

Magyar Telekom

Minősített Időbélyegzés-szolgáltatás

Időbélyegzési Rendje

Egyedi objektum-azonosító (OID):1.3.6.1.4.1.17835.7.1.2.11.3.12.1.8

Verziószám:..... 1.8

Regisztrációs szám:..... HL/13727/2010

Hatályba lépés dátuma:.....2010.06.20.

Változáskezelés

Verziószám	Dátum	A változás leírása
0.90	2004-05-10	Első változat (szakértői munkaanyagok)
0.91	2004-05-17	Javított tervezet
0.92	2004-05-21	Ellenőrzött változat
0.93	2004-05-23	Magyar Telekom Rt.-nek átadott változat
1.0	2004-05-28	Nemzeti Hírközlési Hatósághoz benyújtott változat
1.1	2004-07-17	Hatósági szemlét követő módosítások átvezetés
1.2	2004-09-27	Hatóság részére átadott végleges változat
1.3	2005-09-01	Magyar Telekom névváltásának és következményeinek módosítása
1.4	2005.12.30.	Külső szakértői felülvizsgálat javaslatainak átvezetése
1.5	2006.07.20. 2006.08.19.	Nemzeti Hírközlési Hatóság Hivatalának észrevételei szerinti javítások
1.6	2006.12.18.	2006. évi Hatósági szemle észrevételei szerinti javítások
1.7	2009.03.01	A Hatóság észrevételei szerinti módosítás (HL-923-1/2009)
1.8	2010. 06. 20.	A hitelesítés szolgáltatások kivezetésével és a minősített időbélyegzés szolgáltatás további nyújtása kapcsán végzett felülvizsgálat

Módosítást készítette: Domokos Zoltán	Technológia/ IT üzemeltetési igazgatóság	Senior biztonsági szolgáltatási menedzser
Ellenőrizte: Dr. Barczy Gergely	Csoport Központ / Vállalati üzletágot támogató jogi osztály	Szakértő
Jóváhagyta: Hári Krisztián Péter	Technológia/ IT üzemeltetési igazgatóság	IT biztonsági osztály mb. vezetője

Tartalomjegyzék

Változáskezelés	2
1 Bevezetés	5
1.1 A szabályzat	5
1.2 A TSP hatályai	5
1.3 A Szolgáltató	6
1.4 Időbélyegzés-szolgáltatás meghatározása	7
1.5 Szabványok és jogszabályi megfelelés	8
1.6 TSP elérhetősége, azonosítása	8
1.7 Közösség és alkalmazhatóság	9
2 Általános rendelkezések	10
2.1 Időbélyegzés-szolgáltatás komponensei	10
2.2 Időbélyegzés-szolgáltató	11
2.3 Végfelhasználók	11
2.4 A TSP és az Időbélyegzés Szolgáltatási Szabályzat	11
2.4.1 A TSP és az Időbélyegzés Szolgáltatási Szabályzat kapcsolata	11
2.4.2 Szolgáltató időbélyegzés-szolgáltatáshoz kapcsolódó szabályzatai	12
2.4.3 TSP és IBSzSz kidolgozásának elvei	12
3 Időbélyegzési Rend (TSP)	13
3.1 Áttekintés	13
3.2 Azonosítás	13
3.3 Időbélyegzés-szolgáltatás felhasználó	13
3.4 Időbélyegzés-szolgáltatás megfelelősége	13
4 Kötelezettségek és felelősség	14
4.1 Szolgáltató kötelezettségei végfelhasználók felé	14
4.2 Előfizető kötelezettségei	14
4.3 Érintett félre vonatkozó ajánlások	15
4.4 Felelősség	16
5 Működésre vonatkozó követelmények	17
5.1 Időbélyegzés-szolgáltatás szabályozása és közzététele	17
5.1.1 Időbélyegzés-szolgáltatás szabályozása	17
5.1.2 Időbélyegzés-szolgáltatás közzététele	17
5.2 Kulcsgondozás	19
5.2.1 Az időbélyegzés-szolgáltatás aláíró kulcsának generálása	19
5.2.2 A Szolgáltató magán kulcsának védelme	19
5.2.3 A Szolgáltató nyilvános kulcsának közzététele	19
5.2.4 A Szolgáltató kulcsának érvényessége	19
5.2.5 A Szolgáltató kulcs használatának befejezése	20
5.2.6 A HSM egység életciklusa	20
5.3 Időbélyegzés-szolgáltatás	20

5.3.1	Időbélyeg profil.....	20
5.3.2	Óraszinkronizálás az UTC-vel.....	21
5.4	Időbélyegzés-szolgáltatás üzemeltetése és menedzsmentje.....	22
5.4.1	Biztonsági óvintézkedések.....	22
5.4.2	Komponensek osztályba sorolása	22
5.4.3	Személyzeti óvintézkedések	23
5.4.4	Fizikai óvintézkedések	23
5.4.5	Üzemeltetés	23
5.4.6	Hozzáférési jogosultságok kezelése.....	23
5.4.7	Rendszer telepítése, karbantartása	23
5.4.8	Időbélyegzés-szolgáltatás üzletmenet-folytonossága.....	24
5.4.9	Szolgáltató működésének leállítása	24
5.4.10	Jogsabályi megfelelés.....	24
5.4.11	Időbélyegzés-szolgáltatással kapcsolatos adatok rögzítése	24
5.5	Szervezeti felépítés	25
6	Jelölések, rövidítések és meghatározások.....	26
7	Hivatkozások.....	28

1 Bevezetés

Az **elektronikus aláírással** kapcsolatos szolgáltatások köréből a Magyar Telekom a minősített időbélyegzés szolgáltatást nyújtja.

1.1 A szabályzat

Ez a szabályzat a **Magyar Telekom Nyrt. Minősített** Időbélyegzés-szolgáltató (továbbiakban: Szolgáltató) által nyújtott időbélyegzés-szolgáltatás működésére vonatkozó követelményeket, az időbélyeg szerkezetét, az időbélyegzés szolgáltatás menedzsment, ill. az időbélyegzéshez tartozó kulcsmenedzsment életciklusára vonatkozó szabályokat és egyéb általános követelményeket határoz meg.

A dokumentum teljes neve: **Magyar Telekom Minősített Időbélyegzés-szolgáltatás Időbélyegzési Rendje**.

A dokumentum rövid neve: **Időbélyegzési Rend** (továbbiakban: TSP).

A TSP-ben nem szereplő, az időbélyegzés-szolgáltatással kapcsolatos eljárási és egyéb működési szabályokat a **Magyar Telekom Időbélyegzés Szolgáltatási Szabályzat**¹ (továbbiakban: IBSzSz) [6] tartalmazza.

