Magyar Telekom

Minősített Időbélyegzés Szolgáltatás

Időbélyegzési Rendje

Egyedi objektum-azonosító (OID): 1.3.6.1.4.1.17835.7.1.2.11.3.12.2.5

Verziószám:.....2.5

Regisztrációs szám:.....

Hatályba lépés dátuma:.....2023.03.28.

Változáskezelés

Verzió-szám	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
1.9	2011.12.05	A Nemzeti Média- és Hírközlési Hatóság EF-26838-9/2011 számú határozatának végrehajtásával összefüggő változások, valamint szervezeti változások átvezetése
2.0	2016.09.08	Jogszabályi, valamint szervezeti és személyi változások átvezetése
2.1	2019.01.15	Szervezeti és személyi változások átvezetése
2.2	2021.04.19.	Mátrix tanúsító javaslatainak és az új HSM eszköz átvezetése
2.3	2022.01.31.	NMHH észrevételek javítása
2.4	2022.04.25.	Mátrix észrevételek átvezetése
2.5	2023.03.28.	Mátrix észrevételek átvezetése

Módosítást készítette: Fogarasi Ádám	Technológiai biztonsági központ	IT biztonsági specialista
Ellenőrizte Dr. Demény Péter	Group Legal HUB	Legal Counsel
Jóváhagyta: Keszthelyi Zoltán	Technológiai biztonsági központ	központvezető

Tartalomjegyzék

1 Bevezetés

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 Időbélyegezés-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** (továbbiakban: IB-SzSz) [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.

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 Minősített Időbélyegzés szolgáltatót** (időbélyegző szervezetet) kell érteni. A Szolgáltató jogi értelemben a **Magyar Telekom Nyrt.**

A Szolgáltató minősített szolgáltatóként 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:	1097 Budapest, Könyves Kálmán körút 36.
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:	1097 Budapest, Könyves Kálmán körút 36.
Telefon:	+36 1 481-8401
Fax:	+36-1-481-8405
Postacím:	1541 Budapest
Honlap:	http://www.t-systems.hu/nagyvallalatok/hitelesites_szolgaltatasok/idobelyegzes_szolgaltatas
E-levélcím:	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 authentikációs tanúsítvány visszavonási szolgáltatással kapcsolatos szolgáltatás a fenti munkaidőn túl elérhető az alábbi telefon:

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.

A Magyar Telekom a minősített Időbélyegzés szolgáltatást az [1],[2],[3] jogszabályok és a vonatkozó (a „Hivatkozások"-ban feltüntetett) szabványok előírásai szerint végzi. A jogszabályoknak és szabványoknak történő megfelelést akkreditált tanúsító szervezet megfelelőség-értékelés útján tanúsítja, valamint a Bizalmi felügyelet (a Nemzeti Média-és Hírközlési Hatóság) felügyeli.

1.4 Időbélyegzés-szolgáltatás meghatározása

Az eIDAS Rendelet alapján az „elektronikus időbélyegző": olyan elektronikus adatok, amelyek más elektronikus adatokat egy adott időponthoz kötnek, amivel igazolják, hogy utóbbi adatok léteztek az adott időpontban

A 2015. évi CCXXII törvény 97.§ (1). Ha az elektronikus dokumentum minősített elektronikus aláírással vagy bélyegzővel, vagy **időbélyegzővel** lett ellátva, és az aláírás vagy bélyegző, vagy az **időbélyegző** ellenőrzésének eredményéből más nem következik, vélelmezni kell, hogy a dokumentum tartalma az aláírás vagy a bélyegző, vagy az **időbélyegző** elhelyezése óta nem változott..

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, hiteles ített időforráshoz történő szinkronizálás érdekében és
- maga az **időbélyegzés-szolgáltatás**, amelyet a Szolgáltató minősített időbélyegzés-szolgáltatásként (előfizetéses alapon) nyújt ügyfeleinek.

Az időbélyegek használata során **kétféle alapműveletet** 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 szolgáltat[1]
- a második az Internet alapú hozzáférés, mellyel a lehető legszélesebb felhasználói körre kiterjeszthető a szolgáltatás.

A Szolgáltató időbélyegző infrastruktúrája pontosság és biztonság tekintetében **megfelel** a 24/2016. (VI.30) BM rendelet [3], valamint az ETSI EN 319 421 [4] és az ETSI EN 319 422 [7] szabvány erre 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 EN 319 401 [x], ETSI EN 319 421 [4] és ETSI EN 319 422 [7] [7] EU szabványoknak.

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

Jelen Minősített időbélyegzési rend szerint kiállított időbélyegzők megfelelnek az ETSI EN 319 421 [4] szabvány követelményeinek.

Szolgáltató az általa kiadott időbélyegzőkben saját OID-t szerepeltet, az ETSI időbélyegzési rendet (BTSP) pedig támogatja.

