NISZ

Nemzeti Infokommunikációs Szolgáltató Zrt.

Időbélyegzés
Bizalmi Szolgáltatási Szabályzat
(IBSZ)

Verziószám	2.2
OID	0.2.216.1.200.1100.100.42.3.3.15
Hatályba lépés dátuma	2025.12.01.
Dokumentum besorolása	nyilvános
Jóváhagyó	Adorján István
Adorján István	Digitálisan aláírta: Adorján István Dátum: 2025.11.14 12:17:28 +01'00'

Változáskövetés

verzió	dátum	a változás leírása	készítette	ellenőrizte	jóváhagyta
1.0[1]	2016.12.29	Első, eIDAS megfelelőségértékeléshez elkészített változat	Polysys Kft.	Kővári Ferenc	Ferencz Attila
1.1[2]	2017.04.27	Megfelelőségértékelő szervezet észrevételei alapján módosított változat	Polysys Kft. Kővári Ferenc	Kővári Ferenc	Ferencz Attila
1.2	2017.05.31	Hatályba lépés dátumának pontosítása	Papp Eszter	Kővári Ferenc	Ferencz Attila
1.3	2019.03.25	EN szabványok változásainak követése, egyéb frissítések	Polysys Kft.	Kővári Ferenc	Ferencz Attila
1.4	2019.08.15	Szolgáltató Ügyfélkapcsolati Irodája címének változása	Joláthy Dániel	Kővári Ferenc	Ferencz Attila
1.5	2019.08.30	Szolgáltató Ügyfélkapcsolati Irodája címének átírása a TSA Közzétételi Nyilatkozat mellékletben	Joláthy Dániel	Kővári Ferenc	Ferencz Attila
1.6	2021.03.04	Új PKI ÜKI tanúsítvány átadó helyszín	Kővári Ferenc	dr. Kovács Ferenc	Adorján István
1.7	2023.03.20	A tanúsítványok alkalmazhatósági szabályainak módosítása	Nagy Benjámin	Kővári-Szabó Zoltán	Adorján István
1.8	2024.01.02	Székhelyváltozás átvezetése	Kővári-Szabó Zoltán	Nagy Benjámin	Adorján István
1.9[3]	2024.09.01	• jogszabályi környezet változásából adódó módosítások (E-ügyintézési tv., DÁP tv., eIDAS) • általános felülvizsgálat	Nagy Benjámin	Kővári-Szabó Zoltán	Adorján István
2.0	2024.09.01	• jogszabályi környezet változásából adódó módosítások (E-ügyintézési tv., DÁP tv., eIDAS) • általános felülvizsgálat • OID kiosztási rend módosításának alkalmazása a fedlapon	Nagy Benjámin	Kővári-Szabó Zoltán	Adorján István
2.1	2025.03.18	• Alkalmazhatósági szabályok változása • Új Kiadó (CA) és algoritmuskészlet bevezetése • EN szabványok változásainak követése	Polysys Kft. Kővári-Szabó Zoltán	Buczynszkiné dr. Szabó Zsuzsanna Kővári-Szabó Zoltán Nagy Benjámin	Adorján István távollétében és nevében: Kővári-Szabó Zoltán Nagy Benjámin
2.2	2025.11.13.	• ÁSZF alapú szerződéskötés	Buczynskiné dr. Szabó Zsuzsanna	Kővári-Szabó Zoltán	Adorján István

[1] Nem lépett hatályba
[2] Nem lépett hatályba
[3] Nem lépett hatályba

Tartalomjegyzék

1 BEVEZETÉS

Jelen dokumentum a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. (a továbbiakban: Szolgáltató) Időbélyegzés Bizalmi Szolgáltatási Szabályzata, mely a minősített időbélyegzés szolgáltatására vonatkozik (a továbbiakban: IBSZ).

A Szolgáltató jelen bizalmi szolgáltatási rendben szabályozott bizalmi szolgáltatását a {J1} eIDAS rendelet 42. cikke szerinti, minősített elektronikus időbélyegzőket kibocsátó szolgáltatásként kell értelmezni (a továbbiakban: Szolgáltatás).

Szolgáltató a Szolgáltatást két ügyfélcsoport számára nyújtja:

a) azon állampolgárok számára, akik 2024. szeptember 01. napját megelőzően, elektronikus tároló elemmel ellátott állandó személyazonosító igazolványuk e-aláírás funkciójához kapcsolódó szolgáltatások igénybe vételére szolgáltatási szerződést kötöttek (a továbbiakban: eSzemélyi[4] ügyfelek)[5];

b) a {J7} 320/2024 Korm. rendelet 6. § 6. alpontja szerint kormányzati hitelesítés-szolgáltatás keretében, jogi személy vagy jogi személyiség nélküli szervezetek számára (a továbbiakban: közületi ügyfelek).

Jelen bizalmi szolgáltatási szabályzat meghatározza az időbélyegzés szolgáltatás szereplőit, azok feladatait, kötelezettségeit és felelősségeit, a Szolgáltatás működtetésére vonatkozó követelményeket és szabályokat.

A Szolgáltatás keretében kibocsátott, minősített időbélyegzők hozzákapcsolhatók minősített vagy fokozott biztonságú elektronikus aláírással vagy bélyegzővel hitelesített dokumentumokhoz, valamint tetszőleges, nem hitelesített elektronikus dokumentumokhoz is.

Szolgáltató a jelen bizalmi szolgáltatási rendjének hatálya alatt a minősített időbélyegzés szolgáltatás nyújtását azt követően kezdte meg, hogy annak EU minősített státusza a {J1} eIDAS 22. cikke szerinti Bizalmi Listán feltüntetésre került.

1.1 Áttekintés

A szolgáltatási szabályzat célja, hogy összefoglalja mindazokat az információkat, amelyeket a Szolgáltató Szolgáltatásával kapcsolatba kerülő feleknek ismerni szükséges vagy érdemes. Biztosítja a Szolgáltató működésének átláthatóságát és annak megítélését a Szolgáltatást igénybe vevők számára, hogy az ismertetetett szolgáltatási gyakorlat, a kibocsátott időbélyegzők mennyiben felelnek meg az elvárásaiknak.

Jelen szolgáltatási szabályzat az „Időbélyegzés Bizalmi Szolgáltatási Rend” (IBR) hatálya alá tartozó Szolgáltatásra vonatkozik. Az IBR-nek megfelelően kibocsátott időbélyegzők tartalmazzák az IBR objektumazonosítóját, ami 0.2.216.1.200.1100.100.42.3.3.14.

Jelen dokumentum, valamint az 1.6.3 fejezetben hivatkozott jogszabályok, szabványok és műszaki specifikációk, továbbá a Szolgáltató 1.6.3.3 fejezetben felsorolt nyilvános dokumentumai tartalmának megismerése után, az időbélyegzők használói és elfogadói egyértelműen meg tudják

[4] eSzemélyi: a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI törvény {J3} 29. § (1) bekezdésében meghatározott, elektronikus tároló elemmel ellátott, állandó személyazonosító igazolvány (elektronikuskártya), amely alkalmas az ügyfél elektronikus úton történő közhiteles azonosítására, a polgár kérelmére elektronikus aláírás létrehozására és ahhoz kapcsolódóan időbélyegzés szolgáltatás igénybe vételére, valamint a polgár gyakorolhatja vele a külföldre utazás jogát.

[5] A digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló 2023. évi CIII. törvény 119. § (8) bekezdése alapján 2024. szeptember 01. napját követően az állandó személyazonosító igazolvány tároló elemén az elektronikus aláírás létrehozásához szükséges adat nem helyezhető el, amelynek okán a Szolgáltató erre vonatkozó szolgáltatási szerződést nem köt.

állapítani azok kezelésének módját, az általuk garantált biztonság mértékét, valamint a rájuk vonatkozó technikai, üzleti és pénzügyi garanciákat és jogi felelősségvállalásokat.

Jelen szolgáltatási szabályzat az {Sz1} RFC 3647 nemzetközi ajánlás alapján készült, felépítésében és tartalmában követi annak előírásait. Az ott meghatározott felépítés szigorú megtartása érdekében azok a fejezetek is szerepelnek, melyeknél nincs követelmény előírva; ezekben a fejezetekben a „Nincs kikötés" szöveg szerepel. Értelemszerűen, az {Sz1} RFC 3647 4. fejezetének címe és tartalma megváltoztatásra került, a tanúsítványok életciklusa helyett az időbélyegzés szolgáltatással foglalkozik.

Szolgáltató a jelen szolgáltatási szabályzat alapján nyújtott Szolgáltatást a Bizalmi Felügyeletnek 2017.04.28 napján jelentette be. A Bizalmi Felügyelet erre vonatkozó nyilvántartásának elérhetősége: https://esign.nmhh.hu/bszny/

A Bizalmi Lista elérhetősége (amelyen a Szolgáltatás EU minősített státusza feltüntetésre került):
http://www.nmhh.hu/tl/pub/HU_TL.xml (géppel feldolgozható formátum)
http://www.nmhh.hu/tl/pub/HU_TL.pdf (ember által olvasható formátum)

1.2 Dokumentum neve és azonosítása

Jelen bizalmi szolgáltatási szabályzat teljes neve: NISZ Zrt, „Időbélyegzés Bizalmi Szolgáltatási Szabályzat".

A szolgáltatási szabályzat rövid neve: IBSZ.

A szolgáltatási szabályzat objektum azonosítója és verziószáma a címlapon található.

Jelen IBSZ tartalmazza az IBR bizalmi szolgáltatási rend hatálya alatt kiadott időbélyegzők kibocsátására és felhasználására vonatkozó részletes szabályokat. A szolgáltatási szabályzat hatályba lépését és hatályának megszűnését a 9.10 fejezet tartalmazza.

Jelen IBSZ-nek csak a Szolgáltató elektronikus bélyegzőjével vagy a Szolgáltatásért felelős vezető elektronikus aláírásával ellátott változata tekinthető hitelesnek.

1.2.1 Hitelesítési rendek

Az IBR bizalmi szolgáltatási rend megfelel az {Sz14} EN 319 421 szabvány 5.2 fejezet a) pontjában meghatározott BTSP időbélyegzési rendnek:

```
BTSP : a best practices policy for time-stamp.
itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023)
policy-identifiers(1) best-practices-ts-policy (1)
```

1.3 PKI közösség

1.3.1 Hitelesítő szervezet

A hitelesítő szervezet a Szolgáltató központi szervezete, amely az időbélyegző egységekből, a hitelesítő központokból (CA), a szolgáltatás-támogató informatikai rendszer központi erőforrásaiból, az ezt körülvevő biztonságos fizikai környezetből, valamint az üzemeltető és szolgáltatást ellátó személyzetből áll.

A Szolgáltató saját szervezetén kívül más szervezetek nem működnek közre a Szolgáltatás nyújtásában.

RSA Gyökér hitelesítő központ

A Szolgáltató RSA gyökér hitelesítő központja RSA 4096 bites kulcsával és SHA256 algoritmus felhasználásával szolgáltatói tanúsítványok bocsát ki a produktív hitelesítő központok részére. A gyökér hitelesítő központ főbb adatai a következők.

Subject (alany): CN=Főtanúsítványkiadó - Kormányzati Hitelesítés Szolgáltató, O=NISZ Nemzeti Infokommunikációs Szolgáltató Zrt., L=Budapest, C=HU

Issuer (kibocsátó): CN=Főtanúsítványkiadó - Kormányzati Hitelesítés Szolgáltató, O=NISZ Nemzeti Infokommunikációs Szolgáltató Zrt., L=Budapest, C=HU

A gyökér tanúsítvány SHA1 lenyomata:
FF:B7:E0:8F:66:E1:D0:C2:58:2F:02:45:C4:97:02:92:A4:6E:88:03
A gyökér tanúsítvány SHA256 lenyomata:
C2:15:73:09:D9:AE:E1:7B:F3:4F:4D:F5:E8:8D:BA:EB:A5:7E:03:61:EB:81:4C:BC:23:9F:4D:54:D3:29:A3:8D

ECC Gyökér hitelesítő központ

A Szolgáltató ECC alapú gyökér hitelesítő központja P-384-es görbét alkalmazó ECC kulcsával és SHA384 algoritmus felhasználásával szolgáltatói tanúsítványokat bocsát ki a produktív hitelesítő központok részére. Az ECC gyökér hitelesítő központ főbb adatai a következők.

Subject (alany): CN=GovCA Főtanúsítványkiadó, O=NISZ Nemzeti Infokommunikációs Szolgáltató Zrt., L=Budapest, C=HU

Issuer (kibocsátó): CN=GovCA Főtanúsítványkiadó, O=NISZ Nemzeti Infokommunikációs Szolgáltató Zrt., L=Budapest, C=HU

Az ECC gyökér tanúsítvány SHA1 lenyomata:

49:47:E8:6B:02:1F:F2:E3:94:B3:DD:D4:FD:0F:DA:65:78:E6:49:7F

Az ECC gyökér tanúsítvány SHA256 lenyomata:

B1:ED:0B:29:D0:54:2B:2A:13:71:D9:66:F5:8E:42:0B:9E:BD:9C:A1:9F:B9:B2:AF:81:E6:DE:1E:99:D5:E0:8A

RSA Produktív hitelesítő központ

A Szolgáltató RSA produktív hitelesítő központja RSA 2048 bites kulcsával és SHA256 algoritmus felhasználásával RSA alapú időbélyegzőket hitelesítő tanúsítványokat bocsát ki az időbélyegző egységek számára. A produktív hitelesítő központ főbb adatai a következők.

Subject (alany): CN=Minősített Tanúsítványkiadó v2 - GOV CA, O=NISZ Nemzeti Infokommunikációs Szolgáltató Zrt., L=Budapest, C=HU

Issuer (kibocsátó): CN=Főtanúsítványkiadó - Kormányzati Hitelesítés Szolgáltató, O=NISZ Nemzeti Infokommunikációs Szolgáltató Zrt., L=Budapest, C=HU

ECC Produktív hitelesítő központ

A Szolgáltató ECC alapú produktív hitelesítő központja P-384-es görbét alkalmazó ECC kulcsával és SHA384 algoritmus felhasználásával ECC alapú időbélyegzőket hitelesítő tanúsítványokat bocsátanak ki az Előfizetők, illetve a velük kapcsolatban álló Alanyok részére. Az ECC produktív hitelesítő központ főbb adatai a következők.

Subject (alany): CN=GovCA Minősített Időbélyegző Tanúsítványkiadó, O=NISZ Nemzeti Infokommunikációs Szolgáltató Zrt., L=Budapest, C=HU

Issuer (kibocsátó): CN=GovCA Főtanúsítványkiadó, O=NISZ Nemzeti Infokommunikációs Szolgáltató Zrt., L=Budapest, C=HU

Időbélyegző egységek (TSU)

A Szolgáltatás keretében kiadott időbélyegzők előállítását, hitelesítését végző egységek, melyek a produktív hitelesítő központ által erre célra kiadott elektronikus bélyegző tanúsítványokkal végzik az időbélyegzők hitelesítését. Egy TSU mindig egy tanúsítványt és az ahhoz tartozó magánkulcsot használja az általa előállított időbélyegző hitelesítésére. A Szolgáltató egy vagy több TSU-t üzemeltet mind az RSA mind pedig az ECC környezetben, melyek külön-külön tanúsítványokkal és magánkulcsokkal rendelkeznek.

Az egyes TSU-k elérhetőségét a Szolgáltató weboldalán teszi közzé megjelölve, hogy melyik TSU bocsát ki RSA és melyik ECC alapú időbélyegzőt.

Szabályozási Csoport

A Szabályozási Csoport a Szolgáltató által létrehozott szervezeti egység, amely a bizalmi szolgáltatásokkal kapcsolatos bizalmi szolgáltatási rendek, szolgáltatási szabályzatok és egyéb szabályzatok elkészítéséért, elfogadásáért, karbantartásáért és adminisztrációjáért felelős.

1.3.2 Ügyfélkapcsolati Iroda

A Szolgáltató – saját szervezetén belül – Ügyfélkapcsolati Irodát működtet.

Az Ügyfélkapcsolati Iroda végzi a közületi ügyfelekkel való kapcsolattartást, az adataik felvételét, a hozzáféréseik beállítását, és közreműködik a szolgáltatási szerződés megkötésében.