1.2 A TSP hatályai

A TSP tárgyi hatálya

A TSP tárgyi hatálya az {1.4 Időbélyegzés-szolgáltatás meghatározása} alfejezetben ismertetett szolgáltatás nyújtására és igénybevételére, illetve ezen szolgáltatással kapcsolatos összes objektumra és tárgyi eszközre kiterjed.

A TSP területi hatálya

A TSP területi hatálya Magyarország teljes területe.

A TSP időbeli hatálya

A TSP határozatlan időre szól a címlapon feltüntetett szabályzati verzióra érvényes hatálybalépés dátumától kezdődően. A TSP időbeli hatálya az időbélyegzés-szolgáltatás beszüntetésekor, illetve egy újabb szabályzati verzió hatályba lépésékor szűnik meg.

¹ Az ETSI TS 102 023 szabvány által használt Time Stamping Authority Practice Statement az IBSzSz részét képezi.

A TSP személyi hatálya

A TSP személyi hatálya a {1.7 Közösség és alkalmazhatóság} alfejezetben meghatározott felhasználói közösség minden egyes tagjára, természetes, jogi személyiségű illetve jogi személyiséggel nem rendelkező személyekre egyaránt kiterjed.

1.3 A Szolgáltató

A TSP-ben Szolgáltató alatt a Magyar Telekom Nyrt. által – a saját szervezetén belül – létrehozott **Magyar Telekom Időbélyegzés szolgáltatót** (időbélyegző szervezetet) kell érteni. A Szolgáltatót jogi értelemben a **Magyar Telekom Nyrt.** képviseli.

A Szolgáltató minősített szolgáltatókénti nyilvántartásba vételének napja: 2004. október 01.

A Szolgáltató (Magyar Telekom Nyrt.) adatai a következők:

Név: Magyar Telekom Távközlési Nyilvánosan Működő Részvénytársaság
Cégjegyzékszám: CG 01-10041928
Székhely: 1013 Budapest, Krisztina krt. 55.
Postacím: 1541 Budapest
Telefon: +36-1-458 7346
Fax: +36-1-458 7335
Honlap: <http://www.telekom.hu/>

A Minősített Időbélyegző Szervezet elérési adatai a következők:

Név: Magyar Telekom NyRt./ Minősített Időbélyegző Szervezet
Cím: 1117 Budapest Magyar tudósok körút 9.
Telefon: +36 1 481-7447
Fax: +36-1-481-7455
Postacím: 1541 Budapest
Honlap: http://www.t-systems.hu/nagyvallalatok/hitelesites_szolgáltatások/idobelyegzes_szolgalatas
E-levelelcím: timestamp@telekom.hu

Az Időbélyegző Szervezet általában munkanapokon **8 és 16 óra között** tart nyitva, de egyes napokon ettől eltérő nyitvatartási időpont is lehetséges. Hibabejelentéssel, valamint időbélyegzés kérésre jogosító autentikációs tanúsítvány visszavonási szolgáltatással kapcsolatos szolgáltatás a fenti munkaidőn túl elérhető az alábbi telefonon:

24 órás ügyelet telefonszáma: +36-30-444-17-31

Az Időbélyegző Szervezet aktuális adatai a Szolgáltató fenti internetes honlapján megtekinthetők.

Az időbélyegzés-szolgáltatással kapcsolatos további szervezetek elérhetőségeit az IBSzSz [6] dokumentum tartalmazza.

1.4 Időbélyegzés-szolgáltatás meghatározása

Az Eat 2.§ 16. alapján az időbélyegző: elektronikus dokumentumhoz végérvényesen hozzárendelt vagy azzal logikailag összekapcsolt olyan adat, amely igazolja, hogy az elektronikus dokumentum az időbélyegző elhelyezésének időpontjában változatlan formában létezett.

Az **időbélyegzés-szolgáltatás** során a Szolgáltató az elektronikus dokumentumhoz időbélyegzőt kapcsol.

Az időbélyegzés-szolgáltatás bizonyítékot nyújt arról, hogy egy adatelem változatlan formában létezett egy megadott időpontban (a **létezés** bizonyítéka). Ha az adatelemet az adatkérő azelőtt aláírta, mielőtt továbbította volna az időbélyegzés-szolgáltató számára, akkor az időbélyegzés-szolgáltatás bizonyítékul szolgál arra nézve, hogy az adott adatelem létezett és ezen entitás birtokában volt abban a bizonyos időpontban (a **birtoklás** bizonyítéka). Az időbélyegzés-szolgáltató, mint harmadik fél megbízhatóan gondoskodik az időbélyegzés-szolgáltatásról.

A Szolgáltató által nyújtott időbélyegzés-szolgáltatás hozzákapcsolható fokozott, ill. minősített aláírással ellátott elektronikus dokumentumhoz, továbbá aláírással nem ellátott állományok esetében is használható.

A szolgáltatáshoz kétféle tevékenység köthető:

- **időjel ellátás**, amelyet a Szolgáltató az időbélyegzés szolgáltatáshoz tart fenn, hitelesített időforráshoz történő szinkronizálás érdekében és
- maga az **időbélyegzés-szolgáltatás**, amelyet a Szolgáltató minősített időbélyegzés-szolgáltatásként (előfizetéses alapon) nyújt ügyfeleinek.

Az időbélyegyek használata során **kétféle alapl műveletet** kell elvégezni:

- **időbélyegzést** (folyamatot), amely az adatokat időértékekkel kapcsolja össze kriptográfiai eszközök segítségével és
- **időbélyeg-ellenőrzést** (folyamatot), amely kiértékeli ezeknek az összekötéseknek a megfelelőségét.

Az időbélyegzés-szolgáltatás során a Szolgáltató (bizonyíthatóan) nem ismeri meg az időbélyegzett dokumentum tartalmát, és csak az abból képzett lenyomatot kezeli.

A Szolgáltató két hozzáférési módot ajánl az időbélyegzés-szolgáltatáshoz:

- az első általában egyedi – dedikált – hozzáférés, melyen jellemzően a nagy forgalmú ügyfelek részére szolgálat²
- a második az Internet alapú hozzáférés, mellyel a lehető legszélesebb felhasználói körre kiterjeszhető a szolgáltatás.

A Szolgáltató időbélyegző infrastruktúrája pontosság és biztonság tekintetében **megfelel** a 3/2005 (III.18) IHM rendelet vonatkozó előírásainak.

1.5 Szabványok és jogszabályi megfelelés

Jelen TSP tartalmában és szerkezetében összhangban van az időbélyegzés-szolgáltatókra és időbélyegzés-szolgáltatásra vonatkozó követelményekről szóló ETSI TS 102 023 [4] és az időbélyeg profilra vonatkozó ETSI TS 101 861 [7] EU szabványoknak.

