

# Általános Időbélyegzési Rend



**NetLock Informatikai és Hálózatbiztonsági Korlátolt Felelősségű Társaság**

Nyilvántartási szám (OID): ----- 1.3.6.1.4.1.3555.1.16.20080107

A Szabályzat hatályának kezdőnapja: ----- 2008. január 7.

OLDALAK SZÁMA: ----- 14, AZAZ TIZENNÉGY

© COPYRIGHT 2002, NETLOCK KFT. ----- MINDEN JOG FENNTARTVA

Jóváhagyta: ----- Rózsahegyi Zsolt ügyvezető

Jóváhagyás dátuma: ----- 2008. január 7.

Jóváhagyom: .....

PH.

| OID                            | Változás leírása  | Készítő   | Ellenőrző        |
|--------------------------------|---|---|------------------|
| 1.3.6.1.4.1.3555.1.16.20060728 | Első nyilvános változat   | Dr. Szentirmai László                           | Dr. Nagy Zsolt   |
| 1.3.6.1.4.1.3555.1.16.20060828 | Hivatali észrevételek alapján történt pontosítás  | NetLock Szabályzat<br>Elfogadó Egység<br>(SZEE) | Rózsahegyi Zsolt |
| 1.3.6.1.4.1.3555.1.16.20060907 | Hivatali észrevételek alapján történt pontosítás<br>(időbélyeg szolgáltatás külön szolgáltatásként is<br>nyújtható) | NetLock Szabályzat<br>Elfogadó Egység<br>(SZEE) | Rózsahegyi Zsolt |
| 1.3.6.1.4.1.3555.1.16.20071114 | Cím módosítása, általánosság biztosítása<br>érdekében szükséges módosítások   | NetLock Szabályzat<br>Elfogadó Egység<br>(SZEE) | Dr. Nagy Zsolt   |
| 1.3.6.1.4.1.3555.1.16.20080107 |   | NetLock Szabályzat<br>Elfogadó Egység<br>(SZEE) | Dr. Nagy Zsolt   |

## Hivatkozások

Jelen dokumentum az alábbi dokumentumokra hivatkozik:

[1] 2001. évi XXXV. Törvény az elektronikus aláírásról

[2] 3/2005. (III. 18.) IHM rendelet az elektronikus aláírásokkal kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről.

[3] ETSI TS 102 023 v1.2.1 (2003-01) Policy requirements for time-stamping authorities

