MÁV INFORMATIKA
Kereskedelmi, Szolgáltató és Tanácsadó
Korlátolt Felelősségű Társaság

Időbélyegzési rend nem-minősített időbélyegzés szolgáltatáshoz (ISZR-NM)

Verziószám	**1.0**
OID szám	**1.3.6.1.4.1.14868.3.1.1**
Hatósági nyilvántartásba vétel napja	**2007. 09. 19.**
Hatósági nyilvántartásba vétel száma	**HL-22614-7/2007.**
Hatálybalépés dátuma	**2007. 09. 19.**

MÁV INFORMATIKA Kereskedelmi, Szolgáltató és Tanácsadó Kft.
1012 Budapest, Krisztina krt. 37/a., 1253 Budapest Pf. 28, Tel.: 457-9300, fax: 457-9500, e-mail: mavinformatika@mavinformatika.hu

Változás követés

Verzió	Dátum	A változás leírása	Készítette	Ellenőrizte	Jóváhagyta
1.0	2007.09.04.	Bejelentéssel együtt benyújtott első változat	Néder Ferenc	Kovács Árpád	Hosszú Sándor István

TARTALOMJEGYZÉK

1. Bevezetés

A MÁV INFORMATIKA Kft. mint kereskedelmi hitelesítés-szolgáltató 2002. novemberétől nyújt fokozott biztonságú elektronikus aláíráshoz kapcsolódó (nem-minősített) hitelesítés-szolgáltatást.

E dokumentum a MÁV INFORMATIKA Kft.-nek (továbbiakban Szolgáltató) az {J1} (Eat.) hatálya alá tartozó, az Eat. 6. § 1. b) pontja szerinti nem-minősített időbélyegzés szolgáltatására vonatkozó eljárási rendet és működési követelményeket tartalmazza, valamint leírja a Szolgáltató által kiadott időbélyegek használatának feltételeit.

A Szolgáltató a nem-minősített időbélyegzés-szolgáltatást a vele előfizetői szerződéses viszonyban álló Előfizetők részére nyújtja. Az időbélyegek felhasználói az Előfizetők mellett az időbélyeget ellenőrző érintett felek.

Az ISZR-NM nyilvános dokumentum, melyet a Szolgáltató az internetes honlapján keresztül teszi mindenki számára elérhetővé.

1.1 Áttekintés

Jelen időbélyegzési rend meghatározza az időbélyegzés szolgáltatás szereplőit, azok feladatait, kötelezettségeit és felelősségét, az időbélyegzés szolgáltató működésére vonatkozó követelményeket, az időbélyeg szerkezetét, az időbélyegzés-szolgáltatásra, valamint az azt támogató informatikai rendszerre vonatkozó működési követelményeket és szabályokat.

A MÁV INFORMATIKA Kft. az időbélyegzés szolgáltatást a fokozott biztonságú elektronikus aláírás hitelesítés-szolgáltatásaival együtt kapcsolódó szolgáltatásként, vagy azoktól függetlenül önálló szolgáltatásként nyújtja ügyfelei részére. Az időbélyegzési rend ezért mint önálló és különálló dokumentum határozza meg az időbélyegzés-szolgáltatás követelményeit és legfontosabb eljárásait. A részletes szabályokat a kapcsolódó szabályzatok (lásd: 1.6 pont) írják le.

1.2 A dokumentum neve és azonosítója

A Szolgáltató jelen dokumentumot az ISO/IEC és az ITU szabványok által előírt regisztrációs eljárásnak megfelelően eljárva regisztrálja.

A jelen dokumentum teljes neve:	Időbélyegzési rend nem-minősített időbélyegzés-szolgáltatáshoz. A jelen dokumentumban és a kapcsolódó szabályzatokban ISZR-NM-ként történik rá hivatkozás.
Azonosítója:	ISZR-NM
OID:	1.3.6.1.4.1.14868. 3.1.1

1.3 A szolgáltató és a felhasználói közösség

1.3.1 Szolgáltató adatai

Név:	MÁV INFORMATIKA Kereskedelmi, Szolgáltató és Tanácsadó Korlátolt Felelősségű Társaság
Cégjegyzék szám:	01-09-563711
Székhely:	1012 Budapest, Krisztina krt. 37/a.
Levelezési cím:	1253 Budapest Pf. 28
Telefonszám:	(36-1) 457-9300
Telefax szám:	(36-1) 457-9500
Internetes honlap címe:	*http://www.mavinformatika.hu/*
Szolgáltatás internetes honlapjának címe:	*http://www.mavinformatika.hu/ca/*

Illetékes fogyasztóvédelmi felügyelőség:

Közép-magyarországi Regionális Közigazgatási Hivatal Fogyasztóvédelmi Felügyelősége

1052 Budapest, Városház u. 7.

Levélcím: 1364 Budapest, Pf. 270.

