MICROSEC

e-Szignó Hitelesítés Szolgáltató

eIDAS Rendelet szerinti nem minősített időbélyegzés-szolgáltatás szolgáltatási szabályzat

ver. 2.11 * 2019-08-05

Hatálybalépés: 2019-09-25 [1]

Azonosító	1.3.6.1.4.1.21528.2.1.1.202.2.11 * 2019-08-05
Verzió	2.11 * 2019-08-05
Első verzió hatálybalépése	2017-09-30
Biztonsági besorolás	TERVEZET
Jóváhagyta	Vanczák Gergely
Jóváhagyás dátuma	2019-08-02
Hatálybalépés dátuma	2019-09-25 [2]

Microsec Számítástechnikai Fejlesztő zártkörűen működő Részvénytársaság
1033 Budapest, Ángel Sanz Briz út 13. C. épület

Verzió	A változás leírása	Hatálybalépés	Készítette
2.4	eIDAS követelmények szerinti első önálló nem fokozott időbélyegzési szabályzat.	2017-09-30	Dr. Szőke Sándor
2.5	Módosítások az NMHH észrevételei alapján.	2017-11-01	Dr. Szőke Sándor
2.7	Éves felülvizsgálat.	2018-09-15	Dr. Szőke Sándor
2.8	Változások az auditor javaslatai alapján.	2018-12-14	Dr. Szőke Sándor
2.11	Éves felülvizsgálat.	2019-09-25	Dr. Szőke Sándor

Tartalomjegyzék

1. Bevezetés **10**
1.1. Áttekintés . . . 10
1.2. Dokumentum neve és azonosítója . . . 10
1.2.1. A dokumentum főbb azonosító adatai . . . 10
1.2.2. Megfelelés . . . 11
1.2.3. Hatály . . . 11
1.2.4. Időbélyegzési rend . . . 11
1.3. PKI szereplők . . . 11
1.3.1. Szolgáltató . . . 11
1.3.2. Ügyfelek . . . 13
1.3.3. Érintett felek . . . 13
1.4. Az időbélyegző felhasználhatósága . . . 13
1.5. A dokumentum adminisztrálása . . . 13
1.5.1. A dokumentum adminisztrációs szervezete . . . 13
1.5.2. Kapcsolattartó személy . . . 14
1.5.3. A Szolgáltatási szabályzat *Nem minősített időbélyegzési rend*nek való megfelelőségéért felelős személy/szervezet . . . 14
1.5.4. A Szolgáltatási szabályzat elfogadási eljárása . . . 14
1.6. Fogalmak és rövidítések . . . 14
1.6.1. Fogalmak . . . 14
1.6.2. Rövidítések . . . 19

2. Közzététel és tanúsítványtár **19**
2.1. Adatbázisok - tanúsítványtárak . . . 19
2.2. A tanúsítványokra vonatkozó információk közzététele . . . 19
2.2.1. Szolgáltatói információ közzététele . . . 19
2.3. A közzététel időpontja vagy gyakorisága . . . 20
2.3.1. Kikötések és feltételek közzétételi gyakorisága . . . 20

3. Az Időbélyegző egység tanúsítványa és az Időbélyegzés **20**
3.1. A felhasználó azonosítása . . . 20
3.2. Az Időbélyegző egység tanúsítványa . . . 20
3.3. Az Időbélyegző . . . 21
3.3.1. Időbélyegző kérés . . . 21
3.3.2. Időbélyegző válasz . . . 22
3.4. Az Időbélyegzőben szereplő idő pontossága . . . 24
3.5. Óraszinkronizálás . . . 25
3.5.1. A szökőmásodpercek kezelése . . . 25

3.5.2. Nyári időszámítás kezelése . . . 25
3.6. Az Időbélyegző ellenőrzése . . . 25
3.7. A szolgáltatás rendelkezésre állása . . . 26
3.8. Nem minősített időbélyegzők kibocsátása . . . 26
3.9. Az Időbélyegző egység kulcshasználata . . . 26
3.10. Az Időbélyegző szolgáltatás elérési módjai . . . 26

4. A tanúsítványok életciklusára vonatkozó követelmények 27
4.1. A kulcspár és a tanúsítvány használata . . . 27
4.1.1. A magánkulcs és a tanúsítvány használata . . . 27
4.1.2. Az Érintett felek nyilvános kulcs és tanúsítvány használata . . . 27

5. Elhelyezési, eljárásbeli és üzemeltetési előírások 27
5.1. Fizikai követelmények . . . 27
5.1.1. A telephely elhelyezése és szerkezeti felépítése . . . 28
5.1.2. Fizikai hozzáférés . . . 28
5.1.3. Áramellátás és légkondicionálás . . . 29
5.1.4. Beázás és elárasztódás veszély kezelése . . . 29
5.1.5. Tűz megelőzés és tűzvédelem . . . 30
5.1.6. Adathordozók tárolása . . . 30
5.1.7. Hulladék megsemmisítése . . . 30
5.1.8. A mentési példányok fizikai elkülönítése . . . 30
5.2. Eljárásbeli előírások . . . 31
5.2.1. Bizalmi szerepkörök . . . 31
5.2.2. Az egyes feladatok ellátásához szükséges személyzeti létszámok . . . 32
5.2.3. Az egyes szerepkörökben elvárt azonosítás és hitelesítés . . . 32
5.2.4. Egymást kizáró szerepkörök . . . 32
5.3. Személyzetre vonatkozó előírások . . . 33
5.3.1. Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények . . . 33
5.3.2. Előélet vizsgálatára vonatkozó eljárások . . . 34
5.3.3. Képzési követelmények . . . 34
5.3.4. Továbbképzési gyakoriságok és követelmények . . . 35
5.3.5. Munkabeosztás körforgásának sorrendje és gyakorisága . . . 35
5.3.6. Felhatalmazás nélküli tevékenységek büntető következményei . . . 35
5.3.7. Szerződéses viszonyban foglalkoztatottakra vonatkozó követelmények . . . 35
5.3.8. A személyzet számára biztosított dokumentációk . . . 36
5.4. Naplózási eljárások . . . 36
5.4.1. A tárolt események típusai . . . 36
5.4.2. A naplófájl feldolgozásának gyakorisága . . . 39

5.4.3. A naplófájl megőrzési időtartama . . . 39
5.4.4. A naplófájl védelme . . . 39
5.4.5. A naplófájl mentési eljárásai . . . 40
5.4.6. A naplózás adatgyűjtési rendszere . . . 40
5.4.7. Az eseményeket kiváltó alanyok értesítése . . . 40
5.4.8. Sebezhetőség felmérése . . . 40
5.5. Adatok archiválása . . . 41
5.5.1. Az archivált adatok típusai . . . 41
5.5.2. Az archívum megőrzési időtartama . . . 41
5.5.3. Az archívum védelme . . . 41
5.5.4. Az archívum mentési folyamatai . . . 42
5.5.5. Az adatok időbélyegzésére vonatkozó követelmények . . . 42
5.5.6. Az archívum gyűjtési rendszere . . . 42
5.5.7. Archív információk hozzáférését és ellenőrzését végző eljárások . . . 42
5.6. Szolgáltatói kulcs cseréje . . . 42
5.7. Kompromittálódást és katasztrófát követő helyreállítás . . . 43
5.7.1. Váratlan esemény és kompromittálódás kezelési eljárások . . . 43
5.7.2. Meghibásodott IT erőforrások, szoftverek és/vagy adatok . . . 44
5.7.3. Magánkulcs kompromittálódása esetén követendő eljárások . . . 44
5.7.4. Működés folyamatosságának biztosítása katasztrófát követően . . . 44
5.8. Az Időbélyegzés-szolgáltató leállítása . . . 45

6. Műszaki biztonsági óvintézkedések 45
6.1. Kulcspár előállítása és telepítése . . . 46
6.1.1. Kulcspár előállítása . . . 46
6.1.2. Kulcsméretek . . . 46
6.1.3. A nyilvános kulcs paraméterek előállítása, a minőség ellenőrzése . . . 47
6.1.4. A kulcshasználat célja (az X.509 v3 kulcs használati mező tartalmának megfelelően) . . . 47
6.2. A magánkulcsok védelme . . . 47
6.2.1. Kriptográfiai modulra vonatkozó szabványok és előírások . . . 47
6.2.2. Magánkulcs többszereplős (n-ből m) használata . . . 48
6.2.3. Magánkulcs letétbe helyezése . . . 48
6.2.4. Magánkulcs mentése . . . 48
6.2.5. Magánkulcs archiválása . . . 48
6.2.6. Magánkulcs bejuttatása hardver kriptográfiai eszközbe, vagy onnan történő exportja . . . 49
6.2.7. Magánkulcs tárolása hardver kriptográfiai eszközben . . . 49
6.2.8. A magánkulcs aktiválásának módja . . . 49

6.2.9. A magánkulcs deaktiválásának módja . . . 49
6.2.10. A magánkulcs megsemmisítésének módja . . . 50
6.2.11. A hardver kriptográfiai eszközök értékelése . . . 50
6.3. A kulcspár kezelés egyéb szempontjai . . . 50
6.3.1. A tanúsítványok és kulcspárok használatának periódusa . . . 50
6.4. Aktivizáló adatok . . . 51
6.4.1. Aktivizáló adatok előállítása és telepítése . . . 51
6.4.2. Az aktivizáló adatok védelme . . . 52
6.4.3. Az aktivizáló adatok kezelésének egyéb szempontjai . . . 52
6.5. Informatikai biztonsági előírások . . . 52
6.5.1. Speciális informatikai biztonsági műszaki követelmények . . . 52
6.5.2. Az informatikai biztonság értékelése . . . 52
6.6. Életciklusra vonatkozó műszaki előírások . . . 53
6.6.1. Rendszerfejlesztési előírások . . . 53
6.6.2. Biztonságkezelési előírások . . . 53
6.6.3. Életciklusra vonatkozó biztonsági előírások . . . 54
6.7. Hálózati biztonsági előírások . . . 55
6.8. Időbélyegzés . . . 56

7. Tanúsítvány, CRL és OCSP profilok 56
7.1. Tanúsítvány profil . . . 56
7.1.1. Verzió szám(ok) . . . 56
7.1.2. Tanúsítvány kiterjesztések . . . 57

8. A megfelelőség vizsgálata 59
8.1. Az ellenőrzések körülményei és gyakorisága . . . 60
8.2. Az auditor és szükséges képesítése . . . 60
8.3. Az auditor és az auditált rendszerelem függetlensége . . . 60
8.4. Az auditálás által lefedett területek . . . 60
8.5. A hiányosságok kezelése . . . 61
8.6. Az eredmények közzététele . . . 61

9. Egyéb üzleti és jogi kérdések 61
9.1. Díjak . . . 61
9.1.1. Visszatérítési politika . . . 61
9.2. Anyagi felelősségvállalás . . . 62
9.2.1. Pénzügyi követelmények . . . 62
9.2.2. Felelősségbiztosítás . . . 62
9.3. Bizalmasság . . . 63
9.3.1. Bizalmas információk köre . . . 63

9.3.2. Bizalmas információk körén kívül eső adatok . . . 63
9.3.3. Bizalmas információ védelme . . . 63
9.4. Személyes adatok védelme . . . 64
9.4.1. Adatkezelési szabályzat . . . 64
9.4.2. Személyes adatok . . . 65
9.4.3. Személyes adatnak nem minősülő adatok . . . 65
9.4.4. Személyes adatok védelme . . . 65
9.4.5. Személyes adatok felhasználása . . . 65
9.4.6. Adatkezelés . . . 65
9.4.7. Egyéb adatvédelmi követelmények . . . 65
9.5. Szellemi tulajdonjogok . . . 65
9.6. Tevékenységért viselt felelősség és helytállás . . . 66
9.6.1. A szolgáltató felelőssége és helytállása . . . 66
9.6.2. Az Ügyfél felelőssége és helytállása . . . 67
9.6.3. Az Érintett fél felelőssége . . . 68
9.6.4. Egyéb szereplők tevékenységéért viselt felelősség és helytállás . . . 68
9.7. Helytállás érvénytelenségi köre . . . 68
9.8. A felelősség korlátozása . . . 68
9.9. Kártérítési kötelezettség . . . 68
9.9.1. A szolgáltató kártérítési kötelezettsége . . . 68
9.9.2. Az előfizető kártérítési kötelezettsége . . . 69
9.9.3. Az érintett felek kártérítési kötelezettsége . . . 69
9.10. Érvényesség és megszűnés . . . 69
9.10.1. Érvényesség . . . 69
9.10.2. Megszűnés . . . 69
9.10.3. A megszűnés következményei . . . 69
9.11. A felek közötti kommunikáció . . . 69
9.12. Módosítások . . . 69
9.12.1. Módosítási eljárás . . . 70
9.12.2. Értesítések módja és határideje . . . 70
9.12.3. Az OID megváltoztatása . . . 70
9.13. Vitás kérdések rendezése . . . 70
9.14. Irányadó jog . . . 71
9.15. Az érvényben lévő jogszabályoknak való megfelelés . . . 71
9.16. Vegyes rendelkezések . . . 72
9.16.1. Teljességi záradék . . . 72
9.16.2. Átruházás . . . 72
9.16.3. Részleges érvénytelenség . . . 72
9.16.4. Igényérvényesítés . . . 72
9.16.5. Vis maior . . . 72
9.17. Egyéb rendelkezések . . . 72

A. Hivatkozások **73**

1. Bevezetés

Jelen dokumentum a Microsec Számítástechnikai Fejlesztő zártkörűen működő Részvénytársaság (továbbiakban: Microsec vagy *Nem minősített időbélyegzés-szolgáltató*) által üzemeltetett e-Szignó Hitelesítés Szolgáltató által kidolgozott *Nem minősített időbélyegzési szolgáltatási szabályzat*ot tartalmazza.

A *Nem minősített időbélyegzési szolgáltatási szabályzat* megfelel az eIDAS Rendelet [1] által támasztott követelményeknek, az ezen szabályoknak megfelelően nyújtott szolgáltatás a rendelet szerinti bizalmi szolgáltatás.

A *Nem minősített időbélyegzés-szolgáltató* a bizalmi szolgáltatás nyújtását 2017. szeptember 30-án jelentette be a Nemzeti Média- és Hírközlési Hatóságnak.

1.1. Áttekintés

A *Nem minősített időbélyegzési szolgáltatási szabályzat* egy "szabálygyűjtemény, amely egy *Időbélyegző* felhasználhatóságát határozza meg egy közös biztonsági követelményekkel rendelkező közösség és/vagy alkalmazások egy osztálya számára".

A *Nem minősített időbélyegzési szolgáltatási szabályzat* egyike a *Nem minősített időbélyegzés-szolgáltató* által kiadott azon dokumentumoknak, amelyek a *Nem minősített időbélyegzés-szolgáltató* által nyújtott szolgáltatás feltételeit együttesen szabályozzák. További dokumentumok például az Általános szerződési feltételek, a *Nem minősített időbélyegzési rend*, a felhasználókkal és a partnerekkel kötött egyéb szerződések.

A jelen dokumentum 1.6 fejezete számos fogalmat definiál, amelyeket más területeken nem, vagy nem teljesen ilyen értelmezésben használnak. Az ilyen értelemben használandó fogalmakat a dokumentumban minden esetben nagy kezdőbetűvel írva, döntött betűk használatával jelöljük.

1.2. Dokumentum neve és azonosítója

1.2.1. A dokumentum főbb azonosító adatai

Kibocsátó	e-Szignó Hitelesítés Szolgáltató
Dokumentum címe	eIDAS Rendelet szerinti nem minősített időbélyegzés-szolgáltatás szolgáltatási szabályzat
Azonosító	1.3.6.1.4.1.21528.2.1.1.202
Dokumentum verziószáma	2.11 * 2019-08-05
Hatályba lépés ideje	2019-09-25 [3]

A *Nem minősített időbélyegzési szolgáltatási szabályzat* aktuális változata a *Nem minősített időbélyegzés-szolgáltató* honlapján, illetve a *Nem minősített időbélyegzés-szolgáltató* ügyfélszolgálati irodájában érhető el.

[3] tervezett dátum, még elhalasztható

1.2.2. Megfelelés

A jelen *Nem minősített időbélyegzési szolgáltatási szabályzat* szerint kiállított *Időbélyegző*k megfelelnek az alábbi követelményeknek:

- ETSI EN 319 421 [16] szerinti
  BTSP: a best practices policy for time-stamp
  OID: itu-t(0) identified-organization(4) etsi(0)time-stamp-policy(2023)policy-identifiers(1) best-practices-ts-policy (1)

A *Nem minősített időbélyegzés-szolgáltató* az általa kibocsátott *Időbélyegző*kben saját OID azonosítóját szerepelteti, a fenti ETSI időbélyegzési rendet (BTSP) pedig támogatja.

1.2.3. Hatály

Jelen *Nem minősített időbélyegzési szolgáltatási szabályzat* 2019-09-25 [4]
-i hatálybalépési dátumtól visszavonásáig hatályos.

A *Nem minősített időbélyegzési szolgáltatási szabályzat* hatálya kiterjed az 1.3. alfejezetben azonosított közösség minden egyes tagjára.

Jelen *Nem minősített időbélyegzési szolgáltatási szabályzat* területi hatálya Magyarországra terjed ki. A *Nem minősített időbélyegzés-szolgáltató* működésére vonatkozóan a mindenkori magyar jogszabályok az irányadóak.

A jelen *Nem minősített időbélyegzési szolgáltatási szabályzat* szerint nyújtott szolgáltatás az egész világon elérhető. A *Nem minősített időbélyegzési szolgáltatási szabályzat* szerint létrejött *Időbélyegző*k érvényessége független attól, hogy mely földrajzi helyen készültek, illetve mely földrajzi helyen használják őket.

1.2.4. Időbélyegzési rend

A jelen *Nem minősített időbélyegzési szolgáltatási szabályzat* az alábbi *Nem minősített időbélyegzési rend* követelményeinek való megfelelést vállalja fel:

- " e-Szignó Hitelesítés Szolgáltató – eIDAS Rendelet szerinti nem minősített időbélyegzési rend. ", OID: 1.3.6.1.4.1.21528.2.1.1.201.2.11 * 2019-08-05, [28].

A *Nem minősített időbélyegzési rend* mindenkori aktuális és minden korábbi változata elérhető az alábbi címen:

`https://e-szigno.hu/letoltesek/dokumentumok-es-szabalyzatok/`

1.3. PKI szereplők

1.3.1. Szolgáltató

A *Nem minősített időbélyegzés-szolgáltató* egy olyan *Bizalmi szolgáltató*, amely *Bizalmi szolgáltatás* keretében *Időbélyegző*ket bocsát ki, és ellátja az ehhez kapcsolódó feladatokat.

[4] tervezett dátum, még elhalasztható

A *Nem minősített időbélyegzés-szolgáltató* adatai:

Név:	Microsec Számítástechnikai Fejlesztő zártkörűen működő Részvénytársaság
Cégjegyzékszám:	01-10-047218 Fővárosi Törvényszék Cégbírósága
Székhely:	1033 Budapest, Ángel Sanz Briz út 13.
Telefonszám:	(+36-1) 505-4444
Telefax szám:	(+36-1) 505-4445
Internet cím:	`https://www.microsec.hu`, `https://www.e-szigno.hu`

A *Nem minősített időbélyegzés-szolgáltató* szervezetén belül az e-Szignó Hitelesítés Szolgáltató, mint önálló üzleti egység látja el a szolgáltatással kapcsolatos feladatokat. Ezen önálló üzleti egység a következő két részből áll:

- ügyfélszolgálati iroda,
- hitelesítő szervezet.

Ügyfélszolgálati iroda

Az ügyfélszolgálati iroda az *Előfizető*vel való kapcsolattartásért felelős. Az iroda és a fogyasztóvédelmi szerv elérhetősége:

A szolgáltató egység neve:	e-Szignó Hitelesítés Szolgáltató
Ügyfélszolgálati iroda:	1033 Budapest, Ángel Sanz Briz út 13., Graphisoft Park South Area, C épület
Ügyfélszolgálati iroda nyitvatartási ideje:	munkanapokon 8:30-16:30 között előzetes időpont egyeztetés alapján
Ügyfélszolgálati iroda telefonszáma:	(+36-1) 505-4444
Ügyfélszolgálati iroda email címe:	`info@e-szigno.hu`
Visszavonási kérelmek fogadása:	`visszavonas@e-szigno.hu`
A szolgáltatással kapcsolatos információk elérése:	`https://www.e-szigno.hu`
Panaszok bejelentésének helye:	Microsec zrt. 1033 Budapest, Ángel Sanz Briz út 13., Graphisoft Park South Area, C épület
Illetékes fogyasztóvédelmi felügyelőség:	Budapest Főváros Kormányhivatal Fogyasztóvédelmi Felügyelőség 1052 Budapest, Városház u. 7. 1364 Budapest, Pf. 144.
Illetékes békéltető testület elérhetősége:	Budapesti Békéltető Testület 1016 Budapest, Krisztina krt. 99. III. em. 310. Levelezési cím: 1253 Budapest, Pf.: 10.

A szolgáltatás főbb elemei

A szolgáltatás a következő elemekből áll:

- időbélyegző kérés fogadása, amely során a *Nem minősített időbélyegzés-szolgáltató* rendszere azonosítja az *Előfizető*t és fogadja a kérését,
- *Időbélyegző* előállítás, amely során a *Nem minősített időbélyegzés-szolgáltató* rendszere előállítja az időbélyegzés kérésnek megfelelő, az aktuális, hiteles időpontot tartalmazó *Időbélyegző*t;
- *Időbélyegző* kibocsátás, amely során a *Nem minősített időbélyegzés-szolgáltató* eljuttatja az *Előfizető*nek a kérése alapján számára előállított *Időbélyegző*t;
- belső pontos időt előállító rendszer, amely az UTC időhöz szinkronizálva az *Időbélyegző*kbe kerülő pontos idő forrását szolgáltatja.

1.3.2. Ügyfelek

Az *Előfizető* (Ügyfél), aki előfizet a *Nem minősített időbélyegzés-szolgáltató* által nyújtott Időbélyegzés szolgáltatásra, és a szolgáltatás keretében díjfizetés ellenében *Időbélyegző*ket kér a *Nem minősített időbélyegzés-szolgáltató*tól. Az *Előfizető* lehet természetes vagy jogi személy, egy *Előfizető* nevében akár több természetes személy is kérhet *Időbélyegző*ket.

1.3.3. Érintett felek

Érintett fél, aki ellenőrzi és felhasználja a *Nem minősített időbélyegzés-szolgáltató* által kibocsátott *Időbélyegző*ket. Az *Érintett fél* nem áll szerződéses kapcsolatban a *Nem minősített időbélyegzés-szolgáltató*val.

1.4. Az időbélyegző felhasználhatósága

Az *Időbélyegző* hitelesen igazolja, hogy az *Időbélyegző*vel ellátott elektronikus dokumentum az adott formában már létezett az *Időbélyegző*ben megadott időpontot megelőzően.