[4] ETSI TS 101 861 v1.1.1 (2001-08) Time Stamping Profile

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

# Tartalomjegyzék

|  |           |
|--|-----------|
| <b>Általános Időbélyegzési Rend</b> .....  | <b>1</b>  |
| <b>NetLock Informatikai és Hálózatbiztonsági Korlátolt Felelősségű Társaság</b> .....  | <b>1</b>  |
| <b>1 Bevezetés</b> .....   | <b>6</b>  |
| <b>1.1 Áttekintés</b> .....  | <b>6</b>  |
| <b>1.2 Azonosítás</b> .....  | <b>6</b>  |
| <b>1.3 Közösség</b> .....  | <b>6</b>  |
| 1.3.1 Időbélyegzés-szolgáltató.....  | 6         |
| 1.3.2 Igénybevevők.....  | 6         |
| <b>1.4 Kapcsolattartás</b> .....   | <b>7</b>  |
| <b>1.5 Az Időbélyegzési Rend és a Szolgáltatási Szabályzat kapcsolata</b> .....        | <b>7</b>  |
| <b>2 Időbélyegzési rend</b> .....  | <b>8</b>  |
| <b>2.1 Áttekintés</b> .....  | <b>8</b>  |
| <b>2.2 Megfelelés</b> .....  | <b>8</b>  |
| <b>3 Kötelezettségek és felelősségek</b> .....   | <b>9</b>  |
| <b>3.1 Az időbélyegzés-szolgáltató kötelezettségei</b> .....                           | <b>9</b>  |
| 3.1.1 Általános kötelezettségek .....  | 9         |
| 3.1.2 Időbélyegzés-szolgáltató kötelezettségei a felhasználóval szemben .....          | 9         |
| <b>3.2 Felhasználó kötelezettségei</b> .....   | <b>9</b>  |
| <b>3.3 Javaslatok az érintett fél számára</b> .....                                    | <b>9</b>  |
| <b>3.4 Felelősség</b> .....  | <b>9</b>  |
| <b>4 Működésre vonatkozó követelmények</b> .....                                       | <b>10</b> |
| <b>4.1 Szolgáltatási és közzétételi szabályozás</b> .....                              | <b>10</b> |
| <b>4.2 Közzétételi nyilatkozat</b> .....   | <b>10</b> |
| <b>4.3 Kulcsmenedzsment</b> .....  | <b>10</b> |
| 4.3.1 Időbélyegzés-szolgáltatás szolgáltatói kulcspárjának generálása .....            | 10        |
| 4.3.2 Időbélyegzés-szolgáltatás szolgáltatói aláíró kulcsának védelme.....             | 11        |
| 4.3.3 Időbélyegzés-szolgáltatás szolgáltatói nyilvános kulcsának közzététele .....     | 11        |
| 4.3.4 Tanúsítvány élettartama.....   | 11        |
| 4.3.5 Időbélyegzés-szolgáltatás szolgáltatói aláíró kulcsának használatának vége ..... | 11        |
| 4.3.6 Az alkalmazott kriptográfiai modul életciklusa.....                              | 11        |
| <b>4.4 Időbélyegzés-szolgáltatás</b> .....   | <b>11</b> |
| 4.4.1 Időbélyeg .....  | 11        |
| 4.4.2 Óraszinkronizálás.....   | 12        |
| <b>4.5 Az időbélyegzés-szolgáltatás menedzsmentje</b> .....                            | <b>12</b> |
| 4.5.1 Biztonsági intézkedések.....   | 12        |
| 4.5.2 Rendszerelemek osztályba sorolása.....   | 12        |
| 4.5.3 Személyzeti biztonság .....  | 12        |
| 4.5.4 Fizikai biztonság .....  | 12        |

|            |   |           |
|------------|---|-----------|
| 4.5.5      | Üzemeltetés menedzsment.....                                    | 12        |
| 4.5.6      | Hozzáférés-menedzsment .....                                    | 12        |
| 4.5.7      | Rendszer telepítése és karbantartása.....                       | 13        |
| 4.5.8      | Az időbélyegzés-szolgáltató leállítása .....                    | 13        |
| 4.5.9      | Jogszabályi megfelelés .....                                    | 13        |
| 4.5.10     | Időbélyegzés-szolgáltatással kapcsolatos adatok naplózása ..... | 13        |
| <b>5</b>   | <b><i>Melléklet</i></b> .....                                   | <b>14</b> |
| <b>5.1</b> | <b>Szolgáltatói (időbélyegző) tanúsítványok profilja</b> .....  | <b>14</b> |
| <b>5.2</b> | <b>Időbélyeg-profil</b> .....                                   | <b>14</b> |

# 1 Bevezetés

Jelen dokumentum célja, hogy egy időbélyegzési rendként összefoglalja mindazon minimum követelményeket, amelyek az időbélyegzési szolgáltatás igénybevételére és a kibocsátott időbélyeg ellenőrzésére vonatkoznak. Ezen időbélyegzési rendet alkalmazó szolgáltatók a jelen dokumentumban nem szabályozott kérdésekben szolgáltatási szabályzatuknak megfelelően járnak el.

## 1.1 Áttekintés

Az időbélyegzési rend szabálygyűjtemény, mely az időbélyegzés szolgáltatásra vonatkozó követelményeket határozza meg egy közös biztonsági követelményekkel rendelkező közösség és/vagy alkalmazások egy osztálya számára. A dokumentum tartalmi vonatkozásokban eleget tesz az [1] Elektronikus aláírás törvény, és egyéb hazai jogszabályok ([2]) előírásainak és ajánlásainak, és felhasználja az [3] ETSI követelményeket, valamint egyéb nemzetközi ajánlásokat.

