MICROSEC

e-Szignó Hitelesítés Szolgáltató

eIDAS Rendelet szerinti minősített időbélyegzés-szolgáltatás szolgáltatási szabályzat

ver. 2.22

Hatálybalépés: 2021-06-30

Azonosító	1.3.6.1.4.1.21528.2.1.1.169.2.22
Verzió	2.22
Első verzió hatálybalépése	2016-07-01
Biztonsági besorolás	NYILVÁNOS
Jóváhagyta	Vanczák Gergely
Jóváhagyás dátuma	2021-06-23
Hatálybalépés dátuma	2021-06-30

Microsec Számítástechnikai Fejlesztő zártkörűen működő Részvénytársaság

1033 Budapest, Ángel Sanz Briz út 13.

Verzió	Hatálybalépés	A változás leírása
2.0	2016-07-01	eIDAS követelmények szerinti első önálló időbélyegzési szabályzat.
2.1	2016-09-05	- Módosítások az NMHH észrevételei alapján.
2.2	2016-10-30	- Módosítások a tanúsító észrevételei alapján.
2.4	2017-09-30	- Éves felülvizsgálat.
2.6	2018-03-24	- Teljes felülvizsgálat. - Kisebb módosítások.
2.7	2018-09-15	- Éves felülvizsgálat.
2.8	2018-12-14	- Változások az auditor javaslatai alapján.
2.11	2019-09-25	- Éves felülvizsgálat.
2.13	2020-03-05	- Hatály. - HSM követelmények. - Kisebb pontosítások.
2.14	2020-05-26	- Kisebb pontosítások.
2.17	2020-10-28	- Pontosítások az auditor és a felügyelő hatóság észrevételei alapján. - Kisebb pontosítások.
2.19	2020-12-28	- Szökőmásodpercek kezelése. - Kisebb módosítások.
2.22	2021-06-30	- Megfelelőség értékelés eredményeinek közzététele. - Kisebb pontosítások.

Tartalomjegyzék

1. Bevezetés

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

A *Minősített időbélyegzés-szolgáltató* szolgáltatásait a vele szerződéses viszonyban álló *Ügyfel*ek részére biztosítja.

Jelen *Minősített időbélyegzési szolgáltatási szabályzat* a fenti szolgáltatások nyújtásának kereteit, a részletes eljárási és egyéb működési szabályokat tartalmazza.

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

A *Minősített időbélyegzés-szolgáltató* a bizalmi szolgáltatás nyújtását 2016. július 1-jén jelentette be a Nemzeti Média- és Hírközlési Hatóságnak.

A minősített bizalmi szolgáltatás megfelelőségértékelését független vizsgáló szervezetként a TÜV Informationstechnik GmbH (továbbiakban TÜViT) végezte.

A sikeres megfelelőség értékelési vizsgálat alapján a Nemzeti Média- és Hírközlési Hatóság 2016. december 20-án nyilvántartásba vette és a magyar bizalmi listában [35] publikálta a bejegyzett minősített bizalmi szolgáltatást.

A minősített bizalmi szolgáltatás megfelelőségértékelését független vizsgáló szervezetként 2020. októberétől a Hunguard Kft. (továbbiakban Hunguard) végzi.

A *Minősített időbélyegzés-szolgáltató* az *Ügyfel*ek részére legfontosabb információkat egy Szolgáltatási kivonat formájában is rendelkezésre bocsátja. A Szolgáltatási kivonat a 2.1 fejezetben leírtak szerint kerül publikálásra.

1.1. Áttekintés

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

Jelen *Minősített időbélyegzési szolgáltatási szabályzat* célja, hogy összefoglalja mindazokat az információkat, amelyeket a *Minősített időbélyegzés-szolgáltató*val kapcsolatba kerülő *Ügyfel*eknek tudniuk érdemes. Ezzel elő kívánja segíteni, hogy *Ügyfel*ei és leendő *Ügyfel*ei:

- minél könnyebben megismerhessék a *Minősített időbélyegzés-szolgáltató* által kínált szolgáltatások részleteit, feltételeit és a szolgáltatás nyújtásának gyakorlati hátterét;
- átláthassák a *Minősített időbélyegzés-szolgáltató* működését, és ennek révén minél könnyebben eldönthessék, hogy a szolgáltatások megfelelnek-e, illetve az egyes szolgáltatások melyik típusa felel meg igényeiknek, elvárásaiknak.

Jelen dokumentum feladata továbbá, hogy segítségével a *Minősített időbélyegzés-szolgáltató* által kibocsátott *Időbélyegző*k használói és elfogadói egyértelműen meg tudják állapítani azok kezelésének módját, az általuk garantált biztonság mértékét, valamint a rájuk vonatkozó technikai, üzleti és pénzügyi garanciákat és jogi felelősségvállalásokat.

A végfelhasználóknak az igénybe vett szolgáltatással kapcsolatos tevékenységére vonatkozó előírásokat jelen *Minősített időbélyegzési szolgáltatási szabályzat*on kívül az *Időbélyegzési rend* [37], az Általános Szerződési Feltételek, a szolgáltatóval kötött Szolgáltatási szerződés, illetve egyéb, a *Minősített időbélyegzés-szolgáltató*tól független szabályzat illetve dokumentum is tartalmazhat.

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 időbélyegzés-szolgáltatás szolgáltatási szabályzat
Azonosító	1.3.6.1.4.1.21528.2.1.1.169
Dokumentum verziószáma	2.22
Hatályba lépés ideje	2021-06-30

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

1.2.2. Megfelelés

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

- ETSI EN 319 421 [19] 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 *Minősített időbélyegzés-szolgáltató* az általa kibocsátott *Időbélyegző*kben saját OID azonosítóját szerepelteti, a fenti ETSI időbélyegzési rendet (BTSP) pedig támogatja.

1.2.3. Időbélyegzési rend

A *Minősített időbélyegzési rend*et 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

A jelen *Minősített időbélyegzési szolgáltatási szabályzat* szerint nyújtott bizalmi szolgáltatás megfelel az alábbi *Minősített időbélyegzési rend* követelményeinek:

OID	MEGNEVEZÉS	RÖVID NÉV
1.3.6.1.4.1.21528.2.1.1.186.2.22	eIDAS Rendelet szerinti minősített időbélyegzési rend.	MIR

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

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

A részletes követelményeket az " e-Szignó Hitelesítés Szolgáltató – eIDAS Rendelet szerinti minősített időbélyegzési rend. ver.2.22." [36] dokumentum tartalmazza.

1.2.4. Hatály

Tárgyi hatály

A *Minősített időbélyegzési szolgáltatási szabályzat* az 1.3.1. fejezetben ismertetett szolgáltatások nyújtására és igénybevételére vonatkozik.

Időbeli hatály

A *Minősített időbélyegzési szolgáltatási szabályzat* jelen verziója 2021-06-30 -i hatálybalépési dátumtól visszavonásig hatályos. A hatályosság automatikusan megszűnik a szolgáltatások beszüntetésekor vagy a *Minősített időbélyegzési szolgáltatási szabályzat* újabb verziójának hatályba lépésekor.

Személyi hatály

A *Minősített időbélyegzési szolgáltatási szabályzat* személyi hatálya kiterjed az 1.3. alfejezetben azonosított közösség minden tagjára.

A *Minősített időbélyegzés-szolgáltató* elsősorban az Európai Unió állampolgárai és az Európai Unió területén bejegyzett szervezetek részére nyújtja bizalmi szolgáltatásait, de nem zárja ki szolgáltatásaiból más országok természetes és jogi személyeit sem, amennyiben azok elfogadják a *Minősített időbélyegzés-szolgáltató* által követett szabályrendszert és a szolgáltatások nyújtásához szükséges ellenőrzések kellően biztonságosan és gazdaságosan megvalósíthatók.

Fogyatékkal élők

A *Minősített időbélyegzés-szolgáltató* törekszik arra, hogy az általa nyújtott szolgáltatásokhoz a lehető legmagasabb színvonalon biztosítsa az egyenlő esélyű hozzáférést.

A szolgáltatás esélyegyenlőségének megteremtése érdekében minden lehetséges és ésszerű eszköz alkalmazásával törekszik arra, hogy szolgáltatásai akadálymentesen elérhetőek legyenek a fogyatékkal élő személyek számára is. Különösen fontos számára, hogy a fogyatékkal élő ügyfelek a fogyatékossággal nem érintett ügyfelekkel azonos minőségű, speciális igényeikhez igazodó szolgáltatásban részesülhessenek.

A *Minősített időbélyegzés-szolgáltató* az ügyfelekkel együttműködve, a *Minősített időbélyegzési szolgáltatási szabályzat* által meghatározott keretek között törekszik a személyes igényeknek leginkább megfelelő ügyintézési forma biztosítására.

Területi hatály

A jelen *Minősített időbélyegzési szolgáltatási szabályzat* az európai uniós jogon alapulva a magyar jog alapján Magyarországon nyújtott szolgáltatásokra vonatkozó konkrét követelményeket is tartalmaz.

A *Minősített időbélyegzés-szolgáltató* kiterjesztheti a szolgáltatás területi hatályát, ez esetben a *Minősített időbélyegzési szolgáltatási szabályzat* előírásainak megfelelő, azoknál nem enyhébb követelményeket alkalmaz. A külföldi *Ügyfel*ek számára nyújtott szolgáltatások *Minősített időbélyegzési szolgáltatási szabályzat*tól eltérő részletes feltételeit egyedi Szolgáltatási szerződésben szabályozhatja.

A jelen *Minősített időbélyegzési szolgáltatási szabályzat* szerint nyújtott szolgáltatás az egész világon elérhető. A jelen *Minősített időbélyegzési szolgáltatási szabályzat* szerint kibocsátott *Időbélyegző*k érvényessége független attól, hogy mely földrajzi helyről küldték a kérést, illetve mely földrajzi helyen kívánják azt felhasználni.

A jelen *Minősített időbélyegzési szolgáltatási szabályzat* szerint nyújtott szolgáltatás kizárólag a jelen *Minősített időbélyegzési szolgáltatási szabályzat*ban, valamint a *Időbélyegzési rend*ben leírtak szerint használható fel.

1.3. PKI szereplők

1.3.1. Bizalmi Szolgáltató

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

A *Minősített időbélyegzés-szolgáltató* adatai

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

Ügyfélszolgálati iroda

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

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

A Szolgáltató bemutatása

A Microsec zrt. a 910/2014/EU rendelet [1] (továbbiakban: eIDAS) szerinti EU minősített bizalmi szolgáltató.

A Microsec zrt. (illetve jogelődje, a Microsec Kft.) az elektronikus aláírással kapcsolatos szolgáltatásainak nyújtását a 2001. évi XXXV. törvény [3] (továbbiakban: Eat.) hatálya alatt indította el:

- 2002. május 30-tól kezdve nyújt az Eat. szerinti nem minősített elektronikus aláírás hitelesítés-szolgáltatást, időbélyegzés szolgáltatást és aláírás-létrehozó adat elhelyezése aláírás-létrehozó eszközön szolgáltatást (regisztrációs szám: MH 6834 1/2002);
- 2005. május 15-től kezdve nyújt az Eat. szerinti minősített hitelesítés-szolgáltatást, időbélyegzés szolgáltatást és aláírás-létrehozó adat elhelyezése aláírás-létrehozó eszközön szolgáltatást;
- 2007. február 1-től kezdve nyújt az Eat. szerinti minősített elektronikus archiválás szolgáltatást (a nyilvántartásba vételről szóló határozat ügyiratszáma: HL-3549- 2/2007).

2016. július 1-én az eIDAS és az azt kiegészítő 2015. évi CCXXII törvény [6] hatálybalépésével európai szinten egységesen megváltozott az elektronikus aláírással kapcsolatos szolgáltatások teljes rendszere.