1.5. A dokumentum adminisztrálása

1.5.1. A dokumentum adminisztrációs szervezete

Jelen *Nem minősített időbélyegzési szolgáltatási szabályzat* adminisztrációját ellátó szervezet adatai az alábbi táblázatban találhatók:

Szervezet neve	Microsec e-Szignó Hitelesítés Szolgáltató
Szervezet címe	Magyarország, H-1033 Budapest, Ángel Sanz Briz út 13.
Telefonszám	+36 1 505-4444
Fax szám	+36 1 505-4445
Email cím	info@e-szigno.hu

1.5.2. Kapcsolattartó személy

Jelen *Nem minősített időbélyegzési szolgáltatási szabályzat*tal kapcsolatos kérdésekben közvetlenül az alábbi személyhez lehet fordulni:

Kapcsolattartó	Folyamatszervezés részleg vezetője
Szervezet neve	Microsec zrt.
Szervezet címe	Magyarország, H-1033 Budapest, Ángel Sanz Briz út 13. C épület
Telefonszám	+36 1 505-4444
Fax szám	+36 1 505-4445
Email cím	info@e-szigno.hu

1.5.3. A Szolgáltatási szabályzat *Nem minősített időbélyegzési rend*nek való megfelelőségéért felelős személy/szervezet

Egy *Nem minősített időbélyegzési szolgáltatási szabályzat*nak a benne meghivatkozott *Nem minősített időbélyegzési rend*nek való megfelelőségéért és az abban foglaltak szerinti szolgáltatás nyújtásáért az adott *Nem minősített időbélyegzési szolgáltatási szabályzat*ot kibocsátó szolgáltató a felelős.

A *Nem minősített időbélyegzési szolgáltatási szabályzat*ok és a szolgáltatások nyújtása feletti felügyeletet a Nemzeti Média- és Hírközlési Hatóság látja el. A Nemzeti Média- és Hírközlési Hatóság nyilvántartást vezet a követelményeknek megfelelő *Nem minősített időbélyegzési rend*ekről valamint az ezeket alkalmazó *Nem minősített időbélyegzés-szolgáltató*król.

1.5.4. A Szolgáltatási szabályzat elfogadási eljárása

A *Nem minősített időbélyegzési szolgáltatási szabályzat* új verziójának illetve tetszőleges módosításának megírása, elfogadása és kibocsátása egységes folyamatok szerint – a 9.12.1 fejezetben részletezett módon – történik.

1.6. Fogalmak és rövidítések

1.6.1. Fogalmak

Adatközpont	Számítógépes rendszerek és a hozzájuk kapcsolódó komponensek elhelyezésére és üzemeltetésére kialakított létesítmény. Ezek a komponensek rendszerint magukba foglalják a távközlési rendszereket és kommunikációs kapcsolatokat, redundáns áramforrást, adattárolókat, légkondicionáló, tűzvédelmi és biztonsági rendszereket.
Bizalmi felügyelet	"A *Bizalmi szolgáltatás*ok felügyeletét ellátó hatóság a Nemzeti Média- és Hírközlési Hatóság." (2015. évi CCXXII. törvény [5] 91.§ 1. bekezdés)

Bizalmi szolgáltatás (Trust Service)	"Rendszerint díjazás ellenében nyújtott, az alábbiakból álló elektronikus szolgáltatások: • elektronikus aláírások, elektronikus bélyegzők vagy elektronikus időbélyegzők, ajánlott elektronikus kézbesítési szolgáltatások, valamint az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok létrehozása, ellenőrzése és érvényesítése; vagy • *Weboldal-hitelesítő tanúsítvány*ok létrehozása, ellenőrzése és érvényesítése; vagy • elektronikus aláírások, bélyegzők vagy az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok megőrzése; " (eIDAS [1] 3. cikk 16. pont)
Bizalmi szolgáltatási rend (Trust Service Policy)	"Olyan szabálygyűjtemény, amelyben egy *Bizalmi szolgáltató*, igénybe vevő vagy más személy valamely *Bizalmi szolgáltatás* használatának feltételeit írja elő igénybe vevők valamely közös biztonsági követelményekkel rendelkező csoportja vagy meghatározott alkalmazások számára. " (2015. évi CCXXII. törvény [5] 1. § 8. pont)
Bizalmi szolgáltató (Trust Service Provider)	"Egy vagy több *Bizalmi szolgáltatás*t nyújtó természetes vagy jogi személy; a *Bizalmi szolgáltató* lehet minősített vagy nem minősített *Bizalmi szolgáltató*." (eIDAS [1] 3. cikk 19. pont)
Elektronikus időbélyegző (Electronic Time Stamp)	"Olyan elektronikus adatok, amelyek más elektronikus adatokat egy adott időponthoz kötnek, amivel igazolják, hogy utóbbi adatok léteztek az adott időpontban. " (eIDAS [1] 3. cikk 33. pont)
Előfizető (Subscriber)	A Szolgáltatóval valamely szolgáltatás igénybevétele érdekében Szolgáltatási szerződést kötő személy vagy szervezet.
Érintett fél (Relying Party)	Az *Időbélyegző* elfogadója, aki az *Időbélyegző*t használja.

Gyökér tanúsítvány (Root Certificate)	Más néven legfelső szintű tanúsítvány. Önhitelesített *Tanúsítvány*, amelyet adott *Hitelesítő egység* saját maga számára bocsátott ki, azaz saját magánkulcsával van aláírva, így a saját – a tanúsítványban szereplő – nyilvános kulcsával ellenőrizhető.
Hardver kriptográfiai eszköz (HSM: Hardware Security Module)	Egy olyan hardver alapú biztonságos eszköz, mely előállítja, tárolja és védi a kriptográfiai kulcsokat, valamint biztonságos környezetet biztosít a kriptográfiai funkciók végrehajtására.
Hitelesítés-szolgáltató	Olyan *Bizalmi szolgáltató*, aki/amely a hitelesítés-szolgáltatás keretében azonosítja az igénylő személyét, *Tanúsítvány*t bocsát ki, nyilvántartásokat vezet, fogadja a *Tanúsítvány*okkal kapcsolatos változások adatait, valamint nyilvánosságra hozza a *Tanúsítvány*hoz tartozó szabályzatokat, és a *Tanúsítvány* aktuális állapotára (különösen esetleges visszavonására) vonatkozó információkat.
Hitelesítő egység	A *Hitelesítés-szolgáltató* rendszerének egy egysége, amely *Tanúsítvány*ok digitális aláírását végzi. Egy *Hitelesítő egység*hez mindig egy elektronikus aláírás vagy bélyegző létrehozásához használt adat (magánkulcs) tartozik. Előfordulhat, hogy egy *Hitelesítés-szolgáltató* egyszerre több *Hitelesítő egység*et is működtet.
Időbélyegzési rend	Olyan *Bizalmi szolgáltatási rend*, amelyben egy szolgáltató, igénybe vevő vagy más személy (szervezet) valamely *Időbélyegző* felhasználásának feltételeit írja elő az igénybe vevők valamely közös biztonsági követelményekkel rendelkező csoportja, illetőleg meghatározott alkalmazások számára.
Időbélyegzés-szolgáltató	Olyan *Bizalmi szolgáltató*, amely *Bizalmi szolgáltatás* keretében *Időbélyegző*ket bocsát ki, és ellátja az ehhez kapcsolódó feladatokat.
Időbélyegző egység	Az *Időbélyegzés-szolgáltató* rendszerének egy egysége, amely az *Időbélyegző*k aláírását vagy bélyegzését végzi. Egy időbélyegző egységhez mindig egy elektronikus aláírás vagy bélyegző létrehozáshoz használt adat tartozik. Előfordulhat, hogy egy *Időbélyegzés-szolgáltató* egyszerre több időbélyegző egységet is működtet.
Kompromittálódás	Egy kriptográfiai kulcs abban az esetben tekintendő kompromittálódottnak, ha vélelmezhető, hogy illetéktelen személynek is hozzáférése van hozzá.

Köztes hitelesítő egység	Olyan *Hitelesítő egység* amelynek *Tanúsítvány*át egy másik *Hitelesítő egység* bocsátotta ki.
Kriptográfiai kulcs (Cryptographic Key)	Olyan – kriptográfiai transzformációt vezérlő – egyedi digitális jelsorozat, amelynek ismerete szükséges titkosításhoz és dekódoláshoz, illetve digitális aláírás előállításához és ellenőrzéséhez.
Kulcsgondozás (Key Management)	A kriptográfiai kulcsok előállítása, a felhasználókhoz történő eljuttatása vagy ennek algoritmikus megvalósítása, továbbá a kulcsok nyilvántartása, tárolása, archiválása, visszavonása, törlése, amely szoros kapcsolatban áll az alkalmazott biztonsági eljárásmóddal.
Magánkulcs	A Nyilvános kulcsú infrastruktúrában egy szereplőhöz tartozó aszimmetrikus kriptográfiai kulcspár azon eleme, amelyet az *Alany*nak szigorúan titokban kell tartania. A *Hitelesítés-szolgáltató* a *Tanúsítvány*ok kibocsátása során a *Hitelesítő egység* magánkulcsát használja arra, hogy a *Tanúsítvány*t védő elektronikus aláírást vagy bélyegzőt elhelyezze rajta.
Nyilvános kulcs	A Nyilvános kulcsú infrastruktúrában egy szereplőhöz tartozó aszimmetrikus kriptográfiai kulcspár azon eleme, amelyet nyilvánosságra kell hozni. A nyilvánosságra hozatal jellemzően egy *Tanúsítvány* formájában történik, amely összekapcsolja a szereplő nevét az ő nyilvános kulcsával. A *Tanúsítvány*ok hitelességét az őket kibocsátó *Hitelesítő egység* nyilvános kulcsa segítségével lehet ellenőrizni.
Nyilvános kulcsú infrastruktúra (Public Key Infrastructure, PKI)	Aszimmetrikus kulcsú kriptográfiára épülő infrastruktúra, beleértve a kriptográfiai algoritmusokat, kulcsokat, tanúsítványokat, a rájuk vonatkozó szabványokat és jogszabályokat, a mögöttes intézményrendszert, a különböző szolgáltatókat és eszközöket is.
Rendkívüli üzemeltetési helyzet	Olyan, a *Nem minősített időbélyegzés-szolgáltató* üzemmenetében zavart okozó rendkívüli helyzet, amikor a *Nem minősített időbélyegzés-szolgáltató* rendes üzemmenetének folytatására ideiglenesen vagy véglegesen nincsen lehetőség.
Szervezet	Jogi személy.

Szolgáltatási szabályzat (Trust Service Practice Statement)	"A *Bizalmi szolgáltató* nyilatkozata az egyes *Bizalmi szolgáltatás*ok nyújtásával kapcsolatosan alkalmazott részletes eljárási vagy más működési követelményekről. " (2015. évi CCXXII. törvény [5] 1. § 41. pont)
Szolgáltatási szerződés	"A *Bizalmi szolgáltató* és a *Bizalmi szolgáltatás*i ügyfél között létrejött szerződés, amely a *Bizalmi szolgáltatás* nyújtására és a szolgáltatás igénybevételére vonatkozó feltételeket tartalmazza. " (2015. évi CCXXII. törvény [5] 1. § 42. pont)
Tanúsítvány (Certificate)	"Az elektronikus aláírás tanúsítvány, az elektronikus bélyegző tanúsítvány és a *Weboldal-hitelesítő tanúsítvány*, valamint mindazon, a *Bizalmi szolgáltatás* keretében a szolgáltató által kibocsátott elektronikus igazolás, amely tartalmazza a tanúsítványra vonatkozó érvényesítési adatot és a tanúsítvány használatához szükséges kapcsolódó adatokat, és amely elektronikus dokumentum megbízhatóan védve van a kibocsátáskor és az érvényességi ideje alatt rendelkezésre álló technológiákkal elkövetett hamisítás ellen. " (2015. évi CCXXII. törvény [5] 1. § 44.)
Tanúsítványkérelem	Az *Igénylő* által, a Szolgáltató számára a *Tanúsítvány* kibocsátás érdekében benyújtott adatok és nyilatkozatok, amelyekben többek között az *Igénylő* megerősíti a *Tanúsítvány*ba kerülő adatok valódiságát.
Tanúsítványtár	Különböző *Tanúsítvány*okat tartalmazó adattár. Tanúsítványtára van egy Szolgáltatónak is, amelyben az általa kibocsátott *Tanúsítvány*okat publikálja, de Tanúsítványtárnak nevezzük az *Érintett fél* számítógépén a használt alkalmazás számára elérhető *Tanúsítvány*okat tartalmazó rendszert is.
Ügyfél	Az *Előfizető* másik elnevezése.
Visszavonás	A *Tanúsítvány* érvényességének megszüntetése a *Tanúsítvány*ban is feltüntetett érvényességi idő lejárta előtt. A *Tanúsítvány* visszavonása végleges, visszavont *Tanúsítvány* többet nem tehető érvényessé.
Visszavonási állapot nyilvántartás	A *Hitelesítés-szolgáltató* által vezetett belső nyilvántartás a felfüggesztett, illetőleg a visszavont *Tanúsítvány*okról, amelyek tartalmazzák legalább a felfüggesztés vagy visszavonás tényét, és a felfüggesztés vagy visszavonás időpontját másodperc pontossággal.

1.6.2. Rövidítések

CRL	Certificate Revocation List	Tanúsítvány visszavonási lista
eIDAS	electronic Identification, Authentication and Signature	A 910/2014/EU rendelet általánosan használt hivatkozása
GMT	Greenwich Mean Time	Greenwichi középidő
IERS	International Earth Rotation and reference System Service	Nemzetközi Földforgás és Referenciarendszer Szolgálat
LDAP	Lightweight Directory Access Protocol	Protokoll címtár szolgáltatás eléréséhez
NMHH		Nemzeti Média- és Hírközlési Hatóság
OCSP	Online Certificate Status Protocol	Online tanúsítvány-állapot protokoll
OID	Object Identifier	Objektum azonosító
PKI	Public Key Infrastructure	Nyilvános kulcsú infrastruktúra
TAI	International Atomic Time	Nemzetközi atomidő
TSA	Time Stamping Authority	Időbélyegzés szolgáltató
TSP	Trust Service Provider	Bizalmi szolgáltató
TSU	Time-Stamping Unit	Időbélyegző Egység
TDS	TSA Disclosure Statement	TSA Közzétételi nyilatkozat
UTC	Coordinated Universal Time	Egyezményes koordinált világidő

2. Közzététel és tanúsítványtár

2.1. Adatbázisok - tanúsítványtárak

A *Nem minősített időbélyegzés-szolgáltató* publikálja a működése alapjául szolgáló *Nem minősített időbélyegzési rend*et, *Nem minősített időbélyegzési szolgáltatási szabályzat*ot valamint a szerződési feltételeket tartalmazó egyéb dokumentumokat.

2.2. A tanúsítványokra vonatkozó információk közzététele

A *Nem minősített időbélyegzés-szolgáltató* közzéteszi a honlapján a szolgáltatói *Tanúsítvány*ait.

2.2.1. Szolgáltatói információ közzététele

A *Nem minősített időbélyegzés-szolgáltató* nyilvánosságra hozza szerződéses feltételeit és szabályzatait a honlapján elektronikus formában.

A honlapon a hatálybalépés előtt publikálásra kerülnek a bevezetésre váró új dokumentumok.

A honlapon az érvényben levő dokumentumokon kívül elérhető valamennyi dokumentum összes korábbi verziója is.

A szabályzatok és szerződési feltételek aktuális verziója nyomtatott formában olvasható a *Nem minősített időbélyegzés-szolgáltató* ügyfélszolgálati irodájában.

A *Nem minősített időbélyegzés-szolgáltató* a szerződéskötést követően tartós adathordozón bocsátja az *Ügyfél* rendelkezésére a *Nem minősített időbélyegzési rend*et, a *Nem minősített időbélyegzési szolgáltatási szabályzat*ot és a Szolgáltatási szerződést.

A *Nem minősített időbélyegzés-szolgáltató* értesíti *Ügyfel*eit az Általános szerződési feltételek változásáról.

2.3. A közzététel időpontja vagy gyakorisága

2.3.1. Kikötések és feltételek közzétételi gyakorisága

A *Nem minősített időbélyegzési szolgáltatási szabályzat*tal kapcsolatos új verziók közzététele a 9.12. fejezetben ismertetett eljárásoknak megfelelően történik.

A *Nem minősített időbélyegzés-szolgáltató* szükség szerint hozza nyilvánosságra egyéb szabályzatait, szerződéses feltételeit, illetve azok újabb változatait.

A *Nem minősített időbélyegzés-szolgáltató* a rendkívüli információkat a jogszabályi előírásoknak megfelelően, – annak hiányában pedig szükség szerint – késedelem nélkül közzé teszi.

3. Az Időbélyegző egység tanúsítványa és az Időbélyegzés

3.1. A felhasználó azonosítása

A szolgáltatás a *Nem minősített időbélyegzés-szolgáltató Előfizető*i által vehető igénybe a *Nem minősített időbélyegzés-szolgáltató* által az *Előfizető* részére a szolgáltatási szerződés megkötésekor átadott elérési módokon.

3.2. Az Időbélyegző egység tanúsítványa

A *Nem minősített időbélyegzés-szolgáltató* az *Időbélyegző egység* nyilvános kulcsát közzéteszi a honlapján *Tanúsítvány* formájában a szolgáltatói *Tanúsítvány*ok között.

A *Időbélyegző egység Tanúsítvány*át a Microsec e-Szignó Hitelesítés Szolgáltató adja ki, amely az eIDAS szerinti minősített *Bizalmi szolgáltató*ként az ETSI EN 319 411-1 [11] és az ETSI EN 319 411-2 [12] szerinti bizalmi szolgáltatást is nyújt.

A *Nem minősített időbélyegzés-szolgáltató* csak akkor kezdi meg egy új magánkulccsal az *Időbélyegző*k kibocsátását, ha

- a *Tanúsítvány* aláírását ellenőrizte a megbízható *Hitelesítés-szolgáltató*ig visszavezetett teljes érvényességi láncon;
- meggyőződött a magánkulcs és a *Tanúsítvány*ban publikált nyilvános kulcs összetartozásáról;
- az adott magánkulcshoz tartozó *Tanúsítvány* már feltöltésre került az *Időbélyegző egység*be.

3.3. Az Időbélyegző

A *Nem minősített időbélyegzés-szolgáltató* által kibocsátott *Időbélyegző* megfelel az IETF RFC 3161 [21] és az ETSI EN 319 422 [17] szabványoknak;

Ennek megfelelően az *Időbélyegző* jellemzői:

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

Az *Időbélyegző egység*ek a *Nem minősített időbélyegzés-szolgáltató* biztonságos *Adatközpont*jában működnek, ami garantálja az *Időbélyegző*ben megadott időértékek megfelelőségét (lásd 6. fejezet).

Az *Időbélyegző egység*(ek) *Időbélyegző*k kibocsátásához használt belső órája visszavezethető az UTC pontos időre (lásd 3.4. fejezet).

Az *Időbélyegző*ben megadott időpont pontossága megfelel az *Időbélyegzési rend*ben meghatározott követelményeknek (lásd 3.4. fejezet). A vállalt pontosság magában az *Időbélyegző*ben is feltüntetésre kerül (lásd 3.3.2. fejezet).

Az *Időbélyegző egység* nem bocsát ki *Időbélyegző*t, amint észleli hogy a belső óra pontossága a megadott mértéket meghaladóan eltér a UTC szerinti pontos időtől (lásd 3.4. fejezet).

A *Nem minősített időbélyegzés-szolgáltató* az *Időbélyegző egység*ek magánkulcsait az *Időbélyegző*k hitelesítésétől eltérő célra nem használja (lásd 6.1.2. fejezet).

A kulcsok élettartamának lejárta után a magánkulcsok törlésre kerülnek a 6.3.1. fejezetben leírtak szerint, így a *Időbélyegző egység*ek nem tudnak *Időbélyegző*t kibocsátani a lejárt magánkulccsal.

3.3.1. Időbélyegző kérés

A *Nem minősített időbélyegzés-szolgáltató* támogatja az IETF RFC 3161 [21] 2.4.1. fejezete szerinti *Időbélyegző* kéréseket beleértve az alábbi mezők használatát:

- "reqPolicy"
- "nonce"
- "certReq"
- "extensions"

A *Nem minősített időbélyegzés-szolgáltató* az ETSI TS 119 312 [18] szerinti és az aktuális Nemzeti Média- és Hírközlési Hatóság algoritmusokkal kapcsolatos határozatban kijelölt lenyomatképző algoritmusokat fogad be az *Időbélyegző* kérésekben. A lenyomatképző algoritmusok kiválasztásánál figyelembe veszi az *Időbélyegző* tervezett felhasználási idejét és a lenyomatképző függvény várható megfelelőségi időtartamát.

A jelenleg támogatott lenyomatképző algoritmusok:

sha256	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) sha256(1) }
sha512	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) sha512(3) }

Az időbélyegző kérés felépítése

- Verzió (Version)
  Az Időbélyegző kérés formátuma az IETF RFC 3161 [21] szerinti "v1" verziónak felel meg, így a mezőbe az "1" érték kerül.
- Üzenet lenyomat (MessageImprint)
  Az *Időbélyegző*vel ellátandó adat, ami két részből áll:
  - Lenyomatképző algoritmus (hashAlgorithm)
    A lenyomatképző algoritmus OID azonosítója, amellyel a lenyomat készült
  - Lenyomat (hashedMessage)
    maga a lenyomat, amit el kell látni *Időbélyegző*vel. Az adat hossza megfelel a megadott lenyomatképző algoritmusnak.
- *Nem minősített időbélyegzési rend* azonosító (reqPolicy)
  opcionális mező
  Azt mondja meg, hogy az *Időbélyegző*t milyen *Nem minősített időbélyegzési rend* szerint kérik kibocsátani.
- Nonce (nonce)
  opcionális mező
  Maximum 64 bites egész szám, az *Időbélyegző* egyediségének biztosítására szolgál. A "nonce" szerepeltetése esetén a válaszban ugyanennek az értéknek kell szerepelnie.
- Tanúsítvány igénylése (certReq)
  alapértelmezetten "FALSE"
  Amennyiben a kérésben "TRUE " értékkel szerepel, a válaszban meg kell küldeni a "SigningCertificate attribute" attributumban hivatkozott *Időbélyegző egység Tanúsítvány*t.
- Kiterjesztések (extensions)
  opcionális mező
  Az igénylő itt adhat meg plusz információt. A *Nem minősített időbélyegzés-szolgáltató* nem támogatja a mező használatát. Amennyiben ezt a mezőt tartalmazó kérés érkezik, a *Nem minősített időbélyegzés-szolgáltató* nem bocsát ki *Időbélyegző*t, helyette a válaszban "unacceptedExtension" hibaüzenetet küld vissza.

3.3.2. Időbélyegző válasz

A *Nem minősített időbélyegzés-szolgáltató* támogatja az IETF RFC 3161 [21] 2.4.2. fejezete szerinti *Időbélyegző* válaszokat az alábbi kiegészítésekkel:

- "accuracy";
- "nonce".

Amennyiben a "nonce" mező szerepel az *Időbélyegző* kérésben, ugyanazzal az értékkel szerepel az *Időbélyegző* válaszban is.

