



# Magyar Telekom

## Minősített Időbélyegzés Szolgáltatás

### Szolgáltatási Szabályzata

Egyedi objektum-azonosító (OID): ..... 1.3.6.1.4.1.17835.7.1.2.11.3.13.3.5

Verziószám: ..... 3.5

Hatályba lépés dátuma: ..... 2026.05.28.



## Változáskezelés

| Verzió-szám | Dátum         | A változás leírása                                                                                                                |
|-------------|---------------|-----------------------------------------------------------------------------------------------------------------------------------|
| 0.90        | 2003-10-10    | Első változat (szakértői munkaanyagok)                                                                                            |
| 0.91        | 2003-10-26    | Javított tervezet (első változat)                                                                                                 |
| 0.92        | 2003-10-31    | Javított tervezet (ellenőrzött változat)                                                                                          |
| 0.93        | 2003-11-30    | Javított tervezet (kiegészített és ellenőrzött harmadik változat)                                                                 |
| 0.94        | 2003-12-15    | A kiviteli dokumentumokkal egyeztetett változat                                                                                   |
| 0.95        | 2004-01-30    | A tesztek és jogi ellenőrzések alapján módosított első változat                                                                   |
| 0.96        | 2004-03-05    | A szolgáltatói ellenőrzések után javított változat                                                                                |
| 0,97        | 2004-03-11    | Matáv Workshop utáni javított változat                                                                                            |
| 1.0         | 2004-03-30    | Hatósági kérelemben beadott szabályzat                                                                                            |
| 1.1         | 2004-07-17    | Hatósági szemlét követő változások átvezetése                                                                                     |
| 1.2         | 2004-09-23    | Hatóság részére átadott végső változat                                                                                            |
| 1.3         | 2005-09-01    | Magyar Telekom névváltásának és következményeinek módosítása                                                                      |
| 1,4         | 2005-11-15    | Hatósági ellenőrzést követő változások átvezetése                                                                                 |
| 1.5         | 2005-12-30    | Hatósági és külső ellenőrzéseket követő változások átvezetése                                                                     |
| 1.6         | 2006-07-20    | Nemzeti Hírközlési Hatóság Hivatalának észrevételei szerinti javítások                                                            |
| 1.7         | 2006-12-18    | Ket.-es fejlesztésekhez és a 2006. évi Hatósági szemléhez kapcsolódó módosítások                                                  |
| 1.71        | 2007-03-10    | Hatósági észrevételek szerint valamint az rfc 3647szerint módosított változat                                                     |
| 1.8         | 2009.03.01    | A Hatóság észrevételei szerinti módosítás (HL-923-1/2009)                                                                         |
| 1.9         | 2010. 06. 20. | Hitelesítés szolgáltatás kivezetésével beállt változások átvezetése                                                               |
| 2.0         | 2010.11.09.   | EASZ és Hatósági észrevételek átvezetése                                                                                          |
| 2.1         | 2011.12.05.   | Hatósági észrevétel (9.2 pont javítása) és szervezeti változás átvezetése. Az algoritmus határozatból adódó változások átvezetése |
| 2.2         | 2014.10.08    | Felülvizsgálat, EASZ és Hatósági észrevételek átvezetése, kriptográfiai modul adatainak változása                                 |
| 2.3         | 2015.12.21    | Felelősségbiztosítás adatainak megváltozása                                                                                       |
| 2.4         | 2017.05.11    | Jogszabályi, szervezeti és személyi változások átvezetése. 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                                                                      |
| 2.7         | 2022.01.31.   | NMHH észrevételek javítása                                                                                                        |
| 2.8         | 2022.04.25.   | Mátrix észrevételek átvezetése                                                                                                    |
| 2.9         | 2023.03.28.   | NMHH és Mátrix észrevételek átvezetése.                                                                                           |
| 3.0         | 2024.04.02.   | NMHH és Mátrix észrevételek átvezetése, A Hatóság észrevételei szerinti módosítás (K/5414/2024)                                   |
| 3.1         | 2024.07.10.   | Kulcsmentés eljárás változásának átvezetése                                                                                       |
| 3.2         | 2024.09.27    | Dáptv. -re való hivatkozás átvezetése                                                                                             |



|     |             |                                                                |
|-----|-------------|----------------------------------------------------------------|
| 3.3 | 2025.09.05. | Megfelelőség értékelő észrevételeinek és változások átvezetése |
| 3.4 | 2026.03.02  | Éves felülvizsgálat, adatok pontosítása                        |
| 3.5 | 2026.05.28. | Új HSM eszközök átvezetése                                     |

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



# TARTALOMJEGYZÉK

|                                                                           |           |
|---------------------------------------------------------------------------|-----------|
| <b>VÁLTOZÁSKEZELÉS .....</b>                                              | <b>2</b>  |
| <b>1 BEVEZETÉS .....</b>                                                  | <b>9</b>  |
| 1.1 ÁTTEKINTÉS .....                                                      | 9         |
| 1.1.1 A Szabályzat .....                                                  | 9         |
| 1.1.2 A Szabályzat hatályai .....                                         | 9         |
| 1.1.3 A szolgáltató .....                                                 | 10        |
| 1.1.4 Szolgáltatások .....                                                | 11        |
| 1.1.5 Szabványok és előírások .....                                       | 12        |
| 1.1.6 Időbélyegzés-szolgáltatás .....                                     | 12        |
| 1.2 A DOKUMENTUM NEVE ÉS AZONOSÍTÓJA .....                                | 13        |
| 1.3 PKI SZEREPLŐK .....                                                   | 14        |
| 1.3.1 Időbélyegző szervezet .....                                         | 14        |
| 1.3.2 Előfizetők, érintett felek .....                                    | 15        |
| 1.3.3 Egyéb szereplők .....                                               | 15        |
| 1.4 A SZOLGÁLTATÁSI SZABÁLYZAT ADMINISZTRÁLÁSA .....                      | 16        |
| 1.4.1 Adminisztrációért felelős szervezet és kapcsolattartó személy ..... | 16        |
| 1.4.2 A Szolgáltatási Szabályzat elfogadási eljárása .....                | 17        |
| 1.4.3 Szabályzat -változtatási eljárások .....                            | 17        |
| 1.5 MEGHATÁROZÁSOK .....                                                  | 18        |
| 1.6 RÖVIDÍTÉSEK ÉS JELÖLÉSEK .....                                        | 19        |
| 1.7 HIVATKOZÁSOK .....                                                    | 19        |
| <b>2 KÖZZÉTÉTELRE ÉS TÁROLÁSRA VONATKOZÓ FELELŐSSÉGEK .....</b>           | <b>21</b> |
| 2.1 ADATBÁZISOK .....                                                     | 21        |
| 2.2 AZ IDŐBÉLYEGZŐKRE VONATKOZÓ INFORMÁCIÓK KÖZZÉTÉTELE .....             | 21        |
| 2.3 A KÖZZÉTÉTEL GYAKORISÁGA .....                                        | 22        |
| 2.4 AZ ADATBÁZISOK ELÉRÉSÉNEK SZABÁLYOZÁSA .....                          | 22        |
| <b>3 AZONOSÍTÁS ÉS HITELESÍTÉS .....</b>                                  | <b>23</b> |
| 3.1 MEGNEVEZÉSI KONVENCIÓK .....                                          | 23        |
| 3.1.1 Márkanévek elismerése, azonosításuk és szerepük .....               | 23        |
| <b>4 MŰKÖDÉSRE VONATKOZÓ KÖVETELMÉNYEK – IDŐBÉLYEGZÉS .....</b>           | <b>24</b> |
| 4.1 IDŐBÉLYEGZÉS SZOLGÁLTATÁS IGÉNYLÉSE .....                             | 24        |
| 4.2 AZ IDŐBÉLYEGZÉS SZOLGÁLTATÁS TELJESÍTÉSE .....                        | 25        |
| 4.3 MINŐSÍTETT IDŐBÉLYEGZÉS-SZOLGÁLTATÁS JOGHATÁSA .....                  | 25        |



|       |                                                                                                                                                                                                                                                                                                                                                                                                             |           |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| 4.4   | AZ IDŐBÉLYEGZÉS SZOLGÁLTATÁS IGÉNYBEVÉTELÉNEK VÉGE .....                                                                                                                                                                                                                                                                                                                                                    | 25        |
| 5     | <b>ELHELYEZÉSI, IRÁNYÍTÁSI ÉS MŰKÖDTETÉSI ELŐÍRÁSOK.....</b>                                                                                                                                                                                                                                                                                                                                                | <b>26</b> |
| 5.1   | FIZIKAI ELŐÍRÁSOK.....                                                                                                                                                                                                                                                                                                                                                                                      | 26        |
| 5.1.1 | A telephely elhelyezése és szerkezeti felépítése .....                                                                                                                                                                                                                                                                                                                                                      | 26        |
| 5.1.2 | Fizikai hozzáférés.....                                                                                                                                                                                                                                                                                                                                                                                     | 27        |
| 5.1.3 | Áramellátás, légkondicionálás.....                                                                                                                                                                                                                                                                                                                                                                          | 27        |
| 5.1.4 | Beázás és elárasztás veszélyeztetettsége .....                                                                                                                                                                                                                                                                                                                                                              | 28        |
| 5.1.5 | Tűz megelőzés és tűzvédelem .....                                                                                                                                                                                                                                                                                                                                                                           | 28        |
| 5.1.6 | Adathordozók tárolása .....                                                                                                                                                                                                                                                                                                                                                                                 | 29        |
| 5.1.7 | Hulladék megsemmisítése és selejtezés .....                                                                                                                                                                                                                                                                                                                                                                 | 29        |
| 5.1.8 | A mentési példányok fizikai elkülönítése.....                                                                                                                                                                                                                                                                                                                                                               | 29        |
| 5.1.9 | Hálózati redundancia.....                                                                                                                                                                                                                                                                                                                                                                                   | 29        |
| 5.2   | <b>ELJÁRÁSBELI ÓVINTÉZKEDÉSEK .....</b>                                                                                                                                                                                                                                                                                                                                                                     | <b>29</b> |
| 5.2.1 | Bizalmi munkakörök .....                                                                                                                                                                                                                                                                                                                                                                                    | 30        |
| 5.2.2 | Az egyes feladatokhoz szükséges személyzeti létszámok .....                                                                                                                                                                                                                                                                                                                                                 | 32        |
| 5.2.3 | Az egyes munkakörökben elvárt azonosítás és hitelesítés .....                                                                                                                                                                                                                                                                                                                                               | 32        |
| 5.2.4 | Egymást kizáró munkakörök .....                                                                                                                                                                                                                                                                                                                                                                             | 32        |
| 5.3   | <b>SZEMÉLYZETRE VONATKOZÓ ELŐÍRÁSOK.....</b>                                                                                                                                                                                                                                                                                                                                                                | <b>33</b> |
| 5.3.1 | Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények ..                                                                                                                                                                                                                                                                                                                             | 33        |
| 5.3.2 | Előélet vizsgálatára és biztonsági háttér ellenőrzésekre vonatkozó eljárások.....                                                                                                                                                                                                                                                                                                                           | 34        |
| 5.3.3 | Kiképzési követelmények .....                                                                                                                                                                                                                                                                                                                                                                               | 35        |
| 5.3.4 | Továbbképzési gyakoriságok és követelmények .....                                                                                                                                                                                                                                                                                                                                                           | 35        |
| 5.3.5 | Munkabeosztás körforgásának gyakorisága és sorrendje .....                                                                                                                                                                                                                                                                                                                                                  | 36        |
| 5.3.6 | A felhatalmazás nélküli tevékenységek büntető következményei .....                                                                                                                                                                                                                                                                                                                                          | 36        |
| 5.3.7 | A szerződéses alkalmazottakra vonatkozó követelmények .....                                                                                                                                                                                                                                                                                                                                                 | 36        |
| 5.3.8 | Kinevezési eljárás .....                                                                                                                                                                                                                                                                                                                                                                                    | 37        |
| 5.3.9 | A személyzet számára biztosított dokumentációk.....                                                                                                                                                                                                                                                                                                                                                         | 37        |
| 5.4   | <b>NAPLÓZÁSI ELJÁRÁSOK .....</b>                                                                                                                                                                                                                                                                                                                                                                            | <b>37</b> |
| 5.4.1 | A tárolt események típusai.....                                                                                                                                                                                                                                                                                                                                                                             | 38        |
| 5.4.2 | A napló állomány feldolgozásának gyakorisága.....                                                                                                                                                                                                                                                                                                                                                           | 38        |
| 5.4.3 | A napló-állomány megőrzési időtartama .....                                                                                                                                                                                                                                                                                                                                                                 | 38        |
| 5.4.4 | A napló állomány védelme .....                                                                                                                                                                                                                                                                                                                                                                              | 39        |
| 5.4.5 | A napló állomány mentési folyamatai .....                                                                                                                                                                                                                                                                                                                                                                   | 39        |
| 5.4.6 | A napló gyűjtési rendszere .....                                                                                                                                                                                                                                                                                                                                                                            | 39        |
| 5.4.7 | Log-elemzés .....                                                                                                                                                                                                                                                                                                                                                                                           | 39        |
| 5.5   | <b>ADATOK ARCHIVÁLÁSA.....</b>                                                                                                                                                                                                                                                                                                                                                                              | <b>39</b> |
| 5.5.1 | Az archivált adatok típusai.....                                                                                                                                                                                                                                                                                                                                                                            | 40        |
| 5.5.2 | Az archívum megőrzési időtartama.....                                                                                                                                                                                                                                                                                                                                                                       | 40        |
| 5.5.3 | Szolgáltató valamennyi (papíralapú vagy elektronikus) iratot avonatkozó tanúsítvány érvényességének lejártától számított 10 évig, illetőleg velük kapcsolatban esetlegesen felmerült jogvita jogerős lezárásáig megőrzi. Szolgáltató a Szolgáltatási Szabályzatot és annak módosításait hatályon kívül helyezést követően 10 évig megőrzi, illetve gondoskodik annak megőrzéséről. Az archívum védelme..... | 40        |



|        |                                                                                               |    |
|--------|-----------------------------------------------------------------------------------------------|----|
| 5.5.4  | Az archívum mentési folyamatai.....                                                           | 40 |
| 5.5.5  | Archív információ hozzáférését és ellenőrzését végző eljárások.....                           | 40 |
| 5.6    | KOMPROMITTÁLÓDÁST ÉS KATASZTRÓFÁT KÖVETŐ HELYREÁLLÍTÁS .....                                  | 41 |
| 5.6.1  | Váratlan esemény és kompromittálódás kezelési eljárások .....                                 | 41 |
| 5.6.2  | Meghibásodott számítási erőforrások, szoftverek és/vagy adatok.....                           | 41 |
| 5.6.3  | Egy szolgáltatói egység kulcsának kompromittálódása .....                                     | 42 |
| 5.6.4  | Működés folyamatosságának biztosítása katasztrófát követően .....                             | 42 |
| 5.6.5  | Egy szolgáltatói egység órájának 1 másodpercnél nagyobb eltérése az UTC időtől<br>42          |    |
| 5.7    | INCIDENSKEZELÉS .....                                                                         | 43 |
| 5.8    | VÁLTOZÁSKÉZELÉS.....                                                                          | 43 |
| 5.9    | IDŐSZINKRONIZÁCIÓ .....                                                                       | 43 |
| 5.10   | IDŐBÉLYEG SZOLGÁLTATÓ VAGY SZERVEZET LEÁLLÍTÁSA.....                                          | 44 |
| 6      | MŰSZAKI BIZTONSÁGI ÓVINTÉZKEDÉSEK .....                                                       | 45 |
| 6.1    | KULCSPÁR ELŐÁLLÍTÁS ÉS TELEPÍTÉS.....                                                         | 45 |
| 6.1.1  | Kulcspár előállítás.....                                                                      | 45 |
| 6.1.2  | A szolgáltatói nyilvános kulcs közzététele.....                                               | 45 |
| 6.1.3  | Kulcs méretek .....                                                                           | 45 |
| 6.1.4  | A nyilvános kulcs paraméterek előállítása és ellenőrzése .....                                | 45 |
| 6.1.5  | A kulcs használat célja (az X.509 v3 kulcs használati mező tartalmának<br>megfelelően).....   | 46 |
| 6.1.6  | Magyar Telekom SuperProxy védelme .....                                                       | 46 |
| 6.2    | A SZOLGÁLTATÓI MAGÁNKULCSOK VÉDELME ÉS A KRIPTOGRÁFIAI MODULOKKAL KAPCSOLATOS<br>ELŐÍRÁSOK 47 |    |
| 6.2.1  | Kriptográfiai modulra vonatkozó szabványok.....                                               | 47 |
| 6.2.2  | A több-szereplős ("n-ből m") magánkulcs visszaállítás ellenőrzése .....                       | 47 |
| 6.2.3  | Magánkulcs mentése .....                                                                      | 47 |
| 6.2.4  | Magánkulcs archiválása .....                                                                  | 48 |
| 6.2.5  | Magánkulcs bejuttatása a kriptográfiai modulba .....                                          | 48 |
| 6.2.6  | Magánkulcs tárolása a kriptográfiai modulba .....                                             | 48 |
| 6.2.7  | A magánkulcs aktiválásának módja.....                                                         | 48 |
| 6.2.8  | A magánkulcs aktív állapotának megszüntetési módja .....                                      | 48 |
| 6.2.9  | A magánkulcs megsemmisítésének módja .....                                                    | 48 |
| 6.2.10 | A kriptográfiai modulok értékelése .....                                                      | 49 |
| 6.3    | A KULCSPÁR KEZELÉSÉNEK EGYÉB SZEMPONTJAI.....                                                 | 50 |
| 6.3.1  | A tanúsítványok és a kulcspárok használatának periódusa.....                                  | 50 |
| 6.4    | INFORMATIKAI BIZTONSÁGI ÓVINTÉZKEDÉSEK.....                                                   | 51 |
| 6.4.1  | Speciális informatikai biztonsági műszaki követelmények.....                                  | 51 |
| 6.4.2  | Informatikai biztonsági minősítés .....                                                       | 53 |
| 6.4.3  | A szolgáltatásban alkalmazott termékek kezelése .....                                         | 53 |
| 6.5    | ÉLETCIKLUSRA VONATKOZÓ MŰSZAKI ÓVINTÉZKEDÉSEK.....                                            | 54 |
| 6.5.1  | Rendszerfejlesztési óvintézkedések .....                                                      | 54 |
| 6.5.2  | Biztonságkezelési óvintézkedések.....                                                         | 54 |
| 6.5.3  | Az életciklusra vonatkozó biztonság osztályozása .....                                        | 54 |



