MÁV INFORMATIKA

Kereskedelmi, Szolgáltató és Tanácsadó
Zártkörűen Működő Részvénytársaság

Időbélyegzés Szolgáltatási Rend

Verziószám	**5.0**
OID szám	**1.3.6.1.4.1.14868.3.5**
Hatósági nyilvántartásba vétel napja	**2008. 01. 01.**
Hatósági nyilvántartásba vétel száma	**HL-7691-2/2008c**
Hatálybalépés dátuma	**2008. 01. 01.**

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

Időbélyegzés Szolgáltatási Rend verziók

Verzió	Dátum	A változás leírása	Készítette	Ellenőrizte	Jóváhagyta
1.0	2003.05.27	Az Időbélyegzés Szolgáltatási Rend véglegesítésre előkészített változata.	Bodlaki Ákos		
1.1	2003.07.29	Minősítési eljárásra beadott 1.0 változattal kapcsolatos észrevételekkel módosítva.	Bodlaki Ákos		
1.2	2004. 01. 21.	Felülvizsgált, módosított változat	Néder Ferenc		
2.0	2005. 07. 21.	Jogszabálykövetés és névváltozás miatt módosított változat	Néder Ferenc		
3.0	2005. 08. 18.	Felülvizsgált, módosított változat	Néder Ferenc		
4.0	2006. 03. 30.	Az NHH észrevételeivel módosított változat	Néder Ferenc		
5.0	2008. 01. 01.	A Szolgáltató adatainak változásával korrigált változat	Néder Ferenc	Juhász György, PKI SZE vezető	Hosszú Sándor István, vezérigazgató

TARTALOMJEGYZÉK

1. Bevezetés

A MÁV INFORMATIKA Zrt. (továbbiakban: Időbélyegzés Szolgáltató vagy Szolgáltató, rövidítve: ISZ) mint minősített hitelesítés szolgáltató időbélyegzés szolgáltatást is nyújt a minősített hitelesítés szolgáltatókra vonatkozó követelményeket kielégítő informatikai, fizikai és személyi környezetben.

Az ISZ által nyújtott időbélyegzés szolgáltatás hozzákapcsolható mind fokozott biztonságú, mind minősített aláírással ellátott dokumentumokhoz, valamint elektronikusan alá nem írt állományokhoz is.

Jelen Időbélyegzés Szolgáltatási Rend (továbbiakban: ISZR) meghatározza az időbélyegzés szolgáltatás szereplőit, azok feladatait, kötelezettségeit és felelősségét, az ISZ működésére vonatkozó követelményeket, az időbélyeg szerkezetét, az időbélyegzés szolgáltatás menedzsment és az időbélyegzéshez tartozó kulcsmenedzsment életciklusára vonatkozó szabályokat.

Összhangban az időbélyegzés szolgáltatókra vonatkozó követelményekről szóló ETSI TS 102 023 EU szabvány 7.1.1 fejezetével, a jelen ISZR a Szolgáltatóra, az időbélyeget előállító informatikai rendszerre és az időbélyegzés szolgáltatásra vonatkozó általános követelményeket határozza meg. A gyakorlatban megvalósított megoldásokat és szabályokat az ISZ „Szolgáltatási Szabályzat Minősített Elektronikus Aláírással Kapcsolatos Szolgáltatásokhoz” című dokumentuma (továbbiakban: HSZSZ-M) tartalmazza. Az időbélyegzés szolgáltatás szabályzata1 beépül ezen HSZSZ-M-be, annak részét képezi.

Az ISZR és a HSZSZ-M nyilvános dokumentumok, melyeket a Szolgáltató az internetes honlapján keresztül teszi mindenki számára elérhetővé.

2. Az ISZR hatálya

Az ISZR időbeli hatálya

Az ISZR időbeli hatálya a címlapon feltüntetett hatálybalépés dátumával kezdődik és megszűnik egy újabb ISZR verzió hatályba lépésével vagy a szolgáltatási tevékenység beszüntetésekor.

Az ISZR személyi hatálya

Az ISZR személyi hatálya az ISZ-re és az 5.3 pontban meghatározott felhasználó közösségre terjed ki.

Az ISZR tárgyi hatálya kiterjed:

a. az ISZR-ben meghatározott szolgáltatásokra,

b. az ISZ-nek az időbélyegzés szolgáltatással kapcsolatban álló összes objektumára, tárgyi eszközére.

3. Jogszabályi és szabályzati megfelelés

Az ISZR tartalmában és szerkezetében megfelel az elektronikus aláírásról szóló 2001. évi XXXV. törvénynek, az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről szóló 3/2005. (III. 18.) IHM rendeletnek, a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről szóló 2/2002. (IV.26) MeHVM irányelvnek, valamint az időbélyegzés szolgáltatókra vonatkozó követelményekről szóló ETSI TS 102 023 (2003.04) EU szabványnak.

Ezen túlmenően a jelen ISZR összhangban van a MÁV INFORMATIKA Zrt. belső szabályzataival, ezen belül a PKI szolgáltatásokra vonatkozó üzemeltetési és biztonsági szabályzatokkal.

4. Általános koncepció

4.1. Időbélyegzés szolgáltatás

Az időbélyegzés szolgáltatás két szolgáltatási komponensből áll:

a. időbélyeg előállítás,

b. időbélyegzés szolgáltatás menedzsment.

[1] Az ETSI TS 102 023 szabvány által használt Time Stamping Authority Practice Statement fogalomnak felel meg.

Az időbélyegzés szolgáltatást biztosító informatikai rendszer két fő összetevőből áll:

a. az időbélyegeket előállító és kibocsátó egységek,

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

- felügyeli az időbélyegző szerverek működését, kiesés esetén irányítja az áttérést a meleg tartalék szerverre,
- biztosítja az időbélyegző szerverek belső időszinkronját,
- biztosítja a belső időszinkronizálást végző óra négy egymástól független UTC2 időalappal történő időszinkronizálását,
- figyeli az időbélyegző szerver belső órájának a pontossági tartományból való kilépését, ennek bekövetkezés esetén a szolgáltatás leállítását és a hibaüzenet kiadását az előfizetők felé,
- támogatja az installációs, a karbantartási, a naplózási, az archiválási, a mentési és a leállítási műveleteket.

