

Magyar Telekom

Minősített Időbélyegzés Szolgáltatás

Szolgáltatási Kivonata

Egyedi objektum-azonosító (OID):.....1.3.6.1.4.1.17835.7.1.2.11.3.13.2.6
Verziószám:.....2.6
Hatályba lépés dátuma:.....2021. 04. 19.

Változáskezelés

Verzió-szám	Dátum	A változás leírása
2.4	2007.05.10	Első változat (szakértői munkaanyagok), auditori észrevételek átvezetése
2.5	2019.01.15	Mátrix tanúsító javaslatainak átvezetése
2.6	2021.04.19.	Mátrix tanúsító javaslatainak és az új HSM eszköz átvezetése

Módosítást készítette: Fogarasi Ádám	Technológiai biztonsági központ	IT biztonsági specialista
Ellenőrizte: Dr. Demény Péter	Csoport jogi igazgatóság	Jogi szakértő
Jóváhagyta: Keszthelyi Zoltán	Technológiai biztonsági központ	központvezető

TARTALOMJEGYZÉK

VÁLTOZÁSKEZELÉS.....	2
1 BEVEZETÉS.....	4
1.1 MEGFELELÉS.....	4
1.2 A SZOLGÁLTATÓ	5
1.3 IDŐBÉLYEGZŐ SZERVEZET.....	5
1.4 AZ IDŐBÉLYEGZŐ FELHASZNÁLHATÓSÁGA.....	6
1.5 A SZOLGÁLTATÁSI SZABÁLYZAT ADMINISZTRÁLÁSA.....	6
1.6 MEGHATÁROZÁSOK	7
1.7 RÖVIDÍTÉSEK ÉS JELÖLÉSEK.....	7
1.8 HIVATKOZÁSOK.....	8
2 MŰKÖDÉSRE VONATKOZÓ KÖVETELMÉNYEK - IDŐBÉLYEGZÉS	9
2.1 AZ IDŐBÉLYEGZÉS.....	9
2.2 AZ IDŐBÉLYEGZŐ ELLENŐRZÉSE.....	9
2.3 AZ IDŐBÉLYEGZÉS SZOLGÁLTATÁS IGÉNYLÉSE	9
2.4 AZ IDŐBÉLYEGZÉS SZOLGÁLTATÁS TELJESÍTÉSE.....	10
2.5 AZ IDŐBÉLYEGZÉS SZOLGÁLTATÁS IGÉNYBEVÉTELÉNEK VÉGE.....	10
3 ELHELYEZÉSI, IRÁNYÍTÁSI ÉS MŰKÖDTETÉSI ELŐÍRÁSOK.....	10
3.1 NAPLÓZÁSI ELJÁRÁSOK	10
3.1.1 A tárolt események típusai.....	10
3.1.2 A tárolt események típusai.....	11
3.2 ADATOK ARCHIVÁLÁSA.....	11
3.2.1 Az archivált adatok megőrzési időtartama.....	11
4 MŰSZAKI, BIZTONSÁGI ÓVINTÉZKEDÉSEK.....	11
4.1 SZOLGÁLTATÓI KULCSOK ELŐÁLLÍTÁSA.....	11
4.2 KRIPTOGRAFIAI MODULOK MEGFELELŐSÉGE.....	11
4.3 A TANÚSÍTVÁNYOK ÉS A KULCSPÁROK HASZNÁLATÁNAK PERIÓDUSA	12
4.4 SZOLGÁLTATÓI KULCSOK MENTÉSE	12
5 MEGFELELŐSÉG.....	12
6 EGYÉB ÜZLETI ÉS JOGI KÉRDÉSEK.....	13
6.1 IDŐBÉLYEGZÉS SZOLGÁLTATÁSI DÍJAK	13
6.2 DÍVISSZATÉRÍTÉS.....	13
6.3 ANYAGI FELELŐSSÉGVÁLLALÁS, FELELŐSSÉGBIZTOSÍTÁS.....	13
6.4 A SZEMÉLYES ADATOK VÉDELME.....	13
6.5 TEVÉKENYSÉGÉRT VISELT FELELŐSSÉG ÉS HELYTÁLLÁS.....	14
6.5.1 Az időbélyegzés szolgáltató felelőssége és helytállása	14
6.5.2 Az előfizető és érintett fél felelőssége és helytállása.....	14
6.5.3 Felelősségi korlátozások.....	15
6.5.4 Vitás kérdések megoldása.....	15
6.5.5 Irányadó jog.....	16

1 Bevezetés

Ez a szabályzat a **Magyar Telekom Nyrt.** (ebben a dokumentumban: Szolgáltató) minősített időbélyegzés szolgáltatás tevékenységével kapcsolatos részletes eljárási és működési szabályokat tartalmazza.