|       |                                                                     |    |
|-------|---------------------------------------------------------------------|----|
| 6.5.4 | <i>Behatolási tesztek</i> .....                                     | 54 |
| 6.5.5 | <i>Kapacitás figyelés és tervezés</i> .....                         | 55 |
| 6.5.6 | <i>Kockázatelemzés</i> .....                                        | 55 |
| 6.5.7 | <i>Jogosultságkezelés</i> .....                                     | 56 |
| 6.6   | <b>HÁLÓZATBIZTONSÁGI ÓVINTÉZKEDÉSEK</b> .....                       | 56 |
| 6.7   | <b>HSM TANÚSÍTOTTSÉG MEGLÉTÉNEK ELLENŐRZÉSE</b> .....               | 56 |
| 7     | <b>TANÚSÍTVÁNY PROFIL</b> .....                                     | 58 |
| 7.1   | VERZIÓ SZÁM(OK) .....                                               | 58 |
| 7.2   | TANÚSÍTVÁNY-KITERJESZTÉSEK .....                                    | 58 |
| 7.3   | AZ ALGORITMUS OBJEKTUM-AZONOSÍTÓJA .....                            | 60 |
| 7.4   | ELNEVEZÉSI FORMÁK .....                                             | 60 |
| 7.5   | ELNEVEZÉSRE VONATKOZÓ KORLÁTOZÁSOK .....                            | 60 |
| 7.6   | AZ IDŐBÉLYEGZÉSI REND OBJEKTUM-AZONOSÍTÓJA .....                    | 61 |
| 7.7   | A „HITELESÍTÉSI REND KORLÁTOZÁS” KITERJESZTÉS HASZNÁLATA .....      | 61 |
| 7.8   | SZABÁLYZATMINŐSÍTŐ SZINTAXIS ÉS SZEMANTIKA .....                    | 61 |
| 7.9   | A KRITIKUS IDŐBÉLYEGZÉSI REND KITERJESZTÉS FELDOLGOZÁSA .....       | 61 |
| 7.10  | IDŐBÉLYEGZŐ PROFIL .....                                            | 61 |
| 8     | <b>MEGFELELŐSÉGI AUDIT ÉS EGYÉB ELLENŐRZÉSEK</b> .....              | 62 |
| 8.1   | AZ ELLENŐRZÉSEK KÖRÜLMÉNYEI ÉS GYAKORISÁGA .....                    | 62 |
| 8.2   | AZ AUDITOR ÉS SZÜKSÉGES KÉPESÍTÉSE .....                            | 62 |
| 8.3   | AZ AUDITOR ÉS AZ AUDITÁLT RENDSZER FÜGGETLENSÉGE .....              | 63 |
| 8.4   | AZ AUDITÁLÁS ÁLTAL LEFEDETT TERÜLETEK .....                         | 63 |
| 8.5   | A HIÁNYOSSÁGOK KEZELÉSE .....                                       | 63 |
| 8.6   | AZ EREDMÉNYEK KÖZZÉTÉTELE .....                                     | 63 |
| 9     | <b>EGYÉB ÜZLETI ÉS JOGI KÉRDÉSEK</b> .....                          | 64 |
| 9.1   | DÍJAK .....                                                         | 64 |
| 9.2   | ANYAGI FELELŐSSÉGVÁLLALÁS, FELELŐSSÉGBIZTOSÍTÁS .....               | 64 |
| 9.3   | AZ ÜZLETI INFORMÁCIÓK BIZALMASSÁGA .....                            | 64 |
| 9.4   | A SZEMÉLYES ADATOK VÉDELME .....                                    | 65 |
| 9.4.1 | <i>Bizalmasan kezelendő információ-típusok</i> .....                | 66 |
| 9.4.2 | <i>Információszoolgáltatás a hatóságok részére</i> .....            | 66 |
| 9.4.3 | <i>Információszoolgáltatás polgári eljárás keretében</i> .....      | 66 |
| 9.4.4 | <i>A tulajdonos kérésére történő felfedés</i> .....                 | 67 |
| 9.5   | SZELLEMI TULAJDONJOGOK .....                                        | 67 |
| 9.6   | TEVÉKENYSÉGÉRT VISELT FELELŐSSÉG ÉS HELYTÁLLÁS .....                | 67 |
| 9.6.1 | <i>Az időbélyegzés szolgáltató felelőssége és helytállása</i> ..... | 67 |
| 9.6.2 | <i>Az előfizető felelőssége és helytállása</i> .....                | 68 |
| 9.6.3 | <i>Az érintett fél felelőssége</i> .....                            | 68 |
| 9.7   | HELYTÁLLÁS ÉRVÉNYTELENSÉGI KÖRE .....                               | 68 |
| 9.8   | FELELŐSSÉGI KORLÁTOZÁSOK .....                                      | 68 |
| 9.9   | KÁRTÉRÍTÉSI KÖTELEZETTSÉGEK .....                                   | 68 |
| 9.10  | ÉRVÉNYESSÉG .....                                                   | 69 |



|      |                                                          |    |
|------|----------------------------------------------------------|----|
| 9.11 | A FELEK KÖZÖTTI KOMMUNIKÁCIÓRA VONATKOZÓ ELŐÍRÁSOK.....  | 69 |
| 9.12 | DISZKRIMINÁCIÓ MENTESSÉG.....                            | 69 |
| 9.13 | KIEGÉSZÍTÉSEK .....                                      | 69 |
| 9.14 | VITÁS KÉRDÉSEK MEGOLDÁSA .....                           | 70 |
| 9.15 | IRÁNYADÓ JOG .....                                       | 70 |
| 9.16 | AZ ÉRVÉNYBEN LÉVŐ JOGSZABÁLYOKNAK VALÓ MEGFELELŐSÉG..... | 70 |

## 1 Bevezetés

### 1.1 Áttekintés

#### 1.1.1 A Szabályzat

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 ([13]) együttesen szabályozzák {ld. 1.7 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.

#### 1.1.2 A Szabályzat hatályai

##### A Szabályzat tárgyi hatálya

A Szabályzat tárgyi hatálya az {1.1.4 Szolgáltatások} alfejezetben ismertetett szolgáltatások nyújtására és igénybevételeire, illetve ezen szolgáltatásokkal kapcsolatos összes objektumra és tárgyi eszközre kiterjed.

##### A Szabályzat területi hatálya

A Szabályzat területi hatálya az **Európai Unió** teljes területe.

## A Szabályzat időbeli hatálya

A Szabályzat határozatlan időre szól a címlapon feltüntetett jelen szabályzati verzióra érvényes hatálybalépés dátumától kezdődően. (A Szabályzat időbeli hatálya a szolgáltatás beszüntetésekor, illetve egy újabb szabályzati verzió hatályba lépésekor szűnik meg.)

## A Szabályzat személyi hatálya

A Szabályzat személyi hatálya a teljes közösség {ld. **0** PKI szereplők} minden egyes tagjára, természetes, jogi személyiségű, illetve jogi személyiséggel nem rendelkező személyekre (szervezetekre) egyaránt kiterjed.

### 1.1.3 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 Szolgáltatót jogi értelemben a **Magyar Telekom Nyrt.** képviseli.

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 910/2014/EU rendelet, a hatályos magyar jogszabályok (2023. évi CIII. 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. A tanúsítvány sorszáma: 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 (2023. évi CIII. 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) szerint a Mátix Kft. végezte, amelyről a kibocsátott tanúsítvány az alábbi linken érhető el:

<https://matrix-tanusito.hu/it-tanusitvanyok>

A magyar nemzeti bizalmi lista elérhetősége:

- humán olvasható PDF formátumban: [http://www.nmhh.hu/tl/pub/HU\\_TL.pdf](http://www.nmhh.hu/tl/pub/HU_TL.pdf)
- géppel feldolgozható XML formátumban: [http://www.nmhh.hu/tl/pub/HU\\_TL.xml](http://www.nmhh.hu/tl/pub/HU_TL.xml)

A Nemzeti Média- és Hírközlési Hatóság bizalmi szolgáltatásokkal kapcsolatos nyilvántartása az alábbi elérhetőségen található:

<https://esign.nmhh.hu/bszny/>

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

|                        |                                                               |
|------------------------|---------------------------------------------------------------|
| <b>Név:</b>            | Magyar Telekom Távközlési Nyilvánosan Működő Részvénytársaság |
| <b>Cégjegyzékszám:</b> | CG 01-10041928                                                |
| <b>Székhely:</b>       | 1097 Budapest, Könyves Kálmán körút 36.                       |
| <b>Postacím:</b>       | 1541 Budapest                                                 |
| <b>Telefon:</b>        | 1400                                                          |
| <b>Honlap:</b>         | <a href="http://www.telekom.hu/">http://www.telekom.hu/</a>   |

A Szolgáltató **alvállalkozók** bevonásával végzi az alábbi tevékenységeket:

- Létesítményüzemeltetés, áramellátás
- Fizikai és elektronikai védelmi berendezések időszakos felülvizsgálata, karbantartása és javítása
- Egyes alkalmazások, eszközök új verzióinak tesztelése
- Üzemszerű rendszerelem cserék előkészítése, implementációs, és tesztelési tervek elkészítése,
- Üzemeltetés támogatás, konfigurációs és hardening feladatok szakértői előkészítése
- Sebezhetőség vizsgálatok

Az **alvállalkozók** tevékenységéért a Szolgáltató **teljes felelősséggel tartozik**.

#### 1.1.4 Szolgáltatások

A Magyar Telekom Nyrt. tevékenységi köre – egyebek mellett – kiterjed az időbélyegzés szolgáltatásra és az ehhez kötődő fejlesztési és tanácsadási tevékenységekre.

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 bizonyítéku 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 hozzáférhető aláírással ellátott elektronikus dokumentumhoz, továbbá aláírással nem ellátott állományok esetében is használható.

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.

### 1.1.5 Szabványok és előírások

A Szabályzat tartalmi vonatkozásokban eleget tesz az [1], [2], [3] és [4] szerinti EU és hazai jogszabályok előírásainak, kapcsolódó rendeleteinek és ajánlásainak. {ld. 1.7 **Hivatkozások**}.

Jelen szabályzathoz kapcsolódó időbélyeg felhasználásának joghatásairól a minősített időbélyegzés szolgáltatásra vonatkozó Általános Szerződési Feltételek (ÁSZF) című dokumentum előírásai is rendelkeznek, amely megtalálható a Szolgáltató honlapján a <https://www.telekom.hu/vallalati-megoldasok/nagyvallalatok/hitelesites-szolgáltatások/idobelyegzes-szolgáltatás>.

A szolgáltató az ETSI EN 301 549 szabványt figyelembe veszi.

### 1.1.6 Időbélyegzés-szolgáltatás

Az eIDAS 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.

A szolgáltatáshoz kétféle tevékenység köthető:

- maga az **időbélyegzés-szolgáltatás**, amelyet a Szolgáltató minősített időbélyegzés-szolgáltatásként (előfizetési alapon) nyújt ügyfeleinek.
- a szolgáltatást biztosító menedzsment folyamatok - **időjel ellátás**

Az időbélyegek 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 szolgáltat<sup>1</sup>,
- 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, valamint az ETSI EN 319 421 és az ETSI EN 319 422 szabvány erre vonatkozó előírásainak.

## 1.2 A dokumentum neve és azonosítója

Jelen szabályzat neve: **A Magyar Telekom Minősített Időbélyegzés-szolgáltatás Szolgáltatási Szabályzata.**

A szabályzat rövid neve: Magyar Telekom IBSzSz, vagy egyszerűen csak IBSzSz, (ebben a dokumentumban még Szabályzat).

A Szabályzat az alábbi adatokkal azonosítható:

**Egyedi objektum-azonosító (OID):** ..... a Szabályzat fedőlapján található

**Verziószám:** ..... a Szabályzat fedőlapján található

**A hatályba lépés dátuma<sup>2</sup>:** ..... a Szabályzat fedőlapján található

A Szabályzat hivatalos és aktuális verziója a Szolgáltató elektronikus aláírásával ellátva megtalálható és letölthető a Szolgáltató internetes honlapjának következő oldalról:

[https://www.telekom.hu/vallalati-megoldasok/nagyvallalatok/hitelesites\\_szolgáltatások/idobelyegzes\\_szolgáltatás](https://www.telekom.hu/vallalati-megoldasok/nagyvallalatok/hitelesites_szolgáltatások/idobelyegzes_szolgáltatás)

<sup>1</sup> Ez bizonyos technikai korlátozásokat jelent, például megkövetelheti a *bérelt vonali* kommunikációs csatornák vagy egyéb egyedi megoldásokhasználatát.

<sup>2</sup> A Szabályzat aktuális verziójára vonatkozik.

## 1.3 PKI szereplők

A Szolgáltató jelen szabályzatban tárgyalt szolgáltatásaihoz tartozó közösség (a továbbiakban: Közösség) az alábbiakból áll.

### 1.3.1 Időbélyegző szervezet

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

A Szervezet a [timestamp@telekom.hu](mailto: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 visszavonási listák 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:** 1400  
**Postacím:** 1541 Budapest  
**Honlap:** [https://www.telekom.hu/vallalati-megoldasok/nagyvallalatok/hitelesites\\_szolgáltatások/idobelyegzes\\_szolgáltatás](https://www.telekom.hu/vallalati-megoldasok/nagyvallalatok/hitelesites_szolgáltatások/idobelyegzes_szolgáltatás)  
**E-levélcím:** [timestamp@telekom.hu](mailto: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: +36-30-444-1731**

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

### 1.3.2 Előfizetők, érintett felek

A Szolgáltató által nyújtott szolgáltatások végfelhasználói az alábbiak lehetnek:

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

Az **előfizető** olyan tetszőleges természetes vagy jogi személy, vagy jogi személyiséggel nem rendelkező szervezet lehet, aki/amely elfogadja a Szolgáltató szabályzataiban meghatározott kötelezettségeket, és aki (eltérő megállapodás hiányában) fizet a szolgáltatásért.

Az előfizető szerződéses viszonyban áll a Szolgáltatóval a vonatkozó Időbélyegzés Szolgáltatói Szerződésben (továbbiakban: ISzSz) [12], jelen IBSzSz, Magyar Telekom Időbélyegzés-szolgáltatás Általános Szerződési Feltételek (továbbiakban: ÁSZF) [11] és a TSP [13] 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.

A Szolgáltató szabályzatai semmilyen formában sem korlátozzák az érintett felek körét.

### 1.3.3 Egyéb szereplők

Egyéb szereplőként meg kell említeni:

- Magyar Telekom Nyrt. Platform fejlesztési és üzemeltetési ágazat ISP csoportot, mint az időjel ellátó rendszer üzemeltetőjét, aki ezt a tevékenységét az Időbélyegző Szervezet részére végzi
- A Szabályzat szerinti 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](mailto: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](mailto:bekelteto.testulet@bkik.hu)

## 1.4 A Szolgáltatási Szabályzat adminisztrálása

### 1.4.1 Adminisztrációért felelős szervezet és kapcsolattartó személy

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 nyilvános<sup>3</sup> szabályzatok (ÁSZF, Időbélyegzési Rend) el(ő)készít(t)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:** 1097 Budapest, Könyves Kálmán körút 36.

**Telefon:** 1400

**Mobil:** +36 30 444-1731

**e-Mail:** [timestamp@telekom.hu](mailto:timestamp@telekom.hu)

**Postacím:** 1541 Budapest

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

---

<sup>3</sup> A belső szabályozások kezelésével kapcsolatos felelősök külön belső utasításban vannak rögzítve

### 1.4.2 A Szolgáltatási Szabályzat elfogadási eljárása

A szabályozási tevékenységgel megbízott szolgáltatási menedzser összegyűjti a Szabályzatra (vagy az egyéb nyilvános szabályzatra) vonatkozó észrevételeket, illetve változtatási igényeket, majd elkészít(tet)i a módosított szabályzattervezetet. Az így előállított szabályozás változat feladásra kerül a Magyar Telekom Szabályozási környezet véleményezési, jóváhagyási workflow-ba. A szabályozási workflow különböző pontján tett észrevételekkel kiegészített szabályozás változat ismét jóváhagyási workflow-ba kerül, ahol jóváhagyás esetén hatályba lép és a szabályozási környezet részévé válik. Ezt követően a szolgáltatási menedzser eleget tesz a belső és külső (Bizalmi Felügyelet és ügyfelek) tájékoztatási kötelezettségeknek, az 1.4.3 fejezet szerint.