Telefon: 318-2681, telefax: 318-1639

Email: fogyasztovedelem@pest.b-m.hu

Kapcsolat az ügyfelekkel:

Az ügyfélkapcsolatok (általános és részletes tájékozódás, szerződéskötés stb.) biztosítása érdekében a Szolgáltató Ügyfélkapcsolati Irodákat tart fenn, melyeket az ügyfelek személyesen azok nyitvatartási idejében kereshetnek fel. A mindenkori nyitvatartási rendeket a Szolgáltató a Szolgáltatás honlapján teszi közzé.

A központi Ügyfélkapcsolati Iroda címe: Budapest, I. Krisztina krt. 37/a.

A központi Ügyfélkapcsolati Iroda munkaidőben elérhető telefonon a +36-1-457-95-78 és a +36-1-457-9507 előfizetői közvetlen számon, egyébként a +36 30 633-8666 (üzenetrögzítő is egyben) mobil számon, vagy telefaxon a +36-1-457-9510, vagy a +36 1 457-9509 számon, valamint elektronikus levélben a *hiteles@mavinformatika.hu* címen.

A területi ügyfélkapcsolati irodák címe és elérhetősége a Szolgáltatás Internetes honlapján keresztül érhető el.

Az Ügyfélkapcsolati Irodák mellett a Szolgáltató folyamatos (7x24 órás) ügyfélszolgálatot (Help Desk szolgálatot) is biztosít. Az Ügyfélszolgálat elérhető a +36 80 39-93-93-as zöldszámon, a +36-1-457-93-93 közvetlen számon, a +36-1-457-93-00 központi számon, valamint elektronikus levélben a *helpdesk@mavinformatika.hu* címen.

Panaszok bejelentésének helye:

a. személyesen az Ügyfélkapcsolati Irodákban

b. írásban a Szolgáltató székhelyére címezve

c. telefonon az Ügyfélkapcsolati Irodákban vagy az Ügyfélszolgálatnál

d. elektronikus levélben a *mavinformatika@mavinformatika.hu* és a *hiteles@mavinformatika.hu* címeken

1.3.2 A Szolgáltató regisztráló és hitelesítő egységei

1.3.2.1 Ügyfélkapcsolati Irodák ("ÜKI")

Az Ügyfélkapcsolati Irodák (rövidítve: ÜKI) a Szolgáltató és a vele szerződéses alapon együttműködő Társaságok (mint szerződött közreműködők) azon szervezeti egységei, amelyek az időbélyegzés szolgáltatás igénylőinek regisztrációját végzik, valamint a szolgáltatásra vonatkozó előfizetői szerződések adminisztrációs feladatait látják el. Regisztráció során a Szolgáltató elvégzi az igénylő azonosítását és biztosítja a szolgáltatás igénybevételéhez szükséges eszközöket (jellemzően authentikációs tanúsítványt) és hozzáférési jogosultságokat.

1.3.2.2 Hitelesítő Központ és Időbélyegző Egység

A Hitelesítő Központ (rövidítve: CA) illetve az ahhoz kapcsolódó Időbélyegző Egység (rövidítve: TSA) a szolgáltatás-támogató informatikai rendszer központi erőforrásaiból, az ezt körül vevő biztonságos fizikai környezetből, valamint a szolgáltatást ellátó személyzetből áll. A TSA feladata az időbélyeg-kérések elbírálása (a jogosultság ellenőrzése) és az időbélyegek előállítása.

Amennyiben Szolgáltató több időbélyegző egységgel rendelkezik, biztosítania kell az egyes időbélyegző egységek egyértelmű azonosíthatóságát.

1.3.3 Előfizető

Az Előfizető a Szolgáltatóval szerződéses viszonyban álló felhasználó, aki számára a Szolgáltató időbélyeget bocsát ki. Előfizető lehet természetes vagy jogi személy. A szerződési feltételeket az {Sz8} Általános Szerződési Feltételek (ÁSZF-PKI) rögzíti.

1.3.3.1 Előfizetők informatikai eszközei

Időbélyeget nemcsak személyek, hanem az Előfizetők informatikai eszközei (szerverek, kommunikációs kapcsolatok, alkalmazások, stb.) is kérhetnek (pl. tranzakciók időpontjának hitelesítése céljából). Az informatikai eszköz ebben az esetben az Előfizető részére kiadott hozzáférési jogosultság – jellemzően authentikációs tanúsítvány magánkulcs - felhasználója.

1.3.4 Érintett fél

Az Érintett fél az időbélyeg ellenőrzése során az időbélyeget aláíró szolgáltatói tanúsítvány érvényességi ellenőrzésére hagyatkozva jár el. Az Előfizetők egyes informatikai eszközei (szerverek, kommunikációs kapcsolatok, alkalmazások, stb.) is lehetnek az időbélyeg kapcsán érintett felek.

1.4 A Időbélyegzési rend adminisztrációja

1.4.1 Rend hatálya

Az ISZR-NM időbeli hatálya a hatálybalépés dátumával kezdődik és határozatlan időre szól. Időbeli hatálya megszűnik egy újabb verzió hatályba lépésével vagy az időbélyegzési tevékenység beszüntetésekor.

Az ISZR-NM személyi hatálya a Szolgáltatóra és az Előfizetőre terjed ki.

