

e-Szignó Hitelesítés Szolgáltató

eIDAS Rendelet szerinti minősített időbélyegzési rend

ver. 2.14

Hatálybalépés: 2020-05-26



Azonosító	1.3.6.1.4.1.21528.2.1.1.186.2.14
Verzió	2.14
Első verzió hatálybalépése	2005-04-01
Biztonsági besorolás	NYILVÁNOS
Jóváhagyta	Vanczák Gergely
Jóváhagyás dátuma	2020-05-22
Hatálybalépés dátuma	2020-05-26

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

Verzió	A változás leírása	Hatálybalépés	Készítette
1.0	Első változat.	2005-04-01	Berta István Zsolt, Endródi Csilla Belső auditor: Tóth Elemér
2.0	A belső auditor javaslatai alapján átdolgozott változat (azonos az 1.1-es verzióval)	2005-04-15	Berta István Zsolt, Belső auditor: Tóth Elemér
3.0	Apróbb javítások	2005-05-02	Berta István Zsolt, Belső auditor: Tóth Elemér
3.2	A hatósági szemlét követő módosítások	2005-08-08	Berta István Zsolt, Belső auditor: Tóth Elemér
4.0	Módosítás az általános szerződési feltételek megváltozása miatt	2006-11-19	Berta István Zsolt
4.1	Új OID hozzárendelése.	2006-12-04	Berta István Zsolt
4.2	A fogyasztóvédelem elérhetősége megváltozott.	2007-10-28	Berta István Zsolt
4.3	A fogyasztóvédelem elérhetősége ismét megváltozott.	2008-01-01	Berta István Zsolt
4.4	Nem lépett hatályba.	2008-10-01	Berta István Zsolt
4.5	Az időbélyegek naplózásának megszüntetése.	2008-12-20	Berta István Zsolt
5.0	Cégforma változás.	2012-05-01	Berta István Zsolt
5.1	Kisebbségi változtatások.	2013-08-01	Dr. Szőke Sándor

Verzió	A változás leírása	Hatálybalépés	Készítette
2.0	eIDAS követelmények szerinti új rend új OID azonosítóval.	2016-07-01	Dr. Szőke Sándor
2.1	Módosítások az NMHH észrevételei alapján.	2016-09-05	Szomolya Melinda, Dr. Szőke Sándor
2.2	Módosítások a tanúsító észrevételei alapján.	2016-10-30	Dr. Szőke Sándor
2.4	Éves felülvizsgálat.	2017-09-30	Dr. Szőke Sándor
2.6	Teljes felülvizsgálat. Kisebb módosítások.	2018-03-24	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
2.13	Hatály. HSM követelmények. Kisebb pontosítások.	2020-03-05	Dr. Szőke Sándor
2.14	Kisebb pontosítások.	2020-05-26	Dr. Szőke Sándor

© 2020, Microsec zrt. Minden jog fenntartva.

Tartalomjegyzék

1. Bevezetés	11
1.1. Áttekintés	11
1.2. Dokumentum neve és azonosítója	11
1.2.1. A dokumentum főbb azonosító adatai	11
1.2.2. Megfelelés	11
1.2.3. Időbélyegzési rend	12
1.2.4. Hatály	13
1.3. PKI szereplők	13
1.3.1. Bizalmi Szolgáltató	13
1.3.2. Ügyfelek	13
1.3.3. Érintett felek	14
1.4. Az időbélyegző felhasználhatósága	14
1.5. A dokumentum adminisztrálása	14
1.5.1. A dokumentum adminisztrációs szervezete	14
1.5.2. Kapcsolattartó személy	14
1.5.3. A Szolgáltatási szabályzat <i>Minősített időbélyegzési rendnek</i> való megfelelőségéért felelős személy/szervezet	14
1.5.4. A Szolgáltatási szabályzat elfogadási eljárása	15
1.6. Fogalmak és rövidítések	15
1.6.1. Fogalmak	15
1.6.2. Rövidítések	19
2. Közzététel és adattár felelőségek	20
2.1. Adattárak	20
2.2. A tanúsítványokra vonatkozó információk közzététele	20
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	21
3.1. A felhasználó azonosítása	21
3.2. Az Időbélyegző egység tanúsítványa	21
3.3. Az Időbélyegző	21
3.3.1. Időbélyegző kérés	22
3.3.2. Időbélyegző válasz	22
3.4. Az Időbélyegzőben szereplő idő pontossága	23
3.5. Óraszinkronizálás	23
3.5.1. A szökőmásodpercek kezelése	23
3.5.2. Nyári időszámítás kezelése	23

3.6.	Az Időbélyegző ellenőrzése	23
3.7.	A szolgáltatás rendelkezésre állása	24
3.8.	Nem minősített időbélyegzők kibocsátása	24
3.9.	Az Időbélyegző egység kulcshasználata	24
3.10.	Az Időbélyegző szolgáltatás elérési módjai	24
4.	A tanúsítványok életciklusára vonatkozó követelmények	25
4.1.	A kulcspár és a tanúsítvány használata	25
4.1.1.	A magánkulcs és a tanúsítvány használata	25
4.1.2.	Az Érintett felek nyilvános kulcs és tanúsítvány használata	25
5.	Elhelyezési, eljárásbeli és üzemeltetési előírások	25
5.1.	Fizikai követelmények	25
5.1.1.	A telephely elhelyezése és szerkezeti felépítése	26
5.1.2.	Fizikai hozzáférés	26
5.1.3.	Áramellátás és légkondicionálás	27
5.1.4.	Beázás és elárasztódás veszély kezelése	27
5.1.5.	Tűz megelőzés és tűzvédelem	27
5.1.6.	Adathordozók tárolása	27
5.1.7.	Hulladék megsemmisítése	28
5.1.8.	A mentési példányok fizikai elkülönítése	28
5.2.	Eljárásbeli előírások	28
5.2.1.	Bizalmi szerepkörök	28
5.2.2.	Az egyes feladatok ellátásához szükséges személyzeti létszámok	29
5.2.3.	Az egyes szerepkörökben elvárt azonosítás és hitelesítés	29
5.2.4.	Egymást kizáró szerepkörök	30
5.3.	Személyzetre vonatkozó előírások	30
5.3.1.	Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények	30
5.3.2.	Előélet vizsgálatára vonatkozó eljárások	31
5.3.3.	Képzési követelmények	31
5.3.4.	Továbbképzési gyakoriságok és követelmények	31
5.3.5.	Munkabeosztás körforgásának sorrendje és gyakorisága	32
5.3.6.	Felhatalmazás nélküli tevékenységek büntető következményei	32
5.3.7.	Szerződéses viszonyban foglalkoztatottakra vonatkozó követelmények	32
5.3.8.	A személyzet számára biztosított dokumentációk	32
5.4.	Naplózási eljárások	32
5.4.1.	A tárolt események típusai	32
5.4.2.	A naplófájl feldolgozásának gyakorisága	35
5.4.3.	A naplófájl megőrzési időtartama	35

5.4.4.	A naplófájl védelme	35
5.4.5.	A naplófájl mentési eljárásai	36
5.4.6.	A naplózás adatgyűjtési rendszere	36
5.4.7.	Az eseményeket kiváltó alanyok értesítése	36
5.4.8.	Sebezhetőség felmérése	36
5.5.	Adatok archiválása	36
5.5.1.	Az archivált adatok típusai	36
5.5.2.	Az archívum megőrzési időtartama	37
5.5.3.	Az archívum védelme	37
5.5.4.	Az archívum mentési folyamatai	38
5.5.5.	Az adatok időbélyegzésére vonatkozó követelmények	38
5.5.6.	Az archívum gyűjtési rendszere	38
5.5.7.	Archív információk hozzáférését és ellenőrzését végző eljárások	38
5.6.	Szolgáltatói kulcs cseréje	38
5.7.	Kompromittálódást és katasztrófát követő helyreállítás	39
5.7.1.	Váratlan esemény és kompromittálódás kezelési eljárások	39
5.7.2.	Meghibásodott IT erőforrások, szoftverek és/vagy adatok	39
5.7.3.	Magánkulcs kompromittálódása esetén követendő eljárások	40
5.7.4.	Működés folyamatosságának biztosítása katasztrófát követően	40
5.8.	Az Időbélyegzés-szolgáltató leállítása	40
6.	Műszaki biztonsági óvintézkedések	41
6.1.	Kulcspár előállítás és telepítése	41
6.1.1.	Kulcspár előállítás	41
6.1.2.	Kulcsméret	42
6.1.3.	A nyilvános kulcs paraméterek előállítása, a minőség ellenőrzése	42
6.1.4.	A kulcshasználat célja (az X.509 v3 kulcs használati mező tartalmának megfelelően)	42
6.2.	A magánkulcsok védelme	43
6.2.1.	Kriptográfiai modulra vonatkozó szabványok és előírások	43
6.2.2.	Magánkulcs többszereplős (n-ből m) használata	43
6.2.3.	Magánkulcs letétbe helyezése	43
6.2.4.	Magánkulcs mentése	44
6.2.5.	Magánkulcs archiválása	44
6.2.6.	Magánkulcs bejuttatása hardver kriptográfiai eszközbe, vagy onnan történő exportja	44
6.2.7.	Magánkulcs tárolása hardver kriptográfiai eszközben	44
6.2.8.	A magánkulcs aktiválásának módja	44
6.2.9.	A magánkulcs deaktiválásának módja	44

6.2.10.	A magánkulcs megsemmisítésének módja	45
6.2.11.	A hardver kriptográfiai eszközök értékelése	45
6.3.	A kulcspár kezelés egyéb szempontjai	45
6.3.1.	A tanúsítványok és kulcspárok használatának periódusa	45
6.4.	Aktivizáló adatok	46
6.4.1.	Aktivizáló adatok előállítása és telepítése	46
6.4.2.	Az aktivizáló adatok védelme	46
6.4.3.	Az aktivizáló adatok kezelésének egyéb szempontjai	47
6.5.	Informatikai biztonsági előírások	47
6.5.1.	Speciális informatikai biztonsági műszaki követelmények	47
6.5.2.	Az informatikai biztonság értékelése	47
6.6.	Életciklusra vonatkozó műszaki előírások	47
6.6.1.	Rendszerfejlesztési előírások	47
6.6.2.	Biztonságkezelési előírások	48
6.6.3.	Életciklusra vonatkozó biztonsági előírások	48
6.7.	Hálózati biztonsági előírások	49
6.8.	Időbélyegzés	50
7.	Tanúsítvány, CRL és OCSP profilok	50
7.1.	Tanúsítvány profil	50
7.1.1.	Verzió szám(ok)	50
7.1.2.	Tanúsítvány kiterjesztések	51
8.	A megfelelés vizsgálat	54
8.1.	Az ellenőrzések körülményei és gyakorisága	54
8.2.	Az auditor és szükséges képesítése	55
8.3.	Az auditor és az auditált rendszerelem függetlensége	55
8.4.	Az auditálás által lefedett területek	55
8.5.	A hiányosságok kezelése	55
8.6.	Az eredmények közzététele	56
9.	Egyéb üzleti és jogi kérdések	56
9.1.	Díjak	56
9.1.1.	Visszatérítési politika	56
9.2.	Anyagi felelősségvállalás	56
9.2.1.	Pénzügyi követelmények	56
9.2.2.	Felelősségbiztosítás	57
9.3.	Bizalmasság	57
9.3.1.	Bizalmas információk köre	57
9.3.2.	Bizalmas információk körén kívül eső adatok	58

9.3.3.	Bizalmas információ védelme	58
9.4.	Személyes adatok védelme	58
9.4.1.	Adatkezelési terv	58
9.4.2.	Személyes adatok	58
9.4.3.	Személyes adatnak nem minősülő adatok	59
9.4.4.	Személyes adatok védelme	59
9.4.5.	Személyes adatok felhasználása	59
9.4.6.	Adatkezelés	59
9.4.7.	Egyéb adatvédelmi követelmények	59
9.5.	Szellemi tulajdonjogok	59
9.6.	Tevékenyséért viselt felelősség és helytállás	60
9.6.1.	A szolgáltató felelőssége és helytállása	60
9.6.2.	Az Ügyfél felelőssége és helytállása	61
9.6.3.	Az Érintett fél felelőssége	61
9.6.4.	Egyéb szereplők tevékenységéért viselt felelősség és helytállás	62
9.7.	Helytállás érvénytelenségi köre	62
9.8.	A felelősség korlátozása	62
9.9.	Kártérítési kötelezettség	62
9.9.1.	A szolgáltató kártérítési kötelezettsége	62
9.9.2.	Az előfizető kártérítési kötelezettsége	62
9.9.3.	Az érintett felek kártérítési kötelezettsége	62
9.10.	Érvényesség és megszűnés	63
9.10.1.	Érvényesség	63
9.10.2.	Megszűnés	63
9.10.3.	A megszűnés következményei	63
9.11.	A felek közötti kommunikáció	63
9.12.	Módosítások	63
9.12.1.	Módosítási eljárás	63
9.12.2.	Értesítések módja és határideje	64
9.12.3.	Az OID megváltoztatása	64
9.13.	Vitás kérdések rendezése	64
9.14.	Irányadó jog	64
9.15.	Az érvényben lévő jogszabályoknak való megfelelés	64
9.16.	Vegyes rendelkezések	65
9.16.1.	Teljességi záradék	65
9.16.2.	Átruházás	65
9.16.3.	Részleges érvénytelenség	65
9.16.4.	Igényérvényesítés	65
9.16.5.	Vis maior	65
9.17.	Egyéb rendelkezések	65

A. Hivatkozások

66

1. Bevezetés

Jelen dokumentum a Microsec Számítástechnikai Fejlesztő zrt. (továbbiakban: Microsec vagy *Minősített időbélyegzés-szolgáltató*) által üzemeltetett e-Szignó Hitelesítés Szolgáltató által meghatározott minősített időbélyegzési szolgáltatásra vonatkozó *Minősített időbélyegzési rendet* tartalmazza.

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

1.1. Áttekintés

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

A *Minősített időbélyegzési rend* alapvető követelményeket fogalmaz meg az *Időbélyegzőkkel* kapcsolatban elsősorban az *Időbélyegzőt* kibocsátó *Minősített időbélyegzés-szolgáltató* részére. Ezen követelmények teljesítésének módját, illetve az itt megnevezett eljárások részletes leírását a *Minősített időbélyegzés-szolgáltató* által kibocsátott *Minősített időbélyegzési szolgáltatási szabályzat*nak kell tartalmaznia.

A *Minősített időbélyegzési rend* egyike a *Minősített időbélyegzés-szolgáltató* által kiadott azon dokumentumoknak, amelyek a *Minősített időbélyegzés-szolgáltató* által nyújtott szolgáltatások feltételeit együttesen szabályozzák. További dokumentumok például az Általános szerződési feltételek, a *Minősített időbélyegzési szolgáltatási szabályzat*, 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 minősített időbélyegzési rend
Azonosító	1.3.6.1.4.1.21528.2.1.1.186
Dokumentum verziószáma	2.14
Hatályba lépés ideje	2020-05-26

A *Minősített időbélyegzési rend* aktuális változata a *Minősített időbélyegzés-szolgáltató* honlapján, illetve a *Minősített időbélyegzés-szolgáltató* ügyfélszolgálati irodájában érhető el.