A szabályzatok elrendelése és életbe léptetése a Szolgáltató vezetőinek jóváhagyásával, az erre vonatkozó belső utasítás alapján történik.

Jelen szolgáltatási szabályzat Időbélyegzési Rendnek való megfelelőségét közzététel előtt Szolgáltató megvizsgálta. A vizsgálatot külső független szakértő is elvégzi évente rendszeresen végzett auditja során.

Ezen felül a Szabályzat megfelelőségét a vonatkozó törvények, jogszabályok, valamint szakmai előírások tekintetében a Bizalmi Felügyelet is megvizsgálja a szabályzat nyilvántartásba vételét (illetve hatályba lépését) megelőzően.

### 1.4.3 Szabályzat -változtatási eljárások

Egy időszak alatt összegyűlt változási igényeket Szolgáltató kötegelve szerkeszti új szabályzati változattá, törekedve arra, hogy új szabályzatot csak a lehető legritkábban kelljen kibocsátania.

#### Értesítés nélkül, illetve értesítéssel változtatható elemek

A szabályzatok bármely részének (elemének) módosítása esetén az erről szóló értesítés és tájékoztatás a következő alfejezet szerint történik. Nincsenek olyan elemek, melyeket Szolgáltató értesítés nélkül változtatna meg jelen szabályzatában (illetve nyilvános szabályzataiban).

#### Szabályzati objektum-azonosítót vagy -mutatót változtató módosítások

Jelen szabályzat és az időbélyegzés szolgáltatással kapcsolatos egyéb nyilvános szabályzatok módosított változatai mindig új verziószámmal kerülnek nyilvánosságra. A szabályzatok módosítása a szabályzatok objektum-azonosítóját is módosítja.

A verziószám egy tizedes értékkel növekszik (pl. 1.6-ot követi az 1.7-es), az objektum-azonosítónak pedig az utolsó számjegye növekszik egy értékkel. (pl. 1.3.6.1.4.1.17835.7.1.2.8.2.1.13.3.4 –et követi az 1.3.6.1.4.1.17835.7.1.2.8.2.1.13.3.5).

#### ▪ Közzétételi és tájékoztatási elvek

### A szabályzat közzététele és nyilvántartásba vétele

Szolgáltató nyilvános szabályzatainak a változásokkal egybeszerkesztett új verzióját, annak hatályba lépését megelőzően 30 nappal benyújtja azt a Hatóság részére, nyilvántartásba vétel céljából, ezzel egyidejűleg elhelyezi nyilvános internetes honlapján a szolgáltatás tervezett szabályzat változásai közé.

Amennyiben nem érkezik észrevétel, a szabályzatot a rendszeradminisztrátor szerepét betöltő kolléga, mint hatályos dokumentumot helyezi el nyilvános internetes honlapján, ezzel egyidejűleg a korábbi változatot elhelyezi a „hatályát veszített szabályzatok” közé.

### A szabályzatban nem tárgyalt elemek

A Szolgáltató nyilvános szabályzataiban csak azon eljárásait hozza nyilvánosságra, melyek ismerete a szolgáltatás biztonságát nem veszélyezteti. Szolgáltató több belső biztonsági és egyéb szabályzattal, operatív szintű előírással rendelkezik, melyeket bizalmasan kezel (jelen szolgáltatási szabályzat több ilyen is megemlít). A 8. fejezetben leírt tanúsítási eljárások ezeket a dokumentumokat is vizsgálják.

## 1.5 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 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 | A 2023. évi CIII. törvény 8.§ 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                                                                                                                                                                                                                             |

## 1.6 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.

## 1.7 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] 2023. évi CIII. törvény a digitális államról és a digitális szolgáltatások nyújtásának egyes 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
- [15] ETSI EN 319 401 EU szabvány: General Policy Requirements for Trust Service Providers
- [16] RFC6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP

## 2 Közzétételre és tárolásra vonatkozó felelősségek

A Szolgáltató a szolgáltatói tanúsítványokat – Gyökér hitelesítő és időbélyegző tanúsítványok- valamint a Gyökér hitelesítő visszavonási listáját nyilvánosan elérhető weblapján teszi elérhetővé. ([https://www.telekom.hu/vallalati-megoldasok/nagyvallalatok/hitelesites\\_szolgaltatasok/idobelyegzes\\_szolgaltatas](https://www.telekom.hu/vallalati-megoldasok/nagyvallalatok/hitelesites_szolgaltatasok/idobelyegzes_szolgaltatas))

### 2.1 Adatbázisok

Adatbázisok alatt a Szolgáltató honlapján közzétett adatokat értjük. Itt a szolgáltatásokra vonatkozó kikötéseket, feltételeket, szabályzatokat; valamint a rendkívüli információkat is közzéteszik. A Szolgáltató weboldala **HTTP** lekérdezésekkel érhető el.

A **weboldal** elérhetőségét a Szolgáltató folyamatosan (az év minden napján, **0-24 óra** között) biztosítja, a karbantartáshoz szükséges idők kivételével. A Szolgáltató a tervezett karbantartásokat munkaidőn kívüli időszakokra ütemezi, és ezekről a karbantartás megelőzően **24 órával** értesítést tesz közzé a honlapján.

### 2.2 Az időbélyegzőkre vonatkozó információk közzététele

#### Kikötések és feltételek közzététele

A Szolgáltató szerződéses feltételeit és szabályzatait – és ezek részeként az időbélyegzésre vonatkozó információkat - elektronikus formában (MS-Word és/vagy Adobe Acrobat formátumokban) hozza nyilvánosságra az internetes honlapjának oldalain.

Elérhetőség [https://www.telekom.hu/vallalati-megoldasok/nagyvallalatok/hitelesites\\_szolgaltatasok/idobelyegzes\\_szolgaltatas](https://www.telekom.hu/vallalati-megoldasok/nagyvallalatok/hitelesites_szolgaltatasok/idobelyegzes_szolgaltatas)

A dokumentumok korábban érvényben lévő változatai is megtalálhatóak itt az aktuális verziók mellett. A dokumentumok nyomtatott változatai semmilyen formában sem tekinthetők hivatalos példánynak vagy hiteles másolatnak.

#### Rendkívüli információk közzététele

A Szolgáltató a következő eseményekről hirdetést jelentethet meg egy országos terjesztésű napilapban:

- új szolgáltatás beindítása,
- valamely szolgáltatás tervezett beszüntetése vagy tartós (**24 órát** meghaladó) szüneteltetése,
- tevékenységének befejezése, ld. még 5.10 fejezetet.

#### Tanúsítványok nyilvánosságra hozatala

A Szolgáltató az általa működtetett időbélyegző egységek tanúsítványait a következő módszerekkel teszi közzé:

- Az időbélyegzőt aláíró kulcsok tanúsítványát és a rá vonatkozó – Magyar Telekom Gyökér Hitelesítő által kiadott - tanúsítvány visszavonási listát a honlapján keresztül teszi közzé.

### **A tanúsítványok visszavonásának és felfüggesztésének nyilvánosságra hozatala**

A Szolgáltató az általa működtetett Időbélyegző egységek tanúsítványaival kapcsolatos állapot-információkat a következő módszerrel teszi közzé:

- Az Időbélyegző egységek tanúsítványainak állapotváltozását a Szolgáltató weboldalán hozza nyilvánosságra.

## **2.3 A közzététel gyakorisága**

### **Kikötések és feltételek közzétételi gyakorisága**

A Szabályzattal kapcsolatos új verziók közzététele az 1.4.3 alfejezetben ismertetett eljárásoknak megfelelően történik.

A Szolgáltató szükség szerinti gyakorisággal bocsátja ki az egyéb szabályzatait és szerződéses feltételeit, illetve az újabb változatokat.

### **Rendkívüli információk közzétételi gyakorisága**

A Szolgáltató a rendkívüli információkat közzéteszi a jogszabályi előírásoknak megfelelően, illetve ennek hiányában akkor, amikor arra szükség van.

## **2.4 Az adatbázisok elérésének szabályozása**

A Szolgáltató által közzétett kikötések és feltételek, a rendkívüli események, az időbélyegző egység tanúsítványok és állapot információk nyilvános információk. Olvasás illetve lekérdezés céljából bárki korlátozás nélkül elérheti ezeket az információkat, a közzététel sajátosságainak megfelelően, Interneten keresztül.

A Szolgáltató által közölt információkat kizárólag csak a Szolgáltató egészítheti ki, törölheti vagy módosíthatja. A Szolgáltató különböző védelmi mechanizmusokat működtet az információk jogosulatlan módosításának megakadályozására.



## **3 Azonosítás és hitelesítés**

### **3.1 Megnevezési konvenciók**

#### **3.1.1 Márkanevek elismerése, azonosításuk és szerepük**

A Szolgáltató a szolgáltatása során bejegyzett védjegyet nem alkalmaz.

## 4 Működésre vonatkozó követelmények – időbélyegzés

A Szolgáltató minősített időbélyegzés szolgáltatást jelen szabályzat előírásai alapján nyújt.

### 4.1 Időbélyegzés szolgáltatás igénylése

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.

Amennyiben az igényelő kéri, a szolgáltatás nyilvános dokumentumainak helyszíni tanulmányozására is lehetősége van, valamint szóban történő tájékoztatást is kaphat a szolgáltatással kapcsolatban.

Az Időbélyegzés Szolgáltatási Szerződés és Megrendelőlap valamint a Szolgáltató szabályzatai és termékismertetői megtalálhatók a Szolgáltató honlapján is, így előzetesen is áttekinthetők és kitölthetők.

A szolgáltatási szerződés ezt követő aláírásával születik meg szolgáltató és igénylő között az előfizetői szerződés, az Általános Szerződési Feltételek (ÁSZF) rendelkezéseinek megfelelően.

Az igénylő aláírásával egyúttal nyilatkozik arról is, hogy Szolgáltató feltételei és kikötései, saját kötelezettségei vonatkozásában tájékoztatást kapott, azokat elfogadja.

Az **Időbélyegzés Szolgáltatási Szerződés és Megrendelőlap tartalma** ezt követően Szolgáltató nyilvántartásába kerül mind elektronikus, mind papír formában.

Minősített időbélyeg-szolgáltatást természetes személy, vagy szervezet egyaránt igényelhet, személyesen a Szolgáltató székhelyén (Ld:1.3.1), telefonon, e-mail-ben, levélben.

Az igénybevételre két módon kerülhet sor:

- a Szolgáltatóval történő eseti megállapodás, vagy
- a Szolgáltató által nyújtott ajánlatok, csomagok elfogadott megrendelése keretében.

Az igénylés Szolgáltatóhoz való beérkezésétől számított 15 napon belül a Szolgáltató felveszi a kapcsolatot az igénylővel, s az ajánlatot elfogadja, az igénylőt felszólítja hiánypótlásra, pontosításra, vagy a Szolgáltató döntése szerint az ajánlatot visszautasítja, amennyiben az Igénylő a hiánypótlási, pontosítási felszólításnak 15 napon belül nem tesz eleget, a Szolgáltatóval szemben a Szolgáltatás korábbi igénybevételéből eredően díjtartozása van, vagy amennyiben a szolgáltatás nyújtásával más ügyfelek kiszolgálása veszélybe kerül.

## 4.2 Az időbélyegzés szolgáltatás teljesítése

Szolgáltató az RFC 3161 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.

Az időbélyegző szolgáltatás geo-redundánsan lett kialakítva, a terhelés egyenletes elosztásért, és a folyamatos akadálymentes kiszolgálásért a hálózati HA megoldás felel. A rendszer terheltségének a figyelése a rendszerüzemeltetők feladata.

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.

Felhasználó vállalja a szolgáltatási díjak megfizetését, valamint elfogadja, hogy a szolgáltatás díjának megfizetését nem tagadhatja meg arra való hivatkozással, hogy érdekkörébe tartozó területen és eszközökön keresztül jogosulatlan személy vette igénybe a jelen szerződés tárgyát képező szolgáltatást.

## 4.3 Minősített Időbélyegzés-szolgáltatás joghatása

Az [1] EU rendelet alapján, „Az elektronikus időbélyegző joghatása és bírósági eljárásokban bizonyítékként való elfogadhatósága nem tagadható meg kizárólag amiatt, hogy az elektronikus formátumú, illetve nem felel meg a minősített elektronikus időbélyegzőkre vonatkozó követelményeknek. A minősített elektronikus időbélyegző esetében vélelmezni kell az általa feltüntetett dátum és időpont pontosságát, valamint az adott dátumhoz és időponthoz kapcsolt adatok sértetlenségét.”.

## 4.4 Az időbélyegzés szolgáltatás igénybevételének vége

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

## 5 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.

### 5.1 Fizikai előírások

Szolgáltató gondoskodik arról, hogy a kritikus szolgáltatásokhoz történő fizikai hozzáférés ellenőrzött legyen, és a kritikus szolgáltatások nyújtásához szükséges eszközök használatából eredő kockázatot minimalizálják.

A fizikai óvintézkedések célja a Szolgáltató információira és fizikai körleteire irányuló jogosulatlan hozzáférés, károkozás és illetéktelen behatolás megakadályozása.

A biztosított védelem arányban áll a Szolgáltató által végzett kockázat elemzésben megállapított kockázatokkal.

A leginkább veszélyeztetett szolgáltatásokat az Időbélyegző Szervezet védett számítógép termeiben valósítják meg. Ezek a számítógép termék speciálisan erre a célra lettek tervezve és kialakítva, és tervezésénél több különböző védelmi szempont (a telephely elhelyezése és szerkezeti felépítése, a fizikai hozzáférés /beléptetés ellenőrzése és felügyelete/, áramellátás, légkondicionálás, beázás és elárasztódás elleni védekezés, tűzmegelőzés és tűzvédelem, adathordozók tárolása, stb.) érvényesítésére is sor került.

Az Időbélyegző Szervezet valamennyi kritikus szolgáltatását biztonsági körletben valósítja meg, és az ehhez szükséges valamennyi eszközt a biztonsági körletek részét képező védett számítógép termekben helyezte el. A termék túlmelegedés elleni védelmére kialakításra kerül helyiségenként elektromos hőérzékelő berendezés mely a kritikus hőmérséklet elérése előtt riasztási jelzést továbbít a létesítmény épület-felügyeleti rendszeréhez. A helyiségekben gyengeáramú szükség-megvilágítás került telepítésre mely egyben a menekülési útvonalat is jelöli. A padló burkolata csúszásmentes, antistatikus és terhelő nyomásnak ellenálló.

Az Időbélyegző Szervezet számítógép terme önálló biztonsági körletnek minősül. Ezen belül valósulnak meg a kritikus szolgáltatások, és itt került elhelyezésre az ezekhez szükséges valamennyi eszköz.

#### 5.1.1 A telephely elhelyezése és szerkezeti felépítése

Az Időbélyegző Szervezet védett számítógép terme a befogadó épület területén elkülönítetten került kialakításra. Az elkülönített biztonsági körlet három egymásba nyíló, összesen egy bejárattal rendelkező ablaktalan helyiségből áll, melyben elhelyezésre kerültek a számítógépszerverek és az üzemeltetésükhöz szükséges teljes infrastruktúra.

### 5.1.2 Fizikai hozzáférés

Az Időbélyegző Szervezet védett számítógép terme úgy lett kialakítva, hogy illetéktelen személyek egyáltalán ne juthassanak be, a biztonsági őrség viszont rövid idő alatt meg tudja közelíteni riasztás esetén. A biztonsági körletnek nincs ablaka, a bejárat ajtón kívül csak falbontással lehet behatolni ide. A biztonsági körlet integráltan megvalósított behatolás jelző (riasztó) és beléptető (kártyaolvasó) rendszerrel van ellátva. A biztonság növelése érdekében egy falbontás érzékelő riasztó rendszer került telepítésre és beüzemelésre.

A védett számítógép termekbe az ott dolgozó bizalmi munkakört betöltő munkatársakon kívül más személyek (pl. karbantartók, takarítók) csak külön felhatalmazással és kísérettel léphetnek be.

A védett számítógép termekbe történő belépések minden esetben naplózásra kerülnek.

### 5.1.3 Áramellátás, légkondicionálás

#### Áramellátás

Az Időbélyegző Szervezet védett számítógép termeinek zavartalan áramellátása kiemelten fontos a folyamatos üzemeltetés biztosítása érdekében. A helyiségek betáplálására 3x60 amper tápellátás áll rendelkezésre, fáziselosztással, bemeneti zavaroszűrővel és érintésvédelemmel.

A következő védelmi megoldások együttese biztosított:

- szünetmentes központi energia ellátás (épület szünetmentes egység)
- szünetmentes energia ellátás a rack szekrénybe szerelt UPS-egységek által,
- villamos zavar, villám és túlfeszültség védelem,

Az alkalmazott üzemmód pedig az alábbi:

- az üzemi táp kimaradása vagy csökkenése esetén a rendszer átkapcsol a tartalék tápra,
- ha a tartalék táp sem használható, akkor a rendszer fokozatosan leállítja a szervereket,

Zárlati leoldásra szelektív áramkörök segítségével a gépteremben több egymástól független működésű rendszer lett kialakítva a folyamatos üzemeltetés támogatására. A villamos zavar, villám és túlfeszültség védelem szempontjából a gépterem nagy értékű, kritikus szolgáltatásokat biztosító berendezései védve vannak a különböző vezetett és sugárzott villamos zavarok, villámok miatt bekövetkező túlfeszültség hatásai ellen:

- a rendszert külön mechanizmusok védik a villámok által keltett elektromágneses impulzusok (EMI) hatása ellen,

- az üzemeltetett berendezések a sugárzott elektromágneses zavarás elleni védelem mindkét elvárását teljesítik: egyrészt védettek az üzemelési környezetükben jelen levő hatások ellen, másrészt nem bocsátanak ki olyan zavaró elektromágneses jeleket, amely a környezetükben üzemelő többi berendezés működését zavarhatná.