Az TSP tartalmi vonatkozásokban eleget tesz a hazai jogszabályok előírásainak, ajánlásainak és Szolgáltató belső szabályzatainak, továbbá felhasználja a [5] műszaki specifikációt.

1.6 TSP elérhetősége, azonosítása

A dokumentum teljes neve az {1.1 Szabályzat} alfejezetben található. A TSP az alábbi adatokkal azonosítható:

Egyedi objektum-azonosító (OID): TSP fedőlapján található
Regisztrációs szám:..... TSP fedőlapján található
Verziószám: TSP fedőlapján található
A hatályba lépés dátuma..... TSP fedőlapján található
Az időbélyegző-szolgáltatás **technikai azonosítója:**..... Magyar Telekom TSA v1.0.

A TSP nyilvános dokumentum, melynek mindenkor aktuális változatát Szolgáltató az Interneten a http://www.t-systems.hu/nagyvallalatok/hitelesites_szolgaltatasok/idobelyegzes_szolgaltatas

címen keresztül teszi elérhetővé.

² Ez bizonyos technikai korlátozásokat jelent, például megkövetelheti a *bérelt vonali* kommunikációs csatornák vagy egyéb egyedi megoldások használatát.

1.7 Közösség és alkalmazhatóság

A Szolgáltató időbélyegzés szolgáltatásához tartozó közösség (a továbbiakban: **Közösség**) az alábbiakból áll:

- a Szolgáltató időbélyegzés szolgáltatás szervezetei:
 - Időbélyegző szervezet, mint az időbélyegző szerverek üzemeltetéséért felelős szervezet, ügyfélszolgálat.
- A Magyar Telekom Technológia és Üzemeltetés és Fenntartás Igazgatóság, NGN Alkalmazás üzemeltetési osztály, mint az időjel ellátó rendszer üzemeltetője,
- a végfelhasználók {2.3 alfejezet}.

2 Általános rendelkezések

2.1 Időbélyegzés-szolgáltatás komponensei

A hiteles időadathoz kétféle tevékenység köthető:

- **időbélyegzés-szolgáltatás**, amellyel a Szolgáltató minősített időbélyegzés-szolgáltatásként (előfizetéses alapon) támogatja belső és külső ügyfeleit.
- Időbélyegzés szolgáltatást menedzselő folyamatok, **hiteles időjel ellátás**

Az időbélyegzés-szolgáltatás során **kétféle alaplételemet** kell elvégezni:

- **időbélyegzést** (folyamatot), amely az adatokat időértékekkel kapcsolja össze kriptográfiai eszközök segítségével
- és
- **időbélyeg-ellenőrzést** (folyamatot), amely az alábbi funkciókat látja el:
 - kiértékeli az időbélyegzéskor használt összeköttetések megfelelőségét, ill. szükség esetén beavatkozik,
 - felügyeli az időbélyegző szerverek belső szinkronizálását, működését, leállás esetén beavatkozik,
 - biztosítja az időbélyegzéshez használt időjel UTC³ időalaphoz való szinkronizálását,
 - időbélyegző szerverek forgalmát felügyeli, karbantartja, szükséges mentéseket elvégzi,
 - felügyeli az időbélyegyek időpontjának hitelességét az {5.3.2 Óraszinkronizálás az UTC-vel} alfejezetben leírtak alapján.

Az időbélyegzéshez használt kulcspárhoz tartozó tanúsítványokat Szolgáltató a Magyar Telekom Root CA-ból adja ki. A Magyar Telekom Root CA működtetésével kapcsolatban az IBSzSz[6] 6. fejezete tartalmaz bővebben információt

Az időbélyegzés-szolgáltatás során a Szolgáltató (bizonyíthatóan) nem ismeri meg az időbélyegzett dokumentum tartalmát, és csak az abból képzett lenyomatot kezeli.

A Szolgáltató időbélyegző infrastruktúrája pontosság és biztonság tekintetében **megfelel** a 3/2005 (III.18) IHM rendelet erre vonatkozó előírásainak.

³ UTC: Coordinated Universal Time

2.2 Időbélyegzés-szolgáltató

Az időbélyegzés-szolgáltatást az {1.3 A Szolgáltató} alfejezetben meghatározott Szolgáltató nyújtja.

2.3 Végfelhasználók

A Szolgáltató által nyújtott időbélyegzés-szolgáltatás végfelhasználói az alábbiak lehetnek:

- előfizető, aki az időbélyegzés-szolgáltatást Szolgáltatóval kötött szerződés alapján igénybe veszi,
- érintett fél.

Az **előfizető** olyan tetszőleges természetes vagy jogi személy, vagy jogi személyiséggel nem rendelkező szervezet lehet, aki/amely elfogadja a Szolgáltató szabályzataiban (különösképpen jelen TSP-ben) meghatározott kötelezettségeket, és aki fizet a szolgáltatásért.

Az előfizető szerződéses viszonyban áll a Szolgáltatóval a vonatkozó Időbélyegzés Szolgáltatói Szerződésben (továbbiakban: ISzS [9], Magyar Telekom Időbélyegzés-szolgáltatás Általános Szerződési Feltételek (továbbiakban: ÁSZF) [8] és a TSP dokumentumokban foglaltak szerint. A Szolgáltató az előfizetővel elsősorban az Időbélyegző Szervezeten keresztül tart kapcsolatot. Előfizető az időbélyegzés-szolgáltatást kizárólag a TSP-ben és ISzS-ben meghatározott módon és célra veheti igénybe.

Az **érintett fél** természetes vagy jogi személy, vagy jogi személyiséggel nem rendelkező szervezet lehet, a Közösség olyan tagja, aki az elektronikus dokumentum fogadója és egy hitelesített időpontra hagyatkozva jár el az aláírás és/vagy az időbélyeg hitelességének ellenőrzésekor.

2.4 A TSP és az Időbélyegzés Szolgáltatási Szabályzat

2.4.1 A TSP és az Időbélyegzés Szolgáltatási Szabályzat kapcsolata

Szolgáltató, mint minősített időbélyegzés-szolgáltató nyújtja az {1 Bevezetés} fejezetben meghatározott szolgáltatásokat. Szolgáltató az általa nyújtott időbélyegzés szolgáltatásra vonatkozóan rendelkezik szolgáltatási szabályzattal, melynek rövidített neve: IBSzS [6]. A TSP-ben nem szabályozott, az időbélyegzés-szolgáltatásra vonatkozó jogi, kereskedelmi és egyéb eljárási szabályokat, a Szolgáltató aktuális IBSzS dokumentuma tartalmazza.

Az IBSzS nyilvános dokumentum, melynek mindenkori aktuális változatát Szolgáltató az Interneten a

http://www.t-systems.hu/nagyvallalatok/hitelesites_szolgáltatások/idobelyegzes_szolgalatas

címen keresztül teszi elérhetővé.

