MÁV INFORMATIKA

Kereskedelmi, Szolgáltató és Tanácsadó Kft.

Trust&Sign

Időbélyegzés Szolgáltatási Politika

Verziószám	**1.2**
Hatálybalépés dátuma	**2004. március 1.**

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

A dokumentum neve	Időbélyegzés Szolgáltatási Politika*
Verziószám	1.2
Üzemelő időbélyegző szoftver verzió-szám (Technikai azonosító)	Trust&Sign TSA V1.0
Nemzeti Hírközlési Hatóság regisztrá-ciós szám	MH-10145-6/2003
Időbélyegzés Szolgáltatási Politika ob-jektum azonosító (OID)	1.3.6.1.4.1.14868.3
Első hatálybalépés időpontja	2003. 08. 15.
Aktuális változat hatálybaléptetés időpontja	2004. 03. 01.
Következő felülvizsgálat időpontja:	2005. 01. 31.

* A MÁV INFORMATIKA Kft. Időbélyegzés Szolgáltatási Politikája megfelel az elektronikus aláírásról szóló 2001. évi XXXV. törvénynek, az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről szóló 16/2001. (IX. 1.) MeHVM rendeletnek, a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről szóló 2/2002. (IV.26) MeHVM irányelvnek, valamint követi az időbélyegzés szolgáltatókra vonatkozó követelményekről szóló ETSI TS 102 023 EU szabványt.

.

Időbélyegzés Szolgáltatási Politika verziók

Verzió	Dátum	A változás leírása	Hatálybalépés dátuma	Készítette
1.0	2003.05.27	Az Időbélyegzés Szolgáltatási Politika véglegesítésre előkészített változata.		Bodlaki Ákos
1.1	2003.07.29	Minősítési eljárásra beadott 1.0 változattal kapcsolatos észrevételekkel módosítva.	2003.08.15.	Bodlaki Ákos
1.2	2004. 01. 21.	Felülvizsgált, módosított változat	2004. 03. 01.	Néder Ferenc

TARTALOMJEGYZÉK

1. Bevezetés

A MÁV INFORMATIKA Kft. (továbbiakban: Időbélyegzés Szolgáltató vagy Szolgáltató, röv.: 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 fokozott, illetve minősített aláírással ellátott, valamint elektronikusan nem aláírt állományokhoz is.

Ezen Időbélyegzés Szolgáltatási Politika (továbbiakban: ISzP) meghatározza az ISz által nyújtott időbélyegzés szolgáltatásban résztvevőket, azok 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 ISzP az ISz-re, az időbélyegzés szolgáltató rendszerre és a szolgáltatásra vonatkozó általános követelményeket határozza meg. Ezen követelményeknek megfelelő, a gyakorlatban megvalósított megoldásokat és szabályokat a MÁV INFORMATIKA Kft. „Hitelesítés Szolgáltatási Szabályzat Minősített Elektronikus Aláírással Kapcsolatos Szolgáltatásokhoz" című dokumentuma (továbbiakban: HSzSz) tartalmazza. Az időbélyegzés szolgáltatás szabályzata[2] beépül ezen HSzSz-be, annak részét képezi.

Az ISzP és a HSzSz nyilvános dokumentumok. A Szolgáltató ezen dokumentumok mindenkori aktuális változatát az Interneten a *http://www.mavinformatika.hu/ca/* címen keresztül teszi mindenki számára elérhetővé.

Az aktuális időbélyegző alkalmazás technikai azonosító: Trust&Sign TSA V1.0

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

2. Az ISzP hatálya

Az ISzP időbeli hatálya

Az ISzP időbeli hatálya a változáskezelési táblázatban feltüntetett, a jelen verzióra érvényes hatálybalépés dátumától kezdődően határozatlan időre szól. Időbeli hatálya megszűnik a szolgáltatási tevékenység beszüntetésekor, illetve egy újabb ISzP verzió hatályba lépésékor.

Az ISzP személyi hatálya

Az ISzP személyi hatálya az ISz-re és az 5.3 pontban meghatározott felhasználó közösségre terjed ki.

Az ISzP tárgyi hatálya a következőkre terjed ki:

- az ISzP-ben meghatározott szolgáltatásokra,
- az ISz-nek az időbélyegzés szolgáltatással valamilyen kapcsolatban álló összes objektumára, tárgyi eszközére.

3. Jogszabályi és szabályzati megfelelés

Az ISzP tartalmában és szerkezetében megfelel az elektronikus aláírásról szóló 2001. évi XXXV. törvénynek, az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről szóló 16/2001. (IX. 1.) MeHVM 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 ISzP összhangban van a MÁV INFORMATIKA Kft. belső szabályzataival, ezen belül a Trust&Sign szolgáltatásokra vonatkozó üzemeltetési és biztonsági szabályzatokkal.