A Microsec 2016. július 1-jétől nyújtja eIDAS Rendelet szerinti nem minősített bizalmi szolgáltatásait, valamint elindította természetes személyek számára az eIDAS Rendelet szerinti minősített aláíró tanúsítványok kibocsátását.

A Microsec 2016. december 20-ától nyújtja az alábbi eIDAS Rendelet szerinti minősített bizalmi szolgáltatásait:

- minősített elektronikus bélyegző tanúsítványok kibocsátása
- minősített elektronikus időbélyegzés
- minősített elektronikus archiválás.

Microsec 2019. január 2-ától nyújtja az alábbi eIDAS Rendelet szerinti minősített bizalmi szolgáltatást:

- minősített weboldal hitelesítő tanúsítvány kibocsátás.

Microsec 2020. május 29-étől nyújtja az alábbi eIDAS Rendelet szerinti minősített bizalmi szolgáltatás komponenst

- minősített elektronikus aláírás/bélyegző létrehozására alkalmas távoli kulcsmenedzsment szolgáltatás.

Minőség és információbiztonság

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

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

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

A Microsec kétszintű kockázatelemzése az információ technológiai kockázatokon túlmenően kiterjed a teljes szervezetre és az üzleti kockázatokra is. A kockázatelemzés legalább évente felülvizsgálatra kerül. A kockázatelemzés eredménye alapján a *Minősített időbélyegzés-szolgáltató*

- intézkedéseket hoz a feltárt sérülékenységek megszüntetésére, és/vagy
- elfogadja az azonosított maradvány kockázatokat a döntés indokainak rögzítésével.

A *Minősített időbélyegzés-szolgáltató* honlapján minden érintett fél számára elérhetővé teszi Információbiztonsági Politikáját az alábbi linken:

`https://www.microsec.hu/hu/biztonsagi-garanciak`

Az Információbiztonsági politika minden változása ily módon kerül publikálásra a web oldalon keresztül.

A *Minősített időbélyegzés-szolgáltató* a szükséges mértékben tájékoztatja a harmadik feleket az Információbiztonsági politika változásairól, beleértve az előfizetőket, az érintett feleket, a tanúsító szervezeteket, a felügyelő és egyéb hatóságokat.

A *Minősített időbélyegzés-szolgáltató* azok bizalmas jellege miat nem hozza nyilvánosságra belső Biztonsági szabályzatait. Alvállalkozót, szerződéses partnereit és az egyéb érintett feleket a szerződés megkötésekor a szükséges mértékben tájékoztatja a rájuk vonatkozó biztonsági szabályokról.

Szolgáltatások

A *Minősített időbélyegzés-szolgáltató* az eIDAS Rendelet [1] által meghatározott alábbi bizalmi szolgáltatásokat nyújthatja az *Előfizető* számára jelen *Minősített időbélyegzési szolgáltatási szabályzat* keretében:

- minősített elektronikus időbélyegző létrehozása

A *Minősített időbélyegzés-szolgáltató* a szolgáltatásokat jelen *Minősített időbélyegzési szolgáltatási szabályzat* keretében minősített bizalmi szolgáltatóként nyújtja.

1.3.2. Ügyfelek

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

1.3.3. Érintett felek

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

1.4. Az időbélyegző felhasználhatósága

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

1.5. A dokumentum adminisztrálása

1.5.1. A dokumentum adminisztrációs szervezete

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

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

1.5.2. Kapcsolattartó személy

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

Kapcsolattartó	Folyamatszervezés részleg vezetője
Szervezet neve	Microsec zrt.
Szervezet címe	Magyarország, H-1033 Budapest, Ángel Sanz Briz út 13.
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 rend*nek való megfelelőségéért felelős személy/szervezet

A jelen *Minősített időbélyegzési szolgáltatási szabályzat*nak a benne meghivatkozott *Minősített időbélyegzési rend*nek való megfelelőségéért felelős személy:

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

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

1.5.4. A Szolgáltatási szabályzat elfogadási eljárása

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

1.6. Fogalmak és rövidítések

1.6.1. Fogalmak

Adatközpont	Számítógépes rendszerek és a hozzájuk kapcsolódó komponensek elhelyezésére és üzemeltetésére kialakított létesítmény. Ezek a komponensek rendszerint magukba foglalják a távközlési rendszereket és kommunikációs kapcsolatokat, redundáns áramforrást, adattárolókat, légkondicionáló, tűzvédelmi és biztonsági rendszereket.
Bizalmi felügyelet	"A *Bizalmi szolgáltatás*ok felügyeletét ellátó hatóság a Nemzeti Média- és Hírközlési Hatóság." (2015. évi CCXXII. törvény [6] 91.§ 1. bekezdés)
Bizalmi szolgáltatás (Trust Service)	"Rendszerint díjazás ellenében nyújtott, az alábbiakból álló elektronikus szolgáltatások: • elektronikus aláírások, elektronikus bélyegzők vagy elektronikus időbélyegzők, ajánlott elektronikus kézbesítési szolgáltatások, valamint az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok létrehozása, ellenőrzése és érvényesítése; vagy • *Weboldal-hitelesítő tanúsítvány*ok létrehozása, ellenőrzése és érvényesítése; vagy • elektronikus aláírások, bélyegzők vagy az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok megőrzése; " (eIDAS [1] 3. cikk 16. pont)

Bizalmi szolgáltatási rend (Trust Service Policy)	"Olyan szabálygyűjtemény, amelyben egy *Bizalmi szolgáltató*, igénybe vevő vagy más személy valamely *Bizalmi szolgáltatás* használatának feltételeit írja elő igénybe vevők valamely közös biztonsági követelményekkel rendelkező csoportja vagy meghatározott alkalmazások számára. " (2015. évi CCXXII. törvény [6] 1. § 8. pont)
Bizalmi szolgáltató (Trust Service Provider)	"Egy vagy több *Bizalmi szolgáltatás*t nyújtó természetes vagy jogi személy; a *Bizalmi szolgáltató* lehet minősített vagy nem minősített *Bizalmi szolgáltató*." (eIDAS [1] 3. cikk 19. pont)
Elektronikus időbélyegző (Electronic Time Stamp)	"Olyan elektronikus adatok, amelyek más elektronikus adatokat egy adott időponthoz kötnek, amivel igazolják, hogy utóbbi adatok léteztek az adott időpontban. " (eIDAS [1] 3. cikk 33. pont)
Előfizető (Subscriber)	A Szolgáltatóval valamely szolgáltatás igénybevétele érdekében Szolgáltatási szerződést kötő személy vagy szervezet.
Érintett fél (Relying Party)	Az *Időbélyegző* elfogadója, aki az *Időbélyegző*t használja.
Gyökér tanúsítvány (Root Certificate)	Más néven legfelső szintű tanúsítvány. Önhitelesített *Tanúsítvány*, amelyet adott *Hitelesítő egység* saját maga számára bocsátott ki, azaz saját magánkulcsával van aláírva, így a saját – a tanúsítványban szereplő – nyilvános kulcsával ellenőrizhető.
Hardver kriptográfiai eszköz (HSM: Hardware Security Module)	Egy olyan hardver alapú biztonságos eszköz, mely előállítja, tárolja és védi a kriptográfiai kulcsokat, valamint biztonságos környezetet biztosít a kriptográfiai funkciók végrehajtására.
Hitelesítés-szolgáltató	Olyan *Bizalmi szolgáltató*, aki/amely a hitelesítés-szolgáltatás keretében azonosítja az igénylő személyét, *Tanúsítvány*t bocsát ki, nyilvántartásokat vezet, fogadja a *Tanúsítvány*okkal kapcsolatos változások adatait, valamint nyilvánosságra hozza a *Tanúsítvány*hoz tartozó szabályzatokat, és a *Tanúsítvány* aktuális állapotára (különösen esetleges visszavonására) vonatkozó információkat.

Hitelesítő egység	A *Hitelesítés-szolgáltató* rendszerének egy egysége, amely *Tanúsítvány*ok elektronikus aláírását vagy bélyegzését végzi. Egy *Hitelesítő egység*hez mindig egy elektronikus aláírás vagy bélyegző létrehozásához használt adat (magánkulcs) tartozik. Előfordulhat, hogy egy *Hitelesítés-szolgáltató* egyszerre több *Hitelesítő egység*et is működtet.
Időbélyegzési rend	Olyan *Bizalmi szolgáltatási rend*, amelyben egy szolgáltató, igénybe vevő vagy más személy (szervezet) valamely *Időbélyegző* felhasználásának feltételeit írja elő az igénybe vevők valamely közös biztonsági követelményekkel rendelkező csoportja, illetőleg meghatározott alkalmazások számára.
Időbélyegzés-szolgáltató	Olyan *Bizalmi szolgáltató*, amely *Bizalmi szolgáltatás* keretében *Időbélyegző*ket bocsát ki, és ellátja az ehhez kapcsolódó feladatokat.
Időbélyegző egység	Az *Időbélyegzés-szolgáltató* rendszerének egy egysége, amely az *Időbélyegző*k aláírását vagy bélyegzését végzi. Egy időbélyegző egységhez mindig egy elektronikus aláírás vagy bélyegző létrehozáshoz használt adat tartozik. Előfordulhat, hogy egy *Időbélyegzés-szolgáltató* egyszerre több időbélyegző egységet is működtet.
Kompromittálódás	Egy kriptográfiai kulcs abban az esetben tekintendő kompromittálódottnak, ha vélelmezhető, hogy illetéktelen személynek is hozzáférése van hozzá.
Köztes hitelesítő egység	Olyan *Hitelesítő egység* amelynek *Tanúsítvány*át egy másik *Hitelesítő egység* bocsátotta ki.
Kriptográfiai kulcs (Cryptographic Key)	Olyan – kriptográfiai transzformációt vezérlő – egyedi digitális jelsorozat, amelynek ismerete szükséges titkosításhoz és dekódoláshoz, illetve elektronikus aláírás vagy bélyegző előállításához és ellenőrzéséhez.
Kulcsgondozás (Key Management)	A kriptográfiai kulcsok előállítása, a felhasználókhoz történő eljuttatása vagy ennek algoritmikus megvalósítása, továbbá a kulcsok nyilvántartása, tárolása, archiválása, visszavonása, törlése, amely szoros kapcsolatban áll az alkalmazott biztonsági eljárásmóddal.
magánkulcs	A Nyilvános kulcsú infrastruktúrában egy szereplőhöz tartozó aszimmetrikus kriptográfiai kulcspár azon eleme, amelyet az *Alany*nak szigorúan titokban kell tartania. A *Hitelesítés-szolgáltató* a *Tanúsítvány*ok kibocsátása során a *Hitelesítő egység* magánkulcsát használja arra, hogy a *Tanúsítvány*t védő elektronikus aláírást vagy bélyegzőt elhelyezze rajta.