Az eSzemélyi tulajdonosok számára nyújtott időbélyegzés szolgáltatás vonatkozásában az Ügyfélkapcsolati Iroda nem működik közre. Az eSzemélyi ügyfelekkel való kapcsolattartás módját, a szolgáltatási szerződés megkötésének eljárását a BSZ-ESZIG szabályzat tartalmazza.

1.3.3 Előfizetők

Előfizető a Szolgáltatóval szerződéses viszonyban álló állampolgár vagy szervezet (jogi személy vagy közhiteles nyilvántartásban szereplő, jogi személyiség nélküli szervezet), aki / amely megrendeli a Szolgáltatótól a Szolgáltatást, és azt igénybe veszi, azaz időbélyegző kéréseket nyújt be Szolgáltatóhoz, amelyekre elektronikus időbélyegzőt tartalmazó válaszokat (röviden időbélyegeket) kap.

Előfizető lehet a(z):

a) eSzemélyi ügyfél vagy

b) a közületi ügyfél.

A közületi ügyfelek Előfizető kapcsolattartót jelölhetnek ki, akit a képviseleti joggal rendelkező személy (pl. cégjegyzésre jogosult) felhatalmaz, illetve feljogosít a szolgáltatással kapcsolatos ügyekben Előfizető szervezete nevében eljárni, akár meghatározott esetekre kiterjedő aláírási joggal is. Szolgáltató a későbbiekben – a képviseletre jogosult személy(ek)en felül – ezen személy aláírását fogadja el a szolgáltatással kapcsolatos ügyekben, különösen a annak igénylési vagy lemondási folyamatában, az ezekhez kapcsolódó kérelmeken. Kapcsolattartó kijelölésének hiányában Szolgáltató csak a képviseleti joggal rendelkező személy (pl. cégjegyzésre jogosult) aláírását fogadja el a szolgáltatással kapcsolatos ügyekben.

Jelen dokumentumban a továbbiakban az Előfizető Kapcsolattartója kifejezés a fentiek szerint kijelölt személyt, illetve kijelölés hiányában a képviseleti joggal rendelkező (pl. cégjegyzésre jogosult) személyt jelenti.

Az Előfizetők felelősségeit a 9.6.3 fejezet tartalmazza.

1.3.4 Érintett felek

Érintett Fél: az időbélyegzővel ellátott elektronikus dokumentumot fogadó természetes vagy jogi személy, aki/amely az elektronikus időbélyegzőre hagyatkozva jár el a dokumentum időbeliségének és sértetlenségének vagy a dokumentumhoz kapcsolódó elektronikus aláírás vagy elektronikus bélyegző ellenőrzésekor.

1.3.5 Egyéb felek

Bizalmi Felügyelet

A Bizalmi Felügyelet ellátja a Szolgáltató és az általa nyújtott bizalmi szolgáltatások felügyeletét, ellenőrzi a szolgáltatások jogszabályi megfelelőségét. Többek között, figyelemmel kíséri a bizalmi szolgáltatásokkal kapcsolatos technológia és kriptográfiai algoritmusok fejlődését és határozatba foglalja a bizalmi szolgáltatók által a szolgáltatásaik nyújtása során használható biztonságos kriptográfiai algoritmusokat, és az azok meghatározott paraméterekkel történő alkalmazására vonatkozó követelményeket.

1.4 Az elektronikus időbélyegző alkalmazhatósága

Az IBSZ hatálya alatt kiadott időbélyegzők a {J1} eIDAS 42. cikke szerinti minősített elektronikus időbélyegzők, melyek alkalmasak az időbélyegzett adatok sértetlenségének, valamint az elektronikus aláírás vagy bélyegzés dátumának és időpontjának bizonyítására.

A minősített elektronikus időbélyegző joghatását a {J1} eIDAS 41. cikke határozza meg. E szerint, a minősített elektronikus időbélyegzőt bírósági eljárásokban bizonyítékként el kell fogadni és vélelmezni kell az általa feltüntetett dátum és időpont pontosságát, valamint az adott dátumhoz és időponthoz kapcsolt adatok sértetlenségét.

A Szolgáltató által a Szolgáltatás keretében kiadott időbélyegzők azonosíthatók azáltal, hogy azokat az időbélyegző egységek olyan elektronikus bélyegzés célú tanúsítvánnyal hitelesítik, amelyben (a `Subject` mezőben) szerepel a Szolgáltató közhiteles nyilvántartás szerinti teljes neve és közösségi adószáma. Emellett a Szolgáltatás keretében kiadott időbélyegzők tartalmazzák az IBR objektumazonosítóját is.

1.4.1 Engedélyezett időbélyegző használat

Az eSzemélyi ügyfelek a Szolgáltatást csak és kizárólag az elektronikus tároló elemmel rendelkező személyazonosító igazolványuk e-aláírás funkciójának felhasználásával történő elektronikus aláíráshoz kapcsolódóan jogosultak igénybe venni, magánszemélyként.

A közületi ügyfelek számára a Szolgáltatás használatára vonatkozóan nincs ilyen jellegű korlátozás.

A fentieken túl a Szolgáltatás keretében kibocsátott időbélyegzők csak a {D1} Általános Szerződési Feltételekben, illetve a {D2} Szolgáltatási Szerződésben rögzített feltételekkel használhatók fel.

1.4.2 Tiltott időbélyegző használat

Az eSzemélyi ügyfelek számára a Szolgáltatás használata üzleti, munkahelyi vagy ilyen jellegű szakmai tevékenység céljából nem megengedett.

Az eSzemélyi ügyfél által igényelhető időbélyegzők számát Szolgáltató jogosult korlátozni.

1.5 Szabályzat adminisztráció

1.5.1 Szabályzatot karbantartó szervezet

A Szolgáltatónak szervezetén belül Szabályozási Csoportot működtet, amely többek között jelen bizalmi szolgáltatási szabályzat karbantartásáért is felelős.

1.5.2 Kapcsolat

Szolgáltató adatai

Cégjegyzék szám:	01-10-041633
Székhely:	1149 Budapest, Róna utca 52-80.
Levélcím:	1389 Budapest, Pf.: 133.
Telefon:	+36 1 459-4200
Fax:	+36 1 303-1000
Internetes honlap címe:	www.nisz.hu
Adatvédelmi és adatbiztonsági szabályzat:	A https://hiteles.gov.hu/szabalyzatok oldalon, az „*Adatkezelési tájékoztató kormányzati hitelesítés-szolgáltatásokhoz*” címen érhető el.

Illetékes fogyasztóvédelmi felügyelőség

Budapest Főváros Kormányhivatala, Fogyasztóvédelmi Főosztály

Cím:	1051 Budapest, Sas utca 19.
Telefon:	+36 1 450-2598
Email:	fogyved_kmf_budapest@bfkh.gov.hu

Illetékes békéltető testület

Budapesti Békéltető Testület

Cím:	1016 Budapest, Krisztina krt. 99. I. em. 111.
Levelezési cím:	1253 Budapest, Pf.:10.
Telefon:	+36 1 488 2131
Email:	bekelteto.testulet@bkik.hu

1.5.2.1 Kapcsolat az ügyfelekkel eSzemélyi esetén

Az időbélyegzés szolgáltatást igénybe vevő eSzemélyi tulajdonosok a Kormányzati Ügyfélvonalon vehetik fel Szolgáltatóval a kapcsolatot.

Telefon:	1818 Kormányzati Ügyfélvonal, külföldről: +36 1 550-1858
Email:	ekozig@1818.hu
Postacím:	Kormányzati Ügyfélvonal, 1389 Budapest, Pf: 133

Az időbélyegzés szolgáltatást igénybe vevő eSzemélyi tulajdonosok előzőekben foglalt elérhetőségek valamelyikén terjeszthetnek elő panaszt a Szolgáltató számára.

1.5.2.2 Kapcsolat az ügyfelekkel közületi ügyfelek esetében

Ügyfélkapcsolati Iroda

A közületi ügyfelekkel való kapcsolattartás érdekében a Szolgáltató Ügyfélkapcsolati Irodát tart fenn, mely egyben a Szolgáltatásért illetékes szervezeti egység, és amelyet a közületi ügyfelek személyesen, emailben, illetve telefonon a nyitvatartási időkben kereshetnek fel. A mindenkori nyitvatartási időket a Szolgáltató a Szolgáltatás internetes honlapján teszi közé.

Cím:	1097 Budapest, Vaskapu utca 30/b.
Telefon:	+36 1 795-7200
Email:	info@hiteles.gov.hu
Szolgáltatás internetes honlapja	https://hiteles.gov.hu/

Telefonos Ügyfélszolgálat

A Szolgáltatás nyújtásához felhasznált rendszerrel kapcsolatos műszaki hibák bejelentésére a Szolgáltató folyamatos (7x24 órás) ügyfélszolgálatot (Help Desk) biztosít.

Telefon:	+36 1 795-7300
Email:	helpdesk@nisz.hu

1.5.3 Szabályzat alkalmasságának meghatározása

A Szolgáltató legalább évente egyszer megvizsgálja a bizalmi szolgáltatási szabályzat tartalmi és formai megfelelőségét a vonatkozó jogszabályok, előírások és műszaki szabványok tekintetében, melynek eredményeit változtatási igényként figyelembe veszi.

Amennyiben a változtatási igények befolyásolhatják a Szolgáltatásnak az Alanyok, Előfizetők vagy Érintett Felek általi elfogadását, a Szolgáltató erről előzetes értesítést tesz közzé a Szolgáltatások internetes honlapján.

A változtatási igényeket a Szabályozási Csoport gyűjti, a módosításokat elvégzi, majd ellenőrzésre és jóváhagyásra előterjeszti.

1.5.4 Szabályzat jóváhagyásának eljárása

Az ellenőrzésre, illetve jóváhagyásra a Szolgáltató belső szervezete, illetve a Szolgáltatásért felelős vezetője rendelkezik hatáskörrel és felelősséggel.

A jóváhagyás előtt a Szolgáltató megvizsgálja a szolgáltatási szabályzat bizalmi szolgáltatási rendnek való megfelelését.

A szolgáltatási szabályzat jogszabályoknak való megfelelőségét a Bizalmi Felügyelet is ellenőrzi.

A jóváhagyott szolgáltatási szabályzat a Szolgáltató elektronikus bélyegzőjével vagy a Szolgáltatásért felelős vezető elektronikus aláírásával kerül hitelesítésre.

A jóváhagyott szolgáltatási szabályzatot a Szolgáltatásért felelős vezető lépteti hatályba a szabályzat hitelesítése által. A hatályba lépés napját a dokumentum címlapja tartalmazza.

A szolgáltatási szabályzat új verziója mindig új verziószámmal kerül nyilvánosságra és egy munkanapon belül közzétételre a Szolgáltató internetes honlapján.

Az új verzió kötelező érvényű az összes Előfizetőre, továbbá az abban foglalt változásokat javasolt figyelembe vennie az összes, a bizalmi szolgáltatási rend előző verzióinak hatálya alatt kibocsátott időbélyegeket felhasználó Érintett Félnek.

1.6 Fogalmak, rövidítések és hivatkozások

1.6.1 Fogalmak

Jelen szabályzatban használt fogalmak értelmezése megegyezik a Szolgáltatásra vonatkozó jogszabályokban (1.6.3.1 fejezetben) szereplő meghatározásokkal.

Az ezen felül alkalmazott fogalmak meghatározását az IBR szabályzat 1.6.1 fejezete tartalmazza.

1.6.2 Rövidítések

BTSP	Best Practices Policy for Time-Stamp	legjobb gyakorlatok időbélyegzés szolgáltatásra
CA	Certification Authority	hitelesítő központ
CRL	Certificate Revocation List	tanúsítvány visszavonási lista
ECC	Elliptic Curve Criptogaphy	elliptikus görbe alapú aláíró algoritmus
HTTPS	HyperText Transfer Protocol Secure	biztonságos hipertext átviteli protokoll
OCSP	Online Certificate Status Protocol	valós idejű tanúsítvány-állapot protokoll
PKI	Public Key Infrastructure	nyilvános kulcsú infrastruktúra
RSA	Rivest–Shamir–Adleman	aláíró algoritmus
SHA	Secure Hash Algorithm	lenyomatképző algoritmus
TDS	TSA Disclosure Statement	TSA Közzétételi Nyilatkozat
TSA	Time-Stamping Authority	időbélyegzés szolgáltató
TSU	Time-Stamping Unit	időbélyegző egység
URI	Uniform Resource Identifier	elérhetőség helyét és módját leíró webcím
UTC	Coordinated Universal Time	egyezményes koordinált világidő

1.6.3 Hivatkozások

1.6.3.1 Jogszabályi hivatkozások

{J1} 910/2014/EU Európai Parlament és a Tanács rendelete a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről
(a továbbiakban: eIDAS)

{J2} 2023. évi CIII. a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól[6]
(a továbbiakban: DÁP tv.)

{J3} 1992. évi LXVI. törvény a polgárok személyi adatainak és lakcímének nyilvántartásáról
(a továbbiakban: Nytv.)

{J4} 2016. évi CXXX. törvény a polgári perrendtartásról
(a továbbiakban: Pp.)

{J5} 2013. évi V. törvény a Polgári Törvénykönyvről
(a továbbiakban: Ptk.)

{J6} 321/2024 (XI. 6.) Korm. rendelet
a digitális állampolgárság egyes szabályairól

{J7} 320/2024 (XI. 6.) Korm. rendelet
a digitális állam megvalósításához kapcsolódó egyes szervezetek kijelöléséről

{J8} 24/2016 (VI. 30.) BM rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről

{J9} 322/2024 (XI. 6.) Korm. rendelet a digitális szolgáltatások, a digitális állampolgárság szolgáltatások és támogató szolgáltatások részletes műszaki követelményeiről

{J10} 679/2016/EU Európai Parlament és Tanács rendelete 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
(a továbbiakban: GDPR)

{J11} 2555/2022/EU Európai Parlament és a Tanács irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról
(továbbiakban: NIS2 irányelv)

{J12} 2024. évi LXIX. Törvény Magyarország kiberbiztonságáról
(továbbiakban: kiberbiztonsági tv.)

{J13} 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről

[6] A DÁP tv. 121. § helyezte hatályon kívül az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény (röviden: E-ügyintézés tv.) rendelkezéseit. Figyelembe véve, hogy a DÁP tv. 118. §-ában foglalt bekezdések alapján az E-ügyintézés tv. bizonyos részei 2025.07.01. napjáig alkalmazhatóak, így a Szolgáltató is eljárásai során – ahol ez értelmezhető és szükséges – figyelembe veszi az abban foglaltakat.

1.6.3.2 Szabványok és műszaki-technikai specifikációk

{Sz1}	RFC 3647	Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework
{Sz2}	EN 319 401	General policy requirements for Trust Service Providers
{Sz3}	EN 319 411-1	Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
{Sz4}	EN 319 412-1	Certificate Profiles; Part 1: Overview and common data structures
{Sz5}	EN 319 412-2	Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
{Sz6}	EN 319 412-3	Certificate Profiles; Part 3: Certificate profile for certificates issues to legal persons
{Sz7}	EN 319 412-5	Certificate Profiles; Part 5: QCStatements
{Sz8}	RFC 5280	Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile
{Sz9}	ITU-T X.520	Information technology - Open Systems Interconnection - The Directory: Selected attribute types
{Sz10}	RFC 4514	Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names
{Sz11}	ITU-T X.509	Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate framework
{Sz12}	RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
{Sz13}	EN 319 411-2	Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
{Sz14}	EN 319 421	Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
{Sz15}	EN 319 422	Time-Stamping protocol and time-stamp token profiles
{Sz16}	RFC 3161	Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)
{Sz17}	RFC 5816	ESSCertIDV2 update to RFC 3161
{Sz18}	ETSI TS 119 312	Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
{Sz19}	MSZ/ISO/IEC 15408	ISO/IEC 15408 (parts 1 to 3): Information technology – Security techniques – Evaluation criteria for IT security
{Sz20}	ISO/IEC 19790	ISO/IEC 19790:2012: Information technology – Security techniques – Security requirements for cryptographic modules

{Sz21}	FIPS 140-2	FIPS PUB 140-2 (2001): Security Requirements for Cryptographic Modules
{Sz22}	RFC 2616	Hypertext Transfer Protocol – HTTP/1.1
{Sz23}	FIPS 140-3	FIPS PUB 140-3 (2019): Security Requirements for Cryptographic Modules

1.6.3.3 Hivatkozott dokumentumok

{D1}	ÁSZF-GOVCA	Általános Szerződési Feltételek a NISZ Zrt. kormányzati hitelesítés szolgáltatásaihoz
{D2}	SZSZ	Szolgáltatási Szerződés
{D3}		NISZ Zrt. Szervezeti és Működési Szabályzata
{D4}		NISZ Zrt. Adatvédelmi és adatbiztonsági előírásai
{D5}		NISZ Zrt. PKI szolgáltatások informatikai biztonságpolitikája
{D6}		NISZ Zrt. PKI szolgáltatások biztonsági szabályzata
{D7}		NISZ Zrt. PKI szolgáltatások üzletmenet-folytonossági terve
{D8}		NISZ eIDAS tanúsítványprofilok
{D9}		Tanúsítvány megrendelő és regisztrációs űrlap
{D10}	BSZ-ESZIG	Bizalmi Szolgáltatási Szabályzat a személyazonosító igazolványokhoz kibocsátott minősített tanúsítványokhoz
{D11}		NISZ Zrt. tájékoztatója az eSzemélyi -hez kapcsolódó időbélyegzés szolgáltatás igénybe vételének műszaki feltételeiről

2 KÖZZÉTÉTEL ÉS TANÚSÍTVÁNYTÁR

2.1 Szabályzatok elérhetősége

A Szolgáltató gondoskodik arról, hogy a Szolgáltatással kapcsolatos szabályzatok, az időbélyegző egységek tanúsítványai visszavonási állapotára vonatkozó információk, valamint az egyéb közérdekű szolgáltatói információk az Előfizetők és Érintett Felek részére folyamatosan rendelkezésre álljanak. Szolgáltató az információk elérhetőségét az év minden napján, napi 24 órában, 99,9 %-os rendelkezésre állással biztosítja, úgy, hogy a kiesés nem lépheti túl esetenként a 3 órás időtartamot.