4. Általános koncepció

4.1. Időbélyegzés szolgáltatás

Az időbélyegzés szolgáltatás két szolgáltatási komponensből áll:

- időbélyeg előállítás,
- időbélyegzés menedzsment.

Ennek megfelelően az időbélyegzés szolgáltatást biztosító informatikai rendszer két fő összetevőből áll:

1. az időbélyegeket előállító és kibocsátó egységek,
2. az időbélyegeket előállító és kibocsátó egységek funkcionális és megbízható működését menedzselő és felügyelő alrendszer, amely a következő funkciókat látja el:
    - felügyeli a kettőzött időbélyegző szerver működését, kiesés esetén irányítja az áttérést a meleg tartalék szerverre,
    - biztosítja az időbélyegző szerver belső időszinkronizálását,
    - biztosítja a belső időszinkronizálást végző óra négy egymástól független UTC[3] időalappal történő időszinkronizálását,
    - biztosítja az időbélyegző szerver belső órájának a pontossági tartományból való kilépésének figyelését, 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.

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

4.2. Időbélyegzés szolgáltató (ISz)

A 4.1 pontban meghatározott időbélyegzést támogató informatikai rendszer üzemeltetője a minősített hitelesítés szolgáltatóként regisztrált MÁV INFORMATIKA Kft., amely időbélyegzés szolgáltatást nyújt a 4.3 pontban meghatározott időbélyeg felhasználók részére.

4.3. Időbélyeg felhasználó fél

Időbélyeg felhasználó fél (ügyfél) lehet:

1. bármely európai uniós állampolgárságú természetes személy, aki az ISz-el időbélyegzés szolgáltatásra a Minősített Általános Szerződési Feltételek (továbbiakban: ÁSzF) szerint szerződést köt,
2. bármely jogi személy, amely az ISz-el időbélyegzés szolgáltatásra az ÁSzF 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 Kft., vagy más hitelesítés szolgáltató nyújtja.

Természetes személyek önmaguk felelősek a végfelhasználókra vonatkozó szabályok betartásáért és kötelezettségek teljesítéséért.

A jogi személyek által az ISz-el megkötött szerződésben vállalt, a végfelhasználókra vonatkozó szabályok betartásáért és kötelezettségek teljesítéséért a jogi személy a felelős. Ezért jogi személy köteles ezt a végfelhasználók feladatává tenni, és tájékoztatni őket az időbélyegzés szolgáltatásra vonatkozó szabályokról és kötelezettségekről, illetve megadni az ISz által közzétett, az időbélyegzés szolgáltatásokra vonatkozó elérhetőséget.

4.4. Az Időbélyegzés Szolgáltatási Politika és az Időbélyegzés Szolgáltatási Szabályzat kapcsolata

4.4.1. Az ISzP célja

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

A MÁV INFORMATIKA Kft. 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 ISzP mint önálló és különálló dokumentum határozza meg a követelményeknek és szabályoknak való megfelelést.

A MÁV INFORMATIKA Kft. mint minősített hitelesítés szolgáltató a minősített hitelesítés szolgáltatásra és a kapcsolódó szolgáltatásokra vonatkozóan rendelkezik hitelesítés szolgáltatási szabályzattal (HSzSz-el), ezért az ISzP-ben meghatározott követelményekhez és szabályokhoz kapcsolódó konkrét megoldásokat – így az időbélyegzés szolgáltatás szabályait is – a MÁV INFORMATIKA Kft. „Hitelesítés Szolgáltatási Szabályzat Minősített Elektronikus Aláírással Kapcsolatos Szolgáltatásokhoz” című dokumentuma tartalmazza. Ez a szabályzat a *http://www.mavinformatika.hu/ca/* web lapon keresztül érhető el.

4.4.2. Az ISzP és a Szolgáltató egyéb kapcsolódó szabályzatai

Az ISzP és az időbélyegzés szolgáltatás működtetése a MÁV INFORMATIKA Kft. szabályzatai közül a következőket érinti:

A szabályzat neve	A szabályzat státusza	A szabályzat hozzáférhetősége
Általános Szerződési Feltételek Minősített Elektronikus Aláíráshoz Kapcsolódó Szolgáltatásokhoz (ÁSzF)	Nyilvános	Interneten közzétéve
Hitelesítés Szolgáltatási Szabályzat Minősített Elektronikus Aláíráshoz Kapcsolódó Szolgáltatásokhoz (HSzSz)	Nyilvános	Interneten közzétéve

A Trust&Sign Hitelesítés Szolgáltatás Biztonsági Szabályzata	Belső használatra	Csak jogosultsággal bíró belső személyeknek
A Trust&Sign Hitelesítés Szolgáltatás Informatikai Biztonságpolitikája	Belső használatra	Csak jogosultsággal bíró belső személyeknek
A Trust&Sign Hitelesítés Szolgáltatás Üzletmenet-folytonossági Terve	Belső használatra	Csak jogosultsággal bíró belső személyeknek

1. táblázat

Az ISz a fenti szabályzatokkal való harmonizálást a HSzSz 8.1 pontjában előírt változásmenedzsment követelményeknek megfelelően elvégezte és a felmerülő változásoknak megfelelően az ISzP-t és a kapcsolódó szabályzatokat karbantartja.