Minősített bizalmi szolgáltatás (Qualified Trust Service)	"Olyan *Bizalmi szolgáltatás* amely megfelel az eIDAS Rendeletben foglalt alkalmazandó követelményeknek." (eIDAS [1] 3. cikk 17. pont)
Minősített bizalmi szolgáltató (Qualified Trust Service Provider)	"Olyan *Bizalmi szolgáltató* amely egy vagy több *Minősített bizalmi szolgáltatás*t 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 *Tanúsítvány* formájában történik, amely összekapcsolja a szereplő nevét az ő nyilvános kulcsával. A *Tanúsítvány*ok hitelességét az őket kibocsátó *Hitelesítő egység* nyilvános kulcsa segítségével lehet ellenőrizni.
Nyilvános kulcsú infrastruktúra (Public Key Infrastructure, PKI)	Aszimmetrikus kulcsú kriptográfiára épülő infrastruktúra, beleértve a kriptográfiai algoritmusokat, kulcsokat, tanúsítványokat, a rájuk vonatkozó szabványokat és jogszabályokat, a mögöttes intézményrendszert, a különböző szolgáltatókat és eszközöket is.
Rendkívüli üzemeltetési helyzet	Olyan, a *Minősített időbélyegzés-szolgáltató* üzemmenetében zavart okozó rendkívüli helyzet, amikor a *Minősített időbélyegzés-szolgáltató* rendes üzemmenetének folytatására ideiglenesen vagy véglegesen nincsen lehetőség.
Szervezet	Jogi személy.
Szolgáltatási szabályzat (Trust Service Practice Statement)	"A *Bizalmi szolgáltató* nyilatkozata az egyes *Bizalmi szolgáltatás*ok nyújtásával kapcsolatosan alkalmazott részletes eljárási vagy más működési követelményekről. " (2015. évi CCXXII. törvény [6] 1. § 41. pont)
Szolgáltatási szerződés	"A *Bizalmi szolgáltató* és a *Bizalmi szolgáltatás*i ügyfél között létrejött szerződés, amely a *Bizalmi szolgáltatás* nyújtására és a szolgáltatás igénybevételére vonatkozó feltételeket tartalmazza. " (2015. évi CCXXII. törvény [6] 1. § 42. pont)

Tanúsítvány (Certificate)	"Az elektronikus aláírás tanúsítvány, az elektronikus bélyegző tanúsítvány és a *Weboldal-hitelesítő tanúsítvány*, valamint mindazon, a *Bizalmi szolgáltatás* keretében a szolgáltató által kibocsátott elektronikus igazolás, amely tartalmazza a tanúsítványra vonatkozó érvényesítési adatot és a tanúsítvány használatához szükséges kapcsolódó adatokat, és amely elektronikus dokumentum megbízhatóan védve van a kibocsátáskor és az érvényességi ideje alatt rendelkezésre álló technológiákkal elkövetett hamisítás ellen. " (2015. évi CCXXII. törvény [6] 1. § 44.)
Tanúsítványkérelem	Az *Igénylő* által, a Szolgáltató számára a *Tanúsítvány* kibocsátás érdekében benyújtott adatok és nyilatkozatok, amelyekben többek között az *Igénylő* megerősíti a *Tanúsítvány*ba kerülő adatok valódiságát.
Tanúsítványtár	Különböző *Tanúsítvány*okat tartalmazó adattár. Tanúsítványtára van egy Szolgáltatónak is, amelyben az általa kibocsátott *Tanúsítvány*okat publikálja, de Tanúsítványtárnak nevezzük az *Érintett fél* számítógépén a használt alkalmazás számára elérhető *Tanúsítvány*okat tartalmazó rendszert is.
Ügyfél	Az *Előfizető* másik elnevezése.
Visszavonás	A *Tanúsítvány* érvényességének megszüntetése a *Tanúsítvány*ban is feltüntetett érvényességi idő lejárta előtt. A *Tanúsítvány* visszavonása végleges, visszavont *Tanúsítvány* többet nem tehető érvényessé.
Visszavonási állapot nyilvántartás	A *Hitelesítés-szolgáltató* által vezetett belső nyilvántartás a felfüggesztett, illetőleg a visszavont *Tanúsítvány*okról, amelyek tartalmazzák legalább a felfüggesztés vagy visszavonás tényét, és a felfüggesztés vagy visszavonás időpontját másodperc pontossággal.

1.6.2. Rövidítések

CRL	Certificate Revocation List	Tanúsítvány visszavonási lista
eIDAS	electronic Identification, Authentication and Signature	A 910/2014/EU rendelet általánosan használt hivatkozása
GMT	Greenwich Mean Time	Greenwichi középidő
IERS	International Earth Rotation and reference System Service	Nemzetközi Földforgás és Referenciarendszer Szolgálat
LDAP	Lightweight Directory Access Protocol	Protokoll címtár szolgáltatás eléréséhez
NMHH		Nemzeti Média- és Hírközlési Hatóság
OCSP	Online Certificate Status Protocol	Online tanúsítvány-állapot protokoll
OID	Object Identifier	Objektum azonosító

PKI	Public Key Infrastructure	Nyilvános kulcsú infrastruktúra
TAI	International Atomic Time	Nemzetközi atomidő
TSA	Time Stamping Authority	Időbélyegzés szolgáltató
TSP	Trust Service Provider	Bizalmi szolgáltató
TSU	Time-Stamping Unit	Időbélyegző Egység
TDS	TSA Disclosure Statement	TSA Közzétételi nyilatkozat
UTC	Coordinated Universal Time	Egyezményes koordinált világidő

2. Közzététel és adattár felelősségek

2.1. Adattárak

A *Minősített időbélyegzés-szolgáltató* nyilvánosságra hozza szerződéses feltételeit és szabályzatait a honlapján elektronikus formában az alábbi linken:

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

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

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

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

A *Minősített időbélyegzés-szolgáltató* a szerződéskötést követően weboldalán publikálva teszi letölthetővé elektronikusan aláírt PDF fájl formájában az *Ügyfél* részére az Általános Szerződési Feltételeket, a *Szolgáltatási kivonat*ot, a *Minősített időbélyegzési rend*et és a *Minősített időbélyegzési szolgáltatási szabályzat*ot. A *Minősített időbélyegzés-szolgáltató* az egyedi Szolgáltatási szerződést papír alapon kézi aláírással és pecséttel hitelesítve, vagy minősített elektronikus aláírással ellátott PDF formátumú elektronikus dokumentum formájában bocsátja az *Ügyfél* rendelkezésére.

A *Minősített időbélyegzés-szolgáltató* értesíti *Ügyfel*eit az Általános Szerződési Feltételek változásáról.

2.2. A tanúsítványokra vonatkozó információk közzététele

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

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 [38] 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 szolgáltatás csak a *Minősített időbélyegzés-szolgáltató Előfizető*i által vehető igénybe az *Előfizető* sikeres azonosítását követően.

Az azonosítás az igénybevett szolgáltatástól függően az *Előfizető*nek kiadott autentikációs tanúsítvánnyal vagy felhasználónévvel és jelszóval történik. Az egyes elérési módokhoz eltérő URL tartozik az alábbiak szerint:

Alapértelmezett minősített időbélyegzés szolgáltatás elérhetősége

Általános (standard) felhasználás:

- Felhasználónév és jelszó: `https://btsa.e-szigno.hu/tsa`
- Autentikációs tanúsítvány: `https://tsa.e-szigno.hu/tsa`

Nagyfogyasztói (high) felhasználás:

- Felhasználónév és jelszó: `https://btsa2.e-szigno.hu/tsa`
- Autentikációs tanúsítvány: `https://tsa2.e-szigno.hu/tsa`

Korlátozott (low) felhasználás:

- Felhasználónév és jelszó: `https://btsa3.e-szigno.hu/tsa`
- Autentikációs tanúsítvány: `https://tsa3.e-szigno.hu/tsa`

RSA alapú minősített időbélyegzés szolgáltatás elérhetősége

Az időbélyegző tanúsítvány érvényességi ideje 2022. december 30.
Általános (standard) felhasználás:

- Felhasználónév és jelszó: `https://btsa.e-szigno.hu/tsa-rsa`
- Autentikációs tanúsítvány: `https://tsa.e-szigno.hu/tsa-rsa`

Nagyfogyasztói (high) felhasználás:

- Felhasználónév és jelszó: `https://btsa2.e-szigno.hu/tsa-rsa`
- Autentikációs tanúsítvány: `https://tsa2.e-szigno.hu/tsa-rsa`

Korlátozott (low) felhasználás:

- Felhasználónév és jelszó: `https://btsa3.e-szigno.hu/tsa-rsa`
- Autentikációs tanúsítvány: `https://tsa3.e-szigno.hu/tsa-rsa`

ECC alapú minősített időbélyegzés szolgáltatás elérhetősége

Általános (standard) felhasználás:

- Felhasználónév és jelszó: `https://btsa.e-szigno.hu/tsa-ecc`
- Autentikációs tanúsítvány: `https://tsa.e-szigno.hu/tsa-ecc`

Nagyfogyasztói (high) felhasználás:

- Felhasználónév és jelszó: `https://btsa2.e-szigno.hu/tsa-ecc`
- Autentikációs tanúsítvány: `https://tsa2.e-szigno.hu/tsa-ecc`

Korlátozott (low) felhasználás:

- Felhasználónév és jelszó: `https://btsa3.e-szigno.hu/tsa-ecc`
- Autentikációs tanúsítvány: `https://tsa3.e-szigno.hu/tsa-ecc`

A szolgáltatás hozzáférési ponton keresztül a *Minősített időbélyegzés-szolgáltató* csak minősített *Időbélyegző*ket bocsát ki.

3.2. Az Időbélyegző egység tanúsítványa

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

A *Időbélyegző egység Tanúsítvány*át a Microsec e-Szignó Hitelesítés Szolgáltató adja ki, amely az eIDAS szerinti minősített *Bizalmi szolgáltató*ként az ETSI EN 319 411-1 [13] és az ETSI EN 319 411-2 [14] szerinti bizalmi szolgáltatást is nyújt.

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

- az adott magánkulcshoz tartozó *Tanúsítvány* már publikálásra került a nemzeti Bizalmi szolgáltatói listán [35];
- a *Tanúsítvány* aláírását ellenőrizte a megbízható *Hitelesítés-szolgáltató*ig visszavezetett teljes érvényességi láncon;
- meggyőződött a magánkulcs és a *Tanúsítvány*ban publikált nyilvános kulcs összetartozásáról;
- az adott magánkulcshoz tartozó *Tanúsítvány* már feltöltésre került az *Időbélyegző egység*be.

Az Időbélyegző egység megnevezése

- commonName (CN) – OID: 2.5.4.3
  A mező tartalmazza az *Időbélyegző egység* típusának megnevezését, a kulcs generálás évét és egy az adott éven belüli sorszámot. Az *Időbélyegző egység* típusa az alábbiak valamelyike lehet:
  - "Qualified eIDAS e-Szigno TSA"
  - "e-Szigno Qualified TSA"
- Organization (O) – OID: 2.5.4.10
  "Microsec Ltd."
  Időbélyegzés-szolgáltató neve angolul, ékezet nélkül.
- Organization Identifier (OrgId) – OID: 2.5.4.97
  "VATHU-23584497"
  Időbélyegzés-szolgáltató adószáma.

  Kitöltése opcionális.
- Organizational Unit (OU) – OID: 2.5.4.11
  Nem kerül kitöltésre.
- Locality (L) – OID: 2.5.4.7
  "Budapest"
  Időbélyegzés-szolgáltató székhelye szerinti város neve ékezet nélkül.

- CountryName (C) – OID: 2.5.4.6
  "HU"
  Az *Időbélyegzés-szolgáltató* székhelye szerinti ország ISO 3166-1 [23] szerinti kétbetűs kódja.
- Email address (EMAIL) – OID: 1.2.840.113549.1.9.1
  Nem kerül kitöltésre.

Az Időbélyegző egység alternatív nevei

A mező nem szerepel az *Időbélyegző egység* számára kibocsátott *Tanúsítvány*ban.