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

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 mindenkori aktuális változatát Szolgáltató az Interneten a http://www.t-systems.hu/nagyvallalatok/hitelesites_szolgaltatasok/idobelyegzes_szolgaltatas

címen keresztül teszi elérhetővé.

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 Platform fejlesztési ágazat ISP csoport, mint az időjelt 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 alapműveletet** 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 UTC[2] időalaphoz való szinkronizálását,
  - időbélyegző szerverek forgalmát felügyeli, karbantartja, szükséges mentéseket elvégzi,
  - felügyeli az időbélyegek időpontjának hitelességét az {5.3.2 Óraszinkronizálás az UTC-vel} alfejezetben leírtak alapján.

Az időbélyegzéshez használt kulcspárhoz tartozó tanúsítványokat Szolgáltató a Magyar Telekom RootCA 2011-ből adja ki. A Magyar Telekom RootCA 2011 működtetésével kapcsolatban az IB-SzSz[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 24/2016. (VI.30) BM rendelet, valamint az ETSI EN 319 421 [4] és az ETSI EN 319 422 [7] szabvány erre vonatkozó előírásainak.

[2] 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: ISzSz [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 ISzSz-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: IBSzSz [6]. A TSP-ben nem szabályozott, az időbélyegzés-szolgáltatásra vonatkozó jogi, kereskedelmi és egyéb eljárási szabályokat, a Szolgáltató aktuális IBSzSz dokumentuma tartalmazza.

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

http://www.t-systems.hu/nagyvallalatok/hitelesites_szolgaltatasok/idobelyegzes_szolgaltatas

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 [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 időbélyegző 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 megfelelőssége

Szolgáltató az időbélyegzés-szolgáltatás vonatkozásában az {1.5 Szabványok és jogszabályi megfelelés} alfejezetben meghatározott jogszabályi és egyéb műszaki szabványok szerinti megfelelőségét, 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 helytállása} 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 időbélyegző nem tartalmaz hibás adatot,
- nem ismeri meg az időbélyegzett dokumentum tartalmát, és csak az abból képzett lenyomatot kezeli,
- időbélyegző aláíró kulcsát csak az időbélyegzés keretén belül használja,
- az időbélyegzőt 1 másodpercen belüli pontossággal adja ki,
- 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 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 szoftver alkalmazásról, 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 authentikációs tanúsítvány kiállításához szükséges adatokat.

– Előfizető köteles a Szolgáltató képviselőjétől megkapott authentikációs 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 igénybevételéről, valamint az authentikációs tanúsítványhoz tartozó magánkulcs illetéktelen felhasználásának megakadályozásáról Elfizető köteles a jogosult felhasználóinak is tájékoztatást és útmutatót adni.

– Előfizető köteles késedelem nélkül értesíteni a Szolgáltatót, amennyiben az authentikációs tanúsítvány magánkulcsa kompromittálódott, illetve tudomására jutott annak illetéktelen felhasználása. Az authentikációs 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 authentikációs tanúsítvánnyal történt időbélyegző 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 időbélyegzőre kíván hagyatkozni, akkor javasolt ellenőrizni az időbélyegzőt, valamint az időbélyegző egység (időbélyegző szerver) tanúsítványának, illetve az ezt kiadó Magyar Telekom RootCA 2011 tanúsítványának érvényességét az érvényes visszavonási állapotinformáció felhasználásával, a szabályzatoknak megfelelően.

A Szolgáltató által kiadott időbélyegzők ajánlott ellenőrzési lépései a következők:

– annak megvizsgálása, hogy az időbélyegzőt 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 időbélyegzőt felhasználók az IBSzSz-ben [6] meghatározott gyakorisággal közzétett CRL alapján ellenőrizhetik, amely a

http://www.t-systems.hu/nagyvallalatok/hitelesites_szolgaltatasok/idobelyegzes_szolgaltatas 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 authentikációs 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 authentikációs 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 időbélyegzőkben 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_szolgaltatasok/idobelyegzes_szolgaltatas

címen keresztül teszi közzé. A web oldalon 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) mindenkori aktuális változatát a

http://www.t-systems.hu/nagyvallalatok/hitelesites_szolgaltatasok/idobelyegzes_szolgaltatas

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 RootCA 2011 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 NMHH 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 szoftver-alkalmazással 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 időbélyegzőre 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 Média- és Hírközlési Hatóság (Bizalmi Felügyelet),

- Külső független vizsgáló 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, vagy CC EAL 4 szerint bevizsgált kriptográfiai modulban (Hardware Security Modul, továbbiakban: HSM) történik.

A Szolgáltató időbélyegzés-szolgáltatását kiszolgáló időbélyegző egységek saját kulcsai kriptográfiai modulban (HSM) keletkeznek és teljes életciklusuk alatt a HSM-ekben maradnak.

A Szolgáltató időbélyegző egységeinek kriptográfiai moduljai megfelelnek a [4] EU szabvány 7.6.3 pontjában foglaltaknak.

