MÁV INFORMATIKA
Kereskedelmi, Szolgáltató és Tanácsadó
Korlátolt Felelősségu Társaság

Idobélyegzés Szolgáltatási Rend

Verziószám	**2.0**
OID szám	**1.3.6.1.4.1.14868.3.2**
Hatósági nyilvántartásba vétel napja	**2005. július 22.**
Hatósági nyilvántartásba vétel száma	**HL-12638-4/2005**
Hatálybalépés dátuma	**2005. július 22.**

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

Idobélyegzés Szolgáltatási Rend verziók

Verzió	Dátum	A változás leírása	Készítette
1.0	2003.05.27	Az Idobélyegzés Szolgáltatási Rend véglegesítésre elokészített változata.	Bodlaki Ákos
1.1	2003.07.29	Minosítési 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

TARTALOMJEGYZÉK

1. Bevezetés

A MÁV INFORMATIKA Kft. (továbbiakban: Idobélyegzés Szolgáltató vagy Szolgáltató, rövidítve: ISZ) mint minosített hitelesítés szolgáltató idobélyegzés szolgáltatást is nyújt a minosített hitelesítés szolgáltatókra vonatkozó követelményeket kielégíto informatikai, fizikai és személyi környezetben.

Az ISZ által nyújtott idobélyegzés szolgáltatás hozzákapcsolható fokozott, illetve minosített aláírással ellátott, valamint elektronikusan nem aláírt állományokhoz is.

Ezen Idobélyegzés Szolgáltatási Rend (továbbiakban: ISZR) meghatározza az ISZ által nyújtott idobélyegzés szolgáltatásban résztvevoket, azok kötelezettségeit és felelosségét, az ISZ muködésére vonatkozó követelményeket, az idobélyeg szerkezetét, az idobélyegzés szolgáltatás menedzsment és az idobélyegzéshez tartozó kulcsmenedzsment életciklusára vonatkozó szabályokat.

Összhangban az idobélyegzés szolgáltatókra vonatkozó követelményekrol szóló ETSI TS 102 023 EU szabvány 7.1.1 fejezetével, a jelen ISZR az ISZ-re, az idobélyegzés szolgáltató rendszerre és a szolgáltatásra vonatkozó általános követelményeket határozza meg. Ezen követelményeknek megfelelo, a gyakorlatban megvalósított megoldásokat és szabályokat a MÁV INFORMATIKA Kft. „Szolgáltatási Szabályzat Minosített Elektronikus Aláírással Kapcsolatos Szolgáltatásokhoz” címu dokumentuma (továbbiakban: HSZSZ-M) tartalmazza. Az idobélyegzés szolgáltatás szabályzata[1] beépül ezen HSZSZ-M-be, annak részét képezi.

Az ISZR és a HSZSZ-M nyilvános dokumentumok. A Szolgáltató ezen dokumentumok mindenkori aktuális változatát az Interneten a *http://www.mavinformatika.hu/ca/* címen keresztül teszi mindenki számára elérhetové.

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

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

2. Az ISZR hatálya

Az ISZR idobeli hatálya

Az ISZR idobeli hatálya a változáskezelési táblázatban feltüntetett, a jelen verzióra érvényes hatálybalépés dátumától kezdodoen határozatlan idore szól. Idobeli hatálya megszunik a szolgáltatási tevékenység beszüntetésekor, illetve egy újabb ISZR verzió hatályba lépésékor.

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 a következokre terjed ki:

- az ISZR-ben meghatározott szolgáltatásokra,
- az ISZ-nek az idobélyegzés szolgáltatással valamilyen 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 követelményekrol szóló 3/2005. (III. 18.) IHM rendeletnek, a minosített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekrol szóló 2/2002. (IV.26) MeHVM irányelvnek, valamint az idobélyegzés szolgáltatókra vonatkozó követelményekrol szóló ETSI TS 102 023 (2003.04) EU szabványnak.

Ezen túlmenoen a jelen ISZR összhangban van a MÁV INFORMATIKA Kft. belso szabályzataival, ezen belül a PKI szolgáltatásokra vonatkozó üzemeltetési és biztonsági szabályzatokkal.

4. Általános koncepció

4.1. Idobélyegzés szolgáltatás

Az idobélyegzés szolgáltatás két szolgáltatási komponensbol áll:

- idobélyeg eloállítás,
- idobélyegzés menedzsment.

Ennek megfeleloen az idobélyegzés szolgáltatást biztosító informatikai rendszer két fo összetevobol áll:

1. az idobélyegeket eloállító és kibocsátó egységek,
2. az idobélyegeket eloállító és kibocsátó egységek funkcionális és megbízható muködését menedzselo és felügyelo alrendszer, amely a következo funkciókat látja el:
   - felügyeli a kettozött idobélyegzo szerver muködését, kiesés esetén irányítja az áttérést a meleg tartalék szerverre,
   - biztosítja az idobélyegzo szerver belso idoszinkronizálását,
   - biztosítja a belso idoszinkronizálást végzo óra négy egymástól független UTC[2] idoalappal történo idoszinkronizálását,
   - biztosítja az idobélyegzo szerver belso órájának a pontossági tartományból való kilépésének figyelését, ennek bekövetkezés esetén a szolgáltatás leállítását és a hibaüzenet kiadását az elofizetok felé,
   - támogatja az installációs, a karbantartási, a naplózási, az archiválási, a mentési és a leállítási muveleteket.