4.2. Időbélyegzés szolgáltató (ISZ)

Az időbélyegzés szolgáltatást biztosító informatikai rendszer üzemeltetője a minősített hitelesítés szolgáltatóként regisztrált MÁV INFORMATIKA Zrt.

4.3. Időbélyeget felhasználó fél

Időbélyeget felhasználó fél (ügyfél, végfelhasználó) lehet:

a. bármely európai uniós állampolgárságú természetes személy, aki az ISZ-el időbélyegzés szolgáltatásra az Általános Szerződési Feltételek Minősített Elektronikus Aláírással Kapcsolatos Szolgáltatásokhoz (továbbiakban: ÁSZF-M) szerint szerződést köt,

b. bármely Európai Unióban bejegyzett cég (jogi személy), amely az ISZ-el időbélyegzés szolgáltatásra az ÁSZF-M szerint szerződést köt.

Időbélyegzés szolgáltatásra az ISZ-el az előzőekben meghatározott bármely ügyfél szerződést köthet, függetlenül attól, hogy számára az elektronikus hitelesítés szolgáltatást a MÁV INFORMATIKA Zrt., vagy más hitelesítés szolgáltató nyújtja.

Természetes személyek önmaguk felelősek a végfelhasználókra vonatkozó szabályok betartásáért.

A jogi személyek által az ISZ-el megkötött szerződésben vállalt, a végfelhasználókra vonatkozó szabályok betartásáért a jogi személy a felelős. Ezért a szerződő jogi személy feladata végfelhasználók tájékoztatása az időbélyegzés szolgáltatásra vonatkozó szabályokról, illetve tájékoztatni őket az ISZ-nek az időbélyegzés szolgáltatásokra vonatkozó elérhetőségeiről.

4.4. Az Időbélyegzés Szolgáltatási Rend és a szolgáltatási szabályzat kapcsolata

Az ISZR célja

Az ISZR az Időbélyegzés Szolgáltatóra, az időbélyegzés szolgáltatásra, valamint az azt támogató informatikai rendszerre vonatkozóan általános követelményeket és szabályokat határoz meg.

A MÁV INFORMATIKA Zrt. az időbélyegzés szolgáltatást a minősített hitelesítés-szolgáltatással együtt kapcsolódó szolgáltatásként, vagy a hitelesítés szolgáltatástól függetlenül önállóan igénybe vehető szolgáltatásként teljesíti az időbélyegzést felhasználó ügyfelek felé. Ezért az ISZR mint önálló és különálló dokumentum határozza meg a követelményeknek és szabályoknak való megfelelést.

A MÁV INFORMATIKA Zrt. mint minősített hitelesítés szolgáltató a minősített hitelesítés szolgáltatásra és a kapcsolódó szolgáltatásokra vonatkozóan rendelkezik szolgáltatási szabályzattal (HSZSZ-M-el), ezért az ISZR-ben meghatározott követelményekhez és általános szabályokhoz kapcsolódó konkrét megoldásokat – így az időbélyegzés szolgáltatás részletes szabályait is – a Szolgáltató HSZSZ-M-je tartalmazza.

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

4.4.1. Az ISZR és a Szolgáltató egyéb kapcsolódó szabályzatai

Az ISZR és az időbélyegzés szolgáltatás működtetése a Szolgáltató szabályzatai közül a következőket érinti:

A szabályzat neve	A szabályzat státusza	A szabályzat hozzáférhetősége
Általános Szerződési Feltételek minősített elektronikus aláírással kapcsolatos szolgáltatásokhoz (ÁSZF-M)	Nyilvános	Interneten közzétéve
Szolgáltatási Szabályzat minősített elektronikus aláírással kapcsolatos szolgáltatásokhoz (HSZSZ-M)	Nyilvános	Interneten közzétéve
A PKI Szolgáltatások Biztonsági Szabályzata	Belső használatra	Csak jogosultsággal bíró belső személyeknek
A PKI Szolgáltatások Informatikai Biztonságpolitikája	Belső használatra	Csak jogosultsággal bíró belső személyeknek
A PKI Szolgáltatások Üzletmenet-folytonossági Terve	Belső használatra	Csak jogosultsággal bíró belső személyeknek

1. táblázat

Az ISZ a fenti szabályzatokkal való harmonizálást a HSZSZ-M 8.1 pontjában előírt változásmenedzsment követelményeknek megfelelően karbantartja.

5. Időbélyegzési rend

5.1. Áttekintés

Az ISZ időbélyegzés szolgáltatásra vonatkozó rendje a következők szerint érvényes:

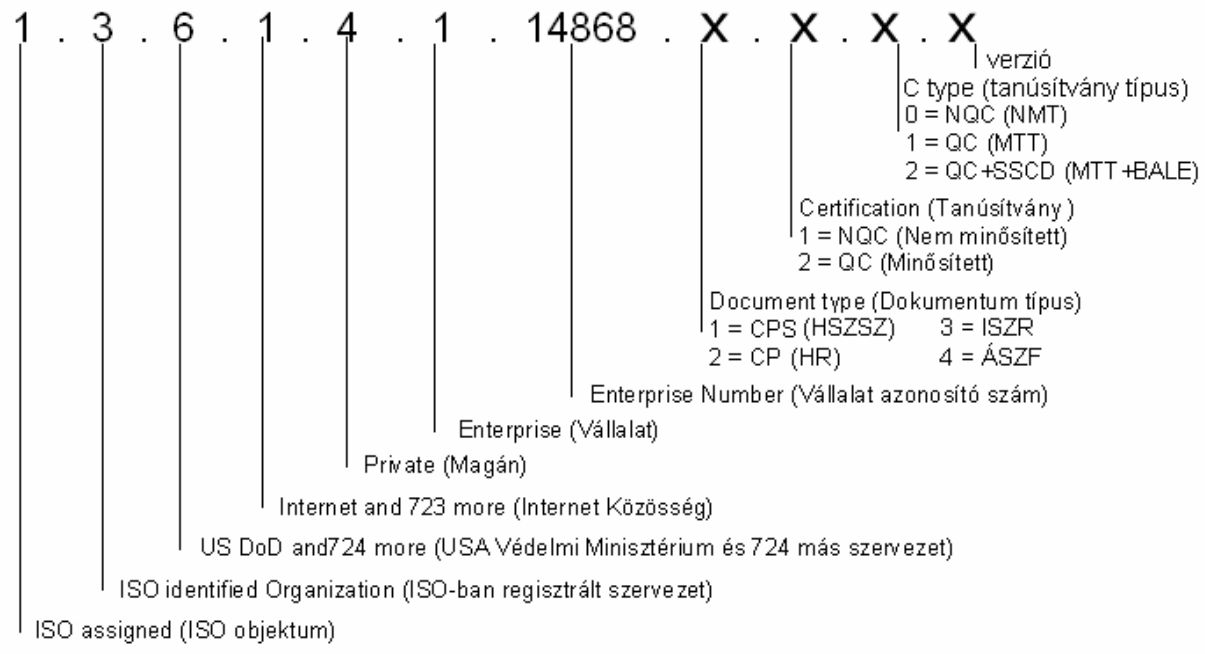
a. Az időbélyegzés szolgáltatást igénybe veheti a Szolgáltatóval szerződéses viszonyban álló természetes vagy jogi személy, függetlenül attól, hogy részére az elektronikus aláírás hitelesítés-szolgáltatást a MÁV INFORMATIKA Zrt. vagy más hitelesítés szolgáltató nyújtja.