A szabályokra vonatkozó követelményeit jelen dokumentum időbélyegzési rend formájában határozza meg. A jelen dokumentumnak megfelelően kibocsátott időbélyegek tartalmaz(hat)nak egy időbélyegzési rend azonosítót (OID-t), amelyet az érintett felek arra használhatnak, hogy meghatározzák a tanúsítványok alkalmazhatóságát és megbízhatóságát egy adott alkalmazás tekintetében.

## 1.2 Azonosítás

Jelen dokumentum:

- Teljes neve: NetLock Kft. Általános Időbélyegzési Rendje
- Rövid neve: Általános Időbélyegzési Rend
- Verziószáma: a fedőlapon található verziószám

A Szabályzat hivatalos és aktuális verziója megtalálható és letölthető:

- Szolgáltató Internetes oldalairól: [www.netlock.hu](http://www.netlock.hu)

## 1.3 Közösség

### 1.3.1 Időbélyegzés-szolgáltató

Az időbélyegzés-szolgáltatást csak a hatályos jogszabályok alapján nyilvántartásba vett szolgáltató nyújthat.

### 1.3.2 Igénybevevők

A szolgáltatások nyilvánosak legyenek, vagyis az alábbi korlátozásokkal bárki lehessen igénybevevő:

- felhasználó: tetszőleges természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki/amely az időbélyeg-szolgáltatást igénybe veszi,
- érintett fél: tetszőleges természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki/amely elfogadja az időbélyeg-szolgáltatás során kibocsátott időbélyegeket és elfogadja a Szolgáltatási Szabályzatban az érintett fél számára javasolt eljárásokat. Az érintett fél szerződéses kapcsolatban nem áll az időbélyegzés-szolgáltatóval.

## **1.4 Kapcsolattartás**

*A hitelesítés-szolgáltató adatai:*

Az időbélyegzés-szolgáltató kapcsolattartáshoz szükséges adatait a Szolgáltatási Szabályzatában ismertesse.

*Szabályzatért felelős egység:*

A szabályzatokkal kapcsolatos kérdésekkel és észrevételekkel közvetlenül a szabályzatért felelős egység legyen megkereshető.

## **1.5 Az Időbélyegzési Rend és a Szolgáltatási Szabályzat kapcsolata**

Az Időbélyegzési Rend a Szolgáltató által nyújtott időbélyegzési szolgáltatásra vonatkozó általános követelményeket előírásokat tartalmazza. Az időbélyegzés-szolgáltató a szolgáltatási szabályzatában határozza meg ezen általános előírásoknak való konkrét megfelelést és a követelmények gyakorlati teljesítését.

Ennek megfelelően az Időbélyegzési Rend legyen összhangban a szolgáltató által kibocsátott szolgáltatási szabályzattal, az általános szerződési feltételekkel, illetve egyéb, a szolgáltató belső működését szabályozó dokumentumokkal.

## 2 Időbélyegzési rend

### 2.1 Áttekintés

Az időbélyegzés-szolgáltatást az időbélyegzés-szolgáltatóval szerződéses kapcsolatban levő természetes vagy jogi személy veheti igénybe.

A szolgáltatás során az időbélyegzés-szolgáltató által kibocsátott időbélyeg feleljen meg az ETSI [4] és az X.509 szabványrendszer [5] időbélyegzésre vonatkozó előírásainak. Az időbélyegzés során a felhasználó által időbélyegezni kért dokumentum lenyomatát, illetve az időbélyeg-kibocsátás időpontját az időbélyegzés-szolgáltató a saját szolgáltatói tanúsítványában foglalt nyilvános kulcs magán párjával elektronikusan írja alá.

### 2.2 Megfelelés

Az időbélyegzés-szolgáltató feleljen meg hatályos vonatkozó jogszabályi előírásoknak, nemzetközi szabványoknak és saját belső szabályzatainak. Az említett előírásoknak való folyamatos és pontos megfelelést rendszeresen, külső és belső auditorok által végzett vizsgálatok biztosítsák.