4.2. Idobélyegzés szolgáltató (ISZ)

A 4.1 pontban meghatározott idobélyegzést támogató informatikai rendszer üzemeltetoje a minosített hitelesítés szolgáltatóként regisztrált MÁV INFORMATIKA Kft., amely idobélyegzés szolgáltatást nyújt a 4.3 pontban meghatározott idobélyeg felhasználók részére.

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

4.3. Idobélyeg felhasználó fél

Idobélyeg felhasználó fél (ügyfél) lehet:

1. bármely európai uniós állampolgárságú természetes személy, aki az ISZ-el idobélyegzés szolgáltatásra az Általános Szerzodési Feltételek Minosített Elektronikus Aláírással Kapcsolatos Szolgáltatásokhoz (továbbiakban: ÁSZF-M) szerint szerzodést köt,
2. bármely jogi személy, amely az ISZ-el idobélyegzés szolgáltatásra az ÁSZF-M szerint szerzodést köt.

Idobélyegzés szolgáltatásra az ISZ-el az elozoekben meghatározott bármely ügyfél szerzodést köthet, függetlenül attól, hogy számára az elektronikus hitelesítés szolgáltatást a MÁV INFORMATIKA Kft., vagy más hitelesítés szolgáltató nyújtja.

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

A jogi személyek által az ISZ-el megkötött szerzodésben vállalt, a végfelhasználókra vonatkozó szabályok betartásáért és kötelezettségek teljesítéséért a jogi személy a felelos. Ezért jogi személy köteles ezt a végfelhasználók feladatává tenni, és tájékoztatni oket az idobélyegzés szolgáltatásra vonatkozó szabályokról és kötelezettségekrol, illetve megadni az ISZ által közzétett, az idobélyegzés szolgáltatásokra vonatkozó elérhetoséget.

4.4. Az Idobélyegzés Szolgáltatási Rend és a szolgáltatási szabályzat kapcsolata

4.4.1. Az ISZR célja

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

A MÁV INFORMATIKA Kft. az idobélyegzés szolgáltatást a minosített hitelesítésszolgáltatással együtt kapcsolódó szolgáltatásként, vagy a hitelesítés szolgáltatástól függetlenül önállóan igénybe veheto szolgáltatásként teljesíti az idobélyegzést felhasználó ügyfelek felé. Ezért az ISZR mint önálló és különálló dokumentum határozza meg a követelményeknek és szabályoknak való megfelelést.

A MÁV INFORMATIKA Kft. mint minosített hitelesítés szolgáltató a minosített hitelesítés szolgáltatásra és a kapcsolódó szolgáltatásokra vonatkozóan rendelkezik szolgáltatási szabályzattal (HSZSZ-M-el), ezért az ISZR-ben meghatározott követelmé-

nyekhez és szabályokhoz kapcsolódó konkrét megoldásokat – így az idobélyegzés szolgáltatás szabályait is – a MÁV INFORMATIKA Kft. „Szolgáltatási Szabályzat Minosített Elektronikus Aláírással Kapcsolatos Szolgáltatásokhoz" címu dokumentuma tartalmazza. Ez a szabályzat a *http://www.mavinformatika.hu/ca/* web lapon keresztül érheto el.

4.4.2. Az ISZR és a Szolgáltató egyéb kapcsolódó szabályzatai

Az ISZR és az idobélyegzés szolgáltatás muködtetése a MÁV INFORMATIKA Kft. szabályzatai közül a következoket érinti:

A szabályzat neve	A szabályzat státusza	A szabályzat hozzáférhetosége
Általános Szerzodési Feltételek Minosített Elektronikus Aláírással Kapcsolatos Szolgáltatásokhoz (ÁSZF-M)	Nyilvános	Interneten közzétéve
Hitelesítés Szolgáltatási Szabályzat Minosített Elektronikus Aláírással Kapcsolatos Szolgáltatásokhoz (HSZSZ-M)	Nyilvános	Interneten közzétéve
A PKI Szolgáltatások Biztonsági Szabályzata	Belso használatra	Csak jogosultsággal bíró belso személyeknek
A PKI Szolgáltatások Informatikai Biztonságpolitikája	Belso használatra	Csak jogosultsággal bíró belso személyeknek
A PKI Szolgáltatások Üzletmenet-folytonossági Terve	Belso használatra	Csak jogosultsággal bíró belso személyeknek

1. táblázat

Az ISZ a fenti szabályzatokkal való harmonizálást a HSZSZ-M 8.1 pontjában eloírt változásmenedzsment követelményeknek megfeleloen elvégezte és a felmerülo változásoknak megfeleloen az ISZR-t és a kapcsolódó szabályzatokat karbantartja.

4.4.3. A kidolgozás elvei

A jelen ISZR csak általánosan érvényesítendo követelményeket és szabályokat tartalmaz. Az azok teljesítését célzó konkrét és gyakorlati megoldásokat, így az idobélyegzést támogató informatikai rendszer architektúráját és konfigurációját, annak üzemeltetését, a fizikai és a személyi környezet konkrét kialakítását, biztonságmenedzsmentjét, valamint az egyéb szabályokat és megoldásokat a minosített tanúsítványokra vonatkozó HSZSZ-M és az 1. táblázatban meghatározott dokumentumok tartalmazzák.