b. Az állományok vonatkozásában érvényes mind elektronikus aláírással ellátott, mind el nem látott állományokra.

Az időbélyegzési folyamat során, az ISZ és az időbélyegzés felhasználó közötti kommunikáció protokolljára vonatkozóan, az ISZ betartja az IETF RFC 3161 szabványt; az időbélyegzést támogató szolgáltatói alkalmazásra, valamint az időbélyeg szerkezetére és tartalmára vonatkozóan betartja az ETSI TS 101 861 szabványt. Az időbélyegek tartalmazzák a jelen ISZR objektum azonosítóját (OID) és az időbélyeg kibocsátás pontosságát. A időbélyeget a Szolgáltató elektronikus aláírással hitelesíti. Az időbélyeget aláíró szolgáltatói kulcs tanúsítványát a MÁV INFORMATIKA Zrt., mint fölérendelt hitelesítés szolgáltató adja fokozott biztonságú eszköz tanúsítványként.

5.2. Az ISZR azonosítása

Az ISZR-t objektumként értelmezve OID-vel azonosítjuk. Az időbélyegekben megadott ISZR OID felépítését az 1. ábra mutatja meg.



1. ábra

Jelen dokumentum teljes neve: **A MÁV INFORMATIKA Zrt. Időbélyegzés Szolgáltatási Rendje.**

A jelen dokumentumban ISZR-ként történik rá hivatkozás.
Az ISZR nyilvános dokumentum, amely a Szolgáltató internetes honlapján keresztül érhető el.

Jelen ISZR-nek csak a Szolgáltató aláírásával ellátott változata tekinthető hitelesnek.

5.3. Felhasználó közösség és alkalmazhatóság

Az időbélyegzés szolgáltatást minden, a 4.3 pontban meghatározott szerződéses fél igénybe veheti, függetlenül attól, hogy az időbélyeget nyilvános vagy zárt körben használja.

5.4. Megfelelés

Az ISZ a hatályos jogszabályoknak, a nemzetközi ajánlásoknak és a belső szabályzatainak való megfelelést függetlenül belső és külső auditorok által rendszeresen elvégzett vizsgálatokkal biztosítja, amelyek gyakoriságára, módjára, kiterjedésére és a hiányosságok kezelésére vonatkozóan a HSZSZ-M 2.7 pontja rendelkezik.

6. Kötelezettségek és felelősségek

6.1. Az Időbélyegzés Szolgáltató kötelezettségei

Az ISZ-nek kötelezettségei vannak:

a. az előfizetők és az időbélyeg felhasználók,

b. a Nemzeti Hírközlési Hatóság (továbbiakban: NHH), mint hatóság,

felé.

6.1.1. Általános kötelezettségek

Az ISZ kötelezettséget vállal arra, hogy szolgáltatásaiban érvényesíti a jelen ISZR-t, betartja az 5.1 pontjában meghatározott szabványokat, a 7.4.10 pontban meghatározott jogszabályokat, valamint az időbélyegzésre vonatkozó azon szabályokat, amelyeket a 4.4.1 pontban felsorolt kapcsolódó szabályzatai rögzítenek.

6.1.2. Az ISZ kötelezettségei az időbélyeget felhasználók felé

Az ISZ a következőkre vállal kötelezettséget az időbélyeget felhasználók felé:

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

b. a kibocsátott időbélyeg nem tartalmaz hibás adatot,

c. időbélyeget aláíró szolgáltatói kulcsot csak az időbélyegzés keretén belül használja,

d. az időbélyeget 1 másodpercen belüli pontossággal adja ki,

e. az időbélyegzési rendszer belső óráját 0,1 másodperc pontossággal szinkronizálja az UTC időalaphoz.

f. az időbélyegzés szolgáltatás biztonságát a minősített hitelesítés szolgáltatókra vonatkozó követelmények szerint biztosítja,

g. rögzít az időbélyegzéssel kapcsolatos minden fontos eseményt, ezeket naplózza és a napló állományokat biztonságosan archiválja.

h. alvállalkozói felé érvényesíti, hogy azok a 4.4.1 pontban felsorolt szabályzatokkal összhangban nyújtsák szolgáltatásaikat. Ennek betartását az ISZ az alvállalkozóknál rendszeresen ellenőrzi.

6.1.3. Az ISZ kötelezettségei az NHH felé

Az ISZ a következő kötelezettségeket teljesíti az NHH, mint hatóság felé:

a. fenntartja a minősített szolgáltatókra előírt biztonsági szintet,

b. betartja az Eat. és a 3/2005. (III. 18.) IHM. rendeletben az NHH, mint hatóság felé előírt bejelentési kötelezettségeket,

c. az NHH felügyeleti ellenőrzései során tett észrevételeknek megfelelően a szükséges módosításokat az előírt határidőre elvégzi.

6.2. Az időbélyeget felhasználók feladatai

Az időbélyeget felhasználók feladata a kért időbélyeg vétele után meggyőződni az időbélyeg aláírás helyességéről és az aláíró kulcs tanúsítványának érvényességéről. Ennek módját részletesen a HSZSZ-M 2.1.3 pontja tartalmazza.