A Szolgáltató nem hozza nyilvánosságra azokat az érzékeny és/vagy bizalmas információkat tartalmazó dokumentációkat, melyek biztonsági intézkedéseket, eljárási szabályokat és belső biztonsági szabályzatokat tartalmaznak.

2.2 A szolgáltatói információ közzététele

A Szolgáltató a szolgáltatói tanúsítványokat (beleértve az időbélyegző egységek tanúsítványait), valamint a Szolgáltatással, illetve a szolgáltatói tanúsítványokkal kapcsolatos szabályzatokat és egyéb közérdekű szolgáltatói információkat internetes honlapján (https://hiteles.gov.hu) teszi közzé.

Szolgáltató az időbélyegző egységek által használt tanúsítványokat az internetes honlapján elérhető nyilvános tanúsítványtárban teszi közzé és biztosítja ezek kereshetőségét és elérhetőségét a tanúsítvány lejártát követő 10 évig.

Szolgáltató az egyéb szolgáltatói (gyökér és produktív hitelesítő központok) tanúsítványokat internetes honlapján teszi közzé.

A Szolgáltató az időbélyegző egységek tanúsítványaival kapcsolatos visszavonási állapot információkat CRL és OCSP formájában is biztosítja. A visszavonási állapot információk közzétételével kapcsolatos információkat a 4.8 fejezet tartalmazza.

2.3 A közzététel gyakorisága

Szolgáltató a Szolgáltatással kapcsolatos szabályzatokat azok változása esetén közzé teszi legalább 30 nappal a változás hatályba lépését megelőzően.

Szolgáltató az időbélyegző egységek által használt tanúsítványokat és egyéb szolgáltatói tanúsítványokat legkésőbb azok éles üzembe helyezését megelőző 24 órán belül közzé teszi.

Szolgáltató az időbélyegző egységek visszavonási állapotával kapcsolatos CRL-t legalább 24 óránként frissíti, azaz két egymást követő CRL kibocsátási között idő nem haladja meg a 24 órát. Amennyiben egy tanúsítvány állapota megváltozik, a Szolgáltató a változást követően haladéktalanul, de legfeljebb 1 órán belül új CRL-t állít elő és tesz közzé.

Szolgáltató az OCSP szolgáltatása keretében minden OCSP kérésre friss választ állít elő és ad vissza.

2.4 Hozzáférés-ellenőrzések

Szolgáltató olvasás céljára korlátozás nélküli hozzáférést biztosít a szolgáltatói tanúsítványokhoz (beleértve az időbélyegző egységek tanúsítványait), ezek visszavonási információihoz, valamint a Szolgáltatással kapcsolatos szabályzatokhoz.

Szolgáltató biztonsági intézkedésekkel és eljárási szabályokkal gondoskodik az információk jogosulatlan megváltoztatása, törlése, sérülése és megsemmisülése elleni védelemről.

A szabályzatoknak csak az elektronikus aláírással vagy bélyegzővel ellátott formája tekinthető hitelesnek, a dokumentumok nyomtatott változatai semmilyen formában nem tekinthetők hivatalos példánynak vagy hiteles másolatnak.

3 AZONOSÍTÁS

A Szolgáltató az időbélyegzők kiadását a felhasználók előzetes azonosításához köti.

3.1 Időbélyegzés szolgáltatás igénylése

3.1.1 eSzemélyi ügyfelek esetén

A {J2} DÁP tv. 119. § (8) bekezdése alapján az állandó személyazonosító igazolvány tároló elemén az elektronikus aláírás létrehozásához szükséges adat nem helyezhető el, amelynek okán a Szolgáltató 2024. szeptember 01. napjától további Szolgáltatási szerződést nem köt. Az időbélyegzés szolgáltatást továbbra is biztosítja azon eSzemélyi ügyfelek számára, akik rendelkeznek érvényes és hatályos Szolgáltatási szerződéssel, amely 2024. szeptember 01. napját megelőzően került megkötésre.

A további információkat a {D1} BSZ-ESZIG 4.1.2 fejezet tartalmazza.

3.1.2 Közületi ügyfelek esetén

Időbélyegzés szolgáltatást csak jogi személy vagy közhiteles nyilvántartásban szereplő, jogi személyiség nélküli szervezet igényelhet.

Az időbélyegzés szolgáltatás igénybevétele a Szolgáltató és az Előfizető között megkötött Szolgáltatási Szerződés keretében lehetséges. Ezen szerződés keretében Előfizető írásbeli nyilatkozatot ad arra vonatkozóan, hogy a Szolgáltató nyilvánosan közzétett szabályzataiban részletesen tárgyalt kötelezettségeit, felelősségét és jogait ismeri és elfogadja azokat.

1) A Szolgáltató kétféle szerződéskötési folyamatot követ:
   a) bizonyos feltételek együttes fennállása esetén a szolgáltatási szerződés létrejön az Általános Szerződési Feltételek (ÁSZF-GOVCA) elfogadásával,
   b) minden más esetben a Szolgáltató és az Előfizető egyedileg létrejött szolgáltatási szerződést (a továbbiakban: Egyedi Szolgáltatási Szerződés) köt.
2) A Szolgáltató és az Előfizető az alábbi feltételek együttes fennállása esetén szolgáltatási szerződést köt Általános Szerződési Feltételek (ÁSZF-GOVCA) elfogadásával:
   a) az Előfizető számára az igényelt tanúsítvány-szolgáltatás jogszabály alapján díjmentesen biztosítható(ak)[7],
   b) az Előfizető az adott tanúsítvány-szolgáltatáshoz nem igényelt úgynevezett Minősített Elektronikus Aláírást Létrehozó Eszközt (röviden: MALE, angolul: QSCD; az elérhető termékeket a Szolgáltató hivatalos honlapján teszi közzé),
   c) az Előfizető személyazonosítása és az elkészült tanúsítvány-szolgáltatás átadás-átvétele díjmentes formában valósul meg (különösképpen a Szolgáltató telephelyén),
   d) az Előfizető a megrendelő űrlapon egyértelmű nyilatkozatával megértette és elfogadta az ÁSZF-GOVCA aktuális verzióját és a benne foglaltakat,
   e) a megrendelő űrlap Szolgáltató számára történő elektronikus levélformában történő beküldésekor az Előfizető nem élt az egyedi Szolgáltatási szerződéskötés lehetőségével.

[7] A DÁP tv. 39. § (6) bekezdés szerint a tanúsítvány-szolgáltatás díjmentesen biztosítható a DÁP tv. 9. § (2) bekezdés szerinti szerveknek, szervezeteknek és intézményeknek. Az adott jogszabály alapján a díjmentességet az Ügyfélkapcsolati Iroda állapítja meg (úgynevezett igénybevételi jogalap validáció).

3) A Szolgáltató nyilvános ajánlata és a szolgáltatás ÁSZF-GOVCA-ban foglaltakkal összhangban történő igénylése eredményeképp a Szolgáltatási Szerződés megkötöttnek minősül, ha:
   a) az Előfizető igénye megfelel az előzőekben megjelölt feltételeknek,
   b) a megrendelő űrlap hiánypótlás nélkül feldolgozható;
   c) a tanúsítvány-szolgáltatás kibocsátása (gyártás) megvalósult.

A Szolgáltatási szerződés 3) pontban megjelölt módon történő megkötése írásbelinek minősül.

A Egyedi Szolgáltatási Szerződés megkötéséhez a {D9} Tanúsítvány megrendelő és regisztrációs űrlap kitöltése és cégszerű aláírása szükséges. Ezen űrlap keretében Előfizető nyilatkozik arról, hogy az általa kijelölt természetes személy (Előfizető Kapcsolattartója) a Szolgáltatás igénybevételéhez szükséges autentikációs tanúsítványt igényeljen, illetve vegyen át Szolgáltatótól, a kapcsolódó magánkulccsal együtt.

Ehhez kapcsolódóan az alábbi dokumentumok bemutatása szükséges:
- Előfizető szervezetének 30 napnál nem régebbi cégkivonata vagy egyéb hivatalos okmánya (pl. alapító okirat);[8]
- az aláírásra jogosult vezető tisztségviselő aláírási címpéldánya.

Az Ügyfélkapcsolati Iroda megtagadhatja az Egyedi Szolgáltatási Szerződés megkötését, ha:
- Előfizető, mint szervezet kiléte nem állapítható meg minden kétséget kizáró módon;
- az Előfizető részéről eljáró természetes személy (Előfizető Kapcsolattartója) által bemutatott személyazonosító okmányok személyhez tartozásával, valódiságával vagy érvényességével kapcsolatban kétsége merül fel;
- egyéb, indokolt esetben.

A Szolgáltatási Szerződés megkötését követően Szolgáltató átadja Előfizető Kapcsolattartója részére a Szolgáltatás igénybe vételéhez szükséges autentikációs tanúsítványt és a kapcsolódó magánkulcsot (CD-n, .p12 kiterjesztésű fájlban), illetve a tanúsítvány telepítéséhez szükséges jelszót tartalmazó PIN-borítékot („aktivizáló kódot”).

3.2 Azonosítás és jogosultság ellenőrzés

3.2.1 eSzemélyi ügyfelek esetén

Az eSzemélyi tulajdonos az időbélyegzés szolgáltatás igénybevételéhez olyan alkalmazást kell használjon, amellyel az időbélyegző kérés elektronikusan aláírható az eSzemélyi-n levő magánkulccsal a {D11} eSzemélyihez kapcsolódó időbélyegzés szolgáltatás igénybevételének műszaki feltételeiről tájékoztatónak megfelelően.

3.2.2 Közületi ügyfelek esetén

Az időbélyegzés szolgáltatás igénybevételekor a Szolgáltató az Előfizetővel felépített biztonságos csatornán (HTTPS) keresztüli tanúsítvány alapú kliens azonosítást alkalmaz.

[8] A szervezeti adatok igazolhatóak közhiteles nyilvántartásban foglalt adatokkal is.

4 Az időbélyegzés szolgáltatás

Az elektronikus időbélyegző „*olyan elektronikus adatokat tartalmaz, amelyek más elektronikus adatokat egy adott időponthoz kötnek, amivel igazolják, hogy az utóbbi adatok léteztek az adott időpontba*n” ({J1} eIDAS 3. cikk, 33. bekezdés).

Szolgáltató a jelen bizalmi szolgáltatási szabályzata hatálya alatt minősített időbélyegzés szolgáltatást nyújt, melyről a legfontosabb információkat tartalmazó, TSA Közzétételi Nyilatkozatot (TDS) készített. A TDS-t a jelen szolgáltatási szabályzat melléklete tartalmazza.

Az elektronikus időbélyegző kérésének és felhasználásának folyamata röviden az alábbi:

- Előfizető – egy erre alkalmas számítógépes programmal – kiszámítja az időbélyegzővel ellátandó elektronikus dokumentum lenyomatát és azzal szabványos időbélyegző kérést állít elő;
- Előfizető számítógépes programja az időbélyegző kérést Interneten elküldi Szolgáltatónak;
- Szolgáltató azonosítja Előfizetőt és elbírálja, hogy jogosult-e időbélyegzőt kérni:
    - eSzemélyi ügyfél esetén: Szolgáltató az időbélyegzőt azt követően bocsátja ki, hogy meggyőződött arról, hogy Előfizető birtokolja azt az eSzemélyi-t, amellyel kapcsolatban a szerződéses jogviszony létrejött. Ennek céljából Szolgáltató megköveteli, hogy az időbélyegző kérést Előfizető a beküldés előtt az eSzemélyi-n tárolt minősített tanúsítványához tartozó magánkulccsal írja alá.
      Ehhez Előfizetőnek olyan számítógépes programot kell használnia az időbélyegző kérés összeállítására, amely képes az időbélyegző kérés aláírására, a {D11} tájékoztatóban leírtaknak megfelelően.
      Az időbélyegző kérelem elfogadása vagy visszautasítása a kérésen elhelyezett elektronikus aláírás ellenőrzését és jogosultság ellenőrzését követően automatikusan történik.
    - Közületi ügyfél esetén: az időbélyegző kérelmet az Előfizető erre feljogosított felhasználói küldhetnek be. Előfizető azzal jogosítja fel a szervezetén belüli felhasználókat, hogy rendelkezésükre bocsátja a 3.1.2 fejezetben leírt autentikációs tanúsítványt, a kapcsolódó magánkulcsot és aktivizáló kódot.
      Az időbélyegző kérelem elfogadása vagy visszautasítása azzal történik meg, hogy a HTTPS biztonságos csatorna az autentikációs tanúsítványon alapuló kliens azonosítással létrejön-e vagy sem.
- Szolgáltató ellenőrzi az időbélyegző kérés formai és tartalmi megfelelőségét, illetve azt, hogy időbélyegző válasz kiadható-e;
- sikeres ellenőrzést követően Szolgáltató szabványos időbélyegző választ állít elő és küld vissza Interneten keresztül Előfizető számára;
- Előfizető számítógépes programja ellenőrzi a kapott időbélyegző választ;
- sikeres ellenőrzést követően Előfizető számítógépes programja az időbélyegzőt:
    - hozzákapcsolja az adott elektronikus dokumentumhoz; vagy
    - elhelyezi abban az elektronikus aláírásban vagy bélyegzőben, melyet az adott elektronikus dokumentum hitelesítésére hoztak létre.
- a későbbiekben, Előfizető vagy bármely Érintett Fél az elektronikus időbélyegzőt felhasználhatja arra, hogy bizonyítsa:
    - az elektronikus dokumentum, amelyhez az időbélyegzőt hozzákapcsolták, létezett az időbélyegben szereplő időpontban és az elektronikus dokumentum az időbélyegző hozzákapcsolását követően nem változott meg; vagy

- az elektronikus aláírás vagy bélyegző - melyet az adott elektronikus dokumentum hitelesítése céljára hoztak létre, és amelyben az elektronikus időbélyegző szerepel – biztosan az időbélyegzőben jelzett időpontot megelőzően került létrehozásra.

4.1 Időbélyegző kérés

Előfizetőnek olyan számítógépes programot kell használnia az időbélyegző kéréséhez, amely képes az {Sz16} RFC 3161 szabvány 2.4.1 fejezetének megfelelő időbélyegző kérést előállítani és azt a 3.2 fejezetben leírt azonosítási eljárással beküldeni.

Szolgáltató csak olyan időbélyegző kérést fogad, melyben a tartalmazott lenyomat (`messageImprint`) algoritmusa SHA256.