2.4.2 Szolgáltató időbélyegzés-szolgáltatáshoz kapcsolódó szabályzatai

Az Szolgáltató időbélyegzés-szolgáltatáshoz kapcsolódó nyilvános szabályzatai a következők:

- TSP (jelen dokumentum),
- IBSzSz [6],
- ÁSzF [8].

2.4.3 TSP és IBSzSz kidolgozásának elvei

A TSP a Szolgáltatóra és időbélyegzés-szolgáltatására vonatkozó követelményeket tartalmazza.

Az IBSzSz az adott konkrét gyakorlati megvalósítást támogató szervezeti, folyamati, személyzeti szabályokat tartalmazza, a Szolgáltató belső és nyilvános szabályzatai alapján, azokkal összhangban.

3 Időbélyegzési Rend (TSP)

3.1 Áttekintés

A Szolgáltató időbélyegzés-szolgáltatását a {2.3 Végfelhasználók} alfejezetben meghatározott előfizetők a Szolgáltatóval kötött szerződésben meghatározott célra vehetik igénybe. Szolgáltató nem korlátozza az időbélyegzés-szolgáltatás felhasználását az időbélyeggel ellátott elektronikus irat típusa vagy hitelesítése vonatkozásában.

Szolgáltató az időbélyegzés-szolgáltatás működésére vonatkozó általános követelmények vonatkozásában a [4] szabványt, míg a felhasználói és az időbélyegzést támogató alkalmazásaira és az időbélyeg profiljára – szerkezeti és tartalmi összetételére –vonatkozóan az ETSI TS 101 861 [7] szabványt követi.

Az időbélyegzés-szolgáltatás során, Szolgáltató közte és a végfelhasználók közötti kommunikáció tekintetében betartja az [5] szabványt, továbbá biztosítja az időbélyegzés-szolgáltatás pontosságát. Pontosság tekintetében az eltérés mindig kisebb kell legyen, mint 1 másodperc.

3.2 Azonosítás

Jelen TSP azonosítása és elérhetősége az {1.6 TSP elérhetősége, azonosítása} alfejezetben meghatározott módon történik.

Minden időbélyeg tartalmazza jelen TSP OID számát.

3.3 Időbélyegzés-szolgáltatás felhasználó

A Szolgáltató időbélyegzés-szolgáltatását az {1.7 Közösség és alkalmazhatóság} alfejezetben meghatározott Közösség, valamint a Szolgáltatóval kötött szerződés alapján és abban meghatározott módon Előfizetők vehetik igénybe.

3.4 Időbélyegzés-szolgáltatás megfelelése

Szolgáltató az időbélyegzés-szolgáltatás vonatkozásában az {1.5 Szabványok és jogszabályi megfelelés} alfejezetben meghatározott jogszabályi és egyéb műszaki szabványok szerinti megfeleléseit, külső és belső auditorok által rendszeresen elvégzett ellenőrzésekkel biztosítja.

4 Kötelezettségek és felelősség

A Szolgáltató alapvető kötelezettsége, hogy vállalt időbélyegzés-szolgáltatását a jelen és egyéb nyilvános szabályzatokkal, szerződéssel – a [6], [7], [8], [9] dokumentumok –, továbbá a Szolgáltató belső biztonsági szabályzataival összhangban nyújtsa.

Szolgáltató általános kötelezettségei az IBSzSz [6] dokumentum {9.6.1 Az időbélyegzés szolgáltató felelőssége és helyállása} alfejezetben került meghatározásra.

4.1 Szolgáltató kötelezettségei végfelhasználók felé

Szolgáltató időbélyegzés-szolgáltatás során a következő kötelezettségeket vállalja a végfelhasználók irányába:

- 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,
- nem ismeri meg az időbélyegzett dokumentum tartalmát, és csak az abból képzett lenyomatot kezeli,
- időbélyeg aláíró kulcsát csak az időbélyegzés keretén belül használja,
- az időbélyegyet 1 másodpercen belüli pontossággal adja ki,
- az időbélyegzés-szolgáltatás megbízhatóságát és biztonságát a minősített hitelesítés-szolgáltatókra vonatkozó követelmények szerint biztosítja,
- rögzíti az időbélyegzéssel kapcsolatos minden fontos eseményt, ezeket naplózza és a napló állományokat biztonságosan tárolja.

4.2 Előfizető kötelezettségei

Szolgáltató időbélyegzés-szolgáltatása során, az előfizetővel szemben támasztott kötelezettségeket az alábbiak határozzák meg.

- Az időbélyegzés-szolgáltatáshoz Előfizető köteles gondoskodni a Szolgáltató időbélyegző egységeihez való kommunikáció kialakításáról (pl. Internet vagy bérelt vonali kapcsolat), valamint a szolgáltatás igénybevételéhez szükséges szoftveralkalmazásról, a Szolgáltatóval előzetesen egyeztetett műszaki feltételek alapján. Szolgáltató a teljes a folyamat során

köteles együttműködni előfizetővel. Előfizető és Szolgáltató megállapodhatnak abban, hogy a fent említett kommunikációs kapcsolat kialakítását és/vagy szoftveralkalmazást Szolgáltató biztosítja, külön díj ellenében.

- Előfizető köteles megadni a Szolgáltatóival kötött szerződésben rögzítettek szerint az időbélyegzés szolgáltatás igénybevétele céljából Szolgáltató által Előfizető részére kiállítandó autentikációs tanúsítvány kiállításához szükséges adatokat.
- Előfizető köteles a Szolgáltató képviselőjétől megkapott autentikációs tanúsítványt a szolgáltatásra jogosult felhasználói számára átadni illetve telepíteni; ennek keretében köteles teljes gonddal eljárni, hogy megelőzze a tanúsítványhoz tartozó magánkulcs (és ezáltal a szolgáltatás) illetéktelen felhasználását. A szolgáltatás igénybevételeéről valamint az autentikációs tanúsítványhoz tartozó magánkulcs illetéktelen felhasználásának megakadályozásáról Előfizető köteles a jogosult felhasználóinak is tájékoztatást és útmutatót adni.
- Előfizető köteles késedelem nélkül értesíteni a Szolgáltatót, amennyiben az autentikációs tanúsítvány magánkulcsa kompromittálódott, illetve tudomására jutott annak illetéktelen felhasználása. Az autentikációs tanúsítvány illetéktelen felhasználásából következő károkért a Szolgáltató nem vállal felelősséget.
- Előfizető köteles az időbélyegzés-szolgáltatás díját a Szolgáltatóval kötött szerződés szerint megfizetni. A díj számítás alapja az autentikációs tanúsítvánnyal történt időbélyeg-kérés sikeres kiszolgálása. A Szolgáltatási Szerződés ettől eltérően is rendelkezhet.