6.3. Az Érintett fél felelőssége

Az Érintett fél feladataira általában érvényesek a HSZSZ-M 2.1.3, a felelősségére a HSZSZ-M 2.2.3 pontjában leírt szabályok.

Egy időbélyeggel ellátott állomány vétele után az Érintett félnek ellenőriznie kell az ISZ általi aláírás megtörténtét, az ISZ Tanúsítvány érvényességét a Visszavont Tanúsítványok Listája segítségével a HSZSZ-M 2.1.3 pontjában leírt módon.

6.4. Felelősség

Az ISZ felelősségére és a saját hibájából adódó kár megtérítésére vonatkozóan a HSZSZ-M 2.2.1 és a 2.3. pontjai érvényesek.

7. Az ISZ működési követelményei

7.1. Szolgáltatási és a közzétételi szabályozás

7.1.1. Időbélyegzés szolgáltatás szabályozása

Az időbélyegzés szolgáltatást a MÁV INFORMATIKA Zrt. a PKI Szolgáltató Egységen belül, egy olyan időbélyegző informatikai alrendszerrel biztosítja, amely a minősített elektronikus aláírás hitelesítést szolgáltató informatikai rendszerrel közös fizikai környezetben működik.

Az időbélyegzés szolgáltatást a Szolgáltató folyamatosan (az év minden napján, 24 órában), 99,9%-os rendelkezésre állással biztosítja úgy, hogy a szolgáltatás kiesése esetenként nem lépheti túl a 3 órás időtartamot.

A MÁV INFORMATIKA Zrt.-t a Hírközlési Felügyelet 2003 április 3-án minősített hitelesítés-szolgáltatóként regisztrálta. A fentiek alapján az időbélyegző informatikai alrendszer, annak fizikai és személyi környezete megfelel a minősített hitelesítés szolgáltatási követelményeknek. A megfelelést biztosító technikai, működtetési, menedzselési és biztonsági megoldásokat és szabályokat a HSZSZ-M rögzíti. A HSZSZ-M megfelelő pontjai tartalmazzák az időbélyegzés szolgáltatás következő vonatkozásait is:

- Szolgáltató és felhasználó közösség, alkalmazhatóság (HSZSZ-M 1.4 pont),
- Feladatok és hatáskörök (HSZSZ-M 2.1 pont),
- A szolgáltató és felhasználó közösség tagjainak felelőssége (HSZSZ-M 2.2 pont),
- Az anyagi felelősség mértéke (HSZSZ-M 2.3 pont),
- Irányadó jog (HSZSZ-M 2.4.1 pont),
- Érvénytelenség, hatályosság, megszűnés, értesítések (HSZSZ-M 2.4.2 pont),
- Közzététel (HSZSZ-M 2.6 pont),
- A megfelelőség vizsgálata (HSZSZ-M 2.7 pont),
- Azonosítás és hitelesítés (HSZSZ-M 3. pont),
- A működésre vonatkozó követelmények (HSZSZ-M 4. pont),
- Biztonsági audit eljárások (HSZSZ-M 4.7 pont),
- Adatarchiválás (HSZSZ-M 4.8 pont),
- A folyamatos üzemmenet biztosítása (katasztrófa elhárítás) (HSZSZ-M 4.9 pont),
- Hitelesítés-szolgáltatási tevékenység megszüntetése (HSZSZ-M 4.10 pont),
- Fizikai, eljárásrendi, és humán biztonsági szabályozások (HSZSZ-M 5. pont),
- Kulcspár előállítás (HSZSZ-M 6.1.1 pont),
- Aláírás-létrehozó adat védelme (HSZSZ-M 6.2 pont),
- Számítógép biztonsági szabályok (HSZSZ-M 6.5 pont),
- Életciklus technikai szabályok (HSZSZ-M 6.6 pont),
- Kriptográfiai modul ellenőrzése (HSZSZ-M 6.8 pont),
- Tanúsítvány és kulcs-visszavonási profil (HSZSZ-M 7. pont).

7.1.2. Közzétételi nyilatkozat

Az ETSI TS 102 023 szabvány 7.1 pontja szerint az ISZ-nek az időbélyegzés szolgáltatás használatával kapcsolatos információkat és feltételeket tartalmazó közzétételi nyilatkozatot kell nyilvánosan elérhetővé tennie.

Az időbélyegzési renddel kapcsolatosan az ISZ a 2. táblázat szerinti nyilatkozatot teszi közzé, amely a szolgáltatás honlapján keresztül érhető el.

A szabály megnevezése	A szabály kifejtése
Időbélyegzés szolgáltatás szabályozása	Időbélyegzés szolgáltatás részletes szabályait a MÁV INFORMATIKA Zrt. „Szolgáltatási Szabályzat minősített elektronikus aláírással kapcsolatos szolgáltatásokhoz” című dokumentuma (HSZSZ-M) tartalmazza.
A Szolgáltató elérhetősége	**Név:** MÁV INFORMATIKA Kereskedelmi, Szolgáltató és Tanácsadó Zártkörűen Működő Részvénytársaság **Cégjegyzék szám:** 01-10-045838 **Székhely:** 1012 Budapest, Krisztina krt. 37/a. **Levélcím:** 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:** Nemzeti Fogyasztóvédelmi Hatóság Közép-magyarországi Regionális Felügyelősége 1052 Budapest, Városház u. 7. Telefon: 318-2681, telefax: 318-1639, Email: *fogyasztovedelem@pest.b-m.hu* Fogyasztókapcsolati Iroda 1088 Budapest, József krt. 6. Telefonszám: + 36 1 459 4999, +36 1 459 4836 Ingyenes zöldszám: +36 80 201 205, Telefax: +36 1 303 9075 **Ügyfélkapcsolati Iroda:** A központi Ügyfélkapcsolati Iroda címe: Budapest, I. Krisztina krt. 37/a. tel.: +36-1-457-95-78 e-mail: *hiteles@mavinformatika.hu* A területi ügyfélkapcsolati irodák címe és elérhetősége a Szolgáltatás Internetes honlapján keresztül érhető el. **Ügyfélszolgálat: tel.:** központi szám: +36-1-457-93-00, közvetlen szám: +36-1-457-93-93, zöldszám +36 80 39-93-93, **e-mail:** *helpdesk@mavinformatika.hu* **Panaszok bejelentésének helye:** személyesen az ügyfélkapcsolati irodán, írásban a Szolgáltató telephelyére címezve, telefonon és faxon az ügyfélkapcsolati irodán vagy az ügyfélszolgálatnál, elektronikus levélben az ügyfélszolgálat e-mail címére.
ISZR azonosító (OID)	1.3.6.1.4.1.14868.3.5
Alkalmazható hash algoritmus	2/2002. (IV.26) MeHVM irányelv 1. melléklet 2. táblázata szerint
Az időbélyegben szereplő idő pontossága	Összhangban a 2/2002. (IV.26) MeHVM irányelv 219. pontjával, az UTC-vel szinkronizált idő pontossága: 1 másodpercen belül van.