1.2.2. Megfelelés

A jelen *Minősített időbélyegzési rend* szerint kiállított *Időbélyegzők* megfelelnek az alábbi követelményeknek:

- ETSI EN 319 421 [18] 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 követelményeknek való megfelelés kinyilatkoztatása érdekében a *Minősített időbélyegzés-szolgáltató* két megoldás közül választhat:

- a fenti OID azonosítót szerepeltetnie kell az általa kibocsátott *Időbélyegző*kben;
- amennyiben a *Minősített időbélyegzés-szolgáltató* az általa kibocsátott *Időbélyegző*kben saját OID azonosítóját szerepelteti, a *Minősített időbélyegzési szolgáltatási szabályzatában* és a TSA megfeleléségi nyilatkozatában ki kell jelentenie a fenti ETSI időbélyegzési rend (BTSP) támogatását.

1.2.3. Időbélyegzési rend

A *Minősített időbélyegzési rendet* azonosító OID első hét száma a Microsec egyedi azonosítója az alábbiak szerint:

(1)	International Organization for Standardization (ISO)	Nemzetközi Szabványügyi Szervezet (ISO)
(3)	Organization identification schemes registered according to ISO/IEC 6523-2	Az ISO/IEC 6523-2 szerint regisztrált szervezeti azonosító rendszer
(6)	United States Department of Defense (DoD)	Amerikai Védelmi Minisztérium (DoD)
(1)	Internet	Internet
(4)	Private projects	Magán projektek
(1)	Private enterprises	Magán vállalatok
(21528)	MICROSEC Ltd.	Microsec zrt.

A további számok rendszerét a Microsec saját hatáskörben osztotta ki, értelmezésük az alábbiak szerinti:

(1.3.6.1.4.1.21528)	MICROSEC Ltd.
(2)	e-Szignó Hitelesítés Szolgáltató
(1)	dokumentumok
(1)	nyilvános dokumentumok
(x)	dokumentum egyedi azonosító sorszáma
(y)	dokumentum verziója
(z)	dokumentum alverziója

Jelen dokumentum az alábbi *Minősített időbélyegzési rend(ek)*et definiálja:

OID	MEGNEVEZÉS	RÖVID NÉV
1.3.6.1.4.1.21528.2.1.1.186.2.14	eIDAS Rendelet szerinti minősített időbélyegzési rend.	MIR

A *Minősített időbélyegzési rend* mindenkor aktuális és minden korábbi változata elérhető az alábbi címen:

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

1.2.4. Hatály

Jelen *Minősített időbélyegzési rend* 2020-05-26 -i hatálybalépési dátumtól visszavonásáig hatályos. A hatályosság automatikusan megszűnik a *Minősített időbélyegzési rend* újabb verziójának hatályba lépésekor.

Jelen *Minősített időbélyegzési rendet* és az ezen alapuló *Minősített időbélyegzési szolgáltatási szabályzatokat* legalább évente felül kell vizsgálni, és gondoskodni kell az esetlegesen megváltozott követelményekhez illetve igényekhez igazodó módosításokról.

A *Minősített időbélyegzési rend* hatálya kiterjed az 1.3. alfejezetben azonosított közösség minden egyes tagjára.

A jelen *Minősített időbélyegzési rend* a magyar jog alapján Magyarországon, elsősorban magyar *Ügyfelek* részére, magyar nyelven nyújtott szolgáltatásokra vonatkozó konkrét követelményeket tartalmaznak. A *Minősített időbélyegzés-szolgáltató* kiterjesztheti a szolgáltatás területi hatályát, ez esetben a magyar viszonyokra alkalmazható előírásoknak megfelelő, azoknál nem enyhébb követelményeket kell alkalmaznia. Ennek részleteit a *Minősített időbélyegzési szolgáltatási szabályzatban* kell rögzíteni.

1.3. PKI szereplők

1.3.1. Bizalmi Szolgáltató

A *Minősített időbélyegzés-szolgáltató* egy olyan *Bizalmi szolgáltató*, amely *Bizalmi szolgáltatás* keretében *Időbélyegzőket* bocsát ki, és ellátja az ehhez kapcsolódó feladatokat.

Jelen dokumentum előírásai vonatkoznak mindazon *Minősített időbélyegzés-szolgáltatókra*, akik a *Minősített időbélyegzési szolgáltatási szabályzatukban* vállalják a jelen dokumentumban szereplő *Minősített időbélyegzési rend(ek)* valamelyikének való megfelelést.

1.3.2. Ügyfelek

Az *Előfizető* (Ügyfél), aki előfizet a *Minősített időbélyegzés-szolgáltató* által nyújtott *Időbélyegzési szolgáltatásra*, és a szolgáltatás keretében díjfizetés ellenében *Időbélyegzőket* kér a *Minősített időbélyegzés-szolgáltatótól*. Az *Előfizető* lehet természetes vagy jogi személy, egy *Előfizető* nevében akár több természetes személy is kérhet *Időbélyegzőket*.

1.3.3. Érintett felek

Érintett fél, aki ellenőrzi és felhasználja a *Minősített időbélyegzés-szolgáltató* által kibocsátott *Időbélyegzőket*. Az *Érintett fél* nem áll szerződéses kapcsolatban a *Minősített időbélyegzés-szolgáltatóval*.

1.4. Az időbélyegző felhasználhatósága

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

1.5. A dokumentum adminisztrálása

1.5.1. A dokumentum adminisztrációs szervezete

Jelen *Minősített időbélyegzési rend* adminisztrációját ellátó szervezet adatai az alábbi táblázatban találhatóak:

Szervezet neve	Microsec e-Szignó Hitelesítés Szolgáltató
Szervezet címe	Magyarország, H-1033 Budapest, Angel 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 *Minősített időbélyegzési renddel* kapcsolatos kérdésekben közvetlenül az alábbi személyhez lehet fordulni:

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

1.5.3. A Szolgáltatási szabályzat *Minősített időbélyegzési rendnek* való megfeleléséért felelős személy/szervezet

A *Minősített időbélyegzési szolgáltatási szabályzatnak* a benne meghivatkozott *Minősített időbélyegzési rendnek* való megfeleléséért és az abban foglaltak szerinti szolgáltatás nyújtásáért az adott *Minősített időbélyegzési szolgáltatási szabályzatot* kibocsátó szolgáltató a felelős.

A *Minősített időbélyegzési szolgáltatási szabályzatok* 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 *Minősített időbélyegzési rendekről* valamint az ezeket alkalmazó *Minősített időbélyegzés-szolgáltatókról*.

1.5.4. A Szolgáltatási szabályzat elfogadási eljárása

A jelen *Minősített időbélyegzési rend*nek való megfelelést kinyilatkoztató *Minősített időbélyegzési szolgáltatási szabályzat* elfogadási eljárását a *Minősített időbélyegzés-szolgáltatónak* ismertetnie kell az adott *Minősített időbélyegzési szolgáltatási szabályzatban*.

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 <i>Bizalmi szolgáltatások</i> felügyeletét ellátó hatóság a Nemzeti Média- és Hírközlési Hatóság." (2015. évi CCXXII. törvény [5] 91.§ 1. bekezdés)
Bizalmi szolgáltatás (Trust Service)	<p>"Rendszerint díjazás ellenében nyújtott, az alábbiakból álló elektronikus szolgáltatások:</p> <ul style="list-style-type: none"> • elektronikus aláírások, elektronikus bélyegzők vagy elektronikus időbélyegzők, ajánlott elektronikus kézbesítési szolgáltatások, valamint az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok létrehozása, ellenőrzése és érvényesítése; vagy • <i>Weboldal-hitelesítő tanúsítványok</i> létrehozása, ellenőrzése és érvényesítése; vagy • elektronikus aláírások, bélyegzők vagy az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok megőrzése;
Bizalmi szolgáltatási rend (Trust Service Policy)	<p>" (eIDAS [1] 3. cikk 16. pont)</p> <p>"Olyan szabálygyűjtemény, amelyben egy <i>Bizalmi szolgáltató</i>, igénybe vevő vagy más személy valamely <i>Bizalmi szolgáltatás</i> használatának feltételeit írja elő igénybe vevők valamely közös biztonsági követelményekkel rendelkező csoportja vagy meghatározott alkalmazások számára. " (2015. évi CCXXII. törvény [5] 1. § 8. pont)</p>

Bizalmi szolgáltató (Trust Service Provider)	"Egy vagy több <i>Bizalmi szolgáltató</i> st nyújtó természetes vagy jogi személy; a <i>Bizalmi szolgáltató</i> lehet minősített vagy nem minősített <i>Bizalmi szolgáltató</i> ." (eIDAS [1] 3. cikk 19. pont)
Elektronikus időbélyegző (Electronic Time Stamp)	"Olyan elektronikus adatok, amelyek más elektronikus adatokat egy adott időponthoz kötnék, 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 <i>Időbélyegző</i> elfogadója, aki az <i>Időbélyegző</i> t használja.
Gyökér tanúsítvány (Root Certificate)	Más néven legfelső szintű tanúsítvány. Önhitelesített <i>Tanúsítvány</i> , amelyet adott <i>Hitelesítő egység</i> 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 <i>Bizalmi szolgáltató</i> , aki/amely a hitelesítés-szolgáltatás keretében azonosítja az igénylő személyét, <i>Tanúsítványt</i> bocsát ki, nyilvántartásokat vezet, fogadja a <i>Tanúsítványokkal</i> kapcsolatos változások adatait, valamint nyilvánosságra hozza a <i>Tanúsítványhoz</i> tartozó szabályzatokat, és a <i>Tanúsítvány</i> aktuális állapotára (különösen esetleges visszavonására) vonatkozó információkat.
Hitelesítő egység	A <i>Hitelesítés-szolgáltató</i> rendszerének egy egysége, amely <i>Tanúsítványok</i> digitális aláírását végzi. Egy <i>Hitelesítő egység</i> hez mindig egy elektronikus aláírás vagy bélyegző létrehozásához használt adat (magánkulcs) tartozik. Előfordulhat, hogy egy <i>Hitelesítés-szolgáltató</i> egyszerre több <i>Hitelesítő egységet</i> is működtet.

Időbélyegzési rend	Olyan <i>Bizalmi szolgáltatási rend</i> , amelyben egy szolgáltató, igénybe vevő vagy más személy (szervezet) valamely <i>Időbélyegző</i> felhasználásának feltételeit írja elő az igénybe vevők valamely közös biztonsági követelményekkel rendelkező csoportja, illetőleg meghatározott alkalmazások számára.
Időbélyegzés-szolgáltató	Olyan <i>Bizalmi szolgáltató</i> , amely <i>Bizalmi szolgáltatás</i> keretében <i>Időbélyegzőket</i> bocsát ki, és ellátja az ehhez kapcsolódó feladatokat.
Időbélyegző egység	Az <i>Időbélyegzés-szolgáltató</i> rendszerének egy egysége, amely az <i>Időbélyegzők</i> aláírását vagy bélyegzését végzi. Egy időbélyegző egységhez mindig egy elektronikus aláírás vagy bélyegző létrehozáshoz használt adat tartozik. Előfordulhat, hogy egy <i>Időbélyegzés-szolgáltató</i> 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 <i>Hitelesítő egység</i> amelynek <i>Tanúsítványát</i> egy másik <i>Hitelesítő egység</i> 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 felhasználókhöz 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 <i>Alany</i> nak szigorúan titokban kell tartania. A <i>Hitelesítés-szolgáltató</i> a <i>Tanúsítványok</i> kibocsátása során a <i>Hitelesítő egység</i> magánkulcsát használja arra, hogy a <i>Tanúsítványt</i> védő elektronikus aláírást vagy bélyegzőt elhelyezze rajta.
Minősített bizalmi szolgáltatás (Qualified Trust Service)	"Olyan <i>Bizalmi szolgáltatás</i> amely megfelel az eIDAS Rendeletben foglalt alkalmazandó követelményeknek." (eIDAS [1] 3. cikk 17. pont)

Minősített bizalmi szolgáltató (Qualified Trust Service Provider)	"Olyan <i>Bizalmi szolgáltató</i> amely egy vagy több <i>Minősített bizalmi szolgáltatást</i> nyújt, és amelynek minősített státusát a felügyeleti szerv jóváhagyta. " (eIDAS [1] 3. cikk 20. pont)
Nyilvános kulcs	A Nyilvános kulcsú infrastruktúrában egy szereplőhöz tartozó aszimmetrikus kriptográfiai kulcspár azon eleme, amelyet nyilvánosságra kell hozni. A nyilvánosságra hozatal jellemzően egy <i>Tanúsítvány</i> formájában történik, amely összekapcsolja a szereplő nevét az ő nyilvános kulcsával. A <i>Tanúsítványok</i> hitelességét az őket kibocsátó <i>Hitelesítő egység</i> 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 <i>Minősített időbélyegzés-szolgáltató</i> üzemmenetében zavart okozó rendkívüli helyzet, amikor a <i>Minősített időbélyegzés-szolgáltató</i> rendes üzemmenetének folytatására ideiglenesen vagy véglegesen nincsen lehetőség.
Szervezet	Jogi személy.
Szolgáltatási szabályzat (Trust Service Practice Statement)	"A <i>Bizalmi szolgáltató</i> nyilatkozata az egyes <i>Bizalmi szolgáltatások</i> nyújtásával kapcsolatosan alkalmazott részletes eljárási vagy más működési követelményekről. " (2015. évi CCXXII. törvény [5] 1. § 41. pont)
Szolgáltatási szerződés	"A <i>Bizalmi szolgáltató</i> és a <i>Bizalmi szolgáltatási</i> ügyfél között létrejött szerződés, amely a <i>Bizalmi szolgáltatás</i> 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 <i>Weboldal-hitelesítő tanúsítvány</i> , valamint mindazon, a <i>Bizalmi szolgáltatás</i> 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 <i>Igénylő</i> által, a Szolgáltató számára a <i>Tanúsítvány</i> kibocsátás érdekében benyújtott adatok és nyilatkozatok, amelyekben többek között az <i>Igénylő</i> megerősíti a <i>Tanúsítvány</i> ba kerülő adatok valóságát.
Tanúsítványtár	Különböző <i>Tanúsítvány</i> okat tartalmazó adattár. Tanúsítványtára van egy Szolgáltatónak is, amelyben az általa kibocsátott <i>Tanúsítvány</i> okat publikálja, de Tanúsítványtárnak nevezzük az <i>Érintett fél</i> számítógépén a használt alkalmazás számára elérhető <i>Tanúsítvány</i> okat tartalmazó rendszert is.
Ügyfél	Az <i>Előfizető</i> másik elnevezése.
Visszavonás	A <i>Tanúsítvány</i> érvényességének megszüntetése a <i>Tanúsítvány</i> ban is feltüntetett érvényességi idő lejárta előtt. A <i>Tanúsítvány</i> visszavonása végleges, visszavont <i>Tanúsítvány</i> többet nem tehető érvényessé.
Visszavonási állapot nyilvántartás	A <i>Hitelesítés-szolgáltató</i> által vezetett belső nyilvántartás a felfüggesztett, illetőleg a visszavont <i>Tanúsítvány</i> 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 adattár felelőségek

2.1. Adattárak

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

A honlapon legalább 30 nappal a hatálybalépés előtt kerüljenek publikálásra a bevezetésre váró új dokumentumok.

