NISZ
NEMZETI INFOKOMMUNIKÁCIÓS
SZOLGÁLTATÓ ZRT.

Tájékoztató

a NISZ Zrt. elektronikus aláírással kapcsolatos szolgáltatásairól

Elektronikus aláírás hitelesítés és időbélyegzés szolgáltatás, titkosító és autentikációs tanúsítvány kiadás

Érvényes: 2015. március 6-tól

Ferencz
Attila
József

Digitálisan aláírta: Ferencz Attila József
DN: c=HU, l=Budapest, o=NISZ Nemzeti Infokommunikációs Szolgáltató Zrt., title=igazgató, serialNumber=DO20130917-1DO27, cn=Ferencz Attila József, postalCode=1081, street=Csokonai u. 3.
Dátum: 2015.04.01 15:26:29 +02'00'

1. Bevezető

A NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. az elektronikus aláíráshoz kapcsolódó szolgáltatásait 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 tulajdonosok és nyilvános kulcsuk összetartozását. A szolgáltatási szabályzatainkban rögzített azonosítási-hitelesítési eljárást követően, az általunk kiadott tanúsítványok megfelelnek a magyar jogszabályoknak, valamint a nemzetközi szabványoknak és ajánlásoknak.

Szolgáltatásainkat bejelentettük az illetékes szerveknek, így pl. a Nemzeti Média- és Hírközlési Hatóságnak is, amely az e-aláírással kapcsolatos szolgáltatásainkat rendszeresen ellenőrzi.

2. Fogalmak, szolgáltatásaink rövid ismertetése

Elektronikus aláírás: elektronikus dokumentumhoz azonosítás céljából logikailag hozzárendelt vagy azzal elválaszthatatlanul összekapcsolt elektronikus adat.
Elektronikus dokumentum: elektronikus eszköz útján értelmezhető adat-együttes.
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 elektronikus 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 dokumentumban bármilyen változtatás történik, akkor az elektronikus aláírás nem fejthető vissza.

A PKI alapú ***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 küldött 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.

A PKI alapú ***autentikáció*** során egy személy vagy szervezet, illetve egy informatikai eszköz (pl. webszerver) tanúsítványa segítségével azonosítja magát és igazolja, bizonyítja kilétét távoli szerverekre/rendszerekbe történő belépés céljából (felhasználónév és jelszó helyett).

*Az **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 időbélyeg másodperc pontossággal tartalmazza a bélyegzés időpontját és ezzel a dokumentum egy adott időpontban meglévő állapotát rögzíti; az időbélyegzővel ellátott elektronikus dokumentumon minden utólagosan végrehajtott módosítás érzékelhető.

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, HSZSZ-M, HSZSZ-T), az **Általános Szerződési Feltételeinkben** (ÁSZF-PKI) valamint az **Időbélyegzés Szolgáltatási Rend** (ISZR) **és Hitelesítési Rendek (**HR-MTT, HR-NMT, HR-TET**)** c**.** dokumentumokban adjuk meg, melyekhez a szolgáltatások internetes honlapján, a *http://hiteles.gov.hu/szabalyzatok* 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.

3. Hogyan kell elektronikusan aláírni?

Maga az elektronikus aláírás azt jelenti, hogy a felhasználó a **magánkulcsával** (aláírás-létrehozó 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 PIN kóddal lehet aktivizálni. Nem-minősített tanúsítványok esetében a magánkulcsot és a tanúsítványt elektronikus fájlban adjuk át, a PIN kódot pedig külön, zárt borítékban kapja meg az ügyfél. A minősített aláírás céljából kibocsájtott tanúsítványoknál további előírás, hogy a magánkulcs és a tanúsítvány külön eszközön, biztonságos adathordozón/speciális biztonsági, kriptográfiai eszközben (chipkártya, USB csatlakozású token) kerüljön tárolásra, ezt nevezik ún. BALE-nek (Biztonságos Aláírás-létrehozó Eszköz).

Az elektronikus aláírás hitelességének, sértetlenségének biztosítása érdekében nagyon fontos a PIN kód, a magánkulcs – és amennyiben van – a BALE biztonságos őrzése, használata. **Ezek, akárcsak a személyi igazolvány, a bankkártya és más személyes azonosságunkat jelző eszköz, megőrzése komoly felelősséget a felhasználóra, hiszen a magánkulcs és a PIN kód biztonságos használata csak addig garantált, amíg azok nem kerülnek illetéktelen kézbe.**

Amennyiben Ön rendelkezik tanúsítvánnyal, saját érdekében kérjük, haladéktalanul tájékoztassa társaságunkat, ha az aláírás-létrehozó eszköze elveszett, illetéktelen személyhez került, illetve bármi más rendellenességet észlel.