4.4.3. A kidolgozás elvei

A jelen ISzP csak általánosan érvényesítendő követelményeket és szabályokat tartalmaz. Az azok teljesítését célzó konkrét és gyakorlati megoldásokat, így az időbélyegzést támogató informatikai rendszer architektúráját és konfigurációját, annak üzemeltetését, a fizikai és a személyi környezet konkrét kialakítását, biztonságmenedzsmentjét, valamint az egyéb szabályokat és megoldásokat a minősített tanúsítványokra vonatkozó HSzSz és az 1. táblázatban meghatározott dokumentumok tartalmazzák.

Az ISzP összhangban van az 1. táblázat szerinti szabályzatokkal, az azokban meghatározott alapfogalmakat használja és nem tartalmaz azokkal párhuzamos vagy ellentétes szabályozást.

5. Időbélyegzés politika

5.1. Áttekintés

Az ISz időbélyegzési szolgáltatásra vonatkozó politikája a következők szerint érvényes:

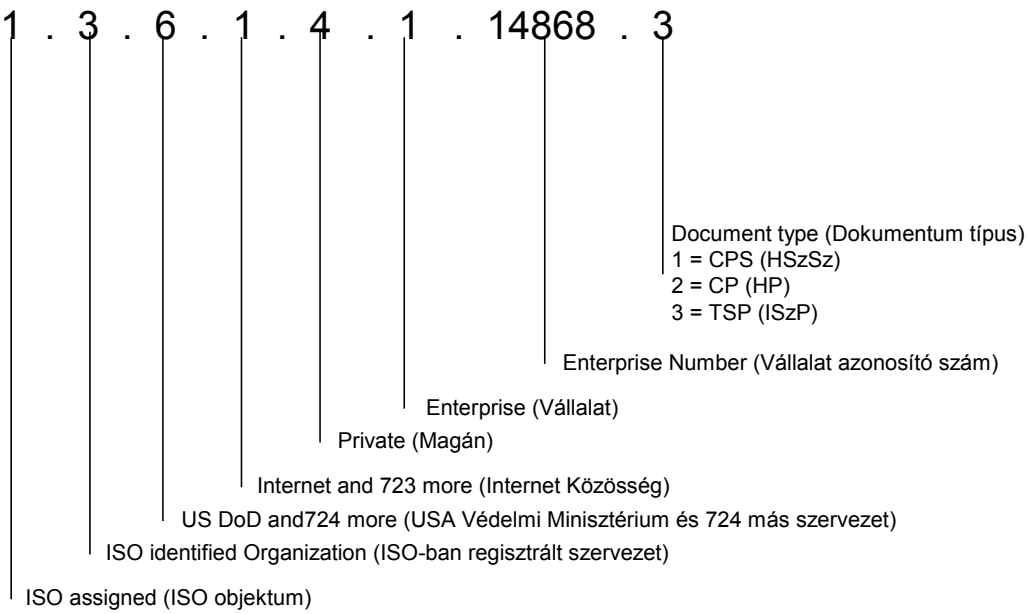
- Az időbélyegzés felhasználók vonatkozásában az időbélyegzés szolgáltatást minden szerződéses viszonyban álló természetes vagy jogi személy igénybe veheti, függetlenül attól, hogy az elektronikus hitelesítés szolgáltatást a MÁV INFORMATIKA Kft. vagy más hitelesítés szolgáltató nyújtja.
- Az állományok vonatkozásában érvényes mind elektronikus aláírással ellátott, mind el nem látott állományokra.

Az alapkövetelményekre és az időbélyegzési folyamat során, az ISz és az időbélyegzés felhasználó közötti kommunikáció protokolljára vonatkozóan, az ISz betartja az IETF RFC 3161 szabványt. A felhasználói és az időbélyegzést támogató szolgáltatói alkalmazásra, valamint az időbélyeg szerkezetére és tartalmára vonatkozóan betartja az ETSI TS 101 861 szabványt. Minden időbélyeg tartalmazza a jelen ISzP 5.2 pontjában meghatározott objektum azonosítóját (OID) és az időbélyeg kibocsátás pontosságát, amelynek 1 másodpercen belül kell lenni.

Az ISz aláíró kulcsát kísérő tanúsítványt a MÁV INFORMATIKA Kft., mint fölérendelt hitelesítés szolgáltató adja fokozott biztonságú eszköz tanúsítványként.

5.2. Az ISzP azonosítása

Az ISzP-t objektumként értelmezve OID-vel azonosítjuk. Az időbélyegekben megadott ISzP OID-t a 1. ábra mutatja meg.