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

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

A *Minősített időbélyegzés-szolgáltató* a szerződéskötést követően tartós adathordozón bocsássa az *Ügyfél* rendelkezésére a *Minősített időbélyegzési rendet*, a *Minősített időbélyegzési szolgáltatási szabályzatot* és a *Szolgáltatási szerződést*.

A *Minősített időbélyegzés-szolgáltató* értesítse *Ügyfeleit* az *Általános Szerződési Feltételek* változásáról.

2.2. A tanúsítványokra vonatkozó információk közzététele

A *Minősített időbélyegzés-szolgáltató* tegye közzé a honlapján a szolgáltatói *Tanúsítványait*.

2.3. A közzététel időpontja vagy gyakorisága

2.3.1. Kikötések és feltételek közzétételi gyakorisága

A szolgáltatás szempontjából leglényegesebb kikötéseket és feltételeket tartalmazza az *Ügyfél* által a szerződéskötés során aláírandó szolgáltatási szerződés, vagy az abban meghivatkozott *Általános Szerződési Feltételek* [32] dokumentum.

A *Minősített időbélyegzés-szolgáltató* évi rendszerességgel illetve rendkívüli változtatási igény esetén soron kívül átvizsgálja az *Általános Szerződési Feltételek* dokumentumot 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.

A *Minősített időbélyegzés-szolgáltató* a jóváhagyott dokumentumot legalább 30 nappal a tervezett hatálybalépés előtt véleményezésre megküldi a Nemzeti Média- és Hírközlési Hatóság részére és publikálja honlapján.

A *Minősített időbélyegzés-szolgáltató* a közzétett új Általános Szerződési Feltételek tervezettel kapcsolatos észrevételeket a hatálybalépést megelőző 14. napig fogadja az alábbi címen:

info@e-szigno.hu

Érdemi változtatást igénylő észrevétel esetén a dokumentumot megváltoztatja.

Az Általános Szerződési Feltételek észrevételekkel módosított változatát a *Minősített időbélyegzés-szolgáltató* a hatálybalépést megelőző 7. napon lezárja és közzé teszi.

3. Az Időbélyegző egység tanúsítványa és az Időbélyegzés

3.1. A felhasználó azonosítása

A *Minősített időbélyegzés-szolgáltató* az *Időbélyegzők* kibocsátását a felhasználók előzetes azonosításához kötheti. Az azonosítás módját ismertetni kell a *Minősített időbélyegzési szolgáltatási szabályzatban*.

3.2. Az Időbélyegző egység tanúsítványa

Az *Időbélyegző egység* nyilvános kulcsának sértetlenségének és hitelességének biztosítása érdekében:

- az *Időbélyegző egység* nyilvános kulcsát közzé kell tenni *Tanúsítvány* formájában;
- az *Időbélyegző egység Tanúsítványát* olyan *Hitelesítés-szolgáltatónak* kell kibocsátania, amely az ETSI EN 319 411-1 [12] szerinti szolgáltatást nyújt;
- a 910/2014/EU rendelet [1] szerinti minősített *Időbélyegzőket* kibocsátó *Időbélyegző egység Tanúsítványát* olyan *Hitelesítés-szolgáltatónak* kell kibocsátania, amely az ETSI EN 319 411-2 [13] szerinti szolgáltatást nyújt;
- az *Időbélyegző egység* csak akkor bocsáthat ki *Időbélyegzőket*, ha már rendelkezik az *Időbélyegzők* ellenőrzésére szolgáló *Tanúsítvánnyal*, és annak aláírását ellenőrizte a megbízható *Hitelesítés-szolgáltatóig* visszavezetett teljes érvényességi láncon.

3.3. Az Időbélyegző

Az *Időbélyegzőre* vonatkozó követelmények:

- az *Időbélyegző* feleljen meg az IETF RFC 3161 [24] és az ETSI EN 319 422 [19] szabványoknak;
- az *Időbélyegzőt* biztonságos körülmények között kell kibocsátani és a helyes időt kell tartalmaznia;

- az *Időbélyegző egység*(ek) *Időbélyegzők* kibocsátásához használt belső órája visszavezethető kell legyen legalább egy UTC laboratórium által szolgáltatott pontos időre;
- az *Időbélyegző*ben megadott időpont meg kell feleljen az UTC által szolgáltatott időértéknek, az eltérés nem haladhatja meg az *Időbélyegzési rendben* vagy az *Időbélyegző*ben magában megadott pontosság értékét;
- az *Időbélyegző egység* nem bocsáthat ki *Időbélyegzőt*, amint észleli hogy a belső óra pontossága a megadott mértéknél jobban eltér a UTC szerinti pontos időtől;
- az *Időbélyegzők* hitelesítésére használt magánkulcsok más célra nem használhatók;
- az *Időbélyegző egység*nek vissza kell utasítania minden *Időbélyegző* kibocsátási kérelmet a kulcsok élettartamának lejárta után.

3.3.1. Időbélyegző kérés

Az időbélyegző kliens támogassa az IETF RFC 3161 [24] 2.4.1. fejezete szerinti *Időbélyegző* kéréseket. Ajánlott az alábbi mezők támogatása:

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

A *Minősített időbélyegzés-szolgáltató* támogassa mindegyik kiterjesztés használatát.

A *Minősített időbélyegzés-szolgáltató* az ETSI TS 119 312 [20] szerinti és az aktuális Nemzeti Média- és Hírközlési Hatóság algoritmusokkal kapcsolatos határozatban kijelölt lenyomatképző algoritmusokat fogadhat be az *Időbélyegző* kérésekben. A lenyomatképző algoritmusok kiválasztásánál figyelembe kell venni az *Időbélyegző* tervezett felhasználási idejét és a lenyomatképző függvény várható megfeleléségi időtartamát.

3.3.2. Időbélyegző válasz

A *Minősített időbélyegzés-szolgáltató* támogassa az IETF RFC 3161 [24] 2.4.2. fejezete szerinti *Időbélyegző* válaszokat az alábbi kiegészítésekkel:

- kötelező az "accuracy" mező támogatása;
- ajánlott a "nonce" mező támogatása.

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

A *Minősített időbélyegzés-szolgáltató* az ETSI TS 119 312 [20] szerinti és az aktuális Nemzeti Média- és Hírközlési Hatóság algoritmusokkal kapcsolatos határozatban kijelölt kriptográfiai algoritmuskészleteket és kulcshosszakat használhat az *Időbélyegzők* aláírására. A kriptográfiai algoritmuskészletek és kulcshosszak kiválasztásánál figyelembe kell venni az *Időbélyegző* tervezett felhasználási idejét.

3.4. Az Időbélyegzőben szereplő idő pontossága

A kibocsátott *Időbélyegző*ekben szereplő idő pontossága 1 másodpercen belül kell legyen.

- az *Időbélyegző egység* óráját védeni kell az olyan fenyegetéstől, amely lehetővé tenné az óra észrevétlen átállítását a vállalt pontossági tartományon kívüli értékre;
- a *Minősített időbélyegzés-szolgáltató*nak észlelnie kell, ha az *Időbélyegző*be írandó belső idő a vállalt pontossági tartományon kívül esik;
- amint a *Minősített időbélyegzés-szolgáltató* észleli, hogy az *Időbélyegző*be írandó belső idő a vállalt pontossági tartományon kívül esik, szüneteltetnie kell az *Időbélyegző* kibocsátását;

3.5. Óraszinkronizálás

Az *Időbélyegző egység* óráját a vállalt pontosságon belül szinkronizálni kell az UTC időhöz. Az *Időbélyegző egység* órájának kalibrációját úgy kell végezni, hogy az óra ne csúszhasson ki a vállalt pontosságból.

3.5.1. A szökőmásodpercek kezelése

A *Minősített időbélyegzés-szolgáltató*nak el kell végeznie az óraszinkronizációt az illetékes szervezet értesítése alapján szökőmásodperc előfordulásakor. A változtatást a kitűzött nap utolsó percében kell végrehajtani az ETSI 319 421 [18] C függelékében meghatározottak szerint az ITU-R TF.460-6 [29] ajánlásnak megfelelően.

3.5.2. Nyári időszámítás kezelése

Az *Időbélyegző*ekben UTC formában megadott időpontot az egyes alkalmazások eltérő módon és formátumban jeleníthetik meg a felhasználó részére, gyakran helyi időt használva. A megjelenítés ilyen módja félreértésekre adhat okot az *Érintett felek*nek különböző időzónákban, illetve a nyári időszámítás idején, különösen a tavaszi és őszi óraátállítás környékén.

A jelzett időpont értelmezésével kapcsolatos lehetséges problémákra a *Minősített időbélyegzési szolgáltatási szabályzat*ban fel kell hívni az *Érintett felek* figyelmét.

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 *Minősített időbélyegzés-szolgáltató Tanúsítványával*;
- 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-szolgáltató* felelősségvállalás megfelelő.

3.7. A szolgáltatás rendelkezésre állása

A *Minősített időbélyegzés-szolgáltató*nak biztosítania kell a szolgáltatás, valamint a *Minősített időbélyegzés-szolgáltató* által kibocsátott *Időbélyegzők* használatára vonatkozó kikötések és feltételek folyamatos elérhetőségét éves szinten legalább 99.9% -os rendelkezésre állás mellett, ahol az eseti szolgáltatáskiesések időtartama legfeljebb 3 óra.

3.8. Nem minősített időbélyegzők kibocsátása

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

A külön *Időbélyegző egység* nem feltétlenül jelent különálló hardvert és szoftvert, de a különféle biztonsági szintű szolgáltatások elkülönítéséhez legalább:

- külön magánkulcsot és *Tanúsítványt* kell használni;
- különböző hozzáférési pontokat kell biztosítani.

3.9. Az Időbélyegző egység kulcshasználata

Az *Időbélyegző egységekben* be kell tartani az alábbi követelményeket:

- csak olyan algoritmusokat és kulcsméreteket használhatnak az *Időbélyegzők* hitelesítésére, amelyek megfelelnek az alábbi követelményeknek:
 - ETSI TS 119 312 [20];
 - 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* eszközbe;
- amennyiben több *HSM* eszköz is ugyanazt az aláíró vagy bélyegző létrehozó magánkulcsot használja, akkor azoknak ugyanahhoz a *Tanúsítványhoz* kell tartozniuk;
- egy *Időbélyegző egységben* egyidőben csak egy *Időbélyegző* aláíró vagy bélyegző létrehozó magánkulcs lehet aktív;
- egy hardver-szoftver egység több különböző *Időbélyegző egységet* is kiszolgálhat a fenti követelmények betartása esetén.

3.10. Az Időbélyegző szolgáltatás elérési módjai

A szolgáltatás kizárólag a biztonságos HTTPS protokollon keresztül vehető igénybe. A biztonságos csatorna a *Előfizető* azonosítási módjától függően az alábbi módon épül fel:

- felhasználónév és jelszó alapú azonosítás esetén az *Időbélyegző egység Tanúsítványa* alapján.
- autentikációs *Tanúsítvány* alapú felhasználó azonosítás esetén a kliens és a szerver *Tanúsítványok* kölcsönös azonosítása alapján.

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 *Időbélyegzők* hitelesítésére használható, a magánkulcs más célú felhasználása tilos.

4.1.2. Az Érintett felek nyilvános kulcs és tanúsítvány használata

A *Tanúsítvány* használata során a *Minősített időbélyegzés-szolgáltató* által garantált biztonsági szint megtartásához ajánlott, hogy az *Érintett fél* megfelelő körültekintéssel járjon el, és feleljen meg a *Minősített időbélyegzési szolgáltatási szabályzatban* leírt követelményeknek, különös tekintettel az alábbiakra:

- ellenőrizze a *Tanúsítvány* érvényességét és visszavonási állapotát;
- vegyen figyelembe minden korlátozást, amely a *Tanúsítványban* vagy a *Tanúsítványban* meghivatkozott szabályzatokban szerepel.

5. Elhelyezési, eljárásbeli és üzemeltetési előírások

A *Minősített időbélyegzés-szolgáltatónak* széles körben elismert szabványoknak megfelelő fizikai, eljárásbeli és személyzeti biztonsági óvintézkedéseket, valamint az ezeket érvényre juttató adminisztratív és irányítási eljárásokat kell alkalmaznia.

A *Minősített időbélyegzés-szolgáltató* vezessen nyilvántartást a szolgáltatás nyújtásával kapcsolatos rendszerelemekről és erőforrásokról, és végezzen ezekkel kapcsolatos kockázatelemzést. Az egyes elemekkel kapcsolatban alkalmazzon a kockázatokkal arányos védelmi megoldásokat.

A *Minősített időbélyegzés-szolgáltatónak* figyelemmel kell kísérnie a kapacitás igényeket és biztosítania kell, hogy megfelelő feldolgozási teljesítmény és tárolási kapacitás álljon rendelkezésre a szolgáltatás nyújtásához.

5.1. Fizikai követelmények

A *Minősített időbélyegzés-szolgáltatónak* gondoskodnia kell arról, hogy a kritikus szolgáltatásokhoz történő fizikai hozzáférés ellenőrzött legyen és a kritikus szolgáltatások eszközeit érintő fizikai kockázatát minimalizálja.

A fizikai óvintézkedések célja a *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 kell megvalósítani.

A biztosított védelem mértéke legyen megfelelő a *Minősített időbélyegzés-szolgáltató* által végzett kockázatelemzésben megállapított fenyegetettség mértékének.

5.1.1. A telephely elhelyezése és szerkezeti felépítése

A *Minősített időbélyegzés-szolgáltató* informatikai rendszereit fizikai és logikai védelemmel ellátott, megfelelően biztonságos *Adatközpont*ban kell elhelyezni és üzemeltetni, amely megakadályozza az illetéktelen hozzáférést. Az *Adatközpont* elhelyezése és kialakítása során egymásra épülő és egymást támogató védelmi megoldásokat kell alkalmazni – mint pl. őrzés, biztonsági zárok, 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 *Minősített időbélyegzés-szolgáltatónak* védenie kell a szolgáltatás nyújtásában részt vevő eszközeit és berendezéseit a jogosulatlan fizikai hozzáféréstől az eszközök manipulálásának megakadályozása érdekében. A *Minősített időbélyegzés-szolgáltatónak* biztosítania kell, hogy:

- az *Adatközpont*ba történő minden belépés regisztrálásra kerül;
- az *Adatközpont*ba csak két – bizalmi szerepkört betöltő, erre feljogosított – munkatárs egyidejű azonosítása után lehet belépni, legalább az egyik munkatársnak rendszeradminisztrátornak kell lennie;
- 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 gépterem belül sem tárolhatók nyílt formában.