Külön akkumulátoros **szünetmentes tápegységek** biztosítják az alábbi berendezések áramellátását áramszünet esetén:

- tűzjelző berendezés (**24 óras** üzemképességgel teljes áramszünet esetén),
- telefonközpont (**6 óras** áramszüneti üzemképességgel).

### Légkondicionálás

Az Időbélyegző Szervezet védett számítógép terme hűtésigényének kiszolgálását helyiségenkénti levegő hűtését egy ipari klíma illetve 1 db tartalékként létesített split klíma biztosítja..

## 5.1.4 Beázás és elárasztás veszélyeztetettsége

Az Időbélyegző Szervezet biztonsági körleteinek kialakítása során figyelembe vették az elárasztás veszélyének minimalizálását. A biztonsági körletek teljes területe mentes a vizesblokkoktól, illetve a közelben nincs sem csatorna, sem vízvezeték. A biztonság növelése érdekében egy nedvességérzékelő riasztó rendszer került telepítésre és beüzemelésre.

## 5.1.5 Tűz megelőzés és tűzvédelem

Az Időbélyegző Szervezet géptermét befogadó épületben a helyiségek védelmére kiépített automata tűzvédelmi rendszer működik.

A helyiségek tűzvédelmét egy tűzjelző és oltóközpont biztosítja. A tűzvédelmi jelzések az épület felügyeleti rendszerre kerültek beintegrálásra, mely a jelzéseket a Magyar Telekom Nyrt. **24 óras** diszpécsterszolgálatához továbbítja, ahol a szükséges intézkedéseket megteszik. Tűzriasztás esetén az épület-felügyeleti rendszer a légbefújást automatikusan leállítja.

A helyiségek bejáratát tűzgátló ajtó választja el a létesítménytől, így a kialakított termek önálló tűzszakaszt képeznek.

A kiépített tűzvédelmi rendszert (melynek fő elemei: füstérzékelő- és tűzjelző rendszerek, oltókapszulák) az illetékes tűzoltó parancsnokság engedélyezte, rendszeres felülvizsgálatuk biztosított.

### 5.1.6 Adathordozók tárolása

Az Időbélyegző Szervezet biztonsági körletében egy kódzáras tűzbiztos szekrény szolgál az adathordozók biztonságos tárolására. A szekrényben az Időbélyegző Szervezet mentési példányait tárolják {ld. 5.1.8 A mentési példányok fizikai elkülönítése}. Itt kerülnek elhelyezésre adminisztrálásához, üzemeltetéséhez szükséges adathordozók, ill. az üzemeltetési dokumentációk elektronikus formában.

### 5.1.7 Hulladék megsemmisítése és selejtezés

Az Időbélyegző Szervezet biztonsági körleteiben a bizalmas minősítésű adatokat tartalmazó elektronikus adathordozókat, még tartalmuk törlése után sem használják fel nem minősített adatok tárolására. A feleslegessé vált, bizalmas minősítésű adatokat tartalmazó adathordozókat fizikailag megsemmisítik:

- a papíralapú dokumentumokat zúzógéppel felaprítják,
- a hajlékony lemezeket (házából való kibontás után) zúzógéppel felaprítják,
- a merev lemezeket (a befogadó épületben központilag biztosított célberendezés felhasználásával) demagnetizálás után fizikailag összetörik.

### 5.1.8 A mentési példányok fizikai elkülönítése

Az Időbélyegző Szervezet biztonság-kritikus szolgáltatásaira vonatkozó adatok mentési példányait az Időbélyegző Szervezet biztonsági körletében és a Magyar Telekom Központi Katasztrófa Adattárában (a továbbiakban: megőrzési hely) tárolják.

### 5.1.9 Hálózati redundancia

A Magyar Telekom Nyrt. törekszik mindig a geo-redundáns hálózat kialakítására, kiváltképp a kritikus szolgáltatások esetén. Erre a 739-es utasítás (ÜZLETMENET-FOLYTONOSSÁG IRÁNYÍTÁSA) és a 1352-es utasításra (HÁLÓZAT TECHNOLÓGIAI KATASZTRÓFA-ELHÁRÍTÁS) íté ki. Az időbélyeg szolgáltatás esetén a hálózati megvalósítást a topológia ábrák prezentálják.

## 5.2 Eljárásbeli óvintézkedések

Az eljárásbeli óvintézkedések célja, hogy a bizalmi munkakörök kijelölésével és elkülönítésével, az egyes munkakörök felelősségének dokumentálásával, az egyes feladatokhoz szükséges személyzeti létszámok, valamint az egyes munkakörökben elvárt azonosítás és hitelesítés meghatározásával Szolgáltató kiegészítse, egyúttal fokozza a fizikai és személyzetre vonatkozó óvintézkedések hatásosságát.

### 5.2.1 Bizalmi munkakörök

Szolgáltató a 24/2016 (VI.30.) BM rendelet 2§ 1. pontja alapján következő bizalmi munkaköröket határozza meg az alábbi felelősségkörökkel:

- szolgáltató informatikai rendszeréért általánosan felelős vezető.
- biztonsági tisztviselő,
- rendszeradminisztrátor,
- rendszerüzemeltető,
- független rendszervizsgáló,

A **Szolgáltatóval munkaviszonyban** álló, változó helyszínen dolgozó **biztonsági tisztviselő** a szolgáltatás biztonságáért általánosan felelős személy munkaköre. Felelős:

- a különböző biztonsági óvintézkedések kidolgozásáért,
- a különböző biztonsági óvintézkedések rendszeres felülvizsgálatáért, a szükségessé váló módosítások kezdeményezéséért,
- a biztonsági óvintézkedések érvényre jutásáért, betartatásáért,
- az informatikai rendszerek biztonsági szintjének megőrzéséért (rendszeres auditok szervezésével).

Az **Időbélyegző Szervezettel munkaviszonyban** álló, változó helyszínen dolgozó **biztonsági tisztviselő** közreműködik (egy másik, bizalmi munkakört betöltő társa jelenlétében) az alábbi tevékenységeknél:

- a Szolgáltató időbélyegző szerver kulcsainak generálásánál,
- a Szolgáltató időbélyegző szerver kulcsainak megsemmisítésénél,

Az **Időbélyegző Szervezettel munkaviszonyban** álló **rendszeradminisztrátorok**:

- telepítik, konfigurálják és karbantartják az Időbélyegző Szervezet védett számítógép termében üzemeltetett megbízható rendszereket,
- beállítják a fenti megbízható rendszerek kezdeti hálózati konfigurációját,
- kezelik az Időbélyegző Szervezet állományába tartozó rendszeroperátorok vonatkozásában a rendszerhez való hozzáféréseket (account felvétele, jogosultságok beállítása, módosítása, kezdeti jelszó beállítása, a távozó, illetve munkakört váltó rendszeroperátorok hozzáférési jogainak azonnali megszüntetése),
- letöltik és installálják a felügyeletük alatt üzemeltetett operációs rendszerre és adatbázisra kiadott biztonsági javítócsomagokat, ezen keresztül gondoskodnak az informatika biztonsági szint folyamatos megőrzéséről,

- rendszeres időnként ellenőrzik az Időbélyegző Szervezet védett géptermeiben üzemeltetett informatikai rendszernek és információinak a sértetlenségét,
- elvégzik az Időbélyegző Szervezet védett számítógép termében üzemeltetett megbízható rendszer hálózati konfigurációjának kezdeti beállítását,
- ellenőrzik (áttekintik és kiértékelik) és karbantartják (archiválják és törlik) az általuk felügyelt tűzfalak, behatolást detektáló rendszerek biztonsági naplóját,
- közreműködik az időbélyegző tanúsítványok generálásánál,
- gondoskodik a tűzfalakra, behatolást detektáló rendszerekre kiadott biztonsági javítócsomagok letöltéséről, installálásáról, ezen keresztül a biztonsági szint naprakész megőrzéséről.
- szükség esetén helyreállításokat hajtanak végre.

Az **Időbélyegző Szervezettel munkaviszonyban álló rendszerüzemeltetők** folyamatosan üzemeltetik az Időbélyegző Szervezet védett számítógép termében működő megbízható rendszereket, melynek során:

- közreműködik az időbélyegző tanúsítványok generálásánál,
- tanúsítványokat generál(tat)nak az Időbélyegző Szervezet számára,
- negyedévente archiválást végeznek,
- mentéseket készítenek és gondoskodik a rendszermentések, illetve az Időbélyegző Szervezet rendszermentés másolatainak biztonságos tárolásáról,
- gondoskodik a rendszermentésekről készített, elkülönítetten őrzendő másolati példányok megőrzési helyre történő szállításáról {ld. **5.1.8 A mentési példányok fizikai elkülönítése**} ,
- szükség esetén helyreállításokat hajtanak végre.

A Szolgáltatóval munkaviszonyban álló független **rendszerüzemeltetők**:

- ellenőrzik (áttekintik) és karbantartja (archiválja és törli) az Időbélyegző Szervezet védett számítógép termében működő megbízható rendszer biztonsági naplóját,
- szükség esetén az általuk készített archívumokban keresést végeznek.

Valamennyi fent megnevezett bizalmi munkakört a munkaköri leírások dokumentálják.

A bizalmi munkakörökbe az Adatgazda nevezi ki Szolgáltató munkatársait, a biztonsági alapellenőrzés sikeres befejezése után {ld. **5.3.1 pont**}.

**Regisztrációs feleős** pozíciót a minősített időbélyeg szolgáltatásban nem szükséges és nem tölt be senki.

### 5.2.2 Az egyes feladatokhoz szükséges személyzeti létszámok

Általánosan teljesül a Szolgáltató egészére, hogy minden munkatárs csak a saját munkakörének megfelelő funkciókat aktivizálja.

Az Időbélyegző Szervezetnél az alábbi kettős felügyeletet igénylő **munkafolyamatok** vannak, amelyhez két bizalmi munkakört betöltő személy együttes jelenléte (és előzetes, sikeres hitelesítése) szükséges:

- a Szolgáltató időbélyegző szerver kulcsainak generálásánál,
- a Szolgáltató időbélyegző szerver kulcsainak megsemmisítésénél,
- a Szolgáltató Gyökér Hitelesítő Egységének üzembe helyezése, tanúsítvány kiadása, visszavonása, visszavonási listák kiadása
- a Szolgáltató TrustedTimeStamp szerverei HSM-jében használt nyilvános kulcsait tartalmazó **adathordozóknak** a Gyökér Hitelesítő Egységhez való továbbításánál, illetve az erre, a Gyökér Hitelesítő Egység által kibocsátott tanúsítvány visszaszállításánál. (megjegyzés: a szerverből két példány van, két külön HSM modulal).

Szolgáltató vonatkozó belső szabályzata meghatározza az egyes feladatokhoz szükséges személyzeti létszámokat is.

### 5.2.3 Az egyes munkakörökben elvárt azonosítás és hitelesítés

Az Időbélyegző Szervezet valamennyi bizalmi munkakört betöltő munkatársának azonosítása és hitelesítése a Magyar Telekom hatályos szabályzataiban rögzített eljárásokkal történik. Sikeres hitelesítés előtt egyetlen biztonság kritikus tevékenységet sem lehet végrehajtani.

### 5.2.4 Egymást kizáró munkakörök

Szolgáltató gyakorlatában a bizalmi munkakörök között **személyi átfedések nincsenek**, minden személy csak egy bizalmi munkakört tölt be, az erre vonatkozó jogszabályi<sup>4</sup> előírásoknak megfelelően. A kialakított és működtetett helyettesítési rend biztosítja a jogszabályban rögzített összeférhetetlenségi előírások betartását.

---

<sup>4</sup> 24/2016. (VI. 30.) BM rendelet

## 5.3 Személyzetre vonatkozó előírások

A személyzetre vonatkozó óvintézkedések célja az emberi hibák, lopás, csalás és a lehetőségekkel való visszaélés kockázatának csökkentése.

Ennek érdekében Szolgáltató külön a személyzetre vonatkozó belső előírással rendelkezik, és ezek szerint jár el, így a személyi biztonsággal már a felvételi szakaszban foglalkozik, beleértve a szerződések megkötését, illetve azok alkalmazás során történő ellenőrzését.

Valamennyi bizalmi munkakör esetén a felvételre jelentkezőket biztonsági ellenőrzésnek vetik alá. Minden bizalmi munkakört betöltő alkalmazottnak és külső félnek, akik Szolgáltató szolgáltatásaival kapcsolatba kerülnek, titoktartási nyilatkozatot kell aláírni.

Szolgáltató egyúttal biztosítja a valamennyi munkakör betöltéséhez szükséges közös, általános, illetve az egyes munkakörök betöltéséhez szükséges speciális szakmai ismereteket megszerzését, illetve továbbfejlesztését.

Ennek érdekében Szolgáltató egy két lépcsős (tájékoztatás + továbbképzés) képzési rendszert valósít meg:

- a tájékoztatás valamennyi, a Szolgáltató szolgáltatásaival és az érintett informatikai rendszerével kapcsolatba kerülő munkatárs számára egységes {ld. 5.3.3 pont},
- a továbbképzés moduláris, és az egyes bizalmi munkakörök szerint eltérő felépítésű tananyag szerint történik, a személyre szóló éves továbbképzési terveknek megfelelően {ld. 5.3.4 pont}.

### 5.3.1 Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

Az Időbélyegző Szervezet minden bizalmi munkakörére jelölt személyének (emberi megbízhatóságuk és szakmai alkalmasságuk ellenőrzése céljából) egy kezdeti ellenőrzésen (biztonsági alapellenőrzésen) kell keresztülmennie.

A biztonsági alapellenőrzés során az ellenőrzést végző szakemberek, az életrajzban megadott adatokat (életrajzi elemek, referenciák, szakmai előmenetel, stb.) ellenőrzik. Ennek során:

- a képzettségre vonatkozó adatokat egybevetik a jelölt által benyújtandó bizonyítványokkal, diplomákkal,
- a gyakorlati tapasztalatra vonatkozó állításokat személyes referenciákon keresztül, publikációkra alapozva, illetve egyéb úton igazolják.

A bizalmi munkakört betöltő (vagy arra jelölt) személyek és a vezető tisztségviselők esetén büntetlen előélet igazolása (hatósági erkölcsi bizonyítvány beszerzése és bemutatása) is szükséges.

Az egyes bizalmi munkakörök betöltéséhez szükséges képzettség és gyakorlat a következő.

- Informatikai rendszerért általánosan felelős vezető:

- szakirányú felsőfokú végzettség, valamint
- legalább három év informatika biztonsággal összefüggésben szerzett szakmai gyakorlat.

- biztonsági tisztviselő, rendszeradminisztrátor, rendszervizsgáló, rendszerüzemeltető:

- középfokú szakirányú végzettség vagy szakképesítés és legalább öt év informatika biztonsággal összefüggésben szerzett szakmai gyakorlat, vagy
- szakirányú felsőfokú végzettség vagy felsőfokú szakképesítés és legalább három év informatika biztonsággal összefüggésben szerzett szakmai gyakorlat.

Az informatika biztonsággal kapcsolatos valamennyi bizalmi munkakört<sup>5</sup> betöltő munkatársra nézve továbbképzési terv készül, melyet évente áttekintenek (egyúttal az időközben elvégzett továbbképzési, oktatási anyagokkal kiegészítene), illetve az adott munkakörhöz tartozó szakmai ismeretek megújulása, változása függvényében aktualizálnak.

A munkakör betöltését ellenőrzést követően az illetékes vezető hagyja jóvá.<sup>F</sup>

### 5.3.2 Előélet vizsgálatára és biztonsági háttér ellenőrzésekre vonatkozó eljárások

Valamennyi bizalmi munkakört betöltő munkatárs biztonsági alapellenőrzésen esik túl {ld. 5.3.1}, emellett mindenkinek időszakos biztonsági ellenőrzéseken is át kell esniük.

Nem tölthet be bizalmi munkakört az a személy, aki akár az alap, akár egy időszakos biztonsági ellenőrzésen a “elfogadhatatlanul nagy biztonsági kockázat” minősítést kapja<sup>6</sup>.

Az időszakos biztonsági ellenőrzésre rendszeres időnként kerül sor:

- a biztonsági tisztviselők esetében **3 évente**,
- egyéb bizalmi munkakörök esetében **5 évente**.

---

<sup>5</sup>

<sup>6</sup> Ilyen esetekben Szolgáltató gondoskodik a megfelelő személy kijelöléséről.

Az ellenőrzés során vizsgálják a munkatárs erkölcsi bizonyítványát és olyan körülményeket, melyek kockázati tényezőt jelentenek. E mellett figyelembe veszik a közvetlen vezetők véleményét is. A megtekintett erkölcsi bizonyítványok igénylését, sorszámát az ellenőrzést végző kolléga rögzíti és megőrzi későbbi visszaellenőrizhetőség érdekében. Az ellenőrzés megtörténtéről aláírt jegyzőkönyv készül mely az erkölcsi bizonyítvány szemrevételezésének dátumát és az érintettek aláírását is tartalmazza.