## 3 Kötelezettségek és felelősségek

### 3.1 Az időbélyegzés-szolgáltató kötelezettségei

#### 3.1.1 Általános kötelezettségek

Az időbélyegzés-szolgáltató vállaljon kötelezettséget arra, hogy szolgáltatása során betartja a hatályos vonatkozó jogszabályi előírásokat és nemzetközi szabványokat és működését a Szolgáltatási Szabályzatban meghatározott módon végezze.

A szolgáltatás részletes leírását és körülményeit elsősorban a felhasználóval kötött szolgáltatási szerződés, ezenkívül az általános szerződési feltételek, illetve a szolgáltatási szabályzat tartalmazza.

#### 3.1.2 Időbélyegzés-szolgáltató kötelezettségei a felhasználóval szemben

Az időbélyegzés-szolgáltató a következő kötelezettségeket vállalja a felhasználóval szemben:

- Az időbélyegzés-szolgáltató a felhasználótól érkező kérésekre időbélyeget bocsát ki. A kibocsátott időbélyeg a felhasználó által küldött lenyomatot és egyedi sorozatszámot változatlan formában tartalmazza, elektronikusan aláírva.
- Az időbélyegzés-szolgáltató nem ismerheti meg az időbélyeggel ellátott dokumentum tartalmát, mivel hozzá a felhasználó kérésére csak a dokumentum lenyomata kerül.
- Az időbélyeget 1 másodperc pontossággal kell kiadnia. Ennek megfelelően az időbélyegzés-szolgáltatónak a belső óráját megfelelő pontossággal kell szinkronizálnia az UTC időalaphoz és gondoskodnia kell a pontosság folyamatos fenntartásáról.
- Az időbélyegzés-szolgáltatás biztonságát és megbízhatóságát a szolgáltatókra (minősített, nem minősített) vonatkozó követelmények szerint kell biztosítani.
- Az időbélyegzés-szolgáltatónak az időbélyegzési eljárással kapcsolatos összes fontos, de legalább a jogszabályokban meghatározott eseményeket rögzítenie kell, a napló állományokat pedig jogszabályi előírásoknak megfelelően biztonságosan archiválnia kell.

### 3.2 Felhasználó kötelezettségei

A felhasználó kötelezettségeit az időbélyegzés-szolgáltatóval kötött szolgáltatási szerződés, az általános szerződési feltételek, valamint a szolgáltatási szabályzat tartalmazza.

### 3.3 Javaslatok az érintett fél számára

Az érintett félnek a tőle elvárható gondosság érdekében javasolt ellenőrizni az időbélyegen szereplő aláírás helyességéről és az időbélyegzés-szolgáltató szolgáltatói aláíró kulcsának érvényességét a Szolgáltatási Szabályzatban meghatározott módon.

### 3.4 Felelősség

Nincs külön előírás, a közösség (lásd 1.3 pont) tagjainak felelősségét a Szolgáltató saját szolgáltatási szabályzatában kell meghatározni.

## 4 Működésre vonatkozó követelmények

### 4.1 Szolgáltatási és közzétételi szabályozás

Az időbélyegzés-szolgáltató az időbélyegzés-szolgáltatást biztonságos fizikai, szabályozási és személyi környezetben nyújtja. Ezen rendszer feleljen meg a jogszabályok által előírt, az időbélyegzés-szolgáltatókra vonatkozó követelményeknek is.

### 4.2 Közzétételi nyilatkozat

Az időbélyegzés-szolgáltató tegye közzé a szolgáltatással kapcsolatos információkat és dokumentumokat.

Továbbiakban az alábbi tartalmú nyilatkozatot tegye meg az időbélyegzés-szolgáltatással kapcsolatban:

- Az időbélyegzési szolgáltatás szolgáltatói tanúsítványát közzé kell tennie.
- Időbélyegzés során csak a Nemzeti Hírközlési Határozat jogerős határozatában közzétett lenyomatképző algoritmusokat használhatja.
- Az időbélyegben szereplő idő pontosságának az UTC-hez képest 1 másodpercen belül kell lennie.
- A szolgáltatás nyújtásának feltétele a felhasználóval megkötött szolgáltatási szerződés.
- Az érintett félnek a tőle elvárható gondosság érdekében javasolt meggyőződnie az időbélyegen szereplő aláírás helyességéről és az időbélyegzés-szolgáltató szolgáltatói aláíró kulcsának érvényességéről a Szolgáltatási Szabályzatban előírtaknak megfelelően.
- Az időbélyegzés-szolgáltatás nyújtása során keletkezett archivált naplóállományokat az időbélyegzés-szolgáltatónak a keletkezésüktől számított legalább 10 évig, illetve a velük kapcsolatban esetlegesen felmerült vita jogerős lezárásáig meg kell őriznie.
- Az időbélyegzés-szolgáltató az eljárása során különösen az alábbi jogszabályoknak való megfelelést kell vállalnia:

2001:XXXV. törvény az elektronikus aláírásról

3/2005 (III. 18.) IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről.

- Az esetleges viták rendezése az általános szerződési feltételek vonatkozó rendelkezései szerint történik.
- A minősített időbélyegzés-szolgáltató hatályos jogszabályoknak és előírásoknak való megfelelést a Nemzeti Hírközlési Hatóság rendszeresen vizsgálja.

### 4.3 Kulcsmenedzsment

#### 4.3.1 Időbélyegzés-szolgáltatás szolgáltatói kulcspárjának generálása

Az időbélyegzés-szolgáltató a kulcselőállítás olyan eszközön belül hajtsa végre, amely kellően biztonságos és megfelel a jogszabályi előírásoknak, azaz rendelkezik a kijelölt tanúsító szervezet által kibocsátott, megfelelő tanúsítvánnyal és szerepel a Nemzeti Hírközlési Hatóság nyilvántartásában.

### 4.3.2 Időbélyegzés-szolgáltatás szolgáltatói aláíró kulcsának védelme

Az időbélyegzés-szolgáltató az aláíró kulcsot olyan eszközben tárolja, amely kellően biztonságos és megfelel a jogszabályi előírásoknak, azaz rendelkezik a kijelölt tanúsító szervezet által kibocsátott, megfelelő tanúsítvánnyal és szerepel a Nemzeti Hírközlési Hatóság nyilvántartásában.

### 4.3.3 Időbélyegzés-szolgáltatás szolgáltatói nyilvános kulcsának közzététele

Az időbélyegzés-szolgáltatón az időbélyegzés-szolgáltatás szolgáltatói nyilvános kulcsát tegye közzé.

### 4.3.4 Tanúsítvány élettartama

Az időbélyegzés-szolgáltatás szolgáltatói tanúsítványának érvényességi ideje maximum 5 év.

### 4.3.5 Időbélyegzés-szolgáltatás szolgáltatói aláíró kulcsának használatának vége

Az időbélyegzés-szolgáltató vissza kell vonnia és meg kell semmisítenie az aláíró kulcsot az alábbi esetekben:

- A kulcs és tanúsítványa érvényessége lejár
- A kulcs kompromittálódik
- Időbélyegzés-szolgáltató egyéb okból visszavonja és megsemmisíti a kulcsot és a tanúsítványt

### 4.3.6 Az alkalmazott kriptográfiai modul életciklusa

Az időbélyegzés-szolgáltató gondoskodjon az időbélyegzés-szolgáltatás szolgáltatói kulcsait tartalmazó kriptográfiai hardvereszköz biztonságos kezeléséről és tárolásáról a modul teljes életciklusa alatt. A modul szállítására, telepítésére és üzembe helyezésére szigorú biztonsági feltételek közt kerülhet sor.

Amennyiben a modul kikerül az időbélyegzés-szolgáltató rendszeréből, előtte a benne tárolt kulcsokat meg kell semmisíteni.