A *Nem minősített időbélyegzés-szolgáltató* az ETSI TS 119 312 [18] szerinti és az aktuális Nemzeti Média- és Hírközlési Hatóság algoritmusokkal kapcsolatos határozatban kijelölt

kriptográfiai algoritmuskészleteket és kulcshosszakat használ az *Időbélyegző*k aláírására. A kriptográfiai algoritmuskészletek és kulcshosszak kiválasztásánál figyelembe veszi az *Időbélyegző* tervezett felhasználási idejét.

A támogatott kriptográfiai algoritmuskészlet:

sha256WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1)sha256WithRSAEncryption(11) }
sha512WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1)sha512WithRSAEncryption(13) }
ecdsa-with-SHA256	{ iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2) }

A támogatott ETSI Időbélyegző profil azonosítója (BTSP):
itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) baseline-ts-policy (1).

Az időbélyegző válasz felépítése

- státusz (PKIStatusInfo)
  Az IETF RFC 3161 [21] 2.4.2 fejezet szerinti státusz információ a kibocsátás sikerességéről.
- *Időbélyegző* token (TimeStampToken)
  opcionális mező
  A státusz mező "0" vagy "1" értéke esetén tartalmazza a kibocsátott *Időbélyegző*t, egyéb státusz érték esetén a mező nem szerepel a válaszban.

Az időbélyegző token felépítése

Az IETF RFC 3161 [21] 2.4.2 fejezet szerinti, az *Időbélyegző egység* által aláírt *Időbélyegző* token, amelynek mezői:

- Verzió (version)
  Az *Időbélyegző* token formátuma az IETF RFC 3161 [21] szerinti "v1" verziónak felel meg, így a mezőbe az "1" érték kerül.
- *Nem minősített időbélyegzési rend* azonosító (policy)
  kötelező mező
  Azt mondja meg, hogy az *Időbélyegző*t milyen *Nem minősített időbélyegzési rend* szerint bocsátották ki. Amennyiben a "reqPolicy" mező szerepelt a kérésben is, csak a kérésnek megfelelő OID támogatása esetén bocsátható ki *Időbélyegző*, egyéb esetben a kérés "unacceptedpolicy" hibaüzenettel elutasításra kerül.
- Üzenet lenyomat (messageImprint)
  Az *Időbélyegző*vel ellátott adat a kéréssel egyező tartalommal.
- sorszám (serialNumber)
  kötelező mező
  Az *Időbélyegző egység* által kibocsátott valamennyi *Időbélyegző*re egyedi sorszám az egység teljes élettartama alatt. Maximális mérete 160 bit.

- Idő (genTime)
  kötelező mező
  UTC formában megadott időpont, amelyben az *Időbélyegző*t kibocsátották. A *Nem minősített időbélyegzés-szolgáltató* által kibocsátott *Időbélyegző*kben a "genTime" érték másodperc pontossággal kerül megadásra az RFC 5280 [22] szerint.

- Pontosság (accuracy)
  opcionális mező
  A mezőben megadható, hogy a tokenben megadott időpont legfeljebb mennyi idővel térhet el az UTC időtől. A *Nem minősített időbélyegzés-szolgáltató* által kibocsátott *Időbélyegző*kben minden esetben szerepelteti az "Accuracy" mezőt.

- Sorrend (ordering)
  alapértelmezetten "FALSE"
  A mező értéke akkor lehetne "TRUE", ha a kibocsátott *Időbélyegző*ket a megadott időérték alapján egyértelműen sorrendbe lehetne tenni. A *Nem minősített időbélyegzés-szolgáltató* által kibocsátott *Időbélyegző*k nagy száma miatt ez a feltétel nem teljesíthető, ezért a mező az *Időbélyegző*kben minden esetben "FALSE" értékkel szerepel.

- Nonce (nonce)
  opcionális mező
  Maximum 64 bites egész szám, az *Időbélyegző* egyediségének biztosítására szolgál. Amennyiben a kérésben szerepel, a válaszban is kötelezően szerepel ugyanazzal az értékkel.

- tsa (tsa)
  opcionális mező
  Megadható benne az *Időbélyegző egység* neve. Amennyiben a mező szerepel, a megadott névnek egyeznie kell az aláíró *Tanúsítvány*ban megadott egyik "subject name" értékkel.

- Kiterjesztések (extensions)
  opcionális mező

  A *Nem minősített időbélyegzés-szolgáltató* nem használ kiterjesztéseket.

3.4. Az Időbélyegzőben szereplő idő pontossága

A *Nem minősített időbélyegzés-szolgáltató* garantálja, hogy az általa kibocsátott *Időbélyegző*kben szereplő idő eltérése az UTC időtől legfeljebb 1 másodperc lehet.

Az *Időbélyegző egység* óráját szolgáltató rendszerek a *Nem minősített időbélyegzés-szolgáltató* szigorúan védett *Adatközpont*jában találhatók, ami lehetetlenné teszi az óra észrevétlen átállítását.

A *Nem minősített időbélyegzés-szolgáltató* folyamatosan monitorozza a belső időt biztosító rendszereit. Amint a belső idő UTC időtől való eltérése meghaladja a 0.1 másodpercet, a *Nem minősített időbélyegzés-szolgáltató* felfüggeszti az *Időbélyegző*k kibocsátását.

A *Nem minősített időbélyegzés-szolgáltató* belső órájának pontosságát a *Nem minősített időbélyegzés-szolgáltató* biztonsági bizottsága évente megvizsgálja.

3.5. Óraszinkronizálás

Az *Időbélyegző*ben megadott időpontot a *Nem minősített időbélyegzés-szolgáltató* belső órája adja, amelyet a *Nem minősített időbélyegzés-szolgáltató* két egymástól független Stratum-1 UTC referencia időforrással szinkronizál:

- az egyik pontos idő forrás a műhold alapú GPS jelet használja;
- a másik pontos idő forrás a hosszúhullámú pontos idő szolgáltatásra (DCF77) támaszkodik.

A *Nem minősített időbélyegzés-szolgáltató* a fenti két független Stratum-1 időforráshoz 0,1 másodperc pontossággal szinkronizálja saját belső óráját. E szinkronizációt a *Nem minősített időbélyegzés-szolgáltató* naponta legalább négy alkalommal elvégzi.

A *Nem minősített időbélyegzés-szolgáltató* a belső óra pontosságának ilyen szinten tartásával garantálja, hogy a kiadott *Időbélyegző*k pontossága legfeljebb 1 másodperccel tér el az UTC időalaptól.

3.5.1. A szökőmásodpercek kezelése

Szökőmásodperc előfordulásakor a *Nem minősített időbélyegzés-szolgáltató* elvégzi az óraszinkronizációt az illetékes szervezet előzetes értesítése alapján a megadott időpontban az ETSI 319 421 [16] C függelékében meghatározottak szerint az ITU-R TF.460-6 [25] ajánlásnak megfelelően.

A pozitív szökőmásodperc az adott nap 23:59:59 UTC után következik be, ez után 23:59:60 következik, majd folytatódik az UTC idő a szokásos, következő napi 00:00:00-val.

3.5.2. Nyári időszámítás kezelése

A *Nem minősített időbélyegzés-szolgáltató* UTC időt ír a kibocsátott *Időbélyegző*kbe.

A *Nem minősített időbélyegzés-szolgáltató* felhívja az *Érintett felek* figyelmét, hogy az egyes alkalmazások az *Időbélyegző*kben megadott időpontokat eltérő módon és formátumban jeleníthetik meg a felhasználó részére, gyakran helyi időt használva. A megjelenítés ilyen módja félreértésekre adhat okot a *Érintett felek*nek különböző időzónákban, illetve a nyári időszámítás idején, különösen a tavaszi és őszi óraátállítás környékén.

3.6. Az Időbélyegző ellenőrzése

Az *Időbélyegző*n szereplő elektronikus aláírás vagy elektronikus bélyegző érvényességének ellenőrzése során az *Érintett fél*nek célszerű az ETSI EN 319 102-1 [9] specifikációban leírtak szerint eljárnia.

Az *Időbélyegző* ellenőrzése során:

- ellenőrizni kell, hogy összetartozik-e az időbélyegzett dokumentum az *Időbélyegző*vel és a *Nem minősített időbélyegzés-szolgáltató Tanúsítvány*ával;
- ellenőrizni kell az *Időbélyegző*n szereplő aláírást;

- ellenőrizni kell, hogy az *Időbélyegző* megfelel-e az adott célra, többek között, hogy pontossága, megbízhatósága, valamint a hozzá kapcsolódó Időbélyegzés-szolgáltatói felelősségvállalás megfelelő.

3.7. A szolgáltatás rendelkezésre állása

A *Nem minősített időbélyegzés-szolgáltató* biztosítja a szolgáltatás, valamint a *Nem minősített időbélyegzés-szolgáltató* által kibocsátott *Időbélyegző*k használatára vonatkozó kikötések és feltételek folyamatos elérhetőségét éves szinten legalább 99% -os rendelkezésre állás mellett, ahol az eseti szolgáltatáskiesések időtartama legfeljebb 24 óra.

3.8. Nem minősített időbélyegzők kibocsátása

A 910/2014/EU rendelet [1] szerinti minősített *Időbélyegző*ket kibocsátó *Időbélyegző egység* nem bocsáthat ki nem minősített *Időbélyegző*ket.

Az e-Szignó Hitelesítés Szolgáltató által üzemeltetett *Nem minősített időbélyegzés-szolgáltató* csak nem minősített *Időbélyegző*ket bocsát ki.

3.9. Az Időbélyegző egység kulcshasználata

Az *Időbélyegző egység*ekben be kell tartani az alábbi követelményeket:

- csak olyan algoritmusokat és kulcsméreteket használnak az *Időbélyegző*k hitelesítésére, amelyek megfelelnek az alábbi követelményeknek:
  - ETSI TS 119 312 [18];
  - a 2015. évi CCXXII törvény [5] 92. § (1) b) szerint kiadott aktuális Nemzeti Média- és Hírközlési Hatóság algoritmusokkal kapcsolatos határozat.
- az aláíró vagy bélyegző létrehozó magánkulcsot lehetőleg ne importálják egyszerre több *HSM eszköz*be;
- amennyiben több *HSM eszköz* is ugyanazt az aláíró vagy bélyegző létrehozó magánkulcsot használja, akkor azoknak ugyanahhoz a *Tanúsítvány*hoz kell tartozniuk;
- egy *Időbélyegző egység*ben egyidőben csak egy *Időbélyegző* aláíró vagy bélyegző létrehozó magánkulcs lehet aktív;
- egy hardver-szoftver egység több különböző *Időbélyegző egység*et is kiszolgálhat a fenti követelmények betartása esetén.

3.10. Az Időbélyegző szolgáltatás elérési módjai

A *Nem minősített időbélyegzés-szolgáltató* a szolgáltatási szerződés megkötésekor átadja az *Előfizető*nek a szolgáltatás elérhetőségének módját.

4. A tanúsítványok életciklusára vonatkozó követelmények

4.1. A kulcspár és a tanúsítvány használata

4.1.1. A magánkulcs és a tanúsítvány használata

Az *Időbélyegző egység* magánkulcsa kizárólag az *Időbélyegző egység* által kibocsátott *Időbélyegző*k hitelesítésére használható, a magánkulcs más célú felhasználása tilos.

4.1.2. Az Érintett felek nyilvános kulcs és tanúsítvány használata

A *Tanúsítvány* használata során a *Nem minősített időbélyegzés-szolgáltató* által garantált biztonsági szint megtartásához ajánlott, hogy az *Érintett fél* megfelelő körültekintéssel járjon el, különös tekintettel az alábbiakra:

- ellenőrizze a *Tanúsítvány* érvényességét és visszavonási állapotát;
- a *Tanúsítvány*ra vonatkozó ellenőrzéseket célszerű elvégeznie a teljes tanúsítványláncra vonatkozóan;
- javasolt ellenőrizni, hogy a *Tanúsítvány* a célnak megfelelő *Hitelesítési rend* alapján lett-e kibocsátva;
- vegyen figyelembe minden korlátozást, amely a *Tanúsítvány*ban vagy a *Tanúsítvány*ban meghivatkozott szabályzatokban szerepel.

5. Elhelyezési, eljárásbeli és üzemeltetési előírások

A *Nem minősített időbélyegzés-szolgáltató* széles körben elismert szabványoknak megfelelő fizikai, eljárásbeli és személyzeti biztonsági óvintézkedéseket, valamint az ezeket érvényre juttató adminisztratív és irányítási eljárásokat alkalmaz.

A *Nem minősített időbélyegzés-szolgáltató* nyilvántartást vezet a szolgáltatás nyújtásával kapcsolatos rendszerelemekről és erőforrásokról, és ezekkel kapcsolatos kockázatelemzést végez. Az egyes elemekkel kapcsolatban a kockázatokkal arányos védelmi megoldásokat alkalmaz.

A *Nem minősített időbélyegzés-szolgáltató* figyelemmel kíséri a kapacitás igényeket és biztosítja, hogy megfelelő feldolgozási teljesítmény és tárolási kapacitás álljon rendelkezésre a szolgáltatás nyújtásához.

5.1. Fizikai követelmények

A *Nem minősített időbélyegzés-szolgáltató* gondoskodik arról, hogy a kritikus szolgáltatásokhoz történő fizikai hozzáférés ellenőrzött legyen és a kritikus szolgáltatások eszközeit érintő fizikai kockázatát minimalizálja.

A fizikai óvintézkedések célja a *Nem minősített időbélyegzés-szolgáltató* által birtokolt információra illetve fizikai zónáira irányuló jogosulatlan hozzáférés, károkozás és illetéktelen behatolás megakadályozása.

A kritikus és érzékeny információt feldolgozó szolgáltatásokat biztonságos helyszíneken valósítják meg a *Nem minősített időbélyegzés-szolgáltató* rendszerében.

A biztosított védelem mértéke megfelel a *Nem minősített időbélyegzés-szolgáltató* által végzett kockázatelemzésben megállapított fenyegetettség mértékének.

A megfelelő védelem biztosítása érdekében:

- A *Nem minősített időbélyegzés-szolgáltató* védett számítógéptermében valósítja meg a szigorúbban védendő szolgáltatásokat. Ez a számítógépterem speciálisan erre a célra lett tervezve és kialakítva, tervezésénél különböző védelmi szempontok [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.] egységes érvényesítésére került sor.
- A *Nem minősített időbélyegzés-szolgáltató* valamennyi kritikus szolgáltatását egy külön biztonsági zónában valósítja meg, az ehhez szükséges valamennyi eszközt egy – a biztonsági zóna részét képező – védett számítógépteremben helyezi el.

5.1.1. A telephely elhelyezése és szerkezeti felépítése

A *Nem minősített időbélyegzés-szolgáltató* informatikai rendszereit fizikai és logikai védelemmel ellátott, megfelelően biztonságos *Adatközpont*ban helyezte el és üzemelteti, amely megakadályozza az illetéktelen hozzáférést. Az *Adatközpont* elhelyezése és kialakítása során egymásra épülő és egymást támogató védelmi megoldásokat alkalmaz – őrzés, biztonsági zárak, behatolás érzékelők, videó megfigyelő rendszer, beléptető rendszer stb. – amelyek együttesen egy erős védelmi szintet biztosítanak a szolgáltatásban részt vevő informatikai rendszerek és a szolgáltató által tárolt bizalmas adatok megóvására.

5.1.2. Fizikai hozzáférés

A *Nem minősített időbélyegzés-szolgáltató* védi a szolgáltatás nyújtásában részt vevő eszközeit és berendezéseit a jogosulatlan fizikai hozzáféréstől az eszközök manipulálásának megakadályozása érdekében. A *Nem minősített időbélyegzés-szolgáltató* biztosítja, hogy:

- az *Adatközpont*ba történő minden belépés regisztrálásra kerül;
- az *Adatközpont*ba csak a megfelelő jogosultságokkal rendelkező, bizalmi szerepkört betöltő munkatársak léphetnek be önállóan;
- az önálló jogosultsággal nem rendelkező személyek csak indokolt esetben, a szükséges ideig tartózkodhatnak a gépteremben megfelelő jogosultságú kísérő személyzettel;
- a belépési logokat folyamatosan archiválják és legalább hetente megvizsgálják.

Az eszközök aktivizáló adatai (jelszavak, PIN kódok) a géptermen belül sem tárolhatók nyílt formában.

Jogosulatlan személyek jelenlétében:

- a bizalmas adatokat tartalmazó adathordozókat fizikailag elzárva tartják;

- a bejelentkezett terminálokat nem hagyják felügyelet nélkül;
- nem végeznek olyan munkafolyamatot, amely során bizalmas adat felfedésre kerülhet.

A gépterem elhagyásakor az adminisztrátornak ellenőriznie kell, hogy:

- az *Adatközpont* minden berendezése megfelelően biztonságos üzemállapotban van;
- egyetlen terminálon sem maradt bejelentkezve;
- a fizikai tároló eszközök megfelelően be lettek zárva;
- a fizikai védelmet biztosító rendszerek, berendezések megfelelően működnek;
- a riasztó rendszer aktiválva lett.

A rendszeres fizikai biztonsági vizsgálatokat kijelölt felelősök végzik. A vizsgálatok eredményét megfelelő naplóbejegyzésekben rögzítik.

5.1.3. Áramellátás és légkondicionálás

A *Nem minősített időbélyegzés-szolgáltató Adatközpont*jában olyan szünetmentes áramellátó rendszert alkalmaz, amely:

- megfelelő teljesítménnyel rendelkezik az adatközpont informatikai és a kisegítő létesítményi rendszerei áramellátásának biztosítására;
- megvédi az informatikai berendezéseket a külső hálózatból érkező feszültség ingadozások, feszültség kimaradások, tüskék és egyéb zavarok ellen;
- tartós áramszünet esetére saját áramtermelő berendezéssel rendelkezik, amely - üzemanyag utántöltést lehetővé téve - tetszőleges időtartamig képes a szükséges energia biztosítására.

Az *Adatközpont*ba nem juthat be közvetlenül a külső környezet levegője. Az *Adatközpont* levegőjének tisztaságát megfelelő szűrőrendszer alkalmazása biztosítja, amely kiszűri a levegőből a különféle szennyeződéseket (por, szennyező anyagok, korrozív anyagok, mérgező vagy gyúlékony anyagok). A szellőző rendszer megfelelő szűrés mellett biztosítja az operátorok biztonságos munkavégzéséhez szükséges mennyiségű friss levegőt.

A levegő nedvességtartalma az informatikai rendszerek által megkívánt szintre van csökkentve.

A *Nem minősített időbélyegzés-szolgáltató* megfelelő teljesítményű hűtőrendszert használ a szükséges üzemi hőmérséklet biztosítása, az informatikai eszközök túlhevülésének megakadályozása érdekében.

5.1.4. Beázás és elárasztódás veszély kezelése

A *Nem minősített időbélyegzés-szolgáltató* biztonsági zónájának kialakítása során fontos szempont volt a beázás és elárasztódás veszélyének minimalizálása. A biztonsági zóna teljes területe mentes a vizesblokkoktól, nincs a közelében sem csatorna sem vízvezeték. A védett számítógépteremben a biztonságot tovább növeli az álpadló alkalmazása.

5.1.5. Tűz megelőzés és tűzvédelem

A *Nem minősített időbélyegzés-szolgáltató Adatközpont*jában az illetékes tűzoltóparancsnokság által jóváhagyott tűzvédelmi rendszer működik.

Minden helyiségben jól látható helyen található a vonatkozó előírásoknak megfelelő típusú és mennyiségű kézi tűzoltó készülék.

5.1.6. Adathordozók tárolása

A *Nem minősített időbélyegzés-szolgáltató* megvédi valamennyi adathordozóját a jogosulatlan hozzáféréstől és a véletlen rongálódástól. Minden napló és archív adatot legalább két példányban hoz létre. A példányokat egymástól fizikailag elkülönítve tárolja, egymástól biztonságos távolságra lévő helyszíneken. A tárolt adathordozókat védi a káros környezeti behatásoktól, mint pl. alacsony vagy magas hőmérséklet, szennyeződés, nedvesség, napfény, erős mágneses tér, erős sugárzás.

A *Nem minősített időbélyegzés-szolgáltató* az elsődleges adathordozókat kódzáras, tűzálló páncélszekrényekben tárolja a hitelesítő szervezet operátori helyiségében, a másolati példányokat páncélszekrényben az ügyfélszolgálati irodában.

5.1.7. Hulladék megsemmisítése

A *Nem minősített időbélyegzés-szolgáltató* a környezetvédelmi előírások betartásával gondoskodik feleslegessé vált eszközeinek, adathordozóinak megsemmisítéséről.

A *Nem minősített időbélyegzés-szolgáltató* a bizalmas minősítésű adatokat tartalmazó elektronikus adathordozókat még tartalmuk törlése után sem használja fel nem bizalmas minősítésű adatok tárolására, az ilyen eszközök nem vihetők ki a *Nem minősített időbélyegzés-szolgáltató* területéről. A *Nem minősített időbélyegzés-szolgáltató* a meghibásodott vagy bármely más okból használhatatlanná, feleslegessé vált, bizalmas minősítésű adatokat tartalmazó adathordozókat – a selejtezési szabályzatának megfelelően – fizikailag megsemmisíti:

- a papíralapú dokumentumokat iratmegsemmisítő géppel felaprítja;
- a merevlemezeket szétszereli és a kritikus alkatrészeket összetöri;
- az optikai lemezeket erre alkalmas iratmegsemmisítő géppel megsemmisíti.

5.1.8. A mentési példányok fizikai elkülönítése

A *Nem minősített időbélyegzés-szolgáltató* legalább heti rendszerességgel előállít olyan mentést, amiből meghibásodás esetén a teljes szolgáltatás helyreállítható. A mentéseket - legalább az utolsó teljes mentést is beleértve - egy olyan külső helyszínen tárolja, amelynek a fizikai és működési védelme azonos az elsődleges helyszínével. Az elsődleges és a tartalék helyszínek között biztosítja az adatok biztonságos továbbítását.

A mentett állományokból legalább évente szúrópróbaszerű kiválasztással jegyzőkönyvezett helyreállítási tesztet végez.

5.2. Eljárásbeli előírások

A *Nem minősített időbélyegzés-szolgáltató* gondoskodik arról, hogy rendszereit biztonságosan, szabályszerűen, a meghibásodás minimális kockázata mellett üzemeltesse.

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

A *Nem minősített időbélyegzés-szolgáltató* belső irányítási rendszere biztosítja a jogszabályoknak és belső szabályzatainak megfelelő működést. Rendszerében minden rendszerelemhez és minden folyamathoz egyértelműen hozzárendelhető az adott rendszerelemért, vagy folyamatért felelős személy. A *Nem minősített időbélyegzés-szolgáltató* rendszerében élesen elkülönülnek egymástól a fejlesztési és üzemeltetési folyamatok. A rendszer megfelelő működését a független rendszervizsgáló és a *Nem minősített időbélyegzés-szolgáltató* belső folyamatainak rendszeres ellenőrzése biztosítja.

5.2.1. Bizalmi szerepkörök

A *Nem minősített időbélyegzés-szolgáltató* feladatai ellátásához bizalmi szerepköröket hozott létre. A jogosultságok és funkciók oly módon lettek megosztva az egyes bizalmi szerepkörök között, hogy egyedül egyetlen felhasználó se legyen képes a biztonsági védelmi intézkedések megkerülésére.