### 5.3.3 Kiképzési követelmények

Az Időbélyegző Szervezet területén dolgozó valamennyi munkatárs felvételét követően, a saját munkakörének betöltéséhez szükséges elméleti és gyakorlati alapkiképzésben vesz részt.

Valamennyi munkakörbe való végleges kinevezésnek feltétele az alapkiképzésen való részvétel, s az ezt követő írásos teszten legalább “megfelelő” eredmény elérése.

Szolgáltató belső utasításában részletesen szabályozott a bizalmi szerepkörbe történő beléptetést megelőző alapfelkészítés, kinevezés.

Rendszerüzemeltetői munkakörben kinevezett (véglegesített) munkatárs a kinevezést követő **két hétig** megfelelő gyakorlattal rendelkező kollégával közösen van beosztva (nem lehetséges, hogy a két egyszerre szolgálatban lévő rendszeroperátor mindegyike az adott munkahelyen kezdő). ). A két hét eltelte után a kinevezett rendszerüzemeltető ellátja a mindenkori rendszerüzemeltetői feladatokat.

### 5.3.4 Továbbképzési gyakoriságok és követelmények

Minden bizalmi munkakört betöltő munkatárs esetében továbbképzési terv készül. (Ez tartalmazza az arra az évre beütemezett szervezett belső továbbképzéseket, illetve külső tanfolyamokon, egyéb továbbtanulási formákban való ismeretszerzést.) A személyes továbbképzési tervet a humánpolitikai részleg bevonásával, a közvetlen vezető évente áttekinti, értékeli és (az érintett munkatárs beleegyezésével) aktualizálja.

Abban az esetben, amikor az időbélyegzés szolgáltatásban jelentős változás következik be, valamennyi munkatárs, az őt érintő mélységben továbbképzésben részesül, illetve megkapja a számára szükséges dokumentációkat.

Kiseb változások bekövetkezése előtt a munkatársak írásos tájékoztatást kapnak a változásokról.

### 5.3.5 Munkabeosztás körforgásának gyakorisága és sorrendje

Körforgás az egyes munkabeosztások között a Szervezet nem tervez.

### 5.3.6 A felhatalmazás nélküli tevékenységek büntető következményei

Valamennyi bizalmi munkakört betöltő munkatárs esetén, a munkakörbe kinevezéskor a foglalkoztatási dokumentumok részeként

- írásos tájékoztatást kapott jogszabályi kötelezettségeiről, jogairól, a személyes adatai kezelésére vonatkozó minősítési és kezelési szabályokról,
- munkaköri leírást kapott, mely tartalmazta az őt érintő biztonsági feladatokat,
- titoktartási nyilatkozatot írt alá, melyben a biztonsági intézkedések be nem tartásával járó, őt érintő következmények (büntető szankciók) is megfogalmazódtak.

Mindezek tartalmazzák azokat a munkajogi vagy büntető következményeket, melyek a különböző fegyelem- munkaköri kötelezettség- illetve törvénytiszteltetési szankcionálják.

Amennyiben egy munkatárs (gondatlanságból fakadóan vagy szándékosan) megsérti a fenti szabályokat, ellene büntető intézkedéseket hoznak (melyek az elkövetés módjától és következményétől függően a jutalom megvonástól fegyelmi eljárás indításán és kártérítésen át, egészen a hatósági feljelentésig terjedhet).

### 5.3.7 A szerződéses alkalmazottakra vonatkozó követelmények

Szolgáltató bizalmi munkakörben csak vele (vagy az Időbélyegző Szervezettel) munkaviszonyban álló személyt alkalmaz.

Szolgáltató az egyéb feladatok ellátására, alvállalkozói vagy megbízásos szerződésben foglalkoztatott szerződő személyeket (külső munkavállalókat és ideiglenes alkalmazottakat egyaránt) csak az "ellenőrzött beszállítók" listájáról választ. Az ellenőrzött beszállítókkal az Időbélyegző Szervezet előzetesen írásos megállapodást köt, melyben vállalta Szolgáltató **biztonságpolitikájának** elfogadását.

Valamennyi szerződő fél – még a tényleges munkavégzés megkezdése előtt – titoktartási nyilatkozatot ír alá, melyben vállalja, hogy a munkavégzés során későbbiekben megismerendő üzleti/vállalati titkokat illetéktelen személynek fel nem fedi, s egyéb módon sem hasznosítja. A titoktartási nyilatkozat záró része tartalmazza a megszegése esetén alkalmazandó szankciókat is.

A külső munkavállalók és ideiglenes alkalmazottak szakmai kiképzésben nem részesülnek, erre nem kötelezettek<sup>7</sup>.

### 5.3.8 Kinevezési eljárás

A kinevezés eljárás előfeltétele a szükséges tudás elsajátítása, próbaidő lejárt. A kinevezési eljárás végén a kinevezésről jegyzőkönyvet kell felvenni, amit a kinevezett alkalmazott és a biztonsági tisztviselő ír alá. A jegyzőkönyvet meg kell őrizni.

### 5.3.9 A személyzet számára biztosított dokumentációk

Minden bizalmi munkakört betöltő munkatárs megkapja a következő dokumentumokat:

- a **kinevezési** eljárás, illetve az alapkiképzés során:
  - Szolgáltató szervezeti „Biztonsági kódex”,
  - aláírt titoktartási nyilatkozat,
  - egyéni munkaköri leírás.
- a tervezett és rendkívüli **továbbképzések** alkalmával:
  - az adott oktatási formához tartozó oktatási segédanyagok.
- egyéb esetekben:
  - személyes továbbképzési terv (évenkénti aktualizálása után),
  - a munkavégzést érintő kisebb változások leírása (a változások előtt),
  - módosított biztonsági politika (a bekövetkező változások előtt).

A szervezeti biztonságpolitikában bekövetkező változásokról írásos értesítők formájában mindenki tájékoztatást kap {ld. **5.3.4** Továbbképzési gyakoriságok és követelmények} az említett továbbképzés előtt.

## 5.4 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.

---

<sup>7</sup> A külső munkavállalókat eleve úgy választják meg, hogy az adott munkafeladathoz minden szakmai ismerettel és gyakorlattal rendelkezzenek. Az ideiglenes alkalmazottak olyan jellegű munkát végeznek, melyhez nincs szükség ki- és továbbképzésre.

A naplóbejegyzésben rögzíteni kell az esemény követhetőségéhez, rekonstruálásához szükséges adatokat és az eseményt előidéző felhasználó vagy más személy adatait.

#### 5.4.1 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

#### 5.4.2 A napló állomány feldolgozásának gyakorisága

Szolgáltató naplóbejegyzéseinek átvizsgálása különböző gyakorisággal, belső üzemeltetési utasításban rögzített rendszerességgel megtörténik. Szolgáltató hálózati védelmi riasztás funkciókkal is rendelkeznek az erőforrásokhoz történő jogosulatlan hozzáférés észlelésének jelzésére. Ilyen riasztási esetekben a naplóbejegyzéseket soron kívül átvizsgálják. Rendellenességek észleléskor, reklamáció esetén, vagy egyéb megkeresések kapcsán szintén sor kerülhet a napló adatok rendkívüli átvizsgálására.

#### 5.4.3 A napló-állomány megőrzési időtartama

A napló-állományokat 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.

Az archiv adathordozókat tűzbiztos pécélszekrényben, illetve a Magyar Telekom katasztrófa adattár helyiségében őrizzük meg.

#### 5.4.4 A napló állomány védelme

A napló állományt a véletlen és szándékos rongálások ellen **biztonsági mentések** védik (ld. 5.4.5 pont). A személyes adatokat tartalmazó naplóbejegyzések esetében Szolgáltató gondoskodik az adatok bizalmas tárolásáról. A napló állományokhoz való hozzáférésre csak azok jogosultak, akiknek erre munkakörük folytán szükségük van. Szolgáltató a hozzáféréseket biztonságos módon ellenőrzi.

Szolgáltató a keletkezett naplóadatok védelme érdekében helyi és valós idejű központi naplógyűjtést is végez. A központi naplógyűjtő hozzáférés szabályozása garantálja a naplóadatok sértetlenségét.

#### 5.4.5 A napló állomány mentési folyamatai

A naplóállományokat a rendszerszervizsgáló negyedévente archiválja egyszer írható médiára aláírt formában. A mentési médiák a Magyar Telekom Központi Katasztrófa Adattárában kerülnek megőrzésre.

A mentések operatív folyamatait Szolgáltató erre vonatkozó belső szabályzatai írják le részletesen.

#### 5.4.6 A napló gyűjtési rendszere

A naplóbejegyzéseket az alkalmazások automatikusan gyűjtik és tárolják a napló állományokban. A médiákat Szolgáltató saját munkatársai szállítják a megőrzési helyre.

#### 5.4.7 Log-elemzés

A naplóbejegyzések feldolgozása során Szolgáltató naplóadat elemzéseket végez. A napi rendszerességgel végzett feldolgozáson túl Szolgáltató szakemberei havonta áttekintik a rendkívüli eseményeket és ezek alapján elemzéseket végeznek. Ezen elemzések alapján Szolgáltató lépéseket tesz a rendszer biztonságának javítására.

### 5.5 Adatok archiválása

Szolgáltató informatikai rendszerének biztonsági és egyéb naplózási folyamatait ugyanazon rendszerek végzik, ugyanazon módszerek segítségével. Jelen fejezetben csak Szolgáltató ettől eltérő papír alapú és egyéb speciális archiválási rendszerét ismertetjük.

### 5.5.1 Az archivált adatok típusai

Szolgáltató szervezete a szerződéskötési eljárás során keletkező iratot tárol és megőrzi. Így tárolják:

- a Szolgáltatóhoz benyújtott valamennyi papír alapú kérelmet,
- Szolgáltató és az előfizető között megkötött valamennyi megállapodást.
- Rendszer naplók archiválása

### 5.5.2 Az archívum megőrzési időtartama

**5.5.3** Szolgáltató valamennyi (papíralapú vagy elektronikus) iratot avonatközö tanúsítvány érvényességének lejártától számított 10 évig, illetőleg velük kapcsolatban esetlegesen felmerült jogvita jogerős lezárásáig megőrzi. Szolgáltató a Szolgáltatási Szabályzatot és annak módosításait hatályon kívül helyezést követően 10 évig megőrzi, illetve gondoskodik annak megőrzéséről. Az archívum védelme

Az iratok biztonságos megőrzéséről és tárolásáról Szolgáltató egy Adattár segítségével gondoskodik, amelyhez a Szolgáltatónak a meghatározott munkatársai rendelkeznek hozzáférési engedéllyel.

A Szolgáltató az időbélyegzés szolgáltatás során elektronikus formában tárolt archivált adatállományt **legalább fokozott biztonságú aláírással** és minősített **időbélyegzővel** látja el.

### 5.5.4 Az archívum mentési folyamatai

Az elektronikus másolati példányban létező iratokat (amennyiben keletkeznek ilyenek) egyszer írható médiára rendszeresen mentik.

A rendszer naplókat a központi logtárban őrizzük.

### 5.5.5 Archív információ hozzáférését és ellenőrzését végző eljárások

Az archívumhoz Szolgáltató ügyfélszolgálatán keresztül biztosít hozzáférést. A hozzáférés előfizetőnek a rá vonatkozó adatokhoz lehetséges, más feleknek a 9.4.2, 9.4.3 és 9.4.4 alfejezetek szerint. Szolgáltató a jogosultságot minden esetben ellenőrzi, és azt naplózza.

## 5.6 Kompromittálódást és katasztrófát követő helyreállítás

### 5.6.1 Váratlan esemény és kompromittálódás kezelési eljárások

Rendkívüli üzemeltetési helyzet bekövetkezése esetén a szolgáltató haladéktalanul értesíti az NMHH Bizalmi Felügyeletet és szükség esetén a Nemzeti Adatvédelmi és Információszabadság Hatóságot a rendkívüli üzemeltetési helyzet bekövetkezéséről a következő tartalommal:

- a) a rendkívüli üzemeltetési helyzet kezdetének, és ha eltér, észlelésének időpontja és a rendkívüli üzemeltetési helyzet leírása,
- b) a rendkívüli üzemeltetési helyzet hatása (ennek részeként biztonsági esemény esetén az érintett szolgáltatások, informatikai vagyonelemek és az érintett személyes adatok körének leírása, az érintett bizalmi szolgáltatási ügyfelek száma),
- c) a rendkívüli üzemeltetési helyzet várható időtartama,
- d) a rendkívüli üzemeltetési helyzet elhárítása és jövőbeli elkerülése érdekében tett és tervezett intézkedések, és
- e) a rendkívüli üzemeltetési helyzet megszűnése.

A Szolgáltató a rendkívüli üzemeltetési helyzetről értesíti a szolgáltatást igénybe vevő azon szerződött ügyfeleit, akiket a rendkívüli üzemeltetési helyzet érint, valamint az erről szóló tájékoztatást az interneten elérhetővé teszi.

A Szolgáltató Katasztrófa elhárítási tervben (DRP) részletesen szabályozza a különböző sérülések és katasztrófahelyzetek (beleértve valamely szolgáltatói magánkulcs kompromittálódását, vagy kritikus hardver/szoftver elem meghibásodását is) esetén követendő eljárásokat. A következő fejezetekben e katasztrófa elhárítási irányelveket foglaljuk össze.

Kompromittálódás esetén az 5.6.3 alfejezetben írtak kerülnek alkalmazásra.

Minden változást 30 nappal előre a szolgáltató benyújt a bizalmi felügyelet felé.

### 5.6.2 Meghibásodott számítási erőforrások, szoftverek és/vagy adatok

Szolgáltató megnövelt biztonságú eszközökkel és rendszerekkel rendelkezik, a hardver- és szoftver-meghibásodások, valamint az adatsérülések minimalizálása érdekében. A szolgáltatások helyreállíthatóságát Szolgáltató háttérszerződése és saját tartalékeszközei garantálják. Szolgáltató rendszeres mentései és tranzakció naplózása biztosítja az adatok visszaállíthatóságát valamely adattároló eszköz kiesésének esetére. Ez a rendszer a legrosszabb esetben az előző napi adatok helyreállítására képes.

Szolgáltató katasztrófa elhárítási terve eseményjelentési előírásokkal rendelkezik valamennyi eszköze meghibásodása, illetve rendellenes működése tekintetében (ezek egy része automatizált, más része a kezelőszemélyzet felelőssége). A jelentéseket szakértő személyzet értékeli ki, és válaszadás eljárásokat foganatosítva minimalizálja az esetleges károkat és szolgáltatás kieséseket.

### 5.6.3 Egy szolgáltatói egység kulcsának kompromittálódása

Szolgáltató katasztrófa elhárítási terve a szolgáltatói magánkulcsok<sup>8</sup> kompromittálódása esetére akciótervvel rendelkezik. Az akcióterv a szolgáltatói nyilvános kulcs visszavonása mellett feltárja a kompromittálódás körülményeit, intézkedik az ez által érintett valamennyi fél értesítéséről, megteszi a szükséges lépéseket a kompromittálódás megismétlődése ellen és szükség esetén új kulccsal látja el a szolgáltatói egységet.

### 5.6.4 Működés folyamatosságának biztosítása katasztrófát követően

Szolgáltató **elsődleges működési helyszínein** kívül másodlagos helyszínekkel is rendelkezik. Természeti vagy más katasztrófát követően, illetve Szolgáltató berendezéseinek olyan mértékű meghibásodását illetően, mely a fentiek szerint nem kezelhető, Szolgáltató a másodlagos helyszínen is képes szolgáltatásainak beindítására. Szolgáltató a helyreállítás során a visszavonási nyilvántartások elérhetőségét elsőként, minden más szolgáltatást és tevékenységet megelőzően biztosítja. Ennek érdekében azok több független forrásból is folyamatosan rendelkezésre állnak (web-es elérés, címtár szolgáltatás produktív és DR site-on).

A szolgáltatások elindítását Szolgáltató 3 órán belül vállalja.

### 5.6.5 Egy szolgáltatói egység órájának 1 másodpercnél nagyobb eltérése az UTC időtől

A Szolgáltató olyan gyakorisággal szinkronizálja az időbélyegző egységeit az időjel-ellátó egységhez, hogy az eltérés nem haladhatja meg az 1 másodpercet. Szolgáltató olyan időbélyegző rendszert működtet, amely a megengedettől nagyobb eltérés esetén az időbélyeg kéréseket elutasítja, az időbélyegzés kiadását felfüggeszti. Szolgáltató katasztrófa elhárítási terve erre az esetre akciótervvel rendelkezik. Az akcióterv a probléma okának feltárása mellett lépéseket tartalmaz a szinkron helyre állítása, illetve valamennyi érintett fél felé történő kommunikációra.

---

<sup>8</sup> Ide nem csak az időbélyegző egységek tartoznak, de egyéb – az időbélyegzés szolgáltatásban részt vevő - alkalmazások és személyek kulcsai is.

## 5.7 Incidenskezelés

Szolgáltató rendszereiben egységes incidenskezelési folyamatot működtet. A folyamat szabályozását Szolgáltató nem nyilvános belső szabályzói tartalmazzák. Az incidensekről PostMortem készül, melyeket a szolgáltatás kockázatelemzési dokumentumának felülvizsgálata során felhasználnak.

## 5.8 Változáskezelés

Szolgáltató rendszereiben a Magyar Telekom szervezeteire egységes belső utasítás szerint végzi a változáskezelést. Az utasítás részletesen szabályozza a folyamat működtetését és mechanizmusait.