3.3. Az Időbélyegző

A *Minősített időbélyegzés-szolgáltató* által kibocsátott *Időbélyegző* megfelel az IETF RFC 3161 [26], az IETF RFC 5816 [29] és az ETSI EN 319 422 [20] szabványoknak;
Ennek megfelelően az *Időbélyegző* jellemzői:

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

Az *Időbélyegző egység*ek a *Minősített időbélyegzés-szolgáltató* biztonságos *Adatközpont*jában működnek, ami garantálja az *Időbélyegző*ben megadott időértékek megfelelőségét (lásd 6. fejezet).
Az *Időbélyegző egység*(ek) *Időbélyegző*k kibocsátásához használt belső órája visszavezethető az UTC pontos időre (lásd 3.4. fejezet).
Az *Időbélyegző*ben megadott időpont pontossága megfelel az *Időbélyegzési rend*ben meghatározott követelményeknek (lásd 3.4. fejezet). A vállalt pontosság magában az *Időbélyegző*ben is feltüntetésre kerül (lásd 3.3.2. fejezet).
Az *Időbélyegző egység* nem bocsát ki *Időbélyegző*t, amint észleli hogy a belső óra pontossága a megadott mértéket meghaladóan eltér a UTC szerinti pontos időtől (lásd 3.4. fejezet).
A *Minősített időbélyegzés-szolgáltató* az *Időbélyegző egység*ek magánkulcsait az *Időbélyegző*k hitelesítésétől eltérő célra nem használja (lásd 6.1.2. fejezet).
A kulcsok élettartamának lejárta után a magánkulcsok törlésre kerülnek a 6.3.1. fejezetben leírtak szerint, így a *Időbélyegző egység*ek nem tudnak *Időbélyegző*t kibocsátani a lejárt magánkulccsal.

3.3.1. Időbélyegző kérés

A *Minősített időbélyegzés-szolgáltató* támogatja az IETF RFC 3161 [26] 2.4.1. fejezete szerinti *Időbélyegző* kéréseket beleértve az alábbi mezők használatát:

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

- "extensions"

A *Minősített időbélyegzés-szolgáltató* az ETSI TS 119 312 [21] szerinti és az aktuális Nemzeti Média- és Hírközlési Hatóság algoritmusokkal kapcsolatos határozatban kijelölt lenyomatképző algoritmusokat fogad be az *Időbélyegző* kérésekben. A lenyomatképző algoritmusok kiválasztásánál figyelembe veszi az *Időbélyegző* tervezett felhasználási idejét és a lenyomatképző függvény várható megfelelőségi időtartamát.

A jelenleg támogatott lenyomatképző algoritmusok:

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

Az időbélyegző kérés felépítése

- Verzió (Version)
  Az Időbélyegző kérés formátuma az IETF RFC 3161 [26] szerinti "v1" verziónak felel meg, így a mezőbe az "1" érték kerül.
- Üzenet lenyomat (MessageImprint)
  Az *Időbélyegző*vel ellátandó adat, ami két részből áll:
  - Lenyomatképző algoritmus (hashAlgorithm)
    A lenyomatképző algoritmus OID azonosítója, amellyel a lenyomat készült
  - Lenyomat (hashedMessage)
    maga a lenyomat, amit el kell látni *Időbélyegző*vel. Az adat hossza megfelel a megadott lenyomatképző algoritmusnak.
- *Minősített időbélyegzési rend* azonosító (reqPolicy)
  opcionális mező
  Azt mondja meg, hogy az *Időbélyegző*t milyen *Minősített időbélyegzési rend* szerint kérik kibocsátani.
- Nonce (nonce)
  opcionális mező
  Maximum 64 bites egész szám, az *Időbélyegző* egyediségének biztosítására szolgál. A "nonce" szerepeltetése esetén a válaszban ugyanennek az értéknek kell szerepelnie.
- Tanúsítvány igénylése (certReq)
  alapértelmezetten "FALSE"
  Amennyiben a kérésben "TRUE " értékkel szerepel, a válaszban meg kell küldeni a "SigningCertificate attribute" attributumban hivatkozott *Időbélyegző egység Tanúsítvány*t.
- Kiterjesztések (extensions)
  opcionális mező
  Az igénylő itt adhat meg plusz információt. A *Minősített időbélyegzés-szolgáltató* kizárólag a (Qualified Certificate Statements) kiterjesztés használatát támogatja. Amennyiben más kiterjesztést tartalmazó kérés érkezik, a *Minősített időbélyegzés-szolgáltató* nem bocsát ki *Időbélyegző*t, helyette a válaszban "unacceptedExtension" hibaüzenetet küld vissza.

3.3.2. Időbélyegző válasz

A *Minősített időbélyegzés-szolgáltató* támogatja az IETF RFC 3161 [26] 2.4.2. fejezete szerinti *Időbélyegző* válaszokat az alábbi kiegészítésekkel:

- "accuracy";
- "nonce".

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

A *Minősített időbélyegzés-szolgáltató* az ETSI TS 119 312 [21] szerinti és az aktuális Nemzeti Média- és Hírközlési Hatóság algoritmusokkal kapcsolatos határozatban kijelölt kriptográfiai algoritmuskészleteket és kulcshosszakat használ az *Időbélyegző*k aláírására. A kriptográfiai algoritmuskészletek és kulcshosszak kiválasztásánál figyelembe veszi az *Időbélyegző* tervezett felhasználási idejét.

A támogatott kriptográfiai algoritmuskészlet:

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

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

Az időbélyegző válasz felépítése

- státusz (PKIStatusInfo)
  Az IETF RFC 3161 [26] 2.4.2 fejezet szerinti státusz információ a kibocsátás sikerességéről.
- *Időbélyegző* token (TimeStampToken)
  opcionális mező
  A státusz mező "0" vagy "1" értéke esetén tartalmazza a kibocsátott *Időbélyegző*t, egyéb státusz érték esetén a mező nem szerepel a válaszban.

Az időbélyegző token felépítése

Az IETF RFC 3161 [26] 2.4.2 fejezet szerinti, az *Időbélyegző egység* által aláírt *Időbélyegző* token, amelynek mezői:

- Verzió (version)
  Az *Időbélyegző* token formátuma az IETF RFC 3161 [26] szerinti "v1" verziónak felel meg, így a mezőbe az "1" érték kerül.

- *Minősített időbélyegzési rend* azonosító (policy)
  kötelező mező
  Azt mondja meg, hogy az *Időbélyegző*t milyen *Minősített időbélyegzési rend* szerint bocsátották ki. Amennyiben a "reqPolicy" mező szerepelt a kérésben is, csak a kérésnek megfelelő OID támogatása esetén bocsátható ki *Időbélyegző*, egyéb esetben a kérés "unacceptedpolicy" hibaüzenettel elutasításra kerül.

- Üzenet lenyomat (messageImprint)
  Az *Időbélyegző*vel ellátott adat a kéréssel egyező tartalommal.

- sorszám (serialNumber)
  kötelező mező
  Az *Időbélyegző egység* által kibocsátott valamennyi *Időbélyegző*re egyedi sorszám az egység teljes élettartama alatt. Maximális mérete 160 bit.

- Idő (genTime)
  kötelező mező
  UTC formában megadott időpont, amelyben az *Időbélyegző*t kibocsátották. A *Minősített időbélyegzés-szolgáltató* által kibocsátott *Időbélyegző*kben a "genTime" érték másodperc pontossággal kerül megadásra az RFC 5280 [28] szerint.

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

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

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

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

- Kiterjesztések (extensions)

  A *Minősített időbélyegzés-szolgáltató* az általa kibocsátott valamennyi *Időbélyegző*ben szerepelteti ezt a kiterjesztést.

  A *Minősített időbélyegzés-szolgáltató* az *Időbélyegző* eIDAS szerinti minősített státuszának jelzésére az alábbi kiterjesztést használja:

– Minősített tanúsítvánnyal kapcsolatos állítások (Qualified Certificate Statements) – nem kritikus
OID: 1.3.6.1.5.5.7.1.3
A kiterjesztésben egyetlen állítás szerepel: "esi4-qtstStatement-1"
OID: 0.4.0.19422.1.1

3.4. Az Időbélyegzőben szereplő idő pontossága

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

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

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

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

3.5. Óraszinkronizálás

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

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

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

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

3.5.1. A szökőmásodpercek kezelése

Szökőmásodperc előfordulásakor a *Minősített időbélyegzés-szolgáltató* elvégzi az óraszinkronizációt az illetékes szervezet előzetes értesítése alapján a megadott időpontban az ETSI 319 421 [19] C függelékében meghatározottak szerint az ITU-R TF.460-6 [32] ajánlásnak megfelelően.

A pozitív szökőmásodperc az adott nap 23:59:59 UTC után következik be, az időmérés 1 másodpercre leáll, majd folytatódik az időmérés a szokásos, következő napi 00:00:00 UTC idővel.

Negatív szökőmásodperc esetén az adott nap 23:59:58 UTC után kimarad a 23:59:59 UTC másodperc és rögtön a következő napi 00:00:00 UTC következik.

3.5.2. Nyári időszámítás kezelése

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

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

3.6. Az Időbélyegző ellenőrzése

Az *Időbélyegző*n szereplő elektronikus aláírás vagy elektronikus bélyegző érvényességének ellenőrzése során az *Érintett fél*nek célszerű az ETSI EN 319 102-1 [10] specifikációban leírtak szerint eljárnia.

Az *Időbélyegző* ellenőrzése során:

- ellenőrizni kell, hogy összetartozik-e az időbélyegzett dokumentum az *Időbélyegző*vel és a *Minősített időbélyegzés-szolgáltató Tanúsítvány*ával;
- ellenőrizni kell az *Időbélyegző*n szereplő aláírást;
- ellenőrizni kell, hogy az *Időbélyegző* megfelel-e az adott célra, többek között, hogy pontossága, megbízhatósága, valamint a hozzá kapcsolódó Időbélyegzés-szolgáltatói felelősségvállalás megfelelő.

3.7. A szolgáltatás rendelkezésre állása

A *Minősített időbélyegzés-szolgáltató* biztosítja a szolgáltatás, valamint a *Minősített időbélyegzés-szolgáltató* által kibocsátott *Időbélyegző*k 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 *Időbélyegző*ket kibocsátó *Időbélyegző egység* nem bocsáthat ki nem minősített *Időbélyegző*ket.

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

3.9. Az Időbélyegző egység kulcshasználata

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

- csak olyan algoritmusokat és kulcsméreteket használnak az *Időbélyegző*k hitelesítésére, amelyek megfelelnek az alábbi követelményeknek:
  - ETSI TS 119 312 [21];

  - a 2015. évi CCXXII törvény [6] 92. § (1) b) szerint kiadott aktuális Nemzeti Média- és Hírközlési Hatóság algoritmusokkal kapcsolatos határozat.

- az aláíró vagy bélyegző létrehozó magánkulcsot lehetőleg ne importálják egyszerre több *HSM eszköz*be;
- amennyiben több *HSM eszköz* is ugyanazt az aláíró vagy bélyegző létrehozó magánkulcsot használja, akkor azoknak ugyanahhoz a *Tanúsítvány*hoz kell tartozniuk;
- egy *Időbélyegző egység*ben egyidőben csak egy *Időbélyegző* aláíró vagy bélyegző létrehozó magánkulcs lehet aktív;
- egy hardver-szoftver egység több különböző *Időbélyegző egység*et is kiszolgálhat a fenti követelmények betartása esetén.

3.10. Az Időbélyegző szolgáltatás elérési módjai

A 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 Tanúsítvány*a alapján.
- autentikációs *Tanúsítvány* alapú felhasználó azonosítás esetén a kliens és a szerver *Tanúsítvány*ok 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 *Időbélyegző*k hitelesítésére használható, a magánkulcs más célú felhasználása tilos.

4.1.2. Az Érintett felek nyilvános kulcs és tanúsítvány használata

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

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

5. Elhelyezési, eljárásbeli és üzemeltetési előírások

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

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

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

5.1. Fizikai követelmények

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

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

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

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

A megfelelő védelem biztosítása érdekében:

- A *Minősített időbélyegzés-szolgáltató* védett számítógéptermében valósítja meg a szigorúbban védendő szolgáltatásokat. Ez a számítógépterem speciálisan erre a célra lett tervezve és kialakítva, tervezésénél különböző védelmi szempontok [a telephely elhelyezése és szerkezeti felépítése, a fizikai hozzáférés (beléptetés ellenőrzése és felügyelete), áramellátás, légkondicionálás, beázás és elárasztódás elleni védekezés, tűzmegelőzés és tűzvédelem, adathordozók tárolása stb.] egységes érvényesítésére került sor.
- A *Minősített időbélyegzés-szolgáltató* valamennyi kritikus szolgáltatását egy külön biztonsági zónában valósítja meg, az ehhez szükséges valamennyi eszközt egy – a biztonsági zóna részét képező – védett számítógépteremben helyezi el.