A *Nem minősített időbélyegzés-szolgáltató* a következő bizalmi szerepköröket határozza meg az alábbi felelősségi körökkel:

A *Nem minősített időbélyegzés-szolgáltató* informatikai rendszeréért általánosan felelős vezető: Az informatikai rendszerért felelős személy.

Biztonsági tisztviselő: Biztonságtechnikai főmunkatárs, a szolgáltatás biztonságáért általánosan felelős személy.

Rendszeradminisztrátor: Infrastruktúra adminisztrátor. Feladata a *Nem minősített időbélyegzés-szolgáltató* rendszereinek telepítése, konfigurálása, karbantartása. Felelős a rábízott rendszerelemek megbízható és folyamatos működéséért, valamint a technológia fejlődésének nyomon követéséért, az egyes rendszerelemekben való biztonsági rések felderítéséért és megoldási javaslatok kidolgozásáért.

Operátor: Rendszerüzemeltető, az informatikai rendszer folyamatos üzemeltetését, mentését és helyreállítását végző személy.

Független rendszervizsgáló: A *Nem minősített időbélyegzés-szolgáltató* naplózott, illetve archivált adatállományát vizsgáló, a *Nem minősített időbélyegzés-szolgáltató* által a szabályszerű működés érdekében megvalósított kontroll intézkedések betartásának ellenőrzéséért, a meglévő eljárások folyamatos vizsgálatáért és monitorozásáért felelős személy.

A bizalmi szerepkörök ellátására a *Nem minősített időbélyegzés-szolgáltató* biztonságért felelős vezetője formálisan kinevezi a *Nem minősített időbélyegzés-szolgáltató* munkatársait.

Bizalmi szerepkört csak a *Nem minősített időbélyegzés-szolgáltató*val munkaviszonyban álló személyek láthatnak el, megbízási szerződés keretében a bizalmi szerepkörök nem láthatók el.

A bizalmi szerepkörökről a *Nem minősített időbélyegzés-szolgáltató* naprakész nyilvántartást vezet, a változásokat haladéktalanul bejelenti a Nemzeti Média- és Hírközlési Hatóságnak.

5.2.2. Az egyes feladatok ellátásához szükséges személyzeti létszámok

A *Nem minősített időbélyegzés-szolgáltató* biztonsági és üzemeltetési szabályzata előírja, hogy csak védett környezetben, kettő, bizalmi szerepkört betöltő munkatárs egyidejű fizikai jelenlétében végezhetők el az alábbi műveletek:

- a *Nem minősített időbélyegzés-szolgáltató* saját szolgáltatói kulcspárjának generálása;
- a szolgáltatói magánkulcs mentése;
- a szolgáltatói magánkulcs aktiválása;
- a szolgáltatói magánkulcs megsemmisítése.

A felsorolt műveleteket végrehajtó személyek közül legalább az egyiknek rendszeradminisztrátornak kell lennie és a másik személy nem lehet független rendszervizsgáló.

A felsorolt műveletek végrehajtása során illetéktelen személy nem lehet jelen a helyiségben.

5.2.3. Az egyes szerepkörökben elvárt azonosítás és hitelesítés

A *Nem minősített időbélyegzés-szolgáltató* informatikai rendszerét kezelő felhasználók egyedi azonosító adatokkal rendelkeznek, amely lehetővé teszi a felhasználók biztonságos azonosítását és hitelesítését.

A felhasználók a hitelesítés-szolgáltatás szempontjából kritikus informatikai rendszerekhez csak azonosítás és hitelesítés után férhetnek hozzá.

Az azonosító és hitelesítő adatok a felhasználói jogosultságok megszűnésekor haladéktalanul visszavonásra kerülnek.

Az informatikai rendszer minden felhasználója és az adminisztratív folyamatok minden szereplője személy szerint kerül azonosításra. A fizikai hozzáférés ellenőrzéséhez a *Nem minősített időbélyegzés-szolgáltató* RFID kártyára épülő beléptető rendszert használ, a logikai hozzáférés ellenőrzése *Elektronikus aláírást létrehozó eszköz*ön kiadott VPN *Tanúsítvány*ok segítségével történik. Sikeres hitelesítés nélkül egyetlen biztonsági szempontból kritikus feladatot sem lehet végrehajtani. A *Nem minősített időbélyegzés-szolgáltató* minden munkatársa annak megfelelő hozzáférési jogosultsággal rendelkezik, amely a feladatköre ellátásához elengedhetetlenül szükséges.

5.2.4. Egymást kizáró szerepkörök

A *Nem minősített időbélyegzés-szolgáltató* munkatársai egyidejűleg több bizalmi szerepkört is betölthetnek, de a *Nem minősített időbélyegzés-szolgáltató* biztosítja, hogy:

- a biztonsági tisztviselő és a regisztrációs felelős nem töltheti be a független rendszervizsgálói szerepkört;

- a rendszeradminisztrátor nem töltheti be a biztonsági tisztviselő és a független rendszervizsgálói szerepkört;
- az informatikai rendszerért általánosan felelős vezető nem láthatja el a biztonsági tisztviselő és a független rendszervizsgáló feladatkörét.

A fentieken túl a *Nem minősített időbélyegzés-szolgáltató* törekszik a bizalmi szerepkörök teljes szétválasztására.

5.3. Személyzetre vonatkozó előírások

A *Nem minősített időbélyegzés-szolgáltató* gondoskodik arról, hogy személyzeti politikája, illetve a munkatársak alkalmazására vonatkozó gyakorlata fokozza és támogassa a *Nem minősített időbélyegzés-szolgáltató* működésének megbízhatóságát. A személyzetre vonatkozó óvintézkedések célja az emberi hibák, lopás, csalás és a visszaélések kockázatának csökkentése.

A *Nem minősített időbélyegzés-szolgáltató* már a felvételi szakaszban foglalkozik a személyi biztonsággal, beleértve a szerződések megkötését, illetve azok alkalmazás során történő ellenőrzését. Valamennyi bizalmi szerepkör esetén a szerepkört betöltő személyeknek kinevezésükkor érvényes erkölcsi bizonyítvánnyal kell rendelkezniük. Minden bizalmi szerepkört betöltő alkalmazottnak és külső félnek – aki a *Nem minősített időbélyegzés-szolgáltató* szolgáltatásaival kapcsolatba kerül – titoktartási nyilatkozatot kell aláírnia.

A *Nem minősített időbélyegzés-szolgáltató* egyúttal biztosítja valamennyi munkakör betöltéséhez a szükséges közös, általános, illetve az egyes szerepkörök betöltéséhez szükséges speciális szakmai ismeretek megszerzését, illetve továbbfejlesztését.

5.3.1. Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

Felvételi követelményként a *Nem minősített időbélyegzés-szolgáltató* minden dolgozója számára legalább középfokú végzettséget ír elő, de a *Nem minősített időbélyegzés-szolgáltató* a továbbiakban is gondot fordít arra, hogy dolgozói megfelelő képzésben részesüljenek. Közvetlenül a felvételt követően a *Nem minősített időbélyegzés-szolgáltató* új dolgozóit képzésben részesíti, melynek keretében el kell sajátítania a munkája elvégzéséhez szükséges ismereteket. A *Nem minősített időbélyegzés-szolgáltató* általában támogatja a dolgozók szakmai fejlődését, valamint elvárja, hogy a dolgozók saját szakterületükön önállóan fejlesszék tudásukat. A *Nem minősített időbélyegzés-szolgáltató* bizonyos dolgozóinak munkaköri kötelessége a technikai és üzleti újdonságok felderítése és összegyűjtése, rendszerezése, és ezen ismeretek megosztása munkatársaikkal.

A *Nem minősített időbélyegzés-szolgáltató*nál bizalmi szerepkört csak olyan személy tölthet be, akinek a befolyásmentességét és szakértelmét a *Nem minősített időbélyegzés-szolgáltató* igazolni tudja. A bizalmi szerepkört betöltő személyeknek mentesnek kell lenniük az összeférhetetlenségtől, amely veszélyeztethetné a *Nem minősített időbélyegzés-szolgáltató* tevékenységének pártatlanságát.

Az informatikai rendszerért általánosan felelős vezető csak olyan személy lehet, aki rendelkezik:

- szakirányú felsőfokú végzettséggel (matematikusi, fizikusi egyetemi végzettség vagy a műszaki tudományterületre tartozó mérnöki szakon szerzett főiskolai vagy egyetemi végzettség);

- legalább három év, az informatikai biztonsággal összefüggésben szerzett szakmai gyakorlattal.

5.3.2. Előélet vizsgálatára vonatkozó eljárások

A *Nem minősített időbélyegzés-szolgáltató* vezető munkakörben illetve bizalmi szerepkörben csak olyan alkalmazottakat foglalkoztat, akik:

- büntetlen előélettel rendelkeznek és nincs ellenük folyamatban olyan eljárás, amely a büntetlenséget befolyásolhatja;
- nem állnak a bizalmi szolgáltatási tevékenység gyakorlását kizáró foglalkozástól eltiltás hatálya alatt.

Kinevezéskor a *Nem minősített időbélyegzés-szolgáltató* vezető munkakört betöltő alkalmazottjának nyilatkozatával, bizalmi szerepkört betöltő alkalmazottjának 3 hónapnál nem régebbi erkölcsi bizonyítvánnyal kell igazolnia büntetlen előéletét.

A *Nem minősített időbélyegzés-szolgáltató* a felvételi eljárás során ellenőrzi a jelentkező önéletrajzában megadott releváns információk valódiságát, úgy mint előző munkahely, szakmai referenciák, legfontosabb képzettség.

5.3.3. Képzési követelmények

A *Nem minősített időbélyegzés-szolgáltató* az újonnan felvett alkalmazottakat képzésben részesíti, amely során elsajátítják az adott munkakör ellátásához szükséges mértékben:

- a PKI alapismereteket;
- a *Nem minősített időbélyegzés-szolgáltató* informatikai rendszerének sajátosságait és kezelésének módját;
- a szerepkörük ellátásához szükséges speciális ismereteket;
- a *Nem minősített időbélyegzés-szolgáltató* nyilvános és belső szabályzataiban meghatározott folyamatokat, eljárásokat;
- az egyes tevékenységek jogi következményeit;
- az alkalmazandó informatikai biztonsági szabályokat;
- az adatvédelmi szabályokat.

A *Nem minősített időbélyegzés-szolgáltató* éles informatikai rendszereihez csak a képzést sikeresen teljesítő alkalmazottak kapnak hozzáférési jogosultságot.

5.3.4. Továbbképzési gyakoriságok és követelmények

A *Nem minősített időbélyegzés-szolgáltató* gondoskodik arról, hogy az alkalmazottak folyamatosan a megfelelő tudással rendelkezzenek, így szükség esetén továbbképzést, vagy ismétlő jellegű képzést kell tartani.

A *Nem minősített időbélyegzés-szolgáltató* továbbképzést tart, ha folyamataiban vagy informatikai rendszerében változás áll be.

A képzési anyag legalább 12 havonta felülvizsgálatra kerül, és tartalmazza az új fenyegetéseket és biztonsági megoldásokat.

A továbbképzés megfelelően dokumentálásra kerül, amelyből egyértelműen megállapítható a továbbképzés tematikája és a résztvevő dolgozók köre.

5.3.5. Munkabeosztás körforgásának sorrendje és gyakorisága

A *Nem minősített időbélyegzés-szolgáltató* nem alkalmaz kötelező jellegű körforgást az egyes munkabeosztások között.

5.3.6. Felhatalmazás nélküli tevékenységek büntető következményei

A *Nem minősített időbélyegzés-szolgáltató* a dolgozókkal kötendő munkaszerződésben szabályozza a dolgozók felelősségre vonásának lehetőségeit a dolgozó által elkövetett mulasztások, hibák, vétlen vagy szándékos károkozások esetére. Amennyiben egy munkatárs – szándékosan vagy gondatlanul – kötelezettségeit megsérti, vele szemben a *Nem minősített időbélyegzés-szolgáltató* szankciót alkalmazhat, amelyet az elkövetés módjára és következményeire tekintettel állapít meg. Szankcióként alkalmazható a jutalom megvonása, fegyelmi eljárás, elbocsátás, kinevezés visszavonása vagy büntetőjogi felelősségre vonás kezdeményezése.

Valamennyi bizalmi szerepkört betöltő munkatárs a szerepkörbe kinevezéskor a foglalkoztatási dokumentumok részeként:

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

A felsorolt dokumentumok tartalmazzák azokat a munkajogi következményeket és egyéb szankciókat, amelyek kötelezettségszegés esetén alkalmazhatóak.

5.3.7. Szerződéses viszonyban foglalkoztatottakra vonatkozó követelmények

A *Nem minősített időbélyegzés-szolgáltató* bizalmi munkakörben csak vele munkaviszonyban álló személyt alkalmaz.

Az egyéb feladatok ellátására alvállalkozói vagy megbízásos szerződésben foglalkoztatott szerződő személyeket a *Nem minősített időbélyegzés-szolgáltató* lehetőség szerint a korábban már minősített

beszállítók listájáról választ. A beszállítókkal a *Nem minősített időbélyegzés-szolgáltató* a munkavégzést megelőzően írásban szerződést köt.

Valamennyi szerződő fél – még a tényleges munkavégzés megkezdése előtt – titoktartási nyilatkozatot ír alá, melyben vállalja, hogy a munkavégzés során későbbiekben megismert üzleti/vállalati titkokat illetéktelen személynek nem fedi fel, egyéb módon nem hasznosítja. A titoktartási nyilatkozat tartalmazza a megszegése esetén alkalmazandó szankciókat is. A szerződés alapján foglalkoztatott külső munkavállalókkal szemben elvárás a megfelelő szakismeret megléte, részükre a *Nem minősített időbélyegzés-szolgáltató* nem tart képzéseket.

5.3.8. A személyzet számára biztosított dokumentációk

A *Nem minősített időbélyegzés-szolgáltató* folyamatosan biztosítja a dolgozók részére a szerepkörük ellátásához szükséges aktuális dokumentációk, szabályzatok rendelkezésre állását.

Minden bizalmi munkakört betöltő munkatárs írásban megkapja a következő dokumentumokat:

- a *Nem minősített időbélyegzés-szolgáltató* szervezeti biztonsági szabályzata;
- aláírandó titoktartási nyilatkozat;
- egyéni munkaköri leírás;
- a tervezett és rendkívüli továbbképzések alkalmával az adott oktatási formához tartozó oktatási segédanyagokat.

A szervezeti biztonsági szabályzatban bekövetkező változásokról írásos értesítő formájában minden dolgozó tájékoztatást kap.

5.4. Naplózási eljárások

A *Nem minősített időbélyegzés-szolgáltató* a biztonságos informatikai környezet fenntartása érdekében a teljes informatikai rendszerét átfogó eseménynaplózó és ellenőrző rendszert üzemeltet.

5.4.1. A tárolt események típusai

A *Nem minősített időbélyegzés-szolgáltató* az általánosan elfogadott informatikai biztonsági gyakorlatnak megfelelően naplóz minden olyan biztonsággal kapcsolatos eseményt, amely információt szolgáltathat az informatikai rendszerben vagy annak fizikai környezetében történt eseményekről, változásokról. Minden naplóbejegyzésnél eltárolja:

- az esemény időpontját;
- az esemény típusát;
- a végrehajtás sikerességét illetve sikertelenségét;
- a felhasználó vagy rendszer azonosítóját, aki/amely az eseményt kiváltotta.

Az összes lényeges naplóbejegyzést elérhetővé teszi a független rendszervizsgálók részére, akik a *Nem minősített időbélyegzés-szolgáltató* működésének megfelelőségét vizsgálják.

A *Nem minősített időbélyegzés-szolgáltató* naplózza minimálisan az alábbi eseményeket:

- IDŐBÉLYEGZÉS
  - az *Időbélyegző*k kibocsátásával kapcsolatos események;
  - az óra szinkronizációja az UTC időhöz, beleértve az üzemszerű újrakalibrálásokat is;
  - a szinkronizáció elvesztése;
- NAPLÓZÁS
  - a naplózó rendszer vagy egyes komponenseinek leállítása, újraindítása;
  - a naplózás bármilyen beállításának módosítása, mint pl. gyakoriság, riasztási küszöb érték, vizsgált esemény;
  - a tárolt naplózási adatok módosítása vagy törlése;
  - a naplózó rendszer hibája miatt végzett tevékenységek;
- RENDSZER BEJELENTKEZÉSEK
  - sikeres bejelentkezések, sikertelen bejelentkezési próbálkozások bizalmi szerepkörökbe;
  - jelszó alapú azonosítás esetén:
    * az engedélyezett sikertelen bejelentkezési próbálkozások számának megváltoztatása;
    * az engedélyezett sikertelen bejelentkezési próbálkozások számának elérése felhasználói bejelentkezéskor;
    * sikertelen bejelentkezések miatt zárolt felhasználó újbóli engedélyezése;
  - az azonosítási technika változtatása (például jelszó alapúról PKI alapúra);
- KULCSKEZELÉS
  - a szolgáltatói kulcsok teljes életciklusára vonatkozó valamennyi esemény (kulcsgenerálás, betöltés, elmentés stb.);
- TANÚSÍTVÁNY KEZELÉS
  - az *Időbélyegző egység*ek *Tanúsítvány*ainak kibocsátásával, állapotváltozásával kapcsolatos minden esemény;
- ADATMOZGÁSOK
  - bármilyen, a biztonság szempontjából kritikus adat manuális bevitele a rendszerbe;
  - a rendszer által fogadott, biztonsági szempontból fontos adatok, üzenetek;
- HSM
  - HSM installálása;

  - HSM eltávolítása;
  - HSM selejtezése, megsemmisítése;
  - HSM szállítása;
  - HSM tartalmának törlése (nullázás);
  - HSM feltöltése kulcsokkal, tanúsítványokkal;
- KONFIGURÁCIÓ VÁLTOZÁSA
  - hardver;
  - szoftver;
  - operációs rendszer;
  - javító csomag;
- FIZIKAI HOZZÁFÉRÉS, TELEPHELY BIZTONSÁG
  - személy belépése a CA komponenseket tartalmazó biztonsági területre és onnan kilépése;
  - hozzáférés egy CA rendszer komponenshez;
  - a fizikai biztonság ismert vagy gyanított megsértése;
  - tűzfal és router forgalmak;
- MŰKÖDÉSI RENDELLENESSÉGEK
  - rendszerösszeomlás, hardver hiba;
  - szoftveres hibák;
  - szoftverintegritás ellenőrzési hiba;
  - hibás vagy rossz helyre továbbított üzenetek;
  - hálózatot ért támadások, támadási kísérletek;
  - berendezés hiba;
  - elektromos hálózati üzemzavar;
  - szünetmentes tápegység hiba;
  - lényeges hálózati szolgáltatás hozzáférési hiba;
  - a *Nem minősített időbélyegzési rend* vagy a *Nem minősített időbélyegzési szolgáltatási szabályzat* megsértése;
  - operációs rendszer órájának törlése;
- EGYÉB ESEMÉNYEK
  - személy kinevezése biztonsági szerepkörbe;
  - operációs rendszer telepítése;
  - PKI alkalmazás telepítése;
  - rendszer elindítása;
  - belépési kísérlet a PKI alkalmazásba;

– jelszó módosítási, beállítási kísérlet;
– a belső adatbázis elmentése, visszaállítása mentésből;
– fájl műveletek (pl. létrehozás, átnevezés, áthelyezés);
– adatbázis hozzáférés.

5.4.2. A naplófájl feldolgozásának gyakorisága

A *Nem minősített időbélyegzés-szolgáltató* független rendszervizsgálói a keletkezett naplóbejegyzéseket minden munkanapon átvizsgálják.

A kiértékelés során meggyőződnek a vizsgált naplóállományok hitelességéről és sértetlenségéről, ellenőrzik a bejegyzésekben talált hibaüzeneteket, szükség esetén dokumentálják az eltérést és intézkedéseket hoznak az eltérés okának megszüntetése érdekében.

Az informatikai rendszerek ellenőrzésére a *Nem minősített időbélyegzés-szolgáltató* automatizált ellenőrző rendszereket is használ, amelyek előre beállított szempontok szerint folyamatosan figyelik a keletkező naplóbejegyzéseket és szükség esetén riasztják az üzemeltetés munkatársait.

A vizsgálat tényе, a vizsgálat eredményei és az esetleges feltárt hiányosságok elhárítása érdekében meghozott intézkedések megfelelően dokumentálásra kerülnek.

5.4.3. A naplófájl megőrzési időtartama

Az online rendszerből való kitörlés előtt a naplóállományokat a *Nem minősített időbélyegzés-szolgáltató* archiválja és gondoskodik azok biztonságos megőrzéséről az 5.5.2 fejezetben meghatározott ideig.

Ezen időtartamig a *Nem minősített időbélyegzés-szolgáltató* biztosítja az archivált adatok olvashatóságát, megőrzi az ehhez szükséges szoftver és hardver eszközöket.

5.4.4. A naplófájl védelme

A *Nem minősített időbélyegzés-szolgáltató* az előírt megőrzési ideig tárolja és védi a keletkezett naplóállományokat. A megőrzési idő teljes időtartama alatt biztosítja a naplóadatok:

- védelmét az illetéktelen felfedés ellen: a naplóállományokhoz csak az arra jogosultak – elsősorban a független rendszervizsgálók – férhetnek hozzá;
- rendelkezésre állását: a jogosultak számára biztosítja a naplóállományokhoz való hozzáférést;
- integritását: megakadályozza például a naplóállományokban bármilyen adat módosítását, törlését, bejegyzések sorrendjének megváltoztatását.

A *Nem minősített időbélyegzés-szolgáltató* a naplóbejegyzéseket minősített *Időbélyegző*vel látja el, a naplóbejegyzések törlések és beszúrások észrevétlen végrehajtását kizáró módon kerülnek tárolásra.

A naplóállományt a véletlen és szándékos rongálások ellen biztonsági mentések védik. A személyes adatokat tartalmazó naplóbejegyzések esetében a *Nem minősített időbélyegzés-szolgáltató* gondoskodik az adatok bizalmas tárolásáról. A naplóállományokhoz való hozzáférésre

csak azok jogosultak, akiknek erre munkakörük folytán feltétlenül szükségük van. A *Nem minősített időbélyegzés-szolgáltató* a hozzáféréseket biztonságos módon ellenőrzi. A naplóállományokat a *Nem minősített időbélyegzés-szolgáltató* biztonságos környezetben őrzi. Az állományokról a működés másodlagos helyszínén másolati példányokat is tart.

5.4.5. A naplófájl mentési eljárásai

Az üzemeltetés során az egyes rendszerekben folyamatosan keletkező naplóbejegyzésekből napi naplóállományok generálódnak.

A napi naplóállományokat a *Nem minősített időbélyegzés-szolgáltató* 2 példányban archiválja és a példányokat egymástól fizikailag elkülönülő helyszíneken az előírt ideig megőrzi.

A mentés operatív folyamatait a *Nem minősített időbélyegzés-szolgáltató* mentési szabályzatai írják le részletesen.