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

5. Idobélyegzési rend

5.1. Áttekintés

Az ISZ idobélyegzés szolgáltatásra vonatkozó rendje a következok szerint érvényes:

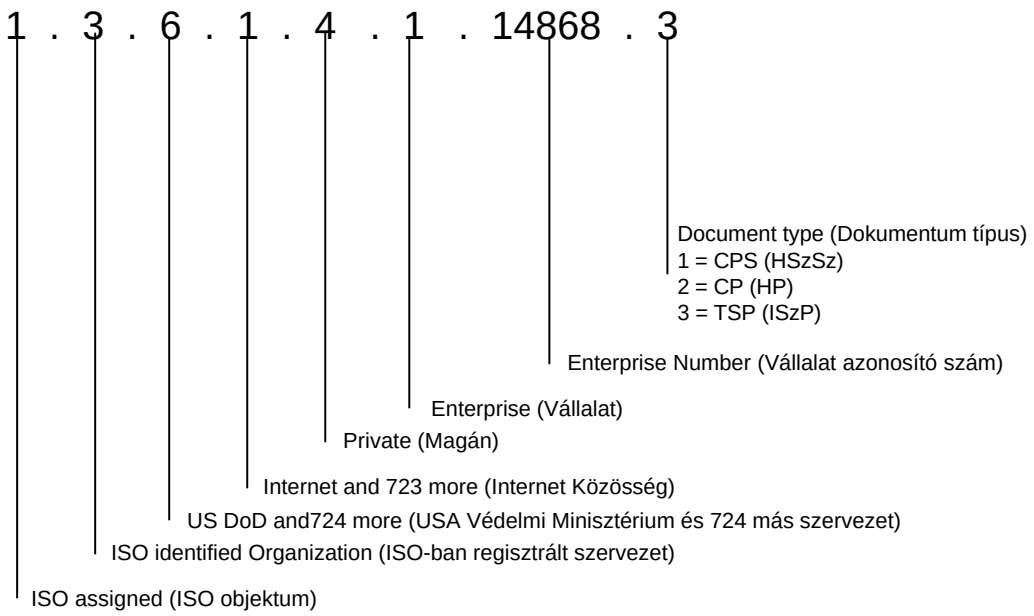
- Az idobélyegzés felhasználók vonatkozásában az idobélyegzés szolgáltatást minden szerzodéses viszonyban álló természetes vagy jogi személy igénybe veheti, függetlenül attól, hogy az elektronikus hitelesítés szolgáltatást a MÁV INFORMATIKA Kft. vagy más hitelesítés szolgáltató nyújtja.
- Az állományok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

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

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

5.2. Az ISZR azonosítása

Az ISZR-t objektumként értelmezve OID-vel azonosítjuk. Az idobélyegekben megadott ISZR OID-t a 1. ábra mutatja meg.



1. ábra

Jelen dokumentum teljes neve: **A MÁV INFORMATIKA Kft. Idobélyegzés Szolgáltatási Rendje.**

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

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

5.3. Felhasználó közösség és alkalmazhatóság

Az idobélyegzés szolgáltatást minden, a 4.3 pontban meghatározott szerzodéses fél igénybe veheti, függetlenül attól, hogy az idobélyeget nyilvános vagy zárt körben használja.

5.4. Megfelelés

Az ISZ a hatályos jogszabályoknak, a nemzetközi ajánlásoknak és a belso szabályzatainak való megfelelést független belso és külso auditorok által rendszeresen elvégzett vizsgálatokkal biztosítja, amelyek gyakoriságára, módjára, kiterjedésére és a hiányosságok kezelésére vonatkozóan a HSZSZ-M 2.7 pontja mérvadó.

6. Kötelezettségek és felelosség

6.1. Az ISZ kötelezettségei

Az ISZ-nek három irányban vannak kötelezettségei:

- az idobélyeg felhasználók,
- a Nemzeti Hírközlési Hatóság (továbbiakban: NHH), mint hatóság,
- az alvállalkozói

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 idobélyegzésre vonatkozó azon szabályokat, amelyek a következo dokumentumokban lettek meghatározva:

- Általános Szerzodési Feltételek a Minosített Elektronikus Aláírással Kapcsolatos Szolgáltatásokhoz,
- idobélyegzésre vonatkozó Elofizetoi Szerzodés,
- Szolgáltatási Szabályzat Minosített Elektronikus Aláírással Kapcsolatos Szolgáltatásokhoz
- a PKI Szolgáltatások Biztonsági Szabályzata,
- a PKI Szolgáltatások Informatikai Biztonságpolitikája,
- a PKI Szolgáltatások Üzletmenet-folytonossági Terve.

6.1.2. Az ISZ kötelezettségei az idobélyeget felhasználók felé

Az ISZ kötelezettséget vállal a következokre az idobélyeget felhasználók felé:

- biztosítja, hogy az idobélyegzo válasz, az idobélyegzéssel összefüggésben hozzáadottaktól eltekintve, ugyanazokat az adatokat tartalmazza, amelyeket a kérelem tartalmazott,
- a kibocsátott idobélyeg nem tartalmaz hibás adatot,
- idobélyeg aláíró kulcsát csak az idobélyegzés keretén belül használja,
- az idobélyeget 1 másodpercen belüli pontossággal adja ki,
- az idobélyegzési rendszer belso óráját 0,1 másodperc pontossággal szinkronizálja az UTC idoalaphoz.