Szolgáltató ennek keretében végzi a Patch management tevékenységét, az esetlegesen szükségessé váló konfigurációs, illetve szoftverváltoztatásokat, upgrdae-keket. A változás menedzsment folyamat engedélyezési és tájékoztatási workflow révén kontrollált, megfelelően dokumentált.

Az üzemeltető csapat éves rendszerességgel elvégzi a rendszerellenőrzéseket.

A biztonsági frissítések megléte az üzemeltető csapat feladata, amelyek telepítése a gyártóval való egyeztetés után eldöntendő.

## 5.9 Időszinkronizáció

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 időbélyegyek 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.

## 5.10 Időbélyeg szolgáltató vagy szervezet leállítása

A Szolgáltató a szolgáltatás tervezett megszüntetése esetén legkevesebb **60 nappal** a szolgáltatás leállítását megelőzően értesíti az előfizetőket és a Bizalmi Felügyeletet. Szolgáltató ezt követően már nem köt új előfizetői szerződést és a tervezett megszűnés előtt legalább 20 nappal leállítja az időbélyegzés szolgáltatást. Haladéktalanul megkezd az egyeztetéseket más minősített bizalmi szolgáltatóval az Dáptv. 92.§-ban foglaltak végrehajtására. A Szolgáltató az időbélyegzés szolgáltatás leállítása előtt intézkedik a az időbélyeg szolgáltatáshoz kapcsolódó tanúsítvány(ok) visszavonásáról. A Szolgáltató a szolgáltatás befejezésekor az informatikai rendszerében foglalt adatairól teljes körű, minősített Időbélyegzővel ellátott mentést készít. A szolgáltatás leállítása során elvégzendő feladatokról Szolgáltató leállítási tervvel rendelkezik.

## 6 Műszaki biztonsági óvintézkedések

A Szolgáltató, biztonságtechnikailag értékelt és minősített termékekből álló, megbízható informatikai rendszert használ szolgáltatásai nyújtásához.

### 6.1 Kulcspár előállítás és telepítés

Szolgáltató gondoskodik valamennyi általa (saját maga, egyes szervezeti egységei) generált magánkulcs biztonságos és az ipari szabványoknak megfelelő generálásáról.

A szolgáltató egyszerre egy egységben egy időbélyeg aláíró kulcsot használhat.

#### 6.1.1 Kulcspár előállítás

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 sehol nem kell továbbítani.

Az Időbélyegző Szervezet az alábbi kulcspárt használja:

- Időbélyeget aláíró kulcs (TrustedTimeStamp szerverek kulcsai).

#### 6.1.2 A szolgáltatói nyilvános kulcs közzététele

Az Időbélyegző Szervezet mindenki számára elérhetővé teszi a szolgáltatói nyilvános kulcsokat tartalmazó tanúsítványokat a **Címtárban**, valamint a Szolgáltató honlapján.

#### 6.1.3 Kulcs méretek

az Időbélyegző szerverek aláíró kulcsának mérete: .....2048 bit

#### 6.1.4 A nyilvános kulcs paraméterek előállítása és ellenőrzése

Az Időbélyegző Szervezet digitális aláírásra az **RSA algoritmust** használja.

Az RSA algoritmussal van aláírva a rendszer által kibocsátott **időbélyegző**, és ezt az algoritmust használják a rendszeren belül is a letagadhatatlanság biztosítására.

A kulcsgenerálás paramétereinek megfelelőségét két szempontból ellenőrzi a rendszer:

- a paraméterekhez felhasznált véletlenszám generálás megfelelőségének ellenőrzése (statisztikailag kellőképpen véletlenszerű-e a generálás),

- a paraméterekre vonatkozó feltételek, összefüggések teljesülésének ellenőrzése.

A véletlenszám generálás megfelelőségének ellenőrzése:

- A rendszerben használt valamennyi kriptográfiai hardver modul képes az általa generált bitsorozat egyenletességének és függetlenségének statisztikai tesztelésére. A modulok lehetővé teszik a tesztek meghívását egy szabványos interfészen keresztül.
- A külső interfészen meghívható tesztelési utasításon kívül a hardver modulok is folyamatosan tesztelik saját véletlenszám generálásukat.

A paraméterekre vonatkozó feltételek, összefüggések teljesülésének ellenőrzése:

- A rendszerben használt valamennyi kriptográfiai hardver modul a kulcsgenerálás során generált paraméterekre ellenőrzi, hogy azok a rájuk vonatkozó korlátok közé esnek-e, illetve teljesülnek-e az egymás közötti, kötelező összefüggések.

### 6.1.5 A kulcs használat célja (az X.509 v3 kulcs használati mező tartalmának megfelelően)

### 6.1.6 Magyar Telekom SuperProxy védelme

- A Magyar Telekomban használt SuperProxy egy paicvezető megoldás, a konfigurációs fájlokat egy külön repository-ban tárolva. A szerverek geo-redundásan lettek elhelyezve a Magyar Telekom súlyponti telephelyein.

A "kulcs használati" mezők lehetséges (egyúttal kötelezően kitöltendő) értékei az alábbiak:

| Kulcs megnevezése                      | A "kulcs használati" mező értéke                              | Kritikus / Nem kritikus |
|----------------------------------------|---------------------------------------------------------------|-------------------------|
| az időbélyegző egységek aláíró kulcsai | <b><i>NonRepudiation</i></b>                                  | K                       |
|                                        | az „Extended Key Usage” mezőbe:<br><b><i>timeStamping</i></b> | K                       |

## 6.2 A Szolgáltatói magánkulcsok védelme és a kriptográfiai modulokkal kapcsolatos előírások

### 6.2.1 Kriptográfiai modulra vonatkozó szabványok

A Szolgáltató Időbélyegző szervezete a kriptográfiai kulcsok gondozását külön hardver modulban valósítja meg.

A Szolgáltató az időbélyeget aláíró magánkulcsait, valamint a Magyar Telekom Root CA magánkulcsát - a Bizalmi Felügyelet által nyilvántartásba vett, tanúsításra jogosult szervezet által erre a célra kiadott igazolással rendelkező – kriptográfiai hardver modulban (a továbbiakban: HSM) kezeli.

| Kriptográfiai modul                | Főmver verzió  |
|------------------------------------|----------------|
| nShield5s Hardware Security Module | v13.5.1        |
| Trident HSM                        | Trident v3.1.3 |

Az Időbélyegző Szervezet kulcsainak generálása a HSM eszközzel történik, amely megfelel a [10] EU szabvány 7.6.3 pontjában foglaltaknak.

Az Időbélyegző Szervezet kulcsainak előállítása **On-board hardver** generálással történik.

Fentiek során a Nemzeti Média- és Hírközlési Hatóság (NMHH) által a [4] dokumentumban jelzett algoritmusok használata megengedett.

### 6.2.2 A több-szereplős (“n-ből m”) magánkulcs visszaállítás ellenőrzése

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

### 6.2.3 Magánkulcs mentése

A Szolgáltatónál az Időbélyegző Szervezet magánkulcsai nem kerülnek mentésre, azokat a HSM **maga generálja**, és a magánkulcs semmilyen körülmények között nem hagyja el a modult.

Ha a fenti aláíró magánkulcsok megsemmisülnek, akkor helyettük új kulcsok kerülnek generálásra.

## 6.2.4 Magánkulcs archiválása

A Szolgáltató a magánkulcsokat, beleértve a Magyar Telekom hitelesítő kulcsokat, HSM által biztosított mentési formátumban archiválja.

## 6.2.5 Magánkulcs bejuttatása a kriptográfiai modulba

Az Időbélyegző Szervezet magánkulcsait a HSM **maga generálja**, és a magánkulcs a modult kizárólag a HSM által biztosított mentési formátumban hagyja el. (.

## 6.2.6 Magánkulcs tárolása a kriptográfiai modulba

A szolgáltatói magánkulcsok tárolása kriptográfiai modulban történik, a hozzáférés-ellenőrzésekkel együtt az előző alfejezeteknek megfelelően.

## 6.2.7 A magánkulcs aktiválásának módja

A HSM kriptográfiai hardver modulok magánkulcsa csak aktív állapotban használható. A kulcsot a HSM indításakor aktiválni kell. Az így aktivált magánkulcs mindaddig használható, amíg a modul aktív állapotban marad.

## 6.2.8 A magánkulcs aktív állapotának megszüntetési módja

A HSM kriptográfiai hardver modul magánkulcsa akkor deaktiválódik, ha a modul (szabályos vagy szabálytalan módon) kikerül az aktív állapotból. Ez az alábbi esetben következik be:

- a jogosult adminisztrátor törli a kulcsot,
- a kriptográfiai modul áramellátása megszakad (kikapcsolás vagy tápellátási probléma),
- a kriptográfiai modul hibaállapotba kerül.

Az így deaktivált magánkulcs mindaddig nem használható, amíg a modul ismét aktív állapotba nem kerül.

## 6.2.9 A magánkulcs megsemmisítésének módja

Az Időbélyegző Szervezet HSM kriptográfiai hardver moduljaiban tárolt magánkulcsok megsemmisítése a Biztonsági tisztviselő, a rendszer adminisztrátor és rendszer operátor együttes jelenlétében sikeres hitelesítésük után, a szükséges kulcsmegsemmisítő funkciók kiváltásával történhet.

## 6.2.10A kriptográfiai modulok értékelése

A 6.2.1 ponttal összhangban az alábbi táblázat tartalmazza a Szolgáltató által alkalmazott kriptográfiai hardver modulokra nézve, az ezek ellenőrzése, bevizsgálása és értékelése során megállapított legfontosabb tényeket, tulajdonságokat:

| Kriptográfiai modul              | HSM (nChiper nShield)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A modul fizikai konfigurációja   | <ul style="list-style-type: none"> <li>• Önálló modul</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Szolgáltatások                   | <ul style="list-style-type: none"> <li>• kriptográfiai műveletek (kódolás, dekódolás, üzenet sértetlenség, digitális aláírás generálás, digitális aláírás ellenőrzés)</li> <li>• kulcsmenedzsment (kulcs generálás, védett kulcstárolás, kulcs klónozás, „n-ből m” aktivizálás, kulcs nullázás)</li> <li>• kriptográfiai menedzsment funkciók (naplózási paraméterek bevitele és beállítása, alarm kezelés és visszaállítás/resetelés/)</li> <li>• felhasználó által választható ön-tesztek végrehajtása (kriptográfiai algoritmus tesztek, szoftver/főrmver tesztek, a kritikus funkciók tesztjei, statisztikus véletlenszám generátor teszt)</li> <li>• "státusz kijelzés" (a következőket jelzik ki: aktív szerepkör, a modul kriptográfiai státusza /nullázott, beavatkozás következményeként fellépő, betöltött, inicializált/, hiba kód (ha a modul hiba állapotban van))</li> </ul> |
| Az operációs rendszer biztonsága | A modulok nem nyújtanak olyan eszközt, amelynek segítségével egy operátor a modul hatáskörébe nem tartozó szoftvereket / főrmvereket tölthet be és hajthat végre. Ezért ez a kérdéskör jelen modulokra nem releváns.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Kriptográfiai kulcskezelés       | <p>A modulok védik a tárolt titkos és magánkulcsokat a jogosulatlan felfedéssel, módosítással és helyettesítéssel szemben.</p> <p>A modulok védik a tárolt nyilvános kulcsokat a jogosulatlan módosítással és kicseréléssel szemben.</p> <p>A kulcsgenerálás és a kulcs megsemmisítésének módszere szabványos és biztonságos</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Kriptográfiai algoritmusok       | A modulok FIPS által jóváhagyott illetve a Nemzeti Média- és Hírközlési Hatóság által a [4] dokumentumban jelzett algoritmusokat alkalmaznak.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Öntesztek                        | A modulok képesek öntesztek végrehajtására, annak kimutatására, hogy megfelelően működnek                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Értékelési szint                 | FIPS 140-2 szabvány szerint 3. szinten bevizsgált                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

| Kriptográfiai modul              | HSM (Trident)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A modul fizikai konfigurációja   | <ul style="list-style-type: none"> <li>• Önálló modul</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Szolgáltatások                   | <ul style="list-style-type: none"> <li>• kriptográfiai műveletek (kódolás, dekódolás, üzenet sértetlenség, digitális aláírás generálás, digitális aláírás ellenőrzés)</li> <li>• kulcsmenedzsment (kulcs generálás, védett kulcstárolás, kulcs klónozás, „n-ből m” aktivizálás, kulcs nullázás)</li> <li>• kriptográfiai menedzsment funkciók (naplózási paraméterek bevitele és beállítása, alarm kezelés és visszaállítás/resetelés/)</li> <li>• felhasználó által választható ön-tesztek végrehajtása (kriptográfiai algoritmus tesztek, szoftver/főrmver tesztek, a kritikus funkciók tesztjei, statisztikus véletlenszám generátor teszt)</li> <li>• "státusz kijelzés" (a következőket jelzik ki: aktív szerepkör, a modul kriptográfiai státusza /nullázott, beavatkozás következményeként fellépő, betöltött, inicializált/, hiba kód (ha a modul hiba állapotban van))</li> </ul> |
| Az operációs rendszer biztonsága | A modulok nem nyújtanak olyan eszközt, amelynek segítségével egy operátor a modul hatáskörébe nem tartozó szoftvereket / főrmvereket tölthet be és hajthat végre. Ezért ez a kérdéskör jelen modulokra nem releváns.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Kriptográfiai kulcskezelés       | <p>A modulok védik a tárolt titkos és magánkulcsokat a jogosulatlan felfedéssel, módosítással és helyettesítéssel szemben.</p> <p>A modulok védik a tárolt nyilvános kulcsokat a jogosulatlan módosítással és kicseréléssel szemben.</p> <p>A kulcsgenerálás és a kulcs megsemmisítésének módszere szabványos és biztonságos</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Kriptográfiai algoritmusok       | A modulok FIPS által jóváhagyott illetve a Nemzeti Média- és Hírközlési Hatóság által a [4] dokumentumban jelzett algoritmusokat alkalmaznak.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Öntesztek                        | A modulok képesek öntesztek végrehajtására, annak kimutatására, hogy megfelelően működnek                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Értékelési szint                 | FIPS 140-2 szabvány szerint 3. szinten bevizsgált                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

### 6.3 A kulcspár kezelésének egyéb szempontjai

#### 6.3.1 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.**



A kulcsok lejárata után eltörölendők.

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 láncan ellenőrzi, mielőtt azokat az időbélyegző egységekbe beimportálja.

## 6.4 Informatikai biztonsági óvintézkedések

### 6.4.1 Speciális informatikai biztonsági műszaki követelmények

Szolgáltató a Minősített Időbélyegzés Szolgáltatásban alkalmazott időbélyegző egységeit a Magyar Telekom Gyökér Hitelesítő (továbbikában: Magyar Telekom Root CA) egységében hitelesíti. A Magyar Telekom Root CA-t a Magyar Telekom Technológiai biztonsági központ (Időbélyegző Szervezet) működteti, önálló megbízható környezetben. A Magyar Telekom Root CA off-line CA, hálózati kapcsolattal nem rendelkezik. A Szolgáltató a Magyar Telekom Root CA magán kulcsát kriptográfiai modulban kezeli, amely megfelel a [10] EU szabvány 7.6.3 pontjában foglaltaknak.

A Magyar Telekom Root CA az általa kibocsátott tanúsítvány visszavonását követően azonnal, de legalább 180 naponta tanúsítvány visszavonási listát (CRL) ad ki, melyet a folyamatosan elérhetővé tesz a

<https://www.telekom.hu/vallalati-megoldasok/nagyvallalatok/hitelesites-szolgalattasok/idobelyegzes-szolgalattas>

lapon és a címtárban.

Az Időbélyegző Szervezet olyan megbízható informatikai rendszereket alkalmaz, mely az alábbi termékeken alapul:

#### **LDAP gyártású Trident HSM**

Az időbélyegző rendszerbe TridentHSM eszközök kerültek beépítésre..

- RedHat alapú szerver(ek),

#### **Nyilvános LDAP szervíz (HA gép-pár)**

- Operációs rendszer [GNU/Linux + HA (HeartBeat HA szoftver)],
- Kernel verzió: folyamatosan frissített stabil verzió.

**Tűzfal A10 (HA gép-pár)**

- Operációs rendszer [GNU/Linux + HA ],
- Kernel verzió: folyamatosan frissített stabil verzió,
- A10 alkalmazásszintű tűzfal szoftver.
- Timestamp gateway

Az operációs rendszerek által megvalósított biztonsági funkciók az alábbiak:

- **biztonsági naplózás** (a központi adminisztrátori hozzáférések és tevékenységek rögzítése, a biztonsági napló védelme, az ahhoz való hozzáférés rendszervizsgáló szerepkörre korlátozása),
- a felhasználói adatok védelme (a **hozzáférés ellenőrzési** szabályok alapjainak érvényre juttatása /rendszer fájlok védelme, a felhasználói adatok csak alkalmazáson keresztüli elérésének biztosítása/, a tárolt adatok sértetlenségének védelme /beleértve a vírusok, káros és engedély nélküli szoftverek elleni védekezés támogatását is/, a maradvány információ védelmének megvalósítása),
- **azonosítás és hitelesítés** (a központi adminisztrátorok azonosítása és hitelesítése, az operációs rendszer által biztosított funkciók elérésének sikeres hitelesítéshez kötése),
- **biztonságkezelés** (a biztonsági szerepkörök kezelése, a hozzáférési jogosultságok szerepkörök szerinti beállítása, módosítása),
- **biztonsági funkciók megbízható védelme** (alap biztonsági tesztelés végrehajtása, biztonságos állapot megőrzése hiba esetén, a hozzáférés ellenőrzés megkerülhetetlenségének biztosítása, a különböző alkalmazói folyamatok által használt tartományok elkülönítése).