1. ábra

Jelen dokumentum teljes neve: **A MÁV INFORMATIKA Kft. Időbélyegzés Szolgáltatási Politikája.**

A jelen dokumentumban ISzP-ként történik rá hivatkozás.
Az ISzP nyilvános dokumentum, amely a Szolgáltató *http://www.mavinformatika.hu/ca/* web lapján keresztül érhető el.

Jelen ISzP-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 független belső és külső auditorok által rendszeresen elvégzett vizsgálatokkal biztosítja, amelyek gyakoriságára, módjára, kiterjedésére és a hiányosságok kezelésére vonatkozóan a HSzSz 2.7 pontja mérvadó.

6. Kötelezettségek és felelősség

6.1. Az ISz kötelezettségei

Az ISz-nek három irányban vannak kötelezettségei:

- az időbélyeg felhasználók,
- a Nemzeti Hírközlési Hatóság[4] (továbbiakban: NHH), mint hatóság,
- az alvállalkozói

felé.

6.1.1. Általános kötelezettségek

Az ISz kötelezettséget vállal arra, hogy szolgáltatásaiban érvényesíti a jelen ISzP-t, betartja az 5.1 pontjában meghatározott szabványokat, a 7.4.10 pontban meghatározott jogszabályokat, valamint az időbélyegzésre vonatkozó azon szabályokat, amelyek a következő dokumentumokban lettek meghatározva:

- Általános Szerződési Feltételek a Minősített Elektronikus Aláírással Kapcsolatos Szolgáltatásokhoz,
- időbélyegzésre vonatkozó Előfizetői Szerződés,
- Hitelesítés Szolgáltatási Szabályzat Minősített Elektronikus Aláírással Kapcsolatos Szolgáltatásokhoz
- a Trust&Sign Hitelesítés Szolgáltatás Biztonsági Szabályzata,
- a Trust&Sign Hitelesítés Szolgáltatás Informatikai Biztonságpolitikája,
- a Trust&Sign Hitelesítés Szolgáltatás Üzletmenet-folytonossági Terve.

6.1.2. Az ISz kötelezettségei az időbélyeget felhasználók felé

Az ISz kötelezettséget vállal a következőkre az időbélyeget felhasználók felé:

- biztosítja, hogy az időbélyegző válasz, az időbélyegzéssel összefüggésben hozzáadottaktól eltekintve, ugyanazokat az adatokat tartalmazza, amelyeket a kérelem tartalmazott,
- a kibocsátott időbélyeg nem tartalmaz hibás adatot,
- időbélyeg aláíró kulcsát csak az időbélyegzés keretén belül használja,
- az időbélyeget 1 másodpercen belüli pontossággal adja ki,

[4] Jogelődje 2003. december 31-ig: Hírközlési Felügyelet, rövidítve: HIF

- az időbélyegzési rendszer belső óráját 0,1 másodperc pontossággal szinkronizálja az UTC időalaphoz.
- az időbélyegzés szolgáltatás megbízhatóságát és biztonságát a minősített hitelesítés szolgáltatókra vonatkozó követelmények szerint biztosítja,
- rögzít az időbélyegzéssel kapcsolatos minden fontos eseményt, ezeket naplózza és a napló állományokat biztonságosan archiválja.

6.1.3. Az ISz kötelezettségei az NHH felé

Az ISz a következő kötelezettségeket vállalja az NHH, mint hatóság felé:

- biztosítja és fenntartja a minősítéskori szolgáltatási és biztonsági szintet,
- betartja a 2001. évi XXXV. törvény és a 16/2001. (IX. 1.) MeHVM rendeletben az NHH, mint hatóság felé előírt bejelentési kötelezettségeket,
- az NHH ellenőrzések során tett észrevételeknek megfelelően a szükséges módosításokat az előírt határidőre elvégzi.

6.1.4. Az ISz kötelezettségei az alvállalkozói felé

Az ISz kötelezettséget vállal arra, hogy az alvállalkozók felé érvényesíti, hogy azok a 6.1.1 pontban felsorolt szabályzatokkal összhangban nyújtsák szolgáltatásaikat. Ennek betartását az ISz az alvállalkozóknál rendszeresen ellenőrzi.

6.2. Az időbélyeget felhasználók kötelezettségei

Az időbélyeget felhasználók kötelesek a kért időbélyeg vétele után meggyőződni az időbélyeg aláírás helyességéről és az aláíró kulcs tanúsítványának érvényességéről. Ennek módját részletesen a minősített HSzSz 2.1.7 pontja tartalmazza.

6.3. Az Érintett fél kötelezettségei

Az Érintett fél kötelezettségeire általában érvényesek a minősített HSzSz 2.1.8, a felelősségére a minősített HSzSz 2.2.7 pontjában leírt szabályok.

Egy időbélyeggel ellátott állomány vétele után az Érintett félnek ellenőriznie kell az ISz általi aláírás megtörténtét, az ISz Tanúsítvány érvényességét a Tanúsítvány Visszavonási Lista (CRL[5]) segítségével a minősített HSzSz 2.1.7 pontjában leírt módon.