- az idobélyegzés szolgáltatás megbízhatóságát és biztonságát a minosített hitelesítés szolgáltatókra vonatkozó követelmények szerint biztosítja,
- rögzít az idobélyegzéssel kapcsolatos minden fontos eseményt, ezeket naplózza és a napló állományokat biztonságosan archiválja.

6.1.3. Az ISZ kötelezettségei az NHH felé

Az ISZ a következo kötelezettségeket vállalja az NHH, mint hatóság felé:

- biztosítja és fenntartja a minosítéskori szolgáltatási és biztonsági szintet,
- betartja a 2001. évi XXXV. törvény és a 3/2005. (III. 18.) IHM. rendeletben az NHH, mint hatóság felé eloírt bejelentési kötelezettségeket,
- az NHH ellenorzések során tett észrevételeknek megfeleloen a szükséges módosításokat az eloírt határidore 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 ellenorzi.

6.2. Az idobélyeget felhasználók kötelezettségei

Az idobélyeget felhasználók kötelesek a kért idobélyeg vétele után meggyozodni az idobélyeg aláírás helyességérol és az aláíró kulcs tanúsítványának érvényességérol. Ennek módját részletesen a minosített HSZSZ-M 2.1.7 pontja tartalmazza.

6.3. Az Érintett fél kötelezettségei

Az Érintett fél kötelezettségeire általában érvényesek a minosített HSZSZ-M 2.1.8, a felelosségére a minosített HSZSZ-M 2.2.7 pontjában leírt szabályok.

Egy idobélyeggel ellátott állomány vétele után az Érintett félnek ellenoriznie kell az ISZ általi aláírás megtörténtét, az ISZ Tanúsítvány érvényességét a Tanúsítvány Visszavonási Lista (CRL[3]) segítségével a minosített HSZSZ-M 2.1.7 pontjában leírt módon.

Amennyiben az ellenorzés az ISZ Tanúsítvány érvényességének lejárta után történik, akkor az ellenorzést a minosített HSZSZ-M 2.1.8 pontjában leírt módszerrel kell elvégezni.

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

6.4. Felelosség

Az ISZ felelosségére és a saját hibájából elkövetett hibából adódó kár megtérítésére vonatkozóan a minosített HSZSZ-M 2.2.1, 2.2.2 és a 2.3.1 pontjai érvényesek.

7. Az ISZ muködési követelményei

7.1. Szolgáltatási és a közzétételi szabályozás

7.1.1. Idobélyegzés szolgáltatás szabályozása

Az idobélyegzés szolgáltatást a MÁV INFORMATIKA Kft. a PKI Szolgáltató Egységen belül, egy olyan idobélyegzo informatikai alrendszerrel végzi, amely a minosített hitelesítés szolgáltató informatikai rendszerrel közös fizikai környezetben muködik. Az idobélyegzo informatikai alrendszer, valamint annak személyi és fizikai környezete megfelel a MeH ITB 12. ajánlás és ebbol adódóan az ITSEC[4] ajánlás fokozott biztonsági követelményeinek. A teljes szolgáltató rendszer megfelel a minosített hitelesítés szolgáltatókra vonatkozó 3/2005. (III. 18.) IHM. rendeletnek és a 2/2002. (IV.26) MeHVM irányelvnek.

A MÁV INFORMATIKA Kft.-t a Hírközlési Felügyelet 2003 április 3-án minosített hitelesítés szolgáltatóként regisztrálta. A fentiek alapján az idobélyegzo informatikai alrendszer, annak fizikai és személyi környezete megfelel a minosített szolgáltatási követelményeknek. A megfelelést biztosító technikai, muködtetési, menedzselési és biztonsági megoldásokat és szabályokat a HSZSZ-M határozza meg. A HSZSZ-M megfelelo pontjai tartalmazzák az idobélyegzés következo vonatkozásait is:

- Szolgáltató és felhasználó közösség, alkalmazhatóság (HSZSZ-M 1.3 pont),
- Feladatok és hatáskörök (HSZSZ-M 2.1 pont),
- A szolgáltató és felhasználó közösség tagjainak felelossége (HSZSZ-M 2.2 pont),
- Az anyagi felelosség korlátjai (HSZSZ-M 2.3 pont),
- Irányadó jog (HSZSZ-M 2.4.1 pont),
- Érvénytelenség, hatályosság, megszunés, értesítések (HSZSZ-M 2.4.2 pont),
- Közzététel és Tanúsítványtár (HSZSZ-M 2.6 pont),
- A megfeleloség vizsgálata (HSZSZ-M 2.7 pont),
- Azonosítás és hitelesítés(HSZSZ-M 3. pont),
- A muködésre vonatkozó követelmények (HSZSZ-M 4. pont),
- Biztonsági audit eljárások (HSZSZ-M 4.5 pont),
- Adatarchiválás (HSZSZ-M 4.6 pont),
- Katasztrófa elhárítás, Aláírás létrehozó adat kompromittálódás (HSZSZ-M 2.4.8 pont),

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

- Hitelesítés szolgáltató tevékenység megszüntetése (HSZSZ-M 4.9 pont),
- Fizikai, eljárásrendi, és humán biztonsági szabályozások (HSZSZ-M 5. pont),
- Kulcspár eloállítás és telepítés (HSZSZ-M 6.1 pont),
- Aláírás létrehozó adat védelme (HSZSZ-M 6.2 pont),
- Számítógép biztonsági szabályok (HSZSZ-M 6.5 pont),
- Életciklus technikai szabályok (HSZSZ-M 2.4.1 pont),
- Kriptográfiai modul ellenorzése (HSZSZ-M 2.4.1 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 idobélyegzés szolgáltatás használatával kapcsolatos információkat és feltételeket tartalmazó közzétételi nyilatkozatot kell nyilvánosan elérhetové tennie.