A szabály megnevezése	A szabály kifejtése
Az időbélyegzés alkalmazhatóságának korlátjai	Természetes személy előfizető: az Európai Unió állampolgára Jogi személy előfizető: az Európai Unióban bejegyzett cég. Az időbélyegzés szolgáltatás igénybevételéhez érvényes NHH által regisztrált hitelesítés szolgáltató által kibocsátott, azonosítás-hitelesítésre alkalmas Tanúsítvány vagy egyéb, az előfizető egyértelmű azonosítását lehetővé tevő adat (pl. felhasználónév és jelszó) szükséges.
Az időbélyeg ellenőrzés módja	Egy időbélyeggel ellátott állomány vétele után indokolt meggyőződni az időbélyeg aláírás helyességéről és a szolgáltatói aláíró kulcs tanúsítványának érvényességéről a HSZSZ-M 2.1.3 pontjában leírt módon.
Időbélyegző rendszer naplók archiválási időtartama	A 3/2005. (III. 18.) IHM. rendelettel összhangban az archivált naplókat keletkezésüktől számított 10 évig, illetőleg a velük kapcsolatban esetlegesen felmerült jogvita jogerős lezárásáig megőrződnek meg kell őrizni.
Hatályos jogszabályok az időbélyegzés vonatkozásában	♦ 2001. évi XXXV. törvény az elektronikus aláírásról. ♦ 3/2005. (III. 18.) IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről. ♦ 2/2002. (IV.26) MeHVM irányelv a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről. ♦ 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról. ♦ 1995. évi CXXII. törvény a polgárok személyes adatainak nyilvántartásáról szóló 1992. évi LXVI. törvény módosításáról szóló törvény. ♦ 1996. évi LVII. törvény a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról.
Az ISZ felelősségének korlátozása	Az ISZ felelősségéből adódó kár megtérítésére vonatkozóan az ÁSZF-M 5.1.1 pontja érvényes.
Eljárás jogi viták rendezésére	A jogi viták rendezésére az ÁSZF-M 9. pontja érvényes
Nyilvántartásba vételi eljárás	Nemzeti Hírközlési Hatóság

2. táblázat

7.2. A kulcsmenedzsment életciklusa

7.2.1. Az ISZ kulcs generálása

A szolgáltatói kulcspár generálása a 3/2005. (III. 18.) IHM. rendeletnek és a 2/2002. (IV.26) MeHVM irányelv 212. pontjának megfelelően az NHH által regisztrált tanúsító cég által tanúsított, az NHH által nyilvántartásba vett kriptográfiai modulban történik. Lásd részletesebben: HSZSZ-M 6.1.1 pont.

A kulcspár előállítás fizikai védelme és személyi környezete megfelel a minősített hitelesítés szolgáltatókra vonatkozó követelményeknek. Lásd részletesebben: HSZSZ-M 5. pont.

7.2.2. Az időbélyegző egység kulcsának védelme

Az időbélyegző egység aláíró kulcsa egy, a 3/2005. (III. 18.) IHM. rendeletnek és a 2/2002. (IV.26) MeHVM irányelv 212. pontjának megfelelően az NHH által regisztrált tanúsító cég által tanúsított, az NHH által nyilvántartásba vett kriptográfiai modulban történik. Lásd részletesebben: HSZSZ-M 6.2 pont.

Az időbélyegző egység aláíró kulcsának fizikai védelme és személyi környezete megfelel a minősített hitelesítés szolgáltatókra vonatkozó követelményeknek. Lásd részletesebben: HSZSZ-M 5. pont.

7.2.3. Az időbélyegző egység nyilvános kulcsának közzététele

Az időbélyegző egység nyilvános kulcsa és tanúsítványa a szolgáltató internetes honlapján keresztül érhető el.

7.2.4. Az időbélyegző egység kulcsának megújítása

Az időbélyegző egység kulcsának megújítása tanúsítványa érvényességi idejének lejártakor történik, hacsak addig a kulcs nem kompromittálódott. A kulcs megújítás szabályait részletesen a minősített HSZSZ-M 4.7 pontja, a kompromittálódás elkerülésére foganatosított, illetve a bekövetkezés esetén megvalósítandó intézkedéseket részletesen a HSZSZ-M 4.8 pontja és a PKI Szolgáltatások Üzletmenet-folytonossági Terve tartalmazza.

7.2.5. Az időbélyegző egység kulcsmenedzsment életciklusának vége

Az időbélyegző egység kulcsmenedzsment életciklusa következő esetekben fejeződik be:

1. a kulcs és tanúsítványának érvényességi ideje lejár,
2. a kulcs kompromittálódik,
3. katasztrófa esemény vagy a MÁV INFORMATIKA Zrt. minősített Root CA aláíró kulcsának kompromittálódása miatt a szolgáltatás befejeződik.

Az 1. esetben a kulcs megújításra kerül a 7.2.4. pont szerint.

A 2. esetben a tanúsítványt azonnal vissza kell vonni és az aláíró kulcsot meg kell semmisíteni.

7.2.6. Az időbélyeget aláíró kripto-modul életciklus menedzsmentje

A jelen ISZR 7.2.2 pontjában meghatározott követelményeknek megfelelő időbélyeget aláíró kripto-modul a HSZSZ-M 5.1.1 pontjában ismertetett, fokozott biztonsági szintű Bizalmi Központban, egy a MÁV INFORMATIKA Zrt. vezetése által felállított bizottság előtt került installálásra és üzembe helyezésre. A bizottság az üzembe helyezés előtt ellenőrizte a kripto-modul sértetlenségét.
A kripto-modul üzemeltetése a Bizalmi Központban történik a minősített hitelesítés-szolgáltatás követelményeinek megfelelő körülmények között és személyzet által.