Másik oldalról 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 az aláíró fél tanúsítványa, mellyel azonosíthatja az aláírót.
Cégünk a **tanúsítványban** „igazolja” az Ön személyazonosságát, és garantálja a címzett számára az Ön személyének, magánkulcsának (aláírás-létrehozó adat) és nyilvános kulcsának egymáshoz tartozását. Az aláírás elfogadásához a címzettnek indokolt ellenőrizni a tanúsítvány érvényességét a tanúsítványtárunkban. A NISZ Zrt. által kiadott tanúsítványok a nyilvános tanúsítványtárban megtekinthetők. Az érvénytelen tanúsítványok egy ún. visszavonási listában is fel vannak tüntetve. A tanúsítványtár és a visszavont (tehát érvénytelen) tanúsítványok listája Internetes honlapunkon keresztül érhető el, a *http://hiteles.gov.hu* weboldalon.

3. A végfelhasználói tanúsítványok fajtái

3.1.Aláírói tanúsítványok

A fokozott biztonságú, illetve minősített aláírói tanúsítvány technológiai háttere nagyrészt 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 aláírás-létrehozó 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.

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

Munkatársi tanúsítvány (fokozott biztonságú és minősített)
Egy adott szervezet alkalmazottjaként (munkatársaként), illetve tisztségviselőjeként igényelhető.
Ez a tanúsítvány többek között azt is tanúsítja, hogy egy természetes személy valamely szervezet tagja, emellett tartalmazhatja a szervezetben betöltött pozícióját is.

Szervezeti vagy Eszköz tanúsítvány (fokozott biztonságú és minősített)
Nem természetes személy, hanem egy adott szervezet, szervezeti egység vagy adott szervezet által üzemeltetett informatikai eszköz (szerver) részére kerül kiadásra.

Közigazgatási eljárásokban használható (KET-es) tanúsítványok olyan aláíró tanúsítványok, melyek speciális követelményeknek (elsősorban a 78/2010. (III. 25.) Korm. rendelet által előírtaknak) is eleget kell tegyenek. KET-es aláírói tanúsítványok kiadhatók személyek, szervezetek és szervezeti eszközök részére.

3.2.Nem aláírás célú tanúsítványok

Titkosító tanúsítvány

Egy adott szervezet saját maga, alkalmazottja (munkatársa), illetve tisztségviselője, továbbá valamilyen eszköze részére igényelheti.
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.

Autentikációs tanúsítvány

Egy adott szervezet saját maga, alkalmazottja (munkatársa), illetve tisztségviselője, továbbá informatikai eszköze részére is igényelheti.

SSL tanúsítvány

Az autentikációs tanúsítvány speciális típusa az **SSL tanúsítvány**. Az SSL technológiát a webhelyekkel, szerverekkel történő kommunikáció, illetve adatcsere titkosítására és hitelesítésére használják. Alapvetően 3 fajtája létezik: az SSL tanúsítvány egy domain hitelesítésére szolgál, a Wildcard SSL tanúsítvány a „*” karakter révén több aldomaint is hitelesíthet, az ún. UCC tanúsítvány pedig több domain hitelesítésére használható. Ezen tanúsítványokat jellemzően szervezetek igényelhetik, a fix IP címmel rendelkező informatikai eszközeik (pl. Web szerver) részére, létező külső domainek ill. aldomainek esetén.

4. A NISZ Zrt. szolgáltatói tanúsítványai

A NISZ Zrt. szolgáltatói tanúsítványai 2014 szeptemberétől szerepelnek a Windows tanúsítványtárában, ezért azok a programok és böngészők (pl. Internet Explorer, Chrome), amelyek a Windows tanúsítványtárát használják, elfogadják a NISZ Zrt. által kiadott végfelhasználói tanúsítványokat.

Azonban továbbra is fontos, hogy a NISZ Zrt. szolgáltatói tanúsítványait feltelepítsék olyan programokba (pl. Adobe Reader, Mozilla Firefox), amelyek nem a Windows tanúsítványtárából dolgoznak. A szolgáltatói tanúsítványok feltelepítése nélkül ezek a programok nem tudják végigfuttatni a hitelesítési láncot és hibaüzenetet küldenek a NISZ Zrt. által kiállított végfelhasználói tanúsítványok használatánál vagy ellenőrzésénél.

A cégünk által üzemeltetett számítógépekre a NISZ Zrt. vállalja a szolgáltatói tanúsítványok telepítését, így ezeken a gépeken minden program, böngésző kezelni tudja a NISZ Zrt. által kibocsátott tanúsítványokat.
Egyéb intézmények a honlapunkról letölthetik a szolgáltatói tanúsítványainkat, és a mellékelt útmutató alapján telepíthetik a saját számítógépeikre.

5. 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 bocsátjuk ki.

Tanúsítványok megújítása
A NISZ Zrt. által kiadott előfizetői tanúsítványok érvényességi ideje 2 év. A tanúsítvány lejárta előtt 30 nappal az előfizetőt e-mailben értesítjük a frissítés szükségességéről, egyúttal – fokozott tanúsítvány esetében – az érvényességi idő további egy évre történő megújításának lehetőségére is felhívjuk a figyelmet. A tanúsítványok megújítására 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 visszavonatásáról.

Felfüggesztés
A felfüggesztést kezdeményezheti az előfizető, az aláíró, vagy egyéb harmadik fél a HSZSZ-nek 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 szervezeti egységünkhöz 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.