Az idobélyegzési politikával kapcsolatosan az ISZ a 2. táblázat szerinti nyilatkozatot teszi közzé, amely a *http://www.mavinformatika.hu/ca/* web lapon keresztül érheto el.

A szabály megnevezése	A szabály kifejtése
Idobélyegzés szolgáltatás szabály ozása	Idobélyegzés szolgáltatás részletes szabályozását a MÁV INFORMATIKA Kft. „Szolgáltatási Szabályzat Minosített Elektronikus Aláírással Kapcsolatos Szolgáltatásokhoz” címu dokumentuma (HSZSZ-M) tartalmazza.
A Szolgáltató elérhetosége	**Név:** MÁV INFORMATIKA Kereskedelmi, Szolgáltató és Tanácsadó Kft. **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 ido: 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

A szabály megnevezése	A szabály kifejtése
	• telefonon és faxon az ügyfélkapcsolati irodán vagy az ügyfélszolgálatnál • elektronikus levélben az ügyfélszolgálat e-mail címére. **Az ISZR és a HSZSZ-M elérhetosége:** http://www.mavinformatika.hu/ca
ISZR azonosító	1.3.6.1.4.1.14868.3.2
Alkalmazható hash algoritmus	2/2002. (IV.26) MeHVM irányelv 1. melléklet 2. táblázata szerint
Az idobélyeg érvényességi ideje	Azonos az idobélyeg aláíró kulcs tanúsítványának érvényességi idejével, amely 3 év, feltéve, hogy ezen ido alatt nem történik meg az aláíró kulcs kompromittálódása.
Az idobélyegben szereplo ido pontossága	Összhangban a 2/2002. (IV.26) MeHVM irányelv 219. pontjával, az UTC-vel szinkronizált ido pontossága: 1 másodpercen belül van.
Az idobélyegzés alkalmazhatóságának korlátjai	Természetes személy elofizeto: az Európai Unió állampolgára Jogi személy elofizeto: az Európai Unióban bejegyzett cég. Az idobélyegzés szolgáltatás igénybevételéhez érvényes NHH által regisztrált hitelesítés szolgáltató által kibocsátott, azonosítás-hitelesítésre alkalmas Tanúsítvány szükséges[5].
Idobélyeg felhasználók kötelezettségei	Kötelesek az idobélyeg vétele után meggyozodni az idobélyeg aláírás helyességérol és az aláíró kulcs tanúsítványának érvényességérol. Lásd részletesen: HSZSZ-M 2.1.7 pont.
Érintett fél kötelezettségei és felelossége	A kötelezettségek általában érvényesek a HSZSZ-M 2.1.8, a felelosségére a HSZSZ-M 2.2.7 pontjában leírt szabályok.
Az Érintett fél által történo idobélyeg ellenorzés módja	Egy idobélyeggel ellátott állomány vétele után ellenorizni kell az ISZ általi aláírás megtörténtét, az ISZ privát kulcsának esetleges kompromittálódását, az ISZ Tanúsítvány érvényességét a HSZSZ-M 2.1.7 pontjában leírt módon. Amennyiben az ellenorzés az ISZ Tanúsítvány érvényességének lejárta után történik, akkor a HSZSZ-M 2.1.8 pontjában leírt módszer szerint kell eljárni.
Idobélyegzo rendszer naplók archiválási idotartama	A 3/2005. (III. 18.) IHM. rendelettel összhangban az archivált naplókat keletkezésüktol számított 10 évig, illetoleg a velük kapcsolatban esetlegesen felmerült jogvita jogeros lezárásáig megorzodnek meg kell orizni.
Hatályos jogszabályok az idobélyegzés vonatkozá-	♦ 2001. évi XXXV. törvény az elektronikus aláírásról. ♦ 3/2005. (III. 18.) IHM rendelet az elektronikus aláírással kapcsolatos

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

A szabály megnevezése	A szabály kifejtése
sában	szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekrol. ♦ 2/2002. (IV.26) MeHVM irányelv a minosített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekrol. ♦ 1992. évi LXIII. törvény a személyes adatok védelmérol és a közérdeku 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 felelosségének korlátozása	Az ISZ felelosségére és a saját hibájából elkövetett hibából adódó kár megtérítésére vonatkozóan a HSZSZ-M 2.2.1, 2.2.2 és a 2.3.1 pontjai érvényesek.
Eljárás jogi viták rendezésére	Az ÁSZF-M 9. pontja szerint
A jogszabályoknak és a belso szabályzatoknak való megfelelés vizsgálata	Külso független auditor: Erdosi Péter Máté Nyilvántartásba vételi eljárás: Nemzeti Hírközlési Hatóság

2. táblázat

7.2. A kulcsmenedzsment életciklusa

7.2.1. Az ISZ kulcs generálása

Az ISZ kulcs generálása a 3/2005. (III. 18.) IHM. rendeletnek és a 2/2002. (IV.26) MeHVM irányelv 212. pontjának megfeleloen 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 kulcs eloállítás fizikai védelme és személyi környezete megfelel a minosített hitelesítés szolgáltatókra vonatkozó követelményeknek. Lásd részletesebben: HSZSZ-M 5. pont.