Erősen javasolt, hogy Előfizető számítógépes programja támogassa a kérésben a `reqPolicy`, `nonce` és `certReq` mezők használatát:

- ha a kérésben szerepel a `reqPolicy` mező, akkor annak az IBR objektumazonosítóját kell tartalmaznia;
- erősen javasolt a kérésben szerepeltetni a `nonce` mezőt, mely az időbélyegző egyediségét biztosítja;
- erősen javasolt a `certReq` mezőben a TRUE értékkel kérni azt, hogy az időbélyegző válaszban az időbélyeget hitelesítő tanúsítvány is szerepeljen, annak érdekében, hogy az időbélyegző hitelessége a későbbiekben könnyen ellenőrizhető legyen.

Az időbélyegző kérés nem tartalmazhat kiterjesztéseket (`extensions`).

Szolgáltató nem támogatja az {Sz22} RFC 2616 14.20 fejezete szerinti `Expect` HTTP header-t az időbélyegző kérés beküldése során.

4.2 Időbélyegzés szolgáltatás elérhetősége és rendelkezésre állása

A Szolgáltatás kizárólag csak biztonságos HTTPS protokollon, ügyfélazonosítást követően vehető igénybe.

Szolgáltató biztosítja, hogy a Szolgáltatás az Előfizetők részére folyamatosan – 99,9 %-os szinten - rendelkezésre álljon úgy, hogy egy eseti szolgáltatáskiesés időtartama nem haladhatja meg a három órát.

4.2.1 Szolgáltatás elérhetősége

4.2.1.1 Szolgáltatás elérhetősége eSzemélyi ügyfelek számára

Az időbélyegzés szolgáltatás elérhetősége: *https://eszigts.hiteles.gov.hu/ts*

4.2.1.2 Szolgáltatás elérhetősége közületi ügyfelek számára

Az időbélyegzés szolgáltatás elérhetősége: *https://tsa.hiteles.gov.hu/ts*

4.3 Időbélyegző kérés elfogadása vagy visszautasítása

Szolgáltató ellenőrzi a kapott időbélyegző kérés formai és tartalmi megfelelőségét.

Szolgáltató visszautasítja az időbélyegző kérést, ha:

- Előfizető azonosítása sikertelen;

- a kérés formátuma vagy tartalma nem felel meg a 4.1 fejezetben leírt követelményeknek;
- az időbélyegző egység belső órája a vállalt pontosságnál nagyobb mértékkel eltér az UTC pontos időtől;
- az időbélyegző egység pontos idő szinkronizációja sikertelen;
- az időbélyegző egység magánkulcsához tartozó tanúsítvány nincs beimportálva az időbélyegző egységbe vagy annak HSM moduljába;
- az időbélyegző egység magánkulcsának használati időtartama (6.3.2 fejezet) lejárt;
- az időbélyegző egység tanúsítványa lejárt vagy még nem érvényes;
- az időbélyegző egység tanúsítványa hitelességének ellenőrzése (beleértve az {Sz8} RFC 5280 6. fejezete szerinti tanúsítási útvonal felépítést, érvényesítést és a visszavonás ellenőrzést is) sikertelen.

Szolgáltató elfogadja az időbélyegző kérést, ha fenti ellenőrzések mindegyike sikeresen megtörtént.

4.4 Időbélyegző válasz

A Szolgáltatás keretében kiadott időbélyegző válasz mindenben megfelel az {Sz16} RFC 3161, valamint az {Sz15} EN 319 422 szabványnak.

Szolgáltató a Szolgáltatás keretében csak és kizárólag minősített időbélyegzőket ad ki.

Az időbélyegző válasz tartalmazza:

- a verziószámot „1” értékkel (a `version` mezőben);
- az IBR objektum azonosítóját (a `policy` mezőben);
- a kérésben levő lenyomatot (a `messageImprint` mezőben);
- az időbélyegző egyedi sorszámát (a `serialNumber` mezőben);
- a dátumot és pontos időpontot a vállalt pontossággal (a `genTime` mezőben);
- a vállalt pontosságot (az `accuracy` mezőben);
- a `nonce` véletlenszámot, ha a kérésben szerepelt olyan;
- az adott időbélyegző ellőállítását végző időbélyegző egység azonosítóit (a `tsa` mezőben);
- annak jelzését, hogy az időbélyegző EU minősített bizalmi szolgáltatásban került kiadásra (a `QcStatements` kiterjesztésben a `tst-EuQcCompliance`[9] nyilatkozattal);
- az időbélyegző egység által az időbélyegző hitelesítésére használt tanúsítványt (a `SignedData` / `certificates` mezőben).

Az időbélyegző nem tartalmaz:

- sorrendiség jelzést (`ordering` mezőt) vagy azt csak hamis (`FALSE`) értékkel tartalmazhatja;
- kritikus jelzésű kiterjesztést (`extension`);
- a `QcStatements` kiterjesztésen kívül más kiterjesztést.

[9] OID: 0.4.0.19422.1.1

4.5 Időbélyegző válasz hitelessége

Szolgáltató a kiadott időbélyegzők hitelességét azáltal biztosítja, hogy a Szolgáltatás keretében kiadott időbélyegzők az időbélyegző egységek által az erre a célra kiadott tanúsítvány és a kapcsolódó magánkulcs felhasználásával hitelesítésre kerülnek, melynek formátuma megfelel az {Sz15} EN 319 422, {Sz16} RFC 3161, valamint az {Sz17} RFC 5816 szabványok vonatkozó előírásainak.

Az időbélyegző hitelesítésére használt elektronikus bélyegző algoritmusát lásd a 6.1.5 pontban.

4.5.1 Időbélyegző egységek tanúsítványa

Az időbélyegzők hitelesítésére használt magánkulcshoz tartozó nyilvános kulcs tanúsítvánnyal került hitelesítésre és azt Szolgáltató közzé teszi az internetes honlapján elérhető nyilvános tanúsítványtárban.

Az időbélyegzők hitelesítésére használt tanúsítványok jellemzői:

- a tanúsítvány kiadása egy olyan, a Szolgáltató által működtetett, minősített elektronikus bélyegzés célú tanúsítvány kibocsátására irányuló szolgáltatásban történt, amely a bizalmi szolgáltatási rendjében felvállalja az {Sz5} EN 319 412-2 szabvány követelményeinek teljesítését;
- a tanúsítványhoz kapcsolódó magánkulcs előállítása csak és kizárólag időbélyegző aláírása céljára történt (ezt a tanúsítvány kritikus `extendedKeyUsage` kiterjesztésében az `id-kp-timeStamping`[10] jelzi);

4.5.2 Időbélyegző egységek magánkulcsa és kriptográfiai modulja

Az időbélyegző egységek magánkulcsának algoritmusa és kulcshossza megfelel az {Sz18} ETSI TS 119 312 szabványban javasolt, és a Bizalmi Felügyelet algoritmus határozatában foglalt előírásoknak.

A magánkulcs használati időtartamának korlátozása - az adott algoritmushoz és kulcshosszhoz tartozó, az {Sz18} ETSI TS 119 312 szabványban javasolt időtartamokra - a 6.3.2 fejezetben leírtak szerint történik.

Szolgáltató az időbélyegző egységek tanúsítványhoz kapcsolódó magánkulcsát olyan HSM modulban tárolja és használja, ami megfelel a 6.2.1 fejezetben leírt előírásoknak.

Az időbélyegző egység magánkulcsa csak és kizárólag időbélyegzők hitelesítésére van használva.

Egy adott időbélyegző egységnek egy időben csak egy aktív magánkulcsa lehet.

Egy adott időbélyegző egység magánkulcsát nem szabad más HSM modulba importálni, vagy ha ez feltétlenül szükséges, akkor a magánkulcshoz ugyanaz a tanúsítvány kell, hogy tartozzon az összes HSM modulban.

Az időbélyegző egységek által használt HSM modulokat Szolgáltató megvédi a meghamisítás ellen szállítás és tárolás során.

A magánkulcsok telepítése, aktiválása és az egyéb kulcspár gondozási műveletek fizikailag biztonságos helyszínen, legalább két bizalmi munkakört betöltő személy együttes részvételével történnek.

[10] OID: 1.3.6.1.5.5.7.3.8

Az időbélyegző egység által használt HSM modulnak a használatból történő kivonásakor a rajta levő magánkulcsok a 6.2.10 fejezetben leírt módon megsemmisítésre kerülnek, így a további használatuk gyakorlatilag lehetetlenné válik.

4.6 Az időbélyegzőben szereplő időpont

Szolgáltató az általa működtetett időbélyegző egységek megfelelő beállításaival biztosítja, hogy az időbélyegzőben szereplő időpont pontossága 1 másodpercen belüli legyen.

4.6.1 Óraszinkronizálás

Szolgáltató az időbélyegző egységek belső óráját egy olyan pontos idővel szinkronizálja, amely visszavezethető legalább egy, UTC laboratórium által szolgáltatott, pontos időre.

A kalibrációt olyan módon végzi el, hogy az időbélyegző egység belső órájának eltérése a pontos UTC időtől ne haladhassa meg a vállalt pontosság mértékét.

4.6.2 Időbélyegző egység belső órájának védelme

Szolgáltató az időbélyegző egységeket megvédi minden olyan támadástól vagy behatástól, ami a belső óra kalibrációjának észrevétlen elvesztését eredményezhetné.

A Szolgáltató folyamatosan vizsgálja és észleli az időbélyegző egység belső órája pontos UTC idővel való szinkronizációja sikertelenségét vagy a kalibráció elvesztését.

Szolgáltató szünetelteti az időbélyegzők kiadását (a kérések visszautasításával) mindaddig, míg a belső óra eltérése az UTC időhöz képest a vállalt pontosságon kívül esik.

4.6.3 Szökőmásodpercek kezelése

Szökőmásodperc előfordulásakor a Szolgáltatónak elvégzi az óra szinkronizációt az illetékes szervezet értesítése alapján.

A szökőmásodperc miatti óraátállítást a szökőmásodperc előfordulására kitűzött napon, a nap utolsó percében kerül elvégzésre.

Szolgáltató a nyilvántartásában rögzíti a szökőmásodperc miatti óraátállítás megtörténtének időpontját, 1 másodperc pontossággal.

4.6.4 Nyári időszámítás kezelése

Az időbélyegző UTC időpontot tartalmaz, melyet egyes informatikai alkalmazások eltérő módon és formátumban jeleníthetnek meg a felhasználók számára.

Szolgáltató felhívja az Érintett Felek figyelmét arra, hogy az egyes alkalmazások az időbélyegzett dátumot és időpontot gyakran nem UTC időpontként, hanem a helyi időt használva jeleníthetik meg. Ez a különböző időzónákban levő Érintett Felek számára félreértésekre adhat okot, különösen a tavaszi és őszi óraátállítás környékén.

4.7 Időbélyegző válasz hitelességének ellenőrzése

A Szolgáltatás keretében kiadott időbélyegzők a Szolgáltató elektronikus bélyegzőjével kerülnek hitelesítésre, az időbélyegző egységek által.

Előfizetőnek kötelessége, az Érintett Felek számára erősen javasolt az időbélyegzőre az alábbi ellenőrzések elvégzése:

- az időbélyegző hitelességének ellenőrzése (az azon elhelyezett elektronikus bélyegző kriptográfiai ellenőrzése);
- az időbélyegzőt hitelesítő tanúsítványra az {Sz8} RFC 5280 6. fejezete szerinti tanúsítási útvonal felépítés és érvényesítés elvégzése;
- az időbélyegzőt hitelesítő tanúsítvány visszavonási állapotának ellenőrzése a 4.8 fejezetben ismertetett visszavonási állapot szolgáltatások használatával;
- az olyan felhasználási célok esetén, ahol jogszabályi vagy egyéb követelmény minősített időbélyegző használatát írja elő:
    - ellenőrizni, hogy az időbélyegző tartalmaz `QcStatements` kiterjesztést és abban a `tst-EuQcCompliance`[11] nyilatkozatot; és/vagy
    - ellenőrizni azt, hogy az időbélyegzőt kibocsátó szolgáltatás - a bélyegzett időpontra vonatkoztatva - szerepel-e EU minősített szolgáltatásként és megfelelő státusszal a {J1} eIDAS 22. cikke szerinti Bizalmi Listán.
- a bélyegzett dokumentum összetartozik-e a kapott időbélyegzővel (azaz az időbélyegző `messageImprint` mezőjében szereplő lenyomat és a dokumentumra kiszámított lenyomat egyező);
- az időbélyegben szereplő pontosság, a szabályzatokban vállalt felelősségvállalás az adott célra megfelelő-e;
- archiválás céljára történő felhasználás esetén ellenőrizni, hogy időbélyegzőben szereplő lenyomatok és aláírási algoritmusok megfelelően erősek-e a tervezett megőrzési időtartamra;
- figyelembe venni és betartani minden olyan korlátozást, ami az időbélyegzőben és az időbélyeget hitelesítő tanúsítvány által hivatkozott szabályzatokban szerepel.

4.8 Visszavonási állapot szolgáltatások

4.8.1 Működési jellemzők

Szolgáltató a végfelhasználói és szolgáltatói tanúsítványokhoz kapcsolódó visszavonási információkat mind CRL, mind OCSP formájában biztosítja.

Szolgáltató biztosítja, hogy a visszavonási állapot információ változása mind a CRL, mind az OCSP szolgáltatásban azonosan, konzisztens módon megjelenik, figyelembe véve az egyes szolgáltatásokban eltérő frissítési időket is.

CRL

A Szolgáltató által kibocsátott CRL megfelel az {Sz8} RFC 5280 szabványnak.

A CRL elérhetőségét a tanúsítvány `cRLDistributionPoint` kiterjesztése tartalmazza.

A CRL minden esetben tartalmazza a következő kibocsátás időpontját (`nextUpdate`). A záró CRL (az adott hitelesítő központ által kiadott utolsó CRL) esetén a `nextUpdate` mező tartalma a

[11] OID: 0.4.0.19422.1.1

„99991231235959Z” RFC 5280 {Sz8} szerinti speciális időpont. Szolgáltató biztosítja, hogy az új CRL kibocsátása a `nextUpdate` mezőben jelzett időpont előtt minden esetben megtörténik.

A CRL tartalmaz minden olyan visszavont tanúsítványt, amelynek érvényessége a CRL kibocsátásának időpontjában nem járt még le.

OCSP

A Szolgáltató által biztosított OCSP szolgáltatás megfelel az {Sz12} RFC 6960 szabványnak.

Az OCSP szolgáltatás elérhetőségét a tanúsítvány `authorityInformationAccess` kiterjesztésében, az `ocsp` / `accessLocation` mező tartalmazza.

Az OCSP szolgáltatást Szolgáltató az {Sz12} RFC 6960 2.2 fejezetében meghatározott "Authorized Responder" elvnek megfelelően működteti.

Az OCSP szolgáltatás keretében csak olyan tanúsítványra vonatkozóan kerül pozitív („good” státuszt tartalmazó) válasz kiadásra, amely tanúsítványt az adott hitelesítő központ bocsátott ki (azaz szerepel a tanúsítványtárban) és a tanúsítvány nincs felfüggesztett vagy visszavont állapotban.

Az OCSP válaszadó számára minimum 4 és maximum 21 óránként új, 24 órás érvényességű tanúsítvány kerül kiadásra, annak érdekében, hogy az OCSP választ aláíró tanúsítvány visszavonási állapotát ne kelljen ellenőrizni, ennek jelzésére az OCSP válaszadó tanúsítványában szerepel az `id-pkix-ocsp-nocheck` kiterjesztés.

Az OCSP szolgáltatás keretében a Szolgáltató biztosítja a visszavonási információt a tanúsítvány lejáratát követően is, 10 évig.

4.8.2 Szolgáltatás rendelkezésre állása

A CRL, illetve az OCSP szolgáltatás az év minden napján, napi 24 órában elérhető, 99,9%-os rendelkezésre állással, úgy, hogy a kiesés nem lépheti túl esetenként a 3 órás időtartamot.

4.8.3 Opcionális funkciók

Nincs kikötés.

5 FIZIKAI, ELJÁRÁSBELI ÉS SZEMÉLYZETI BIZTONSÁGI ÓVINTÉZKEDÉSEK

Szolgáltató a Szolgáltatás nyújtása során a kellő, az irányadó szabványoknak megfelelő fizikai, eljárásbeli és személyzeti biztonsági óvintézkedéseket és az ezeket érvényre juttató adminisztratív és irányítási eljárásokat alkalmazza.