5.4.6. A naplózás adatgyűjtési rendszere

A naplóbejegyzéseket az egyes alkalmazások automatikusan gyűjtik és továbbítják a naplózó rendszer felé.

A naplózó funkciók automatikusan indulnak a rendszer indításakor és a rendszer működésének teljes időtartama alatt folyamatosan működnek.

Az automatikus vizsgáló és naplózó rendszerek működési rendellenessége esetén a *Nem minősített időbélyegzés-szolgáltató* felfüggeszti az érintett területek működését az üzemzavar elhárításáig.

5.4.7. Az eseményeket kiváltó alanyok értesítése

A hibaeseményt kiváltó személyeket, szervezeteket és alkalmazásokat a *Nem minősített időbélyegzés-szolgáltató* nem feltétlenül értesíti minden esetben, szükség esetén azonban bevonhatja őket az esemény kivizsgálásába. Az esemény kiváltásában érintett *Ügyfel*eknek ilyen esetben kötelességük a *Nem minősített időbélyegzés-szolgáltató*val való együttműködés a hiba feltárása érdekében.

5.4.8. Sebezhetőség felmérése

A naplóbejegyzések napi rendszerességgel végzett feldolgozásán túl a *Nem minősített időbélyegzés-szolgáltató* szakemberei havonta áttekintik a rendkívüli eseményeket és a sebezhetőségre vonatkozó elemzéseket végeznek, amely alapján a *Nem minősített időbélyegzés-szolgáltató* szükség esetén intézkedéseket hoz a rendszer biztonságának növelésére.

Minden nagyobb jelentőségű feltárt hiányosság vagy külső fenyegetettség esetén az észlelésétől számított 48 órán belül, de legalább évente egyszer a *Nem minősített időbélyegzés-szolgáltató* szakemberei átfogó sebezhetőség vizsgálatot végeznek, amely segítségével feltérképezik a potenciális belső és külső fenyegetettségeket, amelyek jogosulatlan hozzáféréseket eredményezhetnek.

A vizsgálat eredményei alapján a *Nem minősített időbélyegzés-szolgáltató* szükség esetén továbbfejleszti folyamatait, rendszereit a szolgáltatás általános biztonságának növelése érdekében.

5.5. Adatok archiválása

5.5.1. Az archivált adatok típusai

A *Nem minősített időbélyegzés-szolgáltató* felkészült elektronikus és papíralapú dokumentumok megfelelően biztonságos, hosszú idejű archiválására.
A *Nem minősített időbélyegzés-szolgáltató* minimálisan az alábbi jellegű információt archiválja:

- a *Nem minősített időbélyegzés-szolgáltató* akkreditációjával kapcsolatos valamennyi irat;
- a *Nem minősített időbélyegzési rend*(ek) és *Nem minősített időbélyegzési szolgáltatási szabályzat*(ok) valamennyi kibocsátott verziója;
- az Általános szerződési feltételek valamennyi kibocsátott verziója;
- a *Nem minősített időbélyegzés-szolgáltató* működésével kapcsolatos szerződések;
- valamennyi elektronikus és papíralapú naplóbejegyzés.

5.5.2. Az archívum megőrzési időtartama

A *Nem minősített időbélyegzés-szolgáltató* az archivált adatokat az alábbi időtartamokig őrzi meg:

- a *Nem minősített időbélyegzési szolgáltatási szabályzat*ot a hatályon kívül helyezéstől számított 10 évig;
- az *Időbélyegző* kibocsátásával kapcsolatos főbb adatokat a kibocsátástól számított legalább 10 évig.

5.5.3. Az archívum védelme

A *Nem minősített időbélyegzés-szolgáltató* valamennyi archivált adatot két példányban, két egymástól fizikailag elkülönült helyszínen őrzi. Az egyetlen hiteles példányban rendelkezésre álló papíralapú dokumentumról hiteles papíralapú, vagy elektronikus másolatot készít a vonatkozó jogszabályok betartásával.
A két helyszín mindegyike teljesíti az archiválással szemben támasztott biztonsági és egyéb követelményeket.
Az archivált adatok megőrzése során a *Nem minősített időbélyegzés-szolgáltató* gondoskodik az archivált adatok

- sértetlenségének megőrzéséről;
- illetéktelen megismerés elleni védelméről;
- rendelkezésre állásáról;
- hitelességének megőrzéséről.

Az archivált elektronikus adatokat legalább fokozott biztonságú elektronikus aláírással vagy bélyegzővel és minősített *Időbélyegző*vel látja el.

5.5.4. Az archívum mentési folyamatai

A *Nem minősített időbélyegzés-szolgáltató* a papír alapú dokumentumok eredeti példányáról hiteles elektronikus másolatot készít a vonatkozó jogszabályok betartásával.

Az elektronikus másolatokat a többi védendő elektronikus dokumentummal azonos szabályok szerint tárolja.

A *Nem minősített időbélyegzés-szolgáltató* a hiteles elektronikus másolatok archiválása után az eredeti papír alapú dokumentumokat megsemmisítheti.

5.5.5. Az adatok időbélyegzésére vonatkozó követelmények

Valamennyi elektronikus naplóbejegyzés tartalmaz időjelzést, amelyen legalább másodperc pontossággal fel van tüntetve a rendszer által szolgáltatott időpont.

A *Nem minősített időbélyegzés-szolgáltató* biztosítja, hogy a szolgáltatást nyújtó rendszerein a gépidő maximum 1 másodpercre tér el a referenciaidőtől. Az időjel előállításához használt gépidőt naponta legalább négy alkalommal szinkronizálja az UTC időhöz.

A *Nem minősített időbélyegzés-szolgáltató* a napi naplóállományokat minősített *Időbélyegző*vel látja el.

Az archivált adatok megőrzése során szükség esetén (pl. algoritmusváltás, az eredeti *Időbélyegző* érvényességének lejárata) a *Nem minősített időbélyegzés-szolgáltató* gondoskodik az adatok hitelességének megőrzéséről.

5.5.6. Az archívum gyűjtési rendszere

A *Nem minősített időbélyegzés-szolgáltató* védett informatikai rendszerén belül keletkeznek a naplóbejegyzések, onnan csak az elektronikusan aláírt, minősített *Időbélyegző*vel védett naplóállományok kerülhetnek ki.

A szolgáltatás nyújtása során keletkezett papíralapú iratok egy eredeti példányát a *Nem minősített időbélyegzés-szolgáltató* az általa működtetett belső adattárban tárolja és őrzi.

5.5.7. Archív információk hozzáférését és ellenőrzését végző eljárások

A *Nem minősített időbélyegzés-szolgáltató* a naplóállományok előállítását automatikusan végzi, a hitelesített naplóállományokat naponta állítja elő.

Az archivált adatállományokat védi a jogosulatlan hozzáféréstől.

Az arra jogosultaknak biztosítja az archivált adatokhoz való ellenőrzött hozzáférést:

- az *Ügyfel*ek jogosultak a róluk tárolt adatok megtekintésére;
- jogi eljárásokban bizonyíték nyújtása céljából biztosítani kell a szükséges adatokat.

5.6. Szolgáltatói kulcs cseréje

A *Nem minősített időbélyegzés-szolgáltató* gondoskodik arról, hogy az általa használt *Időbélyegző egység*ek folyamatosan rendelkezzenek a működéshez szükséges, érvényes kulccsal

és Tanúsítvánnyal. A szolgáltatói *Tanúsítvány*ok lejárta illetve a hozzájuk kapcsolódó kulcsok használati idejének lejárta előtt elegendő idővel új kulcspárt generál az *Időbélyegző egység* számára, és arról időben értesíti *Ügyfel*eit. Az új szolgáltatói kulcsot a jelen szabályzatnak megfelelően generálja és kezeli.

Amennyiben a *Nem minősített időbélyegzés-szolgáltató* megváltoztatja *Időbélyegző*ket kibocsátó bármely szolgáltatói tanúsítványának kulcsait, az alábbiak szerint jár el:

- publikálja az érintett *Tanúsítvány*ait és nyilvános kulcsait a 2.2 fejezetben meghatározott előírásoknak megfelelően;
- a szolgáltatói kulcscsere után a kibocsátandó *Időbélyegző*ket már csak az új szolgáltatói kulcsok felhasználásával írja alá;
- megőrzi a régi szolgáltatói *Tanúsítvány*ait és nyilvános kulcsait, valamint lehetővé teszi érvényességének ellenőrzését mindaddig, amíg a régi szolgáltatói kulccsal aláírt valamennyi *Időbélyegző* érvényességi ideje lejár.

5.7. Kompromittálódást és katasztrófát követő helyreállítás

A *Nem minősített időbélyegzés-szolgáltató* katasztrófa esetén minden szükséges intézkedést meghoz annak érdekében, hogy a szolgáltatáskiesésből eredő károkat minimalizálja és a szolgáltatásokat a lehető legrövidebb időn belül helyreállítsa.

A bekövetkezett incidens kiértékelése alapján meghozza a szükséges módosító, javító intézkedéseket, hogy az incidens jövőbeli előfordulását megakadályozza.

A hiba elhárítása után az eseményt jelenti a Nemzeti Média- és Hírközlési Hatóságnak, mint felügyeleti szervnek.

5.7.1. Váratlan esemény és kompromittálódás kezelési eljárások

A *Nem minősített időbélyegzés-szolgáltató* rendelkezik üzletmenet folytonossági tervvel. Az üzletmenet folytonossági terv tartalmazza az aláíró kulcs kompromittálódása, a kompromittálódás gyanúja és az *Időbélyegző egység* órájának elállítódása esetén követendő eljárásokat.

Kompromittálódás, kompromittálódás gyanúja vagy az *Időbélyegző egység* órájának elállítódása esetén a *Nem minősített időbélyegzés-szolgáltató* közzéteszi az eseménnyel kapcsolatos információt, valamint nem adhat ki *Időbélyegző*ket a veszélyhelyzet elhárításáig.

Kompromittálódás, kompromittálódás gyanúja vagy az *Időbélyegző egység* órájának elállítódása esetén a *Nem minősített időbélyegzés-szolgáltató* honlapján közzéteszi az érintett *Időbélyegző*k beazonosításához szükséges információkat.

A *Nem minősített időbélyegzés-szolgáltató* kialakított és folyamatosan üzemben tart egy teljes értékű tartalékrendszert, amely az elsődleges helyszíntől biztonságos távolságra, földrajzilag különböző helyszínen található és önállóan is alkalmas a szolgáltatások teljes körű ellátására.

A *Nem minősített időbélyegzés-szolgáltató* folyamatosan teszteli a tartalékrendszer működését és évente felülvizsgálja az üzletmenet folytonossági terveit.

A *Nem minősített időbélyegzés-szolgáltató* megnövelt biztonságú eszközökkel és rendszerekkel rendelkezik a hardver és szoftver meghibásodások valamint az adatsérülések okozta szolgáltatáskiesés minimalizálása érdekében. A szolgáltatások helyreállíthatóságát a *Nem minősített időbélyegzés-szolgáltató* háttérszerződései és saját tartalék eszközei garantálják.

5.7.2. Meghibásodott IT erőforrások, szoftverek és/vagy adatok

A *Nem minősített időbélyegzés-szolgáltató* informatikai rendszereit megbízható hardver és szoftver komponensekből építette fel. A kritikus funkciókat redundáns rendszerelemek alkalmazásával valósította meg úgy, hogy azok egy elem meghibásodása esetén is képesek legyenek a további működésre.

A *Nem minősített időbélyegzés-szolgáltató* naponta teljes mentést készít az adatbázisairól és a keletkezett naplózási eseményekről.

A *Nem minősített időbélyegzés-szolgáltató* olyan gyakorisággal készít teljes rendszermentést, amely biztosítja, hogy abból katasztrófa esetén a teljes szolgáltatás helyreállítható legyen.

A *Nem minősített időbélyegzés-szolgáltató* üzletmenet folytonossági terve pontos előírásokat tartalmaz a kritikus rendszerkomponensek meghibásodásának esetén végrehajtandó feladatokra.

A *Nem minősített időbélyegzés-szolgáltató* a hiba elhárítása és a rendszer integritásának helyreállítása után a lehető leghamarabb újraindítja a szolgáltatásait.

5.7.3. Magánkulcs kompromittálódása esetén követendő eljárások

A *Nem minősített időbélyegzés-szolgáltató* katasztrófa elhárítási terve a szolgáltatói magánkulcsok kompromittálódása esetére akciótervvel rendelkezik. Az akcióterv a szolgáltatói nyilvános kulcs és a hozzá tartozó *Tanúsítvány* visszavonása mellett feltárja a kompromittálódás körülményeit, intézkedik valamennyi *Érintett fél* értesítéséről, megteszi a szükséges lépéseket a kompromittálódás megismétlődése ellen és szükség esetén új kulccsal látja el a szolgáltatói egységet és a kompromittálódás által érintett végfelhasználókat. A *Nem minősített időbélyegzés-szolgáltató* valamely hitelesítő egység kulcsának kompromittálódása esetén haladéktalanul megszünteti az adott kulcs használatát.

A szolgáltatói nyilvános kulcsok visszavonásáról *Nem minősített időbélyegzés-szolgáltató* értesítést tesz közzé.

5.7.4. Működés folyamatosságának biztosítása katasztrófát követően

A *Nem minősített időbélyegzés-szolgáltató* üzletmenet folytonossági tervében meghatározta a természeti vagy egyéb katasztrófa miatt bekövetkezett szolgáltatás leállás esetén végrehajtandó feladatokat.

A katasztrófa bekövetkezése esetén haladéktalanul életbe lépteti a rendelkezéseket és megkezdi a károk elhárítását, a szolgáltatások helyreállítását.

A másodlagos szolgáltatási helyszín az elsődleges telephelytől olyan távolságra található, hogy egy valószínűsíthető katasztrófa ne érhesse mindkét helyszínt egyszerre.

A *Nem minősített időbélyegzés-szolgáltató* a lehető legrövidebb időn belül köteles értesíteni az érintett felhasználókat a katasztrófa bekövetkezéséről.

A szolgáltatások helyreállítása után a *Nem minősített időbélyegzés-szolgáltató* a lehető legrövidebb időn belül helyreállítja a katasztrófa során tönkrement eszközeit és az eredeti szolgáltatás biztonsági szintet.

5.8. Az Időbélyegzés-szolgáltató leállítása

A *Nem minősített időbélyegzés-szolgáltató* a szolgáltatások valamelyikének tervezett megszüntetése esetén legkevesebb 60 nappal a szolgáltatás leállítását megelőzően értesíti a végfelhasználókat és a Nemzeti Média- és Hírközlési Hatóságot.

A *Nem minősített időbélyegzés-szolgáltató* a szolgáltatás leállítására vonatkozó bejelentéssel egyidejűleg nem köt újabb előfizetői szerződést.

A *Nem minősített időbélyegzés-szolgáltató* a tervezett leállás előtt legalább 20 nappal leállítja új *Időbélyegző*k kibocsátását.

A leállás időpontjával egyidejűleg a *Nem minősített időbélyegzés-szolgáltató* leállítja az információ szolgáltatást.

A *Nem minősített időbélyegzés-szolgáltató* a tervezett megszűnés előtt tárgyalásokat kezd más vele azonos besorolású szolgáltatókkal szolgáltatásainak átvételéről. Nyilvántartásait a bizalmas felhasználói adatokkal együtt a 9.3 fejezet szerint mindenképpen átadja egy ilyen szolgáltatónak, vagy megállapodás hiányában a Nemzeti Média- és Hírközlési Hatóságnak, egyéb szolgáltatásait a tárgyalások eredményétől függően átadja vagy átadás nélkül megszünteti.

A szolgáltatás nyújtásához használt *Tanúsítvány*ok visszavonásáról (és a magánkulcsok megsemmisítéséről) – a tárgyalások eredményétől függően – a *Nem minősített időbélyegzés-szolgáltató* fokozatosan intézkedik a 60 napos időszakban.

A *Nem minősített időbélyegzés-szolgáltató* a tárgyalások végeredményéről tájékoztatja az *Ügyfel*eket és a Nemzeti Média- és Hírközlési Hatóságot. A *Nem minősített időbélyegzés-szolgáltató* az *Ügyfel*eket elektronikus levélben, az *Érintett felek*et a honlapján történő közzététel útján tájékoztatja.

A *Nem minősített időbélyegzés-szolgáltató* a szolgáltatás befejezésekor az informatikai rendszerében foglalt adatairól teljes körű, minősített *Időbélyegző*vel ellátott mentést készít.

A *Nem minősített időbélyegzés-szolgáltató* – annak érdekében, hogy adatait átadhassa egy másik szolgáltatónak – az adatokat az új szolgáltató által fogadni képes médián és formátumban helyezi el vagy biztosítja az új szolgáltató számára az adatok eredeti formátumban történő feldolgozásának lehetőségét, amelyekhez átadja a megfelelő eszközöket, dokumentációkat és ismereteket.

6. Műszaki biztonsági óvintézkedések

A *Nem minősített időbélyegzés-szolgáltató* módosítás ellen védett, megbízható, biztonságtechnikailag értékelt termékekből álló informatikai rendszereket használ szolgáltatásai nyújtásához. A *Nem minősített időbélyegzés-szolgáltató* a szolgáltatói kriptográfiai kulcsokat teljes életciklusuk alatt megfelelő tanúsítással rendelkező *HSM eszköz*ökben kezeli.

Mind a *Nem minősített időbélyegzés-szolgáltató*, mind a rendszert szállító és kivitelező vállalkozók jelentős tapasztalatokkal rendelkeznek hitelesítés-szolgáltatás kiépítésében és nemzetközileg elismert technológiát alkalmaznak.

A *Nem minősített időbélyegzés-szolgáltató* folyamatosan nyomon követi a kapacitás igényeket és a trendek felállításával becslést ad a jövőbeni várható kapacitás igényekre. Igény esetén gondoskodik a szűkös kapacitások bővítéséről, ezáltal biztosítja a szükséges feldolgozási és tárolási kapacitások folyamatos rendelkezésre állását.

6.1. Kulcspár előállítása és telepítése

A *Nem minősített időbélyegzés-szolgáltató* gondoskodik valamennyi általa generált magánkulcs biztonságos, a hatályos jogszabályi előírásoknak és az ipari szabványoknak megfelelő előállításáról és kezeléséről.

6.1.1. Kulcspár előállítása

A *Nem minősített időbélyegzés-szolgáltató* a kulcspárok generálásához mindenkor csak olyan kulcsgenerálási algoritmusokat használ, amelyek megfelelnek az alábbi normatívákban megfogalmazott követelményeknek:

- ETSI TS 119 312 [18];
- az Eüt. [5] 92. § (1) b) pontja szerinti aktuális Nemzeti Média- és Hírközlési Hatóság által kiadott algoritmusokkal kapcsolatos határozat.

A *Hitelesítés-szolgáltató* saját kulcspár előállítása esetén biztosítja, hogy:

- A szolgáltatói magánkulcs előállítását fizikailag védett környezetben (lásd 5.1 pont), legalább két, bizalmi szerepkört (lásd 5.2.1 pont) betöltő, erre feljogosított személy együttes részvételével, más illetéktelen személyek jelenlétét kizárva végzi.
- A szolgáltatói magánkulcs előállítását olyan eszközön belül hajtja végre, amely:
  - megfelel az ISO/IEC 19790 [20] követelményeinek, vagy
  - megfelel a FIPS 140-2 [26] 3-as, illetve annál magasabb szintű követelményeinek, vagy
  - megfelel a CEN 14167-2 [27] munkacsoport egyezmény követelményeinek, vagy
  - olyan megbízható rendszer, amely az MSZ/ISO/IEC 15408 [19] szerint, illetve azzal egyenértékű biztonsági kritériumok szerint EAL 4-es vagy magasabb értékelési garancia szinten van értékelve. Az értékelésnek a jelen dokumentum követelményeinek megfelelő biztonsági rendszerterven, vagy biztonsági előirányzaton kell alapulnia.
- A szolgáltatói magánkulcs előállítását egy kulcsgenerálási forgatókönyv alapján végzi.

6.1.2. Kulcsméretek

A *Hitelesítés-szolgáltató* mindenkor csak olyan kriptográfiai algoritmusokat és minimális kulcsméreteket használ, amelyek megfelelnek az alábbi normatívákban megfogalmazott követelményeknek:

- ETSI TS 119 312 [18];
- az Eüt. [5] 92. § (1) b) pontja szerinti aktuális Nemzeti Média- és Hírközlési Hatóság által kiadott algoritmusokkal kapcsolatos határozat.

A *Hitelesítés-szolgáltató* valamennyi jelenleg aktív gyökér és köztes szolgáltatói *Tanúsítvány*ában, az *Időbélyegző egység*ek és OCSP válaszadók *Tanúsítvány*aiban egyaránt legalább 2048 bites RSA kulcsot vagy 256 bites ECC kulcsot használ.

6.1.3. A nyilvános kulcs paraméterek előállítása, a minőség ellenőrzése

A *Hitelesítés-szolgáltató* a kulcsok generálását a 6.1.1. fejezetben leírtak szerint végzi.

Hardveres/szoftveres kulcselőállítás

A *Nem minősített időbélyegzés-szolgáltató* *Időbélyegző*kkibocsátására használt kulcsainak generálása olyan *HSM eszköz*zel történik, amely rendelkezik FIPS 140-2 Level 3 szerinti tanúsítással.

Az egyéb – a *Nem minősített időbélyegzés-szolgáltató* belső működéséhez szükséges – kulcsokat a *Nem minősített időbélyegzés-szolgáltató* vagy *HSM eszköz*ön, vagy biztonságos környezetben üzemelő számítógépen generálja.

A paraméterek megfelelőségének ellenőrzése

A kulcsgenerálás paramétereinek megfelelőségét két szempontból ellenőrzi a rendszer:

- a paraméterekhez felhasznált véletlen szám generálás megfelelőségének ellenőrzése (statisztikailag kellőképpen véletlenszerű-e a generálás),
- a paraméterekre vonatkozó előírások teljesülésének ellenőrzése.

A rendszerben használt valamennyi *HSM eszköz* képes az általa generált bitsorozat egyenletességének és függetlenségének statisztikai tesztelésére. A modulok lehetővé teszik a tesztek meghívását egy szabványos interfészen keresztül.

6.1.4. A kulcshasználat célja (az X.509 v3 kulcs használati mező tartalmának megfelelően)

Az *Időbélyegző egység*ek magánkulcsai csak az *Időbélyegző*k hitelesítésére használhatók fel.

6.2. A magánkulcsok védelme

A *Nem minősített időbélyegzés-szolgáltató* gondoskodik a birtokában lévő magánkulcsok biztonságos kezeléséről, megakadályozza a magánkulcsok felfedését, lemásolását, törlését, módosítását, jogosulatlan használatát. A *Nem minősített időbélyegzés-szolgáltató* csak addig őrzi a magánkulcsokat, ameddig azt a szolgáltatás nyújtása feltétlenül megköveteli.