4.3 Érintett félre vonatkozó ajánlások

Szolgáltató időbélyegzés-szolgáltatás során az érintett féllel nincs szerződéses viszonyban, ezért Szolgáltató kötelezettségek helyett ajánlásokat fogalmaz meg érintett fél irányába. Az érintett félre vonatkozó ajánlásokat az IBSZSZ [6] szabályzat, illetve az alábbiak határozzák meg.

Ha az érintett fél ésszerű módon egy időbélyegre kíván hagyatkozni, akkor javasolt ellenőriznie az időbélyeget, valamint az időbélyegző egység (időbélyegző szerver) tanúsítványának, illetve az ezt kiadó Magyar Telekom Root CA tanúsítványának érvényességét az érvényes visszavonási állapot információ felhasználásával, a szabályzatoknak megfelelően.

A Szolgáltató által kiadott időbélyegek ajánlott ellenőrzési lépései a következők:

- annak megvizsgálása, hogy az időbélyeget a Szolgáltató elektronikusan aláírta,
- a Szolgáltató által történt aláírás az időbélyegzésre szolgáló kulccsal történt-e és a hozzátartozó tanúsítvány érvényes-e,
- a szolgáltatói tanúsítvány érvényességét az időbélyeget felhasználók az IBSzSz-ben [6] meghatározott gyakorisággal közzétett CRL alapján ellenőrizhetik, amely a

http://www.t-systems.hu/nagyvallalatok/hitelesites_szolgáltatások/idobelyegzes_szolgáltatás web lapon keresztül érhető el.

4.4 Felelősség

A Szolgáltató felelősségét az IBSzSz [6] szabályzat {9.6} és a {9.2 Anyagi felelősség vállalás, felelősségbiztosítás} alfejezete, valamint az alábbiak határozzák meg.

Szolgáltató időbélyegző-szervezete felelős az időbélyegzés-szolgáltatás igénybevételéhez szükséges autentikációs tanúsítvány kiállításáért, a kapcsolódó kulcspár létrehozásáért, valamint annak az Előfizető számára védett módon történő átadásáért.

Szolgáltató felelős az Előfizető kérése alapján az időbélyegzés-szolgáltatás igénybevételéhez szükséges autentikációs tanúsítvány visszavonásáért.

Az előfizető és érintett fél felelősségét az IBSzSz [6] szabályzat {9.6.2 Az előfizető felelőssége és helytállása} és a {9.6.3 Az érintett fél felelőssége} alfejezetek határozzák meg.

5 Működésre vonatkozó követelmények

5.1 Időbélyegzés-szolgáltatás szabályozása és közzététele

5.1.1 Időbélyegzés-szolgáltatás szabályozása

A Szolgáltató időbélyegzés-szolgáltatását támogató informatikai rendszerét, az időbélyegeken használt hiteles időjelet az {5.3.2 Óraszinkronizálás az UTC-vel} leírt infrastruktúra biztosítja.

Szolgáltató az időbélyegzés-szolgáltatásai feltételeit, díjazását, egyéb műszaki információkat az Interneten a

http://www.t-systems.hu/nagyvallalatok/hitelesites_szolgáltatások/idobelyegzes_szolgáltatás

címen keresztül teszi közzé. A weboldalon az időbélyegző egység(ek) aláíró tanúsítványa és a vonatkozó CRL letölthető formában elérhető. A közzététel további részleteit a {5.1.2 Időbélyegzés-szolgáltatás közzététele} alfejezet tartalmazza.

Az időbélyegzés-szolgáltatás további szabályozási kérdéseit az IBSzSz [6] szabályzat határozza meg.

5.1.2 Időbélyegzés-szolgáltatás közzététele

Szolgáltató az időbélyegzés-szolgáltatásra vonatkozó Időbélyegzési Rend (azaz jelen dokumentum) mindenkor aktuális változatát a http://www.t-systems.hu/nagyvallalatok/hitelesites_szolgáltatások/idobelyegzes_szolgáltatás címen közzé teszi. A szolgáltatásra vonatkozó további általános szerződéses dokumentumok (ÁSZF, IBSzSz) szintén itt érhetők el.

A Szolgáltató ezen felül a fenti címen elérhetővé teszi az Időbélyegző egység(ek) tanúsítványait is, valamint az ezeket hitelesítő Magyar Telekom Root CA tanúsítványát is.

Az időbélyegzés-szolgáltatásra vonatkozó egyéb információk:

- a) Szolgáltató az Időbélyegző Szervezeten keresztül érhető el. További részleteket a {1.3 A Szolgáltató} alfejezet tartalmazza.
- b) Jelen Időbélyegzési Rend a dokumentum fedlapján található OID számmal azonosítható. További részleteket a {1.6 TSP elérhetősége, azonosítása} alfejezet tartalmazza.

- c) A szolgáltatás kapcsán alkalmazható hash algoritmus: a mindenkor hatályos NHH határozat szerint alkalmazott algoritmus.
- d) Időbélyeget aláíró Szolgáltatói kulcs érvényességi ideje: 5 év, feltéve, hogy a kulcs ez idő alatt nem kompromittálódik.
- e) Az időbélyegben szereplő idő pontossága: UTC ± 1 másodperc (maximum eltérés).
- f) Az időbélyegzés-szolgáltatás igénybevételének feltételei:
- műszaki feltételek: Előfizetőnek rendelkeznie kell megfelelő szoftveralkalmazással és kommunikációs kapcsolattal. További részleteket a {5.1.1 Időbélyegzés-szolgáltatás szabályozása} alfejezet tartalmazza és
 - jogi, kereskedelmi feltételek: a {2.3 Végfelhasználók} és a {4 Kötelezettségek és felelősség} fejezetekben meghatározott feltételek,
- g) Előfizető kötelezettségei: Előfizető köteles betartani a szolgáltatásra vonatkozó szerződéses feltételeket, köteles biztosítani a műszaki feltételeket, továbbá köteles kifizetni a szolgáltatás díjait. További részleteket a {4.2 Előfizető kötelezettségei} alfejezet tartalmazza.
- h) Érintett fél kötelezettségei: érintett félnek javasolt megtennie a szükséges ellenőrzéseket, mielőtt egy időbélyegre hagyatkozva jár el. További részleteket a {4.3 Érintett félre vonatkozó ajánlások} alfejezet tartalmazza.
- i) Időbélyegzés-szolgáltatás naplóállományok megőrzésének időtartama: keletkezésüktől számított 10 évig vagy jogvita esetén az eljárás lezárásáig Szolgáltató megőrzi a naplóállományokat.
- j) Szolgáltató felelősségének korlátozása: ld. részletesen a {4.4 Felelősség} alfejezetben.
- k) Panaszok és jogi viták rendezése: panaszokat faxon lehet benyújtani Szolgáltató minősített Időbélyegző Szervezet részére. További részleteket az ÁSzF [8] tartalmazza.
- l) Külső független ellenőrző, auditáló szervezetek:
- Nemzeti Hírközlési Hatóság (hatósági ellenőrzést végző szervezet),

- Külső független szakértői auditáló szervezet.