Szolgáltató a rendszer kialakításakor kockázat elemzést végzett üzleti kockázatainak felmérésére, valamint a szükséges biztonsági követelmények és működési eljárások meghatározására; a kockázatok felülvizsgálatáról évente rendszeresen, valamint szükség esetén eseti jelleggel gondoskodik. Szolgáltató a szervezetén belüli biztonságkezeléshez szükséges informatikai biztonsági infrastruktúrát folyamatosan fenntartja. A biztonság szintjére hatást gyakorló bárminemű változtatást a Szolgáltató vezetősége hagy jóvá.

A biztonságkezelési szabályokat a Szolgáltató {D5} PKI szolgáltatások biztonságpolitikája tartalmazza. Ez a szabályzat biztonsági okokból nem nyilvános. A Szolgáltató informatikai rendszerei vonatkozásában a {D6} PKI szolgáltatások biztonsági szabályzata érvényesül. Ez a szabályzat szervezeti egység szinten és munkakörökre lebontva rögzíti a biztonságkezeléssel összefüggő feladatokat, felelősségeket és szabályokat, így többek között a bizalmi munkakörök felsorolását, a kinevezési feltételeket és az összeférhetetlenségi kritériumokat.

Szolgáltató megvalósította és folyamatosan fenntartja a Szolgáltatást nyújtó eszközök, rendszerek biztonsági ellenőrzéseit és üzemeltetési eljárásait. A Szolgáltató rendszeres belső ellenőrzései és külső auditjai ezen eljárásokat, a vonatkozó dokumentumokat és a Szolgáltatásra vonatkozó előírások teljesülését rendszeres időközönként vizsgálja.

A fenti eljárásokat a Szolgáltatóval munkaviszonyban álló, megbízható és szakértő üzemeltető személyzet biztosítja.

Szolgáltató gondoskodik arról, hogy eszközei és információi a megfelelő szintű védelemben részesüljenek. Szolgáltató valamennyi informatikai értékéről leltárt vezet, ezek védelmi követelményeit az elvégzett kockázatelemzéssel összhangban osztályokba sorolja és minősíti.

Szolgáltató a tanúsítványok, illetve időbélyegzők előállításában, a visszavonási információk menedzsmentjében közreműködő informatikai rendszereit, berendezéseit és eszközeit a legmagasabb védelmi szintet képező központi géptermében helyezi el.

5.1 Fizikai óvintézkedések

5.1.1 Telephely elhelyezése és szerkezeti felépítése

A Szolgáltató a Szolgáltatás nyújtásában közreműködő informatikai rendszereit fizikai és logikai védelemmel ellátott, legmagasabb védelmi szintet képező objektumában helyezte el és üzemelteti. A telephely elhelyezése és kialakítása során olyan egymásra épülő és egymást támogató védelmi megoldásokat alkalmaz, melyek képesek megakadályozni az illetéktelen hozzáférést és alkalmasak az informatikai rendszerek és Szolgáltató által tárolt bizalmas adatok megóvására.

5.1.2 Fizikai hozzáférés

A Szolgáltató megvédi a Szolgáltatás nyújtásában közreműködő eszközeit és berendezéseit a jogosulatlan fizikai hozzáféréstől az eszközök manipulálásának megakadályozása érdekében.

Ehhez biztosítja az alábbiakat:

- a gépterembe történő minden belépés naplózásra kerül;

- a gépterembe csak a bizalmi szerepkört betöltő, erre feljogosított munkatárs léphet be, azonosítást követően;
- önálló jogosultsággal nem rendelkező személy csak indokolt és engedélyezett esetben, a szükséges időtartamig tartózkodhat a gépteremben megfelelő jogosultságú kísérő személy állandó felügyelete mellett;
- az eszközök aktivizáló adatai (jelszavak, PIN kódok, stb.) a géptermen belül sem tárolhatók nyílt formában;
- jogosulatlan személy jelenlétében:
    - a bizalmas adatokat tartalmazó adathordozókat fizikailag elzárva tartják;
    - a bejelentkezett terminálok nem maradnak felügyelet nélkül;
    - nem végeznek olyan munkafolyamatot, amely során bizalmas adat felfedésre kerülhet;
- a gépterem elhagyásakor ellenőrzésre kerül:
    - minden eszköz és berendezés megfelelően biztonságos üzemállapotban van;
    - minden terminálon megtörtént a kijelentkezés;
    - a fizikai tároló eszközök megfelelően elzárásra kerültek;
    - a fizikai védelmet biztosító rendszerek és berendezések megfelelően működnek.

5.1.3 Áramellátás és légkondicionálás

A Szolgáltató a gépteremben olyan szünetmentes áramellátó rendszert alkalmaz, amely:

- megfelelő teljesítménnyel rendelkezik a gépterem informatikai és kisegítő létesítményi berendezései áramellátásának biztosítására;
- megvédi az informatikai berendezéseket a külső hálózat feszültség ingadozásai, feszültség kimaradásai és egyéb zavarok ellen;
- tartós áramszünet esetére saját áramellátó berendezés biztosítja - üzemanyag utántöltéssel - tetszőlegesen hosszú időtartamig az áramellátást.

Szolgáltató a gépteremben olyan légkondicionáló berendezést alkalmaz, mely biztosítja az alábbiakat:

- az operátorok biztonságos munkavégzéséhez szükséges mennyiségű oxigén biztosított;
- a levegő nedvességtartalma nem haladja meg az informatikai rendszerek által megkívánt szintet;
- hűtés történik a szükséges üzemi hőmérséklet biztosítására, az eszközök és berendezések túlhevülésének megakadályozására.

5.1.4 Beázás és elárasztás veszélyeztetettség

Szolgáltató megvédi a géptermet a beázástól, víz betöréstől és elárasztástól nedvességérzékelő és riasztó rendszer alkalmazásával.

5.1.5 Tűzmegelőzés és tűzvédelem

Szolgáltató a géptermet füst- és tűzérzékelőkkel szerelte fel, melyek automatikusan riasztják az illetékes személyzetet. Minden helyiségben jól látható helyen van elhelyezve a vonatkozó előírásoknak megfelelő típusú és mennyiségű kézi tűzoltó készülék. A gépteremben automatikus tűzoltó rendszer került kialakításra, amely emberi egészségre nem veszélyes és nem károsítja az informatikai eszközöket.

5.1.6 Adathordozók tárolása

Szolgáltató megvédi valamennyi adathordozóját a jogosulatlan hozzáféréstől, a megsemmisüléstől vagy véletlen rongálódástól, jellemzően páncélszekrénybe történő elzárással.

5.1.7 Selejt kezelése és megsemmisítése

Szolgáltató a környezetvédelmi előírások betartásával gondoskodik feleslegessé vált eszközeinek, adathordozóinak megsemmisítéséről. A felesleges eszközök és adathordozók az erre kijelölt munkatárs személyes felügyelete mellett, széleskörűen elfogadott módszerekkel kerülnek használhatatlanná tételre vagy visszaállíthatatlan módon törlésre.

5.1.8 Fizikailag elkülönítetten őrzött mentési példányok

Szolgáltató azt az adatmentést, amiből meghibásodás esetén a teljes szolgáltatás helyreállítható, olyan – az üzemeltetés helyétől eltérő - helyszínen tárolja, mely megfelelő fizikai és működési védelemmel rendelkezik. Biztosítja helyszínek között a mentett adatok biztonságos továbbítását.

Az adatmentést, vagy abból a helyreállítást rendszerüzemeltető bizalmi munkakört betöltő személy végzi el.

5.2 Eljárásbeli előírások

A Szolgáltató gondoskodik arról, hogy informatikai rendszereit biztonságosan, szabályszerűen, a meghibásodás minimális kockázata mellett üzemeltessék. Szolgáltató személyzete a feladatokat olyan eljárásbeli előírások alapján végzi, melyek szinkronban vannak a jogszabályi, szabványi és belső biztonsági előírásokkal.

Az eljárásbeli szabályokat a következő szabályzatok tartalmazzák:

- {D3} a Szolgáltató Szervezeti és Működési szabályzata, mely meghatározza a Szolgáltató szervezeti felépítését, azon belül az egyes szervezetekhez kapcsolt feladat-, felelősség- és hatásköröket;
- jelen szolgáltatási szabályzat, mely a Szolgáltató és a PKI közösség (Előfizetők, Érintett Felek, stb.) viszonyát szabályozza;
- {D6} PKI szolgáltatások biztonsági szabályzata, mely részletesen előírja az adatokhoz és informatikai rendszerekhez, valamint a személyi és fizikai környezethez kapcsolódó biztonsági szabályokat.

5.2.1 Bizalmi munkakörök

Szolgáltató az alábbi bizalmi munkaköröket azonosította, melyektől a Szolgáltatás biztonsága függ:

a) a Szolgáltató informatikai rendszeréért általánosan felelős vezető;

b) biztonsági tisztviselő: a szolgáltatás biztonságáért általánosan felelős személy;

c) rendszeradminisztrátor: az informatikai rendszer telepítését, konfigurálását, karbantartását végző személy;

d) rendszerüzemeltető: az informatikai rendszer folyamatos üzemeltetését, mentését és helyreállítását végző személy;

e) független rendszervizsgáló: a szolgáltató naplózott, illetve archivált adatállományát vizsgáló, a Szolgáltató által a szabályszerű működés érdekében megvalósított kontroll intézkedések

betartásának ellenőrzéséért, a meglévő eljárások folyamatos vizsgálatáért és monitorozásáért felelős személy;

f) regisztrációs felelős: a végtanúsítványok előállításának, kibocsátásának, az életciklus menedzsment tevékenységek és adminisztráció szabályszerű végzéséért felelős személy;

g) visszavonás felelős: a végtanúsítványok visszavonásának és felfüggesztésének jóváhagyásáért felelős személy.*

* A vonatkozó jogszabály ({J8} 24/2016. rendelet) a visszavonás felelős feladatkörét a regisztrációs felelős tevékenységi körébe tartozóan rögzíti.

A bizalmi munkakörökhöz tartozó feladatkörök és felelősségek leírását a Szolgáltató belső, nem nyilvános szabályzata tartalmazza. A bizalmi munkakört betöltő személy munkaviszonyban áll a Szolgáltatóval. Bizalmi munkakörbe Szolgáltató felső vezetősége nevezi ki a munkatársakat. Minden bizalmi munkakört legalább két személy tölt be.

A bizalmi munkakörökön kívül Szolgáltató bizalmi szerepköröket is alkalmaz a Szolgáltatás nyújtásához szükséges feladatok hatékony ellátása céljából. A bizalmi szerepkört betöltő személyek munkaviszonyban állnak a Szolgáltatóval.

A bizalmi munkaköröket és szerepköröket betöltő személyekről Szolgáltató nyilvántartást vezet. A bizalmi munkaköröket tartalmazó nyilvántartásban bekövetkező minden változást a változtatás bevezetése előtt a Bizalmi Felügyeletnek bejelenti.

5.2.2 Az egyes feladatokhoz szükséges személyzeti létszámok

Szolgáltató {D6} biztonsági szabályzata előírja, hogy csak védett környezetben, legalább kettő, bizalmi munkakört betöltő munkatárs egyidejű jelenléte mellett, illetéktelen személy jelenlétét kizárva végezhetők el az alábbi műveletek:

- szolgáltatói kulcspár létrehozása;
- szolgáltatói magánkulcs mentése és visszaállítása;
- szolgáltató magánkulcs aktiválása;
- szolgáltatói magánkulcs megsemmisítése.

5.2.3 Bizalmi munkakörökben elvárt azonosítás és hitelesítés

A bizalmi munkaköröket betöltő személyek azonosítása és hitelesítése multi-faktoros autentikációs mechanizmusokkal történik meg, mielőtt a Szolgáltatás nyújtásában érintett kritikus informatikai rendszerekhez hozzáférhetnének.

5.2.4 Egymást kizáró munkakörök

Szolgáltató biztosítja, hogy a bizalmi munkakörök vonatkozásában:

a) biztonsági tisztviselő nem láthatja el a független rendszervizsgáló, a rendszeradminisztrátor, és az informatikai rendszerért általánosan felelős vezető feladatait;
b) a független rendszervizsgáló nem láthatja el az informatikai rendszerért általánosan felelős vezető, a regisztrációs felelős, és a rendszeradminisztrátor feladatait;
c) törekedni kell a bizalmi munkakörök teljes személyi szétválasztására.

5.3 Személyzetre vonatkozó előírások

Szolgáltató gondoskodik arról, hogy a személyzeti előírásai, a munkatársak alkalmazására vonatkozó gyakorlatai fokozzák és támogassák a Szolgáltató működésének megbízhatóságát.

Szolgáltató kellő számú, a Szolgáltatás nyújtásához szükséges feladatok jellegének, terjedelmének és mennyiségének megfelelő végzettséggel, képzettséggel, szakmai tudással és tapasztalattal rendelkező személyzetet alkalmaz.

Szolgáltató valamennyi bizalmi munkakört betöltő munkatársa mentes minden olyan ütköző érdektől, ami hátrányosan érinthetné a Szolgáltatás megbízhatóságát és biztonságát.

A munkatársak a feladatok szétválasztása és a legkisebb meghatalmazás szempontjai alapján meghatározott munkaköri leírásokkal rendelkeznek.

5.3.1 Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

Szolgáltató biztosítja, hogy bizalmi munkakört csak olyan személyek töltsenek be, akiknek a bizalmi munkakör betöltéséhez szükséges befolyásmentességét és szakértelmét erkölcsi bizonyítvánnyal, szakmai gyakorlattal, végzettséggel és szakképesítéssel igazolni tudja.

A Szolgáltató informatikai rendszeréért általánosan felelős vezető kinevezéséhez szakirányú felsőfokú végzettséggel és legalább három év, az informatikai biztonsággal összefüggésben szerzett szakmai gyakorlattal rendelkezik. Szakirányú felsőfokú végzettség a matematikusi, fizikusi egyetemi végzettség vagy a műszaki tudományterületre tartozó mérnöki szakon szerzett főiskolai vagy egyetemi végzettség.

A biztonsági tisztviselők és rendszervizsgálók esetén szakirányú közép- vagy felsőfokú végzettség, középfokú végzettség esetén legalább három, felsőfokú végzettség esetén legalább egy év informatikai biztonsággal összefüggésben szerzett szakmai gyakorlat szükséges.

A regisztrációs felelős esetén középfokú szakirányú végzettség és legalább egy év informatikai biztonsággal összefüggésben szerzett szakmai gyakorlat szükséges.

A rendszerüzemeltető és rendszeradminisztrátor esetén középfokú szakirányú végzettség és legalább egy év, hasonló munkakörben szerzett szakmai gyakorlat szükséges.

Az egyes bizalmi munkakörök betöltéséhez elvárt szakirányú végzettségek meghatározását a Szolgáltató belső, nem nyilvános szabályzata tartalmazza.

5.3.2 Biztonsági háttér ellenőrzés eljárásai

A Szolgáltató vezetői munkakörben, illetve bizalmi munkakörben vagy szerepkörben csak olyan alkalmazottakat foglalkoztat, akik:

- büntetlen előélettel rendelkeznek és nincs ellenük folyamatban olyan eljárás, ami a büntetlenséget befolyásolhatja (a büntetlen előéletet három hónapnál nem régebbi erkölcsi bizonyítvánnyal kell igazolni);
- nem állnak a bizalmi szolgáltatási tevékenység gyakorlását kizáró foglalkoztatástól eltiltás hatálya alatt;
- a felvételi eljárásban benyújtott önéletrajzban megadott információk valódiságát Szolgáltató igazolni tudta.

Az 5.2.1 fejezetben meghatározott bizalmi munkakör betöltését a legmagasabb szintű biztonsági ellenőrzés (a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvényben meghatározott nemzetbiztonsági ellenőrzés) előzi meg. A többi, a Szolgáltatás nyújtásával kapcsolatos munkakörben, a munkakör betöltését fokozott szintű, a Szolgáltató által végzett biztonsági ellenőrzés előzi meg. Mind a legmagasabb, mind a fokozott biztonsági ellenőrzés lefolytatásához szükséges az érintett személy hozzájárulása. Nem tölthet be bizalmi munkakört az a személy, akinél a biztonsági ellenőrzés kockázatot tár fel.