5.1.1. A telephely elhelyezése és szerkezeti felépítése

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

5.1.2. Fizikai hozzáférés

A *Minősített időbélyegzés-szolgáltató* védi a szolgáltatás nyújtásában részt vevő eszközeit és berendezéseit a jogosulatlan fizikai hozzáféréstől az eszközök manipulálásának megakadályozása érdekében. A *Minősített időbélyegzés-szolgáltató* biztosítja, 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 rendszer-adminisztrátornak 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 géptermen belül sem tárolhatók nyílt formában.

Jogosulatlan személyek jelenlétében:

- a bizalmas adatokat tartalmazó adathordozókat fizikailag elzárva tartják;
- a bejelentkezett terminálokat nem hagyják felügyelet nélkül;
- nem végeznek olyan munkafolyamatot, amely során bizalmas adat felfedésre kerülhet.

A gépterem elhagyásakor az adminisztrátornak ellenőriznie kell, hogy:

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

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

5.1.3. Áramellátás és légkondicionálás

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

- megfelelő teljesítménnyel rendelkezik az adatközpont informatikai és a kisegítő létesítményi rendszerei áramellátásának biztosítására;
- megvédi az informatikai berendezéseket a külső hálózatból érkező feszültség ingadozások, feszültség kimaradások, tüskék és egyéb zavarok ellen;

- tartós áramszünet esetére saját áramtermelő berendezéssel rendelkezik, amely - üzemanyag utántöltést lehetővé téve - tetszőleges időtartamig képes a szükséges energia biztosítására.

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

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

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

5.1.4. Beázás és elárasztódás veszély kezelése

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

5.1.5. Tűz megelőzés és tűzvédelem

A *Minősített időbélyegzés-szolgáltató Adatközpont*jában az illetékes tűzoltóparancsnokság által jóváhagyott tűzvédelmi rendszer működik. A füst és tűzérzékelők vészhelyzet esetén automatikusan riasztják a tűzoltóságot. A gépteremben vízpára alapú, automatikus tűzoltó rendszer lett kialakítva, amely az emberi életre nem veszélyes és nem károsítja az informatikai eszközöket sem.

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

5.1.6. Adathordozók tárolása

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

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

5.1.7. Hulladék megsemmisítése

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

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

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

5.1.8. A mentési példányok fizikai elkülönítése

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

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

5.2. Eljárásbeli előírások

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

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

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

5.2.1. Bizalmi szerepkörök

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

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

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

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

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

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

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

A bizalmi szerepkörök ellátására a *Minősített időbélyegzés-szolgáltató* biztonságért felelős vezetője formálisan kinevezi 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 a *Minősített időbélyegzés-szolgáltató* naprakész nyilvántartást vezet, a változásokat haladéktalanul bejelenti a Nemzeti Média- és Hírközlési Hatóságnak.

5.2.2. Az egyes feladatok ellátásához szükséges személyzeti létszámok

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

- a *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 felhasználók egyedi azonosító adatokkal rendelkeznek, amely lehetővé teszi a felhasználók biztonságos azonosítását és hitelesítését.

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

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

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

5.2.4. Egymást kizáró szerepkörök

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

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

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

5.3. Személyzetre vonatkozó előírások

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

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

5.3.1. Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

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

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 (matematikusi, fizikusi egyetemi végzettség vagy a műszaki tudományterületre tartozó mérnöki szakon szerzett főiskolai vagy egyetemi végzettség);
- legalább három év, az informatikai biztonsággal összefüggésben szerzett szakmai gyakorlattal.

5.3.2. Előélet vizsgálatára vonatkozó eljárások

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

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

Kinevezéskor a *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* a felvételi eljárás során ellenőrzi a jelentkező önéletrajzában megadott releváns információk valódiságát, úgy mint előző munkahely, szakmai referenciák, legfontosabb képzettség.

5.3.3. Képzési követelmények

A *Minősített időbélyegzés-szolgáltató* az újonnan felvett alkalmazottakat képzésben részesíti, 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 kapnak hozzáférési jogosultságot.

5.3.4. Továbbképzési gyakoriságok és követelmények

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

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

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

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

5.3.5. Munkabeosztás körforgásának sorrendje és gyakorisága

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

5.3.6. Felhatalmazás nélküli tevékenységek büntető következményei

A *Minősített időbélyegzés-szolgáltató* a dolgozókkal kötendő munkaszerződésben szabályozza a dolgozók felelősségre vonásának lehetőségeit a dolgozó által elkövetett mulasztások, hibák, vétlen vagy szándékos károkozások esetére. Amennyiben egy munkatárs – szándékosan vagy gondatlanul – kötelezettségeit megsérti, vele szemben a *Minősített időbélyegzés-szolgáltató* szankciót alkalmazhat, amelyet az elkövetés módjára és következményeire tekintettel állapít meg. Szankcióként

alkalmazható a jutalom megvonása, fegyelmi eljárás, elbocsátás, kinevezés visszavonása vagy büntetőjogi felelősségre vonás kezdeményezése.

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

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

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

5.3.7. Szerződéses viszonyban foglalkoztatottakra vonatkozó követelmények

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

Az egyéb feladatok ellátására alvállalkozói vagy megbízásos szerződésben foglalkoztatott szerződő személyeket a *Minősített időbélyegzés-szolgáltató* lehetőség szerint a korábban már minősített beszállítók listájáról választ. A beszállítókkal a *Minősített időbélyegzés-szolgáltató* a munkavégzést megelőzően írásban szerződést köt.

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

5.3.8. A személyzet számára biztosított dokumentációk

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

Minden bizalmi munkakört betöltő munkatárs írásban megkapja a következő dokumentumokat:

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

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

5.4. Naplózási eljárások

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

5.4.1. A tárolt események típusai

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

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

Minden új naplóbejegyzés hozzáadódik a korábban elmentett bejegyzésekhez, az egyszer már elmentett bejegyzés nem kerülhet módosításra vagy törlésre.

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

A *Minősített időbélyegzés-szolgáltató* naplózza minimálisan az alábbi eseményeket:

- BELSŐ ÓRA
  - a belső óra szinkronizációja az UTC időhöz, beleértve az üzemszerű újrakalibrálásokat is;
  - a szinkronizáció elvesztése;
- IDŐBÉLYEGZÉS
  - az *Időbélyegző*k 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 egység*ek *Tanúsítvány*ainak kibocsátásával, állapotváltozásával kapcsolatos minden esemény;

- ADATMOZGÁSOK
  - bármilyen, a biztonság szempontjából kritikus adat manuális bevitele a rendszerbe;
  - a rendszer által fogadott, biztonsági szempontból fontos adatok, üzenetek;

- *HSM 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;
  - szoftver telepítése, frissítése vagy eltávolítása a *Minősített időbélyegzés-szolgáltató* rendszerében;

- 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 RENDELLENESSÉGEK
  - rendszerösszeomlás, hardver hiba;
  - szoftveres hibák;
  - szoftverintegritás ellenőrzési hiba;
  - hibás vagy rossz helyre továbbított üzenetek;
  - hálózatot ért támadások, támadási kísérletek;
  - berendezés hiba;
  - elektromos hálózati üzemzavar;
  - szünetmentes tápegység hiba;
  - lényeges hálózati szolgáltatás hozzáférési hiba;
  - a *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* független rendszervizsgálói a keletkezett naplóbejegyzéseket minden munkanapon átvizsgálják.

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

Az informatikai rendszerek ellenőrzésére a *Minősített időbélyegzés-szolgáltató* automatizált ellenőrző rendszereket is használ, amelyek előre beállított szempontok szerint folyamatosan figyelik a keletkező naplóbejegyzéseket és szükség esetén riasztják az üzemeltetés munkatársait. Az automatizált ellenőrző rendszerekből kapott értesítéseket az IT üzemeltetés munkatársai 24 órán belül feldolgozzák és az eredményeket kiértékelik.

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

5.4.3. A naplófájl megőrzési időtartama

Az online rendszerből való kitörlés előtt a naplóállományokat a *Minősített időbélyegzés-szolgáltató* archiválja és gondoskodik azok biztonságos megőrzéséről az 5.5.2 fejezetben meghatározott ideig, de legalább a keletkezésüktől számított 10 évig.

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

5.4.4. A naplófájl védelme

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

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

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

A naplóállományt a véletlen és szándékos rongálások ellen biztonsági mentések védik. A személyes adatokat tartalmazó naplóbejegyzések esetében a *Minősített időbélyegzés-szolgáltató* gondoskodik az adatok bizalmas tárolásáról. A naplóállományokhoz való hozzáférésre csak azok jogosultak, akiknek erre munkakörük folytán feltétlenül szükségük van. A *Minősített időbélyegzés-szolgáltató* a hozzáféréseket biztonságos módon ellenőrzi. A naplóállományokat a *Minősített időbélyegzés-szolgáltató* biztonságos környezetben őrzi. Az állományokról a működés másodlagos helyszínén másolati példányokat is tart.

5.4.5. A naplófájl mentési eljárásai

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

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

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

5.4.6. A naplózás adatgyűjtési rendszere

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

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

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

5.4.7. Az eseményeket kiváltó alanyok értesítése

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

5.4.8. Sebezhetőség felmérése

A naplóbejegyzések napi rendszerességgel végzett feldolgozásán túl a *Minősített időbélyegzés-szolgáltató* szakemberei figyelik a nyilvánosan elérhető információt a lehetséges sérülékenységekről, szoftver javító csomagokról. Elemzik a gyűjtött információt, osztályba sorolják a sérülékenységet és szükség esetén értesítik a vezetőséget az eredményről és intézkedési tervet javasolnak a rendszer biztonságának növelésére.

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

A vizsgálat eredményei alapján a *Minősített időbélyegzés-szolgáltató*

- intézkedési tervet hoz létre és hajt végre a sérülékenységek megszüntetése érdekében, vagy
- dokumentálja a döntés alapjául szolgáló tényeket, elfogadja a maradvány kockázatokat és nem hoz intézkedési tervet a sérülékenység megszüntetésére.

Az új program verziókat vagy program javító csomagokat a *Minősített időbélyegzés-szolgáltató* először a teszt rendszeren telepíti és csak a sikeres tesztek elvégzése után kerülnek telepítésre a szolgáltatásokat nyújtó éles rendszeren.

Az új szoftver verziók vagy javító csomagok nem kerülnek bevezetésre az éles rendszeren, amennyiben olyan további sérülékenységet vagy instabilitást okoznak a rendszer működésében, ami nagyobb gondot eredményez az alkalmazásukból származó előnynél. Az alkalmazás mellőzésének okát a *Minősített időbélyegzés-szolgáltató* dokumentálja.

5.5. Adatok archiválása

5.5.1. Az archivált adatok típusai

A *Minősített időbélyegzés-szolgáltató* felkészült elektronikus és papíralapú dokumentumok megfelelően biztonságos, hosszú idejű archiválására.

A *Minősített időbélyegzés-szolgáltató* minimálisan az alábbi jellegű információt archiválja:

- 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 őrzi meg:

- a *Minősített időbélyegzési rend*et a hatályon kívül helyezéstől számított legalább 10 évig;
- a *Minősített időbélyegzési szolgáltatási szabályzat*ot 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* valamennyi archivált adatot két példányban, két egymástól fizikailag elkülönült helyszínen őrzi. Az egyetlen hiteles példányban rendelkezésre álló papíralapú dokumentumról hiteles papíralapú, vagy elektronikus másolatot készít a vonatkozó jogszabályok betartásával.