Az időbélyeget aláíró kripto-modul rendszerből történő kivonása esetén az időbélyeget aláíró kulcsot bizottság előtt meg kell semmisíteni.

7.3. Időbélyegzés

Időbélyeg

Az időbélyeg felépítése megfelel az IETF RFC 3161 szabványnak és a jelen ISZR-ben meghatározott egyéb követelményeknek a következők szerint:

- tartalmazza az 5.2 pontban meghatározott ISZR azonosítót,
- tartalmazza az időbélyeg egyedi azonosítóját,
- az időbélyegben megadott időpontot négy, egymástól független forrásból származó UTC időalappal szinkronizált és a 7.1.2 pontbeli közzétételi nyilatkozatban meghatározott, - 1 másodpercen belüli - pontossággal rendelkező belső óra adja,
- az időbélyegző szerver belső órájának pontosságát a HSZSZ-M 4.3 pontjában részletesen ismertetett belső és külső szinkronizáló eljárás biztosítja;
- a külső szinkron háromszorosan tartalékolt és az egyes órajelek esetleges manipulációját ezen redundancia segítségével egy belső kontroll szűri ki;
- a belső órajel hitelességét az időbélyegző alrendszer indításakor egy erre a célra összehívott bizottság tanúsítja;
- üzemközben a belső óra hitelességét a redundáns külső UTC időalapokkal a bizottság által történő összevetés és egy a rendszertől független GPS kapcsolaton keresztül történő, referenciaként használt UTC időlekérdezés biztosítja,
- az ISZ által visszaküldött időbélyeg a kérelmező üzenete által meghatározott adatokat tartalmazza;
- a kérelem része az időbélyeggel ellátandó adat hash lenyomata is;
- az ISZ az időbélyeget csak az időbélyegzés céljára kiadott aláíró kulccsal írja alá,

- az időbélyeg egy olyan ISZ névmegadást tartalmaz, amely tartalmazza:
  - az ISZ országának nevét (C),
  - az ISZ azonosítóját (CN),
  - az időbélyeget kibocsátó egység nevét (O, OU)

7.3.1. Óraszinkronizálás az UTC-vel

Az időbélyegző alrendszer belső órájának a pontossági tartományon belül maradását a HSZSZ-M 4.3 pontjában ismertetett belső és külső szinkronizációs eljárás biztosítja.

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

Ha a hitelességgel kapcsolatban kétely merül fel, akkor az időbélyegző alrendszer indítását hitelesítő bizottság összehívásra kerül és ellenőrzi a külső UTC idők hitelességét, amelyhez egy független GSM kapcsolaton keresztül kapott UTC időt használ referenciaként.

Az időbélyegzés belső órájának pontossága folyamatos ellenőrzés alatt áll. Amennyiben a nagy megbízhatóságú időszinkronizálás ellenére a belső óra pontossága az előírt 1 másodperces tartományból kiesne, az időbélyegzés szolgáltatás leáll, és a hiba kijavításáig minden további kérésre hiba üzenetet küld az előfizetők felé. Ez súlyos üzemzavarnak („B" osztályú eseménynek) minősül, amelyre a PKI Szolgáltatások Üzletmenet-folytonossági Terve tartalmazza az intézkedéseket.

A szolgáltatás az időbélyegző szerver belső órája által egymás után kétszer helyesen vett időszinkronnal indul.

A Szolgáltató a fenti szinkronizációs és ellenőrzési mechanizmusokkal biztosítja a 2/2002. (IV.26) MeHVM irányelv 219. pontjának való megfelelőséget.

Az időbélyegző alrendszer fizikai védelme fokozott szinten biztosított, mert abban a Bizalmi Központban került elhelyezésre, amelyben a minősített hitelesítés szolgáltató rendszer is üzemel. Az időbélyegző alrendszerrel kapcsolatos biztonsági követelményeket, amelyek a megvalósítás során teljesültek, a melléklet tartalmazza.

7.4. Időbélyegzés szolgáltatás menedzsment és működtetés

7.4.1. Biztonságmenedzsment

Mint azt a jelen ISZR 7.1.1 pontja tartalmazza, az időbélyegzés szolgáltatás a hitelesítés szolgáltatással azonos fizikai, szabályozási és személyi környezetben történik, amely megfelel a minősített hitelesítés szolgáltatói követelményeknek.

A biztonságmenedzsment teljes területére a HSZSZ-M 2.8 (Bizalmasság - Adatkezelési Szabályzat), 4.7 (Biztonsági audit eljárások), 4.9 (Katasztrófa elhárítás, Aláírás létrehozó adat kompromittálódás), 5. (Fizikai, eljárásrendi, és humán biztonsági szabályozások), 6.7 (Hálózati biztonsági szabályok) pontjai vonatkoznak.

A biztonságmenedzsment szabályozási hátterét képezik:

a. a PKI Szolgáltatások Informatikai Biztonságpolitikája,

b. a PKI Szolgáltatások Biztonsági Szabályzata,

c. a PKI Szolgáltatások Üzletmenet-folytonossági Terve.

7.4.2. Az eszközök biztonsági osztályba sorolása és menedzsmentje

A PKI Szolgáltatások Informatikai Biztonságpolitikája szerint az időbélyegzést támogató informatikai alrendszer biztonsági osztálybasorolása a következő:

Információvédelem szempontjából	FOKOZOTT BIZTONSÁGI OSZTÁLY
Megbízható működés szempontjából	KIEMELT BIZTONSÁGI OSZTÁLY

Ez megfelel a MeH ITB 12. ajánlás és az ITSEC szerinti biztonsági osztálybasorolásnak.

A minősített hitelesítés szolgáltató rendszerre, annak fizikai és személyi környezetére vonatkozó biztonsági követelményeket a szolgáltató „A minősített hitelesítés szolgáltatás komplex biztonsági követelményrendszere" című dokumentuma tartalmazza. A melléklet ebből az előfizetők számára legfontosabb biztonsági követelményeket tartalmazza.