Az ISZR-NM tárgyi hatálya a nem-minősített időbélyegzés-szolgáltatásra és a Szolgáltatónak a szolgáltatással kapcsolatban álló összes objektumára és tárgyi eszközére terjed ki.

1.4.2 Változáskezelés

1.4.2.1 Változtatási eljárások

A Szolgáltató szervezetén belül Hitelesítési Rend és Szabályozási Csoport működik, amely az ISZR-NM karbantartásáért felelős. Az időbélyegzési rend jogszabályoknak való megfeleléséért a Hitelesítési Rend és Szabályozási Csoport, illetve annak vezetője felel. A változtatási igényeket e csoport gyűjti, a módosításokat elvégzi, a változtatásokat életbe lépteti, az új rend verziókat elektronikus aláírással hitelesíti.

Az időbélyegzési rendet a Szolgáltató vezetése hagyja jóvá és lépteti hatályba.

Az időbélyegzési rend módosított változatai mindig új verziószámmal kerülnek nyilvánosságra.

1.4.2.2 Kapcsolattartó személy

A Szolgáltató részéről a kapcsolattartó személy a PKI szolgáltató egység vezetője. Elérhetőségét a Szolgáltató az ügyfélkapcsolati irodákon keresztül biztosítja.

1.4.3 Közzétételi és tájékoztatási elvek

1.4.3.1 Az ISZR-NM-ben nem tárgyalt elemek

A Szolgáltató nyilvános szabályzataiban csak azon eljárásait hozza nyilvánosságra, melyek ismerete a szolgáltatás biztonságát nem veszélyeztetik. A Szolgáltató több belső biztonsági és egyéb szabályzattal, operatív szintű előírással rendelkezik, melyeket bizalmasan, üzleti titokként kezel.

1.4.3.2 Az ISZR-NM közzététele

A ISZR-NM nyomtatott formában a Szolgáltató ügyfélkapcsolati irodáiban, elektronikus változata a szolgáltatás internetes honlapján érhető el.

1.4.4 Elfogadási eljárások

A jelen ISZR-NM szerkezetében és tartalmában követi az RFC 3647 szabványt azzal az eltéréssel, hogy a rend nem tartalmazza a nem értelmezhető vagy lényegi előírásokat nem tartalmazó fejezeteket, illetve tartalmaz az RFC-ben nem tárgyalt fejezeteket is.

A Szolgáltató a jelen ISZR-NM-t indokolt esetben, de legalább évente felülvizsgálja.

A rend jogszabályoknak való megfelelőségét a Nemzeti Hírközlési Hatóság (NHH) vizsgálja az ISZR-NM aktuális változatának hatálybalépését megelőzően.

Módosítás esetén a Szolgáltató az ISZR-NM változtatásokkal egybeszerkesztett új verziójának tervezetét felülvizsgálat és nyilvántartásba vétel céljából átadja a Nemzeti Hírközlési Hatóság Hivatalának, továbbá tájékoztatás céljából közzéteszi internetes honlapján. A Szolgáltató alkalmanként ezt megelőzően is konzultál az NHH-val a tervezett változtatásairól. Az ISZR-NM új változat hatályba léptetésének feltétele, hogy azt a Nemzeti Hírközlési Hatóság nyilvántartásba vette.

Az időbélyegzési rendnek csak a Szolgáltató aláírásával ellátott változata tekinthető hitelesnek.

1.5 Meghatározások

Aláírás-ellenőrző adat: olyan egyedi adat (jellemzően kriptográfiai nyilvános kulcs), amelyet az elektronikus iratot vagy dokumentumot megismerő személy az elektronikus aláírás ellenőrzésére használ.

Aláírás-létrehozó adat: olyan egyedi adat (jellemzően kriptográfiai magánkulcs), melyet az aláíró az elektronikus aláírás létrehozásához használ.

Biztonságos környezet: Olyan fizikai környezet, mely védett illetéktelen hozzáféréstől, és bizonyos mértékig tűz, víz és egyéb katasztrófaeseményektől, egyéb erőszakos behatásoktól.

Elektronikus aláírás: elektronikusan aláírt elektronikus dokumentumhoz azonosítási célból logikailag hozzárendelt, vagy ahhoz elválaszthatatlanul összekapcsolt elektronikus adat.

Elektronikus dokumentum: elektronikus eszköz útján értelmezhető adategyüttes.

Előfizető: Az a személy vagy szervezet, amely Szolgáltatóval érvényes előfizetői szerződéssel rendelkezik hitelesítés-szolgáltatás vagy időbélyegzés-szolgáltatás igénybe vételére

Elsődleges (root) hitelesítő szervezet: az elsőnek létrehozott, fizikailag is működő hitelesítő szervezet, amely az alája rendelt másodlagos hitelesítő központokat és/vagy az időbélyegző egységek aláíró tanúsítványt hitelesíti,

Érintett fél: Az az entitás (személy/eszköz), aki/amely a magánkulcs felhasználó nyilvános kulcsához vagy egy időbélyeghez tartozó tanúsítvány ellenőrzése alapján egy adott tanúsítványon alapuló nyilvános kulcsú technikára (elektronikus aláírásra, időbélyegre) hagyatkozva jár el.