A Szabályzat célja, hogy összefogja azokat a dokumentumokat és információkat, melyeket a Szolgáltatóval valamilyen módon kapcsolatba kerülő feleknek (elsősorban a végfelhasználóknak) a minősített időbélyegzés szolgáltatással kapcsolatosan tudni érdemes. A Szabályzat biztosítja a Szolgáltató működésének átláthatóságát, s lehetővé teszi annak megállapítását, hogy a Szolgáltató gyakorlata, illetve az időbélyegzés szolgáltatás keretében kiadott időbélyeg mennyiben felel meg a felhasználói és törvényes elvárásoknak. A Szabályzat segítségével az időbélyegzés szolgáltatás megrendelői és elfogadói egyértelműen megállapíthatják az időbélyeg **kezelésének módját**, a garantált **biztonságot** és a szolgáltatásra vonatkozó műszaki, üzleti, pénzügyi **garanciákat** és jogi **felelősségvállalásokat**.

A Szabályzatban meghatározott időbélyegzés szolgáltatást a jelen szabályzat, az ÁSZF ([11]), a vonatkozó Időbélyegzési Rend, valamint az előfizetővel megkötött szerződés ([12]) együttesen szabályozzák {ld. 1.8 Hivatkozások}. Amennyiben az Időbélyegzési Rend, az ÁSZF, valamint jelen szabályzat bármely vonatkozásban ellentmondással vagy eltérő kikötéssel élnének, akkor a vonatkozó Időbélyegzési Rend előírásai tekintendők irányadónak. Az e bekezdésben hivatkozott dokumentumok mindenkor hatályos változata elérhető a

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

honlapon.

A szolgáltatási kivonat megfelel az eIDAS [1] rendelet által támasztott követelményeknek.

1.1 Megfelelés

Jelen szolgáltatási kivonat szerint kiállított időbélyegzők megfelelnek az ETSI EN 319 421 [10] szabvány követelményeinek.

A Minősített időbélyegzés-szolgáltató a bizalmi szolgáltatás nyújtását 2017. augusztus 25-én jelentette be a Nemzeti Média- és Hírközlési Hatóságnak.

A minősített bizalmi szolgáltatás megfelelőségértékelését a TÜV Informationstechnik GmbH (továbbiakban TÜViT) végezte. A megfelelőségértékelési tanúsítvány azonosítója: 9761.17

A sikeres vizsgálat alapján a Nemzeti Média- és Hírközlési Hatóság nyilvántartásba vette és a nemzeti bizalmi listában publikálta a bejegyzett minősített bizalmi szolgáltatást.

Szolgáltató megfelelőségének értékelését az 910/2014/EU rendelet, a hatályos magyar jogszabályok (2015. évi CCXXII törvény, 24/2016. (VI.30.) BM rendelet), valamint a vonatkozó ETSI szabványok (ETSI EN 319 401 v2.1.1, ETSI EN 319 421 v1.1.1) alapján 2020. november hónapban a Mátix Kft. elvégezte, amelyről 2022. november 6-ig tartó érvényességgel „I-MT20T_TAN.QTIMESTAMP” számon tanúsítványt bocsátott ki.

Szolgáltató az általa kiadott időbélyegzőkben saját OID-t szerepeltet - 1.3.6.1.4.1.17835.7.1.2.11.3.12 -, az ETSI időbélyegzési rendet (BTSP) pedig támogatja.

1.2 A szolgáltató

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

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: 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 Szolgáltató **alvállalkozókat** is megbízhat egyes feladatok elvégzésére. Az alvállalkozók tevékenységéért a Szolgáltató teljes felelősséggel tartozik.