Jogosulatlan személyek jelenlétében:

- a bizalmas adatokat tartalmazó adathordozókat fizikailag elzárva kell tartani;
- a bejelentkezett terminálokat nem szabad felügyelet nélkül hagyni;
- nem szabad olyan munkafolyamatot végezni, 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 fizikai biztonsági vizsgálatok rendszeres elvégzésére felelősöket kell kijelölni. A vizsgálatok eredményét megfelelő naplóbejegyzésekben kell rögzíteni.

5.1.3. Áramellátás és légkondicionálás

A *Minősített időbélyegzés-szolgáltató Adatközpont*ban olyan szünetmentes áramellátó rendszert kell alkalmazni, 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 szűrőrendszerrel kell biztosítani, amely kiszűri a levegőből a különféle szennyeződések (por, szennyező anyagok, korrozív anyagok, mérgező vagy gyúlékony anyagok). A szellőző rendszernek megfelelő szűrés mellett biztosítani kell az operátorok biztonságos munkavégzéséhez szükséges mennyiségű friss levegőt.

A levegő nedvességtartalmát az informatikai rendszerek által megkívánt szintre kell csökkenteni.

Megfelelő teljesítményű hűtőrendszert kell használni a szükséges üzemi hőmérséklet biztosítása, az informatikai eszközök túlhevülésének megakadályozása érdekében.

5.1.4. Beázás és elárasztódás veszély kezelése

A *Minősített időbélyegzés-szolgáltató Adatközpont*ját megfelelően védeni kell a vízbetöréstől és az elárasztódástól.

5.1.5. Tűz megelőzés és tűzvédelem

A *Minősített időbélyegzés-szolgáltató Adatközpont*ját füst- és tűzérzékelőkkel kell felszerelni, amelyek automatikusan riasztják a tűzoltóságot. Minden helyiségben jól látható helyen el kell helyezni a vonatkozó előírásoknak megfelelő típusú és mennyiségű kézi tűzoltó készüléket.

A gépteremben automatikus tűzoltó rendszert kell alkalmazni.

5.1.6. Adathordozók tárolása

A *Minősített időbélyegzés-szolgáltató*nak védenie kell valamennyi adathordozóját a jogosulatlan hozzáféréstől és a véletlen rongálódástól. Valamennyi napló és archív adatot duplikáltan kell létrehozni. A két példányt egymástól fizikailag elkülönítve kell tárolni, egymástól biztonságos távolságra lévő helyszíneken. A tárolt adathordozókat védeni kell a káros környezeti behatásoktól, mint pl. alacsony vagy magas hőmérséklet, szennyeződés, nedvesség, napfény, erős mágneses tér, erős sugárzás.

5.1.7. Hulladék megsemmisítése

A *Minősített időbélyegzés-szolgáltató*nak a környezetvédelmi előírások betartásával kell gondoskodnia feleslegessé vált eszközeinek, adathordozóinak megsemmisítéséről.

Az ilyen eszközöket, adathordozókat a *Minősített időbélyegzés-szolgáltató* alkalmazottainak személyes felügyelete alatt, a széleskörűen elfogadott módszereknek megfelelően kell véglegesen törölni vagy használhatatlanná tenni.

5.1.8. A mentési példányok fizikai elkülönítése

A *Minősített időbélyegzés-szolgáltató*nak legalább heti rendszerességgel elő kell állítania olyan mentést, amiből meghibásodás esetén a teljes szolgáltatás helyreállítható. A mentéseket - legalább az utolsó teljes mentést is beleértve - egy olyan külső helyszínen kell tárolni, amelynek a fizikai és működési védelme azonos az elsődleges helyszínével. Az elsődleges és a tartalék helyszínek között meg kell oldani az adatok biztonságos továbbítását.

A mentett állományokból legalább évente szűrőpróbaszerű kiválasztással jegyzőkönyvezett helyreállítási tesztet kell végezni.

5.2. Eljárásbeli előírások

A *Minősített időbélyegzés-szolgáltató*nak gondoskodnia kell 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 *Minősített időbélyegzés-szolgáltató* belső irányítási rendszere biztosítsa a jogszabályoknak és belső szabályzatainak megfelelő működést. Rendszerében minden rendszerelemhez és minden folyamathoz legyen egyértelműen hozzárendelhető az adott rendszerelemért, vagy folyamatért felelős személy. A *Minősített időbélyegzés-szolgáltató* rendszerében élesen különüljenek el egymástól a fejlesztési és üzemeltetési folyamatok. A rendszer megfelelő működését a független rendszervizsgáló és a *Minősített időbélyegzés-szolgáltató* belső folyamatainak rendszeres ellenőrzése biztosítsa.

5.2.1. Bizalmi szerepkörök

A *Minősített időbélyegzés-szolgáltató*nak feladatai ellátásához bizalmi szerepköröket kell létrehoznia. A jogosultságokat és funkciókat oly módon kell megosztani az egyes bizalmi szerepkörök között, hogy egyedül egyetlen felhasználó se legyen képes a biztonsági védelmi intézkedések megkerülésére.

A megvalósítandó bizalmi szerepkörök:

- a szolgáltató informatikai rendszeréért általánosan felelős vezető;
- biztonsági tisztviselő: a szolgáltatás biztonságáért általánosan felelős személy;

- rendszeradminisztrátor: az informatikai rendszer telepítését, konfigurálását, karbantartását végző személy;
- rendszerüzemeltető: az informatikai rendszer folyamatos üzemeltetését, mentését és helyreállítását végző személy;
- független rendszervizsgáló: a szolgáltató naplózott, illetve archivált adatállományát vizsgáló, a 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 *Minősített időbélyegzés-szolgáltató* biztonságért felelős vezetőjének formálisan ki kell nevezni a *Minősített időbélyegzés-szolgáltató* munkatársait.

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

A bizalmi szerepkörökről naprakész nyilvántartást kell vezetni, amit változás esetén haladéktalanul be kell jelenteni a Nemzeti Média- és Hírközlési Hatóságnak.

5.2.2. Az egyes feladatok ellátásához szükséges személyzeti létszámok

A *Minősített időbélyegzés-szolgáltató* biztonsági és üzemeltetési szabályzataiban elő kell írni, hogy csak védett környezetben, kettő, bizalmi szerepkört betöltő munkatárs egyidejű fizikai jelenlétében végezhetők el az alábbi műveletek:

- a *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 *Minősített időbélyegzés-szolgáltató* informatikai rendszerét kezelő felhasználóknak egyedi azonosító adatokkal kell rendelkezniük, 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 adatokat a felhasználói jogosultságok megszűnésekor haladéktalanul vissza kell vonni.

5.2.4. Egymást kizáró szerepkörök

A *Minősített időbélyegzés-szolgáltató* munkatársai egyidejűleg több bizalmi szerepkört is betölthetnek, de a *Minősített időbélyegzés-szolgáltató* köteles biztosítani, 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.

5.3. Személyzetre vonatkozó előírások

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

A *Minősített időbélyegzés-szolgáltató* már a felvételi szakaszban foglalkozzon 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 *Minősített időbélyegzés-szolgáltató* szolgáltatásaival kapcsolatba kerül – titoktartási nyilatkozatot kell aláírnia.

A *Minősített időbélyegzés-szolgáltató* egyúttal biztosítsa 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

A *Minősített időbélyegzés-szolgáltató* valamennyi dolgozójának rendelkeznie kell a munkaköre ellátásához szükséges végzettséggel, gyakorlattal és szakmai tapasztalattal. Már a munkaerő felvétel során a leendő dolgozók kiválasztásánál különös hangsúlyt kell fektetni a személyiségi jegyekre, csak megbízható személyek vehetők fel a bizalmi szerepkörbe.

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

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

- szakirányú felsőfokú végzettséggel (matematikus, fizikus 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 *Minősített időbélyegzés-szolgáltató* vezető munkakörben illetve bizalmi szerepkörben csak olyan alkalmazottakat foglalkoztathat, 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 *Minősített időbélyegzés-szolgáltató* vezető munkakört betöltő alkalmazottjának nyilatkozatával, bizalmi szerepkört betöltő alkalmazottjának 3 hónapnál nem régebbi erkölcsi bizonyítvánnyal kell igazolnia büntetlen előéletét.

A *Minősített időbélyegzés-szolgáltató*nak a felvételi eljárás során ellenőriznie kell a jelentkező önéletrajzában megadott releváns információk valóságát, úgy mint előző munkahely, szakmai referenciák, legfontosabb képzettség.

5.3.3. Képzési követelmények

A *Minősített időbélyegzés-szolgáltató* az újonnan felvett alkalmazottakat ki kell képezze, amely során elsajátítják az adott munkakör ellátásához szükséges mértékben:

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

A *Minősített időbélyegzés-szolgáltató* éles informatikai rendszereihez csak a képzést sikeresen teljesítő alkalmazottak kaphatnak hozzáférési jogosultságot.

5.3.4. Továbbképzési gyakoriságok és követelmények

A *Minősített időbélyegzés-szolgáltató*nak gondoskodnia kell róla, hogy az alkalmazottak folyamatosan a megfelelő tudással rendelkezzenek, így szükség esetén továbbképzést, vagy ismétlődő jellegű képzést kell tartani.

Továbbképzést kell tartani, ha a *Minősített időbélyegzés-szolgáltató* folyamataiban vagy informatikai rendszerében változás áll be.

A képzési anyagot legalább 12 havonta felül kell vizsgálni, és tartalmaznia kell az új fenyegetéseket és biztonsági megoldásokat.

A továbbképzést megfelelően dokumentálni kell, amelyből egyértelműen megállapítható a továbbképzés tematikája és a résztvevő dolgozók köre.

5.3.5. Munkabeosztás körforgásának sorrendje és gyakorisága

Nincs előírás.

5.3.6. Felhatalmazás nélküli tevékenységek büntető következményei

A *Minősített időbélyegzés-szolgáltató*nak a dolgozókkal kötendő munkaszerződésben kell szabályoznia a dolgozók felelősségre vonásának lehetőségeit a dolgozó által elkövetett mulasztások, hibák, véltlen vagy szándékos károkozások esetére. Amennyiben egy munkatárs – szándékosan vagy gondatlanul – kötelezettségeit megsérti, vele szemben a *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.

5.3.7. Szerződéses viszonyban foglalkoztatottakra vonatkozó követelmények

A *Minősített időbélyegzés-szolgáltató* által szerződéses viszonyban foglalkoztatott dolgozókra ugyanolyan szabályokat kell alkalmazni, mint a munkavállalókra.

A bizalmi szerepkört betöltő személynek munkaviszonyban kell állnia a *Minősített időbélyegzés-szolgáltató*val.

5.3.8. A személyzet számára biztosított dokumentációk

A *Minősített időbélyegzés-szolgáltató*nak folyamatosan biztosítania kell a dolgozók részére a szerepkörük ellátásához szükséges aktuális dokumentációk, szabályzatok rendelkezésre állását.

5.4. Naplózási eljárások

A *Minősített időbélyegzés-szolgáltató*nak a biztonságos informatikai környezet fenntartása érdekében a teljes informatikai rendszerét átfogó eseménynaplózó és ellenőrző rendszert kell megvalósítania és üzemeltetnie.

5.4.1. A tárolt események típusai

A *Minősített időbélyegzés-szolgáltató*nak az általánosan elfogadott informatikai biztonsági gyakorlatnak megfelelően naplózni kell minden olyan biztonsággal kapcsolatos eseményt, amely információt szolgáltat az informatikai rendszerben vagy annak fizikai környezetében történt eseményekről, változásokról. Minden naplóbejegyzésnél el kell tárolni:

- az esemény időpontját;

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

Az elmentett naplóbejegyzések nem kerülhetnek módosításra vagy törlésre.

Az összes lényeges naplóbejegyzést elérhetővé kell tenni a független rendszervizsgálók részére, akik a *Minősített időbélyegzés-szolgáltató* működésének megfelelőségét vizsgálják.

Naplózni kell minimálisan az alábbi eseményeket:

- BELSŐ ÓRA
 - a belső óra szinkronizációja az UTC időhöz, beleértve az üzemserű újrakalibrálásokat is;
 - a szinkronizáció elvesztése;
- IDŐBÉLYEGZÉS
 - az *Időbélyegzők* kibocsátásával kapcsolatos események;
- 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, elmentés, betöltés, megsemmisítés stb.);
- TANÚSÍTVÁNY KEZELÉS
 - az *Időbélyegző egységek Tanúsítványainak* 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* eszköz
 - *HSM* eszköz installálása;
 - *HSM* eszköz eltávolítása;
 - *HSM* eszköz selejtezése, megsemmisítése;
 - *HSM* eszköz szállítása;
 - *HSM* eszköz tartalmának törlése (nullázás);
 - *HSM* eszköz feltöltése kulcsokkal, tanúsítványokkal;
- KONFIGURÁCIÓ VÁLTOZÁSA
 - hardver;
 - szoftver;
 - operációs rendszer;
 - javító csomag;
- FIZIKAI HOZZÁFÉRÉS, TELEPHELY BIZTONSÁG
 - személy belépése a bizalmi szolgáltatást nyújtó rendszer komponenseket tartalmazó biztonsági területre és onnan kilépése;
 - hozzáférés egy bizalmi szolgáltatást nyújtó rendszer komponenshez;
 - a fizikai biztonság ismert vagy gyanított megsértése;
 - tűzfal és router forgalmak;
- MŰKÖDÉSI RENDELLENESÉGEK
 - 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 *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 *Minősített időbélyegzés-szolgáltató*nak biztosítania kell a keletkezett naplóállományok rendszeres kiértékelését.

A keletkezett napi naplóállományokat lehetőség szerint a következő munkanapon, de legkésőbb 1 héten belül ki kell értékelni.

A naplóállományok kiértékelését csak a megfelelő szakértelemmel, jogosultságokkal és kinevezéssel rendelkező független rendszervizsgáló végezheti el.

A *Minősített időbélyegzés-szolgáltató* használhat automatizált eszközöket az elektronikus naplóállományok kiértékelésének segítésére. Az automata figyelő rendszerből kapott értesítéseket 24 órán belül fel kell dolgozni és ki kell értékelni.

A kiértékelés során meg kell győződni a vizsgált naplóállományok hitelességéről és sértetlenségéről.

A kiértékelés során elemezni kell a rendszerek által generált hibaüzeneteket.

Statisztikai módszerekkel elemezni kell a forgalmi adatokban bekövetkezett jelentős változásokat.

A vizsgálat tényét, a vizsgálat eredményeit és az esetleges feltárt hiányosságok elhárítása érdekében meghozott intézkedéseket megfelelően dokumentálni kell.

5.4.3. A naplófájl megőrzési időtartama

Az online rendszerből való kitörlés előtt a naplóállományokat archiválni kell és gondoskodni kell azok biztonságos megőrzéséről az 5.5.2 fejezetben meghatározott ideig, de legalább a keletkezésüktől számított 10 évig.