6. Anyagi felelősség

Kártérítésre a NISZ Zrt. az ÁSZF-nek megfelelően, az előfizetői szerződésben megjelölt összeghatárig kötelezhető, bizonyított helytállási kötelezettség esetén.
Az aláíró tanúsítványokhoz különböző tranzakciós limitek társíthatók, például annak függvényében, hogy az aláíró személy az adott szervezeten belül – a belső folyamatok szerint - milyen értékhatárig rendelkezik aláírási jogosultsággal.

Tranzakciós limit: az aláíró tanúsítvány felhasználása során az egy alkalommal (vagyis egy-egy aláírással) az aláíró által vállalható kötelezettség legmagasabb értéke.

Szolgáltatói felelősségvállalás: az egyes tranzakciós limitekkel összefüggő összeg, amely erejéig a NISZ Zrt. – bizonyított helytállási kötelezettség esetén – felelősséget vállal elektronikusan aláírt dokumentumokból származó követelésekért.
A tranzakciós limiteket meghaladó ügyletekben használt elektronikus aláírásokból eredő károkért a NISZ Zrt. nem felel.

Aláírás fajtája	Tranzakciós limit HUF)	Felelősségvállalás (HUF)
Fokozott	0,-	100.000,-
	1.000.000,-	500.000,-
	10.000.000,-	1.000.000,-
Minősített	0,-	500.000,-
	1.000.000,-	1.000.000,-
	20.000.000,-	5.000.000,-
	200.000.000,-	50.000.000,-

7. Szolgáltatási díjak

Kérés esetén telefonon vagy emailen keresztül felvilágosítást nyújtunk a hatályos szolgáltatási díjakról, illetve egyedi árajánlatot adunk.

8. Egyéb szolgáltatások és eszközök

Időbélyegzés szolgáltatás
Az időbélyegzés szolgáltatást Interneten keresztül lehet igénybe venni olyan szoftver alkalmazással, mely támogatja a tanúsítvány alapú autentikációt. Ez az alkalmazás szabványos, RFC3161 szerinti (SHA256 lenyomatképző algoritmussal előállított) időbélyeg kérést küld a NISZ Zrt. időbélyeg szerverének, illetve fogadja az onnan érkező válaszokat.

Az időbélyegzés szolgáltatás igénybevételéhez a NISZ Zrt. díjmentesen biztosítja az autentikációs tanúsítványt.

OCSP szolgáltatás
A NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. valósidejű tanúsítványállapot-ellenőrzést (OCSP szolgáltatást) szolgáltat, segítségével a kormányzati hitelesítés szolgáltató által kibocsátott összes tanúsítvány aktuális visszavonási állapota lekérdezhető. A lekérdezés azonnali, hiteles választ ad egy tanúsítvány állapotáról. OCSP szolgáltatásunk díjmentesen igénybe vehető.

Az elektronikus aláíráshoz szükséges eszközök és szoftverek

Chipkártyák és kártyaolvasók, USB-tokenek
Az aláírás-létrehozó adat elhelyezéséhez chipkártyát, a chipkártyához olvasó egységet biztosítunk. Igény esetén a kártya helyett USB-tokenes eszköz igényelhető, mely közvetlenül a számítógép USB-portjára csatlakoztatható, így használatához nem szükséges a kártyaolvasó megvétele.

Felhasználói szoftverek
Az elektronikus aláírás használatához a tanúsítványon és chipkártyán túl szükség van egy megfelelő szoftveralkalmazásra is. Ilyenek például a Microsoft Office alkalmazások (pl. Word, Excel), melyek segítségével Word dokumentum vagy Excel fájl aláírható, vagy az Adobe Reader alkalmazás, amellyel PDF fájlok aláírása és időbélyegzése is megoldható; az Outlook segítségével pedig elektronikusan aláírt e-mailek is küldhetők.

A fenti ismert programok mellett léteznek speciális célalkalmazások is, amelyek az aláírás mellett támogatják pl. egy mappába összerendelt dokumentumok együttes titkosítását és időbélyegzését is. Ezek beszerzése alapvetően a felhasználók feladata. Amennyiben ügyfelek a tanúsítványok mellé ilyen célalkalmazást is szeretnének rendelni, társaságunk egyedi igényként kezelve megvizsgálja ennek a lehetőségét.

9. További információ és ügyintézés

Amennyiben a fentiekben ismertetett termékek, szolgáltatások kapcsán további tájékoztatásra van szükség, a NISZ Zrt. PKI Ügyfélkapcsolati Irodájának munkatársai készséggel állnak rendelkezésre az alábbiak szerint.

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

- személyesen felkereshető hétfőtől csütörtökig 9 és 16 óra között, pénteken 9 és 15 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 folyamatos (7x24 órás) ügyfélszolgálatot (Help Desk szolgálatot) tartunk fenn. A felfüggesztésért felelős szervezet elérhető:

- a +36 1 795-7300 vagy
- a +36 30 795-7300 számon,
- valamint elektronikus levélben az *smc@nisz.hu* címen.