A két helyszín mindegyike teljesíti az archiválással szemben támasztott biztonsági és egyéb követelményeket.

Az archivált adatok megőrzése során a *Minősített időbélyegzés-szolgáltató* gondoskodik az archivált adatok

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

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

5.5.4. Az archívum mentési folyamatai

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

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

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

5.5.5. Az adatok időbélyegzésére vonatkozó követelmények

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

Az időpontot a *Minősített időbélyegzés-szolgáltató* belső órája adja, amelyet a *Minősített időbélyegzés-szolgáltató* két egymástól független Stratum-1 UTC referencia időforrással szinkronizál:

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

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

A *Minősített időbélyegzés-szolgáltató* a belső óra pontosságának ilyen szinten tartásával garantálja, hogy valamennyi időjelzés pontossága legfeljebb 1 másodperccel tér el az UTC időalaptól.

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

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

5.5.6. Az archívum gyűjtési rendszere

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

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

5.5.7. Archív információk hozzáférését és ellenőrzését végző eljárások

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

Az archivált adatállományokat védi a jogosulatlan hozzáféréstől.

Az arra jogosultaknak biztosítja az archivált adatokhoz való ellenőrzött hozzáférést:

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

5.6. Szolgáltatói kulcs cseréje

A *Minősített időbélyegzés-szolgáltató* gondoskodik arról, hogy az általa használt *Időbélyegző egység*ek folyamatosan rendelkezzenek a működéshez szükséges, érvényes kulccsal és Tanúsítvánnyal. A szolgáltatói *Tanúsítvány*ok lejárta illetve a hozzájuk kapcsolódó kulcsok

használati idejének lejárta előtt elegendő idővel új kulcspárt generál az *Időbélyegző egység* számára, és arról időben értesíti *Ügyfel*eit. Az új szolgáltatói kulcsot a jelen szabályzatnak megfelelően generálja és kezeli.

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

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

5.7. Kompromittálódást és katasztrófát követő helyreállítás

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

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

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

5.7.1. Váratlan esemény és kompromittálódás kezelési eljárások

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

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

Kompromittálódás, kompromittálódás gyanúja vagy az *Időbélyegző egység* órájának elállítódása esetén a *Minősített időbélyegzés-szolgáltató* honlapján közzéteszi az érintett *Időbélyegző*k beazonosításához szükséges információkat. A *Minősített időbélyegzés-szolgáltató* kialakított és folyamatosan üzemben tart egy teljes értékű tartalékrendszert, amely az elsődleges helyszíntől biztonságos távolságra, földrajzilag különböző helyszínen található és önállóan is alkalmas a szolgáltatások teljes körű ellátására.

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

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

A *Minősített időbélyegzés-szolgáltató* úgy alakította ki a bizalmi szolgáltatásokat nyújtó informatikai rendszerét, hogy bármely egy eszköz kiesése esetén képes zavartalanul folytatni a bizalmi szolgáltatások nyújtását.

Amennyiben a *Minősített időbélyegzés-szolgáltató*nak egyszerre több egysége esik ki, a *Minősített időbélyegzés-szolgáltató* legfeljebb 3 óra időtartamon belül képes háttér-rendszerének beindítására, amely biztosítja folyamatosan működő szolgáltatásait a *Minősített időbélyegzés-szolgáltató Ügyfel*ei számára.

5.7.2. Meghibásodott IT erőforrások, szoftverek és/vagy adatok

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

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

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

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

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

5.7.3. Magánkulcs kompromittálódása esetén követendő eljárások

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

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

5.7.4. Működés folyamatosságának biztosítása katasztrófát követően

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

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

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

A *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 helyreállítja a katasztrófa során tönkrement eszközeit és az eredeti szolgáltatás biztonsági szintet.

5.8. Az Időbélyegzés-szolgáltató leállítása

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

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

A *Minősített időbélyegzés-szolgáltató* a tervezett leállás előtt legalább 20 nappal, de az *Ügyfel*ek értesítését követően legalább 14 nappal leállítja új *Időbélyegző*k kibocsátását.

A leállás időpontjával egyidejűleg a *Minősített időbélyegzés-szolgáltató* a következő szolgáltatásokat állítja le:

- műszaki segítségnyújtás,
- információ szolgáltatás.

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

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

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

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

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

6. Műszaki biztonsági óvintézkedések

A *Minősített időbélyegzés-szolgáltató* módosítás ellen védett, megbízható, biztonságtechnikailag értékelt termékekből álló informatikai rendszereket használ szolgáltatásai nyújtásához. A

Minősített időbélyegzés-szolgáltató a szolgáltatói kriptográfiai magánkulcsokat teljes életciklusuk alatt megfelelő tanúsítással rendelkező *HSM eszköz*ökben kezeli.

Mind a *Minősített időbélyegzés-szolgáltató*, mind a rendszert szállító és kivitelező vállalkozók jelentős tapasztalatokkal rendelkeznek PKI alapú rendszerek és bizalmi szolgáltatások kiépítésében és nemzetközileg elismert technológiát alkalmaznak.

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

6.1. Kulcspár előállítása és telepítése

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

6.1.1. Kulcspár előállítása

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

- ETSI TS 119 312 [21];
- az Eüt. [6] 92. § (1) b) pontja szerinti aktuális Nemzeti Média- és Hírközlési Hatóság által kiadott algoritmusokkal kapcsolatos határozat.

Szolgáltatói kulcspárok előállítása

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

- A szolgáltatói magánkulcs előállítását fizikailag védett környezetben (lásd 5.1 pont), legalább két, bizalmi szerepkört (lásd 5.2.1 pont) betöltő, erre feljogosított személy együttes részvételével, más illetéktelen személyek jelenlétét kizárva végzi.
- A szolgáltatói magánkulcs előállítását olyan eszközön belül hajtja végre, amely:
  - megfelel az ISO/IEC 19790 [25] követelményeinek,
  - vagy megfelel a FIPS 140-2 [33] 3-as, illetve annál magasabb szintű követelményeinek,
  - vagy megfelel a CEN 419 221-5 [22] követelményeinek,
  - vagy olyan megbízható rendszer, amely az MSZ/ISO/IEC 15408 [24] szerint, illetve azzal egyenértékű biztonsági kritériumok szerint EAL 4-es vagy magasabb értékelési garancia szinten van értékelve. Az értékelésnek a jelen dokumentum követelményeinek megfelelő biztonsági rendszerterven, vagy biztonsági előirányzaton kell alapulnia.
- A szolgáltatói magánkulcs előállítását egy kulcsgenerálási forgatókönyv alapján végzi.

Szolgáltatói infrastruktúrális kulcspárok előállítása

A *Minősített időbélyegzés-szolgáltató* a saját IT rendszereiben használt infrastruktúrális kulcsok előállítása esetén biztosítja, 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. Kulcsméretek

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

- ETSI TS 119 312 [21];
- az Eüt. [6] 92. § (1) b) pontja szerinti aktuális Nemzeti Média- és Hírközlési Hatóság által kiadott algoritmusokkal kapcsolatos határozat.

A *Minősített időbélyegzés-szolgáltató* az *Időbélyegző egység*ek *Tanúsítvány*aiban legalább 2048 bites RSA kulcsot vagy 256 bites ECC kulcsot használ.

2021-01-01-től a *Minősített időbélyegzés-szolgáltató* az *Időbélyegző egység*ek *Tanúsítvány*aiban legalább 3072 bites RSA kulcsot vagy 256 bites ECC kulcsot használ.

A *Minősített időbélyegzés-szolgáltató* az alábbi ECC görbéket támogatja:

- ECC NIST P-256 (256 bit)

6.1.3. A nyilvános kulcs paraméterek előállítása, a minőség ellenőrzése

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

A paraméterek megfelelőségének ellenőrzése

A kulcsgenerálás paramétereinek megfelelőségét két szempontból ellenőrzi a rendszer:

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

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

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

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

6.2. A magánkulcsok védelme

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

6.2.1. Kriptográfiai modulra vonatkozó szabványok és előírások

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

- megfelelnek az ISO/IEC 19790 [25] követelményeinek,
- vagy megfelelnek a FIPS 140-2 [33] 3-as, illetve annál magasabb szintű követelményeknek,
- vagy megfelelnek a CEN 14167-2 [34] munkacsoport egyezmény követelményeinek,
- vagy megfelelnek a CEN 419 221-5 [22] követelményeinek,
- vagy olyan megbízható rendszerek, amely az MSZ/ISO/IEC 15408 [24] szerint, illetve azzal egyenértékű biztonsági kritériumok szerint 4-es vagy magasabb értékelési garancia szinten vannak értékelve. Az értékelésnek a jelen dokumentum követelményeinek megfelelő biztonsági rendszerterven, vagy biztonsági előirányzaton kell alapulnia.

A *Minősített időbélyegzés-szolgáltató* a szolgáltatói magánkulcsokat a *HSM eszköz*ön kívül csak kódolt formában tárolja. A kódoláshoz csak az Eüt. [6] 92. § (1) b) szerint kiadott aktuális Nemzeti Média- és Hírközlési Hatóság határozat szerinti algoritmusokat és kulcsparamétereket használ, amelyek várhatóan a kulcs teljes élettartama alatt képesek ellenállni a kriptográfiai támadásoknak.

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

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

6.2.2. Magánkulcs többszereplős (n-ből m) használata

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

6.2.3. Magánkulcs letétbe helyezése

A *Minősített időbélyegzés-szolgáltató* a szolgáltatói magánkulcsait nem helyezi letétbe.

6.2.4. Magánkulcs mentése

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

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

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

6.2.5. Magánkulcs archiválása

A *Minősített időbélyegzés-szolgáltató* nem archiválja magánkulcsait.

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

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

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

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

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

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

6.2.7. Magánkulcs tárolása hardver kriptográfiai eszközben

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

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

6.2.8. A magánkulcs aktiválásának módja

A *Minősített időbélyegzés-szolgáltató* szolgáltatói magánkulcsait biztonságos *HSM eszköz*ben tárolja, a használat során betartja a *HSM eszköz* felhasználói útmutatójában és a tanúsítási dokumentumokban megfogalmazott követelményeket. A *HSM eszköz*t csak a hozzá tartozó operátori kártyákkal lehet aktiválni, a *HSM eszköz*ben lévő magánkulcsokat a modul aktiválása előtt

nem lehet használni. A *HSM eszköz*höz tartozó operátori kártyákat a *Minősített időbélyegzés-szolgáltató* biztonságos környezetben tárolja és e kártyákat kizárólag a *Minősített időbélyegzés-szolgáltató* erre jogosult munkatársai érhetik el.

6.2.9. A magánkulcs deaktiválásának módja

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

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

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

6.2.10. A magánkulcs megsemmisítésének módja

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

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

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

6.2.11. A hardver kriptográfiai eszközök értékelése

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

- ISO/IEC 19790 [25] szerinti tanúsítvánnyal,
- vagy FIPS 140-2 Level 3 [33] szerinti tanúsítvánnyal,
- vagy a CEN 14167-2 [34] munkacsoport egyezmény követelményeinek való megfelelést igazoló legalább EAL-4 szintű Common Criteria alapú tanúsítvánnyal,
- vagy a CEN 419 221-5 [22] 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 egység*ek *Tanúsítvány*ainak érvényességi ideje:

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

A *Minősített időbélyegzés-szolgáltató* minden évben az aktuális használatban lévő magánkulcsok használati idejének lejártát megelőzően új magánkulcso(ka)t állít elő és új *Tanúsítvány*(oka)t igényel az *Időbélyegző egység*ei számára.
Az új *Időbélyegző egység* *Tanúsítvány*(ok) használatba vétele után a korábbi magánkulcso(ka)t megsemmisíti, így az egyes magánkulcsokat átlagosan 12 hónapig használja.