Felhasználó (végfelhasználó): olyan egyed, aki/amely az időbélyegzés-szolgáltatás keretében kiadott időbélyegeket a rendeltetésüknek megfelelően használja. Felhasználó lehet előfizető, vagy érintett fél. Eszköz vagy alkalmazás is lehet felhasználó.

Hitelesítő szervezet (CA): a Hitelesítés-szolgáltató azon egysége, amely a hitelesítés-szolgáltatás hitelesítő kulccsal folytatott tevékenységét végzi. A központ fizikailag egy telephelyre koncentráltan, védett, biztonságos körülmények között működik.

Időbélyegzés: az a folyamat, melynek során az elektronikus dokumentumhoz olyan igazolás rendelődik, amely tartalmazza a bélyegzés hiteles időpontját, és amely a dokumentumhoz oly módon kapcsolódik, hogy minden – az igazolás kiadását követő – módosítás érzékelhető

Időbélyeg: elektronikus dokumentumhoz végérvényesen hozzárendelt, vagy azzal logikailag összekapcsolt olyan adat, amely igazolja, hogy az elektronikus dokumentum az időbélyegzés időpontjában változatlan formában létezett

Időbélyegzési rend (ISZR): olyan követelmény- és eljárásgyűjtemény, amelyben egy szolgáltató, igénybe vevő vagy más személy (szervezet) időbélyeg felhasználásának feltételeit írja elő igénybe vevők valamely közös biztonsági követelményekkel rendelkező csoportja vagy meghatározott alkalmazások számára.

Igénylő: Az a személy vagy szervezet, amely Szolgáltatóhoz fordul a hitelesítés-szolgáltatás vagy időbélyegzés-szolgáltatás igénybe vétele céljából. Az Igénylő előfizetői szerződés megkötése után válik Előfizetővé.

Kriptográfiai modul: Hardver alapú biztonsági megoldás, amely alkalmas beépített eljárások segítségével biztonságos kulcsgenerálásra és tárolásra.

Nyilvános (publikus) kulcsú infrastruktúra (PKI): Az elektronikus aláírás, időbélyegzés vagy titkosítás létrehozására, ellenőrzésére, kezelésére szolgáló, aszimmetrikus kulcspárt alkalmazó infrastruktúra, beleértve a mögöttes intézményrendszert, a különböző szolgáltatókat és eszközöket is.

Produktív hitelesítő szervezet: az elsődleges hitelesítő szervezet által létrehozott logikailag vagy fizikailag létező hitelesítő szervezet, amely egy adott alkalmazási, szervezeti, földrajzi stb. területre ad ki tanúsítványokat.

Regisztráló szervezet: A regisztráló szervezetek a Szolgáltató és a vele szerződése alapon együtt működő Társaságok azon szervezeti egységei, amelyek az előfizetők adatainak regisztrációját, ellenőrzését, az igénylő személyazonosságának és hitelességének megállapítását, a tanúsítvány kérelmek összeállítását, a hitelesítő szervezethez történő továbbítását, és egyéb azonosítási, Tanúsítványmenedzsment és adminisztrációs feladatokat látnak el.

Szolgáltatási szabályzat: A hitelesítés szolgáltató (illetve időbélyegzés-szolgáltató) tevékenységével kapcsolatos részletes eljárási és egyéb működési szabályokat tartalmazó szabályzat.

Szolgáltató: elektronikus aláírással kapcsolatos szolgáltatást nyújtó természetes személy, jogi személy vagy jogi személyiség nélküli szervezet.

Tanúsítvány: A hitelesítés-szolgáltató által kibocsátott igazolás, amely a nyilvános kulcsot az elektronikus aláírásról szóló törvény szerint egy meghatározott személyhez kapcsolja és igazolja e személy személyazonosságát vagy valamely más tény fennállását, ideértve a hatósági (hivatali) jelleget.

Tanúsítvány visszavonási lista: Valamely okból visszavont vagy felfüggesztett, azaz érvénytelenített tanúsítványok azonosítóit tartalmazó elektronikus lista, amelyet a hitelesítés szolgáltató bocsát ki.

1.6 Hivatkozások

A Szolgáltató által nyújtott szolgáltatásokra elsősorban a következő jogszabályok mérvadók:

{J1} 2001. évi XXXV. törvény az elektronikus aláírásról (a továbbiakban: Eat.)