7.2.2. Az idobélyegzo egység kulcsának védelme

Az idobélyegzo egység kulcsa egy, a 3/2005. (III. 18.) IHM. rendeletnek és a 2/2002. (IV.26) MeHVM irányelv 212. pontjának megfeleloen az NHH által regisztrált tanúsí-

tó cég által tanúsított, az NHH által nyilvántartásba vett kriptográfiai modulban történik. Lásd részletesebben: HSZSZ-M 6.2 pont.

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

7.2.3. Az idobélyegzo egység nyilvános kulcsának közzététele

Az idobélyegzo egység nyilvános kulcsa és tanúsítványa a *http://www.mavinformatika.hu/ca/* web lapon keresztül érheto el.

7.2.4. Az idobélyegzo egység kulcsának megújítása

Az idobélyegzo egység kulcsának megújítása tanúsítványa érvényességi idejének lejártakor történik, hacsak addig a kulcs nem kompromittálódott. A kulcs megújítás szabályait részletesen a minosített 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 idobélyegzo egység kulcsmenedzsment életciklusának vége

Az idobélyegzo egység kulcsmenedzsment életciklusa következo esetekben fejezodik be:

1. a kulcs és tanúsítványának érvényességi ideje lejár,
2. a kulcs kompromittálódik,
3. katasztrófa esemény, a MÁV INFORMATIKA Kft. minosített root vagy produktív CA aláíró kulcsának kompromittálódása miatt a szolgáltatás vagy befejezodik, vagy a tartalék 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 megsemmisítésérol. Az idobélyegzo egységnek úgy kell muködnie, hogy a régi kulccsal történo idobélyeg aláírást letiltsa.

7.2.6. Az idobélyeget aláíró kripto-modul életciklus menedzsmentje

A jelen ISZR 7.2.2 pontjában meghatározott követelményeknek megfelelo idobélyeget aláíró kripto-modul a HSZSZ-M 5.1.1 pontjában ismertetett, fokozott biztonsági szintu Bizalmi Központban, egy a MÁV INFORMATIKA Kft. vezetése által felállított bizottság elott került installálásra és üzembe helyezésre. A bizottság az üzembe helyezés elott ellenorizte a kripto-modul sértetlenségét.
A kripto-modul üzemeltetése a Bizalmi Központban történik a minosített hitelesítésszolgáltatás követelményeinek megfelelo körülmények között és személyzet által.

Az idobélyeget aláíró kripto-modul rendszerbol történo kivonása esetén az idobélyeget aláíró kulcsot bizottság elott meg kell semmisíteni.

7.3. Idobélyegzés

7.3.1. Idobélyeg

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

- tartalmazza az 5.2 pontban meghatározott ISZR azonosítót,
- tartalmazza az idobélyeg egyedi azonosítóját,
- az idobélyegben megadott idopontot négy, egymástól független forrásból származó UTC idoalappal szinkronizált és a 7.1.2 pontbeli közzétételi nyilatkozatban meghatározott, - 1 másodpercen belüli - pontossággal rendelkezo belso óra adja,
- az idobélyegzo szerver belso órájának pontosságát a HSZSZ-M 4.3 pontjában részletesen ismertetett belso és külso szinkronizáló eljárás biztosítja;
- a külso szinkron háromszorosan tartalékolt és az egyes órajelek esetleges manipulációját ezen redundancia segítségével egy belso kontroll szuri ki;
- a belso órajel hitelességét az idobélyegzo alrendszer indításakor egy erre a célra összehívott bizottság tanúsítja;
- üzemközben a belso óra hitelességét a redundáns külso UTC idoalapokkal a bizottság által történo összevetés és egy a rendszertol független GPS kapcsolaton keresztül történo, referenciaként használt UTC idolekérdezés biztosítja,
- az ISZ által visszaküldött idobélyeg a kérelmezo üzenete által meghatározott adatokat tartalmazza;
- a kérelem része az idobélyeggel ellátandó adat hash lenyomata is;
- az ISZ az idobélyeget csak az idobélyegzés céljára kiadott aláíró kulccsal írja alá,
- az idobélyeg egy olyan ISZ névmegadást tartalmaz, amely tartalmazza:

- az ISZ országának nevét (C),
- az ISZ azonosítóját (CN),
- az idobélyeget kibocsátó egység nevét (O, OU)

7.3.2. Óraszinkronizálás az UTC-vel

Az idobélyegzo alrendszer belso órájának a pontossági tartományon belül maradását a HSZSZ-M 4.3 pontjában ismertetett belso és külso szinkronizációs eljárás biztosítja.

A külso szinkronizálást négy egymástól független UTC idoalap támogatja, amelyekkel nagy megbízhatósággal biztosítható az idobélyegzés belso órájának pontossága, valamint a külso órajelek redundancián alapuló ellenorzésével annak hitelessége is.