5.2 Kulcsgondozás

5.2.1 Az időbélyegzés-szolgáltatás aláíró kulcsának generálása

Szolgáltató gondoskodik arról, hogy a kulcsgondozás vonatkozásában az elismert szabványoknak megfelelő fizikai, eljárásbeli és személyzeti biztonsági óvintézkedések, valamint az ezeket érvényre juttató adminisztratív és irányítási eljárások kerüljenek alkalmazásra. Részletesen az IBSzSz [6] {6 Műszaki biztonsági óvintézkedések} fejezete határozza meg.

Az Időbélyegző Szervezet kulcsainak generálása FIPS 140-2 szabvány szerint 3. szinten bevizsgált kriptográfiai modulban (Hardware Security Modul, továbbiakban: HSM) történik.

A Szolgáltató időbélyegzés-szolgáltatását kiszolgáló időbélyegző szerverek saját kulcsai a saját HSM-eikben keletkeznek és teljes életciklusuk alatt a HSM-ekben maradnak.

A Szolgáltató időbélyegző szervereinek kriptográfiai moduljai a Hatóság által regisztrált tanúsító cég által tanúsított⁴, és a Hatóság által nyilvántartásba vett HSM.

5.2.2 A Szolgáltató magán kulcsának védelme

A Szolgáltató magánkulcsának védelme megfelel a minősített időbélyegzés-szolgáltatókra vonatkozó előírásoknak. Részletesebben az IBSzSz [6] {6.2 A Szolgáltatói magánkulcsok védelme és a kriptográfiai modulokkal kapcsolatos előírások} alfejezete határozza meg.

5.2.3 A Szolgáltató nyilvános kulcsának közzététele

Az időbélyegző(k) nyilvános kulcsa a http://www.t-systems.hu/nagyvallalatok/hitelesites_szolgáltatások/idobelyegzes_szolgaltatás weboldalon keresztül érhető el.

5.2.4 A Szolgáltató kulcsának érvényessége

A Szolgáltató kulcsának érvényessége 5 év. A Szolgáltató kulcsok használatának időtartamát az IBSzSz [6] {6.3.1 A tanúsítványok és a kulcspárok használatának periódusa} alfejezete, a kulcsok archiválását az IBSzSz [6] {6.2.4 Magánkulcs archiválása} alfejezete határozza meg.

⁴HSM tanúsítványának regisztrációs száma: HUNG-T-044-2008

5.2.5 A Szolgáltató kulcs használatának befejezése

A kulcs érvényességi idejének lejártát követően a kulcs megsemmisítésre kerül az IBSzSz [6] {6.2.9 A magánkulcs megsemmisítésének módja} alfejezetben meghatározottak alapján, továbbá az {6.1.1 Kulcspár előállítás} alfejezetben leírtak alapján Szolgáltató új kulcsot generál.

Amennyiben a Szolgáltató aláíró kulcsa érvényességi ideje alatt kompromittálódik Szolgáltató gondoskodik a tanúsítvány azonnali visszavonásáról, a kulcs azonnali megsemmisítéséről és új kulcs generálásáról.

5.2.6 A HSM egység életciklusa

A Szolgáltató HSM egységeinek szállítása, tárolása és üzembe helyezése szigorú fizikai és személyzeti biztonsági szempontok betartása mellett történt.

A HSM eszközök ellenőrzése, bevizsgálása és értékelése során megállapított legfontosabb tényeket, tulajdonságokat a Hatóság által nyilvántartásba vett eszköz tanúsítvány tartalmazza.

A Szolgáltató eszközök üzemeltetésére vonatkozó biztonsági és egyéb előírásokat az {5.4 Időbélyegzés-szolgáltatás üzemeltetése és menedzsmentje} alfejezet írja le.

5.3 Időbélyegzés-szolgáltatás

5.3.1 Időbélyeg profil

Szolgáltató biztosítja az időbélyegek biztonságos kibocsátását és az időbélyegben szereplő időpont pontosságát. Az időbélyeg profil [4] és [7] szabványok alapján a következőket tartalmazza:

Mezőnév	Érték vagy szabály
Verzió <i>Version</i>	A Szolgáltató időbélyegzés-szolgáltatásának technikai azonosítója: Magyar Telekom TSA v1.0 így a mező értéke: „ v1.0 ”
Időbélyeg kérelemben engedélyezett hash algoritmus	SHA-1, SHA-256, SHA-384, SHA-512
Időbélyeg kérelemben megnevezhető szabályzati azonosító (OID)	Megadása nem kötelező, amennyiben mégis megadásra kerül, értéke azonos az időbélyeg válaszban megnevezett szabályzati azonosítóval .
Időbélyeg kérelemben szereplő véletlen szám (nonce) hossza	64 bit
Időbélyeg kérelemben kérhető-e a szolgáltató tanúsítványa (certReq)	Igen

Pontosság	1 másodperc
Rendezés	False
Időbélyeg válaszban megnevezhető szabályzati azonosító (OID)	A mező értéke az időbélyeg kiadásakor hatályos Időbélyegzési Rend (TSP) OID azonosítója
Az időbélyeg válasznál használt hash algoritmus	SHA-1, SHA-256, SHA-384, SHA-512
Az időbélyeg válasznál használt aláíró algoritmus	RSA
Az időbélyeg válasz időfelbontása (genTime)	0,001 másodperc
Időbélyegző szolgáltatás "UTC max offset" értéke	1 másodperc
Támogatott elérési protokoll	HTTPS
"Store and forward protocol" alkalmazása	Nem támogatott
Sorszám mérete	Dinamikus hosszúságú
Sorszám egyedisége	Szolgáltató egyedi sorszámot definiál, amely sorszámozás egyedisége a szolgáltatás lehetséges megszakadása után is fennáll.

Az időbélyeg tartalmi felépítése – fentiekén felül – az alábbi követelményeknek tesz eleget:

- az időbélyegben megadott időpontot több független forrásból származó időalap szolgáltatja, amely így legfeljebb UTC \pm 1 másodpercen belüli eltérést enged meg,
- a belső órajelet az időbélyegző rendszer indításakor szakértő bizottság hitelesítette, egy független külső referencia időforrás segítségével,
- belső óra hitelességét GPS egységen keresztül redundáns külső UTC időalapokkal és Magyar Telekom referencia atomórájához szinkronizálva biztosítja üzem közben,
- a Szolgáltató az időbélyeget kizárólag az időbélyegzés céljára kiadott aláíró kulccsal írja alá,
- az időbélyeg az aláíró tanúsítvány tulajdonos mezőjét tartalmazza.