Az Időbélyegző kulcsok életciklusa

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

- a *Minősített időbélyegzés-szolgáltató* meghatározza az *Időbélyegző egység*ekben használt aláíró kulcsok érvényességének végét, ami legfeljebb a *Tanúsítvány* kibocsátásától számított 18 hónap;
- a kulcs érvényességi ideje nem haladhatja meg a *Tanúsítvány* érvényességi idejét;
- az érvényességi idő nem haladhatja meg az alkalmazott kriptográfiai algoritmusok és kulcs paraméterek érvényességi idejét;
- a *Minősített időbélyegzés-szolgáltató* az *Időbélyegző egység*ek magánkulcsának érvényességi idejét megadja a *Tanúsítvány* "PrivateKeyUsagePeriod" értékének beállításával (lásd 7.1.2. fejezet);
- az *Időbélyegző egység* magánkulcsát nem használja az érvényességi időn túl;
- a *Minősített időbélyegzés-szolgáltató* szervezeti eljárásokat alkalmaz annak biztosítására, hogy az *Időbélyegző egység* magánkulcsának lejárata esetén rendelkezésre álljon az új magánkulcs és *Tanúsítvány*;
- a *Minősített időbélyegzés-szolgáltató* az új magánkulcsok használatbavétele után a lejárt érvényességű, használatból kivont magánkulcs minden példányát megsemmisíti oly módon, hogy a magánkulcs visszaállítása lehetetlenné váljon.

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

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

6.4. Aktivizáló adatok

6.4.1. Aktivizáló adatok előállítása és telepítése

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

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

6.4.2. Az aktivizáló adatok védelme

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

6.4.3. Az aktivizáló adatok kezelésének egyéb szempontjai

Nincs megkötés.

6.5. Informatikai biztonsági előírások

6.5.1. Speciális informatikai biztonsági műszaki követelmények

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

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

6.5.2. Az informatikai biztonság értékelése

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

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

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

A Microsec kétszintű kockázatelemzése az információ technológiai kockázatokon túlmenően kiterjed a teljes szervezetre és az üzleti kockázatokra is. A kockázatelemzés legalább évente felülvizsgálatra kerül. A kockázatelemzés eredménye alapján a *Minősített időbélyegzés-szolgáltató*

- intézkedéseket hoz a feltárt sérülékenységek megszüntetésére, és/vagy
- elfogadja az azonosított maradvány kockázatokat a döntés indokainak rögzítésével.

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 használ, 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.

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

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

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 ellenőrzi kártékony kódok után kutatva.

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

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

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

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

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

6.6.2. Biztonságkezelési előírások

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

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

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

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

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

6.6.3. Életciklusra vonatkozó biztonsági előírások

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

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

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

6.7. Hálózati biztonsági előírások

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

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

- IT rendszereit jól elválasztott biztonsági zónákra osztja;
- elkülöníti az IT rendszer üzemeltetését támogató rendszereit az éles szolgáltatást nyújtó rendszereitől;
- elkülöníti az éles szolgáltatást nyújtó rendszereit a fejlesztésre és tesztelésre szolgáló rendszerektől;
- az elkülönített megbízható rendszerek között csak olyan megbízható kommunikációs csatornákon keresztül létesít kapcsolatot, amelyek logikailag el vannak választva más kommunikációs csatornáktól, megbízható végponti azonosítást használnak és védik a csatornákon küldött adatokat a módosítástól és a felfedéstől;

- az éles szolgáltatást nyújtó IT rendszereit biztonságos hálózati zónában üzemelteti;
- a zónákhoz való hozzáférést és a zónák közötti kommunikációt csak a szolgáltatás nyújtásához szükségesre korlátozza;
- letiltja a nem használt protokollokat és felhasználókat;
- letiltja a használaton kívüli hálózati portokat és szolgáltatásokat;
- csak az IT rendszer megfelelő működéséhez feltétlenül szükséges hálózati alkalmazásokat futtat.
- a használt szabályrendszert rendszeresen felülvizsgálja.

A *Minősített időbélyegzés-szolgáltató* sérülékenységvizsgálatot végez vagy végeztet 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.

A *Minősített időbélyegzés-szolgáltató* legalább 3 havonta ellenőrzi a helyi hálózati eszközök (pl. router) konfigurációjának megfelelőségét a *Minősített időbélyegzés-szolgáltató* által meghatározott követelményeknek.
A *Minősített időbélyegzés-szolgáltató* évente illetve az informatikai rendszerén történt minden jelentős változás után sebezhetőségvizsgálatot végeztet egy külső, független szakemberrel, aki rendelkezik az ilyen vizsgálat elvégzéséhez szükséges képességekkel, szakértelemmel, eszközökkel és etikai kódexekkel.

6.8. Időbélyegzés

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

7. Tanúsítvány, CRL és OCSP profilok

7.1. Tanúsítvány profil

A *Minősített időbélyegzés-szolgáltató* által használt *Időbélyegző egység Tanúsítvány*ok illetve az azokat kibocsátó tanúsítvány láncban található gyökér és köztes hitelesítő egységek *Tanúsítvány*ai megfelelnek az alábbi ajánlásoknak, specifikációknak:

- ITU X.509 Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks [31];

- IETF RFC 3739 [27];
- IETF RFC 5280 [28];
- IETF RFC 6818 [30];
- ETSI EN 319 412-1 [15];
- ETSI EN 319 412-2 [16] természetes személyek számára kibocsátott *Tanúsítvány*ok esetén;
- ETSI EN 319 412-3 [17] nem természetes személyek számára kibocsátott *Tanúsítvány*ok esetén;
- ETSI EN 319 412-5 [18].

7.1.1. Verzió szám(ok)

A *Minősített időbélyegzés-szolgáltató* által használt *Időbélyegző egység Tanúsítvány*ok az X.509 specifikáció [31] szerinti "v3" *Tanúsítvány*ok.
A *Tanúsítvány*ok alapmezői a következők:

- Verzió (Version)
  A *Tanúsítvány* az X.509 specifikáció [31] szerinti "v3" *Tanúsítvány*oknak felel meg, így a mezőbe a "2" érték kerül.
- Sorozatszám (Serial Number)
  A *Tanúsítvány*t kibocsátó hitelesítő egység által generált egyedi azonosító.

  A végfelhasználói *Tanúsítvány*ok esetében a "Serial Number" mező legalább 8 bájt entrópiájú véletlen számot tartalmaz.
- Algoritmus azonosító (Algorithm Identifier)
  A *Tanúsítvány*t hitelesítő elektronikus bélyegző készítéséhez használt kriptográfiai algoritmuskészlet azonosítója (OID). A *Hitelesítés-szolgáltató* a következő kriptográfiai algoritmust használja:
  - "sha256WithRSAEncryption" (1.2.840.113549.1.1.11)
  - "ecdsa-with-SHA256" (1.2.840.10045.4.3.2)
- Aláírás (Signature)
  A *Hitelesítés-szolgáltató* által készített, a *Tanúsítvány*t hitelesítő elektronikus bélyegző, amelyet a *Hitelesítés-szolgáltató* az "Algoritmus azonosító" -ban megadott algoritmuskészlettel hozott létre.
- Kibocsátó (Issuer)
  A *Tanúsítvány*t kibocsátó *Hitelesítő egység* megkülönböztetett neve egyedi X.501 név formátum szerint.
- Érvényesség (notBefore & notAfter)

  A *Tanúsítvány* érvényességének kezdete és vége.

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

- Az Alany azonosítója (Subject)
  Az Alany megkülönböztetett neve egyedi X.501 név formátum szerint.
  Mindig kitöltésre kerül.
- Az Alany nyilvános kulcsának algoritmus-azonosítója (Subject Public Key Algorithm Identifier)

  A mezőbe kerülő érték:

  – "rsaEncryption" (1.2.840.113549.1.1.1)
  – "ecPublicKey" (1.2.840.10045.2.1)
- Az Alany nyilvános kulcsa (Subject Public Key Value)
  Az Alany nyilvános kulcsa.
- Kibocsátó egyedi azonosító (Issuer Unique Identifier)
  Nem kitöltött.
- Az Alany egyedi azonosítója (Subject Unique Identifier)
  Nem kitöltött.

7.1.2. Tanúsítvány kiterjesztések

A *Minősített időbélyegzés-szolgáltató* csak az alábbi, X.509 specifikáció [31] szerinti tanúsítvány kiterjesztéseket használja:

Időbélyegző egység tanúsítványa

- Hitelesítési rendek (Certificate Policies) – nem kritikus
  OID: 2.5.29.32
  E mező tartalmazza az *Időbélyegző egység Tanúsítvány*ának kiadása és használata során érvényes *Hitelesítési rend* azonosítóját, valamint az alkalmazhatóságára vonatkozó egyéb információkat. A mező kitöltése kötelező és nem lehet kritikus. A vonatkozó Szolgáltatási szabályzat hivatkozása megadható ebben a mezőben.
- Kibocsátó kulcsazonosító (Authority Key Identifier) – nem kritikus
  OID: 2.5.29.35
  A *Tanúsítvány*t hitelesítő elektronikus bélyegző létrehozásánál felhasznált szolgáltatói kulcs 40 karakter hosszú egyedi azonosítója.

  A mező értéke: a szolgáltatói nyilvános kulcs SHA-1 lenyomata.
- *Alany* kulcsazonosító (Subject Key Identifier) – nem kritikus
  OID: 2.5.29.14
  Az *Időbélyegző egység* nyilvános kulcsának 40 karakter hosszú egyedi azonosítója.
  A mező értéke: a nyilvános kulcs SHA-1 lenyomata.
- *Alany* alternatív nevei (Subject Alternative Names) – nem kritikus
  OID: 2.5.29.17

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

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

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

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

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

  Az *Időbélyegző egység* számára kibocsátott *Tanúsítvány*okban kizárólag az alábbi értékek szerepelnek:

  "nonRepudiation",

  "digitalSignature".

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

- 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 kizárólag az alábbi érték szerepel:

  "timeStamping (1.3.6.1.5.5.7.3.8)".

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

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

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

  - A *Hitelesítés-szolgáltató* a *Tanúsítvány*ok aktuális visszavonási állapotának gyors és pontos ellenőrizhetősége érdekében online tanúsítvány-állapot szolgáltatást nyújt. Ez az elérhetőség szerepel itt.
  - A tanúsítványlánc felépítésének megkönnyítésére a *Hitelesítés-szolgáltató* megadja 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 szerepelnek a következő állítások:
  - a *Tanúsítvány* EU minősített *Tanúsítvány* – 'id-etsi-qcs 1' (0.4.0.1862.1.1);
  - a *Tanúsítvány*hoz kapcsolódó tranzakciós limit – más néven ügyleti 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* lejárta 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 eszköz*ön 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-qct-eseal' (2)).

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

7.1.3. Időbélyegző profil

Az alkalmazott időbélyegző profil megfelel az IETF RFC 3161 [26] és IETF RFC 5816 [29] specifikáció előírásainak.

8. A megfelelőség vizsgálata

A *Minősített időbélyegzés-szolgáltató* tevékenységét az Európai Uniós 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* külső auditor igénybevételével átvilágíttatja üzemeltetését és az átvilágításról készült részletes megfelelőségértékelési jelentést annak kézhezvételétől számított három munkanapon belül a Nemzeti Média- és Hírközlési Hatóságnak benyújtja. 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 megfelel 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 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers; [12]
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [11]
- ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps. [19]

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

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

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

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

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

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

8.1. Az ellenőrzések körülményei és gyakorisága

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

8.2. Az auditor és szükséges képesítése

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

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

8.3. Az auditor és az auditált rendszerelem függetlensége

A külső auditot olyan személy végzi:

- aki független a vizsgált *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-szolgáltató*val;
- akinek díjazása nem függ az audit során végzett tevékenységének megállapításaitól.