Ha a hitelességgel kapcsolatban kétely merül fel, akkor az idobélyegzo alrendszer indítását hitelesíto bizottság összehívásra kerül és ellenorzi a külso UTC idok hitelességét, amelyhez egy független GSM kapcsolaton keresztül kapott UTC idot használ referenciaként.

Az idobélyegzés belso órájának pontossága folyamatos ellenorzés alatt áll. Amennyiben a nagy megbízhatóságú idoszinkronizálás ellenére a belso óra pontossága az eloírt 1 másodperces tartományból kiesne, az idobélyegzés szolgáltatás leáll, és a hiba kijavításáig minden további kérésre hiba üzenetet küld az elofizetok felé. Ez súlyos üzemzavarnak („B” osztályú eseménynek) minosül, amelyre a PKI Szolgáltatások Üzletmenet-folytonossági Terve tartalmazza az intézkedéseket.

A szolgáltatás az idobélyegzo szerver belso órája által egymás után kétszer helyesen vett idoszinkronnal indul.

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

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

7.4. Idobélyegzés szolgáltatás menedzsment és muködtetés

7.4.1. Biztonságmenedzsment

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

A biztonságmenedzsment teljes területére a HSZSZ-M 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 PKI Szolgáltatások Informatikai Biztonságpolitikája,
- a PKI Szolgáltatások Biztonsági Szabályzata,
- a PKI Szolgáltatások Üzletmenet-folytonossági Terve.

7.4.2. Az eszközök biztonsági osztályba sorolása és menedzsmentje

A PKI Szolgáltatások Informatikai Biztonságpolitikája szerint az idobélyegzést támogató informatikai alrendszer biztonsági osztálybasorolása a következo:

Információvédelem szempontjából	FOKOZOTT BIZTONSÁGI OSZTÁLY
Megbízható muködés szempontjából	FOKOZOTT BIZTONSÁGI OSZTÁLY

Ez megfelel a MeH ITB 12. ajánlás és az ITSEC szerinti biztonsági osztálybasorolásnak[6].

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

A minosített hitelesítés szolgáltató rendszerre, annak fizikai és személyi környezetére vonatkozó biztonsági követelményeket a szolgáltató „A minosített hitelesítés szolgáltatás komplex biztonsági követelményrendszere” címu dokumentuma tartalmazza. A melléklet ebbol az elofizetok számára legfontosabb biztonsági követelményeket tartalmazza.

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

A MÁV INFORMATIKA Kft. társasági szintu biztonságpolitikájának és szabályzatának, valamint a PKI Változásmenedzsment Szabályzatának megfeleloen a hitelesítés és az idobélyegzés 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 minosített 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 minosített szolgáltatói követelményeknek.

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

7.4.5. Muködtetés menedzsment

A muködtetés menedzsment a minosített szolgáltatói követelményeknek felel meg.

A muködtetés menedzsmentre érvényesek a MÁV INFORMATIKA Kft. által üzemeltett informatikai rendszerre alkalmazott társasági szintu muködtetés menedzsment szabályok. Ezeken túlmenoen az idobélyegzést támogató informatikai rendszerre vonatkozóan a muködtetés 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 minosített szolgáltatói követelményeknek.

A muködtetés menedzsmentre érvényesek a MÁV INFORMATIKA Kft. társasági szintu, illetve a PKI Üzleti Egység vonatkozó szabályzatai, amelyek a következok:

- a MÁV INFORMATIKA Kft. Informatikai Biztonságpolitikája,
- a MÁV INFORMATIKA Kft. Informatikai Biztonsági Szabályzata,
- A PKI Szolgáltatások Informatikai Biztonságpolitikája,
- A PKI Szolgáltatások Biztonsági Szabályzata.

7.4.7. A biztonságos rendszer bevezetése és karbantartása

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

- elvégezte a teljes hitelesítés és idobélyegzés szolgáltató rendszer, annak fizikai és személyi környezetének kockázatelemzés alapú vizsgálat, amelynek eredményeit egy vizsgálati jelentés tartalmazza,
- kidolgozta a szolgáltató rendszer megvalósítása elott a minosített 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 következo esetekben kompromittálódik:

1. a MÁV INFORMATIKA Kft. minosített Root CA aláíró kulcs kompromittálódása,
2. a MÁV INFORMATIKA Kft. minosített Produktív CA aláíró kompromittálódása,
3. az ISZ aláíró kulcs kompromittálódása,
4. Az ISZ idoalap kalibrációjának elvesztése

esetén.

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

Az 1., 2. és 3. kulcs kompromittálódás esetei katasztrófa („A” osztályú) eseménynek, a 4. eset súlyos üzemzavarnak („B” osztályú eseménynek) minosülnek, amelyek kezelésére a HSZSZ-M 4.8 pontja és a PKI Szolgáltatások Üzletmenet-folytonossági Terve tartalmazza az intézkedéseket.

7.4.9. Az ISZ muködésének befejezése

Az ISZ befejezi muködését, ha a MÁV INFORMATIKA Kft. tulajdonosa és vezetése ilyen határozatot hoz. Az ISZ muködése befejezésének oka lehet katasztrófa szintu vagy más esemény, amelynek következtében megszünteto határozat születik.