A bizalmi munkakörhöz történő hozzárendeléskor az érintett személy:

- pontos és írásos munkakör leírást vesz át a fölérendelt vezetőtől vagy a Szolgáltató humán szervezetétől;
- titoktartási nyilatkozatot kell aláírnia, melyben három év titoktartási kötelezettség szerepel a kilépés időpontjától számítva;
- szükséges mértékű oktatásban részesül, annak érdekében, hogy a feladat-, felelősség és hatáskörét pontosan megismerje és gyakorolni tudja.

Kilépéskor:

- A kilépésről szóló döntés meghozatalakor a kilépő fizikai és logikai belépési és hozzáférési jogosultságai azonnal megszüntetésre kerülnek. Ezt követően, a kilépő személy csak biztonsági tisztviselő kíséretében léphet be a Szolgáltatással kapcsolatos körletekbe.
- Azonnal vissza kell venni az azonosításhoz és hitelesítéshez használt eszközét, és dokumentáltan meg kell semmisíteni azt. A kapcsolódó tanúsítványokat vissza kell vonni.

5.3.3 Képzési követelmények

A bizalmi munkakörökben Szolgáltató olyan személyeket foglalkoztat, akik az adott munkakör vagy szerepkör ellátásához szükséges mértékben elsajátították:

- a PKI elméletet;
- a kiberbiztonsággal és a személyes adatokkal kapcsolatos szabályokat;
- Szolgáltató informatikai rendszerének sajátosságait és kezelésének módját;
- a szerepkör ellátáshoz szükséges speciális ismereteket;
- Szolgáltató nyilvános és belső szabályzataiban meghatározott folyamatokat és eljárásokat;
- az egyes tevékenységek jogi következményeit;
- az alkalmazandó biztonsági szabályokat.

A Szolgáltató éles informatikai rendszereihez csak a képzést sikeresen záró alkalmazottak kaphatnak hozzáférési jogosultságot.

5.3.4 Továbbképzési gyakoriságok és követelmények

Szolgáltató gondoskodik arról, hogy a munkatársak folyamatosan a megfelelő tudással rendelkezzenek, szükség esetén továbbképzést vagy ismétlő jellegű képzést tart.

Szolgáltató minden lényeges változás esetén megismétli az érintett személyek részére a képzést vagy annak elemeit.

Jelentős változás, azaz a szervezeti biztonságpolitika módosulása, a szoftver vagy hardver változása (upgrade), valamint a kulcs kezelés és biztonság kezelési óvintézkedések változása esetén, valamennyi munkatárs, az őt érintő mélységben továbbképzésben részesül, illetve megkapja a szükséges dokumentációkat.

Kisebb változások esetén a munkatársak a változás bekövetkezte előtt írásos tájékoztatást kapnak.

Szolgáltató legalább évente egyszer továbbképzést biztosít az újonnan ismertté vált sebezhetőségekről, az IT biztonság aktuális gyakorlatáról, a munkatársak saját szakterületét érintően.

5.3.5 Munkabeosztás körforgásának gyakorisága és sorrendje

Nincs kikötés.

5.3.6 Felhatalmazás nélküli tevékenységek büntető következményei

Szolgáltató a dolgozóval kötött munkaszerződésben szabályozza a dolgozó felelősségre vonásának lehetőségét a dolgozó által elkövetett mulasztások, vétlen vagy szándékos károkozás esetére.

5.3.7 Szerződéses munkavállalókra vonatkozó követelmények

Szolgáltató bizalmi munkakörben csak munkaviszonyban álló személyt foglalkoztat.

Az egyéb feladatok ellátására, vállalkozási vagy megbízásos szerződés keretében a beszállítóval Szolgáltató írásos megállapodást köt. A szerződő fél titoktartási nyilatkozatot ír alá, melyben vállalja, hogy a szerződés teljesítésében közreműködő személyek a munkavégzés során birtokukba kerülő üzleti titkokat és bizalmas információkat illetéktelen személynek fel nem fedik, más módon sem hasznosítják, és amely tartalmazza a megszegése esetén alkalmazott szankciókat.

5.3.8 A személyzet számára biztosított dokumentációk

Szolgáltató folyamatosan biztosítja a személyzet részére a munkakörük ellátásához szükséges dokumentációk és szabályzatok rendelkezésre állását.

Minden bizalmi munkakört betöltő munkatárs megkapja írásban:

- egyéni munkaköri leírást;
- a Szolgáltató szervezeti és biztonsági szabályzatait;
- rendszeres és rendkívüli továbbképzések alkalmával az adott oktatási formához tartozó oktatási segédanyagokat.

5.4 A biztonsági naplózás folyamatai

5.4.1 Naplózott esemény típusok

Szolgáltató naplóz minden, az informatikai rendszerével és Szolgáltatás nyújtásával kapcsolatos eseményt. A naplózott adatállomány átfogja a Szolgáltatás nyújtásának teljes folyamatát, és lehetővé teszi, hogy a valós helyzetek megítéléséhez a szükséges mértékben minden, a Szolgáltatással kapcsolatos eseményt rekonstruálni lehessen.

Az informatikai rendszerrel kapcsolatos események különösen a rendszer indítás és leállítás, biztonsági profil változása, rendszer összeomlás és hardver hibák, tűzfal aktivitás, hozzáférési kísérletek, szolgáltatói kulcs kezelés eseményei, óraszinkronizációs események, naplózási funkció elindítása és leállítása, naplózási paraméterek megváltoztatása, naplóadatok tárolásával kapcsolatos hibák, napló adatok integritásának sérülése eseményei.

A Szolgáltatás nyújtásával kapcsolatos események különösen az alábbiak:

- időbélyegző egységek kulcspárjaival kapcsolatos minden esemény;
- időbélyegző egységek és egyéb szolgáltatói tanúsítványok életciklusával kapcsolatos minden esemény;
- időbélyegző kérésekkel és azok kiszolgálásával kapcsolatos minden esemény a teljes folyamatra vonatkozóan;
- időbélyegző egységek működtetésével kapcsolatos minden esemény, beleértve a belső óra szinkronizációs és kalibrációs eseményei, szinkronizáció elvesztése, pontossági tartománytól való eltérést is.

A naplózott adatállomány tartalmazza a naplózott esemény bekövetkeztének dátumát és pontos időpontját, az esemény követhetőségéhez, rekonstruálásához szükséges adatokat, az esemény kiváltásában közreműködő felhasználó vagy más személy nevét vagy azonosítóját.

5.4.2 Naplóállomány feldolgozásának gyakorisága

Szolgáltató biztosítja a naplóállományok rendszeres ellenőrzését és kiértékelését.

A Szolgáltatás nyújtásával kapcsolatos események naplóállományait naponta feldolgozzák a rendszervizsgálók.

Az informatikai rendszer eseményeinek naplóállományait a rendszervizsgálók rendszeres időközönként, a biztonsági szabályzatban meghatározott sűrűséggel végzik el.

5.4.3 Naplóállomány megőrzési időtartama

Szolgáltató a naplóállományokat archiválja és gondoskodik azok biztonságos megőrzéséről az 5.5.2 fejezetben előírt időtartamig. Ezen időtartamig Szolgáltató biztosítja az archivált állományok olvashatóságát, megőrzi az ehhez szükséges hardver és szoftver eszközöket.

5.4.4 Naplóállomány védelme

Szolgáltató a naplóállományokat és azok mentéseit biztonságos, fizikailag is védett környezetben tárolja. A naplóállományokat időbélyegzővel, a naplóállományok archív mentéseit időbélyegzőt is tartalmazó elektronikus aláírással vagy bélyegzővel látja el.

Szolgáltató gondoskodik arról, hogy a naplóállományokhoz és azok mentéseihez csak az arra feljogosított személyek férhessenek hozzá.

5.4.5 Naplóállomány mentési folyamatai

A naplóállományokról Szolgáltató rendszeres mentést készít. A mentéssel kapcsolatos eljárásokat és szabályokat a Szolgáltató belső szabályzata tartalmazza.

5.4.6 Naplózás gyűjtési rendszere

A naplóbejegyzések gyűjtését belső komponens oldja meg. A naplóbejegyzések gyűjtése megkezdődik rendszer indításkor és rendszer leállításig folyamatosan működik, és közben biztosítja a gyűjtött bejegyzések integritását és rendelkezésre állását, szükség esetén a bizalmasságát is.

A naplóbejegyzések gyűjtési rendszerének működési rendellenessége esetén Szolgáltató felfüggeszti az érintett területek működését az üzemzavar elhárításáig.

5.4.7 Rendellenes eseményeket kiváltó alanyok értesítése

A rendellenes eseményeket kiváltó alanyokat (személyeket, szervezeteket) Szolgáltató nem feltétlenül értesíti minden esetben. Szolgáltató szükség esetén bevonhatja az eseményt kiváltó alanyt az esemény kivizsgálásába. Ilyen esetben az érintett Előfizető kötelessége a Szolgáltatóval való együttműködés az esemény feltárása érdekében.

5.4.8 Sebezhetőség értékelések

Szolgáltató a vonatkozó szabványok által meghatározott rendszeres időközönként, a naplóállományok és egyéb információk kiértékelésén alapuló sebezhetőség vizsgálatot és behatolás tesztet végez, mely segítségével feltérképezi a potenciális belső és külső fenyegetéseket, melyek jogosulatlan hozzáférést eredményezhetnek vagy hatással lehetnek a tanúsítvány kibocsátási folyamatra, a tanúsítványban tárolandó adatok megmásítását, módosítását, sérülését vagy megsemmisülését eredményezhetik.

A sebezhetőség vizsgálathoz kapcsolódóan Szolgáltató kockázatelemzésben értékeli az egyes fenyegetések bekövetkeztének valószínűségét és a bekövetkezés esetén várható kárt. Értékeli az alkalmazott folyamatokat, informatikai rendszereket, védelmi intézkedéseket, hogy azok megfelelően képesek-e ellenállni a fenyegetésnek.

A kiértékelést követően Szolgáltató megteszi a megfelelő intézkedéseket annak érdekében, hogy a feltárt sebezhetőség kihasználhatósága ne következzen be.

Szolgáltató folyamatosan figyelemmel kíséri az újonnan ismertté vált, kritikus sebezhetőségeket, és a szükséges ellenintézkedéseket lehetőség szerint 48 órán belül megteszi. Bármely olyan sebezhetőség esetén, melynek kihatása lehet a Szolgáltatás nyújtására, Szolgáltató vagy cselekvési tervet készít és hajt végre annak érdekében, hogy a sebezhetőség ne legyen kihasználható, illetve annak hatása elhanyagolható legyen, vagy dokumentálja annak ténybeli alapját, hogy az adott sebezhetőség nem igényel intézkedést.

5.5 Adatok archiválása

5.5.1 A tárolt adatok típusai

Szolgáltató gondoskodik arról, hogy megőrzésre kerüljön minden olyan információ, amely szükséges ahhoz, hogy egy elektronikus aláírás vagy bélyegző érvényessége bizonyítható legyen, továbbá amely a Szolgáltató és a rendszereinek megfelelő működését alátámasztja.

Ehhez legalább az alábbi információkat tárolja papír alapon vagy elektronikusan:

- a Szolgáltatás igénylésével kapcsolatos minden adat vagy irat, különösen a Szolgáltatási Szerződés, Előfizető által aláírt nyilatkozatok és átvételi elismervények;
- az időbélyegző kérésekkel és azok kiszolgálásával kapcsolatos valamennyi információ a teljes folyamatra vonatkozóan;
- időbélyegző egységek órájának szinkronizációs eseményei, beleértve a normál kalibrációt és pontos idő szinkronizáció elvesztését, vagy a pontossági tartománytól való eltérést is;
- időbélyegző egységek kulcspárjainak életciklusával kapcsolatos események (generálás, használat, használaton kívül helyezés, megsemmisítés);
- időbélyegző egységek által használt tanúsítványok teljes életciklusával kapcsolatos események;
- a bizalmi szolgáltatási rend és szolgáltatási szabályzat valamennyi kibocsátott verziója;
- az Általános Szerződési Feltételek valamennyi kibocsátott verziója;
- a Szolgáltató működésével kapcsolatos szerződések
- valamennyi naplóállomány.

5.5.2 Archívum megőrzési időtartama

Szolgáltató az 5.5.1 fejezetben meghatározott archivált adatokat, az időbélyegző kiadásától számított 10 évig, illetve az időbélyegzővel kapcsolatos jogvita jogerős lezárásáig, szabályzatok, szerződések esetében a hatályon kívül helyezés vagy megszűnés utáni 10 évig őrzi meg.

5.5.3 Archívum védelme

Szolgáltató olyan fizikai védelmet biztosít és biztonsági óvintézkedéseket alkalmaz, melyek fenntartják az archivált adatok sértetlenségét, hitelességét, rendelkezésre állását és a bizalmasságát. Az elektronikus formában archivált adatokat Szolgáltató legalább fokozott biztonságú elektronikus aláírással vagy bélyegzővel, valamint minősített időbélyegzővel látja el.

5.5.4 Archívum mentési eljárásai

Szolgáltató a papír alapú iratokat, dokumentumokat a dokumentumtárban, az elektronikus állományokat pedig több példányban, fizikailag elkülönített helyszíneken őrzi meg, illetve tárolja.

Szolgáltató biztosítja az elektronikus formában archivált állományok adathordozóinak elavulás elleni védelmét a megőrzési időn belül.

5.5.5 Az adatok időbélyegzésére vonatkozó követelmények

Valamennyi naplóbejegyzésben olyan időjel szerepel, amely a 6.8 fejezetben ismertetett időforrásokkal szinkronizált rendszeridőt tartalmazza, melynek pontossága egy másodpercen belüli.

Az elektronikus formában archivált adatokon elhelyezett elektronikus aláírás vagy bélyegző minősített időbélyegzőt tartalmaz.

Szolgáltató az archivált adatok megőrzése során szükség esetén (pl. algoritmus váltás) gondoskodik az elektronikus aláírások vagy bélyegzők, valamint az időbélyegzők hitelességnek fenntartásáról.

5.5.6 Archívum gyűjtési rendszere

A naplóállományok és az egyéb elektronikusan keletkezett adatokat a Szolgáltató védett informatikai rendszerén belül gyűjti. A védett informatikai rendszerből történő kimozgatás során az adatok minősített időbélyegzőt tartalmazó elektronikus aláírással vagy bélyegzővel kerülnek hitelesítésre.

A papíralapú iratokat Szolgáltató elhelyezi a saját dokumentumtárában tárolás és megőrzés céljából.

5.5.7 Archívum hozzáférés és ellenőrzés eljárásai

Szolgáltató az archivált adatokat megvédi a jogosulatlan hozzáféréstől. Szolgáltató a jogosultságot ellenőrzi, és a hozzáféréseket naplózza.

Szolgáltató az Ügyfélkapcsolati Iroda közreműködésével biztosítja az Előfizetők, illetve a kapcsolattartók számára a róluk tárolt személyes adatokra vonatkozó tájékoztatást.

Szolgáltató a 9.4.6 fejezetben ismertetett hatósági vagy jogi eljárásokban a szükséges mértékben a biztosítja a hozzáférést az archívumban tárolt adatokhoz.

5.6 Kulcs átállás

Szolgáltató biztosítja, hogy az időbélyegző egységek folyamatosan rendelkezzenek a működésükhöz szükséges, megfelelően erős algoritmusú és kulcshosszú, érvényes kulccsal és tanúsítvánnyal.

Szolgáltató gondoskodik arról, hogy minden időbélyegző egység kulcspárja és tanúsítványa a magánkulcs használati időtartamának (6.3.2 fejezet) lejárta előtt cserére kerüljön.

5.7 Helyreállítás rendkívüli üzemi helyzetek esetén

Szolgáltató minden szükséges intézkedést meghoz annak érdekében, hogy rendkívüli üzemeltetési helyzet, katasztrófa esetén a szolgáltatás kiesésből származó károkat minimalizálja és a Szolgáltatást a lehető legrövidebb időn belül helyreállítsa. Az eseti szolgáltatáskiesés időtartama nem haladhatja meg a három órát.

A Szolgáltatás 3 órát meghaladó kiesése esetén Szolgáltató haladéktalanul értesíti a Bizalmi Felügyeletet.

Egyéb incidens esetén - amennyiben az jelentős hatást gyakorol a szolgáltatásra vagy az annak keretében tárolt személyes adatokra -, Szolgáltató az esetről való értesüléstől számított 24 órán belül értesíti az Érintett Feleket, valamint jelenti az incidenst a Bizalmi Felügyeletnek.