Amennyiben az ellenőrzés az ISz Tanúsítvány érvényességének lejárta után történik, akkor az ellenőrzést a minősített HSzSz 2.1.8 pontjában leírt módszerrel kell elvégezni.

[5] CRL: Certificate Revocation List, magy.: Tanúsítvány Visszavonási Lista

6.4. Felelősség

Az ISz felelősségére és a saját hibájából elkövetett hibából adódó kár megtérítésére vonatkozóan a minősített HSzSz 2.2.1, 2.2.2 és a 2.3.1 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 Kft. a PKI Üzleti Egységen belül, egy olyan időbélyegző informatikai alrendszerrel végzi, amely a minősített hitelesítés szolgáltató informatikai rendszerrel közös fizikai környezetben működik. Az időbélyegző informatikai alrendszer, valamint annak személyi és fizikai környezete megfelel a MeH 12. ajánlás és ebből adódóan az ITSEC[6] ajánlás fokozott biztonsági követelményeinek. A teljes szolgáltató rendszer megfelel a minősített hitelesítés szolgáltatókra vonatkozó 16/2001. (IX. 1.) MeHVM rendeletnek és a 2/2002. (IV.26) MeHVM irányelvnek.

A MÁV INFORMATIKA Kft.-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 szolgáltatási követelményeknek. A megfelelést biztosító technikai, működtetési, menedzselési és biztonsági megoldásokat és szabályokat a „Hitelesítés Szolgáltatási Szabályzat Minősített Elektronikus Aláírással Kapcsolatos Szolgáltatásokhoz” című dokumentum (HSzSz) határozza meg. A HSzSz megfelelő pontjai tartalmazzák az időbélyegzés következő vonatkozásait is:

- Szolgáltató és felhasználó közösség, alkalmazhatóság (HSzSz 1.3 pont),
- Feladatok és hatáskörök (HSzSz 2.1 pont),
- A szolgáltató és felhasználó közösség tagjainak felelőssége (HSzSz 2.2 pont),
- Az anyagi felelősség korlátjai (HSzSz 2.3 pont),
- Irányadó jog (HSzSz 2.4.1 pont),
- Érvénytelenség, hatályosság, megszűnés, értesítések (HSzSz 2.4.2 pont),
- Közzététel és Címtár (HSzSz 2.6 pont),

- A megfelelőség vizsgálata (HSzSz 2.7 pont),
- Azonosítás és hitelesítés(HSzSz 3. pont),
- A működésre vonatkozó követelmények (HSzSz 4. pont),
- Biztonsági audit eljárások (HSzSz 4.5 pont),
- Adatarchiválás (HSzSz 4.6 pont),
- Katasztrófa elhárítás, Aláírás létrehozó adat kompromittálódás (HSzSz 2.4.8 pont),
- Hitelesítés szolgáltató tevékenység megszüntetése (HSzSz 4.9 pont),
- Fizikai, eljárásrendi, és humán biztonsági szabályozások (HSzSz 5. pont),
- Kulcspár előállítás és telepítés (HSzSz 6.1 pont),
- Aláírás létrehozó adat védelme (HSzSz 6.2 pont),
- Számítógép biztonsági szabályok (HSzSz 6.5 pont),
- Életciklus technikai szabályok (HSzSz 2.4.1 pont),
- Kriptográfiai modul ellenőrzése (HSzSz 2.4.1 pont),
- Tanúsítvány és kulcs-visszavonási profil (HSzSz 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 politikával kapcsolatosan az ISz a 2. táblázat szerinti nyilatkozatot teszi közzé, amely a *http://www.mavinformatika.hu/ca/* web lapon keresztül érhető el.

A szabály megnevezése	A szabály kifejtése
Időbélyegzés szolgáltatás szabályozása	Időbélyegzés szolgáltatás részletes szabályozását a MÁV INFORMATIKA Kft. „Hitelesítés Szolgáltatási Szabályzat Minősített Elektronikus Aláírással Kapcsolatos Szolgáltatásokhoz” című dokumentuma (HSzSz) tartalmazza.
A Szolgáltató elérhetősége	**Név:** MÁV INFORMATIKA Kereskedelmi, Szolgáltató és Tanácsadó Kft.