5.3.2 Óraszinkronizálás az UTC-vel

Szolgáltató biztosítja, hogy az időbélyegzés-szolgáltatáshoz használt időadat szinkronizálódik az UTC idejéhez, attól való eltérése az előírt értéket nem haladja meg. A Szolgáltató időjelet biztosító rendszere (Trusted Time Infrastructure, továbbiakban: TTI) a Magyar Telekom meglévő infrastruktúrájának szerves részeként került kialakításra.

A Szolgáltató által kialakított TTI rendszer hierarchikus időjel ellátási infrastruktúra, melynek egyik időforrása a Magyar Telekom referencia oszcillátora (atomórája). A TTI rendszer szintjei az alábbiak:

- A hierarchia legfelső szintjén elhelyezkedő szerver a referencia időt a GPS műholdakhoz szinkronizálja (amelyek 1 mikroszekundum pontossággal sugározzák a jelet), majd a szinkronizált időjel elérése után átáll a Magyar Telekom atomóra által szolgáltatott nagy pontosságú szinkronjelre. Ezen a szinten található szerver folyamatosan naplóz minden olyan eseményt, amely riasztás, vagy a rendszer üzemeltetése és működése szempontjából fontos.
- A hierarchia második szintjén található időszerverek is fizikailag biztonságosan védett dobozokban vannak megvalósítva, ezzel biztosítva a szigorú hozzáférés védelmet és kontrollt, amelyen keresztül az auditokat és az időkalibrációt végzi.
- A hierarchia harmadik szintjén helyezkedik el a Szolgáltató egység, amely az első két szinthez hasonlóan időauditot és időkalibrációt követően, biztosítja az időbélyegek előállítását. A Szolgáltató egység maximum 1 másodperccel térhet el az időszerver által megadott időjeltől. 1 másodperc vagy attól nagyobb eltérés esetén az időbélyeg kérések elutasításra kerülnek, egészen addig, amíg a rendszer újra nem szinkronizálódik az időszerverek idejéhez.

A TTI rendszer elhelyezése fizikai behatolástól védett kiemelt biztonságú objektumban valósul meg.

5.4 Időbélyegzés-szolgáltatás üzemeltetése és menedzsmentje

Szolgáltató gondoskodik arról, hogy kellő, az elismert szabványoknak megfelelő fizikai, eljárásbeli és személyzeti biztonsági óvintézkedések, valamint az ezeket érvényre juttató adminisztratív és irányítási eljárások kerüljenek alkalmazásra.

5.4.1 Biztonsági óvintézkedések

A vonatkozó biztonsági követelményeket az IBSzSz [6] {6 Műszaki biztonsági óvintézkedések} fejezete határozza meg.

5.4.2 Komponensek osztályba sorolása

A Szolgáltató biztosítja az időbélyegzés-szolgáltatást támogató informatikai rendszer és a rendszer komponenseinek veszélyeztetettség szerinti osztályozását, és ez alapján megfelelő védelmét. A komponensek osztályozását és kockázati tényezők meghatározását, a Szolgáltató „Kockázatok elemzése a Magyar Telekom minősített időbélyegzés szolgáltatás rendszerében” című dokumentuma tartalmazza.

5.4.3 Személyzeti óvintézkedések

A Szolgáltató a szolgáltatásának személyzeti követelményeit az IBSzSz [6] dokumentum {5.2 Eljárásbeli óvintézkedések} és az {5.3 Személyzetre vonatkozó előírások} alfejezetei határozzák meg.

5.4.4 Fizikai óvintézkedések

Az időbélyegzés szolgáltatásra vonatkozó fizikai óvintézkedéseket az IBSzSz [6] dokumentum {5.1 Fizikai előírások} alfejezete határozza meg.

5.4.5 Üzemeltetés

Szolgáltató biztosítja, hogy az időbélyegzés-szolgáltatást támogató informatikai rendszer és a rendszer komponensek üzemeltetése, megfelelően elkészített üzemeltetési szabályzat és egyéb műszaki dokumentációk szerint biztonságos módon, üzemzavar bekövetkezésének veszélye minimális szinten tartásával valósul meg.

Az üzemeltetésre vonatkozó részletes leírásokat a Szolgáltató belső szabályozó dokumentumai tartalmazzák.

5.4.6 Hozzáférési jogosultságok kezelése

Szolgáltató biztosítja, hogy kizárólag meghatározott személyek férnek hozzá az időbélyegzés-szolgáltatást támogató informatikai rendszerhez. A rendszerbe történő beavatkozást és egyéb adminisztrátori, installációs műveleteket kizárólag az erre jogosult személyek végezhetik el.

A jogosultságok kezelését a Szolgáltató belső szabályozói határozzák meg.

5.4.7 Rendszer telepítése, karbantartása

Az időbélyegzés-szolgáltatást támogató informatikai rendszer telepítése Szolgáltató szigorú felügyelet alatt, adminisztrációs és személyzeti biztonsági előírások alapján zajlott. Szolgáltató ezen felül biztosítja a rendszer folyamatos felügyeletét, karbantartását, az esetleges meghibásodások javítását. Minden változtatás konfigurációs napló állományokban kerül rögzítésre. Szolgáltató engedélye nélkül nem hajtható végre a rendszer és komponensei újból konfigurálása, a komponensek funkcióinak módosítása.

5.4.8 Időbélyegzés-szolgáltatás üzletmenet-folytonossága

Szolgáltató minden szükséges intézkedést megtesz annak érdekében, hogy az időbélyegzés-szolgáltatás folyamatos üzemeltetését biztosítsa. Szolgáltató rendelkezik üzletmenet-folytonossági tervvel ill. katasztrófaterffel, amelyek a váratlan események, továbbá egy esetleges katasztrófa bekövetkezése esetén a Szolgáltató számára szükséges feladatokat határozza meg.

Szolgáltató a 3/2005 (III.18.) IHM rendelet 17.§ (1) alapján biztosítja az időbélyegzés szolgáltatás folyamatos rendelkezésre állását – éves szinten 99,5% rendelkezésre állást vállal. Az eseti szolgáltatás kiesés nem haladhatja meg a 3 óra időtartamot.

5.4.9 Szolgáltató működésének leállítása

Szolgáltató működését befejezheti az alábbi esetekben:

- Szolgáltató vezető testületének döntése alapján,
- Hatóság döntése alapján.