Az alkalmazások által megvalósított biztonsági funkciók az alábbiak:

- **biztonsági naplózás** (a rendszeroperátori hozzáférések és tevékenységek rögzítése),
- **biztonságos kommunikáció** (az Időbélyegző Szervezet és az előfizető közötti kommunikáció bizalmosságának, sértetlenségének és hitelességének biztosítása,
- **felhasználói adatok védelme** (a hozzáférés ellenőrzési szabályok érvényre juttatása /az elindított alkalmazások csak a jogosultságnak megfelelő funkciók elérhetőségét biztosítják/, a maradvány információ védelmének támogatása),
- **azonosítás és hitelesítés** (a rendszeroperátorok azonosítása, hitelesítése, az alkalmazások által biztosított funkciók elérésének sikeres hitelesítéshez kötése).

A **kriptográfiai hardver modulok** által megvalósított biztonsági funkciók részletesen az nCipher nShield/payShield User/Administration Guide /Windows/ dokumentációkban található.

A **tűzfal** által megvalósított biztonsági funkciók az alábbiak:

- **biztonsági naplózás** (a hálózati kommunikáció naplózása, a biztonsági napló védelme, az ahhoz való hozzáférés rendszervizsgáló szerepkörre korlátozása, a napló folyamatos elemzése: biztonsági riasztások és automatikus válaszok megvalósítása),
- **felhasználói adatok védelme** (az információ áramlás ellenőrzési szabályok érvényre juttatása /szűrés, a tiltott információ áramlás megakadályozása, megfigyelése,)
- **azonosítás és hitelesítés** (központi adminisztrátorok/ azonosítása, hitelesítése, a tűzfal funkciók elérésének sikeres hitelesítéshez kötése),
- **biztonsági funkciók megbízható védelme** (az információ áramlás ellenőrzés megkerülhetetlenségének biztosítása).
- **A biztonsági napló elemzése a rendszervizsgáló feladata**, amit havi rendszerességgel hajt végre.

#### 6.4.2 Informatikai biztonsági minősítés

Az Időbélyegző Szervezet olyan megbízható informatikai rendszert alkalmaz, mely az alábbi komponenseken alapul:

- (tűzfal) operációs rendszer GNU/Linux,
- (időbélyegző alkalmazás) Linux operációs,
- alkalmazásintű és csomagszűrő tűzfalat működtet.

Az Időbélyegző Szervezet informatikai rendszerében alkalmazott kriptográfiai hardver modulok minősítésére vonatkozóan lásd a {6.2.1 Kriptográfiai modulra vonatkozó szabványok} és {6.2.10 A kriptográfiai modul értékelése} alfejezeteket.

#### 6.4.3 A szolgáltatásban alkalmazott termékek kezelése

A szolgáltatás informatikai rendszereiben alkalmazott hardver és szoftver eszközök beszállítását megelőzően ellenőrizni kell a gyártói csomagolás sértetlenségét, illetve az eszközök sértetlenségét. Az eszközöket használatból történő kivonás előtt adatmentesíteni kell és csak azt követően szállíthatóak ki az üzemeltetési környezetből.

Az alkalmazott termékekről szolgáltató a HP Service Management alkalmazásában létrehozott CMDB-ben vezet nyilvántartást.

## 6.5 Életciklusra vonatkozó műszaki óvintézkedések

### 6.5.1 Rendszerfejlesztési óvintézkedések

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 visszaállítási 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.

### 6.5.2 Biztonságkezelési óvintézkedések

Az Időbélyegző Szervezet szolgáltatásai nyújtásához olyan termékeket használ, amely a helyes konfigurációt megalapozó megfelelő útmutató dokumentációk használatával, valamint a helytelen használat lehetőségének és egyéb sebezhetőségek vizsgálata útján biztosítja az elvárt működést.

### 6.5.3 Az életciklusra vonatkozó biztonság osztályozása

Az Időbélyegző Szervezet által a szolgáltatások nyújtásához használt termékek, életciklusra vonatkozó biztonsági szempontok figyelembevételével kerültek alkalmazásra.

### 6.5.4 Behatolási tesztek

Az időbélyegző infrastruktúra, vagy az alkalmazási környezet jelentős változását követően Szolgáltató dokumentált módon behatolási tesztek végzetet, melynek bizonyítékait dokumentációs rendjében illesztve kezeli. Szolgáltató a kiválasztás során biztosítja, hogy a behatolási tesztekkel megbízott személyek megfelelő felkészültséggel rendelkeznek, illetve szerződésben rögzíti a tesztek végzőkkel kapcsolatos etikai elvárásokat.

Az éves Vulnerability tesztek elvégzésének gyakorisága: Negyedévente legalább egy alkalommal.

Az éves belső penetration tesztek elvégzésének gyakorisága: Évente legalább egy alkalommal.

Az éves független penetration tesztek elvégzésének gyakorisága: Évente legalább egy alkalommal.

Az éves megfelelőségértékelés során feltárt, esetlegesen fennmaradó kockázatokat a releváns vezető tudja felvállalni, aminek tényét jegyzőkönyvben rögzíteni kell és megőrizni.

A vulnerability és penetration tesztek értékelő riportok áttekintése, azokban esetlegesen meghatározott feladatok teljesítése, értékelése és intézkedési terv kidolgozásáért a rendszeradminisztrátor a felelős.

A sebezhetőségi és behatolási tesztek legalább egy rendszerüzemeltetőnek és egy biztonsági tisztviselőnek kötelező áttekintenie alá kell írni és időbélyeggel kell ellátni. Akadályoztatás esetén a feladatot a kijelölt helyettesek látják el.

### 6.5.5 Kapacitás figyelés és tervezés

Szolgáltató rendszeresen figyelemmel kíséri az időbélyegzés szolgáltatás igénybevételének főbb mutatóit: az igénybevett időbélyegzők mennyiségét és az igénybevételi csúcs idősávokat. Szolgáltató méréseket végzett a rendszer gyakorlati kibocsátó képességének meghatározására és annak növelési lehetőségére. A kiszolgáló rendszer megfelelő tartalékokkal rendelkezik, a kockázatelemzési dokumentum éves felülvizsgálata során szolgáltató értékeli a kapacitás képességeket és a jelentkező igényeket.

### 6.5.6 Kockázatelemzés

Szolgáltató évente legalább egy alkalommal felülvizsgálja kockázatelemzési dokumentumát. A felülvizsgálat során figyelembe kell venni

- az elmúlt időszakban bekövetkezett incidenseket, abból levonható következtetéseket
- az alkalmazott eszközökkel kapcsolatosan ismertté vált új kockázatokat
- a külső környezeti változásokból (szervezeti változások is) következő és azonosítható új kockázatokat
- a jelentős infrastruktúra változásból azonosítható új kockázatokat
- valamint a kockázatok csökkentésére lehetséges intézkedéseket, maradvány kockázatokat
- A kapacitási igényeket és képességeket

Az infrastruktúra jelentős változása esetén indokolt a dokumentum soron kívüli felülvizsgálata. A felülvizsgálatról feljegyzés készül, illetve a módosított kockázatelemzési dokumentum kerül jóváhagyásra. Az dokumentumban megfogalmazott új intézkedések egyben akció tervet is képeznek, az eljövendő időszak feladataira. A felülvizsgálatot egy rendszeradminisztrátor végzi. Az ellenőrzésért egy másik rendszeradminisztrátor és a biztonsági tisztviselő felelős. A felülvizsgálat eredményét jegyzőkönyvben kell rögzíteni és megőrizni.

## 6.5.7 Jogosultságkezelés

Az időbélyegzés szolgáltatás informatikai rendszereihez történő hozzáférés a Szolgáltató jogosultságkezelési utasítása alapján működtetett Központi jogosultság menedzsment rendszerben (továbbiakban: IAM) történt igénylés és engedélyezést követően kerülhet beállításra a bizalmi munkakörbe kinevezett felhasználók számára. A bizalmi munkakört betöltő személyek körében bekövetkező változásokat az informatikai rendszerekhez történő hozzáférések tekintetében is átvezeti a Szolgáltató.

## 6.6 Hálózatbiztonsági óvintézkedések

Az időbélyegző rendszer hálózatbiztonsági szempontból tűzfalakkal leválasztott hálózati szegmensben üzemel a Magyar Telekom intranettól, valamint az internettől. Az Időbélyegző Szervezet és az előfizetők közötti kommunikáció védett a bizalmasság, sértetlenség és letagadhatatlanság elvesztése ellen. A magas szintű védelmet titkosítással és digitális aláírással biztosítják.

Nyitott portok:

| PRD                                                                                                                                                                                                                                            | DR                                                                                                                                                                                                                                                                              |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>- heartbeat</li> <li>- sshd</li> <li>- stunnel</li> <li>- exim</li> <li>- ts_gw internet</li> <li>- ts_gw intranet</li> <li>- munin-node</li> <li>- OCSP_GW</li> <li>- https</li> <li>- ldap</li> </ul> | <ul style="list-style-type: none"> <li>- heartbeat</li> <li>- sshd</li> <li>- stunnel</li> <li>- exim</li> <li>- ts_gw internet</li> <li>- ts_gw intranet</li> <li>- munin-node</li> <li>- TS_Gw</li> <li>- OCSP_GW</li> <li>- icmp</li> <li>- https</li> <li>- ldap</li> </ul> |

## 6.7 HSM tanúsítottság meglétének ellenőrzése

A szolgáltatásban használt HSM eszközök tanúsítottságát a rendszeradminisztrátor szerepkört betöltő személy feladata ellenőrizni havonta legalább egyszer, az ellenőrzés eredményéről jegyzőkönyvet kell vezetni és legalább egy évig megőrizni. A jegyzőkönyvet egy bizalmi szerepkört betöltő személynek kell ellenjegyeznie.

Jelen HSM tanúsítottságát a OCSI (Organismo di Certificazione della Sicurezza Informatica) igazolta, a honlapjukon szükséges a tanúsítottság érvényességét ellenőrizni.



<https://www.acn.gov.it/>  
<https://www.tuv-nederland.nl/>

Az ellenőrzésnek ki kell terjednie a megfelelőségi tanúsítvány besorolására (pl. aktív vagy archivált), valamint a tanúsítvány érvényességére, annak várható lejáratí időpontjára és felhasználhatóságára vonatkozó feltételek és kikötések aktuális állapotára.

A HSM tanúsítottság meglétének ellenőrzést a HSM tanúsítvány ellenőrzési rend írja le.

## 7 Tanúsítvány profil

Szolgáltató által használt Időbélyegzői tanúsítvány alap mezői a következők:

| Mezőnév                                                                                                    | Érték vagy szabály                                                                                                                                                                 |
|------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Verzió</b><br><i>Version</i>                                                                            | A tanúsítvány a [8] ajánlásban leírt X509 3-as verziójú tanúsítványnak felel meg {ld. <b>1.7 Hivatkozások</b> }. Ebbe a mezőbe az „ <b>x.509v3</b> ” adat kerül a tanúsítványokon. |
| <b>Sorozatszám</b><br><i>Serial Number</i>                                                                 | A tanúsítványok sorozatszáma: egyedi szám, amelyet a <i>Hitelesítő Egység</i> ad ki.                                                                                               |
| <b>Algoritmus azonosító</b><br><i>Signature Algorithm Identifier</i>                                       | Ez a szám a <i>Szolgáltató tanúsítványokat hitelesítő elektronikus aláírásának</i> algoritmusát azonosítja {ld. 7.3}.                                                              |
| <b>Aláírás</b><br><i>Signature</i>                                                                         | A <i>Szolgáltató</i> tanúsítványt hitelesítő <b>elektronikus aláírása</b> , amelyet a [8] szerint generál és kódol.                                                                |
| <b>Kibocsátó</b><br><i>Issuer</i>                                                                          | A tanúsítványt kibocsátó <i>Időbélyegző Szervezet</i> egyedi tulajdonos azonosítója {ld.7.4}.                                                                                      |
| <b>Érvényesség</b><br><i>Valid From &amp; Valid To</i>                                                     | A tanúsítvány érvényességének kezdete és vége <sup>9</sup> , amely UTC szerinti érték a [8] szerinti kódolással.                                                                   |
| <b>Aláíró (tulajdonos) azonosító</b><br><i>Subject</i>                                                     | Az <i>aláíró</i> (tulajdonos) egyedi neve {ld. 7.4}.                                                                                                                               |
| <b>Aláíró nyilvános kulcsának algoritmus-azonosítója</b><br><i>Subject Public Key Algorithm Identifier</i> | Ebbe a mezőbe az aláírói nyilvános kulcs algoritmusának azonosítója kerül {ld. 7.3}.                                                                                               |
| <b>Aláíró nyilvános kulcsa</b><br><i>Subject Public Key Value</i>                                          | Az aláíró nyilvános kulcsa.                                                                                                                                                        |

### 7.1 Verzió szám(ok)

Szolgáltató a [8] ajánlásban szereplő X509 3. verziónak megfelelő szolgáltatói tanúsítványokat használ.

### 7.2 Tanúsítvány-kiterjesztések

<sup>9</sup> A két időpont közötti időtartam 11 év

Szolgáltató által használt Időbélyegzői tanúsítvány **kiterjesztései** a következők:

| Mezőnév                                                                             | Érték vagy szabály                                                                                                                                                                                                                                                                                                             | Kritikus |
|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| <b>Tanúsítvány irányelv</b><br><i>Certificate Policies</i>                          | Certificate Policy [1]:<br>PolicyIdentifier: 1.3.6.1.4.1.17835.7.1.2.11.3.12.2.2<br>Policy Qualifier Information [1.1]:<br>PKIX CPS Pointer Qualifier (1.3.6.1.5.5.7.2.1)<br>CPS Pointer: https://www.t-systems.hu/nagyvallalatok/hitelesites_szolgaltatasok/idobelyegzes_szolgaltatas<br>{ld. 7.6}                            | Nem      |
| <b>Kibocsátó kulcs azonosító</b><br><i>Authority Key Identifier</i>                 | Kibocsátó kulcsára vonatkozó információ                                                                                                                                                                                                                                                                                        | Nem      |
| <b>Aláíró kulcs azonosító</b><br><i>Subject Key Identifier</i>                      | Alany kulcsára vonatkozó információ                                                                                                                                                                                                                                                                                            | Nem      |
| <b>Alapvető megkötések</b><br><i>Basic Constraints</i>                              | Subject Type=End Entity<br>Path Length Constraint=None                                                                                                                                                                                                                                                                         | Igen     |
| <b>Kulcshasználat</b><br><i>Key Usage</i>                                           | Digital Signature, Non-Repudiation (c0)                                                                                                                                                                                                                                                                                        | Igen     |
| <b>Kiterjesztett Kulcshasználat</b><br><i>Enhanced Key Usage</i>                    | Time Stamping (1.3.6.1.5.5.7.3.8)                                                                                                                                                                                                                                                                                              | Igen     |
| <b>CRL szétosztási pont</b><br><i>CRL Distribution Points</i>                       | CRL Distribution Point [1]:<br>URL=http://eszigno.t-systems.magyartelekom.hu/download_crl?issuer=Magyar%20Telekom%20RootCA%202011<br><br>CRL Distribution Point [2]:<br>URL=ldap://trustcenter.magyartelekom.hu:389/cn=Magyar%20Telekom%20RootCA%202011,c=HU?certificateRevocationList?base?objectClass=certificationAuthority | Nem      |
| <b>Hozzáférés a kiállítói információkhoz</b><br><i>Authority Information Access</i> | Authority Information Access [1]:<br>Access Method: OCSP (1.3.6.1.5.5.7.48.1)<br>Access Location:<br>URI: http://ocsp.magyartelekom.hu/ocsp                                                                                                                                                                                    | Nem      |
| <b>Tanúsítványminősítési nyugta</b><br><i>QC Statements</i>                         | QC Statement [1]:<br>QC Compliance<br>QC Statement [2]:<br>QC Secure Signature Creation Device<br>QC Statement [3]:<br>QC Type<br>EtsiQctEseal (0.4.0.1862.1.6.2)                                                                                                                                                              | Nem      |

### 7.3 Az algoritmus objektum-azonosítója

Szolgáltató által használt Időbélyegzői tanúsítvány aláírásakor az ecdsaWithSHA256: (OID 1 2 840 10045 4 3 2) – NIST P256 - használatos.

### 7.4 Elnevezési formák

Szolgáltató által használt Időbélyegzői tanúsítvány kibocsátó azonosító és az aláíró-azonosító esetében az egyedi X.500 név formátumot alkalmazza, jelen alfejezet szerint a kibocsátó-azonosító (Kibocsátó/Issuer) esetében.