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

5.7.1 Rendkívüli események és kompromittálódás kezelésének eljárásai

Szolgáltató rendelkezik {D7} üzletmenet folytonossági tervvel. Ez a dokumentum biztonsági okokból kifolyólag nem nyilvános.

A rendkívüli üzemeltetési helyzetben a Szolgáltató dokumentálja az eseményeket, azok körülményeit, az elhárításukra megtett intézkedéseket.

Rendkívüli üzemeltetési helyzetben Szolgáltató életbe lépteti az üzletmenet folytonossági tervében megtervezett eljárásait annak érdekében, hogy az üzemeltetés helyreálljon az üzletmenet folytonossági tervben megjelölt időn belül.

A helyreállítás időtartamát az esemény súlyossága, azaz az üzletmenet folytonossági terv szerint értelmezett osztályba sorolása határozza meg.

Szolgáltató kialakította és fenntartja azt a tartalék rendszert, mely a rendkívüli üzemeltetési helyzetben képes a Szolgáltatást, valamint a nyilvános szabályzatok és szolgáltatói tanúsítványok elérhetőségét, illetve a CRL-ek közzétételét biztosítani.

A rendkívüli üzemeltetési helyzet határidőn túli fennállása esetén Szolgáltató haladéktalanul értesíti a Bizalmi Felügyeletet, az esemény bekövetkeztéről, annak hatásáról, várható időtartamáról, az elhárítás érdekében tett és tervezett intézkedésekről, továbbá a rendkívüli üzemeltetési helyzet megszűnéséről.

A rendkívüli üzemeltetési helyzetben Szolgáltató a lehető legrövidebb időn belül tájékoztatást tesz közzé internetes honlapján, valamint, lehetőség szerint, elektronikus levélben értesíti azokat az Előfizetőket, akiket az esemény érint.

A biztonságot érintő vagy a sértetlenség megszűnését eredményező incidens esetén – amennyiben annak hátrányos kihatása van a Szolgáltatást igénybe vevő Előfizetőkre – Szolgáltató indokolatlan késedelem nélkül értesíti az érintett Előfizetőket.

5.7.2 Sérült számítási erőforrások, szoftverek és/vagy adatok

Szolgáltató olyan megbízható rendszert működtet, mely redundáns műszaki megoldásokkal, biztonsági mentésekkel és eljárásokkal a rendszerben bekövetkezett hiba esetén is biztosítja a Szolgáltatás működtetését és elérhetőségét. A pontos és részletes előírásokat és intézkedéseket az üzletmenet folytonossági terv, illetve a Szolgáltató belső szabályzatai tartalmazzák.

5.7.3 Időbélyegző egység magánkulcsának kompromittálódása esetén követendő eljárás

A Szolgáltató magánkulcsának kompromittálódása esetére akciótervvel rendelkezik, melyet az üzletmenet folytonossági tervében tervezett meg. E szerint megteszi az alábbi főbb lépéseket:

- megszünteti az érintett időbélyegző egység és így az érintett magánkulcs használatát;
- visszavonja az érintett magánkulcshoz tartozó tanúsítványt;
- új időbélyegző kulcspárt és tanúsítványt hoz létre;
- értesíti a Bizalmi Felügyeletet;
- intézkedik valamennyi érintett fél értesítéséről;
- közzéteszi azt az információt, ami alapján egyértelműen meg lehet határozni az érintett időbélyegzők körét.

5.7.4 Üzletmenet folytonosság helyreállás katasztrófát követően

Szolgáltató rendelkezik tartalék helyszínnel és informatikai rendszerrel, továbbá megtervezett eljárásokkal az áttelepülésre.

A súlyos üzemzavar és a katasztrófa eseteit - többek között - az különbözteti meg egymástól, hogy katasztrófa esetén nagy valószínűséggel nem csak az informatikai rendszer, hanem annak fizikai környezete is megsemmisül részben vagy egészben. Ez utóbbi esetben egy válságstáb az üzletmenet folytonossági tervben meghatározott módon intézkedik a tartalék helyszínre való áttelepülésről és ott az informatikai rendszer szükséges mértékű visszaállításáról a tartalék helyszínen korábban elhelyezett mentések segítségével.

5.8 A szolgáltatási tevékenység megszüntetése

Szolgáltató rendelkezik olyan bankgaranciával, mely fedezi a szolgáltatási tevékenység megszüntetésének költségeit abban az esetben, ha Szolgáltató csődeljárás alá kerül vagy más okból kifolyólag nem képes önmaga fedezni a költségeket. Ha Szolgáltató ellen felszámolási, végelszámolási vagy egyéb kényszertörlési eljárás indult, erről és a felszámolóról vagy végelszámolóról Szolgáltató haladéktalanul tájékoztatja a Bizalmi Felügyeletet.

Szolgáltató az alábbi, a szolgáltatási tevékenység megszüntetésére vonatkozó tervvel rendelkezik:

- A tervezett megszűnés előtt kellő időben tárgyalásokat kezdeményez más minősített bizalmi szolgáltatókkal a Szolgáltatással járó kötelezettségek - különösen az 5.5.1 fejezetben meghatározott adatoknak a megőrzése az 5.5.2 fejezetben megjelölt időtartamig - átadás-átvételéről.
- Szolgáltató gondoskodik a Szolgáltatás megszüntetéséből fakadó, a felhasználói közösséget érintő zavarok minimalizálásáról. Különösképpen gondoskodik az időbélyegző egységek tanúsítványaival és egyéb szolgáltató tanúsítványokkal kapcsolatban a visszavonási kezelés és közzététel szolgáltatások folyamatos fenntartásáról.
- A megszüntetés előtt legalább 60 nappal korábban:
    - értesíti a Bizalmi Felügyeletet, és internetes honlapján tájékoztatja az felhasználói közösség tagjait;
    - megszünteti a nevében eljáró szerződött alvállalkozói összes felhatalmazását, felbontja a velük kötött szerződéseket, és jogosultságaikat megvonja;
    - beszünteti az időbélyegzők előállítását és kibocsátását;
    - egy megbízható féllel (bizalmi szolgáltatóval) megállapodást köt a Szolgáltatással járó kötelezettségeknek átadás-átvételéről, és ennek másolatát megküldi a Bizalmi Felügyeletnek;
- A megszüntetés előtt legalább 20 nappal korábban:

- visszavonja az összes időbélyegző egység tanúsítványait;
- az időbélyeg egységek magánkulcsait és azok mentéseit olyan módon semmisíti meg, hogy azok használata a továbbiakban már nem lehetséges.

- A megszüntetés napján:
  - Szolgáltató az informatikai rendszerében foglalt adatokról teljes körű, időbélyegzővel és elektronikus aláírással vagy bélyegzővel ellátott mentést készít. A mentett adatállományokat védi a jogosulatlan módosítástól, és biztosítja, hogy az adatállomány tartalmához jogosulatlan személy nem férhet hozzá. A Szolgáltató a megkötött szerződés révén biztosítja, hogy az adatok a megőrzési időn belül az arra jogosult személyek számára hozzáférhetőek és értelmezhetőek.

6 MŰSZAKI BIZTONSÁGI ÓVINTÉZKEDÉSEK

6.1 Kulcspár előállítás és telepítés

6.1.1 Kulcspár előállítás

Szolgáltató az időbélyegző egységek által a kiadott időbélyegző hitelesítésére használt kulcspárokat fizikailag védett környezetben, az erre szolgáló HSM modulban, legalább két bizalmi munkakört betöltő személy együttes részvételével, illetéktelen személy jelenlétének kizárásával generálja. Szolgáltató a kulcspárok előállítását dokumentált „kulcs-ceremónia" eljárás szerint végzi, melyről a vonatkozó szabványi követelményeknek megfelelő jegyzőkönyv készül. A kriptográfiai modul megfelel a 6.2.1 fejezet szerinti követelményeknek, az időbélyegző egységek magánkulcsai teljes életciklusuk alatt abban kriptográfiai modulban maradnak, amelyben az előállításuk történt, más modulba nem kerülnek importálásra.

Az időbélyegző egység kulcspárjának generálása a Szolgáltató által megtervezett és előkészített „kulcs ceremónia" forgatókönyv szerint történik.

Egy időbélyegző egységnek egy időben csak egy aktív kulcspárja lehet.

6.1.2 Magánkulcs eljuttatása a tulajdonoshoz

A magánkulcs az időbélyegző egység által használt HSM modulban kerül előállításra – ezek tulajdonosa a Szolgáltató -, így tulajdonoshoz való eljuttatása nem szükséges.

6.1.3 Nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz

Az időbélyegző egység által használt HSM modulban generált kulcspárhoz PKCS#10 formátumnak megfelelő, a nyilvános kulcshoz tartozó magánkulccsal létrehozott digitális aláírással hitelesített tanúsítványkérelem kerül előállításra, amelyre az 1.3.1 fejezetben azonosított produktív hitelesítő központ az elektronikus bélyegzés célú tanúsítvány kiadására vonatkozó eljárásrend szerint állítja ki a tanúsítványt.

6.1.4 Időbélyegző egységek nyilvános kulcsának közzététele

Szolgáltató az időbélyegző egység nyilvános kulcsát az időbélyegző egység tanúsítványában teszi közzé a 2.2 fejezetben leírtak szerint.

Érintett Feleknek a szolgáltatói tanúsítványokra az {Sz8} RFC 5280 6. fejezetében leírt tanúsítási útvonal felépítést és érvényesítést javasolt elvégezniük az érintett nyilvános kulcs használata előtt.

6.1.5 Kulcs méretek

Szolgáltató a Szolgáltatás nyújtása során – mind a produktív hitelesítő központok, mind az időbélyegző egységek kulcsainak tekintetében – az {Sz18} ETSI TS 119 312 szabványban javasolt szabványos algoritmusokat, paramétereket és kulcshosszokat használ.

Az RSA környezetben a tanúsítványokban használt kulcspárok algoritmusa és kulcshossza, valamint a tanúsítvány hitelesítéséhez használt aláírási algoritmus:

TANÚSÍTVÁNY	KULCSPÁR ALGORITMUSA ÉS KULCSHOSSZA	A TANÚSÍTVÁNY HITELESÍTÉSÉHEZ HASZNÁLT ALGORITMUS
„Főtanúsítványkiadó - Kormányzati Hitelesítés Szolgáltató”	RSA 4096 bit	SHA256withRSA
„Minősített Tanúsítványkiadó v2”	RSA 2048 bit	SHA256withRSA
RSA időbélyegzőt hitelesítő tanúsítványok	RSA 2048 bit	SHA256withRSA

A Szolgáltató az RSA környezetben az időbélyegzőket SHA256withRSA aláírási algoritmus használatával hitelesíti.

Az ECC környezetben a tanúsítványokban használt kulcspárok algoritmusa és kulcshossza, valamint a tanúsítvány hitelesítéséhez használt aláírási algoritmus:

TANÚSÍTVÁNY	KULCSPÁR ALGORITMUSA ÉS KULCSHOSSZA	A TANÚSÍTVÁNY HITELESÍTÉSÉHEZ HASZNÁLT ALGORITMUS
„GovCA Főtanúsítványkiadó”	NIST P-384 (384 bit)	SHA384withECDSA
„GovCA Minősített Időbélyegző Tanúsítványkiadó”	NIST P-384 (384 bit)	SHA384withECDSA
ECC időbélyegzőt hitelesítő tanúsítványok	NIST P-256 (256 bit)	SHA384withECDSA

A Szolgáltató az ECC környezetben az időbélyegzőket SHA386withECDSA aláírási algoritmus használatával hitelesíti.

A Szolgáltató folyamatosan figyelemmel kíséri a technikai fejlődést és ennek függvényében szükség esetén gondoskodik az algoritmus váltásról vagy a kulcshosszak növeléséről.

6.1.6 A nyilvános kulcs paraméterek előállítása és megfelelőségének ellenőrzése

Az időbélyegző egységek kulcspárjainak előállítása a 6.1.1 fejezet szerint védett környezetben és tanúsított HSM modulban, legalább két bizalmi munkakört betöltő személy együttes részvételével, más személyek jelenlétét kizárva történik. A kulcspárok generálása során Szolgáltató betartja a HSM modul tanúsítási jelentésében foglalt előírásokat is.

6.1.7 A kulcs használat célja (X.509 v3 kulcs használati mezőnek megfelelően)

Az időbélyegző egység magánkulcsa csak és kizárólag időbélyegzők hitelesítésére használható.

Szolgáltató az időbélyegző tanúsítványokban a `KeyUsage` és `ExtendedKeyUsage` kiterjesztésekben az {Sz11} ITU-T X.509 v3 szabványnak és a {Sz15} EN 319 422 szabványnak megfelelően jelzi a kulcs használat célját.

	kiterjesztés	kiterjesztés

	kritikus?	KeyUsage	kritikus?	ExtendedKeyUsage
időbélyegző egység tanúsítványa	igen	`contentCommitment`[12]	igen	`timeStamping`

6.2 Magánkulcs védelme és kriptográfiai modul műszaki szabályozások

6.2.1 Kriptográfiai modul szabványok és műszaki szabályozások

Szolgáltató az időbélyegző egységek magánkulcsainak előállítására, tárolására és használatára olyan kriptográfiai modult alkalmaz, amely:

- olyan megbízható rendszer, amelynek értékelése az MSZ/ISO/IEC 15408 {Sz19} szerint, illetve azzal egyenértékű biztonsági kritériumok szerint 4-es vagy magasabb értékelési garancia szinten történt meg; vagy
- megfelel az ISO/IEC 19790 {Sz20} követelményeinek; vagy
- megfelel a FIPS 140-2 {Sz21} 3-as, illetve annál magasabb szintű követelményeknek; vagy
- megfelel a FIPS 140-3 {Sz23} 3-as, illetve annál magasabb szintű követelményeknek.

6.2.2 Több szereplős ("n-ből m") ellenőrzés

Szolgáltató a hitelesítő központokban alkalmazza a több szereplős "n-ből m" ellenőrzést a gyökér hitelesítő központ kulcsgondozási funkcióinak aktivizálásánál.

6.2.3 Magánkulcs letét

Szolgáltató az időbélyegző egységek magánkulcsait nem teszi letétbe.

6.2.4 Magánkulcs visszaállítása

Az időbélyegző egységek magánkulcsai biztonsági okokból mentésre kerülnek. A mentés fizikailag biztonságos helyszínen, legalább kettő bizalmi munkakört betöltő személy részvételével, titkosított formában, speciális eszközök alkalmazásával történik. Szolgáltató az időbélyegző egységek magánkulcsait rendkívüli üzemi helyzetek esetén a titkosított mentésből visszaállíthatja, hasonlóan szigorú fizikai, biztonsági óvintézkedések és eljárási szabályok betartásával, mint ahogy a magánkulcs előállítása eredetileg történt.

6.2.5 Magánkulcs mentése

Az időbélyegző egységek magánkulcsai biztonsági okokból mentésre kerülnek. A mentés fizikailag biztonságos helyszínen, legalább kettő bizalmi munkakört betöltő személy részvételével titkosított formában, speciális eszközök alkalmazásával történik, megfelelő biztonsági óvintézkedések és eljárási szabályok betartásával, melyek garantálják a magánkulcs sértetlenségét és bizalmasságát. A mentett példányok titkosított formában, fizikailag biztonságos környezetben kerülnek megőrzésre.

[12] X.509 előző verzióban és RFC 5280 szabványban: `nonRepudiation`

6.2.6 Magánkulcs bejuttatása a kriptográfiai modulba

Az időbélyegző egységek magánkulcsai teljes életciklusuk alatt a 6.2.1 fejezetben leírt HSM modulban kerülnek tárolásra.

6.2.7 Magánkulcs kriptográfiai modulban történő tárolásának módja

Az időbélyegző egységek magánkulcsai teljes életciklusuk alatt a 6.2.1 fejezetben leírt, tanúsítással rendelkező HSM modulban kerülnek tárolásra. A kulcsok tárolása során Szolgáltató betartja a HSM modul tanúsítási jelentésében foglalt előírásokat.

6.2.8 Magánkulcs aktiválásának módja

Az időbélyegző központok magánkulcsainak aktiválását Szolgáltató a HSM modul gyártói dokumentációjában előírtak szerint végzi el.