1.3 Időbélyegzőszervezet

A Szolgáltató – a saját szervezetén belül, a **Csoport biztonsági igazgatóság** keretében – időbélyegző szervezetet működtet (Időbélyegző Szervezet), melynek feladata a szolgáltatásokhoz kapcsolódó rendszerek üzemeltetése, az időbélyegzésszolgáltatások nyújtása.

A Szervezet a timestamp@telekom.hu elektronikus levélcímen érhető el.

Az Időbélyegző Szervezet feladatai az alábbiak:

- A minősített időbélyegző rendszer üzemeltetése,
- A Magyar Telekom Gyökér hitelesítő működtetése,
- Szolgáltatói tanúsítványok és visszavonáslisták közzététele,
- ügyfélszolgálati teendők: a felhasználókkal való kapcsolattartás és további menedzsment feladatok ellátása.

Az Időbélyegző Szervezet a feladatait a Szabályzat előírásainak megfelelően végzi. Az aktuális ügyek kezelését interneten és telefonon keresztül, illetve (az ügyfélszolgálaton) személyes közreműködéssel látja el.

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 munkanapokon **8 és 16 óra között** tart nyitva, de egyes napokon ettől eltérő nyitvatartási időpont is lehetséges. Hibabejelentéssel, valamint időbélyegzés kérésre jogosító athentikációs tanúsítvány visszavonási szolgáltatással kapcsolatos szolgáltatás a fenti munkaidőn túl elérhető az alábbi telefon, ill. faxszámon:

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

Az Időbélyegző Szervezet aktuális adatai a Szolgáltató fenti internetes honlapján megtekinthetők. Szolgáltató a minősített időbélyegzés szolgáltatást az alábbi elérhetőségen biztosítja: <https://timestamp.magyartelekom.hu>

1.4 Az időbélyegző felhasználhatósága

Az eIDAS [1] Rendelet alapján az „elektronikus időbélyegző”: olyan elektronikus adatok, amelyek más elektronikus adatokat egy adott időponthoz kötnék, amivel igazolják, hogy utóbbi adatok léteztek az adott időpontban. Az időbélyegzés szolgáltatás keretében Szolgáltató az elektronikusan aláírt 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.

1.5 A Szolgáltatási Szabályzat adminisztrálása

A Szolgáltató – szervezetén belül – olyan szervezeti egységet működtet, amely az időbélyegzéssel kapcsolatos szolgáltatásokhoz elengedhetetlen szabályozási feladatokat látja el, beleértve elsősorban a jelen szabályzat valamint az egyéb nyilvános¹ szabályzatok (ÁSZF, Időbélyegzési Rend) el(ő)készít(tet)ésével, egyeztetésével, kiegészítésével, aktualizálásával, jóváhagyásával és megjelentetésével kapcsolatos **összes feladatot**.

A szabályozási szervezet adatai, és azon belül a fenti tevékenységgel megbízott szolgáltatási menedzser elérési adatai a következők:

Név: Magyar Telekom Nyrt. / Technológiai biztonsági központ
Cím: 1117 Budapest Magyar tudósok körút 9.
Telefon: +36 1 481-8401
Mobil: +36 30 444 1731
e-Mail: timestamp@telekom.hu
Fax: +36 1 481-8405
Postacím: 1541 Budapest

A szabályzatokra vonatkozóan a Bizalmi Felügyelettel történő hivatalos kapcsolattartás a Magyar Telekom Csoport szabályozási igazgatóság feladata.

¹ A belső szabályozások kezelésével kapcsolatos felelősök külön belső utasításban vannak rögzítve

1.6 Meghatározások

A Szolgáltató a dokumentumban 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 hagyatkozik
fogadó fél (elfogadó fél)	az elektronikus dokumentum fogadója, aki egy adott időbélyegzőre hagyatkozik
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 valamelyekből 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, igénybevevő vagy más személy (szervezet) valamely időbélyegző felhasználásának feltételeit írja elő igénybevevők valamely közös biztonsági követelményekkel rendelkező csoportja, illetőleg meghatározott alkalmazások számára
végfelhasználó	az előfizető, az elfogadó fél, valamint az érintett fél

1.7 Rövidítések és jelölések.

A dokumentumban az alábbi jelölések és rövidítések szerepelnek:

- [] jelek között a dokumentumokra történő hivatkozások számai szerepelnek,
- { } jelek között egy dokumentum adott fejezetére / alfejezetére történő hivatkozások szerepelnek.