Ennek, valamint a 3/2005. (III. 18.) IHM. rendeletnek és a 2/2002. (IV.26) MeHVM irányelv 212. pontjának megfelelően a MÁV INFORMATIKA Zrt. PKI projektje keretén belül megtörtént a teljes hitelesítés-szolgáltató rendszer, annak fizikai és személyi környezetének kockázatelemzés alapú vizsgálata.

A MÁV INFORMATIKA Zrt. társasági szintű biztonságpolitikájának és szabályzatának, valamint a PKI Változásmenedzsment Szabályzatának megfelelően a hitelesítés és az időbélyegzés szolgáltatást támogató informatikai rendszer hardver és szoftver elemei leltárba lettek véve, amelynek a karbantartása változásmenedzsment keretében valósul meg.

7.4.3. Személyi biztonság

A személyi biztonság megfelel a 7.4.2 pontban meghatározott biztonsági követelményeknek és az ezekkel harmonizáló minősített szolgáltatói követelményeknek.

A személyi biztonság követelményeinek való megfelelést részletesen a HSZSZ-M 5.2 és 5.3 pontjai írják le.

7.4.4. A fizikai infrastruktúra biztonsága

A fizikai infrastruktúra biztonsága megfelel a 7.4.2 pontban meghatározott biztonsági követelményeknek és az ezekkel harmonizáló minősített szolgáltatói követelményeknek.

A személyi biztonság követelményeinek való megfelelést részletesen a HSZSZ-M 5.1 pontja írja le.

7.4.5. Működtetés menedzsment

A működtetés menedzsment a minősített szolgáltatói követelményeknek felel meg.

A működtetés menedzsmentre érvényesek a MÁV INFORMATIKA Zrt. által üzemeltett informatikai rendszerre alkalmazott társasági szintű működtetés menedzsment szabályok. Ezeken túlmenően az időbélyegzést támogató informatikai rendszerre vonatkozóan a működtetés menedzsmentet a PKI Üzemeltetési Kézikönyv és a HSZSZ-M 4., 5. és 6. pontjai szabályozzák.

7.4.6. Hozzáférés menedzsment

A hozzáférés menedzsment megfelel a fokozott biztonsági és a minősített szolgáltatói követelményeknek.

A működtetés menedzsmentre érvényesek a MÁV INFORMATIKA Zrt. társasági szintű, illetve a PKI Üzleti Egység vonatkozó szabályzatai, amelyek a következők:

a. a MÁV INFORMATIKA Zrt. Informatikai Biztonságpolitikája,
b. a MÁV INFORMATIKA Zrt. Informatikai Biztonsági Szabályzata,
c. A PKI Szolgáltatások Informatikai Biztonságpolitikája,
d. A PKI Szolgáltatások Biztonsági Szabályzata.

7.4.7. A biztonságos rendszer bevezetése és karbantartása

A biztonságos időbélyegzés szolgáltatás bevezetése és karbantartása érdekében a MÁV INFORMATIKA Zrt.:

- elvégezte a teljes hitelesítés és időbélyegzés szolgáltató rendszer, annak fizikai és személyi környezetének kockázatelemzés alapú vizsgálat, amelynek eredményeit egy vizsgálati jelentés tartalmazza,
- kidolgozta a szolgáltató rendszer megvalósítása előtt a minősített szint eléréséhez szükséges biztonsági követelményeket,
- a biztonságos rendszer karbantartása a napi operatív, valamint a rendszeres tervezett biztonsági auditok, az ezek nyomán elvégzett korrekciós, valamit a változásmenedzsment intézkedésekkel történik.

7.4.8. Az ISZ kompromittálódása

Az ISZ a következő esetekben kompromittálódik:

1. a MÁV INFORMATIKA Zrt. minősített Root CA aláíró kulcs kompromittálódása,
2. az ISZ aláíró kulcs kompromittálódása,
3. Az ISZ időalap kalibrációjának elvesztése

esetén.

Mindegyik esetben az időbélyegzés szolgáltatást fel kell függeszteni mindaddig, amíg új és érvényes ISZ aláíró kulcs, tanúsítvány, illetve pontosan kalibrált időalap nem áll rendelkezésre. A felfüggesztésről az Interneten a *http://www.mavinformatika.hu/ca/* web lapon keresztül tájékoztatni kell a szerződéses ügyfeleket és az érintett feleket a felfüggesztés tényéről és okáról.

Az 1. és 2. kulcs kompromittálódás esetei katasztrófa („A" osztályú) eseménynek, a 3. eset súlyos üzemzavarnak („B" osztályú eseménynek) minősülnek, amelyek kezelésére a HSZSZ-M 4.8 pontja és a PKI Szolgáltatások Üzletmenet-folytonossági Terve tartalmazza az intézkedéseket.

7.4.9. Az ISZ működésének befejezése

Az ISZ befejezi működését, ha a MÁV INFORMATIKA Zrt. tulajdonosa és vezetése ilyen határozatot hoz. Az ISZ működése befejezésének oka lehet katasztrófa szintű vagy más esemény, amelynek következtében megszüntető határozat születik.

Az ISZ működése felfüggesztésének oka lehet az NHH, mint hatóság felfüggesztő határozata.

7.4.10. Jogszabályoknak való megfelelés

A jogszabályi megfelelés vonatkozásában lásd a 7.1.2 pont (Közzétételi nyilatkozat) erre vonatkozó sorát.

7.4.11. Az időbélyegzés szolgáltatás működtetésével kapcsolatos adatok rögzítése

Az időbélyegzéssel kapcsolatosan a következő adatok kerülnek rögzítésre:

a. az időbélyegzés szolgáltatás fő lépései, a kérelemtől az időbélyeg válasz elküldésig,

b. az ISZ aláíró kulcs életciklusában bekövetkező események (generálás, használat, visszavonás, megsemmisítés),

c. az ISZ aláíró kulcs tanúsítványa életciklusában bekövetkező események (kiadás, használat, visszavonás).

d. a rögzített adatok a HSZSZ-M 4.7.3 pontjával összhangban naponta naplózásra és tárolásra kerülnek. A naplók értékelése naponta megtörténik. A tárolt naplók archiválása a HSZSZ-M 4.8 pontjával összhangban történik.
Az archivált adatok megőrzési ideje 10 év.