[6] ITSEC = Information Technology Security Evaluation Criteria (Információtechnológia Biztonsági Értékelési Kritériumok) az Európai Közösség ajánlása az IT termékek és rendszerek biztonságának funkcionális és minősítési követelményeire

A szabály megnevezése	A szabály kifejtése
	Székhely, telephely: 1012 Budapest, Krisztina krt. 37/a. **Telefonszám:** (36-1) 457-9300 **Telefax szám:** (36-1) 457-9500 **Internet cím:** http://www.mavinformatika.hu **Ügyfélkapcsolati Iroda:** ügyfélfogadási idő: munkanapokon 9-13 óra **tel.:** +36-1-457-95-78 **e-mail:** ica@mavinformatika.hu **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. **Az ISzP és a HSzSz elérhetősége:** http://www.mavinformatika.hu/ca
ISzP azonosító	1.3.6.1.4.1.14868.3
Alkalmazható hash algoritmus	2/2002. (IV.26) MeHVM irányelv 1. melléklet 2. táblázata szerint
Az időbélyeg érvényességi ideje	Azonos az időbélyeg aláíró kulcs tanúsítványának érvényességi idejével, amely 3 év, feltéve, hogy ezen idő alatt nem történik meg az aláíró kulcs kompromittálódása.
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.
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 szükséges[7].
Időbélyeg felhasználók kötelezettségei	Kötelesek az időbélyeg vétele után meggyőződni az időbélyeg aláírás helyességéről és az aláíró kulcs tanúsítványának érvényességéről. Lásd részletesen: HSzSz 2.1.7 pont.
Érintett fél kötelezettségei és felelőssége	A kötelezettségek általában érvényesek a HSzSz 2.1.8, a felelősségére a HSzSz 2.2.7 pontjában leírt szabályok.
Az Érintett fél által történő	Egy időbélyeggel ellátott állomány vétele után ellenőrizni kell az ISz általi aláírás

[7] Magyarország EU tagságától kezdve bármely, az EU-ban regisztrált hitelesítés szolgáltató által kibocsátott, azonosítás-hitelesítésre alkalmas Tanúsítvány megfelel.

A szabály megnevezése	A szabály kifejtése
időbélyeg ellenőrzés módja	megtörténtét, az ISz privát kulcsának esetleges kompromittálódását, az ISz Tanúsítvány érvényességét a HSzSz 2.1.7 pontjában leírt módon. Amennyiben az ellenőrzés az ISz Tanúsítvány érvényességének lejárta után történik, akkor a HSzSz 2.1.8 pontjában leírt módszer szerint kell eljárni.
Időbélyegző rendszer naplók archiválási időtartama	A 16/2001. (IX. 1.) MeHVM 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. ♦ 16/2001. (IX. 1.) MeHVM 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 felelősségére és a saját hibájából elkövetett hibából adódó kár megtérítésére vonatkozóan a HSzSz 2.2.1, 2.2.2 és a 2.3.1 pontjai érvényesek.
Eljárás jogi viták rendezésére	Az ÁSzF 9. pontja szerint
A jogszabályoknak és a belső szabályzatoknak való megfelelés vizsgálata	Külső független auditor: Erdősi Péter Máté Minősítési eljárás: Nemzeti Hírközlési Hatóság (korábban: Hírközlési Felügyelet)

2. táblázat

7.2. A kulcsmenedzsment életciklusa

7.2.1. Az ISz kulcs generálása

Az ISz kulcs generálása a 16/2001. (IX. 1.) MeHVM 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 6.1.1 pont.

A kulcs előállítás fizikai védelme és személyi környezete megfelel a minősített hitelesítés szolgáltatókra vonatkozó követelményeknek. Lásd részletesebben: HSzSz 5. pont.

7.2.2. Az időbélyegző egység kulcsának védelme

Az időbélyegző egység kulcsa egy, a 16/2001. (IX. 1.) MeHVM 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 6.2 pont.

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

7.2.3. Az időbélyegző egység nyilvános kulcsának közzététele

Az időbélyegző egység nyilvános kulcsa és tanúsítványa a *http://www.mavinformatika.hu/ca/* web lapon 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 4.7 pontja, a kompromittálódás elkerülésére foganatosított, illetve a bekövetkezés esetén megvalósítandó intézkedéseket részletesen a HSzSz 4.8 pontja és a Trust&Sign Hitelesítés Szolgáltatás Üzletmenet-folytonossági Terv 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, a MÁV INFORMATIKA Kft. minősített root vagy produktív CA aláíró kulcsának kompromittálódása miatt a szolgáltatás vagy befejeződik, vagy a katasztrófa helyszínen újra indul.

Az 1. és 2. esetekben a kulcs megújításra kerül a 7.2. pont szerint.

Az 1., 2. és 3. esetekben gondoskodni kell a régi kulcs megsemmisítéséről. Az időbélyegző egységnek úgy kell működnie, hogy a régi kulccsal történő időbélyeg aláírást letiltsa.