1.8 Hivatkozások

A Szolgáltató a jelen dokumentumban 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] A Nemzeti Média- és Hírközlési Hatóságnak az elektronikus aláírással kapcsolatos szolgáltatások nyújtása során felhasználható biztonságos kriptográfiai algoritmusok és paramétereik meghatározása tárgyában hozott EF-26838-9/2011 számú határozata.
- [5] ISO 3166
- [6] FIPS PUB 140-2 (1994. január 11.): "Kriptográfiai modulok biztonsági követelményei"
- [7] International Telecommunication Union X.509 "Információ technológia – Nyílt rendszerek kapcsolódása - Könyvtár: Nyilvános kulcs és attribútum tanúsítvány keretrendszer"
- [8] RFC 5280 (Internet X.509 Nyilvános kulcsú infrastruktúra – tanúsítvány és tanúsítvány visszavonási lista profil)
- [9] RFC 3161 (Internet X.509 Nyilvános kulcsú infrastruktúra – Time-Stamp Protocol)
- [10] ETSI EN 319 421 EU szabvány: Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
- [11] Minősített Időbélyegzés szolgáltatások - Általános Szerződési Feltételek (ÁSZF) – Magyar Telekom Nyrt.
- [12] Magyar Telekom Minősített Időbélyegzés szolgáltatás Szolgáltatói Szerződése – röviden Szolgáltatói Szerződés (ISzSz)
- [13] Magyar Telekom Minősített Időbélyegzés-szolgáltatás Időbélyegzési Rendje – röviden (TSP)
- [14] ETSI EN 319 422 EU szabvány: Time-stamping protocol and time-stamp token profiles

2 Működésre vonatkozó követelmények - időbélyegzés

2.1 Az időbélyegzés

Szolgáltató az RFC 3161 (Internet X.509 Nyilvános kulcsú infrastruktúra – Time-Stamp Protocol) [9], valamint az ETSI EN 319 422 (Time-stamping protocol and time-stamp token profiles) [14] szabványon alapuló időbélyegző kérélmeket fogad és időbélyegző válaszokat ad.

Szolgáltató által kibocsátott időbélyegző jellemzői:

- a kérelmező által küldött üzenetben szereplő lenyomatot tartalmazza.
- tartalmazza az időbélyegzési rend OID-jét.
- egyedi azonosítóval rendelkezik.

Szolgáltató az időbélyegzőkben az ETSI TS 119 312 szerinti és az aktuális Nemzeti Média és Hírközlési Hatóság algoritmusokkal kapcsolatos határozatban kijelölt lenyomatképző algoritmusokat fogadja be az időbélyegző kérésekben.

A jelenleg támogatott lenyomatképző algoritmusok:

- sha256
- sha384
- sha512

A Szolgáltató az ETSI TS 119 312 szerinti, és az aktuális Nemzeti Média- és Hírközlési Hatóság algoritmusokkal kapcsolatos határozatban kijelölt kriptográfiai algoritmuskészleteket és kulcshosszakat használja az időbélyegzők aláírására.

A jelenleg támogatott kriptográfiai algoritmuskészletek:

- ecdsaWithSHA256

2.2 Az időbélyegzőellenőrzése

Az Időbélyegzőn szereplő elektronikus aláírás vagy elektronikus bélyegző érvényességének ellenőrzése során az Érintett félnek célszerű az ETSI EN 319 102-1 specifikációban leírtak szerint eljárnia:

- ellenőrizni kell, hogy összetartozik-e az időbélyegzett dokumentum az időbélyegzővel és az Időbélyegzés-szolgáltató tanúsítványával;
- ellenőrizni kell az időbélyegzőn szereplő aláírást;
- Az időbélyegző egység tanúsítványnak érvényességi és visszavonási állapotát, ateljes lánra vonatkozóan;
- ellenőrizni kell, hogy az időbélyegző megfelel-e az adott célra, többek között, hogy pontossága, megbízhatósága, valamint a hozzá kapcsolódó Időbélyegzés-szolgáltatói felelősségvállalás megfelelő;