5.4.4. A naplófájl védelme

A *Minősített időbélyegzés-szolgáltató*nak meg kell védenie a keletkezett naplóállományokat az előírt megőrzési ideig. A megőrzési idő teljes időtartama alatt biztosítania kell a naplóadatokat:

- védelmét az illetéktelen felfedés ellen: a naplóállományokhoz csak az arra jogosultak – elsősorban a független rendszervizsgálók – férhessenek hozzá;
- rendelkezésre állását: a jogosultak számára biztosítani kell a naplóállományokhoz való hozzáférést;
- integritását: meg kell akadályozni a naplóállományokban bármilyen adat módosítását, törlését, bejegyzések sorrendjének megváltoztatását stb.

5.4.5. A naplófájl mentési eljárásai

Az üzemeltetés során az egyes rendszerekben folyamatosan keletkező naplóbejegyzésekből napi naplóállományokat kell előállítani.

A napi naplóállományokat a kiértékelés után 2 példányban archiválni kell és a példányokat egymástól fizikailag elkülönülő helyszíneken az előírt ideig meg kell őrizni.

A mentések pontos menetét a *Minősített időbélyegzési szolgáltatási szabályzat*ban elő kell írni.

5.4.6. A naplózás adatgyűjtési rendszere

A *Minősített időbélyegzés-szolgáltató* a *Minősített időbélyegzési szolgáltatási szabályzat*ában írja elő a naplózási folyamatainak működését.

A *Minősített időbélyegzés-szolgáltató* használhat automatikus vizsgáló és naplózó rendszereket is, amennyiben biztosítani tudja, hogy azok a rendszer indításakor már aktívak és a rendszer leállásáig folyamatosan működnek.

Amennyiben az automatikus vizsgáló és naplózó rendszerek működésében bármilyen rendellenesség lép fel, a *Minősített időbélyegzés-szolgáltató* működését fel kell függeszteni az üzemzavar elhárításáig.

5.4.7. Az eseményeket kiváltó alanyok értesítése

A feltárt hiba esetén a *Minősített időbélyegzés-szolgáltató* saját hatáskörében dönthet, hogy értesíti-e a hibáról az azt kiváltó személyt, szerepkört, eszközt vagy alkalmazást.

5.4.8. Sebezhetőség felmérése

A *Minősített időbélyegzés-szolgáltatónak* évente sebezhetőség vizsgálatot kell végeznie, amely segítségével feltérképezi a potenciális belső és külső fenyegetettségeket, amelyek jogosulatlan hozzáféréseket eredményezhetnek.

Fel kell térképezni továbbá az egyes fenyegetettségek bekövetkezésének valószínűségét és a bekövetkezés esetén várható kárt is.

Rendszeresen értékelnie kell az alkalmazott folyamatokat, védelmi intézkedéseket, informatikai rendszereket, hogy azok megfelelően képesek-e ellenállni a feltárt fenyegetettségeknek.

A feltárt hibák kiértékelése után szükség szerint módosítani kell a védelmi rendszereken, hogy a hasonló hibák a jövőben megakadályozhatók legyenek.

5.5. Adatok archiválása

5.5.1. Az archivált adatok típusai

A *Minősített időbélyegzés-szolgáltatónak* fel kell készülnie elektronikus és papíralapú dokumentumok megfelelően biztonságos, hosszú idejű archiválására.

A *Minősített időbélyegzés-szolgáltatónak* az alábbi jellegű információt kell archiválnia:

- a *Minősített időbélyegzés-szolgáltató* akkreditációjával kapcsolatos valamennyi irat;

- a *Minősített időbélyegzési rend*(ek) valamennyi kibocsátott verziója;
- a *Minősített időbélyegzési szolgáltatási szabályzat*(ok) valamennyi kibocsátott verziója;
- az Általános Szerződési Feltételek valamennyi kibocsátott verziója;
- a *Minősített időbélyegzés-szolgáltató* működésével kapcsolatos szerződések;
- valamennyi elektronikus és papíralapú naplóbejegyzés.

5.5.2. Az archívum megőrzési időtartama

A *Minősített időbélyegzés-szolgáltató* az archivált adatokat az alábbi időtartamokig köteles megőrizni:

- a *Minősített időbélyegzési rendet* a hatályon kívül helyezéstől számított legalább 10 évig;
- a *Minősített időbélyegzési szolgáltatási szabályzatot* a hatályon kívül helyezéstől számított legalább 10 évig;
- Általános Szerződési Feltételeket a hatályon kívül helyezéstől számított legalább 10 évig;
- az *Időbélyegző* kibocsátásával kapcsolatos főbb adatokat a kibocsátástól számított legalább 10 évig;
- minden egyéb archiválandó dokumentomot a keletkezésétől számított legalább 10 évig.

5.5.3. Az archívum védelme

A *Minősített időbélyegzés-szolgáltató* köteles valamennyi archivált adatot két példányban, két egymástól fizikailag elkülönült helyszínen őrizni. Az egyetlen hiteles példányban rendelkezésre álló papíralapú dokumentumról hiteles papíralapú, vagy elektronikus másolat készíthető a vonatkozó jogszabályok betartásával.

A két helyszínen mindegyikének teljesítenie kell az archiválással szemben támasztott biztonsági és egyéb követelményeket.

Az archivált adatok megőrzése során gondoskodni kell 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 kell ellátni.

5.5.4. Az archívum mentési folyamatai

Az archivált adatok másodpéldányát a *Minősített időbélyegzés-szolgáltató* telephelyétől fizikailag eltérő helyszínen kell tárolni az 5.1.8 fejezet előírásainak megfelelően.

5.5.5. Az adatok időbélyegzésére vonatkozó követelmények

Valamennyi elektronikus naplóbejegyzést el kell látni időjellel, amelyen legalább másodperc pontossággal fel van tüntetve a rendszer által szolgáltatott időpont.

A *Minősített időbélyegzés-szolgáltató*nak biztosítania kell, hogy a szolgáltatást nyújtó rendszerein a gépidő maximum 1 másodpercre térjen el a referenciaidőtől. Az időjel előállításához használt gépidőt naponta legalább egy alkalommal szinkronizálni kell az UTC időhöz.

A napi naplóállományokat minősített *Időbélyegző*vel kell ellátni.

Az archivált adatok megőrzése során szükség esetén (pl. algoritmusváltás, az eredeti *Időbélyegző* érvényességének lejáratát) gondoskodni kell az adatok hitelességének megőrzéséről.

5.5.6. Az archívum gyűjtési rendszere

A *Minősített időbélyegzés-szolgáltató* védett informatikai rendszerén belül kell keletkeznie a naplóbejegyzéseknek, onnan csak az elektronikusan aláírt, minősített *Időbélyegző*vel védett naplóállományok kerülhetnek ki.

5.5.7. Archív információk hozzáférését és ellenőrzését végző eljárások

A *Minősített időbélyegzés-szolgáltató* a naplóállományok előállítását manuálisan vagy automatikusan is elvégezheti. Automatikus naplózó rendszer alkalmazása esetén a hitelesített naplóállományokat naponta kell előállítani.

Az archivált adatállományokat védeni kell a jogosulatlan hozzáféréstől.

Az arra jogosultaknak biztosítani kell az archivált adatokhoz való ellenőrzött hozzáférést:

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

5.6. Szolgáltatói kulcs cseréje

A *Minősített időbélyegzés-szolgáltató* gondoskodjon arról, hogy az általa üzemeltetett *Időbélyegző* egységek folyamatosan rendelkezzenek a működéshez szükséges érvényes kulccsal és Tanúsítvánnyal. Ennek érdekében a *Tanúsítványuk* lejáratá illetve a hozzájuk kapcsolódó kulcsok használati idejének lejáratá előtt elegendő idővel generáljon új kulcspárt az *Időbélyegző* egység számára, és arról időben értesítse *Ügyfeleit*. Az új szolgáltatói kulcsot a jelen szabályzatnak megfelelően kell generálni és kezelni.

Amennyiben a *Minősített időbélyegzés-szolgáltató* megváltoztatja az *Időbélyegző*ket kibocsátó bármely szolgáltatói *Tanúsítványának* kulcsait, be kell tartania az alábbi előírásokat:

- publikálnia kell az érintett *Tanúsítványait* 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 írhatja alá;
- meg kell őriznie a régi szolgáltatói *Tanúsítvány*okat és nyilvános kulcsokat.

5.7. Kompromittálódást és katasztrófát követő helyreállítás

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

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

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

5.7.1. Váratlan esemény és kompromittálódás kezelési eljárások

A *Minősített időbélyegzés-szolgáltató*nak rendelkeznie kell üzletmenet folytonossági tervvel. Az üzletmenet folytonossági tervnek tartalmaznia kell 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 *Minősített időbélyegzés-szolgáltató*nak közzé kell tennie az eseménnyel kapcsolatos információt valamint nem adhat ki *Időbélyegző*ket a veszélyhelyzet elhárításáig.

Kompromittálódás, kompromittálódás gyanúja vagy az *Időbélyegző egység* órájának elállítódása esetén a *Minősített időbélyegzés-szolgáltató*nak közzé kell tennie az érintett *Időbélyegző*k beazonosításához szükséges információkat. A *Minősített időbélyegzés-szolgáltató*nak ki kell alakítania és fenn kell tartania egy teljes értékű tartalékrendszert, amely az elsődleges helyszíntől biztonságos távolságra, földrajzilag különböző helyszínen található és önállóan is alkalmas a szolgáltatások teljes körű ellátására.

A *Minősített időbélyegzés-szolgáltató*nak rendszeresen tesztelnie kell a tartalékrendszer működését és évente felül kell vizsgálnia az üzletmenet folytonossági terveit.

Katasztrófa esetén a lehető legrövidebb időn belül helyre kell állítani a szolgáltatások elérhetőségét.

5.7.2. Meghibásodott IT erőforrások, szoftverek és/vagy adatok

A *Minősített időbélyegzés-szolgáltató* informatikai rendszereit megbízható hardver és szoftver komponensekből kell felépíteni. A kritikus funkciókat redundáns rendszerelemek alkalmazásával kell megvalósítani úgy, hogy azok egy elem meghibásodása esetén is képesek legyenek a további működésre.

A *Minősített időbélyegzés-szolgáltató* naponta készítsen teljes mentést az adatbázisairól és a keletkezett naplózási eseményekről.

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

A *Minősített időbélyegzés-szolgáltató* üzletmenet folytonossági terve tartalmazzon pontos előírásokat a kritikus rendszerkomponensek meghibásodásának esetén végrehajtandó feladatokra. A *Minősített időbélyegzés-szolgáltató* a hiba elhárítása és a rendszer integritásának helyreállítása után a lehető leghamarabb indítsa újra a szolgáltatásait.

5.7.3. Magánkulcs kompromittálódása esetén követendő eljárások

A *Minősített időbélyegzés-szolgáltató* magánkulcsának kompromittálódása vagy a kompromittálódás gyanúja esetén haladéktalanul meg kell tenni az alábbi lépéseket:

- vissza kell vonni a *Minősített időbélyegzés-szolgáltató* összes érintett *Tanúsítványát*;
- új szolgáltatói magánkulcsokat kell generálni a szolgáltatások helyreállításához;
- nyilvánosságra kell hozni a visszavont szolgáltatói *Tanúsítványok* adatait a 2.2 fejezetben szabályozott módon;
- a kompromittálódással kapcsolatos információt elérhetővé kell tenni valamennyi *Előfizető* és *Érintett fél* részére;
- súlyos kompromittálódás esetén az *Előfizetők* és *Érintett felek* részére elérhetővé kell tenni azt az információt, amiből egyértelműen meg lehet határozni az érintett *Időbélyegzők* körét.

5.7.4. Működés folyamatosságának biztosítása katasztrófát követően

A *Minősített időbélyegzés-szolgáltató* üzletmenet folytonossági tervében meg kell határozni a természeti vagy egyéb katasztrófa miatt bekövetkezett szolgáltatás leállás esetén végrehajtandó feladatokat.

A katasztrófa bekövetkezése esetén haladéktalanul életbe kell léptetni a rendelkezéseket és meg kell kezdeni a károk elhárítását, a szolgáltatások helyreállítását.

A másodlagos szolgáltatói helyszínt az elsődleges telephelytől olyan távol kell elhelyezni, hogy egy valószínűsíthető katasztrófa ne érhesse mindkét helyszínt egyszerre.

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

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

5.8. Az Időbélyegzés-szolgáltató leállítása

A *Minősített időbélyegzés-szolgáltatónak* a szolgáltatás megszüntetésekor teljesítenie kell a jogszabályokban megfogalmazott követelményeket.

A leállítás során kiemelten kezelendő feladatok:

- a tervezett leállásról időben értesíteni kell az *Érintett feleket* és az *Előfizetőket*;

- a *Minősített időbélyegzés-szolgáltató* tegyen meg mindent annak érdekében, hogy legkésőbb a szolgáltatás leállításáig egy másik szolgáltató átvegye nyilvántartásait és szolgáltatási kötelezettségeit;
- be kell szüntetni az új *Időbélyegzők* kiadását;
- vissza kell vonni a szolgáltatói *Tanúsítványokat* és meg kell semmisíteni a szolgáltatói magánkulcsokat;
- a szolgáltatás megszüntetése után egy teljes rendszermentést és archiválást kell végeznie;
- át kell adni az archivált adatokat a szolgáltatást átvállaló szolgáltatónak vagy a Nemzeti Média- és Hírközlési Hatóságnak.

6. Műszaki biztonsági óvintézkedések

A *Minősített időbélyegzés-szolgáltató*nak módosítás ellen védett, megbízható rendszereket és termékeket kell használnia a kriptográfiai kulcsok és aktivizáló adataik kezelésére a teljes életciklus alatt.

Folyamatosan nyomon kell követni a kapacitás igényeket és becsülni kell a jövőbeni várható kapacitást, hogy biztosítani lehessen a szükséges feldolgozási és tárolási igények rendelkezésre állását.

6.1. Kulcspár előállítása és telepítése

A *Minősített időbélyegzés-szolgáltató*nak gondoskodnia kell az általa generált valamennyi magánkulcs biztonságos, az ipari szabványoknak és a hatályos jogszabályi előírásoknak megfelelő előállításáról és kezeléséről.

6.1.1. Kulcspár előállítása

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

- ETSI TS 119 312 [20];
- 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 biztosítsa, 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 [23] követelményeinek,
 - vagy megfelel a FIPS 140-2 [30] 3-as, illetve annál magasabb szintű követelményeinek,
 - vagy megfelel a CEN 419 221-5 [21] követelményeinek,
 - vagy olyan megbízható rendszer, amely az MSZ/ISO/IEC 15408 [22] 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 előírányzaton kell alapulnia.
- A szolgáltatói magánkulcs előállítását egy kulcsgenerálási forgatókönyv alapján végzi.

A *Minősített időbélyegzés-szolgáltató* a saját IT rendszereiben használt infrastruktúrális kulcsok előállítása esetén biztosítsa, hogy:

- a szolgáltatói infrastruktúrális kulcs előállítását fizikailag védett környezetben (lásd 5.1 pont), bizalmi szerepkört (lásd 5.2.1 pont) betöltő, erre feljogosított személy végzi, más illetéktelen személyek jelenlétét kizárva;
- a kulcs előállítása során maradéktalanul betartja az eszköz felhasználói dokumentációjában szereplő előírásokat.