Szolgáltató működésének leállítása az IBSzSz [6] dokumentum {5.7 Időbélyeg szolgáltató vagy szervezet leállítása} alfejezetében meghatározott módon és lépésekben történik.

5.4.10 Jogsabályi megfelelésség

Szolgáltató időbélyegzés-szolgáltatására vonatkozó jogszabályokat az {1.5 Szabványok és jogszabályi megfelelés} alfejezet határozza meg.

5.4.11 Időbélyegzés-szolgáltatással kapcsolatos adatok rögzítése

Szolgáltató az időbélyegzés-szolgáltatást támogató informatikai rendszer üzemeltetése során napló állományokban legalább az alábbi adatokat rögzíti:

- a rendszerbe történő belépések és az operációs rendszer szempontjából fontos üzenetek rögzítése,
- a rendszer komponensek konfigurálására, a rendszer módosítására, beavatkozásra vonatkozó események rögzítése,
- helyi és külső időforrásokkal való kapcsolatfelvétel és időeltérés.

5.5 Szervezeti felépítés

Szolgáltató időbélyegzés szolgáltatásában közreműködő szervezetek a Magyar Telekom Nyrt. szervezeti felépítésében az alábbi néven szerepelnek:

- Időbélyegző szervezet: Magyar Telekom Nyrt., IT Üzemeltetési Igazgatóság, IT Biztonsági osztály PKI csoport
- A szolgáltatás nyújtásában közreműködik még az Üzemeltetés és Fenntartási Igazgatóság, NGN Alkalmazás üzemeltetési osztálya, aki az időjel rendszer üzemeltetését végzi.

6 Jelölések, rövidítések és meghatározások

A dokumentumban az alábbi jelölések és rövidítések szerepelnek:

- TSP: Időbélyegzési Rend,
- ISzSz: Időbélyegzés Szolgáltató Szerződés,
- ÁSzF: Általános Szerződési Feltételek,
- IBSzSz: Magyar Telekom Időbélyegzés-szolgáltatási Szabályzat,
- OID: Object Identifier (Egyedi objektum-azonosító),
- UTC: Coordinated Universal Time, ITU-R TF460-5 ajánlás szerinti időalap,
- HSM: Hardver Security Modul, Kriptográfiai egység,
- TTI: Trusted Time Infrastructure (időjel szolgáltató infrastruktúra),

{ } jelek között egy dokumentum adott fejezetére / alfejezetére történő hivatkozások szerepelnek.

[] jelek között a dokumentumokra történő hivatkozások számai szerepelnek, lásd: {7 Hivatkozások} alfejezet.

A Szolgáltató a TSP-ben szereplő fogalmakat az alábbi értelemben használja:

Fogalom	Meghatározás (magyarázat)
aktivizáló adatok	a kriptográfiai modul működtetéséhez szükséges adatok, melyeket védeni kell (pl. PIN kód, jelmondat vagy manuálisan birtokolt kulcs-részlet)
elektronikus dokumentum	elektronikus eszköz útján értelmezhető adategyüttes
előfizető	Időbélyegzés esetén maga az igénybevevő.
érintett fél	az elektronikus dokumentum fogadója, aki egy adott időbélyegzőre hagyatkozva jár el
fogadó fél (elfogadó fél)	az elektronikus dokumentum fogadója, aki egy adott időbélyegzőre hagyatkozva jár el
Időbélyegzés szolgáltatási szabályzat	Az Eat. [1] 6. § (1) bekezdése szerinti szolgáltató tevékenységével kapcsolatos részletes eljárási és egyéb működési szabályokat tartalmazó szabályzat
időbélyeg (időbélyegző)	elektronikus dokumentumhoz végérvényesen hozzárendelt, vagy azzal logikailag összekapcsolt olyan adat, amely igazolja, hogy az elektronikus dokumentum az időbélyegző elhelyezésének időpontjában változatlan formában létezett
időbélyegzés-szolgáltató	olyan szolgáltató, amely az időbélyegzés szolgáltatást végzi

kriptográfiai kulcs	olyan kriptográfiai transzformációt vezérlő egyedi jelsorozat, amelynek ismerete a kriptográfiai transzformáció elvégzéséhez, különösen az elektronikus aláírás előállításához vagy ellenőrzéséhez szükséges
tanúsítvány	Időbélyegzés szolgáltatás esetén az időbélyegzők szolgáltatói tanúsítványai.
tanúsítvány visszavonási állapot közzététele	Időbélyegzés szolgáltatás esetén információ nyújtása az elfogadó fél számára az időbélyegző tanúsítványok visszavonásáról. A szolgáltatás lehet valós idejű, vagy az információk előre meghatározott időközönkénti aktualizálásán kell alapulnia.
tanúsítvány visszavonási lista	Időbélyegzés szolgáltatás esetén valamely okból visszavont, azaz érvénytelenített időbélyegző tanúsítványok azonosítóit tartalmazó elektronikus lista, melyet a szolgáltató bocsát ki
Visszavonási nyilvántartások (tanúsítvány visszavonási nyilvántartás)	Időbélyegzés szolgáltatás esetén nyilvántartások a felfüggesztett, illetőleg a visszavont időbélyegző tanúsítványokról, amelyek tartalmazzák legalább a felfüggesztés vagy visszavonás tényét, és a felfüggesztés vagy visszavonás időpontját
időbélyegzési rend	olyan szabálygyűjtemény, amelyben egy szolgáltató, igénybe vevő vagy más személy (szervezet) valamely időbélyegző felhasználásának feltételeit írja elő igénybe vevők valamely közös biztonsági követelményekkel rendelkező csoportja, illetőleg meghatározott alkalmazások számára
végfelhasználó	az előfizető, az elfogadó fél, valamint az érintett fél

7 Hivatkozások

A Szolgáltató jelen TSP-ben az alábbi dokumentumokra hivatkozik:

- [1] 2001. évi XXXV. törvény az elektronikus aláírásról,
- [2] 2/2002. (IV. 26) MeHVM irányelve a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről,
- [3] 3/2005 (III.18.) IHM rendelet az elektronikus aláírásokkal kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről,
- [4] ETSI TS 102 023 EU szabvány: Policy requirements for time-stamping authorities,
- [5] IETF RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP),
- [6] Magyar Telekom Időbélyegzés Szolgáltatási Szabályzata (IBSzSz) – Magyar Telekom Nyrt.
- [7] ETSI TS 101 861 EU szabvány: Time stamping profile
- [8] Magyar Telekom Minősített Időbélyegzés-szolgáltatás Általános Szerződési Feltételek (**ÁSzF**) – Magyar Telekom Nyrt.,
- [9] Magyar Telekom Időbélyegzés Szolgáltatói Szerződése – röviden Szolgáltatói Szerződés (**ISzSz**).