2.3 Az időbélyegzés szolgáltatásigénylése

Időbélyegzés szolgáltatásra vonatkozó igényt benyújthat, aki a Szolgáltató honlapján közzétett Általános Szerződési Feltételeket és jelen Szolgáltatási Szabályzatot megismeri és elfogadja, valamint az ott megjelentetett Megrendelő lapot kitölti és eljuttatja az Időbélyegzés Szolgáltatás ügyfélszolgálat címére.

2.4 Az időbélyegzés szolgáltatásteljesítése

Szolgáltató az RFC 3161 (Internet X.509 Nyilvános kulcsú infrastruktúra – Time-Stamp Protocol) [9], valamint az ETSI EN 319 422 (Time-stamping protocol and time-stamp token profiles)[14] szabványon alapuló időbélyeg kérelmeket fogad és időbélyeg válaszokat ad. Az időbélyeg kérelmek előállításához illetve az időbélyeg válaszok fogadásához, ellenőrzéséhez szükséges programokkal, program modulokkal, infrastruktúrával a Felhasználónak kell rendelkeznie.

A 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 időbélyegzés szolgáltatás eseti szolgáltatás kiesése nem haladhatja meg a 3 óra időtartamot.

A Szolgáltató időbélyegzés-szolgáltatás nyújtása során biztosítja, hogy az időbélyeg válasz – az időbélyegzéssel összefüggésben hozzáadottaktól eltekintve – ugyanazokat az adatokat tartalmazza, amelyeket a kérelem tartalmazott. Az időbélyegzés szolgáltatás során a Szolgáltató - a technológia jellegéből adódóan - nem ismeri meg az időbélyeggel ellátott dokumentum tartalmát, csak az abból képzett lenyomatot.

2.5 Az időbélyegzés szolgáltatásigénybevételének vége

Amennyiben a szolgáltatásra vonatkozó szerződést Előfizető fel kívánja mondani a szerződés lejáratát megelőzően, ezt írásban vagy faxon kell bejelenteni az Időbélyegző Szervezet részére.

3 Elhelyezési, irányítási és működtetési előírások

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.

3.1 Naplózási eljárások

Szolgáltató időbélyegző rendszere széleskörű naplózási tevékenységet folytat. A naplóbejegyzések a bejegyzés pontos idejét, a tevékenység időpontját (ha az a bejegyzés idejétől eltér) és végrehajtóját is tartalmazzák. A pontos időt Szolgáltató pontosidő-egysége biztosítja, ami **legfeljebb 1 másodperces** eltérést engedélyez a valódi időhöz képest. Az eltérések szintén naplózásra kerülnek.

3.1.1 A tárolt események típusai

A időbélyegzési rendszer által az egységekhez történő valamennyi hozzáférés és tevékenység naplózásra kerül. Így naplózásra kerül:

- a rendszerbe történő belépések és az operációs rendszer szempontjából fontos üzenetek rögzítése,
- a rendszer komponensek konfigurálására, a rendszer módosítására, beavatkozásra vonatkozó események rögzítése,
- minden felhasználó kezeléssel kapcsolatos esemény
- minden időbélyegző szolgáltatói kulccsal, tanúsítvánnyal kapcsolatos esemény

- helyi és külső időforrásokkal való kapcsolatfelvétel és időeltérés.
- a szolgáltatások elérhetősége (leállítása, indítása)
- a naplózási szolgáltatások leállítása, indítása

3.1.2 A tárolt események típusai

A napló-állományokat legalább **90 napig** tárolják a keletkezésük helyén. Ezek után az adatokat egyszer írható médiára archiválják, és a napló-állományok archív adathordozóit biztonságosan megőrzik a vonatkozó tanúsítvány érvényességének a lejártától számított **10 évig**, illetőleg a velük kapcsolatban esetleg felmerült jogvita jogerős lezárásáig.