6.2.1. Kriptográfiai modulra vonatkozó szabványok és előírások

A *Nem minősített időbélyegzés-szolgáltató* *Időbélyegző*ket kibocsátó rendszerei az elektronikus aláírás vagy bélyegző létrehozásához használt magánkulcsokat olyan biztonságos hardver eszközökben tárolják, amelyek:

- megfelelnek az ISO/IEC 19790 [20] követelményeinek,
- vagy megfelelnek a FIPS 140-2 [26] 3-as, illetve annál magasabb szintű követelményeknek,

- vagy megfelelnek a CEN 14167-2 [27] munkacsoport egyezmény követelményeinek,
- vagy olyan megbízható rendszerek, amely az MSZ/ISO/IEC 15408 [19] szerint, illetve azzal egyenértékű biztonsági kritériumok szerint 4-es vagy magasabb értékelési garancia szinten vannak értékelve. Az értékelésnek a jelen dokumentum követelményeinek megfelelő biztonsági rendszerterven, vagy biztonsági előirányzaton kell alapulnia.

A használt *HSM eszköz*ök megnevezése a 8. fejezetben található.

A *Nem minősített időbélyegzés-szolgáltató* a szolgáltatói magánkulcsokat a *HSM eszköz*ön kívül csak kódolt formában tárolja. A kódoláshoz csak az Eüt. [5] 92. § (1) b) szerint kiadott aktuális Nemzeti Média- és Hírközlési Hatóság határozat szerinti algoritmusokat és kulcsparamétereket használ, amelyek várhatóan a kulcs teljes élettartama alatt képesek ellenállni a kriptográfiai támadásoknak.

A *Nem minősített időbélyegzés-szolgáltató* a szolgáltatói magánkulcsokat kódolt formában is fizikailag biztonságos helyszínen tárolja az *Adatközpont* páncélszekrényében, ahol azokhoz csak az arra jogosultak férhetnek hozzá.

A *Nem minősített időbélyegzés-szolgáltató* a kriptográfiai algoritmusok vagy kulcsparaméterek gyengülése esetén a kódolt kulcsokat megsemmisíti vagy erősebb védelmet biztosító algoritmus és kulcsparaméterek felhasználásával tovább kódolja.

6.2.2. Magánkulcs többszereplős (n-ből m) használata

A *Nem minősített időbélyegzés-szolgáltató* alkalmazza az "n-ből m" ellenőrzést a magánkulcsokkal kapcsolatos kulcsgondozási funkciók aktivizálásánál. A paraméterek úgy lettek meghatározva, hogy a szolgáltatói magánkulcsaival végzett kritikus műveletek végrehajtásához legalább kettő, bizalmi szerepkört betöltő munkatárs egyidejű jelenlétére legyen szükség.

6.2.3. Magánkulcs letétbe helyezése

A *Nem minősített időbélyegzés-szolgáltató* nem helyezi letétbe saját szolgáltatói magánkulcsát.

6.2.4. Magánkulcs mentése

A *Nem minősített időbélyegzés-szolgáltató* minden szolgáltatói magánkulcsáról biztonsági másolatot készít még a magánkulcs használatbavételét megelőzően a 6.2.1. fejezetben leírtak szerint védett környezetben, legalább két bizalmi szerepkört betöltő személy együttes jelenlétében, más személyek kizárásával. A mentés során a magánkulcs titkosított formában hagyja el a modult, e titkosított kulcsot később másik modulba be lehet tölteni. Mind a mentés, mind a visszatöltés csakis a 6.2.2. fejezetben leírt védelmi mechanizmus mellett végezhető.

A *Nem minősített időbélyegzés-szolgáltató* a biztonsági másolatot két példányban tárolja, ebből legalább az egyik példányt a szolgáltatás nyújtásától eltérő helyszínen.

A biztonsági másolatok kezelésére és megőrzésére ugyanolyan szigorú biztonsági előírások vonatkoznak, mint az éles rendszer üzemeltetésére.

6.2.5. Magánkulcs archiválása

A *Nem minősített időbélyegzés-szolgáltató* nem archiválja magánkulcsait.

6.2.6. Magánkulcs bejuttatása hardver kriptográfiai eszközbe, vagy onnan történő exportja

A *Nem minősített időbélyegzés-szolgáltató* valamennyi szolgáltatói magánkulcsát a követelményeknek megfelelő *HSM eszköz*ben állítja elő.

A magánkulcsok nem léteznek nyílt formában a *HSM eszköz*ön kívül.

A *Nem minősített időbélyegzés-szolgáltató* a magánkulcsot csak biztonsági másolat készítése céljából exportálja a *HSM eszköz*ből.

A magánkulcs *HSM eszköz*ök közötti szállítása csak biztonsági másolat formájában engedélyezett.

A szolgáltatói magánkulcsok exportálása vagy betöltése minden esetben a 6.2.2. fejezetben leírt módon történik.

6.2.7. Magánkulcs tárolása hardver kriptográfiai eszközben

A *Nem minősített időbélyegzés-szolgáltató* a szolgáltatás nyújtásához használt magánkulcsait a 6.2.1. fejezet szerinti kriptográfiai modulokban tartja.

A *HSM eszköz*ben a magánkulcsokat az eszköz tanúsításában meghatározott módon tárolja és használja a vonatkozó kezelési utasítások maradéktalan betartásával.

6.2.8. A magánkulcs aktiválásának módja

A *Nem minősített időbélyegzés-szolgáltató* szolgáltatói magánkulcsait biztonságos *HSM eszköz*ben tárolja, a használat során betartja a *HSM eszköz* felhasználói útmutatójában és a tanúsítási dokumentumokban megfogalmazott követelményeket. A *HSM eszköz*t csak a hozzá tartozó operátori kártyákkal lehet aktiválni, a *HSM eszköz*ben lévő magánkulcsokat a modul aktiválása előtt nem lehet használni. A *HSM eszköz*höz tartozó operátori kártyákat a *Nem minősített időbélyegzés-szolgáltató* biztonságos környezetben tárolja és e kártyákat kizárólag a *Nem minősített időbélyegzés-szolgáltató* erre jogosult munkatársai érhetik el.

6.2.9. A magánkulcs deaktiválásának módja

A *Nem minősített időbélyegzés-szolgáltató* által használt hardver kriptográfia eszközök által kezelt magánkulcs akkor deaktiválódik, ha az eszköz (szabályos vagy szabálytalan módon) kikerül az aktív állapotból. Ez az alábbi esetekben következik be:

- a felhasználó deaktiválja a kulcsot,
- az eszköz áramellátása megszakad (kikapcsolás vagy tápellátási probléma),
- az eszköz hibaállapotba kerül.

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

6.2.10. A magánkulcs megsemmisítésének módja

A *Nem minősített időbélyegzés-szolgáltató* használatból kivont, lejárt érvényességű vagy kompromittálódott szolgáltatói magánkulcsait olyan módon semmisíti meg, amely lehetetlenné teszi a magánkulcs további használatát.

A *Nem minősített időbélyegzés-szolgáltató* a biztonságos *HSM eszköz*ében tárolt szolgáltatói magánkulcsok megsemmisítését a felhasznált *HSM eszköz* felhasználói útmutatójában és a tanúsítási dokumentumokban megfogalmazott eljárásoknak, követelményeknek megfelelően végzi a *Nem minősített időbélyegzés-szolgáltató* két munkatársának (egy infrastruktúra adminisztrátor és egy biztonsági tisztviselő) együttes jelenlétében más személyek jelenlétének kizárásával.

A *Nem minősített időbélyegzés-szolgáltató* dokumentált módon megsemmisíti a magánkulcsról készült minden mentett példányt olyan módon, hogy annak visszaállítása, használata lehetetlenné váljon.

6.2.11. A hardver kriptográfiai eszközök értékelése

A 6.2.1 fejezet előírásaival összhangban a *Nem minősített időbélyegzés-szolgáltató* valamennyi szolgáltatói magánkulcsát olyan *HSM eszköz*ben tárolja, amely:

- rendelkezik ISO/IEC 19790 [20] szerinti tanúsítással,
- vagy rendelkezik FIPS 140-2 Level 3 [26] szerinti tanúsítással,
- vagy rendelkezik a CEN 14167-2 [27] munkacsoport egyezmény követelményeinek való megfelelést igazoló Common Criteria alapú tanúsítvánnyal,
- vagy rendelkezik a Nemzeti Média- és Hírközlési Hatóság által vagy az Európai Unió valamely tagállamában nyilvántartásba vett, elektronikus aláírási termékek értékelésére jogosult független tanúsító szervezet által erre a célra kiadott igazolással.

6.3. A kulcspár kezelés egyéb szempontjai

6.3.1. A tanúsítványok és kulcspárok használatának periódusa

Az Időbélyegző egységek tanúsítványai

A *Nem minősített időbélyegzés-szolgáltató* által üzemeltetett *Időbélyegző egység*ek *Tanúsítvány*ainak érvényességi ideje:

- legfeljebb a kibocsátástól számított 135 hónap;
- nem haladhatja meg azt az időt, amely időpontig a felhasznált kriptográfiai algoritmusok a Nemzeti Média- és Hírközlési Hatóság algoritmusokkal kapcsolatos határozata szerint biztonságosan felhasználhatók;
- nem haladhatja meg a *Tanúsítvány*t kibocsátó szolgáltatói *Tanúsítvány* érvényességi idejét.

A *Nem minősített időbélyegzés-szolgáltató* minden év utolsó negyedévében új magánkulcso(ka)t és 135 hónapig érvényes *Tanúsítvány*(oka)t ad ki az *Időbélyegző egység*ei számára. Az új *Időbélyegző egység Tanúsítvány*(ok) használatba vétele után a korábbi magánkulcso(ka)t megsemmisíti, így az egyes magánkulcsokat átlagosan 12 hónapig használja.

Az Időbélyegző kulcsok életciklusa

Az *Időbélyegző*k hitelesítésére használt magánkulcsokra teljesülnek az alábbi követelmények:

- a *Nem minősített időbélyegzés-szolgáltató* meghatározza az *Időbélyegző egység*ekben használt aláíró kulcsok érvényességének végét, ami a kibocsátástól számított 15 hónap;
- a kulcs 15 hónapos érvényességi ideje nem haladhatja meg a *Tanúsítvány* érvényességi idejét;
- az érvényességi idő nem haladhatja meg az alkalmazott kriptográfiai algoritmusok és kulcs paraméterek érvényességi idejét;
- a *Nem minősített időbélyegzés-szolgáltató* az *Időbélyegző egység*ek magánkulcsának érvényességi idejét megadja a *Tanúsítvány* "PrivateKeyUsagePeriod" értékének beállításával (lásd 7.1.2. fejezet);
- az *Időbélyegző egység* magánkulcsát nem használja az érvényességi időn túl;
- a *Nem minősített időbélyegzés-szolgáltató* szervezeti eljárásokat alkalmaz annak biztosítására, hogy az *Időbélyegző egység* magánkulcsának lejárata esetén rendelkezésre álljon az új magánkulcs és *Tanúsítvány*;
- a *Nem minősített időbélyegzés-szolgáltató* az új magánkulcsok használatbavétele után a lejárt érvényességű, használatból kivont magánkulcs minden példányát megsemmisíti oly módon, hogy a magánkulcs visszaállítása lehetetlenné váljon.

A *Tanúsítvány*ok és a magánkulcsok érvényességi idejét befolyásolhatja, ha a Nemzeti Média- és Hírközlési Hatóság új algoritmusokkal kapcsolatos határozatot ad ki, amely szerint a felhasznált kriptográfiai algoritmus vagy kulcsparaméter már nem biztonságos a kibocsátáskor tervezett felhasználási idő végéig.

Amennyiben ez bekövetkezik, a *Hitelesítés-szolgáltató* visszavonja az érintett *Tanúsítvány*okat.

6.4. Aktivizáló adatok

6.4.1. Aktivizáló adatok előállítása és telepítése

A *Nem minősített időbélyegzés-szolgáltató* a felhasznált *HSM eszköz* felhasználói útmutatójában és az eszköz tanúsítványban megfogalmazott eljárásoknak, követelményeknek megfelelő aktiváló módszereket alkalmaz szolgáltatói magánkulcsainak védelmére.

Jelszó alapú aktivizáló adatok használata esetén a jelszavak kellően bonyolultak a megkívánt védelmi szint biztosítása érdekében.

6.4.2. Az aktivizáló adatok védelme

A *Nem minősített időbélyegzés-szolgáltató* alkalmazottai a magánkulcsok aktiválásához szükséges eszközöket, aktivizáló adatokat biztonságosan kezelik, műszaki és szervezési intézkedések segítségével védik, a jelszavakat csak kódolt formában tárolják.

6.4.3. Az aktivizáló adatok kezelésének egyéb szempontjai

Nincs megkötés.

6.5. Informatikai biztonsági előírások

6.5.1. Speciális informatikai biztonsági műszaki követelmények

A *Nem minősített időbélyegzés-szolgáltató* informatikai rendszereinek konfigurálása és üzemeltetése során biztosítja az alábbi követelmények teljesülését:

- a rendszerhez vagy alkalmazáshoz való hozzáférés engedélyezése előtt a felhasználó azonosságát többfaktoros azonosítással ellenőrzi kártyán tárolt VPN tanúsítvány felhasználásával;
- a felhasználókhoz szerepköröket rendel és biztosítja, hogy minden felhasználó csak a szerepkörének megfelelő jogosultságokkal rendelkezzen;
- minden tranzakcióról naplóbejegyzést állít elő és a naplóbejegyzéseket archiválja;
- a biztonságkritikus folyamatok részére biztosítja, hogy a *Nem minősített időbélyegzés-szolgáltató* belső hálózati tartományai kellően védettek legyenek a jogosulatlan hozzáféréstől;
- megfelelő eljárásokat alkalmaz a kulcsvesztés vagy rendszerhiba után a szolgáltatás visszaállítása érdekében.

6.5.2. Az informatikai biztonság értékelése

A Microsec kiemelten fontosnak tartja *Ügyfel*ei elégedettségét. A magas színvonalú szolgáltatások fenntartása érdekében a *Nem minősített időbélyegzés-szolgáltató* ISO 9001 szabványnak megfelelő minőségirányítási rendszert üzemeltet 2002. január 23. óta. A szabványnak való megfelelést a Lloyd's Register Quality Assurance tanúsította.

A Microsec nagy figyelmet fordít az általa üzemeltetett rendszerek biztonságára, ezért fő tevékenységi területein a ISO/IEC 27001-nek megfelelő információbiztonság-irányítási rendszert (korábban BS 7799) üzemeltet 2003. május 19. óta. A szabványnak való megfelelést a Lloyd's Register Quality Assurance tanúsította.

A minőségirányítási rendszer és az információbiztonság-irányítási rendszer hatóköre kiterjed a Microsec által nyújtott bizalmi szolgáltatásokra is.

A Microsec kétszintű kockázatelemzése az információ technológiai kockázatokon túlmenően kiterjed a teljes szervezetre és az üzleti kockázatokra is. A kockázatelemzés legalább évente felülvizsgálatra kerül.

6.6. Életciklusra vonatkozó műszaki előírások

6.6.1. Rendszerfejlesztési előírások

A *Nem minősített időbélyegzés-szolgáltató* az éles szolgáltatást nyújtó informatikai rendszereiben csak olyan eszközöket, alkalmazásokat használ, amelyek:

- kereskedelmi dobozos szoftverek, amelyeket dokumentált tervezési módszertan szerint terveztek és fejlesztettek;
- a *Nem minősített időbélyegzés-szolgáltató* saját maga által kifejlesztett egyedi hardver és szoftver megoldások, amelyek tervezése során strukturált fejlesztési módszereket és ellenőrzött fejlesztési környezetet használt;
- a *Nem minősített időbélyegzés-szolgáltató* részére megbízható fél által kifejlesztett egyedi hardver és szoftver megoldások, amelyek tervezése során strukturált fejlesztési módszereket és ellenőrzött fejlesztési környezetet használtak;
- olyan nyílt forráskódú szoftverek, amelyek teljesítik a biztonsági követelményeket és amelyek megfelelőségét szoftver verifikáció, strukturált fejlesztés és életciklus menedzsment biztosítja.

Az informatikai eszközök beszerzése a hardver és szoftver komponensek módosítását kizáró módon történik, megbízható és rendszeresen minősített szállítók felhasználásával.

A *Nem minősített időbélyegzés-szolgáltató* a szolgáltatások nyújtásához használt kritikus informatikai eszközöket más célra nem használja.

A *Nem minősített időbélyegzés-szolgáltató* megfelelő védelmi intézkedésekkel megakadályozza, hogy kártékony szoftver kerülhessen a hitelesítés-szolgáltatás nyújtása körében használt eszközökbe.

A hardver és szoftver komponenseket az első használat előtt és azt követően rendszeresen ellenőrzi kártékony kódok után kutatva.

A *Nem minősített időbélyegzés-szolgáltató* a programfrissítések vásárlása vagy fejlesztése során ugyanolyan gondossággal jár el, mint az első verzió beszerzésekor.

A *Nem minősített időbélyegzés-szolgáltató* megbízható, megfelelően képzett személyzetet alkalmaz a szoftverek és eszközök telepítése során.

A *Nem minősített időbélyegzés-szolgáltató* csak a szolgáltatás nyújtásához szükséges szoftvereket telepíti a szolgáltatást nyújtó informatikai berendezéseire.

A *Nem minősített időbélyegzés-szolgáltató* rendelkezik változáskövető rendszerrel, amelyben az informatikai rendszer minden lényeges változtatása dokumentálásra kerül.

A *Nem minősített időbélyegzés-szolgáltató* a jogosulatlan változások észlelése érdekében automatikus monitorozó rendszert üzemeltet, amely rögzíti minden állomány változását és a figyelt állományok változása esetén naplóbejegyzést generál vagy figyelmeztető jelzést küld a rendszer üzemeltetőknek.

6.6.2. Biztonságkezelési előírások

A *Nem minősített időbélyegzés-szolgáltató* változáskövető rendszert használ a szolgáltatásban használt rendszerek telepítésének, konfigurációjának dokumentálására,

üzemeltetésére, ellenőrzésére, monitorozására és karbantartására, beleértve a módosításokat és továbbfejlesztéseket is. A változáskövető rendszer alkalmas arra, hogy észleljen a rendszerben történt bármilyen jogosulatlan változtatást, adatbevitelt, amely érinti a szolgáltatásban használt rendszert, a tűzfalakat, routereket, programokat és egyéb komponenseket. A szolgáltatásban használt program telepítésekor a *Nem minősített időbélyegzés-szolgáltató* minden esetben meggyőződik arról, hogy a telepítendő program a megfelelő verziójú és mentes mindenféle jogosulatlan módosítástól. A *Nem minősített időbélyegzés-szolgáltató* rendszeresen ellenőrzi a szolgáltatói rendszereiben használt programok integritását.

A *Nem minősített időbélyegzés-szolgáltató* által alkalmazott valamennyi *HSM eszköz* ellenőrzésre, bevizsgálásra és értékelésre került. A *Nem minősített időbélyegzés-szolgáltató* ellenőrzi a modulok sértetlenségét:

- az eszközök beszerzését követően az átvétel során,
- a használatbavételt közvetlenül megelőzően,
- rendszeresen az üzemeltetés során.

A használatból véglegesen vagy időlegesen kivont *HSM eszköz*ből a *Nem minősített időbélyegzés-szolgáltató* törli a szolgáltatói kulcsokat.

A *Nem minősített időbélyegzés-szolgáltató* a használaton kívüli *HSM eszköz*öket fizikailag védett helyszínen tárolja.

6.6.3. Életciklusra vonatkozó biztonsági előírások

A *Nem minősített időbélyegzés-szolgáltató* gondoskodik a felhasznált *HSM eszköz*ök védelméről azok teljes életciklusa alatt.

A szolgáltatások nyújtásához használt informatikai eszközök, rendszerek üzemeltetése során a *Nem minősített időbélyegzés-szolgáltató* figyelembe veszi az eszközök életciklusára vonatkozó biztonsági szempontokat, melyek szerint:

- megfelelő tanúsítással rendelkező *HSM eszköz*t használ rendszereiben;
- a *HSM eszköz* átvételekor a minőség ellenőrzése során meggyőződik róla, hogy a szállítás folyamán biztosították a *HSM eszköz*ök feltörés elleni védelmét;
- a *HSM eszköz*öket biztonságos helyen tárolja, a tárolás során biztosítja a *HSM eszköz*ök feltörés elleni védelmét;
- az üzemeltetés során folyamatosan betartja a *HSM eszköz* biztonsági előirányzatában, használati útmutatójában és a tanúsítási jelentésben szereplő követelményeket;
- a használatból kivont *HSM eszköz*ökben tárolt magánkulcsokat olyan módon törli, hogy lehetetlené válik a kulcsok visszaállítása.

6.7. Hálózati biztonsági előírások

A *Nem minősített időbélyegzés-szolgáltató* szigorú ellenőrzés alatt tartja az alkalmazott IT rendszereinek konfigurációját, minden változást dokumentál, beleértve a legkisebb módosítást, fejlesztést, szoftverfrissítést is. A *Nem minősített időbélyegzés-szolgáltató* megfelelő eljárásokat használ az IT rendszereiben bekövetkezett tetszőleges hardver vagy szoftver változás észlelésére, a rendszer telepítésére, karbantartására. A *Nem minősített időbélyegzés-szolgáltató* minden szoftverkomponens első betöltésekor ellenőrzi a komponens eredetiségét, integritását.

A *Nem minősített időbélyegzés-szolgáltató* megfelelő hálózatbiztonsági intézkedéseket alkalmaz, mint például:

- IT rendszereit jól elválasztott biztonsági zónákra osztja;
- elkülöníti az IT rendszer üzemeltetését támogató rendszereit az éles szolgáltatást nyújtó rendszereitől;
- elkülöníti az éles szolgáltatást nyújtó rendszereit a fejlesztésre és tesztelésre szolgáló rendszerektől;
- az elkülönített megbízható rendszerek között csak olyan megbízható kommunikációs csatornákon keresztül létesít kapcsolatot, amelyek logikailag el vannak választva más kommunikációs csatornáktól, megbízható végponti azonosítást használnak és védik a csatornákon küldött adatokat a módosítástól és a felfedéstől;
- az éles szolgáltatást nyújtó IT rendszereit biztonságos hálózati zónában üzemelteti;
- a zónákhoz való hozzáférést és a zónák közötti kommunikációt csak a szolgáltatás nyújtásához szükségesre korlátozza;
- letiltja a nem használt protokollokat és felhasználókat;
- letiltja a használaton kívüli hálózati portokat és szolgáltatásokat;
- csak az IT rendszer megfelelő működéséhez feltétlenül szükséges hálózati alkalmazásokat futtat.
- a használt szabályrendszert rendszeresen felülvizsgálja.

A *Nem minősített időbélyegzés-szolgáltató* sérülékenységvizsgálatot végez vagy végeztet a *Nem minősített időbélyegzés-szolgáltató* nyilvános és privát IP címein:

- a CA/Browser Forum kérésétől számított egy héten belül;
- a *Nem minősített időbélyegzés-szolgáltató* által jelentősnek minősített rendszer vagy hálózati változtatás után;
- legalább minden három (3) hónapban.