## 4.4 Időbélyegzés-szolgáltatás

### 4.4.1 Időbélyeg

Az időbélyegzés-szolgáltató által kibocsátott időbélyeg feleljen meg a vonatkozó jogszabályoknak, az RFC 3161 [5] előírásainak, valamint jelen időbélyegzési rend előírásainak, így különösen:

- Ugyanazon lenyomatot kell tartalmaznia, melyet a felhasználó kérelemként beküldött.
- Tartalmaznia kell az időbélyegzési rend OID azonosítóját,
- Egyedi azonosítószámot kell tartalmaznia.
- Az aláírásra használt szolgáltatói kulcsot az időbélyegzés-szolgáltató más célra nem használhatja.
- Az időbélyegben megadott időpontot az időbélyegzés-szolgáltató belső rendszere adja, melyet minimum 3, egymástól független, az UTC idővel szinkronizált időforrásnak kell kiszolgáltatnia. Ezen időforrások több, mint felének Stratum 1-es szintűnek kell lennie. Ennek során az időbélyegzés-szolgáltatónak garantálnia kell, hogy

belső órája 0,1 másodperces pontossággal szinkronizálja az UTC időalaphoz, és a kibocsátott időbélyegek pontossága legfeljebb 1 másodperccel tér el az UTC időalaptól.

#### **4.4.2 Óraszinkronizálás**

Az időbélyegzés-szolgáltató szinkronizálja az időbélyegzés-szolgáltatás során használt belső óráját az UTC-hez és garantálja, hogy a belső órája maximum 0,1 másodperces eltérését az UTC-től.

### **4.5 Az időbélyegzés-szolgáltatás menedzsmentje**

#### **4.5.1 Biztonsági intézkedések**

Az időbélyegzés-szolgáltató az időbélyegzés-szolgáltatást biztonságos fizikai, szabályozási és személyi környezetben nyújtja. Ezen rendszer feleljen meg a jogszabályok által előírt, az időbélyegzés-szolgáltatókra vonatkozó követelményeknek is. A részletes biztonsági intézkedéseket a cég belső használatú szabályzatai tartalmazzák.

#### **4.5.2 Rendszerelemek osztályba sorolása**

Az időbélyegzés-szolgáltató végezzen kockázatelemzést az üzleti kockázatainak felmérésére, széleskörűen figyelembe véve a szolgáltatásokat, adatokat, eszközöket, információkat fenyegető veszélyforrásokat. A kockázatelemzés eredménye alapján határozza meg a szükséges biztonsági követelményeket és a működési eljárásokat annak érdekében, hogy a felmerülő kockázatokat az elfogadható szintre szorítsa vissza.

#### **4.5.3 Személyzeti biztonság**

A személyzeti biztonságra vonatkozó követelmények feleljenek meg a hitelesítés-szolgáltatókra vonatkozó, hatályos jogszabályi előírásoknak.

#### **4.5.4 Fizikai biztonság**

A fizikai biztonságra vonatkozó követelmények feleljenek meg a hitelesítés-szolgáltatókra vonatkozó, hatályos jogszabályi előírásoknak.

#### **4.5.5 Üzemeltetés menedzsment**

Az üzemeltetés menedzsmentre vonatkozó követelmények feleljenek meg a hitelesítés-szolgáltatókra vonatkozó, hatályos jogszabályi előírásoknak. Ezeket részletesen az időbélyegzés-szolgáltató belső, társasági szintű előírásai tartalmazzák.

Az időbélyegzés-szolgáltató rendelkezzen minőségirányítási rendszerrel, illetve információbiztonsági irányítási rendszerrel, vagy annak megfelelő szabályozással kell rendelkeznie.

#### **4.5.6 Hozzáférés-menedzsment**

Az időbélyegzés-szolgáltató által alkalmazott hozzáférés-menedzsment feleljen meg a hitelesítés-szolgáltatói követelményeknek. Ezen szabályokat a szolgáltatási szabályzatnak, valamint egyéb belső használatú szabályzatoknak kell tartalmaznia.

#### **4.5.7 Rendszer telepítése és karbantartása**

Az időbélyegzés-szolgáltató csak megbízható forrásból származó termékeket és rendszereket használjon és gondoskodjon arról, hogy védve legyenek a jogosulatlan hozzáférésekkel és módosításokkal szemben. Az erre vonatkozó előírásokat a társaság belső szabályzatai tartalmazzák.

Az időbélyegzés-szolgáltató kockázatelemzés keretében folyamatosan mérje a szolgáltató rendszerét érő fizikai és személyi veszélyeket és ennek megfelelően intézkedik a lehetséges kockázatok minimalizálása érdekében.

