás sok tekintetben hasonló módon történik, mint a felfüggesztés. Lényeges azonban, hogy a visszavonási kérelmet csak személyesen és írásban lehet benyújtani a megfelelő azonosítási adatok és a felmerült körülmények közlésével az Ügyfélkapcsolati Irodában. A tanúsítvány ezzel végérvényesen érvényét veszti.

Anyagi felelősség

Kártérítésre a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. az ÁSZF-nek megfelelően, az előfizetői szerződésben megjelölt összeghatárig kötelezhető, bizonyított helytállási kötelezettség esetén.

Szolgáltatási díjak

A mindenkor érvényes szolgáltatási díjakat honlapunkon tesszük közzé, az árváltoztatás egyoldalú jogának fenntartása mellett. Az előfizetőkre vonatkozó hatályos szolgáltatási díjakat Előfizetői Szerződésben rögzítjük.

Milyen egyéb szolgáltatásokat és eszközöket vehet még igénybe?

Időbélyegzés – szolgáltatás

Az időbélyeg az elektronikus dokumentumhoz végérvényesen hozzárendelt, vagy azzal logikailag összekapcsolt olyan adat, amely igazolja, hogy az elektronikus dokumentum az

időbélyegzés időpontjában változatlan formában létezett. Az időbélyegzés szolgáltatás során az elektronikus dokumentumhoz időbélyeget csatolunk, mely időbélyeg a dokumentum tartalmához technikailag úgy kapcsolódik, hogy azon az igazolás kiadását követő minden módosítás érzékelhető.

Titkosítás – hitelesítés szolgáltatás

A dokumentumhoz - annak logikailag elválaszthatatlan részeként – kapcsolódó elektronikus adat a nyilvános kulcs lesz. A nyilvános kulccsal kódolt elektronikus „üzenet” a hozzá tartozó magánkulccsal dekódolható. A technológia (Nyilvános kulcsú Infrastruktúra) és az eljárásrend (azonosítás-hitelesítési eljárás, tanúsítvány, stb.) döntően megegyezik az elektronikus aláírásnál leírtakkal.

OCSP szolgáltatás

OCSP szolgáltatást jelenleg nem nyújtunk.

Fejlesztői és üzleti tanácsadás

Ennek keretében - külön megrendelésre - munkatársaink segítik az elektronikus aláíráshoz szükséges eszközök használatának betanítását, illetve a bevezetést, valamint elvégzik az eszközök üzembe helyezését.

Az elektronikus aláíráshoz szükséges eszközök és szoftverek

Chipkártyák és kártyaolvasók

Az aláírás-létrehozó adat elhelyezéséhez chipkártyát, a chipkártyához olvasó egységet biztosítunk.

Felhasználói szoftverek

Az elektronikus aláírások elhelyezéséhez és az aláírt dokumentumok aláírásának ellenőrzéséhez felhasználói szoftvert biztosítunk. Az aláírás létrehozó szoftver felhasználói jogáért az Előfizető részére díjat számolunk fel, míg az aláírás ellenőrző programunk szabad felhasználású, honlapunkról letölthető.

Kiegészítő biztonsági szoftverek

A kiegészítő biztonsági szoftverekről honlapunkon adunk tájékoztatást.

Információ és ügyintézés

Ügyfélkapcsolati iroda

Az ügyfélkapcsolati iroda címe: 1081 Budapest, Csokonai u. 3.

Az ügyfélkapcsolati iroda:

- személyesen felkereshető munkanapokon 9 és 13 óra között,
- telefonon elérhető munkaidőben a +36 1 795-7200 vagy a +36 30 795-7200 számon,
- elektronikus levélben elérhető bármikor az info@hiteles.gov.hu címen.

A tanúsítványok felfüggesztésére a folyamatos (7x24 órás) ügyfélszolgálatot (Help Desk szolgálatot) tartunk fenn.

Az ügyfélszolgálat elérhető:

- a +36 1 795-7300 vagy
- a ++36 30 795-7300 számon,
- valamint elektronikus levélben a címen.