8.4. Az auditálás által lefedett területek

Az átvizsgálás lefedi az alábbi területeket:

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

8.5. A hiányosságok kezelése

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

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

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 nyilvánosságra hozza honlapján az alábbi linken:

`https://e-szigno.hu/eidas/`

A feltárt hiányosságok részleteit nem publikálja, azokat bizalmas információként kezeli.

A megfelelőségértékelési vizsgálatok tanúsítványai megtekinthetők a tanúsító szervezet publikus weboldalán [1] illetve a *Minősített időbélyegzés-szolgáltató* saját weboldalán az alábbi linken:

`https://e-szigno.hu/eidas/eidas.html`

A magyar nemzeti bizalmi lista elérhetősége:

- ember által olvasható PDF formátumban: `http://www.nmhh.hu/tl/pub/HU_TL.pdf`
- géppel feldolgozható XML formátumban: `http://www.nmhh.hu/tl/pub/HU_TL.xml`

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

http://webpub-ext.nmhh.hu/esign2016/

9. Egyéb üzleti és jogi kérdések

9.1. Díjak

A szolgáltatási díjakat és árakat a *Minősített időbélyegzés-szolgáltató* a honlapján közzéteszi és kérelemre ügyfélszolgálati irodájában is biztosítja olvashatóságát.

Az árlista elérhetősége:

- `https://e-szigno.hu/arlista`

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

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

9.1.1. Visszatérítési politika

Lásd: 9.1. fejezet.

[1] `https://www.hunguard.hu/ugyfeleinknek/tanusitott-termekek-rendszerek/eidas-rendelet-szerinti-bizalmi-szolgaltatas/microsec-zrt/`

9.2. Anyagi felelősségvállalás

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

9.2.1. Pénzügyi követelmények

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

9.2.2. Felelősségbiztosítás

- A *Minősített időbélyegzés-szolgáltató* a megbízhatóság biztosítása érdekében felelősségbiztosítással rendelkezik.
- A felelősségbiztosítási szerződés kiterjed 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 felelősségbiztosítás a meghatározott összeg erejéig fedezetet nyújt a károsultnak a szolgáltató károkozó magatartásával összefüggésben keletkező teljes kárára, függetlenül attól, hogy a kárt szerződésszegéssel vagy szerződésen kívül okozták.
- Ha egy biztosítási eseménnyel kapcsolatban több jogosult megalapozott kártérítési igénye meghaladja a károkra biztosítási eseményenként a felelősségbiztosítási szerződésben meghatározott összeget, akkor a kártérítési igények megtérítése az összes kártérítési igénynek a felelősségbiztosítási szerződésben meghatározott összeghez viszonyított arányában történik.

9.3. Bizalmasság

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

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

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

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

9.3.1. Bizalmas információk köre

A *Minősített időbélyegzés-szolgáltató* bizalmas információként kezeli:

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

9.3.2. Bizalmas információk körén kívül eső adatok

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

9.3.3. Bizalmas információ védelme

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

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

A *Minősített időbélyegzés-szolgáltató* a birtokába jutott bizalmas adatokat az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény [4] rendelkezéseinek megfelelően kezeli, és kizárólag az alábbi esetben fedi fel azokat:

- **Információszolgáltatás a hatóságok részére**

  A *Minősített időbélyegzés-szolgáltató* az Eüt. [6] 90. § (1) bekezdésének megfelelően az általa nyújtott bizalmi szolgáltatások felhasználásával elkövetett bűncselekmények felderítése vagy megelőzése céljából, illetőleg nemzetbiztonsági érdekből – az adatigénylésre külön törvényben meghatározott feltételek teljesülése esetén – a nyomozó hatóságnak és a nemzetbiztonsági szolgálatoknak díjmentesen továbbítja az érintett személyazonosságát igazoló, valamint a *Minősített időbélyegzés-szolgáltató* által egyeztetett adatokat.

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

- **A tulajdonos kérésére történő felfedés**

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

9.4. Személyes adatok védelme

A *Minősített időbélyegzés-szolgáltató* gondoskodik az általa kezelt személyes adatok védelméről, működése és szabályzatai megfelelnek az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény [4] és a 2016/679 EU általános adatvédelmi rendelet [2] rendelkezéseinek.

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

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

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

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

9.4.1. Adatkezelési terv

A *Minősített időbélyegzés-szolgáltató* rendelkezik Adatvédelmi Szabályzattal és Adatkezelési Tájékoztatóval, amelyek részletes előírásokat tartalmaznak a személyes adatok kezelésére.

Az Adatvédelmi Szabályzat megtalálható az e-Szignó Hitelesítés Szolgáltató honlapján az alábbi linken:

`https://e-szigno.hu/minden-dokumentum.html`

Az Adatkezelési Tájékoztató megtalálható az e-Szignó Hitelesítés Szolgáltató honlapján az alábbi linken:

`https://e-szigno.hu/adatkezelesi-tajekoztato.html`

9.4.2. Személyes adatok

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

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

9.4.3. Személyes adatnak nem minősülő adatok

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

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

A jelen *Minősített időbélyegzési szolgáltatási szabályzat* 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 szoftver leírásában vagy magában a szoftverben elérhető illetve ott meghivatkozott helyen található felhasználói útmutató tartalmazza.

9.6. Tevékenységért viselt felelősség és helytállás

9.6.1. A szolgáltató felelőssége és helytállása

A Szolgáltató felelőssége

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

- 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 *Ügyfel*ekkel szemben a Polgári Törvénykönyv [5] 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 [5] általános felelősségi szabálya szerint felelős;
- a *Minősített időbélyegzés-szolgáltató* a felelősségi körén belül keletkezett, bizonyított károkért a szabályzataiban és az *Ügyfél*lel megkötött Szolgáltatási szerződésekben rögzített korlátozásokkal kártérítést fizet (lásd: Pénzügyi felelősség korlátozása 9.8. fejezet);
- ha egy biztosítási eseménnyel kapcsolatban több jogosult megalapozott kártérítési igénye meghaladja a károkra biztosítási eseményenként a felelősségbiztosítási szerződésben meghatározott összeget, akkor a kártérítési igények megtérítése az összes kártérítési igénynek a felelősségbiztosítási szerződésben meghatározott összeghez viszonyított arányában történik.

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

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 szolgáltatást a *Minősített időbélyegzési rend*del, a *Minősített időbélyegzési szolgáltatási szabályzat*tal, az Általános Szerződési 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 helytállása

Az *Előfizető* felelőssége

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

Az *Előfizető* kötelezettségei

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

Az *Előfizető* kötelezettségeit a jelen *Minősített időbélyegzési szolgáltatási szabályzat*, a Szolgáltatási szerződés és annak elválaszthatatlan részét képező Általános Szerződési Feltételek, valamint a vonatkozó *Minősített időbélyegzési rend* tartalmazzák.

Az *Előfizető* jogai

Az *Előfizető* jogosult:

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

9.6.3. Az Érintett fél felelőssége

Az *Érintett felek* saját belátásuk és/vagy szabályzataik alapján dönthetnek az egyes *Tanúsítvány*ok és *Időbélyegző*k 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 rend*ben és a *Minősített időbélyegzési szolgáltatási szabályzat*ban megfogalmazott követelmények, előírások betartása;
- megbízható informatikai környezet és alkalmazások használata;
- az *Időbélyegző* aláírásához használt *Tanúsítvány* visszavonási állapotának ellenőrzése az aktuális CRL vagy OCSP válasz alapján;
- az *Időbélyegző* felhasználására vonatkozó valamennyi korlátozás figyelembevétele, amely a a *Minősített időbélyegzési szolgáltatási szabályzat*ban és a vonatkozó *Minősített időbélyegzési rend*ben 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* korlátozza a szolgáltatással kapcsolatos kártérítési kötelezettségét, ezen korlátozás mértéke káreseményenként 100.000,-Ft.

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

9.9. Kártérítési kötelezettség

9.9.1. A szolgáltató kártérítési kötelezettsége

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

9.9.2. Az előfizető kártérítési kötelezettsége

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

9.9.3. Az érintett felek kártérítési kötelezettsége

Lásd: 9.8. fejezet

9.10. Érvényesség és megszűnés

9.10.1. Érvényesség

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

9.10.2. Megszűnés

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

9.10.3. A megszűnés következményei

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

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

9.11. A felek közötti kommunikáció

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

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

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

9.12. Módosítások

A *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 szolgáltatási szabályzat*ot.

9.12.1. Módosítási eljárás

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

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

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

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

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 felek*et az új dokumentum verziók kibocsátásáról.

9.12.3. Az OID megváltoztatása

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

9.13. Vitás kérdések rendezése

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

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

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

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

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

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

9.14. Irányadó jog

A *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 vonatkozó jogszabályok:

- AZ EURÓPAI PARLAMENT ÉS A TANÁCS 910/2014/EU RENDELETE (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről [1];
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról [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.) Kormányrendelet a bizalmi felügyelet által vezetett nyilvántartások tartalmáról és a bizalmi szolgáltatás nyújtásával kapcsolatos bejelentésekről [9];

9.16. Vegyes rendelkezések

9.16.1. Teljességi záradék

Nincs megkötés.

9.16.2. Átruházás

A jelen *Minősített időbélyegzési szolgáltatási szabályzat* alapján nyújtott szolgáltatásokba bevont alvállalkozók vagy egyéb együttműködő partnerek 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 szolgáltatási szabályzat* 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 szolgáltatási szabályzat* 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 szolgáltatási 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] 2001. évi XXXV. törvény az elektronikus aláírásról (hatályon kívül helyezve 2016. július 1-től) .

[4] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról .

[5] 2013. évi V. törvény a Polgári Törvénykönyvről .

[6] 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól .

[7] 24/2016. (VI. 30.) BM rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről .

[8] 25/2016. (VI. 30.) BM rendelet a bizalmi felügyeletnek fizetendő igazgatási szolgáltatási díjak mértékéről .

[9] 470/2017. (XII. 28.) Korm. rendelet a bizalmi felügyelet által vezetett nyilvántartások tartalmáról és a bizalmi szolgáltatás nyújtásával kapcsolatos bejelentésekről .

[10] 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.

[11] ETSI EN 319 401 V2.3.1 (2021-05); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

[12] 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;.

[13] ETSI EN 319 411-1 V1.3.1 (2021-05); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

[14] ETSI EN 319 411-2 v2.3.1 (2021-05); 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;.

[15] Final draft ETSI EN 319 412-1 V1.4.3 (2021-03); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.

[16] ETSI EN 319 412-2 V2.2.1 (2020-07); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons;.

[17] ETSI EN 319 412-3 V1.2.1 (2020-07); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons.

[18] ETSI EN 319 412-5 V2.3.1 (2020-04); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.

[19] 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.

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

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

[22] CEN 419 221-5; Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services.

[23] ISO 3166-1:2013, Codes for the representation of names of countries and their subdivisions – Part 1: Country codes.

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

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

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

[27] IETF RFC 3739: Internet X.509 Public Key Infrastructure - Qualified Certificates Profile, MARCH 2004.

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

[29] IETF RFC 5816: ESSCertIDv2 Update for RFC 3161, April 2010.

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

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

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

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

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

[35] Magyarország (Hungary): Trusted List (`http://www.nmhh.hu/tl/pub/HU_TL.pdf`).

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

[37] e-Szignó Hitelesítés Szolgáltató - minősített időbélyegzési rend .

[38] e-Szignó Hitelesítés Szolgáltató - Általános Szerződési Feltételek .