{J2} 3/2005. (III. 18.) IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről

{J3} 45/2005. (III. 11.) Korm. rendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással kapcsolatos feladat- és hatásköréről, valamint eljárásának részletes szabályairól

Hivatkozott illetve mérvadó ajánlások, szabványok:

{Sz1} CEN 14167-2 munkacsoport egyezmény: “Védelmi profil kriptográfiai modul időbélyegzés-szolgáltató aláíró műveleteire, mentési funkcióval” (MCSOB-PP)

{Sz2} ITU-T X.509 “Information technology - Open Systems Interconnection - The Directory: Public -key and attribute certificate frameworks” ajánlás 3. verziója

{Sz3} Internet Közösség RFC 3161 ajánlásai

{Sz4} ETSI TS 102 0023 és ETSI TS 101 861 szabványok

{Sz5} NIST FIPS 140-1 Level 1-3

{Sz6} MSZ ISO/EC 27001 szabvány

A Szolgáltató hivatkozott illetve mérvadó dokumentumai:

{Sz7} Szolgáltatási szabályzat fokozott biztonságú elektronikus aláíráshoz kapcsolódó hitelesítés-szolgáltatásokhoz és nem-minősített időbélyegzés szolgáltatáshoz (HSZSZ-F)

{Sz8} Általános Szerződési Feltételek a PKI szolgáltatásokhoz (ÁSZF-PKI)

{Sz9} A Szolgáltató Szervezeti és Működési Szabályzata

{Sz10} A Szolgáltató Titokvédelmi Szabályzata

{Sz11} A Szolgáltató Információbiztonsági szabályzata

{Sz12} A PKI Szolgáltatások biztonsági szabályzata

{Sz13} A PKI Szolgáltatások üzletmenet-folytonossági terve

{Sz14} A PKI szolgáltatások üzemeltetési kézikönyve

2. Általános rendelkezések

2.1 Időbélyegzés szolgáltatás igénylése

Időbélyegzés szolgáltatást igényelhet:

a. természetes személy saját elektronikus aláírásához vagy más célra

b. jogi személy (szervezet) saját munkatársai vagy ügyfelei részére az általa meghatározott célra

c. természetes vagy jogi személy az általa használt informatikai eszközhöz (számítógép, alkalmazás, stb.)

Az időbélyegzésre vonatkozó igényeket az ügyfélkapcsolati irodához kell eljuttatni. Az igénylések formai követelményeit, feldolgozásuk módját, az adminisztráció szabályait a Szolgáltató {Sz7} HSZSZ-F jelű szolgáltatási szabályzata tartalmazza.

Az időbélyegzés szolgáltatás igénybe vételekor (a tényleges időbélyeg kérés folyamatában) a Szolgáltató elvégzi az igénylő azonosítását, azaz vizsgálja az időbélyeget kérelmező jogosultságát.

2.2 Időbélyegzés szolgáltatás

Az időbélyegzés szolgáltatás két szolgáltatási komponensből áll:

a. időbélyeg előállítása

b. időbélyegzés szolgáltatás menedzsment

Az időbélyeget előállító informatikai rendszer (TSA) két fő összetevőből áll:

a. az időbélyeg kérelmeket fogadó és elbíráló, az időbélyegeket előállító és kibocsátó egységből

b. az időbélyegeket előállító és kibocsátó egységek megbízható működését felügyelő és vezérlő egységből, amely a következő funkciókat látja el:

- felügyeli az időbélyegző szerver működését
- biztosítja az időbélyegző szerver belső időszinkronját
- felügyeli az időbélyegző szerver belső órájának a pontosságát; hiba esetén kezdeményezi a szolgáltatás leállítását és a hibaüzenet kiadását a felhasználók felé
- támogatja a naplózási és archiválási műveleteket.

Az időbélyegzés kérelmek teljesítését az időbélyegző egység automatikusan végzi:

a. a kérelmet egy olyan kommunikációs csatornán keresztül fogadja, amelyen keresztül az időbélyeg kérőt a Szolgáltató rendszere azonosítani tudja

b. az időbélyeg kérés kiszolgálása a TSA által aláírt időbélyeg elküldésével valósul meg.

2.3 Feladatok és hatáskörök

2.3.1 A Szolgáltató kötelezettségei

A Szolgáltatónak az időbélyeg felhasználók felé vannak kötelezettségei

Szolgáltató kötelezettséget vállal arra, hogy szolgáltatásaiban érvényesíti a jelen szabályzatot, betartja a vonatkozó szabványokat, jogszabályokat, valamint az időbélyegzésre vonatkozó azon követelményeket, amelyeket a Szolgáltató kapcsolódó szabályzatai rögzítenek.

A Szolgáltató a következőkre vállal kötelezettséget az időbélyeget felhasználók felé:

a. az időbélyegzés szolgáltatás biztonságát a nem-minősített hitelesítés szolgáltatókra vonatkozó követelmények szerint biztosítja

b. biztosítja, hogy az időbélyegző válasz, az időbélyegzéssel összefüggésben hozzáadottaktól eltekintve, ugyanazokat az adatokat tartalmazza, amelyeket a kérelem tartalmazott

c. rögzít az időbélyegzéssel kapcsolatos minden fontos eseményt, ezeket naplózza és a napló-állományokat megőrzi

Fenti követelményekhez kapcsolódó feladatokat Szolgáltató kiadhatja alvállalkozóknak, de ez esetben is Szolgáltató felelős elsődlegesen az alvállalkozók tevékenységéért.