6.1.2. Kulcsméreték

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

- ETSI TS 119 312 [20];
- az Eüt. [5] 92. § (1) b) pontja szerinti aktuális Nemzeti Média- és Hírközlési Hatóság által kiadott algoritmusokkal kapcsolatos határozat.

6.1.3. A nyilvános kulcs paraméterek előállítása, a minőség ellenőrzése

A kulcsparaméterek előállítására vonatkozó követelményeket a 6.1.1. fejezet tartalmazza.

A kulcsok előállításához használt, megfelelő tanúsítvánnyal rendelkező eszközöket a tanúsításban meghatározott követelmények szigorú betartásával kell üzemeltetni a generált kulcsparaméterek minőségének biztosítása érdekében.

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

Az *Időbélyegző egységek* magánkulcsai csak az *Időbélyegzők* hitelesítésére használhatók fel.

6.2. A magánkulcsok védelme

A *Minősített időbélyegzés-szolgáltató* gondoskodnia kell a birtokában lévő magánkulcsok biztonságos kezeléséről, meg kell akadályoznia a magánkulcsok felfedését, lemásolását, törlését, módosítását, jogosulatlan használatát. A *Minősített időbélyegzés-szolgáltató* csak addig őrizheti a magánkulcsokat, ameddig azt a szolgáltatás nyújtása feltétlenül megköveteli.

A *HSM* eszközök kezelése során a használatból kivont *HSM* eszközökben tárolt aláíró magánkulcsokat olyan módon kell törölni, hogy ne legyen lehetséges a kulcsok visszaállítása.

6.2.1. Kriptográfiai modulra vonatkozó szabványok és előírások

A *Minősített időbélyegzés-szolgáltató* *Időbélyegzőket* kibocsátó rendszerei a magánkulcsokat olyan biztonságos hardver eszközökben kell tárolják, amelyek

- megfelelnek az ISO/IEC 19790 [23] követelményeinek,
- vagy megfelelnek a FIPS 140-2 [30] 3-as, illetve annál magasabb szintű követelményeknek,
- vagy megfelelnek a CEN 14167-2 [31] munkacsoport egyezmény követelményeinek,
- vagy megfelelnek a CEN 419 221-5 [21] követelményeinek,
- vagy olyan megbízható rendszerek, amely az MSZ/ISO/IEC 15408 [22] 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 előírányaton kell alapulnia.

A szolgáltatói magánkulcsok a *HSM* eszközön kívül csak kódolt formában tárolhatók. A kódoláshoz csak az Eüt. [5] 92. § (1) b) pontja szerinti aktuális Nemzeti Média- és Hírközlési Hatóság által kiadott algoritmusokkal kapcsolatos határozatban foglalt algoritmusok és kulcsparaméterek használhatók, amelyek várhatóan a kulcs teljes élettartama alatt képesek ellenállni a kriptográfiai támadásoknak.

A szolgáltatói magánkulcsokat kódolt formában is fizikailag biztonságos helyszínen kell tárolni, ahol azokhoz csak az arra jogosultak férhetnek hozzá.

A kriptográfiai algoritmusok vagy kulcsparaméterek gyengülése esetén a kódolt kulcsokat meg kell semmisíteni vagy erősebb védelmet biztosító algoritmus és kulcsparaméterek felhasználásával tovább kell kódolni.

6.2.2. Magánkulcs többszereplős (n-ből m) használata

A *Minősített időbélyegzés-szolgáltató*nak biztosítania kell, 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 *Minősített időbélyegzés-szolgáltató* csak titkosított formában helyezheti letétbe a szolgáltatói magánkulcsait.

6.2.4. Magánkulcs mentése

A *Minősített időbélyegzés-szolgáltató*nak biztonsági másolatokat kell készítenie szolgáltatói magánkulcsairól, ebből legalább egy példányt a szolgáltatás nyújtásától eltérő helyszínen kell tárolni.

A biztonsági másolatok készítése csak védett környezetben, legalább két bizalmi szerepkört betöltő személy együttes jelenlétében, más személyek kizárásával történhet.

A biztonsági másolatok kezelésére és megőrzésére legalább ugyanolyan szigorú biztonsági előírásokat kell alkalmazni, mint az éles rendszer üzemeltetésére.

6.2.5. Magánkulcs archiválása

A *Minősített időbélyegzés-szolgáltató* nem archiválhatja magánkulcsait.

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

A *Minősített időbélyegzés-szolgáltató* valamennyi szolgáltatói magánkulcsát a követelményeknek megfelelő *HSM* eszközben kell előállítani.

A magánkulcsok nem létezhetnek nyílt formában a *HSM* eszközön kívül.

A *Minősített időbélyegzés-szolgáltató* a magánkulcsot csak biztonsági másolat készítése céljából exportálhatja a *HSM* eszközből.

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

6.2.7. Magánkulcs tárolása hardver kriptográfiai eszközben

A *Minősített időbélyegzés-szolgáltató*nak a jelen *Minősített időbélyegzési rendek* szerinti szolgáltatás nyújtásához használt magánkulcsait kriptográfiai modulban kell tartania.

A *HSM* eszközön belüli tárolási formára vonatkozóan nincs előírás.

6.2.8. A magánkulcs aktiválásának módja

A *Minősített időbélyegzés-szolgáltató* szolgáltatói magánkulcsait a felhasznált *HSM* eszköz felhasználói útmutatójában és a tanúsítási dokumentumokban megfogalmazott eljárásoknak, követelményeknek megfelelően kell aktiválni.

6.2.9. A magánkulcs deaktiválásának módja

A *Minősített időbélyegzés-szolgáltató* szolgáltatói magánkulcsait a felhasznált *HSM* eszköz felhasználói útmutatójában és a tanúsítási dokumentumokban megfogalmazott eljárásoknak, követelményeknek megfelelően kell deaktiválni.

6.2.10. A magánkulcs megsemmisítésének módja

A *Minősített időbélyegzés-szolgáltató* használatból kivont, lejárt érvényességű vagy kompromittálódott szolgáltatói magánkulcsait olyan módon kell megsemmisíteni, amely lehetetlenné teszi a magánkulcs további használatát.

A szolgáltatói magánkulcsok megsemmisítését a felhasznált *HSM* eszköz felhasználói útmutatójában és a tanúsítási dokumentumokban megfogalmazott eljárásoknak, követelményeknek megfelelően kell elvégezni.

A magánkulcsról készült minden mentett példányt dokumentált módon meg kell semmisíteni olyan módon, hogy annak visszaállítása, használata lehetetlenné váljon.

6.2.11. A hardver kriptográfiai eszközök értékelése

A 6.2.1 fejezet előírásaival összhangban a *Minősített időbélyegzés-szolgáltató* valamennyi szolgáltatói magánkulcsát olyan *HSM* eszközben kell tárolni, amely rendelkezik:

- ISO/IEC 19790 [23] szerinti tanúsítvánnyal,
- vagy FIPS 140-2 Level 3 [30] szerinti tanúsítvánnyal,
- vagy a CEN 14167-2 [31] munkacsoport egyezmény követelményeinek való megfelelést igazoló legalább EAL-4 szintű Common Criteria alapú tanúsítvánnyal,
- vagy a CEN 419 221-5 [21] követelményeinek való megfelelést igazoló legalább EAL-4 szintű Common Criteria alapú tanúsítvánnyal,
- vagy 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 *Minősített időbélyegzés-szolgáltató* által üzemeltetett *Időbélyegző egységek Tanúsítványainak* érvényességi ideje:

- legfeljebb a kibocsátástól számított 12 év;
- nem haladhatja meg az alkalmazott kriptográfiai algoritmusok és kulcs paraméterek érvényességi idejét;
- nem haladhatja meg a *Tanúsítványt* kibocsátó szolgáltatói *Tanúsítvány* érvényességi idejét.

A *Minősített időbélyegzés-szolgáltató* az aktuális használatban lévő magánkulcs használati idejének lejártát megelőzően időben állítson elő új magánkulcs(ka)t és igényeljen új *Tanúsítvány(oka)t* az *Időbélyegző egységei* számára. Az új *Időbélyegző egység Tanúsítvány(ok)* használatba vétele után a korábbi magánkulcs(ka)t meg kell semmisíteni.

Az Időbélyegző kulcsok életciklusa

Az *Időbélyegzők* hitelesítésére használt magánkulcsok esetében teljesülniük kell az alábbi követelményeknek:

- a *Minősített időbélyegzés-szolgáltató*nak meg kell határoznia az *Időbélyegző egységek*ben használt magánkulcsok érvényességének végét;
- a kulcs érvényességi ideje nem haladhatja meg a *Tanúsítvány* érvényességi idejét;
- a kulcs érvényességi ideje nem haladhatja meg az alkalmazott kriptográfiai algoritmusok és kulcs paraméterek érvényességi idejét;
- az *Időbélyegző egységek* kulcsának érvényességi ideje megadható a használt *HSM eszköz* felparaméterezésekor, vagy a *Tanúsítvány* "PrivateKeyUsagePeriod" értékének beállításával;
- az *Időbélyegző egység* magánkulcsa nem használható az érvényességi időn túl;
- a *Minősített időbélyegzés-szolgáltató*nak szervezeti vagy műszaki eljárásokat kell létrehoznia annak biztosítására, hogy az *Időbélyegző egység* kulcsának lejáratára esetén rendelkezésre álljon az új magánkulcs;
- a kulcs érvényességének lejáratára után a magánkulcs minden példányát meg kell semmisíteni oly módon, hogy a magánkulcs visszaállítása lehetetlen legyen.

A *Tanúsítványok* 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 *Tanúsítványokat*.

6.4. Aktivizáló adatok

6.4.1. Aktivizáló adatok előállítása és telepítése

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

Jelszó alapú aktivizáló adatok használata esetén a jelszavaknak kellően bonyolultnak kell lenniük a megkívánt védelmi szint biztosítása érdekében.

6.4.2. Az aktivizáló adatok védelme

A *Minősített időbélyegzés-szolgáltató* alkalmazottainak a magánkulcsok aktiválásához szükséges eszközöket, aktivizáló adatokat biztonságosan kell tárolniuk, a jelszavak csak kódolt formában tárolhatók.

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 *Minősített időbélyegzés-szolgáltató* informatikai rendszereinek konfigurálása és üzemeltetése során biztosítani kell az alábbi követelmények teljesülését:

- a rendszerhez vagy alkalmazáshoz való hozzáférés engedélyezése előtt a felhasználó azonosságát ellenőrizni kell;
- a felhasználókhöz szerepköröket kell rendelni és biztosítani kell, hogy minden felhasználó csak a szerepkörének megfelelő jogosultságokkal rendelkezzen;
- minden tranzakcióról naplóbejegyzést kell előállítani és a naplóbejegyzéseket archiválni kell;
- a biztonságkritikus folyamatok részére biztosítani kell, hogy a *Minősített időbélyegzés-szolgáltató* belső hálózati tartományai kellően védettek legyenek a jogosulatlan hozzáféréstől;
- megfelelő eljárásokat kell alkalmazni a kulcsvesztés vagy rendszerhiba után a szolgáltatás visszaállítása érdekében.

6.5.2. Az informatikai biztonság értékelése

Az informatikai biztonság és a szolgáltatás minőségének biztosítása érdekében a *Minősített időbélyegzés-szolgáltató* nemzetközileg elfogadott módszertanok szerinti irányítási rendszert kell alkalmazzon, ezek megfelelőségét független tanúsító szervezet által kiállított tanúsítvánnyal kell igazolnia.

6.6. Életciklusra vonatkozó műszaki előírások

6.6.1. Rendszerfejlesztési előírások

A *Minősített időbélyegzés-szolgáltató* az éles szolgáltatást nyújtó informatikai rendszereiben csak olyan eszközöket, alkalmazásokat használhat, amelyek:

- kereskedelmi dobozos szoftverek, amelyeket dokumentált tervezési módszertan szerint terveztek és fejlesztettek;
- a *Minősített időbélyegzés-szolgáltató* saját maga által kifejlesztett egyedi hardver és szoftver megoldások, amelyek tervezése során strukturált fejlesztési módszereket és ellenőrzött fejlesztési környezetet használt;
- a *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.

A beszerzést a hardver és szoftver komponensek módosítását kizáró módon kell elvégezni.

A szolgáltatás nyújtásához használt hardver és szoftver komponensek más célra nem használhatók.

A *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 ellenőrizni kell kártékony kódok után kutatva.

A *Minősített időbélyegzés-szolgáltató* a programfrissítések vásárlása vagy fejlesztése során ugyanolyan gondossággal kell eljárjon, mint az első verzió beszerzésekor.

Megbízható, megfelelően képzett személyzetet kell alkalmazni a szoftverek és eszközök telepítése során.

A *Minősített időbélyegzés-szolgáltató* csak a szolgáltatás nyújtásához szükséges szoftvereket telepítheti a szolgáltatást nyújtó informatikai berendezéseire.

A *Minősített időbélyegzés-szolgáltató* rendelkeznie kell egy változáskövető rendszerrel, amelyben minden változást dokumentálni kell.

A *Minősített időbélyegzés-szolgáltató* alkalmazzon eljárásokat a jogosulatlan változások észlelésére.

6.6.2. Biztonságkezelési előírások

A *Minősített időbélyegzés-szolgáltató* alkalmazzon eljárásokat a szolgáltatásban használt rendszerek telepítésének, konfigurációjának dokumentálására, üzemeltetésére, ellenőrzésére, monitorozására és karbantartására, beleértve a módosításokat és továbbfejlesztéseket is. A változáskövető rendszernek észlelnie kell 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 *Minősített időbélyegzés-szolgáltató* győződjön meg róla, hogy a telepítendő program a megfelelő verziójú és mentes mindenféle jogosulatlan módosítástól. A *Minősített időbélyegzés-szolgáltató* ellenőrizze rendszeresen a szolgáltatói rendszereiben használt programok integritását.

6.6.3. Életciklusra vonatkozó biztonsági előírások

A *Minősített időbélyegzés-szolgáltató* gondoskodnia kell a felhasznált *HSM* eszközök védelméről azok teljes életciklusa alatt.

- Megfelelő tanúsítással rendelkező *HSM* eszközöket kell használni.
- A *HSM* eszközök átvételekor meg kell róla győződni, hogy a szállítás során biztosították a *HSM* eszközök feltörés elleni védelmét.
- A tárolás során biztosítani kell a *HSM* eszközök feltörés elleni védelmét.

- Az üzemeltetés során folyamatosan be kell tartani a *HSM* eszközök biztonsági előírányzatában, használati útmutatójában és a tanúsítási jelentésben szereplő követelményeket.
- A használatból kivont *HSM* eszközökben tárolt magánkulcsokat olyan módon kell törölni, hogy lehetetlenné váljon a kulcsok visszaállítása.
- A használatból kivont *HSM* eszközöket a biztonsági előírányzatában, használati útmutatójában és a tanúsítási jelentésben szereplő követelményeknek megfelelően kell kezelni és megsemmisíteni.