7.2.6. Az időbélyeget aláíró kripto-modul életciklus menedzsmentje

A jelen ISzP 7.2.2 pontjában meghatározott követelményeknek megfelelő időbélyeget aláíró kripto-modul a HSzSz 5.1.1 pontjában ismertetett, fokozott biztonsági szintű Bizalmi Központban, egy a MÁV INFORMATIKA Kft. 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

7.3.1. Időbélyeg

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

- tartalmazza az 5.2 pontban meghatározott ISzP 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 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)

7.3.2. Óraszinkronizálás az UTC-vel

Az időbélyegző alrendszer belső órájának a pontossági tartományon belül maradását a HSzSz 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 Trust&Sign Hitelesítés Szolgáltatás 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 ISzP 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 2.8 (Bizalmasság - Adatkezelési Szabályzat), 4.5 (Biztonsági audit eljárások), 4.8 (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 Trust&Sign Hitelesítés Szolgáltatás Informatikai Biztonságpolitikája,
- a Trust&Sign Hitelesítés Szolgáltatás Biztonsági Szabályzata,
- a Trust&Sign Hitelesítés Szolgáltatás Üzletmenet-folytonossági Terve.

7.4.2. Az eszközök biztonsági osztályba sorolása és menedzsmentje

A Trust&Sign Hitelesítés Szolgáltatás Informatikai Biztonságpolitikája szerint az időbélyegzést támogató informatikai alrendszer biztonsági osztálybasorolása a következő:

Információvédelem szempontjából	FOKOZOTT BIZTONSÁGI OSZTÁLY
Megbízható működés szempontjából	FOKOZOTT BIZTONSÁGI OSZTÁLY

Ez megfelel a MeH 12. ajánlás és az ITSEC szerinti biztonsági osztálybasorolásnak[8].

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 16/2001. (IX. 1.) MeHVM rendeletnek és a 2/2002. (IV.26) MeHVM irányelv 212. pontjának megfelelően a MÁV INFORMATIKA Kft. PKI projektje keretén belül megtörtént a teljes hitelesítésszolgáltató rendszer, annak fizikai és személyi környezetének kockázatelemzés alapú vizsgálata.

A MÁV INFORMATIKA Kft. társasági szintű biztonságpolitikájának és szabályzatának, valamint a Trust&Sign 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.

[8] A megbízható működés szempontjából fokozott biztonsági osztályba sorolt informatikai rendszernek 99,5%-os rendelkezésre állással kell üzemelnie folyamatos üzemet feltételezve. Ez egy hónapos üzemidőre vetítve 3,6 óra megengedett időbélyegzés szolgáltatás kiesést jelent úgy, hogy egy kiesés nem lehet hosszabb, mint 30 perc.

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 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 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 Kft. által üzemeltett informatikai rendszerre alkalmazott társasági szintű működtetés menedzsment szabályok. Ezeken túlmenően az időbélyegzést támogató informatikai rendszerre vonatkozóan a működtetés menedzsmentet a Trust&Sign Üzemeltetési Kézikönyv és a HSzSz 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 Kft. társasági szintű, illetve a PKI Üzleti Egység vonatkozó szabályzatai, amelyek a következők:

- a MÁV INFORMATIKA Kft. Informatikai Biztonságpolitikája,
- a MÁV INFORMATIKA Kft. Informatikai Biztonsági Szabályzata,

- A Trust&Sign Hitelesítés Szolgáltatás Informatikai Biztonságpolitikája,
- A Trust&Sign Hitelesítés Szolgáltatás Biztonsági Szabályzata.

7.4.7. A biztonságos rendszer bevezetése és karbantartása

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

- 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 Kft. minősített Root CA aláíró kulcs kompromittálódása,
2. a MÁV INFORMATIKA Kft. minősített Produktív CA aláíró kompromittálódása,
3. az ISz aláíró kulcs kompromittálódása,
4. 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., 2. és 3. kulcs kompromittálódás esetei katasztrófa („A” osztályú) eseménynek, a 4. eset súlyos üzemzavarnak („B” osztályú eseménynek) minősülnek, amelyek kezelésére a HSzSz

4.8 pontja és a Trust&Sign Hitelesítés Szolgáltatás Üzletmenet-folytonossági Terve tartalmazza az intézkedéseket.

7.4.9. Az ISz működésének befejezése

Az ISz befejezi működését, ha a MÁV INFORMATIKA Kft. 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:

- az időbélyegzés szolgáltatás fő lépései, a kérelemtől az időbélyeg válasz elküldésig,
- az ISz aláíró kulcs életciklusában bekövetkező események (generálás, használat, visszavonás, megsemmisítés),
- az ISz aláíró kulcs tanúsítványa életciklusában bekövetkező események (kiadás, használat, visszavonás).
- a rögzített adatok a HSzSz 4.5 pontjával összhangban naponta naplózásra és tárolásra kerülnek. A naplók értékelése naponta megtörténik. A tárolt naplók archiválása a HSzSz 4.6 pontjával összhangban történik.
  Az archivált adatok megőrzési ideje 10 év.

7.5. Szervezeti séma

Az időbélyegzés szolgáltatást a MÁV INFORMATIKA Kft. Outsourcing Üzletágához tartozó PKI Üzleti Egység végzi.

8. Meghatározások és rövidítések

8.1. Meghatározások

A jelen ISzP a 2001. évi XXXV. törvény és a 16/2001. (IX. 1.) MeHVM rendelet és a 2/2002. (IV. 26) MeHVM irányelv által használt alapfogalmakat használja, amelyek meghatározását a HSzSz 9.2 pontja tartalmazza.