3.2 Adatok archiválása

3.2.1 Az archivált adatok megőrzési időtartama

A Szolgáltató az archivált adatokat az alábbi időtartamig őrzi meg, illetve gondoskodik megőrzéséről:

- a minősített időbélyegzés szolgáltatás Szolgáltatási Szabályzatát a hatályon kívül helyezéstől számított 10 évig,
- az időbélyegző kibocsátásával kapcsolatos adatokat a vonatkozó tanúsítvány érvényességének a lejártától számított 10 évig,

4 Műszaki, biztonsági óvintézkedések

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.

4.1 Szolgáltatói kulcsok előállítása

Az időbélyegző szolgáltatás kulcspárjait egy bizalmi munkakört betöltő személy a biztonsági tisztviselő jelenlétében kriptográfiai modulban generálja. A generált magánkulcsok teljes életciklusuk alatt a kriptográfiai hardverekben maradnak, megsemmisítésükig azt se hová nem kell továbbítani.

4.2 Kriptográfiai modulok megfeleltetése

Szolgáltató az szolgáltatói magánkulcsainak tárolására, az időbélyegzők aláírására az alábbi kriptográfiai modulokat alkalmazza:

Kriptográfiai modul	Hardver verzió	Főrmver verzió
nCipher nShield F3 500	nC4033P-500	2.33.60
nCipher nShield F3 500e	nC4033E-500	2.55.1
Trident HSM	Trident v2.1.3	Trident v2.1.3

Az eszközök rendelkeznek a FIPS 140-2 Level 3 tanúsítással.

4.3 A tanúsítványok és a kulcspárok használatának periódusa

Az Időbélyegző Szervezet időbélyeget aláíró kulcsához tartozó tanúsítvány érvényességi ideje: **Legalább 10 év, de nem több mint 11 év.** Az Időbélyegző Szervezet magán kulcsainak érvényességi ideje: **5 év**

A Magyar Telekom RootCA 2011 magánkulcsának és tanúsítványának érvényességi ideje: **20 év**

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

4.4 Szolgáltatói kulcsok mentése

A Szolgáltatónál az Időbélyegző Szervezet magánkulcsai nem kerülnek mentésre, azokat a kriptográfiai modulban (HSM) állítja elő, és a magánkulcs semmilyen körülmények között nem hagyja el a modult.

Szolgáltató a szolgáltatói magánkulcsot nem állítja helyre, indokolt esetben új kulcspárt generál.

5 Megfelelőség

Szolgáltató megfelelőségének értékelését az 910/2014/EU rendelet, a hatályos magyar jogszabályok (2015. évi CCXXII törvény, 24/2016. (VI.30.) BM rendelet), valamint a vonatkozó ETSI szabványok (ETSI EN 319 401 v2.1.1, ETSI EN 319 421 v1.1.1) alapján 2020. november hónapban a Mátrix Kft. elvégezte, amelyről 2022. november 6-ig tartó érvényességgel „I-MT20T_TAN.QTIMESTAMP” számon tanúsítványt bocsátott ki.

A Magyar Telekom belső folyamataira integrált irányítási rendszert működtet, melyet független vizsgálóval – SGS - tanúsított és a megfelelőséget folyamatosan fenntartja. Az integrált irányítási rendszer elemei:

Megnevezés	Szabvány
Minőségirányítási rendszer	MSZ EN ISO 9001:2015
Környezetközpontú irányítási rendszer	MSZ EN ISO 1401:2015
Információvédelmi irányítási rendszer	MSZ EN ISO 27001:2014
Munkahelyi egészségvédelem és biztonságirányítási rendszer	MSZ 28001:2008
Üzletmenet folytonosságirányítási rendszer	ISO 22301:2010

6 Egyéb üzleti és jogi kérdések

6.1 Időbélyegzésszolgáltatási díjak

A Szolgáltató az időbélyegzés szolgáltatásért díjat számol fel a vonatkozó Szolgáltatási Szerződésben (ISzSz) foglaltak szerint.

6.2 Díjvisszatérítés

Díjvisszatérítésre jogosult az előfizető a Szolgáltatási Szerződésben vállalt szolgáltatási szint nem teljesítése esetén, az abban foglaltak szerint.