6.7. Hálózati biztonsági előírások

A *Minősített időbélyegzés-szolgáltató* tartsa szigorú ellenőrzés alatt az alkalmazott IT rendszereinek konfigurációját, dokumentálja minden változást, beleértve a legkisebb módosítást, fejlesztést, szoftverfrissítést is. A *Minősített időbélyegzés-szolgáltató* vezessen be megfelelő eljárásokat az IT rendszereiben bekövetkezett tetszőleges hardver vagy szoftver változás észlelésére, a rendszer telepítésére, karbantartására. A *Minősített időbélyegzés-szolgáltató* ellenőrizze minden szoftverkomponens első betöltésekor a komponens eredetiségét, integritását.

A *Minősített időbélyegzés-szolgáltató* alkalmazzon megfelelő hálózatbiztonsági intézkedéseket, mint például

- IT rendszereit jól elválasztott biztonsági zónákra kell osztania;
- el kell különítenie az IT rendszer üzemeltetését támogató rendszereit az éles szolgáltatást nyújtó rendszereitől;
- el kell különítenie az éles szolgáltatást nyújtó rendszereit a fejlesztésre és tesztelésre szolgáló rendszerektől;
- az elkülönített megbízható rendszerek között csak olyan megbízható kommunikációs csatornákon keresztül létesíthet 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 kell üzemeltesse;
- a zónákhoz való hozzáférést és a zónák közötti kommunikációt csak a szolgáltatás nyújtásához szükségesre kell korlátoznia;
- le kell tiltani a nem használt protokollokat és felhasználókat;
- tiltsa le a használaton kívüli hálózati portokat és szolgáltatásokat;
- csak az IT rendszer megfelelő működéséhez feltétlenül szükséges hálózati alkalmazásokat futtasson;
- a használt szabályrendszert rendszeresen felül kell vizsgálnia.

A *Minősített időbélyegzés-szolgáltató*nak sérülékenységvizsgálatot kell végeznie vagy végeztetnie a *Minősített időbélyegzés-szolgáltató* nyilvános és privát IP címein:

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

6.8. Időbélyegzés

A *Minősített időbélyegzés-szolgáltató*nak valamely Európai Unió tagállam bizalmi listáján szereplő minősített időbélyegzés-szolgáltató által biztosított *Időbélyegzőket* kell használnia a naplóbejegyzések és egyéb archiválendő elektronikus állományok hitelesítésére.

7. Tanúsítvány, CRL és OCSP profilok

7.1. Tanúsítvány profil

A *Minősített időbélyegzés-szolgáltató* által használt *Időbélyegző egység Tanúsítványok* illetve az azokat kibocsátó tanúsítvány láncban található gyökér és köztes hitelesítő egységek *Tanúsítványai* feleljenek meg az alábbi ajánlásoknak, specifikációknak:

- ITU X.509 Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks [28];
- IETF RFC 3739 [25];
- IETF RFC 5280 [26];
- IETF RFC 6818 [27];
- ETSI EN 319 412-1 [14];
- ETSI EN 319 412-2 [15] természetes személyek számára kibocsátott *Tanúsítványok* esetén;
- ETSI EN 319 412-3 [16] nem természetes személyek számára kibocsátott *Tanúsítványok* esetén;
- ETSI EN 319 412-5 [17].

7.1.1. Verzió szám(ok)

A *Minősített időbélyegzés-szolgáltató* által használt *Időbélyegző egység Tanúsítványok* legyenek az X.509 specifikáció [28] szerinti "v3" *Tanúsítványok*.

A *Tanúsítványok* alapmezői a következők:

- Verzió (Version)
A *Tanúsítvány* az X.509 specifikáció [28] szerinti "v3" *Tanúsítvány*oknak felel meg, így a mezőbe a "2" érték kerül.
- Sorozatszám (Serial Number)
A *Tanúsítványt* kibocsátó hitelesítő egység által generált egyedi azonosító.
A végfelhasználói *Tanúsítványok* esetében a "Serial Number" mezőnek legalább 8 bájt entrópiájú véletlen számot kell tartalmaznia.
- Algoritmus azonosító (Algorithm Identifier)
A *Tanúsítványt* hitelesítő elektronikus aláírás vagy bélyegző készítéséhez használt kriptográfiai algoritmuskészlet azonosítója (OID).
- Aláírás (Signature)
A *Hitelesítés-szolgáltató* által készített, a *Tanúsítványt* hitelesítő elektronikus aláírás vagy bélyegző, amelyet a *Hitelesítés-szolgáltató* az "Algoritmus azonosító" -ban megadott algoritmuskészlettel hozott létre.
- Kibocsátó (Issuer)
A *Tanúsítványt* 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)
Az *Alany* nyilvános kulcsának algoritmus azonosítója.
- 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 *Minősített időbélyegzés-szolgáltató* az X.509 specifikáció [28] szerinti tanúsítvány kiterjesztéseket használhat, saját maga által definiált kritikus kiterjesztések használata nem megengedett.

A tanúsítvány kiterjesztéssel kapcsolatos konkrét előírások:

Időbélyegző egység tanúsítványa

- Hitelesítési rendek (Certificate Policies) – nem kritikus
OID: 2.5.29.32
E mező tartalmazza az *Időbélyegző egység Tanúsítványának* kiadása és használata során érvényes *Hitelesítési rend* azonosítóját, valamint az alkalmazhatóságára vonatkozó egyéb információkat. A mező kitöltése kötelező és nem lehet kritikus. A vonatkozó Szolgáltatási szabályzat hivatkozása megadható ebben a mezőben.
- Kibocsátó kulcsazonosító (Authority Key Identifier) – nem kritikus
OID: 2.5.29.35
A *Tanúsítványt* hitelesítő elektronikus aláírás vagy bélyegző létrehozásánál felhasznált szolgáltatói kulcs 40 karakter hosszú egyedi azonosítója.
Használata kötelező.
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.
Használata kötelező.
- *Alany* alternatív nevei (Subject Alternative Names) – nem kritikus
OID: 2.5.29.17
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 szerepelhet az *Időbélyegző egység* számára kibocsátott *Tanúsítványokban*.
A "pathLenConstraint" mező nem szerepelhet *Időbélyegző egység* számára kibocsátott *Tanúsítványokban*.
- Kulcshasználat (Key Usage) – kritikus
OID: 2.5.29.15
A kulcs engedélyezett használati körének meghatározása.
Az *Időbélyegző egység* számára kibocsátott *Tanúsítványokban* kötelezően beállítandó és kizárólagosan megadandó érték:
"nonRepudiation",
"digitalSignature".
- Kulcshasználati időszak (PrivateKeyUsagePeriod) – nem kritikus
OID: 2.5.29.16
A magánkulcs engedélyezett használati időtartamának meghatározása.
Használata opcionális. Amennyiben alkalmazásra kerül, a "notBefore" és "notAfter" értékek mindegyikét meg kell adni.

- Kiterjesztett kulcshasználat (Extended Key Usage) – kritikus
OID: 2.5.29.37
A kulcs további engedélyezett használati körének meghatározása.
Az *Időbélyegző egység* számára kibocsátott *Tanúsítvány*okban kötelezően beállítandó és kizárólagosan megadandó érték:
"timeStamping (1.3.6.1.5.5.7.3.8)".
- CRL szétesztási 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 *Hitelesítés-szolgáltató* a *Tanúsítvány*ok aktuális visszavonási állapotának gyors és pontos ellenőrizhetősége érdekében online tanúsítvány-állapot szolgáltatást kell nyújtson. Ennek elérhetőségét kell itt szerepeltetni.
 - A tanúsítványlánc felépítésének megkönnyítésére a *Hitelesítés-szolgáltató* adja meg a *Tanúsítvány*t kibocsátó hitelesítési egység *Tanúsítvány*ának http protokollon keresztüli elérési helyét.
- Minősített tanúsítvánnyal kapcsolatos állítások (Qualified Certificate Statements) – nem kritikus
OID: 1.3.6.1.5.5.7.1.3
A mező a minősített *Tanúsítvány*okkal kapcsolatos állítások jelzésére szolgál. Az *Időbélyegző egység Tanúsítvány*ában szerepelniük kell a következő állításoknak:
 - a *Tanúsítvány* EU minősített *Tanúsítvány* – 'id-etsi-qcs 1' (0.4.0.1862.1.1);
 - a *Tanúsítvány*hoz kapcsolódó tranzakciós limit – más néven üzleti érték vagy pénzügyi tranzakciós korlát – 'id-etsi-qcs 2' (0.4.0.1862.1.2)
- opcionális;
 - azon kijelentés, hogy a Szolgáltató a *Tanúsítvány*hoz kapcsolódó regisztrációs adatokat a *Tanúsítvány* lejáratá után 10 évig megőrzi – 'id-etsi-qcs 3' (0.4.0.1862.1.3);
 - azon kijelentés, hogy a *Tanúsítvány*hoz tartozó magánkulcs *Minősített elektronikus aláírást létrehozó eszközön* helyezkedik el – 'id-etsi-qcs 4' (0.4.0.1862.1.4) – kizárólag *Minősített elektronikus aláírást létrehozó eszköz* használatát megkövetelő hitelesítési rendek esetén;
 - az *Időbélyegző egység Tanúsítvány*ára vonatkozó Szolgáltatási szabályzat rövidített, kivonatolt változatát tartalmazó dokumentum elérhetősége – 'id-etsi-qcs 5' (0.4.0.1862.1.5);
 - annak jelzése, hogy a *Tanúsítvány* bélyegzés célra került kibocsátásra – 'id-etsi-qcs 6' (0.4.0.1862.1.6) (a mező értéke 'id-etsi-qcs 6' (2)).

Más tanúsítvány kiterjesztés nem kerülhet kitöltésre.

8. A megfelelés vizsgálat

A *Minősített időbélyegzés-szolgáltató* tevékenységét az Európai Unió szabályozással összhangban a Nemzeti Média- és Hírközlési Hatóság felügyeli. A Nemzeti Média- és Hírközlési Hatóság évente legalább egyszer átfogó helyszíni ellenőrzést tart a *Minősített időbélyegzés-szolgáltató* telephelyén. A helyszíni ellenőrzés előtt a *Minősített időbélyegzés-szolgáltató* köteles külső auditor igénybevételeivel átvilágíttatni üzemeltetését és az átvilágításról készült részletes megfelelésértékelési jelentést annak kézhezvételétől számított három munkanapon belül a Nemzeti Média- és Hírközlési Hatóságnak benyújtani. Az átvizsgálás során azt kell megállapítani, hogy a *Minősített időbélyegzés-szolgáltató* működése megfelel-e az eIDAS Rendeletben [1] és a vonatkozó magyar jogszabályokban megállapított követelményeknek, valamint az alkalmazott *Minősített időbélyegzési rend(ek)*ben és az ennek megfelelő *Minősített időbélyegzési szolgáltatási szabályzat(ok)*ban támasztott követelményeknek.

Az átvilágítás tematikája és módszertana feleljen meg 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 319 403 V2.2.2 (2015-08) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers; [11]
- 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. [18]

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

A megfelelésértékelési jelentés alapján kiállított megfeleléségi tanúsítványt közzé kell tenni a *Minősített időbélyegzés-szolgáltató* honlapján.

A *Minősített időbélyegzés-szolgáltató* fenntartja a jogot, hogy a jelen *Minősített időbélyegzési rend(ek)* alapján működő szolgáltatók tevékenységét tetszőleges időpontban független szakértő bevonásával átvizsgálja a követelmények betartásának ellenőrzése érdekében.

8.1. Az ellenőrzések körülményei és gyakorisága

A *Minősített időbélyegzés-szolgáltató* évente köteles elvégeztetni a megfelelésértékelő vizsgálatot.

8.2. Az auditor és szükséges képesítése

A *Minősített időbélyegzés-szolgáltató* a belső auditokat a független rendszervizsgáló szerepkörrel felruházott alkalmazottai segítségével is elvégezheti.

Az eIDAS és ETSI követelményeknek való megfelelést 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 rendszer elem függetlensége

A külső auditot csak olyan személy végezheti:

- aki független a vizsgált *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 *Minősített időbélyegzés-szolgáltatóval*;

8.4. Az auditálás által lefedett területek

Az átvizsgálásnak le kell fednie minimálisan az alábbi területeket:

- hatályos jogszabályoknak való megfelelés;
- műszaki szabványoknak való megfelelés;
- *Minősített időbélyegzési rend(ek)*nek és *Minősített időbélyegzési szolgáltatási szabályzat(ok)*nak való megfelelés;
- az alkalmazott folyamatok megfelelése;
- a dokumentálás;
- a fizikai biztonság;
- a személyi állomány megfelelése;
- az IT biztonság;
- az adatvédelmi szabályok betartása.

8.5. A hiányosságok kezelése

A független auditor az átvizsgálás eredményét egy részletes átvilágítási jelentésben kell összefoglalja, amely kitér a vizsgált rendszer elemekre, folyamatokra, tartalmazza az átvilágítás során felhasznált bizonyítékokat és vizsgálói megállapításokat. A jelentésben külön fejezetben kell rögzíteni 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.

A független auditornak a feltárt súlyos eltéréseket haladéktalanul jelentenie kell a Nemzeti Média- és Hírközlési Hatóságnak, aki jogosult meghozni a szükséges intézkedéseket.

A *Minősített időbélyegzés-szolgáltató* köteles a független vizsgáló által felvetett problémákra írásban válaszolni, az elhárításukra tett intézkedésekről a következő hatósági szemle alkalmával beszámolni.

A független auditornak a vizsgálati jelentést minden esetben meg kell küldenie a Nemzeti Média- és Hírközlési Hatóságnak.

8.6. Az eredmények közzététele

A *Minősített időbélyegzés-szolgáltató* a vizsgálat eredményét összefoglaló jelentést köteles nyilvánosságra hozni. Nem köteles a független rendszervizsgálat során feltárt hiányosságok publikálására, azokat bizalmas információként kezelheti.

9. Egyéb üzleti és jogi kérdések

9.1. Díjak

A *Minősített időbélyegzés-szolgáltató* által alkalmazható díjakat a vonatkozó szabályozásnak megfelelően nyilvánosan közzé kell tenni.

9.1.1. Visszatérítési politika

Nincs megkötés.

9.2. Anyagi felelősségvállalás

A *Minősített időbélyegzés-szolgáltató* megbízhatósága érdekében anyagi felelősséget vállal a jelen *Hitelesítési rendben*, a vonatkozó *Minősített időbélyegzési szolgáltatási szabályzatban* valamint az *Ügyféllel kötött Szolgáltatási szerződésben* megfogalmazott valamennyi rá vonatkozó kötelezettség maradéktalan betartásáért.