Az ISZ muködése felfüggesztésének oka lehet az NHH, mint hatóság felfüggeszto 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 idobélyegzés szolgáltatás muködtetésével kapcsolatos adatok rögzítése

Az idobélyegzéssel kapcsolatosan a következo adatok kerülnek rögzítésre:

- az idobélyegzés szolgáltatás fo lépései, a kérelemtol az idobélyeg válasz elküldésig,
- az ISZ aláíró kulcs életciklusában bekövetkezo események (generálás, használat, visszavonás, megsemmisítés),
- az ISZ aláíró kulcs tanúsítványa életciklusában bekövetkezo események (kiadás, használat, visszavonás).
- a rögzített adatok a HSZSZ-M 4.5 pontjával összhangban naponta naplózásra és tárolásra kerülnek. A naplók értékelése naponta megtörténik. A tárolt naplók archiválása a HSZSZ-M 4.6 pontjával összhangban történik.
  Az archivált adatok megorzési ideje 10 év.

7.5. Szervezeti séma

Az idobélyegzés szolgáltatást a MÁV INFORMATIKA Kft. 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 Szerzodési Feltételek Minosített Elektronikus Aláírással Kapcsolatos Szolgáltatásokhoz

HSZSZ-M: Szolgáltatási Szabályzat Minosített Elektronikus Aláírással Kapcsolatos Szolgáltatásokhoz

ISZR: Idobélyegzés Szolgáltatási Rend

ISZ: Idobélyegzés Szolgáltató (jelen dokumentumban a MÁV INFORMATIKA Kft.)

NHH: Nemzeti Hírközlési Hatóság

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

CRL: Certificate Revocation List, magyarul: Tanúsítvány Visszavonási Lista

Melléklet

Az idobélyegzést szolgáltató alrendszer informatikai biztonsági követelményei

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

Ezen követelményeket részletesen a szolgáltató „A minosített hitelesítés szolgáltatás komplex biztonsági követelményrendszere" címu dokumentuma tartalmazza.

Itt csak az elofizetok szempontjából legfontosabb követelményeket emeljük ki.

Fizikai biztonsági követelmények

Az idobélyegzés szolgáltató informatikai rendszer a Bizalmi Központba került elhelyezésre, amely a következo követelményeknek felel meg:

- a fokozott biztonsági szintnek megfelelo 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 elott biztonsági szegmens van kialakítva, amelybe anti-passback és naplózási tulajdonságokkal bíró belépteto rendszere keresztül lehet csak bejutni,
- a Bizalmi Központba történo bejutást video biztonsági kamerás rendszer figyeli, amelynek személyes felügyelete folyamatosan biztosított,
- a Bizalmi Központ rendelkezik önálló és kettozött klimatizálással, valamint mozgásérzékelo, tuz- és füstjelzo és tuzoltó rendszerrel,
- a Bizalmi Központ IT eszközei két, egymástól független külso betáplálással támogatott, dízel 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 képezo 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 szerepköru vezetok 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 muködtetési és menedzselési és a biztonsági dokumentáció elektronikusan tárolt,
- a Szolgáltató az érzékeny adatokat tartalmazó adathordozó eszköztol biztonságosan válik meg, amennyiben azokra már nincs szükség,
- 60 DB elnyomással rendelkezo EMC védelemmel ellátott,
- az informatikai rendszer két független nyomvonalon vezetett üvegkábellel kapcsolódik az Internethez,
- a lokális telefonkapcsolat az EMC zónahatáron szuron keresztül kapcsolódik a szolgáltató telefonközpontjához.

A környezetei elemek, rendszerek alábbi állapotjellemzoit monitor rendszer figyeli:

- homérséklet,
- páratartalom
- légnyomás,
- tuzeset érzékelés,
- tápáramellátás üzemkészség,
- légkondicionáló rendszer üzemkészség,
- biztonsági rendszer jelzései.

A bekövetkezo események naplózásra, majd archiválásra kerülnek.

Logikai biztonsági követelmények

Az idobélyegzo szerverhez hozzáférési jogosultsággal rendelkezo üzemeltetok azonosítása-hitelesítése fokozott biztonsági szintnek megfelelo azonosítás-hitelesítés politika szerint történik.

A hozzáférés szabályozását alapvetoen az idobélyegzo szerver operációs rendszere (Windows 2000) határozza meg. A Windows 2000 által nyújtott beállítási lehetoségek figyelembe vételével a fokozott biztonsági szintnek megfelelo beállításokat kell alkalmazni.

Ugyanez érvényes a naplózási és az audit politikára is.

Az idobélyegzo szerver hálózati szintu biztonságát a következo intézkedésekkel kell biztosítani:

- leválasztás az Internetrol tuzfallal,
- az idobélyegzo szerver számára a tuzfalon egy önálló, a többi biztonsági szegmenstol különbözo szegmenst kell létrehozni.

Személyi biztonsági követelmények

A személyek vonatkozásában ugyanazokat a követelményeket kell érvényesíteni a munkakörbe, illetve a szerepkörbe történo kiválasztásnál, a bizalmi szerepkörök

szétválasztásánál, a képzettségi szint és a gyakorlat meghatározásánál, mint amelyek a HSZSZ-M 5.2 és 5.3 pontjaiban szerepelnek.

Az idobélyegzés szolgáltatást támogató rendszer megbízható muködés szempontjából fokozott biztonsági osztályba sorolt.

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

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