6.3 Anyagi felelősségvállalás, felelősségbiztosítás

A Szolgáltató a megbízhatóság biztosítása érdekében felelősségbiztosítással is rendelkezik. A felelősségbiztosítási szerződés kiterjed a Szolgáltató által a szolgáltatások nyújtásával összefüggésben okozott, a Szolgáltatási Szerződésben meghatározott térítendő kárra. A biztosítás egy biztosítási esemény vonatkozásában **10.000.000 Ft** (Tízmillió forint) káreseményenként és összességében évente **50.000.000 Ft** (Ötvenmillió forint) összegig fedezetet biztosít az összes károsultnak okozott károkra. Több azonos okból bekövetkezett, időben összefüggő káresemény egy biztosítási eseménynek minősül.

Ha egy biztosítási eseménnyel kapcsolatban több jogosult megalapozott kártérítési igénye meghaladja a károkra biztosítási eseményenként a felelősségbiztosítási szerződésben meghatározott összeget, akkor a kártérítési igények megtérítése az összes kártérítési igénynek a felelősségbiztosítási szerződésben meghatározott összeghez viszonyított arányában történik.

6.4 A személyes adatok védelme

A Szolgáltató a Szolgáltatás keretében a Szolgáltatási Szerződésben, az ahhoz kapcsolódó dokumentációban, valamint a Szolgáltató által az Előfizetőnek kiadott autentikációs tanúsítványban rögzített, az Előfizetőre, illetve az aláírókra, az Előfizető érintett munkavállalóira, képviselőire és kapcsolattartóira vonatkozó személyes adatokat kezeli, adatkezelőként.

A Szolgáltató különböző társasági és csoport szintű adatvédelmi és adatbiztonsági szabályzatokkal rendelkezik, amelyek a személyes adatok kezelésére általánosságban alkalmazandók, és amelyek a Szolgáltatással kapcsolatos adatkezelésekre is vonatkoznak. Ezek közül kiemelt jelentőségű a Deutsche Telekom Csoport Kötelező Erejű Vállalati Szabályaira vonatkozó szabályzat, amely a Szolgáltatóra nézve is kötelező, és amely nyilvánosan is elérhető: [Binding Corporate Rules Privacy \(BCRP\) \(telekom.com\)](https://www.telekom.com/en/privacy-policy). A Szolgáltatásra vonatkozó speciális adatkezelést jelen Szabályzat és az ahhoz kapcsolódó dokumentumok speciális és operatív szinten tárgyalják.

Szolgáltató az időbélyegzés szolgáltatással összefüggő adatkezelésről tájékoztatót jelentet meg a szolgáltatás honlapján, és a Szolgáltatás körében kezelt személyes adatokat a tájékoztatóban foglaltak szerint kezeli:

http://www.t-systems.hu/static/sw/file/Adatkezelesi_tajekoztato_signed.pdf

6.5 Tevékenységért viselt felelősség és helytállás

A Szolgáltató általános felelőssége:

- a) A Szolgáltató felelősséget vállal az Időbélyegzési Rend dokumentumban leírt eljárásoknak való megfeleléséért, még abban az esetben is, amikor a Szolgáltató egyes tevékenységeit alvállalkozók végzik².
- b) A Szolgáltató a vele szerződéses jogviszonyban álló felekkel (előfizető) szemben a Magyar Köztársaság Polgári Törvénykönyvének a szerződésszegésért való felelősség szabályai szerint felelős.

A Szolgáltató feladata az Időbélyegző Szervezet és a címtár működtetése. A Szolgáltatónak szolgáltatásait a hatályos jogi szabályozással, szolgáltatási szabályzatával és egyéb nyilvánosságra hozott szabályzataival, szerződéses feltételeivel összhangban kell nyújtania. A Szabályzat keretei között végzett szolgáltatói tevékenységekért (beleértve az esetlegesen igénybe vett alvállalkozókat is) a Magyar Telekom Nyrt. a felelős.