6.8. Időbélyegzés

A *Nem minősített időbélyegzés-szolgáltató* a naplóbejegyzések és egyéb archiválandó elektronikus állományok hitelesítésére az e-Szignó Hitelesítés Szolgáltató által kibocsátott minősített elektronikus *Időbélyegző*ket használja.

7. Tanúsítvány, CRL és OCSP profilok

7.1. Tanúsítvány profil

A *Nem minősített időbélyegzés-szolgáltató* által használt *Időbélyegző egység Tanúsítvány*ok illetve a szolgáltatás során használt szolgáltatói (gyökér és köztes) hitelesítő egységek *Tanúsítvány*ai megfelelnek az alábbi ajánlásoknak, specifikációknak:

- ITU X.509 Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks [24];
- IETF RFC 5280 [22];
- IETF RFC 6818 [23];
- ETSI EN 319 412-1 [13];
- ETSI EN 319 412-2 [14] természetes személyek számára kibocsátott *Tanúsítvány*ok esetén;
- ETSI EN 319 412-3 [15] nem természetes személyek számára kibocsátott *Tanúsítvány*ok esetén;

7.1.1. Verzió szám(ok)

A *Nem minősített időbélyegzés-szolgáltató* által használt szolgáltatói (gyökér és köztes) hitelesítő egységek *Tanúsítvány*ai és a *Nem minősített időbélyegzés-szolgáltató* által használt *Időbélyegző egység Tanúsítvány*ok az X.509 specifikáció [24] szerinti "v3" *Tanúsítvány*ok.

A *Nem minősített időbélyegzés-szolgáltató* által használt szolgáltatói (gyökér és köztes) hitelesítő egységek *Tanúsítvány*ai és a *Nem minősített időbélyegzés-szolgáltató* által használt *Időbélyegző egység Tanúsítvány*ok alapmezői a következők:

- Verzió (Version)
  A *Tanúsítvány* az X.509 specifikáció [24] szerinti "v3" *Tanúsítvány*oknak felel meg, így a mezőbe a "2" érték kerül.
- Sorozatszám (Serial Number)
  A *Tanúsítvány*t kibocsátó hitelesítő egység által generált egyedi azonosító.

  A végfelhasználói *Tanúsítvány*ok esetében a "Serial Number" mező legalább 8 bájt entrópiájú véletlen számot tartalmaz.
- Algoritmus azonosító (Algorithm Identifier)
  A *Tanúsítvány*t hitelesítő elektronikus bélyegző készítéséhez használt kriptográfiai algoritmuskészlet azonosítója (OID). A *Nem minősített időbélyegzés-szolgáltató* a következő kriptográfiai algoritmust használja:

  - "sha256WithRSAEncryption" (1.2.840.113549.1.1.11)
  - "ecdsa-with-SHA256" (1.2.840.10045.4.3.2)

- Aláírás (Signature)
  A *Nem minősített időbélyegzés-szolgáltató* által készített, a *Tanúsítvány*t hitelesítő elektronikus bélyegző, amelyet a *Nem minősített időbélyegzés-szolgáltató* az "Algoritmus azonosító" -ban megadott algoritmuskészlettel hozott létre.

- Kibocsátó (Issuer)
  A *Tanúsítvány*t kibocsátó *Hitelesítő egység* megkülönböztetett neve egyedi X.501 név formátum szerint.

- Érvényesség (Valid From & Valid To)
  A *Tanúsítvány* érvényességének kezdete és vége.

  Az időpontok UTC szerint és az IETF RFC 5280-nak megfelelő kódolásban kerülnek rögzítésre.

- Az *Alany* azonosítója (Subject)
  Az *Alany* megkülönböztetett neve egyedi X.501 név formátum szerint.
  Mindig kitöltésre kerül.

- Az *Alany* nyilvános kulcsának algoritmus-azonosítója (Subject Public Key Algorithm Identifier)

  A *Nem minősített időbélyegzés-szolgáltató* az RSA és az ECC algoritmusokat támogatja a végfelhasználói *Tanúsítvány*okban.

  A mezőbe kerülő érték:

  - "rsaEncryption" (1.2.840.113549.1.1.1)
  - "ecPublicKey" (1.2.840.10045.2.1)

- Az *Alany* nyilvános kulcsa (Subject Public Key Value)
  Az *Alany* nyilvános kulcsa.

- Kibocsátó egyedi azonosító (Issuer Unique Identifier)
  Nem kitöltött.

- Az *Alany* egyedi azonosítója (Subject Unique Identifier)
  Nem kitöltött.

7.1.2. Tanúsítvány kiterjesztések

A *Nem minősített időbélyegzés-szolgáltató* csak az alábbi, X.509 specifikáció [24] szerinti tanúsítvány kiterjesztéseket használja:

Időbélyegző egység tanúsítványa

- Hitelesítési rendek (Certificate Policies) – nem kritikus
  OID: 2.5.29.32
  E mező tartalmazza az *Időbélyegző egység Tanúsítvány*ának kiadása és használata során érvényes *Hitelesítési rend* azonosítóját, valamint az alkalmazhatóságára vonatkozó egyéb információkat. A mező kitöltése kötelező és nem lehet kritikus. A vonatkozó *Nem minősített időbélyegzési szolgáltatási szabályzat* hivatkozása megadható ebben a mezőben.

- Kibocsátó kulcsazonosító (Authority Key Identifier) – nem kritikus
  OID: 2.5.29.35
  A *Tanúsítvány*t hitelesítő elektronikus bélyegző létrehozásánál felhasznált szolgáltatói kulcs 40 karakter hosszú egyedi azonosítója.

  A mező értéke: a szolgáltatói nyilvános kulcs SHA-1 lenyomata.

- *Alany* kulcsazonosító (Subject Key Identifier) – nem kritikus
  OID: 2.5.29.14
  Az *Időbélyegző egység* nyilvános kulcsának 40 karakter hosszú egyedi azonosítója.
  A mező értéke: a nyilvános kulcs SHA-1 lenyomata.

- *Alany* alternatív nevei (Subject Alternative Names) – nem kritikus
  OID: 2.5.29.17

  *Időbélyegző egység Tanúsítvány*ában az *Időbélyegzés-szolgáltató* központi email címe kerülhet ide, kitöltése opcionális.

- Alapvető megkötések (Basic Constraints) – kritikus
  OID: 2.5.29.19
  Annak megadása, hogy a *Tanúsítvány* hitelesítő egység számára lett-e kibocsátva.

  A kiterjesztés alapértelmezett értéke CA = "FALSE", ezért ez a kiterjesztés nem szerepel az *Időbélyegző egység* számára kibocsátott *Tanúsítvány*okban.

  A "pathLenConstraint" mező nem szerepel *Időbélyegző egység* számára kibocsátott *Tanúsítvány*okban.

- Kulcshasználat (Key Usage) – kritikus
  OID: 2.5.29.15
  A kulcs engedélyezett használati körének meghatározása.

  Az *Időbélyegző egység* számára kibocsátott *Tanúsítvány*okban kizárólag az alábbi értékek szerepelnek: "nonRepudiation", "digitalSignature".

- Kulcshasználati időszak (PrivateKeyUsagePeriod) – nem kritikus
  OID: 2.5.29.16
  A magánkulcs engedélyezett használati időtartamának meghatározása.
  Az *Időbélyegző egység* számára kibocsátott *Tanúsítvány*okban a *Nem minősített időbélyegzés-szolgáltató* korlátozza a magánkulcs használatának idejét a "notBefore" és "notAfter" értékek megadásával.

- Kiterjesztett kulcshasználat (Extended Key Usage) – kritikus
  A kulcs további engedélyezett használati körének meghatározása.

Az időbélyegző egység számára kibocsátott *Tanúsítvány*okban kizárólag az alábbi érték szerepel:

"timeStamping (1.3.6.1.5.5.7.3.8)".

- CRL szétosztási pont (CRL Distribution Points) – nem kritikus
  OID: 2.5.29.31
  A mező tartalmazza a CRL elérhetőségét http és/vagy LDAP protokollon keresztül.
  Kitöltése kötelező.

- Szolgáltatói információ elérése (Authority Information Access) – nem kritikus
  OID: 1.3.6.1.5.5.7.1.1
  Hitelesítés-szolgáltató által rendelkezésre bocsátott, az időbélyegző egység *Tanúsítvány*ának használatához kapcsolódó egyéb szolgáltatásainak leírása.

  Kötelező a kitöltése, és a mező tartalmazza a következő adatokat:

  – A *Nem minősített időbélyegzés-szolgáltató* a *Tanúsítvány*ok aktuális visszavonási állapotának gyors és pontos ellenőrizhetősége érdekében online tanúsítvány-állapot szolgáltatást nyújt. Ez az elérhetőség szerepel itt.
  – A tanúsítványlánc felépítésének megkönnyítésére a *Nem minősített időbélyegzés-szolgáltató* megadja a *Tanúsítvány*t kibocsátó hitelesítési egység *Tanúsítvány*ának http protokollon keresztüli elérési helyét.

A fenti mezők a megadott szabályok szerint mindig kitöltésre kerülnek. Más tanúsítvány kiterjesztés nem kerül kitöltésre.

8. A megfelelőség vizsgálata

A *Nem minősített időbélyegzés-szolgáltató* rendszeres időközönként megvizsgáltatja működését külső független auditorral. Az audit során felülvizsgálatra kerül, hogy a *Nem minősített időbélyegzés-szolgáltató* működése megfelel-e az alábbi normatív dokumentumoknak:

- AZ EURÓPAI PARLAMENT ÉS A TANÁCS 910/2014/EU RENDELETE (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről [1];
- ETSI EN 319 401 V2.2.1 (2018-04); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [10]
- ETSI EN 319 421 V1.1.1 (2016-03); Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps. [16]

A megfelelőségértékelési vizsgálat eredménye bizalmas dokumentum, csak az arra jogosultak számára hozzáférhető.

A megfelelőségértékelési jelentés alapján kiállított megfelelőségi tanúsítványt a *Nem minősített időbélyegzés-szolgáltató* honlapján közzéteszi.

A *Nem minősített időbélyegzés-szolgáltató* vizsgált és tanúsított elemeket (elektronikus aláírási termékeket, informatikai rendszerelemeket stb.) alkalmaz a szolgáltatásaihoz kapcsolódóan.

A *Nem minősített időbélyegzés-szolgáltató* a szolgáltatások nyújtásához használt valamennyi rendszerelemet biztonsági osztályokba sorolta kockázatmenedzsment rendszere alapján. Ezen rendszerelemekről és a hozzájuk tartozó biztonsági besorolásról a *Nem minősített időbélyegzés-szolgáltató* a kockázatmenedzsment rendszere keretében nyilvántartást vezet.

A *Nem minősített időbélyegzés-szolgáltató* a külső auditon túl saját belső ellenőrzési rendszerrel is rendelkezik, amely segítségével rendszeresen vizsgálja a korábbi auditoknak való megfelelőséget és eltérés esetén megteszi a szükséges lépéseket.

A *Nem minősített időbélyegzés-szolgáltató* 2002 óta rendelkezik az ISO 9001 szabványnak megfelelő minőségirányítási, valamint 2003 óta a ISO/IEC 27001-nek (korábban BS 7799-nek) megfelelő információbiztonság-irányítási rendszerrel, amelyeket külső auditáló szervezet (Lloyd's Register Quality Assurance) auditál és vizsgál felül folyamatosan .

8.1. Az ellenőrzések körülményei és gyakorisága

A *Nem minősített időbélyegzés-szolgáltató* évente külső megfelelőségértékelési auditot hajt végre a szolgáltatások nyújtását végző informatikai rendszerén.

8.2. Az auditor és szükséges képesítése

A *Nem minősített időbélyegzés-szolgáltató* a belső auditokat a független rendszervizsgáló szerepkörrel felruházott alkalmazottai segítségével rendszeresen végzi.

Az eIDAS és ETSI követelményeknek való megfelelőséget igazoló vizsgálatot olyan szervezet végzi el, amely rendelkezik egy EU tagállam nemzeti akkreditációs szervezete által kiadott erre feljogosító felhatalmazással.

8.3. Az auditor és az auditált rendszerelem függetlensége

A külső auditot olyan személy végzi:

- aki független a vizsgált *Nem minősített időbélyegzés-szolgáltató* tulajdonosi körétől, vezetőségétől és üzemeltetésétől;
- aki független a vizsgált szervezettől, vagyis sem saját maga, sem közvetlen hozzátartozója nincs munkaviszonyban vagy üzleti kapcsolatban a *Nem minősített időbélyegzés-szolgáltató*val;
- akinek díjazása nem függ az audit során végzett tevékenységének megállapításaitól.

8.4. Az auditálás által lefedett területek

Az átvizsgálás lefedi az alábbi területeket:

- hatályos jogszabályoknak való megfelelés;
- műszaki szabványoknak való megfelelés;

- *Nem minősített időbélyegzési rend*(ek)nek és *Nem minősített időbélyegzési szolgáltatási szabályzat*(ok)nak való megfelelés;
- az alkalmazott folyamatok megfelelősége;
- a dokumentálás;
- a fizikai biztonság;
- a személyi állomány megfelelősége;
- az IT biztonság;
- az adatvédelmi szabályok betartása.

8.5. A hiányosságok kezelése

A független auditor az átvizsgálás eredményét egy részletes átvilágítási jelentésben foglalja össze, amely kitér a vizsgált rendszerelemekre, folyamatokra, tartalmazza az átvilágítás során felhasznált bizonyítékokat és vizsgálói megállapításokat. A jelentésben külön fejezetben rögzíti a vizsgálat során feltárt eltéréseket és az elhárításukra kitűzött határidőket. A független auditor a vizsgálat során feltárt eltérések, hiányosságok súlyossága alapján a jelentésben rögzíthet:

- opcionálisan figyelembe vehető módosítási javaslatokat;
- kötelezően elhárítandó eltéréseket.

8.6. Az eredmények közzététele

A *Nem minősített időbélyegzés-szolgáltató* a vizsgálat eredményét összefoglaló jelentést nyilvánosságra hozza. A feltárt hiányosságok részleteit nem publikálja, azokat bizalmas információként kezeli.

9. Egyéb üzleti és jogi kérdések

9.1. Díjak

A szolgáltatási díjakat és árakat a *Nem minősített időbélyegzés-szolgáltató* a honlapján közzéteszi és kérelemre nyomtatott formában ügyfélszolgálati irodájában is biztosítja olvashatóságát.

A *Nem minősített időbélyegzés-szolgáltató* az árlistát egyoldalúan módosíthatja. Az árlista módosítását a hatálybalépése előtt 30 nappal a *Nem minősített időbélyegzés-szolgáltató* a honlapján közzéteszi. Az *Ügyfél* számára kedvező változások a 30 naposnál rövidebb határidővel is bevezethetők. Az előre kifizetett szolgáltatások árát a módosítás nem érinti.

A díjak kifizetésével és visszatérítésével kapcsolatos rendelkezéseket a Szolgáltatási szerződés és mellékletei – különösen az Általános szerződési feltételek – tartalmazzák.

9.1.1. Visszatérítési politika

Lásd: 9.1. fejezet.

9.2. Anyagi felelősségvállalás

A *Nem minősített időbélyegzés-szolgáltató* megbízhatósága érdekében anyagi felelősséget vállal a jelen *Nem minősített időbélyegzési rend*ben, a vonatkozó *Nem minősített időbélyegzési szolgáltatási szabályzat*ban valamint az *Ügyfél*lel kötött Szolgáltatási szerződésben megfogalmazott valamennyi rá vonatkozó kötelezettség maradéktalan betartásáért.

9.2.1. Pénzügyi követelmények

A *Nem minősített időbélyegzés-szolgáltató* rendelkezik a szolgáltatások nyújtásával valamint a megszűnésével kapcsolatos költségek biztosításához szükséges anyagi erőforrásokkal.

9.2.2. Felelősségbiztosítás

- A *Nem minősített időbélyegzés-szolgáltató* a megbízhatóság biztosítása érdekében felelősségbiztosítással rendelkezik.
- A felelősségbiztosítási szerződés kiterjed az alábbi, a *Nem minősített időbélyegzés-szolgáltató* által a szolgáltatások nyújtásával összefüggésben okozott károkra:
  - a bizalmi szolgáltatási *Ügyfél*nek a Szolgáltatási szerződés megszegésével összefüggésben okozott károkra;
  - a bizalmi szolgáltatási *Ügyfél*nek és harmadik személynek szerződésen kívüli okozott károkra;
  - a Nemzeti Média- és Hírközlési Hatóságnak a bizalmi szolgáltatási tevékenységet befejező *Nem minősített időbélyegzés-szolgáltató* által okozott költségekre;
  - az eIDAS Rendelet [1] 17. cikk (4) bekezdés e) pontja alapján a Nemzeti Média- és Hírközlési Hatóság által felkért megfelelőségértékelő szervek eljárásának költségeire, ha azt a Nemzeti Média- és Hírközlési Hatóság eljárási költségként érvényesíti.
- A biztosítási szerződésben szereplő felelősségvállalási érték káreseményenként legalább 3.000.000 forint. Több azonos okból bekövetkezett, időben összefüggő káresemény egy biztosítási eseménynek minősül.
- A felelősségbiztosítás a meghatározott összeg erejéig fedezetet nyújt a károsultnak a szolgáltató károkozó magatartásával összefüggésben keletkező teljes kárára, függetlenül attól, hogy a kárt szerződésszegéssel vagy szerződésen kívül okozták.
- 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.

9.3. Bizalmasság

A *Nem minősített időbélyegzés-szolgáltató* az *Ügyfel*ek adatait a jogszabályoknak megfelelően kezeli. A *Nem minősített időbélyegzés-szolgáltató* rendelkezik adatkezelési szabályzattal (lásd 9.4 fejezet), amely a személyes adatok kezelésével kiemelten foglalkozik.

Az *Ügyfél* a Szolgáltatási szerződés aláírásával hozzájárul ahhoz, hogy a személyes adatait a *Nem minősített időbélyegzés-szolgáltató* (az adatkezelési szabályzatnak megfelelő módon) tárolja és kezelje. A hozzájárulás vonatkozik a törvény által meghatározott és nyilvántartásba vett információk harmadik félhez történő továbbítására a *Nem minősített időbélyegzés-szolgáltató* szolgáltatásainak leállítása esetén, valamint – kizárólag a szolgáltatással összefüggő feladatok elvégzése céljából – a *Nem minősített időbélyegzés-szolgáltató* alvállalkozóinak való továbbításra. A *Nem minősített időbélyegzés-szolgáltató* az *Ügyfel*ek adatait kizárólag a szolgáltatásaival összefüggésben használja fel.

A *Nem minősített időbélyegzés-szolgáltató* a tudomására jutott adatokat a jogszabályi követelményeknek megfelelően, az előírt időtartamig megőrzi. A *Nem minősített időbélyegzés-szolgáltató* az adatok megőrzése során gondoskodik az információk sértetlenségéről, bizalmasságáról és biztonságos tárolásáról. Az információkhoz való hozzáférést csak azon személyeknek engedélyezi, akik feladata azt indokolja.

A *Nem minősített időbélyegzés-szolgáltató* az *Ügyfel*ek adatainak továbbítása során gondoskodik a nem nyilvános információk bizalmasságáról és sértetlenségéről.

9.3.1. Bizalmas információk köre

A *Nem minősített időbélyegzés-szolgáltató* bizalmas információként kezeli:

- az *Ügyfel*ek minden adatát, kivéve azokat, amelyeket a 9.3.2. fejezetben nem bizalmasnak tekintett információnak minősít;
- az *Ügyfel*ek adatain kívül:
  - a tranzakciós és naplóadatokat;
  - a nem nyilvános szabályzatokat;
  - minden olyan adatot, amelynek nyilvánosságra hozatala a szolgáltatás biztonságát előnytelenül befolyásolná.

9.3.2. Bizalmas információk körén kívül eső adatok

A *Nem minősített időbélyegzés-szolgáltató* nyilvánosnak tekint miden olyan adatot, amely nyilvánosan elérhető forrásból beszerezhető, vagy amely nyilvánosságra hozatalához az *Előfizető* előzetesen írásban hozzájárult.

9.3.3. Bizalmas információ védelme

A *Nem minősített időbélyegzés-szolgáltató* felelősséggel tartozik az általa kezelt bizalmas adatok védelméért.

A *Nem minősített időbélyegzés-szolgáltató* szerződésben vagy titoktartási nyilatkozat aláírásával kötelezi alkalmazottait, alvállalkozóit, szerződött partnereit a bizalmas adatok védelmére.

A *Nem minősített időbélyegzés-szolgáltató* a birtokába jutott bizalmas adatokat az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény [3] rendelkezéseinek megfelelően kezeli, és kizárólag az alábbi esetben fedi fel azokat:

- **Információszolgáltatás a hatóságok részére**

  A *Nem minősített időbélyegzés-szolgáltató* az Eüt. [5] 90. § (1) bekezdésének megfelelően az általa nyújtott bizalmi szolgáltatások felhasználásával elkövetett bűncselekmények felderítése vagy megelőzése céljából, illetőleg nemzetbiztonsági érdekből – az adatigénylésre külön törvényben meghatározott feltételek teljesülése esetén – a nyomozó hatóságnak és a nemzetbiztonsági szolgálatoknak díjmentesen továbbítja az érintett személyazonosságát igazoló, valamint a *Nem minősített időbélyegzés-szolgáltató* által egyeztetett adatokat.

  A *Nem minősített időbélyegzés-szolgáltató* rögzíti az adatátadás tényét, de arról nem tájékoztatja az érintett *Ügyfel*eket.

- **A tulajdonos kérésére történő felfedés**

  A *Nem minősített időbélyegzés-szolgáltató* az *Ügyfél* személyes kérése vagy az általa hivatalosan, írásban adott felhatalmazása alapján tárja fel a rá vonatkozó bizalmas felhasználói információkat harmadik fél részére.

9.4. Személyes adatok védelme

A *Nem minősített időbélyegzés-szolgáltató* gondoskodik az általa kezelt személyes adatok védelméről, működése és szabályzatai megfelelnek az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény [3] és a 2016/679 EU általános adatvédelmi rendelet [2] rendelkezéseinek.

A *Nem minősített időbélyegzés-szolgáltató* az *Ügyfél*ről nyilvántartott személyes adatokat és információkat a jogszabályi előírásoknak megfelelően

- megőrzi,
- azokat a megőrzési kötelezettség lejártával – amennyiben az *Ügyfél* erről másképpen nem rendelkezik – az ügyfél adatbázisból törli.

A *Nem minősített időbélyegzés-szolgáltató* nyilvántartásában azonosító adatokat, az *Előfizető*ről kizárólag a szolgáltatás igénybevételéhez, valamint a szerződéskötéshez és a számlázáshoz szükséges információkat tárolja.

A *Nem minősített időbélyegzés-szolgáltató* kizárólag olyan esetben adja át harmadik félnek az *Ügyfél* adatait, ha ezt jogszabály előírja vagy ha az *Ügyfél* ebbe írásban beleegyezett.