Az időbélyegzés-szolgáltató rendszereiben telepítést, fejlesztést vagy karbantartást végezni csak megfelelően dokumentált változásmenedzsment eljárások keretében lehet.

#### **4.5.8 Az időbélyegzés-szolgáltató leállítása**

Az időbélyegzés-szolgáltató leállítására a hitelesítés-szolgáltató leállítására vonatkozó szabályok legyenek az irányadóak, a két szolgáltatás eltérő jellegzetességei figyelembevételével. A leállításról a Szolgáltató Szolgáltatási Szabályzatában nyilatkozzon.

#### **4.5.9 Jogsabályi megfelelés**

A jogsabályi megfelelés tekintetében a közzétételi nyilatkozatnál (lásd 4.2 pont) leírtak az irányadóak.

#### **4.5.10 Időbélyegzés-szolgáltatással kapcsolatos adatok naplózása**

Az időbélyegzés-szolgáltató a szolgáltatás során az alábbi adatokat rögzítse:

- Az időbélyegzés lépései
- Az időbélyegzés-szolgáltatás szolgáltatói kulcspárjával és tanúsítványával kapcsolatos események

## 5 Melléklet

Az időbélyegzés-szolgáltató időbélyegző tanúsítványának, illetve az időbélyegkérelem és –válasz feleljen meg az alábbi előírásoknak.

### 5.1 Szolgáltatói (időbélyegző) tanúsítványok profilja

| Mező                   | Tartalom   |
|------------------------|--|
| Common Name            | Az időbélyegző tanúsítvány megnevezése   |
| Organization           | Az időbélyegzés-szolgáltató neve   |
| Organization Unit      | Az időbélyegzés-szolgáltató szervezeti egységének neve                                       |
| Country                | HU   |
| Locality               | Az időbélyegzés-szolgáltató székhelye szerinti város   |
| State                  | - (üres)   |
| E-mail                 | - (üres)   |
| Public Key             | Időbélyegző tanúsítvány nyilvános kulcsa   |
| basic Constraints      | cA = FALSE (kritikus kiterjesztes)   |
| keyUsage               | NonRepudiation (kritikus kiterjesztes)   |
| extendedKeyUsage       | timeStamping (kritikus kiterjesztes)   |
| További kiterjesztések | Egyéb kiterjesztések meghatározhatóak  |
| Version                | V3   |
| Serial number          | Egyedi sorozatszám érték   |
| Validity               | Érvényesség kezdete és vége  |
| Issuer                 | Szolgáltatói (időbélyegző) tanúsítvány aláírására használt szolgáltatói főtanúsítvány adatai |
| Signature              | sha1RSA  |

### 5.2 Időbélyeg-profil

| Mezők, tulajdonságok  | Tartalom, értelmezés   |
|---|--|
| Időbélyeg kérelemben engedélyezett hash algoritmus                  | SHA-1 vagy RIPEMD160   |
| Időbélyeg kérelemben megnevezhető szabályzati azonosító (OID)       | Üresen hagyható vagy a kért szabályzat azonosítója   |
| Időbélyeg kérelemben szereplő véletlen szám (nonce) hossza          | Maximum 64 bit   |
| Időbélyeg kérelemben kérhető-e a szolgáltató tanúsítványa (certReq) | Igen   |
| Időbélyeg válaszban szereplő szabályzati azonosító (OID)            | A kért szabályzat azonosítója  |
| Az időbélyeg válasznál használt hash algoritmus                     | SHA1 vagy RIPEMD160  |
| Az időbélyeg válasznál használt aláíró algoritmus                   | RSA  |
| Kiterjesztések  | Szolgáltató által meghatározott  |
| Verzió  | V1   |
| Sorszám mérete  | Dinamikus hosszúságú   |
| Sorszám egyedisége  | Az időbélyegzőben használt sorszám egyedi a Szolgáltatóra nézve. Ez a tulajdonság ésszerű keretek között fennmarad a szolgáltatás lehetséges megszakadása után is. |