6.5.1 Az időbélyegzés szolgáltató felelőssége és helytállása

- a) Az Időbélyegző Szervezet **felelős**:
 - a kiadott időbélyeg szabványoknak történő megfeleléséért,
 - az időbélyegben szereplő időért,
 - általában a kötelezettségei betartásáért.
- b) Az Időbélyegző Szervezet **nem felelős**:
 - az előfizetők időbélyeg felhasználással kapcsolatos tevékenységeiért,
 - az előfizetők, érintett felek, és mások által kibocsátott szabályzatokért.

6.5.2 Az előfizető és érintett fél felelőssége és helytállása

Az előfizető felelős:

- a Szolgáltatási Szerződés betartásáért,
- a számára kibocsátott autentikációs tanúsítványok és az ehhez tartozó kulcspár tulajdonosi kötelezettségeiért,
- a Szolgáltató haladéktalan értesítéséért és teljes körű tájékoztatásáért vitás ügyekben,
- az időbélyegzés szolgáltatás díja(i)nak szerződés szerinti kifizetéséért, azaz a számlákon szereplő összegek megjelölt időpontig történő kifizetéséért (eltérő megállapodás hiányában),
- általában a kötelezettségei betartásáért.

Az előfizető felelős:

² Az időbélyegzés-szolgáltató általánosan felelős az időbélyegző szervezet, valamint a címtár kötelezettségeiért, tevékenységeiért.

- Az érintett fél felelős a jogszabályokban írt kötelezettségek betartásáért és az adott helyzetben általában elvárható magatartás tanúsításáért, különösen az elektronikus aláírás, az időbélyeg ellenőrzéséért, illetve a tanúsítványok elfogadása során tanúsított körülményekről eljárásért.

6.5.3 Felelősségi korlátozások

A Szolgáltató nem felelős az olyan károkért, mely abból adódott, hogy az érintett fél az időbélyeg ellenőrzése és felhasználása során nem a hatályos jogszabályok és szolgáltatói szabályzatai szerint járt el, illetve nem úgy járt el, ahogyan az adott helyzetben elvárható.

Pénzügyi felelősség korlátozása

A Szolgáltató a kártérítés felső határát összességében korlátozza. A Szolgáltató pénzügyi felelősségével kapcsolatos további részleteket az **IBSzSz** és **ÁSZF** dokumentum tartalmazza.

6.5.4 Vitás kérdések megoldása

A szolgáltatással kapcsolatos bármely vitás kérdés vagy panasz felmerülése esetén a vita jogi útra terelése előtt az előfizetőnek kötelessége a Szolgáltató haladéktalan értesítése és teljes körű tájékoztatása az ügy minden vonatkozását érintően. A felek vitáikat mindenkor megkísérik békés, tárgyalásos úton rendezni.

A Szolgáltató (beleértve az Időbélyegző Szervezetet is) tevékenységével kapcsolatos kérdéseket, kifogásokat és panaszokat az **Hiba! A hivatkozási forrás nem található.** alfejezetben rögzített Időbélyegző Szervezetre vonatkozó elérhetőségeken lehet megtenni.

A szolgáltatással kapcsolatban illetékes fogyasztóvédelmi felügyelőséget, melynek adatai a következők:

Budapest Főváros Kormányhivatal
Fogyasztóvédelmi Főosztály, Fogyasztóvédelmi Osztály
székhely/levelezési cím: 1052 Budapest, Sas u. 19.
tel: (06 1) 450 2598
e-mail cím: fogyved_kmf_budapest@bfkh.gov.hu

A Szabályzat szerinti szolgáltatással kapcsolatban vitás esetek, jogviták rendezésére igénybevehető békéltető testület, melynek adatai a következők:

Budapesti Békéltető Testület
1016 Budapest, Krisztina krt. 99.
1253 Budapest, Pf. 10.
tel.: +361 488 2131
E-mail: bekelteto.testulet@bkik.hu

Az eljárás további részleteit az **ÁSZF** dokumentum 14. pontja tartalmazza

6.5.5 Irányadó jog

A Szolgáltató tevékenységét a mindenkor hatályos magyar jogszabályoknak megfelelően végzi. A Szolgáltató szerződéseire és szabályzataira, azok teljesítésére a magyar jog az irányadó, s azok a magyar jog szerint értelmezendők.