7.5. Szervezeti séma

Az időbélyegzés szolgáltatást a MÁV INFORMATIKA Zrt. PKI Szolgáltató Egység végzi.

8. Meghatározások és rövidítések

8.1. Meghatározások

A jelen ISZR a 2001. évi XXXV. törvény és a 3/2005. (III. 18.) IHM. rendelet és a 2/2002. (IV. 26) MeHVM irányelv által használt alapfogalmakat használja, amelyek meghatározását a HSZSZ-M 9.2 pontja tartalmazza.

8.2. Alkalmazott jelölések

ÁSZF-M: Általános Szerződési Feltételek Minősített Elektronikus Aláírással Kapcsolatos Szolgáltatásokhoz

HSZSZ-M: Szolgáltatási Szabályzat Minősített Elektronikus Aláírással Kapcsolatos Szolgáltatásokhoz

ISZR: Időbélyegzés Szolgáltatási Rend

ISZ: Időbélyegzés Szolgáltató (jelen dokumentumban a MÁV INFORMATIKA Zrt.)

NHH: Nemzeti Hírközlési Hatóság

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

CRL: Certificate Revocation List, magyarul: Visszavont Tanúsítványok Listája

Melléklet

Az időbélyegzést szolgáltató alrendszer informatikai biztonsági követelményei

Az ISZR 7.4.2 pontjában meghatározott biztonsági osztálybasorolás szerint információvédelmi szempontból az időbélyegzés szolgáltatást biztosító informatikai rendszernek, valamint annak fizikai és személyi környezetének a fokozott biztonsági szint követelményeinek kell megfelelniük.

Ezen követelményeket részletesen a szolgáltató „A minősített hitelesítés szolgáltatás komplex biztonsági követelményrendszere” című dokumentuma tartalmazza.

Itt csak az előfizetők szempontjából legfontosabb követelményeket emeljük ki.

Fizikai biztonsági követelmények

A hitelesítő központok és időbélyegző egységek legmagasabb védelmi szintet képező objektuma a Bizalmi Központ, amely a biztonsági szempontból legkritikusabb hardver/szoftver modulokat tartalmazza Az objektum fizikai védelme kielégíti a MeH ITB 12. ajánlás szerinti fokozott biztonsági osztály védelmi követelményeit. A Bizalmi Központ:

a. a fokozott biztonsági szintnek megfelelő szilárdságú határoló felületekkel határolt, ajtói MABISZ minősítéssel rendelkeznek, nyitásukra kulcskezelés szabályozás érvényes

b. előtte biztonsági szegmens van kialakítva, amelybe anti-passback és naplózási tulajdonságokkal bíró beléptető rendszeren keresztül lehet csak bejutni. A bejutást video biztonsági kamerás rendszer figyeli, amelynek személyes felügyelete folyamatosan biztosított,

c. rendelkezik önálló és kettőzött klimatizálással, mozgásérzékelő, tűz-, víz- és füstjelző és tűzoltó rendszerrel, szünetmentes tápáramellátó rendszerrel, az MSZ 274/5T:1993 szabvánnyal összhangban LPZ2 zónahatárig kiépített másodlagos villámvédelemmel valamint 60 DB elnyomással rendelkező EMC védelemmel

d. a Bizalmi Központban a szerverek biztonsági kabinetekben vannak elhelyezve

e. a Bizalmi Központba csak a Biztonsági Szabályzatban meghatározott szerepkörű vezetők és munkatársak léphetnek be meghatározott céllal,

f. a mentési és a primer szoftver adathordozók, a nyers- és a megszemélyesített aláírás-létrehozó eszközök besugárzás és fizikai behatás ellenálló biztonsági szekrényekben vannak tárolva

g. az informatikai rendszer két független nyomvonalon vezetett üvegkábellel kapcsolódik az Internethez,

h. a lokális telefonkapcsolat az EMC zónahatáron szűrőn keresztül kapcsolódik a szolgáltató telefonközpontjához.

Az időbélyegző szerver hálózati szintű biztonságát a következő intézkedésekkel kell biztosítani:

a. leválasztás az Internetről tűzfallal,

b. az időbélyegző szerver számára a tűzfalon egy önálló, a többi biztonsági szegmenstől különböző szegmenst kell létrehozni.

A környezetei elemek, rendszerek állapotjellemzőit monitor rendszer figyeli. A bekövetkező események naplózásra, majd archiválásra kerülnek.

Logikai biztonsági követelmények

Az időbélyegző szerverhez hozzáférési jogosultsággal rendelkező üzemeltetők azonosítása-hitelesítése a MEH ITB szerinti fokozott biztonsági szintnek megfelelő azonosítás-hitelesítés politika szerint történik.

A hozzáférés szabályozását alapvetően az időbélyegző szerver operációs rendszere (Windows 2000) határozza meg. A Windows 2000 által nyújtott beállítási lehetőségek figyelembe vételével a fokozott biztonsági szintnek megfelelő beállításokat kell alkalmazni.

Ugyanez érvényes a naplózási és az audit politikára is.

Személyi biztonsági követelmények

A személyek vonatkozásában ugyanazokat a követelményeket kell érvényesíteni a munkakörbe, illetve a szerepkörbe történő kiválasztásnál, a bizalmi szerepkörök szétválasztásánál, a képzettségi szint és a gyakorlat meghatározásánál, mint amelyek a HSZSZ-M 5.2 és 5.3 pontjaiban szerepelnek.

Rendelkezésre állás

Az időbélyegzés szolgáltatást támogató informatikai rendszer megbízható működés szempontjából kiemelt biztonsági osztályba sorolt.

Ez – folyamatos üzemet feltételezve – 99,9%-os rendelkezésre állási követelményt jelent. Egy éves üzemidőre vetítve 8,5 óra időbélyegzés szolgáltatás kiesés engedhető meg jelent úgy, hogy egy kiesés nem lehet hosszabb, mint 3 óra.

E követelmény kielégítése az időbélyegző szerverek meleg tartalékolásával és a nagy megbízhatóságú rendszert menedzselő szoftver alkalmazásával, illetve súlyos üzemzavar (vagy természeti katasztrófa) esetén egy földrajzilag távol eső hidegtartalékolt időbélyegző egység rendszerbe állításával biztosítható.