8.2. Alkalmazott jelölések

ÁSzF: Általános Szerződési Feltételek Minősített Elektronikus Aláírással Kapcsolatos Szolgáltatásokhoz

HSzSz: Hitelesítés Szolgáltatási Szabályzat Minősített Elektronikus Aláírással Kapcsolatos Szolgáltatásokhoz

ISzP: Időbélyegzés Szolgáltatási Politika

ISz: Időbélyegzés Szolgáltató (jelen dokumentumban a MÁV INFORMATIKA Kft.)

NHH: Nemzeti Hírközlési Hatóság (korábban: HIF – Hírközlési Felügyelet)

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

CRL: Certificate Revocation List, magyarul: Tanúsítvány Visszavonási Lista

Melléklet

Az időbélyegzést szolgáltató alrendszer informatikai biztonsági követelményei

Az ISzP 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

Az időbélyegzés szolgáltató informatikai rendszer a Bizalmi Központba került elhelyezésre, amely a következő követelményeknek felel meg:

- a fokozott biztonsági szintnek megfelelő szilárdságú határoló felületek,
- a Bizalmi Központ bejárati ajtaja és a technikai helyiség ajtaja a MABISZ ajánlásában meghatározott I-es kategóriájú, a perszonalizációs helyiség ajtaja MABISZ III. kategóriájú,
- a Bizalmi Központ objektum előtt biztonsági szegmens van kialakítva, amelybe anti-passback és naplózási tulajdonságokkal bíró beléptető rendszere keresztül lehet csak bejutni,
- a Bizalmi Központba történő bejutást video biztonsági kamerás rendszer figyeli, amelynek személyes felügyelete folyamatosan biztosított,
- a Bizalmi Központ rendelkezik önálló és kettőzött klimatizálással, valamint mozgásérzékelő, tűz- és füstjelző és tűzoltó rendszerrel,
- a Bizalmi Központ IT eszközei két, egymástól független külső betáplálással támogatott, Diesel aggregátoros, szünetmentes tápáramellátó rendszerrel rendelkezik,
- a Bizalmi Központban a szerverek biztonsági kabinetekben vannak elhelyezve,
- a Bizalmi Központra és a kabinetekre a Biztonsági Szabályzat egy fejezetét képező kulcskezelés szabályozás érvényes,

- a Bizalmi Központ az MSZ 274/5T:1993 szabvánnyal összhangban LPZ2 zónahatárig kiépített másodlagos villámvédelemmel ellátott,
- a Bizalmi Központba csak a Biztonsági Szabályzatban meghatározott szerepkörű vezetők és munkatársak léphetnek be,
- a mentési és a primer szoftver adathordozók, a nyers és a megszemélyesített Aláírás létrehozó eszközök besugárzás és fizikai behatás ellenálló biztonsági szekrényekben tároltak,
- a működtetési és menedzselési és a biztonsági dokumentáció elektronikusan tárolt,
- a Szolgáltató az érzékeny adatokat tartalmazó adathordozó eszköztől biztonságosan válik meg, amennyiben azokra már nincs szükség,
- 60 DB elnyomással rendelkező EMC védelemmel ellátott,
- az informatikai rendszer két független nyomvonalon vezetett üvegkábellel kapcsolódik az Internethez,
- a lokális telefonkapcsolat az EMC zónahatáron szűrőn keresztül kapcsolódik a szolgáltató telefonközpontjához.

A környezetei elemek, rendszerek alábbi állapotjellemzőit monitor rendszer figyeli:

- hőmérséklet,
- páratartalom
- légnyomás,
- tűzeset érzékelés,
- tápáramellátás üzemkészség,
- légkondicionáló rendszer üzemkészség,
- biztonsági rendszer jelzései.

A bekövetkező események naplózásra, majd archiválásra kerülnek.

Logikai biztonsági követelmények

Az időbélyegző szerverhez hozzáférési jogosultsággal rendelkező üzemeltetők azonosítása-hitelesítése 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.

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

- leválasztás az Internetről tűzfallal,
- az időbélyegző szerver számára a tűzfalon egy önálló, a többi biztonsági szegmenstől különböző szegmenst kell létrehozni.

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 5.2 és 5.3 pontjaiban szerepelnek.

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

Ez – folyamatos üzemet feltételezve – 99,5%-os rendelkezésre állási követelményt jelent. Egy hónapos üzemidőre vetítve 3,6 óra megengedett időbélyegzés szolgáltatás kiesés engedhető meg jelent úgy, hogy egy kiesés nem lehet hosszabb, mint 30 perc.

E követelmény kielégítése az időbélyegző szerverek meleg tartalékolásával, a nagy megbízhatóságú rendszert menedzselő szoftver alkalmazásával, katasztrófa helyszín és időbélyegző rendszerrel biztosított.