9.4.1. Adatkezelési szabályzat

A *Nem minősített időbélyegzés-szolgáltató* rendelkezik adatkezelési szabályzattal, amely részletes előírásokat tartalmaz a személyes adatok kezelésére. Az adatkezelési szabályzat megtalálható az e-Szignó Hitelesítés Szolgáltató honlapján az alábbi linken:

`https://e-szigno.hu/letoltesek/dokumentumok-es-szabalyzatok/`

9.4.2. Személyes adatok

A *Nem minősített időbélyegzés-szolgáltató* védi az érintettel kapcsolatba hozható, vagy az érintettre vonatkozó következtetést tartalmazó minden olyan személyes adatot, amely nem érhető el nyilvános adatforrásból.

A *Nem minősített időbélyegzés-szolgáltató* csak az *Előfizető*től közvetlenül, vagy annak egyértelmű előzetes hozzájárulásával gyűjt személyes adatokat és csak olyan mértékben, ami a szolgáltatás nyújtásához szükséges.

9.4.3. Személyes adatnak nem minősülő adatok

A *Nem minősített időbélyegzés-szolgáltató* nem köteles bizalmasként kezelni az olyan személyes adatot, amely nyilvános adatforrásból elérhető.

9.4.4. Személyes adatok védelme

A *Nem minősített időbélyegzés-szolgáltató* biztonságosan tárolja és védi az általa kezelt személyes adatokat. Az adatokat megfelelő intézkedésekkel védi különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, valamint nyilvánosságra hozatal ellen.

A *Nem minősített időbélyegzés-szolgáltató* általánosan felelős az Adatkezelési szabályzatában leírtak betartásáért, felelőssége kiterjed az alvállalkozói által végzett tevékenységekre is.

9.4.5. Személyes adatok felhasználása

A *Nem minősített időbélyegzés-szolgáltató* csak a szolgáltatás nyújtásához megkívánt mértékben, az *Ügyfél*lel való kapcsolattartás érdekében használja fel az *Ügyfél* személyes adatait.

9.4.6. Adatkezelés

A *Nem minősített időbélyegzés-szolgáltató* az *Ügyfél* értesítése nélkül is kiadhatja az *Ügyfél*ről tárolt személyes adatokat a vonatkozó jogszabályok által meghatározott esetekben.

9.4.7. Egyéb adatvédelmi követelmények

Nincs előírás.

9.5. Szellemi tulajdonjogok

A *Nem minősített időbélyegzés-szolgáltató* működése során nem sértheti meg harmadik személy szellemi tulajdonjogait.

A jelen *Nem minősített időbélyegzési szolgáltatási szabályzat* a *Nem minősített időbélyegzés-szolgáltató* kizárólagos tulajdonát képezi. Az *Ügyfel*ek és egyéb *Érintett felek* a dokumentumot

csak a jelen *Nem minősített időbélyegzési szolgáltatási szabályzat* előírásainak megfelelően jogosultak felhasználni, minden egyéb kereskedelmi vagy egyéb célú felhasználás szigorúan tilos.

A jelen *Nem minősített időbélyegzési szolgáltatási szabályzat* szabadon terjeszthető, de csak változatlan formában, teljes terjedelemben és az eredet feltüntetésével.

A *Nem minősített időbélyegzés-szolgáltató* által a szolgáltatás igénybevételéhez biztosított szoftverek használatának szabályait a szoftver leírásában vagy magában a szoftverben elérhető illetve ott meghivatkozott helyen található felhasználói útmutató tartalmazza.

9.6. Tevékenységért viselt felelősség és helytállás

9.6.1. A szolgáltató felelőssége és helytállása

A Szolgáltató felelőssége

A *Nem minősített időbélyegzés-szolgáltató* felelősségét jelen *Nem minősített időbélyegzési szolgáltatási szabályzat*, a vonatkozó *Nem minősített időbélyegzési rend*, valamint az *Ügyfél*lel kötött Szolgáltatási szerződés és annak mellékletei tartalmazzák, melyek szerint:

- a *Nem minősített időbélyegzés-szolgáltató* felelősséget vállal az általa támogatott *Nem minősített időbélyegzési rend*(ek)ben leírt eljárásoknak való megfelelésért;
- a *Nem minősített időbélyegzés-szolgáltató* sajátjaként felel az alvállalkozói által a szolgáltatás nyújtása során okozott károkért;
- a *Nem minősített időbélyegzés-szolgáltató* a vele szerződéses jogviszonyban álló *Ügyfel*ekkel szemben a Polgári Törvénykönyv [4] a szerződésszegésért való felelősség szabályai szerint felelős;
- a *Nem minősített időbélyegzés-szolgáltató* a vele szerződéses jogviszonyban nem álló harmadik személlyel (ilyen az *Érintett fél*) szemben a Polgári Törvénykönyv [4] általános felelősségi szabálya szerint felelős;
- a *Nem minősített időbélyegzés-szolgáltató* a felelősségi körén belül keletkezett, bizonyított károkért a szabályzataiban és az *Ügyfél*lel megkötött Szolgáltatási szerződésekben rögzített korlátozásokkal kártérítést fizet (lásd: Pénzügyi felelősség korlátozása 9.8. fejezet);
- 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.

A *Nem minősített időbélyegzés-szolgáltató* nem felelős az *Érintett felek* vagy mások által kibocsátott szabályzatokért.

A Szolgáltató kötelezettsége

A *Nem minősített időbélyegzés-szolgáltató* alapvető kötelezettsége, hogy a szolgáltatásokat a *Nem minősített időbélyegzési rend*del, a *Nem minősített időbélyegzési szolgáltatási szabályzat*tal és egyéb nyilvános szabályzatokkal, a szerződéses feltételekkel, továbbá a vállalati és biztonsági belső szabályzatokkal összhangban nyújtsa. Ezen alapvető kötelezettségek a következők:

- a szolgáltatásnak megfelelő jogi-, szabályozási-, anyagi-, szerződéses stb. keretek megteremtése;
- magas színvonalú és biztonságos szolgáltatások nyújtása a vonatkozó szabályzatok szerint;
- a szolgáltatásokhoz kapcsolódó szervezetek (hitelesítő szervezet, ügyfélszolgálat stb.) folyamatos működtetése és ellenőrzése;
- a szabályzatokban előírt eljárások betartása és az esetleg bekövetkező helytelen működés elkerülése, illetve megszüntetése;
- a szolgáltatások biztosítása minden olyan igénylő számára, aki elfogadja a szabályzatokban rögzített feltételeket;
- a publikus nyilvántartások és saját szabályzatok karbantartása és folyamatos elérhetővé tétele bárki számára az interneten keresztül.

9.6.2. Az Ügyfél felelőssége és helytállása

Az *Előfizető* felelőssége

Az *Előfizető* felelősségét a Szolgáltatási szerződés és annak mellékletei (köztük az Általános szerződési feltételek) határozzák meg.

Az *Előfizető* kötelezettségei

Az *Előfizető* köteles a *Nem minősített időbélyegzés-szolgáltató* szerződéses feltételeinek és szabályzatainak megfelelően eljárni a szolgáltatás igénybevétele során.

Az *Előfizető* kötelezettségeit a jelen *Nem minősített időbélyegzési szolgáltatási szabályzat*, a Szolgáltatási szerződés és annak elválaszthatatlan részét képező Általános szerződési feltételek és egyéb dokumentumok, valamint a vonatkozó *Nem minősített időbélyegzési rend* tartalmazzák.

Az *Előfizető* jogai

Az *Előfizető* jogosult:

- a szolgáltatások igénybevételére a jelen *Nem minősített időbélyegzési szolgáltatási szabályzat*ban leírtak szerint;

9.6.3. Az Érintett fél felelőssége

Az *Érintett felek* saját belátásuk és/vagy szabályzataik alapján dönthetnek az egyes *Időbélyegző*k elfogadásáról és a felhasználás módjáról. Az érvényesség vizsgálata során a *Nem minősített időbélyegzés-szolgáltató* által garantált biztonsági szint megtartásához szükséges, hogy az *Érintett fél* megfelelő körültekintéssel járjon el, ezért különös tekintettel javasolt:

- a *Nem minősített időbélyegzési rend*ben és a *Nem minősített időbélyegzési szolgáltatási szabályzat*ban megfogalmazott követelmények, előírások betartása;
- megbízható informatikai környezet és alkalmazások használata;
- az *Időbélyegző* aláírásához használt *Tanúsítvány* visszavonási állapotának ellenőrzése az aktuális CRL vagy OCSP válasz alapján;
- az *Időbélyegző* felhasználására vonatkozó valamennyi korlátozás figyelembevétele, amely a jelen *Nem minősített időbélyegzési rend*ben és a *Nem minősített időbélyegzési szolgáltatási szabályzat*ban szerepel.

9.6.4. Egyéb szereplők tevékenységéért viselt felelősség és helytállás

Nincs megkötés.

9.7. Helytállás érvénytelenségi köre

A *Nem minősített időbélyegzés-szolgáltató* kizárja felelősségét, amennyiben:

- az Internet, vagy annak egy részének működési hibájából adódóan a tájékoztatás és egyéb kommunikációs kötelezettségeit nem tudja ellátni;
- a károkozás a Nemzeti Média- és Hírközlési Hatóság algoritmusokkal kapcsolatos határozat által elfogadott kriptográfiai algoritmusok hibájából, illetve gyengeségeiből ered.

9.8. A felelősség korlátozása

A *Nem minősített időbélyegzés-szolgáltató* korlátozza a szolgáltatással kapcsolatos kártérítési kötelezettségét, ezen korlátozás mértéke káreseményenként 20.000,-Ft.

Ha egy káreseménnyel kapcsolatban több jogosult megalapozott kártérítési igénye meghaladja a károkra káreseményenként a fenti korlátozás szerint meghatározott összeget, akkor a kártérítési igények megtérítése az összes kártérítési igénynek a korlátozás szerint meghatározott összeghez viszonyított arányában történik.

9.9. Kártérítési kötelezettség

9.9.1. A szolgáltató kártérítési kötelezettsége

A *Nem minősített időbélyegzés-szolgáltató* kártérítési kötelezettségének részletes szabályait jelen szabályzat (lásd: 9.8. fejezet), a Szolgáltatási szerződés és az *Ügyfel*ekkel kötött szerződések tartalmazzák.

9.9.2. Az előfizető kártérítési kötelezettsége

Az *Előfizető* kártérítési felelősséggel tartozik a *Nem minősített időbélyegzés-szolgáltató*nak azokért a veszteségekért és károkért, amelyeket kötelezettségei és a rá vonatkozó ajánlások be nem tartásával okoz számára.

9.9.3. Az érintett felek kártérítési kötelezettsége

Lásd: 9.8. fejezet

9.10. Érvényesség és megszűnés

9.10.1. Érvényesség

A *Nem minősített időbélyegzési szolgáltatási szabályzat* adott verziója hatálybalépésének napja a dokumentum címlapján kerül meghatározásra.

9.10.2. Megszűnés

A *Nem minősített időbélyegzési szolgáltatási szabályzat* visszavonásig illetve a *Nem minősített időbélyegzési szolgáltatási szabályzat* újabb verziójának hatályba lépéséig hatályos időbeli korlátozás nélkül.

9.10.3. A megszűnés következményei

A *Nem minősített időbélyegzési szolgáltatási szabályzat* visszavonása esetén a *Nem minősített időbélyegzés-szolgáltató* honlapján közzéteszi a visszavonás részletes szabályait és a visszavonás után is fennálló jogokat és kötelezettségeket.

A *Nem minősített időbélyegzés-szolgáltató* garantálja, hogy a *Nem minősített időbélyegzési szolgáltatási szabályzat* visszavonása esetén is érvényben maradnak a bizalmas adatok védelmére vonatkozó előírások.

9.11. A felek közötti kommunikáció

A *Nem minősített időbélyegzés-szolgáltató* az *Ügyfel*ekkel történő kapcsolattartás érdekében ügyfélszolgálati irodát működtet.

Az *Ügyfel*ek jognyilatkozataikat a *Nem minősített időbélyegzés-szolgáltató* felé kizárólag írásban, aláírt módon tehetik meg. Szervezet képviseletében történő aláírás csak a képviseleti jogosultság igazolásával együtt érvényes.

Az e-Szignó Hitelesítés Szolgáltató elektronikus levélben tájékoztatja *Ügyfel*eit vagy tájékoztatását honlapján teszi közzé.

9.12. Módosítások

A *Nem minősített időbélyegzés-szolgáltató* fenntartja magának a jogot, hogy a normatív szabályok, biztonsági követelmények, piaci környezet vagy egyéb körülmények változása esetén szabályozott módon megváltoztassa a *Nem minősített időbélyegzési szolgáltatási szabályzat*ot.

9.12.1. Módosítási eljárás

A *Nem minősített időbélyegzés-szolgáltató* nyilvános szabályzataiban csak azon eljárásait hozza nyilvánosságra, melyek ismerete a szolgáltatások biztonságát nem veszélyezteti. A *Nem minősített időbélyegzés-szolgáltató* több belső biztonsági és egyéb szabályzattal, operatív szintű előírással rendelkezik, melyeket bizalmasan kezel (jelen *Nem minősített időbélyegzési szolgáltatási szabályzat* több ilyet is megemlít). A 8.4. fejezetben leírt eljárások ezeket a dokumentumokat is vizsgálják.

A *Nem minősített időbélyegzés-szolgáltató* hitelesítő szervezetén belül működik egy olyan szervezeti egység, amely felelős a szabályzatok és dokumentációk karbantartásáért. A változtatási igényeket e csoport gyűjti, a módosításokat elvégzi, a belső és külső tájékoztatási kötelezettségeknek eleget tesz. A szabályzatot az e-Szignó Hitelesítés Szolgáltató igazgatója hagyja jóvá.

A változtatásokat gyűjtve a csoport belső, nem nyilvános munkaváltozatokat hoz létre a szabályzatokból, melyek a közzététel előtt belső felülvizsgálaton esnek át. A *Nem minősített időbélyegzés-szolgáltató* törekszik arra, hogy új szabályzatot csak a lehető legritkábban kelljen kibocsátania.

A *Nem minősített időbélyegzés-szolgáltató* évi rendszerességgel illetve rendkívüli változtatási igény esetén soron kívül átvizsgálja a *Nem minősített időbélyegzési szolgáltatási szabályzat*ot és elvégzi a szükségesnek tartott változtatásokat. A dokumentum a legkisebb változtatás után is új verziószámot kap és az elfogadási procedúra időigényét figyelembe véve meghatározásra kerül a tervezett hatálybalépés időpontja is.

Nem minősített időbélyegzés-szolgáltató a jóváhagyott dokumentumot a tervezett hatálybalépés előtt publikálja honlapján.

9.12.2. Értesítések módja és határideje

A *Nem minősített időbélyegzés-szolgáltató* a 9.12.1. pontban leírtak szerint értesíti az *Érintett felek*et az új dokumentum verziók kibocsátásáról.

9.12.3. Az OID megváltoztatása

A *Nem minősített időbélyegzés-szolgáltató* a *Nem minősített időbélyegzési szolgáltatási szabályzat* legkisebb változtatása esetén is új verziószámot ad ki, ami része a dokumentum azonosítónak (OID), így a dokumentum minden változása az OID változását eredményezi, vagyis két eltérő tartalmú – hatályba léptetett – dokumentumnak nem lehet azonos OID azonosítója.

9.13. Vitás kérdések rendezése

A *Nem minősített időbélyegzés-szolgáltató* törekszik a működése során felmerülő vitás kérdések békés, tárgyalásos rendezésére. A rendezés során a fokozatosság elvét követi.

A *Nem minősített időbélyegzés-szolgáltató* és az *Ügyfél* kölcsönösen megállapodnak abban, hogy bármilyen vitás kérdés vagy panasz felmerülése esetén, a vita jogi útra való terelése előtt megkísérlik a békés úton, tárgyalással történő egyeztetést. A kezdeményező fél kötelessége, hogy minden érintett többi felet haladéktalanul értesítsen és teljes körűen tájékoztasson az ügy minden vonatkozását illetően.

Az *Ügyfél* vitás kérdés felmerülése esetén jogosult az esetleges bírósági eljárást megelőzően a Budapesti Békéltető Testülethez fordulni.

A *Nem minősített időbélyegzés-szolgáltató* tevékenységével kapcsolatos kérdéseket, kifogásokat és panaszokat az ügyfélszolgálati iroda címére kell eljuttatni írásos formában. A bejelentés kézhezvételétől számított 3 munkanapon belül a *Nem minősített időbélyegzés-szolgáltató* értesíti a bejelentő felet az általa megadott címen a bejelentés fogadásáról és a kivizsgáláshoz szükséges időről. A megjelölt határidőig a *Nem minősített időbélyegzés-szolgáltató* köteles írásban válaszolni a bejelentőnek. A *Nem minősített időbélyegzés-szolgáltató* a válaszadáshoz szükséges információk megadását kérheti a bejelentőtől. A *Nem minősített időbélyegzés-szolgáltató* a panaszt 30 napon belül kivizsgálja, és az eredményekről értesíti a bejelentőt.

Amennyiben a választ a bejelentő nem tartja kielégítőnek, vagy az alapján nem sikerül a *Nem minősített időbélyegzés-szolgáltató* bevonása nélkül rendezni a felmerült vitát, akkor a bejelentő egyeztetést kezdeményezhet a *Nem minősített időbélyegzés-szolgáltató*val és az *Érintett felek*kel. Az egyeztetés minden résztvevőjét írásban értesíteni kell az egyeztetés időpontjáról azt megelőzően 10 munkanappal, és írásban meg kell számukra küldeni a bejelentést, a *Nem minősített időbélyegzés-szolgáltató* válaszát és egyéb szükséges információkat tartalmazó dokumentumokat.

Amennyiben az egyeztetés a panasz benyújtásától számított 30 napon belül nem vezet eredményre, akkor a bejelentő peres útra terelheti az ügyet. Az *Érintett felek* kölcsönösen alávetik magukat a Budapesti II. és III. Kerületi Bíróság, illetve a Fővárosi Törvényszék kizárólagos illetékességének.

9.14. Irányadó jog

A *Nem minősített időbélyegzés-szolgáltató* tevékenységét a mindenkor hatályos magyar jogszabályoknak megfelelően végzi. A *Nem minősített időbélyegzés-szolgáltató* szerződéseire és szabályzataira, azok teljesítésére a magyar jog az irányadó, s azok a magyar jog szerint értelmezendők.

9.15. Az érvényben lévő jogszabályoknak való megfelelés

A vonatkozó jogszabályok:

- AZ EURÓPAI PARLAMENT ÉS A TANÁCS 910/2014/EU RENDELETE (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről [1];
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról [3];
- 2013. évi V. törvény a Polgári Törvénykönyvről [4].
- 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól [5];
- 24/2016. (VI. 30.) BM rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről [6];
- 25/2016. (VI. 30.) BM rendelet a bizalmi felügyeletnek fizetendő igazgatási szolgáltatási díjak mértékéről [7];

- 470/2017. (XII. 28.) Kormányrendelet a bizalmi felügyelet által vezetett nyilvántartások tartalmáról és a bizalmi szolgáltatás nyújtásával kapcsolatos bejelentésekről [8];

9.16. Vegyes rendelkezések

9.16.1. Teljességi záradék

Nincs megkötés.

9.16.2. Átruházás

A jelen *Nem minősített időbélyegzési szolgáltatási szabályzat* alapján nyújtott szolgáltatásokba bevont alvállalkozók vagy egyéb együttműködő partnerek csak a *Nem minősített időbélyegzés-szolgáltató* előzetes írásbeli engedélyével adhatják tovább jogosultságaikat és delegálhatják kötelezettségeiket harmadik félnek.

9.16.3. Részleges érvénytelenség

A jelen *Nem minősített időbélyegzési szolgáltatási szabályzat* egyes rendelkezéseinek tetszőleges okból történő érvénytelenné válása esetén a többi rendelkezés változatlan formában érvényben marad.

9.16.4. Igényérvényesítés

A *Nem minősített időbélyegzés-szolgáltató* kártérítésre, az ügyvédi díjak megfizetésére tarthat igényt a partnerei által okozott károk, veszteségek, költségek megtérítése érdekében. Amennyiben a *Nem minősített időbélyegzés-szolgáltató* egy konkrét esetben nem él kártérítési igényével, az nem jelenti azt, hogy a jövőben hasonló esetben vagy a jelen *Nem minősített időbélyegzési szolgáltatási szabályzat* más rendelkezésének megsértése esetén is lemondana a kártérítési igény érvényesítéséről.

9.16.5. Vis maior

A *Nem minősített időbélyegzés-szolgáltató* nem felelős a *Nem minősített időbélyegzési rend*ben és a *Nem minősített időbélyegzési szolgáltatási szabályzat*ban megfogalmazott kötelezettség hibás vagy késedelmes teljesítéséért, illetve nem teljesítéséért, amennyiben a hiba vagy késedelem oka a *Nem minősített időbélyegzés-szolgáltató* ellenőrzési körén kívül eső, előre nem látható elháríthatatlan külső ok.

9.17. Egyéb rendelkezések

Nincs megkötés.

A. Hivatkozások

[1] AZ EURÓPAI PARLAMENT ÉS A TANÁCS 910/2014/EU RENDELETE (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről .

[2] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) .

[3] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról .

[4] 2013. évi V. törvény a Polgári Törvénykönyvről .

[5] 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól .

[6] 24/2016. (VI. 30.) BM rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről .

[7] 25/2016. (VI. 30.) BM rendelet a bizalmi felügyeletnek fizetendő igazgatási szolgáltatási díjak mértékéről .

[8] 470/2017. (XII. 28.) Korm. rendelet a bizalmi felügyelet által vezetett nyilvántartások tartalmáról és a bizalmi szolgáltatás nyújtásával kapcsolatos bejelentésekről .

[9] ETSI EN 319 102-1 V1.2.1 (2018-08); Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation.

[10] ETSI EN 319 401 V2.2.1 (2018-04); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

[11] ETSI EN 319 411-1 V1.2.2 (2018-04); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

[12] ETSI EN 319 411-2 v2.2.2 (2018-04); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates;.

[13] ETSI EN 319 412-1 V1.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.

[14] ETSI EN 319 412-2 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons;.

[15] ETSI EN 319 412-3 V1.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons.

[16] ETSI EN 319 421 V1.1.1 (2016-03); Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.

[17] ETSI EN 319 422 V1.1.1 (2016-03); Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.

[18] ETSI TS 119 312 V1.3.1 (2019-02); Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.

[19] MSZ/ISO/IEC 15408-2002 Informatika. Biztonságtechnika. Az informatikai biztonságértékelés közös szempontjai, 2002 december .

[20] ISO/IEC 19790:2012: "Information technology – Security techniques – Security requirements for cryptographic modules".

[21] IETF RFC 3161: Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP), August 2001.

[22] IETF RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile, May 2008.

[23] IETF RFC 6818: Updates to the Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile, January 2013.

[24] ITU X.509 Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.

[25] Recommendation ITU-R TF.460-6 (2002): Standard-frequency and time-signal emissions.

[26] FIPS PUB 140-2 (2001 May 25): Security Requirements for Cryptographic Modules.

[27] CEN Workgroup Agreement CWA 14167-2: Cryptographic module for CSP signing operations with backup - Protection profile - CMCSOB PP.

[28] e-Szignó Hitelesítés Szolgáltató - eIDAS rendelet szerinti nem minősített időbélyegzési rend.