2.3.2 Az időbélyeget felhasználók felelőssége

Az időbélyeget felhasználó előfizetők felelőssége a kért időbélyeg vétele után meggyőződni az időbélyeg helyességéről és az időbélyeget aláíró kulcs tanúsítványának érvényességéről a következők szerint:

a. Azonosítani az aláíró szervert az időbélyeget aláíró kulcshoz tartozó tanúsítványban feltűntetett azonosító alapján; egyúttal ellenőrizni az aláíró szerver tanúsítványának érvényességét a tanúsítványban megadott adatok alapján.

Továbbá indokolt elvégezni a teljes tanúsítási lánc ellenőrzését az alábbiak szerint:

b. meggyőződni az aláíró szerver tanúsítványát kibocsátó hitelesítés-szolgáltató kilétéről a kibocsátó hitelesítés-szolgáltató azonosítója alapján

c. meggyőződni az aláíró szerver tanúsítványának integritásáról a kibocsátó hitelesítés-szolgáltató szolgáltatói tanúsítványának segítségével

d. ellenőrizni az aláíró szerver tanúsítványának és hitelesítés-szolgáltató szolgáltatói tanúsítványának állapotát a tanúsítvány visszavonási listák (CRL[1]) áttanulmányozásával

Nem lehet elfogadni az időbélyeget, ha az aláíró szerver tanúsítványa, vagy a tanúsítási lánc tanúsítványainak valamely adata annak érvénytelenségére utal.

Az időbélyeget felhasználó érintett feleknek is ajánlott elvégezni a teljes tanúsítási lánc ellenőrzését a fentiek szerint. Felelősségük az időbélyeg felhasználása során az irányadó jogszabályoknak megfelelő módon, a tőlük elvárható gondossággal eljárni.

[1] CRL: Certificate Revocation List, magyarul: tanúsítvány visszavonási lista

3. Működési követelmények

3.1 Szolgáltatási szint

Az időbélyegzés szolgáltatást a Szolgáltató egy olyan időbélyegző informatikai alrendszerrel biztosítja, amely a nem-minősített elektronikus aláírás hitelesítést szolgáltató informatikai rendszerrel közös (vagy működés és biztonság szempontjából azzal egyenértékű) fizikai környezetben működik.

Az időbélyegben megadott idő 1 másodpercen belüli pontosságot biztosít.

Az időbélyegző egység órájának pontossága folyamatos ellenőrzés alatt áll. Ha ez túllépné a pontossági határt, akkor az ellenőrző program leállítja az időbélyegzés szolgáltatást, és minden további kérésre a hiba kijavításáig hibaüzenetet küld a felhasználók felé. A szolgáltatás akkor indul újra, ha az időszinkron helyreállt és az egy másodperces pontossági határ teljesül.

Az időbélyegzés szolgáltatást a Szolgáltató folyamatosan (az év minden napján, 24 órában), 99%-os rendelkezésre állással biztosítja úgy, hogy a szolgáltatás kiesése esetenként nem lépheti túl a 24 órás időtartamot.

3.2 Időbélyegzés

3.2.1 Időbélyeg

Az időbélyeg felépítése megfelel az {Sz3} IETF RFC 3161 szabványnak és a jelen szabályzatban meghatározott egyéb követelményeknek a következők szerint:

a. tartalmazza a jelen időbélyegzési rend azonosítóját (OID-jét),

b. tartalmazza az időbélyeg egyedi azonosítóját,

c. tartalmazza a releváns időpontot év, hónap, nap, óra, perc, másodperc értékben

d. tartalmazza a kérelmező által elküldött üzenetet (lenyomat)

e. a Szolgáltató az időbélyeget csak az időbélyegzés céljára kiadott aláíró kulccsal írja alá

f. az időbélyeg egy olyan névmegadást alkalmaz, amely tartalmazza:

- a Szolgáltató országának nevét (C),
- a Szolgáltató azonosítóját (CN)[2],
- az időbélyeget kibocsátó egység nevét (O, OU)

3.2.2 Óraszinkronizálás az UTC-vel

Az időbélyegző egység (TSA) belső órájának a pontossági tartományon belül maradását belső és külső szinkronizációs eljárás biztosítja.

A külső szinkronizálást több egymástól független UTC[3] időalap támogatja, amelyekkel nagy megbízhatósággal biztosítható az időbélyegzés belső órájának pontossága, valamint a külső órajelek redundancián alapuló ellenőrzésével annak hitelessége is.

3.3 A kulcsmenedzsment életciklusa

3.3.1 Az időbélyegző egység aláíró kulcsának generálása

Az időbélyeget aláíró szolgáltatói kulcspárt (és a hozzá tartozó szolgáltatói tanúsítványt) a szolgáltató maga generálja a biztonsági szabályzatában rögzített biztonságos körülmények között.

3.3.2 Az időbélyegző egység nyilvános kulcsának közzététele

Az időbélyegző egység aláírói nyilvános kulcsa és szolgáltatói tanúsítványa a Szolgáltató internetes honlapján keresztül érhető el.