9.2.1. Pénzügyi követelmények

A *Minősített időbélyegzés-szolgáltató* a szolgáltatási tevékenységének megszűnésével kapcsolatos költségek biztosítása és a megbízhatóság érdekében köteles az alábbi követelmények legalább egyikének megfelelni:

- A *Minősített időbélyegzés-szolgáltató* legalább huszonötmillió forint összegű, feltétel nélküli és visszavonhatatlan bankgaranciával rendelkezik.
- A *Minősített időbélyegzés-szolgáltató* a Nemzeti Média- és Hírközlési Hatóság mint jogosult javára pénzügyi intézménynél óvadékot tesz le. Az óvadék összege legalább huszonötmillió forint.

- A költségek megfizetéséért hitelesítés-szolgáltató esetén legalább százmillió forint jegyzett tőkéjű európai uniós vállalkozás készfizető kezességét vállal. A kezességvállalás mértéke legalább huszonötmillió forintig terjed.

9.2.2. Felelősségbiztosítás

- A *Minősített időbélyegzés-szolgáltató*nak a megbízhatóság biztosítása érdekében felelősségbiztosítással kell rendelkeznie.
- A felelősségbiztosítási szerződésnek ki kell terjednie az alábbi, a *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 *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 felelősségbiztosításnak a meghatározott összeg erejéig fedezetet kell nyújtania 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 *Minősített időbélyegzés-szolgáltató*nak az *Ügyfelek* adatait a jogszabályoknak megfelelően kell kezelnie.

9.3.1. Bizalmas információk köre

A *Minősített időbélyegzés-szolgáltató*nak a *Minősített időbélyegzési szolgáltatási szabályzat*ában pontosan meg kell határoznia, hogy mely adatok minősülnek bizalmas információnak.

9.3.2. Bizalmas információk körén kívül eső adatok

A *Minősített időbélyegzés-szolgáltató* nyilvánosnak tekinthet minden olyan adatot, amely nem szerepel a bizalmas adatok felsorolásában a *Minősített időbélyegzési szolgáltatási szabályzatban*.

9.3.3. Bizalmas információ védelme

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

A *Minősített időbélyegzés-szolgáltató* szerződésben vagy titoktartási nyilatkozat aláírásával kell kötelezze alkalmazottait, alvállalkozóit, szerződött partnereit a bizalmas adatok védelmére.

A *Minősített időbélyegzés-szolgáltató* *Minősített időbélyegzési szolgáltatási szabályzatában* tételesen meg kell határozni azon eseteket, amikor a *Minősített időbélyegzés-szolgáltató* felfedheti a bizalmas adatokat.

9.4. Személyes adatok védelme

A *Minősített időbélyegzés-szolgáltató* gondoskodnia kell az általa kezelt személyes adatok védelméről. Működésének és szabályzatainak meg kell felelniük az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény [3] és a 2016/679 EU általános adatvédelmi rendelet [2] rendelkezéseinek.

A *Minősített időbélyegzés-szolgáltató* köteles az *Ügyfélről* nyilvántartott személyes adatokat és információkat a jogszabályi előírásoknak megfelelően

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

9.4.1. Adatkezelési terv

A *Minősített időbélyegzés-szolgáltató* rendelkeznie kell Adatkezelési Szabályzattal, amely részletes előírásokat tartalmaz a személyes adatok kezelésére. Az Adatkezelési Szabályzatot nyilvánosságra kell hozni a *Minősített időbélyegzés-szolgáltató* honlapján.

9.4.2. Személyes adatok

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

A *Minősített időbélyegzés-szolgáltató* csak az *Előfizetőtől* közvetlenül, vagy annak egyértelmű előzetes hozzájárulásával gyűjthet személyes adatokat és csak olyan mértékben, ami a szolgáltatás nyújtásához szükséges.

9.4.3. Személyes adatnak nem minősülő adatok

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

9.4.4. Személyes adatok védelme

A *Minősített időbélyegzés-szolgáltató* köteles biztonságosan tárolni és védeni az általa kezelt személyes adatokat. Az adatokat megfelelő intézkedésekkel védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, valamint nyilvánosságra hozatal ellen.

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

9.4.6. Adatkezelés

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

A jelen *Minősített időbélyegzési rend* a *Minősített időbélyegzés-szolgáltató* kizárólagos tulajdonát képezi. Az *Ügyfelek* és egyéb *Érintett felek* a dokumentumot csak a jelen *Minősített időbélyegzési rend* előírásainak megfelelően jogosultak felhasználni, minden egyéb kereskedelmi vagy egyéb célú felhasználás szigorúan tilos.

A jelen *Minősített időbélyegzési rend* szabadon terjeszthető, de csak változatlan formában, teljes terjedelemben és az eredet feltüntetésével.

A *Minősített időbélyegzés-szolgáltató* által a szolgáltatás igénybevételéhez biztosított szoftverek használatának szabályait a *Minősített időbélyegzési szolgáltatási szabályzatban* kell meghatározni.

9.6. Tevékenységért viselt felelősség és helytállás

9.6.1. A szolgáltató felelőssége és helytállása

A Szolgáltató felelőssége

A *Minősített időbélyegzés-szolgáltató* felel a jelen *Minősített időbélyegzési rendben*, a vonatkozó *Minősített időbélyegzési szolgáltatási szabályzatban* valamint az *Ügyféllel* kötött Szolgáltatási szerződésben megfogalmazott valamennyi rá vonatkozó kötelezettség maradéktalan betartásáért, különösen a következő esetekben:

- a *Minősített időbélyegzés-szolgáltató* felelősséget vállal az általa támogatott *Minősített időbélyegzési rend(ek)*ben leírt eljárásoknak való megfelelésért;
- a *Minősített időbélyegzés-szolgáltató* sajátjaként felel az alvállalkozói által a szolgáltatás nyújtása során okozott károkért;
- a *Minősített időbélyegzés-szolgáltató* a vele szerződéses jogviszonyban álló *Ügyfelekkel* szemben a Polgári Törvénykönyv [4] a szerződésszegésért való felelősség szabályai szerint felelős;
- a *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 *Minősített időbélyegzés-szolgáltató* a felelősségi körén belül keletkezett, bizonyított károkért a szabályzataiban és az *Ügyféllel* megkötött Szolgáltatási szerződésekben rögzített korlátozásokkal kártérítést fizet (lásd: Pénzügyi felelősség korlátozása 9.8. fejezet);

A Szolgáltató kötelezettségei az Előfizetővel szemben

A *Minősített időbélyegzés-szolgáltató* köteles:

- az *Előfizetőtől* érkező kérésre az ETSI EN 319 422 [19] specifikációnak megfelelő formátumú *Időbélyegzőt* kibocsátani, amely a kérelemben szereplő lenyomatra vonatkozik és tartalmazza a kérelemben szereplő egyedi sorszámot;
- az *Időbélyegző* pontosságát 1 másodpercen belül tartani (az UTC-től való eltérés legfeljebb 1 másodperc lehet);
- a szolgáltatás megbízhatóságát és biztonságát a minősített időbélyegzés szolgáltatókra vonatkozó követelmények szerint biztosítani;
- naplózni a szolgáltatással kapcsolatos minden fontos eseményt, és e naplófájlokat a jogszabályi előírásoknak megfelelően megőrizni.

A Szolgáltató kötelezettsége

A *Minősített időbélyegzés-szolgáltató* köteles teljesíteni az eIDAS Rendelet [1] 24. cikkének (2) bekezdésében foglalt követelményeket.

A *Minősített időbélyegzés-szolgáltató* alapvető kötelezettsége, hogy a szolgáltatásokat a *Minősített időbélyegzési renddel*, a *Minősített időbélyegzési szolgáltatási szabályzattal* 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 (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 helyállása

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 *Minősített időbélyegzés-szolgáltató* szerződéses feltételeinek és szabályzatainak megfelelően eljárni a szolgáltatás igénybevétele során.

Az *Előfizető* kötelezettségeit a jelen *Minősített időbélyegzési rend*, a Szolgáltatási szerződés és annak mellékletei – különösen az Általános Szerződési Feltételek – és a *Minősített időbélyegzési szolgáltatási szabályzat* írja le.

9.6.3. Az Érintett fél felelőssége

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

- a *Minősített időbélyegzési rendben* és a *Minősített időbélyegzési szolgáltatási szabályzatban* 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 figyelembevétel, amely a a *Minősített időbélyegzési szolgáltatási szabályzatban* és a vonatkozó *Minősített időbélyegzési rendben* szerepel.

9.6.4. Egyéb szereplők tevékenységéért viselt felelősség és helytállás

Nincs megkötés.

9.7. Helytállás érvénytelenségi köre

A *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 *Minősített időbélyegzés-szolgáltató* korlátozhatja kártérítési felelősségét.

9.9. Kártérítési kötelezettség

9.9.1. A szolgáltató kártérítési kötelezettsége

A *Minősített időbélyegzés-szolgáltató* kártérítési kötelezettségének részletes szabályait a *Minősített időbélyegzési szolgáltatási szabályzat*, a Szolgáltatási szerződés vagy az *Ügyfelekkel* kötött szerződések tartalmazzák.

9.9.2. Az előfizető kártérítési kötelezettsége

A *Minősített időbélyegzés-szolgáltató* a *Minősített időbélyegzési szolgáltatási szabályzatban* és a Szolgáltatási szerződésben szabályozza az *Előfizetőkkel* szemben támasztott kártérítési igényeit.

9.9.3. Az érintett felek kártérítési kötelezettsége

A *Minősített időbélyegzés-szolgáltató* a *Minősített időbélyegzési szolgáltatási szabályzatban* szabályozza az *Érintett felekkel* szemben támasztott kártérítési igényeit.

9.10. Érvényesség és megszűnés

9.10.1. Érvényesség

A *Minősített időbélyegzési rend* adott verziója hatálybalépésének napja a dokumentum címlapján kerül meghatározásra.

9.10.2. Megszűnés

A *Minősített időbélyegzési rend* visszavonásig illetve a *Minősített időbélyegzési rend* újabb verziójának hatályba lépéséig hatályos időbeli korlátozás nélkül.

9.10.3. A megszűnés következményei

A *Minősített időbélyegzési rend* visszavonása esetén a *Minősített időbélyegzés-szolgáltató* honlapján közzéteszi a visszavonás részletes szabályait és a visszavonás után is fennálló jogokat és kötelezettségeket.

9.11. A felek közötti kommunikáció

A *Minősített időbélyegzés-szolgáltató* az *Ügyfelekkel* történő kapcsolattartás érdekében működtessen ügyfélszolgálati irodát.

9.12. Módosítások

A *Minősített időbélyegzés-szolgáltató* fenntartja magának a jogot, hogy a normatív szabályok, biztonsági követelmények, piaci környezet vagy egyéb körülmények változása esetén szabályozott módon megváltoztassa a *Minősített időbélyegzési rendet*.

9.12.1. Módosítási eljárás

A *Minősített időbélyegzés-szolgáltató* évi rendszerességgel illetve rendkívüli változtatási igény esetén soron kívül átvizsgálja a *Minősített időbélyegzési rendet* és elvégzi a szükségesnek tartott változtatásokat. A dokumentum a legkisebb változtatás után is új verziószámot kap és az elfogadási procedura időigényét figyelembe véve meghatározásra kerül a tervezett hatálybalépés időpontja is. *Minősített időbélyegzés-szolgáltató* a jóváhagyott dokumentumot legalább 30 nappal a tervezett hatálybalépés előtt véleményezésre megküldi a Nemzeti Média- és Hírközlési Hatóság részére és publikálja honlapján.

A *Minősített időbélyegzés-szolgáltató* a közzétett új szabályzat tervezettel kapcsolatos észrevételeket a hatálybalépést megelőző 14. napig fogadja az alábbi címen:

info@e-szigno.hu

Érdemi változtatást igénylő észrevétel esetén a dokumentumot megváltoztatja.

A szabályzat észrevételekkel módosított változatát a *Minősített időbélyegzés-szolgáltató* a hatálybalépést megelőző 7. napon zárja le és teszi közzé.

9.12.2. Értesítések módja és határideje

A *Minősített időbélyegzés-szolgáltató* a 9.12.1. pontban leírtak szerint értesíti az *Érintett feleket* az új dokumentum verziók kibocsátásáról.

9.12.3. Az OID megváltoztatása

A *Minősített időbélyegzés-szolgáltató* a *Minősített időbélyegzési rend* 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 *Minősített időbélyegzés-szolgáltató* törekedjen a működése során felmerülő vitás kérdések békés, tárgyalásos rendezésére. A rendezés során a fokozatosság elvét kell követni.

9.14. Irányadó jog

A *Minősített időbélyegzés-szolgáltató* tevékenységét a mindenkor hatályos magyar jogszabályoknak megfelelően végzi. A *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 jelen *Minősített időbélyegzési rend* megfelel az alábbi jogszabályoknak:

- 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 *Minősített időbélyegzési rend*nek megfelelően működő szolgáltatók csak a *Minősített időbélyegzés-szolgáltató* előzetes írásbeli engedélyével adhatják tovább jogosultságaikat és delegálhatják kötelezettségeiket harmadik félnek.

9.16.3. Részleges érvénytelenség

A jelen *Minősített időbélyegzési rend* egyes rendelkezéseinek tetszőleges okból történő érvénytelenné válása esetén a többi rendelkezés változatlan formában érvényben marad.

9.16.4. Igényérvényesítés

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

9.16.5. Vis maior

A *Minősített időbélyegzés-szolgáltató* nem felelős a *Minősített időbélyegzési rend*ben és a *Minősített időbélyegzési szolgáltatói szabályzat*ban megfogalmazott kötelezettség hibás vagy késedelmes teljesítéséért, illetve nem teljesítéséért, amennyiben a hiba vagy késedelem oka a *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 319 403 V2.2.2 (2015-08) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers;.
- [12] 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.
- [13] 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;.
- [14] ETSI EN 319 412-1 V1.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.

-
- [15] 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;.
- [16] 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.
- [17] ETSI EN 319 412-5 V2.2.1 (2017-11); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.
- [18] 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.
- [19] ETSI EN 319 422 V1.1.1 (2016-03); Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.
- [20] ETSI TS 119 312 V1.3.1 (2019-02); Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.
- [21] CEN 419 221-5; Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services.
- [22] MSZ/ISO/IEC 15408-2002, Informatika. Biztonságtechnika. Az informatikai biztonságértékelés közös szempontjai, 2002 december .
- [23] ISO/IEC 19790:2012: Information technology – Security techniques – Security requirements for cryptographic modules.
- [24] IETF RFC 3161: Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP), August 2001.
- [25] IETF RFC 3739: Internet X.509 Public Key Infrastructure - Qualified Certificates Profile, MARCH 2004.
- [26] IETF RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile, May 2008.
- [27] IETF RFC 6818: Updates to the Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile, January 2013.
- [28] ITU X.509 Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.
- [29] Recommendation ITU-R TF.460-6 (2002): Standard-frequency and time-signal emissions.
- [30] FIPS PUB 140-2 (2001 May 25): Security Requirements for Cryptographic Modules.
- [31] CEN Workgroup Agreement CWA 14167-2: Cryptographic module for CSP signing operations with backup - Protection profile - CMCSOB PP.
- [32] e-Szignó Hitelesítés Szolgáltató - Általános Szerződési Feltételek .