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

A TSU-k számára kiállított tanúsítványok érvényességét, megbízhatóságát a Szolgáltató a teljes láncon ellenőrzi, mielőtt azokat az időbélyegző egységekbe beimportálja.

Az időbélyegző(k) tanúsítványai a

http://www.t-systems.hu/nagyvallalatok/hitelesites_szolgaltatasok/idobelyegzes_szolgaltatas

weboldalon keresztül érhetőek 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.

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 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 időbélyegzők biztonságos kibocsátását és az időbélyegzőben szereplő időpont pontosságát. Az időbélyeg profil [4] és [7] szabványok alapján a következőket tartalmazza:

Mezőnév	Érték vagy szabály
Verzió *Version*	A Szolgáltató időbélyegzés-szolgáltatásának technikai azonosítója: Magyar Telekom TSA v1.0 így a mező értéke: „**v1.0**”
Időbélyeg kérelemben engedélyezett hash algoritmus	sha256: OID 2.16.840.1.101.3.4.2.1 sha384: OID 2.16.840.1.101.3.4.2.2

	sha512 OID 2.16.840.1.101.3.4.2.3
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 aláíró algoritmus	ecdsaWithSHA256: OID 1 2 840 10045 4 3 2
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 TSU-ként, amely sorszámozás egyedisége a szolgáltatás lehetséges megszakadása után is fennáll.

Az időbélyegző tartalmi felépítése – fentieken felül – az alábbi követelményeknek tesz eleget:

- az időbélyegzőben megadott időpontot több független forrásból származó időalap szolgáltatja, amely így legfeljebb UTC ± 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 időalaphoz szinkronizálva biztosítja üzem közben,
- a Szolgáltató az időbélyegzőt kizárólag az időbélyegzés céljára kiadott aláíró kulccsal írja alá,
- az időbélyegző 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.

- Az időbélyegző rendszer tűzfalai kulcsos autentikációt követően szinkronizálnak a legfelső szinten lévő ntp szerverekhez (ntp.telekom.intra infrastruktúra)

- 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.

- Az időbélyegző szerverek naponta két alkalommal vesznek pontos időjelet, mely rendszer naplóban pontosan rögzített.

A TTI rendszer elhelyezése geo-redundáns módon, fizikai behatolástól védetten, kiemelt biztonságú adatközpontokban 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 szabályzatai 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. katasztrófatervvel, amelyek a váratlan események, továbbá egy esetleges katasztrófa bekövetkezése esetén a Szolgáltató számára szükséges feladatokat határozza meg.

Szolgáltató a 24/2016. (VI.30) BM rendelet 45.§ (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 Jogszabályi megfelelősség

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., Csoport biztonsági igazgatóság, Technológiai biztonsági központ
- A szolgáltatás nyújtásában közreműködik még az Platform fejlesztési és üzemeltetési ágazat ISP csoport, aki az időjel rendszer üzemeltetését végzi.

5.6 Produktív és teszt környezet elválasztása

Annak érdekében, hogy az Időbélyegző Szervezet valamennyi rendszerfejlesztési projektjében a biztonság követelményeit magas színvonalon biztosítsák, a teljes fejlesztés során (már a tervezési és követelmény-meghatározási fázisban is) figyelembe veszik a különös követelményeket.
A teszteléseket és a fejlesztéseket a DR siton hajtjuk végbe, mielőtt éles üzembe kerülne.
A kockázat kerülés érdekében visszaállításai tervet kell készíteni, az esetleges PROD site hibája esetén.

A produktív környezet teljesen elszeparálva jött létre a teszt környezettől. A teszt környezet jelenleg a HSM gyártó által (I4P) biztosított virtuális környezetben valósul meg.

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 adat-együttes
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	A 2015. évi CCXXII. törvény 1§ bekezdése szerint a bizalmi szolgáltató nyilatkozata az egyes bizalmi szolgáltatások nyújtásával kapcsolatosan alkalmazott részletes eljárási vagy más működési követelményekről
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 bizalmi 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] 910/2014 EU rendelet (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról,

[2] 2015. évi CCXXII törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól,

[3] 24/2016. (VI.30) BM rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről,

[4] ETSI EN 319 421 EU szabvány: Policy and Security Requirements forTrust Service Providers issuing Time-Stamps ,

[5] IETF RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP),

[6] Magyar Telekom Időbélyegzés Szolgáltatási Szabályzata (IBSzSz) – Magyar Telekom Nyrt. OID:1.3.6.1.4.1.17835.7.1.2.11.3.13.2.6

[7] ETSI EN 319 422 EU szabvány: Time-stamping protocol and time-stamp token profiles

[8] Magyar Telekom Minősített Időbélyegzés-szolgáltatás Általános Szerződési Feltételek (ÁSzF) – Magyar Telekom Nyrt.,

[9] Magyar Telekom Időbélyegzés Szolgáltatói Szerződése – röviden Szolgáltatói Szerződés (ISzSz).