[2] A CN és / vagy OU mezők jellemzően az időbélyegző egységet is azonosítják

[3] UTC: Coordinated Universal Time, az ITU-R TF.460-5 ajánlás szerint definiált, másodperc felbontású időalap

3.3.3 Az időbélyegző egység aláíró kulcsának megújítása

Az időbélyegző egység aláíró kulcsának megújítása tanúsítványa érvényességi idejének lejárata előtt válik aktuálissá. A kulcs megújítását a Szolgáltató a generáláshoz hasonlóan biztonságos körülmények között végzi.

3.3.4 Az időbélyegző egység kulcsmenedzsment életciklusának vége

Az időbélyegző egység kulcsmenedzsment életciklusa következő esetekben fejeződik be:

a. az időbélyeget aláíró kulcs tanúsítványának érvényességi ideje lejár

b. az időbélyeget aláíró kulcs kompromittálódik

c. a szolgáltatás befejeződik

Az *a.* esetben a lejárat előtt a kulcs megújítható a 3.3.3. pont szerint.

A *b.* esetben az időbélyeget aláíró kulcs tanúsítványát azonnal vissza kell vonni, az aláíró kulcsot meg kell semmisíteni és új kulcspárt kell generálni; továbbá: minden, a kompromittálódott kulccsal aláírt időbélyeget érvényteleníteni kell.

3.4 Időbélyegzés szolgáltatás menedzsment és működtetés

3.4.1 Biztonságmenedzsment

Az időbélyegzés szolgáltatást a Szolgáltató a nem-minősített hitelesítés-szolgáltatásával azonos szintű fizikai, szabályozási és személyi környezetben biztosítja, amely környezet megfelel a nem-minősített hitelesítés szolgáltatói követelményeknek.

A biztonságmenedzsment szabályozási hátterét képezik a Szolgáltató belső biztonsági szabályzatai:

a. a {Sz11} PKI Szolgáltatások informatikai biztonságpolitikája,

b. a {Sz12} PKI Szolgáltatások biztonsági szabályzata,

c. a {Sz13} PKI Szolgáltatások üzletmenet-folytonossági terve.

Ezek a dokumentumok nem nyilvánosak.

3.4.2 Működtetés menedzsment

A működtetés menedzsment a nem-minősített szolgáltatói követelményeknek felel meg.

A működtetés menedzsmentre érvényesek a Szolgáltató által üzemeltett informatikai rendszerekre alkalmazott társasági szintű működtetés menedzsment követelmények. Ezeken túlmenően az időbélyegzést támogató informatikai rendszerre vonatkozóan a működtetés menedzsmentet a {Sz14} PKI üzemeltetési kézikönyv szabályozza.

3.4.3 A szolgáltatás kompromittálódása

Az időbélyegzés szolgáltatás:

a. a Szolgáltató szolgáltatói aláíró kulcsának kompromittálódása,

b. az időalap kalibrációjának elvesztése

esetén kompromittálódik.

A Szolgáltató az időbélyegzés szolgáltatást mindkét esetben felfüggeszti mindaddig, amíg új és érvényes szolgáltatói aláíró kulcs, tanúsítvány, illetve pontosan kalibrált időalap nem áll rendelkezésre. A Szolgáltató szolgáltatói aláíró kulcsának kompromittálódása esetén minden, a kompromittálódott kulccsal aláírt időbélyeget érvényteleníteni kell.

3.4.4 Az Szolgáltató működésének befejezése

A Szolgáltató befejezi működését, ha tulajdonosa és vezetése ilyen határozatot hoz. A Szolgáltató működése befejezésének oka lehet katasztrófa szintű vagy más esemény, amelynek következtében megszüntető határozat születik.

A Szolgáltató a szolgáltatás megszűnése esetén késlekedés nélkül értesíti a Nemzeti Hírközlési Hatóságot és előfizetőit. Ha a megszűnés tervezett, az értesítés legkevesebb 60 nappal megelőzi a szolgáltatás leállítását.

A Szolgáltató működése felfüggesztésének oka lehet az NHH, mint hatóság felfüggesztő határozata is.

3.5 Biztonsági naplózások

A Szolgáltató gondoskodik arról, hogy az időbélyegzés műveletei naplózásra és elemzésre kerüljenek.

A naplózott adatállományok tartalmazzák a naplózott esemény bekövetkeztének dátumát és pontos idejét, az esemény követhetőségéhez, rekonstruálásához szükséges adatokat, az esemény kiváltásában közreműködő felhasználó vagy más személy nevét vagy azonosítóját.

A napló adatok rendszeresen archiválásra kerülnek ellenőrzés, szükségessé váló visszakeresés és újbóli használat céljából.

A naplóadatok megőrzési ideje 10 év.

A Szolgáltató archívumában olyan fizikai védelmet biztosít, amely fenntartja az archivált adatok bizalmasságát és sértetlenségét.

3.6 Katasztrófa elhárítás

3.6.1 A időbélyegzés-szolgáltatás azonnali felfüggesztése

A katasztrófa esemény bekövetkezése az időbélyegzés-szolgáltatás azonnali felfüggesztésével jár. Erről az eseményről a Szolgáltató lehetőségei szerint értesíti a felhasználó közösség tagjait.