Az Időbélyegzési Rendszerben meghatározott időbélyegző tanúsítványok kibocsátó azonosítója (a „Kibocsátó” mező tartalma) a következő:

| Jelölés   | Jelentés                                                               | Adat                       |
|-----------|------------------------------------------------------------------------|----------------------------|
| <b>CN</b> | a tanúsítvány kibocsátását végző szervezet neve ( <i>Common name</i> ) | Magyar Telekom RootCA 2011 |
| <b>O</b>  | a szolgáltató szervezet neve ( <i>Organization</i> )                   | Magyar Telekom             |
| <b>C</b>  | ország név ( <i>Country</i> )                                          | HU                         |

Az Időbélyegzési Rendszerben meghatározott időbélyegző tanúsítványok azonosítója (a „Tulajdonos” mező tartalma) a következő:

| Jelölés                                 | Jelentés                                                                                 | Adat                         |
|-----------------------------------------|------------------------------------------------------------------------------------------|------------------------------|
| <b>CN</b>                               | a tanúsítvány kibocsátását végző szervezet neve ( <i>Common name</i> )                   | TSU[1,2,3,...n] <kiadás éve> |
| <b>organizati<br/>onIdentifi<br/>er</b> | a tanúsítvány kibocsátását végző szervezet azonosítója ( <i>organizationIdentifier</i> ) | VATHU-10773381               |
| <b>OU</b>                               | a szolgáltató szervezeti egység neve ( <i>Organizational unit</i> )                      | TTI                          |
| <b>O</b>                                | a szolgáltató szervezet neve ( <i>Organization</i> )                                     | Magyar Telekom Nyrt.         |
| <b>L</b>                                | a szervezet székhelye - városnév ( <i>Locality</i> )                                     | Budapest                     |
| <b>C</b>                                | ország név ( <i>Country</i> )                                                            | HU                           |

### 7.5 Elnevezésre vonatkozó korlátozások

Szolgáltató ilyen korlátozást nem alkalmaz.

## 7.6 Az Időbélyegzési Rend objektum-azonosítója

Szolgáltató által használt Időbélyegzői tanúsítványok a vonatkozó Időbélyegzési Rend egyedi objektum-azonosítóját tartalmazzák {ld. 7.2 Tanúsítvány-kiterjesztések}.

## 7.7 A „Hitelesítési Rend korlátozás” kiterjesztés használata

Szolgáltató ezt a kiterjesztést nem használja.

## 7.8 Szabályzatminősítő szintaxis és szemantika

Szolgáltató által használt Időbélyegzői tanúsítványok a szolgáltatási szabályzat internetcímét, valamint figyelmeztető szöveget nem tartalmazzák {ld. 7.2 Tanúsítvány-kiterjesztések}.

## 7.9 A kritikus Időbélyegzési Rend kiterjesztés feldolgozása

Szolgáltató által használt Időbélyegzői tanúsítványokban alkalmazott Tanúsítvány-irányelv kiterjesztés nem kritikus. Mindazonáltal Szolgáltató előírásainak és kikötéseinek figyelmen kívül hagyásáért a végfelhasználók a felelősek.

## 7.10 Időbélyegző profil

Az időbélyegző profil leírását az Időbélyegzési Rend dokumentum [14] 5.3.1 fejezete tartalmazza.

## 8 Megfeleléségi audit és egyéb ellenőrzések

### 8.1 Az ellenőrzések körülményei és gyakorisága

A Szolgáltató vizsgált és tanúsított elemeket (elektronikus aláírási termékeket, informatikai rendszerelemeket stb.) alkalmaz az időbélyegzés szolgáltatásaihoz kapcsolódóan, úgymint:

- az időbélyeg előállítására, valamint magánkulcsainak tárolására használt kriptográfiai hardver modult,

A kriptográfiai hardver modulok tanúsítására a használatba vételt megelőzően kerül sor. A tanúsítás érvényességének lejártával a megfelelés-vizsgálatot meg kell ismételni.

A tanúsításhoz és vizsgálatokhoz a Szolgáltató alapvetően külső szervezete(ke)t vesz igénybe {ld. 8.2 Az auditor és szükséges képesítése}. A Szolgáltató e külső tanúsításokon túl saját belső központi ellenőrzési szervezettel is rendelkezik, mely rendszeresen vizsgálja a korábbi tanúsításoknak való megfelelést, és eltérés esetén megteszi a szükséges lépéseket. Ezen felül Szolgáltató informatikai szervezetében saját belső szakértői csoport tevékenykedik, mely az Időbélyegző Szervezet tevékenységét eseti és / vagy tervezett jelleggel megvizsgálja.

A Szolgáltató minősített időbélyegzés-szolgáltatóként történő önkéntes minősítési (akkreditációs) eljárásban a jelen szabályzat hatályba lépésének időpontjáig nem volt minősítve.

### 8.2 Az auditor és szükséges képesítése

A kriptográfiai hardver modulok tanúsítását egy erre feljogosított tanúsító szervezet végzi.

A minősített időbélyegzést kiszolgáló rendszerek és módszerek megfelelésének vizsgálatára külső, független, akkreditációval rendelkező megfelelés-értékelő szervezet, valamint Szolgáltató erre a célra létrehozott belső központi ellenőrzési szervezetének auditorai által kerül sor.

Emellett a Szolgáltató mind belső, mind pedig külső, független rendszervizsgáló(ka)t is megbíz a minőségirányítási és információbiztonsági rendszerek ellenőrzésére. Ezen szakemberek többéves szakmai gyakorlattal valamint megfelelő végzettséggel és szakképesítéssel rendelkeznek.

Mindezekon felül a Szolgáltatónál a Bizalmi Felügyelet is helyszíni szemlét és ellenőrzést tart, évente legalább egy alkalommal.

### 8.3 Az auditor és az auditált rendszer függetlensége

A Szolgáltatóval kapcsolatban tanúsítást végző szervezetek a Szolgáltatótól függetlenek, és befolyástól mentesen végzik tevékenységüket. A vizsgálatot végző külső, független szervezet nem rendelkezik tulajdonrészrel vagy érdekeltséggel a Szolgáltatót illetően, és Szolgáltató nem tulajdonosa közvetlenül vagy közvetve a vizsgálatot végző szervezetnek. A tanúsító szervezetek díjazása nem függ a tanúsítás során végzett tevékenységük megállapításaitól.

### 8.4 Az auditálás által lefedett területek

A vizsgálatok által lefedett területek a következők:

- A kriptográfiai hardver modulok tanúsítása, mely a [11] EU szabvány 7.6.3 pontjában meghatározott követelményeknek való megfelelés vizsgálatára irányul.
- A minősített időbélyegzést kiszolgáló rendszerek és módszerek tanúsítása (beleértve a dokumentálásra, folyamatokra, fizikai és műszaki biztonságra, az érintett személyzetre, valamint az adatvédelemre) mely a vonatkozó jogszabályok<sup>10</sup> előírásainak, a jelen Szabályzatban rögzített Időbélyegzési Rend dokumentumnak valamint Szolgáltató egyéb szabályzatainak való megfelelés vizsgálatára irányul.
- Szolgáltató minőségirányítási és információbiztonsági irányítási rendszere, mely a külső és belső szabványok, ajánlások és leírások követelményei végrehajtásának megfelelésére irányul.

### 8.5 A hiányosságok kezelése

A vizsgálatok vagy a rendszeres helyszíni ellenőrzések során feltárt esetleges hiányosságokat a Szolgáltató az előírt határidőre megszünteti a vizsgálatot végző szervezettől kapott információ és ajánlások alapján.

### 8.6 Az eredmények közzététele

A Szolgáltató a tanúsítások illetve vizsgálatok végeredményét saját honlapján közzéteszi, amennyiben ezek a publikus szabályzatait és dokumentumait érintik. Ez nem vonatkozik a tanúsítási eljárás során feltárt, az eljárás végeredményét nem befolyásoló hiányosságokra és részeredményekre.

---

<sup>10</sup> [1], [2], [3], [11] és kapcsolódó szabványok és vonatkozó ajánlások

## 9 Egyéb üzleti és jogi kérdések

### 9.1 Díjak

A Szolgáltató meghirdetett díjait előzetes értesítés nélkül bármikor módosíthatja. Bármilyen költség számlázására csak közvetlenül a Szolgáltató jogosult.

**Időbélyegzés szolgáltatási díjak.** A Szolgáltató az időbélyegzés szolgáltatásért díjat számol fel a vonatkozó Szolgáltatói Szerződésben (ISzSz) foglaltak szerint.

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

### 9.2 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 Szerződés szerint fizetendő 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.

További információkat a 9.8 és 9.9 fejezetek tartalmaznak.

A Szolgáltató a vagyoni felelősségre vonhatóság, az általa okozott károkkal kapcsolatos saját felelősség, illetve a neki okozott károkért járó kártérítés megállapíthatósága, dokumentálása és bizonyíthatósága érdekében naplózza tevékenységeit, védi a naplóbejegyzések sértetlenségét és hitelességét, valamint hosszú távon megőrzi (archiválja) a naplóadatokat.

### 9.3 Az üzleti információk bizalmassága

Szolgáltató az általános alapszabályokon túlmenően nem alkalmaz egyedi szabályt erre vonatkozóan.

## 9.4 A személyes adatok védelme

A Szolgáltató a Szolgáltatás keretében a Szolgáltatási Szerződésben, az ahhoz kapcsolódó dokumentációban 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.hu/static-tr/sw/file/adatkezelesi-tajekoztato-honlap.pdf). 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:

<https://www.telekom.hu/static-tr/sw/file/adatkezelesi-tajekoztato-honlap.pdf>

A Szolgáltató a felhasználói adatok megőrzése során gondoskodik az információk **sértetlenségéről**, **bizalmasságáról** és **biztonságos tárolásáról**. Az információkhoz való hozzáférést csak azon személyeknek engedélyezi, akik feladata azt indokolja. Így például a felhasználói adatok papír alapú eredeti példányát (felhasználói szerződés) az adott megrendelésben részt vevő tisztviselő kezeli, másnak át nem adja, másoktól elzárt módon tárolja, majd a megrendelés lezárásával a **Magyar Telekom Technológiai biztonsági központ Katasztrófa Adattárában** (ebben a dokumentumban Adattár) helyezi el végső megőrzésre. Az elektronikus rendszerekben csak azon adatok kerülnek rögzítésre, amelyek az időbélyegzés igénybevételéhez szükségesek. A hozzáférések és jogosultságok kezelésére Szolgáltató külön belső szabállyal rendelkezik (Rendszer Biztonsági Megfelelőség dokumentum), melynek alapján a rendszerek megfelelőségét és a jogosultságkezelési szabályok betartását mind belső, mind pedig külső független auditorok és a Bizalmi Felügyelet ellenőrzi rendszeresen.

A Szolgáltató gondoskodik a nem nyilvános információk **bizalmasságáról** és **sértetlenségéről** a felhasználói adatok továbbítása során, továbbá – megbízható rendszerek alkalmazásával és az adatok rendszeres archiválásával – a megfelelő **rendelkezésre állásról**.

### 9.4.1 Bizalmasan kezelendő információ-típusok

- a) A Szolgáltató bizalmas információként kezeli az előfizető minden adatát, kivéve azokat, amelyeket a Hiba! A hivatkozási forrás nem található. alfejezet tárgyal.
- b) A Szolgáltató bizalmas információként kezeli a következő adatokat és dokumentumokat az előbbieken kívül:
  - nem publikus személyes adatok,
  - magánkulcsok és aktivizáló kódok,
  - szolgáltatási szerződések,
  - tranzakciós és napló adatok,
  - nem nyilvános szabályzatok,
  - minden olyan adat, amelynek nyilvánosságra kerülése a szolgáltatás biztonságát előnytelenül befolyásolná.

### 9.4.2 Információszolgáltatás a hatóságok részére

- a) A Szolgáltató az általa nyújtott bizalmi szolgáltatások felhasználásával elkövetett bűncselekményekkel kapcsolatos büntetőeljárás lefolytatása céljából, vagy nemzetbiztonsági érdekből – az adatigénylésre meghatározott jogszabályi feltételek teljesülése esetén – adatokat továbbít a nyomozó hatóságnak, az ügyészségnek, a bíróságnak és a nemzetbiztonsági szolgálatoknak és egyéb feltételek nélkül feltárja a jogszabályban meghatározott bizalmas információkat az [2] törvény 90.§ (1) és (2) bekezdése szerinti körben.
- b) A Szolgáltató rögzíti az a) pontbeli adatátadás tényét, de arról nem tájékoztatja az előfizetőt.
- c) A Szolgáltató olyan esetben is szolgáltathat információt, amikor egyéb jogszabály(ok) ezt előírják.

### 9.4.3 Információszolgáltatás polgári eljárás keretében

- a) A Szolgáltató a tanúsítvány érvényességét érintő polgári peres, illetve nem peres eljárás során – az érintettség igazolása esetén – az ellenérdekű peres félnek vagy képviselőjének, valamint a megkereső bíróságnak feltárhatja a jogszabályban meghatározott bizalmas felhasználói információkat, illetőleg azokat közölheti a megkereső bírósággal az [2] törvény 90.§ (3) bekezdése szerinti körben.
- b) A Szolgáltató rögzíti az a) pontbeli adatátadás tényét, és arról tájékoztatja az előfizetőt.

#### 9.4.4 A tulajdonos kérésére történő felfedés

A Szolgáltató az előfizető hivatalos – írásban adott – felhatalmazása alapján tárja fel a rájuk vonatkozó bizalmas felhasználói információkat harmadik fél részére.

### 9.5 Szellemi tulajdonjogok

- a) A Szolgáltató szabályzatai, szerződéses feltételei Szolgáltató tulajdonát képezik.
- b) A **visszavonási információ** a Szolgáltató tulajdonát képezi.

### 9.6 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 végzik<sup>11</sup>.
- 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.

#### 9.6.1 Az időbélyegzés szolgáltató felelőssége és helytállása

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

---

<sup>11</sup> Az időbélyegzés-szolgáltató általánosan felelős az időbélyegző szervezet, valamint a címtár kötelezettségeiért, tevékenységeiért.

## 9.6.2 Az előfizető felelőssége és helytállása

Az előfizető felelős:

- a Szolgáltatási Szerződés betartásáért,
- 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),
- a kötelezettségei betartásáért.

## 9.6.3 Az érintett fél felelőssége

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 körültekintő eljárásért.

## 9.7 Helytállás érvénytelenségi köre

Szolgáltató nem alkalmaz különleges szabályokat erre vonatkozóan.

## 9.8 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 ÁSzF dokumentum 15. pontja tartalmazza.

## 9.9 Kártérítési kötelezettségek

A Szolgáltató a felelősségi körén belül keletkezett, bizonyított károkért a szabályzataiban és az előfizetővel megkötött szolgáltatási szerződésekben valamint az előző pontban rögzített korlátozásokkal kártérítést fizet.

Az előfizető kártérítési felelősséggel tartoznak a Szolgáltatóval szemben azokért a veszteségekért és károkért, melyeket kötelezettségeik be nem tartásával okoznak számára.

## 9.10 Érvényesség

Jelen szabályzat időbeli hatályát az 1.1.2 pont tartalmazza.

Amennyiben a Szabályzat valamely pontja érvénytelen lenne, az a Szabályzat egészének és más pontjainak érvényességét nem érinti.

A Szabályzat a Közösség valamennyi kötelezettségét, felelősségét és jogát tartalmazza. A Szabályzat egyetlen pontja sem értelmezhető a jelen dokumentumba foglalt értelmezéstől eltérően, bármely más szerződés vagy szabályzat, írott vagy szóbeli kommunikáció következtében, beleértve a Szolgáltató és más szervezet jövőbeli esetleges összeolvadásának esetét is. A Szabályzat csak írott és hitelesített formában módosítható, a Bizalmi Felügyelet által vezetett szabályzat-nyilvántartásban való átvezetés mellett.

## 9.11 A felek közötti kommunikációra vonatkozó előírások

Az előfizető jognyilatkozatait Szolgáltató felé kizárólag írásban, hivatalosan aláírt módon teheti meg. Az előfizető egyéb esetekben a Szolgáltatót írásban, elektronikus levél vagy fax formájában is értesítheti. A Szolgáltató értesítési címei jelen szabályzat 1.1.3 és 1.3.1 alfejezetében találhatóak.

## 9.12 Diszkrimináció mentesség

Elkötelezetten hisszük, hogy a digitalizációnak fontos szerepe van az akadálymentes mindennapok megteremtésében. Munkáltatóként alapvető igényünk, hogy fizikai és digitális munkakörnyezetünk kényelmes és jól használható legyen fogyatékkal élő és megváltozott munkaképességű munkavállalóink számára.

- Akadálymentes üzleteink
- Akadálymentes szolgáltatás
- Fogyatékoságbarát-Munkahely
- GARI (Global Accessibility Reporting Initiative)

A szolgáltató diszkrimináció mentes eljárására vonatkozó nyilatkozat elérhetőségei:

<https://www.telekom.hu/rolunk/fenntarthatosag/sokszinuseg-eselyegyenloseg/kulturank-es-ertekeink>

<https://www.telekom.hu/rolunk/fenntarthatosag/sokszinuseg-eselyegyenloseg/akadalymentes-telekom>

## 9.13 Kiegészítések

Szolgáltató nem alkalmaz különleges szabályokat erre vonatkozóan.



## 9.14 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 megkísérlik békés, tárgyalásos úton rendezni.

A Szolgáltató (beleértve az Időbélyegző Szervezetet is) tevékenységével kapcsolatos kérdéseket, kifogásokat és panaszokat az 1.3.1. alfejezetben rögzített Időbélyegző Szervezetre vonatkozó elérhetőségeken lehet megtenni.

Az eljárás további részleteit az **ÁSZF** dokumentum 18. pontja tartalmazza.

## 9.15 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.

## 9.16 Az érvényben lévő jogszabályoknak való megfelelés

A legfontosabb jogszabályok felsorolását az Időbélyegzési Rend tartalmazza.