3.7 Biztonsági szabályozások

A Szolgáltató az elfogadott szabványoknak megfelelő fizikai, eljárásbeli és személyzeti biztonsági óvintézkedések és az ezeket érvényre juttató adminisztratív és irányítási eljárásokat alkalmazza. Ezen belül:

a. folyamatosan fenntartja a szervezetén belüli biztonságkezeléshez szükséges informatika biztonsági infrastruktúrát

b. biztonsági szabályzatában dokumentálja és folyamatosan fenntartja az időbélyegzés-szolgáltatást nyújtó eszközök, rendszerek és informatikai értékek biztonsági ellenőrzéseit és üzemeltetési eljárásait.

c. gondoskodik arról, hogy személyzeti politikája, illetve a munkatársak alkalmazására vonatkozó gyakorlatai fokozzák és támogassák az időbélyegzés-szolgáltatás működésének megbízhatóságát. Tevékenységéhez kellő számú, a szolgáltatások nyújtásához szükséges feladatok jellegének, terjedelmének és mennyiségének megfelelő végzettséggel, képzettséggel, szakmai ismerettel és tapasztalattal rendelkező személyzetet alkalmaz.

3.8 Műszaki biztonsági óvintézkedések

A Szolgáltató megbízható, biztonságtechnikailag értékelt termékekből álló rendszert használ szolgáltatásai nyújtásához.

A TSA informatikai rendszer szállítója időbélyegzés-szolgáltatási rendszer kiépítésében jelentős tapasztalatokkal rendelkezik, a kor színvonalának megfelelő technológiát alkalmaz.

3.8.1 Szolgáltatói kulcspár előállítás

A Szolgáltató maga generálja a szolgáltatói kulcspárokat (az aláírás-létrehozó és az aláírás-ellenőrző adatokat) fizikailag védett környezetben. A kulcspárok generálását olyan algoritmusokkal valósítja meg amelyek szerepelnek a Nemzeti Hírközlési Hatóság HL-20336-9/2005. sz. határozatának 1. sz. mellékletében.

3.8.2 A szolgáltatói nyilvános kulcsok eljuttatása a felhasználói közösséghez

A Szolgáltató saját szolgáltatói tanúsítványait és ezen keresztül nyilvános kulcsait a szolgáltatás internetes honlapján keresztül teszi mindenki számára elérhetővé.

A szolgáltatói tanúsítványok letölthetők és a felhasználók kliens-alkalmazásaiba installálhatók.

3.8.3 Kulcsméretek, használt algoritmusok

A Szolgáltató a Nemzeti Hírközlési Hatóság Hivatala HL-20336-7/2005. számú határozatának megfelelően időbélyegzés szolgáltatásához az sha-1-with-rsa kriptográfiai algoritmuskészletet használja.

A TSA aláíró kulcsának mérete: legalább 1024 bit

A Szolgáltató folyamatosan figyelemmel kíséri a technikai fejlődést és ennek függvényében gondoskodik a kulcshossz szükséges mértékű növeléséről.

3.9 Számítógép biztonsági követelmények

A Szolgáltató biztonságtechnikai követelményeit a Szolgáltató {Sz12} informatikai biztonsági szabályzata határozza meg.

Az alkalmazott informatikai rendszer biztonsági követelményeit a Szolgáltató az alábbi termékeken alapulva elégíti ki:

- operációs rendszer,
- időbélyegzés alkalmazás,
- hálózati határvédelemi eszközök (tűzfalak, behatolás érzékelők, stb.)

4. A megfelelőség vizsgálata

4.1 Az ellenőrzések gyakorisága és körülményei

A megfelelőségi ellenőrzéseket a Szolgáltatónak évente meg kell ismételni. Ezek az ellenőrzések lehetnek belső auditok is.

4.2 Az auditor és szükséges képesítése

A külső és belső auditálást végző személyeknek függetlennek kell lenniük az időbélyegzés szolgáltatást üzemeltetését végző személyektől.

A külső és belső auditálást csak a megfelelő szakmai ismeretek birtokában lévő, tapasztalt szakemberek végezhetik.

4.3 Az auditor és az auditált rendszerelem függetlensége

Az auditornak (legalább szervezetileg) függetlennek kell lennie az általa ellenőrzött rendszertől.

4.4 Az auditálás által lefedett területek

Az auditálásnak le kell fedni az alábbi területeket:

- fizikai biztonság
- dokumentálás és folyamatok biztonsága
- a személyi állomány biztonsági ellenőrzése
- adatvédelem
- műszaki biztonság
- jogszabályi előírások betartása

4.5 A hiányosságok kezelése

A hiányosságok kezelése a Szolgáltató {Sz12} biztonsági szabályzata szerint történik.

4.6 Az eredmények közzététele

A külső és belső rendszervizsgáló csak a megbízójának adhat információt a szolgáltató tevékenységével kapcsolatban. Az audit és az ellenőrzés eredményei a szolgáltató bizalmas üzleti információi, ezért azokat a Szolgáltató {Sz10} titokvédelmi szabályzata szerint kell kezelni.