6.2.9 Magánkulcs aktív állapotának megszüntetési módja

Szolgáltató biztosítja, hogy az időbélyegző egység aktivált HSM modulja jogosulatlan hozzáférés ellen védett legyen. A HSM modul működése során csak a kiadott időbélyegzők hitelesítésére használható. A magánkulcs eltávolításra kerül a HSM modulból, amikor az időbélyegző egység működése megszűnik.

6.2.10 Magánkulcs megsemmisítésének módja

Szolgáltató az időbélyegző egységek magánkulcsát visszaállíthatatlan módon megsemmisíti, amikor használatuk már nem szükséges, vagy a magánkulcs használati időtartama (6.3.2) lejárt, vagy a kapcsolódó tanúsítvány lejárt vagy visszavonásra került. A magánkulcs és az aktiválásához szükséges minden adat megsemmisítését olyan módon végzi, hogy annak végrehajtása után a magánkulcs semmilyen része ne legyen kikövetkeztethető vagy levezethető.

6.2.11 Kriptográfiai modul értékelése

A 6.2.1 fejezet tartalmazza.

6.3 Kulcspár gondozás egyéb szempontjai

6.3.1 Nyilvános kulcs archiválása

Szolgáltató minden időbélyegző egység által valaha használt tanúsítványt archivál és az érvényesség lejártától – vagy a kapcsolódó magánkulcs használat végétől - számított tíz évig, illetve az időbélyegzővel kapcsolatban esetlegesen felmerült jogvita jogerős lezárásáig megőriz. Az archiválás biztonsági okokból két példányban (redundáns rendszer alkalmazásával) történik. A megőrzési kötelezettségnek Szolgáltató minősített archiválás szolgáltató igénybe vételével is eleget tehet.

6.3.2 Tanúsítvány érvényességi időszaka és kulcspár felhasználás időtartama

Az időbélyegző egységek tanúsítványainak érvényessége: legfeljebb a kibocsátástól számított 9 év. Szolgáltató a magánkulcs használati időtartamát ennél rövidebb, jellemzően az előállítástól számított 1 év időszakban határozza meg.

A kulcs használati időtartama nem lehet hosszabb, mint az {Sz18} ETSI TS 119 312 szabványban javasolt, és a Bizalmi Felügyelet algoritmus határozatában megszabott használati időtartam. A kulcs használati időtartam nem lehet hosszabb, mint a tanúsítvány érvényessége.

Szolgáltató a 6.2.10 fejezetben leírt módon megsemmisíti az időbélyegző egység magánkulcsát és annak minden mentett példányát a használati időtartam lejártakor.

6.4 Aktivizáló adatok

6.4.1 Aktivizáló adatok előállítása és telepítése

Szolgáltató az aktivizáló adatok előállítását és telepítését az időbélyegző egységben használt HSM modul felhasználói útmutatójában leírt eljárásokkal végzi el, melynek során betartja a HSM modul tanúsítási jelentésében foglalt előírásokat is.

6.4.2 Aktivizáló adatok védelme

Szolgáltató biztosítja az időbélyegző egységek magánkulcsai aktivizáló eszközeinek, aktivizáló kódjainak biztonságos tárolását és használatát.

6.4.3 Aktivizáló adatok egyéb szempontjai

Nincs kikötés.

6.5 Informatikai biztonsági óvintézkedések

6.5.1 Informatikai biztonsági műszaki követelmények meghatározása

Az informatikai biztonság műszaki követelményeit a Szolgáltató az {Sz14} EN 319 421 és {Sz2} EN 319 401 szabványoknak az elektronikus időbélyegzőket kibocsátó bizalmi szolgáltatás nyújtására vonatkozó, informatikai biztonsági műszaki követelményeiben határozza meg.

Ennek alapján Szolgáltató olyan megbízható rendszert (beleértve a redundáns kiépítést) és technikákat alakított ki és üzemeltet, melyek biztosítják a Szolgáltató megbízható működését a Szolgáltatások nyújtásához. Ennek ismertetését a Szolgáltató részben jelen szolgáltatási szabályzatban, részben belső biztonsági szabályzataiban írja le.

6.5.2 Informatikai biztonsági értékelés

Szolgáltató a Szolgáltatások nyújtásához kialakított és üzemeltetett informatikai rendszerét a {J13} 7/2024 MK rendelet 1. mellékletében felsorolt szempontok szerint biztonsági osztályba sorolta.

Szolgáltató az informatikai rendszerek biztonsági értékelését a {J12} kiberbiztonsági törvény rendelkezései szerint végzi.

Szolgáltató a Szolgáltatások nyújtásához kialakított és üzemeltetett informatikai rendszerével kapcsolatban teljesíti a {J11} NIS2 irányelv vonatkozó követelményeit.

6.6 Életciklusra vonatkozó műszaki óvintézkedések

6.6.1 Rendszerfejlesztési óvintézkedések

Szolgáltató gondoskodik arról, hogy az általa vagy a nevében végzett valamennyi rendszerfejlesztési projektjében a biztonság követelményeit már a tervezési és követelmény meghatározási fázisban figyelembe vegyék annak érdekében, hogy a biztonság beépüljön az informatikai rendszerekbe.

Az IT életciklusra vonatkozó rendszerfejlesztési szabályokat a Szolgáltató belső információbiztonsági szabályzata tartalmazza, amely pontosan meghatározza a tervezés és előkészítés, a projekt és kivitelezés, a működtetés és a menedzselés, valamint a visszacsatolás, illetve visszavonás/rekonstrukció ciklus időszakok feladatait és az alkalmazott módszertanokat. A belső információbiztonsági szabályzat figyelembe veszi az {Sz14} EN 319 421 szabvány 7. fejezetében előírt követelményeket.

Szolgáltató folyamatosan vizsgálja az időbélyegző egységek informatikai eszközeinek terheltségét és kihasználtságát, ez alapján meghatározza a jövőben várható kapacitás igényeket és ennek megfelelően időben megteszi a szükséges intézkedéseket ahhoz, hogy a Szolgáltatás jövőbeni nyújtásához megfelelő számítási teljesítmény és tároló kapacitás rendelkezésre álljon.

6.6.2 Biztonságkezelési óvintézkedések

Szolgáltató olyan eszközöket és eljárásokat alkalmaz, melyek garantálják a Szolgáltatást megvalósító, megbízható informatikai rendszereinek konfigurációs beállításai, az operációs rendszer beállítások, a hálózati konfigurációs beállítások, továbbá az alkalmazott biztonsági mechanizmusok sértetlenségének és helyes működésének ellenőrzését.

A biztonságkezelési szabályokat a Szolgáltató PKI informatikai biztonságpolitikája {D5}, illetve biztonsági szabályzata {D6} tartalmazza.

6.6.3 Életciklus biztonsági óvintézkedések

Szolgáltató az alábbi táblázatban megadott rendszerességgel elvégzi a Szolgáltatást megvalósító, megbízható informatikai rendszereinek konfigurációs beállításai, az operációs rendszer beállítások, a hálózati konfigurációs beállítások, továbbá az alkalmazott biztonsági mechanizmusok sértetlenségének és helyes működésének ellenőrzését.

biztonsági ellenőrzés típusa		**végzi**	**rendszeresség**
operatív	IT infrastruktúra	rendszerüzemeltető operátorok	naponta
	szolgáltatás nyújtásához használt alkalmazások és naplóik	rendszervizsgálók	naponta
belső ellenőrzés	IT infrastruktúra	biztonsági tisztviselő	évente egyszer
	szolgáltatás nyújtásához használt alkalmazások és naplóik	biztonsági tisztviselő	évente egyszer
	IT infrastruktúra	külső auditor	évente egyszer

külső ellenőrzés	szolgáltatás nyújtásához használt alkalmazások és naplóik	külső auditor	évente egyszer

6.7 Hálózatbiztonsági óvintézkedések

A hálózati védelmi intézkedéseket a Szolgáltató {D6} biztonsági szabályzatában meghatározott követelményeknek megfelelően valósítja meg, melyek figyelembe veszik az {Sz2} EN 319 401 szabvány 7.8 fejezetében és az {Sz14} EN 319 421 szabvány 7.10 fejezetében leírt követelményeket is.

Szolgáltató bizalmi munkakört betöltő munkatársai az időbélyegző egységek informatikai rendszereit úgy konfigurálják, hogy minden, a Szolgáltatás nyújtásához nem szükséges felhasználó és jogosultság, alkalmazás, protokoll, port vagy hálózati szolgáltatás letiltásra vagy eltávolításra kerüljön.

6.8 Időforrások

Az időbélyegző egységek által használt időforrás visszavezethető legalább egy UTC laboratórium által szolgáltatott, pontos időforrásra.

A Szolgáltató az *ntp.gov.hu* és *ntp2.gov.hu* referencia időforrásokat használja, melyek pontossága századmásodpercen belüli.

7 TANÚSÍTVÁNY, CRL ÉS OCSP PROFILOK / CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Tanúsítvány profil

Az időbélyegző egységek által használt tanúsítványok profilja megfelel az {Sz8} RFC 5280, {Sz4} EN 319 412-1, {Sz5} EN 319-412-2, {Sz6} EN 319 412-3, {Sz7} EN 319-412-5 és {Sz15} EN 319 422 szabványok vonatkozó előírásainak.

7.2 CRL profil

Az időbélyegző egységek tanúsítványai visszavonási állapotának ellenőrzése céljára, a Szolgáltató által kiadott visszavonási listák profilja megfelel az {Sz8} RFC 5280 műszaki szabványnak.

7.3 OCSP profil

Az időbélyegző egységek tanúsítványai visszavonási állapotának ellenőrzése céljára, a Szolgáltató által biztosított OCSP szolgáltatásban kiadott válaszok profilja megfelel az {Sz12} RFC 6960 műszaki szabványnak.

8 MEGFELELŐSÉG VIZSGÁLAT ÉS EGYÉB ÉRTÉKELÉSEK

Jelen bizalmi szolgáltatási szabályzat tartalmazza az összes, a nyilvános körben, minősített elektronikus időbélyegzőket kibocsátó bizalmi szolgáltatás nyújtása során teljesíteni szükséges követelményt, melyet különösen az alábbi szabványok határoznak meg:

- EN 319 401: General policy requirements for Trust Service Providers {Sz2}
- EN 319 421: Policy and Security Requirements for Trust Service Providers issuing Time-Stamps {Sz14}
- EN 319 422: Time-Stamping protocol and time-stamp token profiles {Sz15}

8.1 Vizsgálatok gyakorisága és körülményei

Szolgáltató külső és belső vizsgálatokat végez, illetve végeztet annak érdekében, hogy a Szolgáltatással kapcsolatos folyamatai, eszközei, személyzete és környezete mindenkor megfeleljenek a vonatkozó jogszabályi és szabványi követelményeknek. A Szolgáltató érintett szervezetei és munkatársai kötelesek együttműködni a Szolgáltató által kijelölt auditorral, és biztosítani az ellenőrzéshez szükséges feltételeket.

Szabályzatainak megfelelőségét Szolgáltató saját szervezete részéről a Szabályozási Csoport vizsgálja meg. A Szolgáltatás megfelelőségének vizsgálatára Szolgáltató saját belső ellenőrzéseket hajt végre.

A Szolgáltató nyilvános szabályzatait a Bizalmi Felügyelet is megvizsgálja a nyilvántartásba vételi eljárása során, valamint a szabályzatok módosításakor, és megfelelőség esetén közzé teszi a kötelezően benyújtandó szabályzatokat. A Bizalmi Felügyelet rendszeres időközönként átfogó helyszíni ellenőrzés keretében ellenőrizheti Szolgáltató tevékenységét.

Szolgáltató rendelkezik minőségbiztosítási rendszerrel és információbiztonsági irányítási rendszerrel, melyek megfelelő működését külső független rendszervizsgáló ellenőrzési tevékenysége biztosítja. Szolgáltató a külső, illetve a saját ellenőrző szervezet által végzett belső vizsgálatokat a {D6} PKI szolgáltatások biztonsági szabályzatában megjelölt rendszerességgel - évente legalább egyszer biztosítja.

Szolgáltató legalább 24 havonta egyszer megfelelőségértékelést és 12 havonta egyszer felülvizsgálatot végeztet a {J1} eIDAS, illetve a {J2} DÁP tv. követelményeinek való megfelelés tárgykörben. Szolgáltató az elkészült megfelelőségértékelési jelentést annak kézhezvételétől számított három munkanapon belül benyújtja a Bizalmi Felügyeletnek.

Szolgáltató a Szolgáltatások nyújtásához kialakított és üzemeltetett informatikai rendszerére vonatkozóan a kiberbiztonsági követelményeknek való megfelelés bizonyítására kétévente kiberbiztonsági auditot végeztet a Kiberbiztonsági Felügyelet által nyilvántartott auditorok egyikével. Az audit eredményét az auditor a vizsgálat befejezését követően haladéktalanul megküldi Szolgáltatónak és a Kiberbiztonsági Felügyeletnek.

8.2 Auditor azonosítása és képesítése

A megfelelőségértékelés és a kiberbiztonsági audit előkészítésére, illetve az információbiztonsági rendszer ellenőrzésére Szolgáltató külső rendszervizsgálót alkalmaz.

A külső rendszervizsgáló által végzett auditokat Szolgáltató olyan szakértővel vagy szakértői szolgáltatásokat nyújtó szervezettel végezteti el, aki független Szolgáltatótól, illetve az ellenőrzött rendszertől, területtől, és szakértelmét biztosítani tudja a PKI és az informatikai biztonság, valamint

az ezen területekre vonatkozó technikai, technológiai, jogi, szabályzati ismeretek és auditálási módszertanok vonatkozásában.

A Szolgáltató tevékenységére és az informatikai biztonságra vonatkozó belső ellenőrzéseket a Szolgáltató belső szervezete végzi, az ott dolgozó biztonsági tisztviselők bevonásával.

A megfelelőségértékelési vizsgálatot Szolgáltató olyan, a 765/2008/EK rendelet 2. cikkének 13. pontjában meghatározott megfelelőségértékelő szervezettel végezteti el, melyet az említett rendelettel összhangban illetékesnek ismernek el a minősített bizalmi szolgáltató és az általa nyújtott minősített bizalmi szolgáltatások megfelelőségének értékelésére.

A kiberbiztonsági auditot Szolgáltató olyan auditorral végezteti el, amely szerepel a Kiberbiztonsági felügyelet nyilvántartásában, és jogosult a Szolgáltató elektronikus információs rendszerének biztonsági osztálya szerinti auditálásra.

8.3 Auditor függetlensége

A megfelelőségértékelő szervezet, a külső vizsgálatokat végző szervezet, annak munkatársai, valamint a külső rendszervizsgáló teljes mértékben függetlenek Szolgáltatótól.

8.4 Audit során vizsgált területek

Az audit az alábbi területeket fedi le:

- szabályzatok és dokumentációk;
- irányítási és ellenőrzési követelmények;
- személyzeti biztonsági követelmények;
- a szolgáltatói kulcspár kezeléséhez kapcsolódó követelmények;
- üzemeltetési és hozzáférési biztonság;
- fizikai és környezeti biztonság;
- folyamatos szolgáltatás biztosítása;
- adatbiztonság és archiválás.

Az audit során megvizsgálásra kerül, hogy Szolgáltató és az általa nyújtott Szolgáltatás megfelel-e:

- a hatályos jogszabályoknak és szabványoknak;
- a szolgáltatási szabályzatnak, illetve a bizalmi szolgáltatási rendnek.

8.5 Hiányosságok esetén végrehajtandó tevékenységek

Az üzemszerű ellenőrzések, belső és külső auditok, szakértői elemzések által feltárt hiányosságok, hibás gyakorlatok kezelésére Szolgáltató intézkedési tervet készít. A hiányosságokat késlekedés nélkül orvosolja, az intézkedéseket dokumentálja és ellenőrzi.

A Bizalmi Felügyelet által végzett helyszíni ellenőrzések során feltárt esetleges hiányosságokat Szolgáltató a hatósággal megállapodott határidőn belül megszünteti a hatályos jogszabályok alapján és a hatóságtól kapott információk és ajánlások figyelembe vételével.

8.6 Eredmény kommunikációja

A belső és külső auditot, szakértői elemzést végző személyek csak a megbízójuknak adhatnak információt a Szolgáltató tevékenységével kapcsolatban. Az audit és az ellenőrzés eredményei a Szolgáltató bizalmas üzleti információi, ezért azokat a társaság titokvédelmi előírásai szerint kell kezelni, azonban a hiányosságok felszámolásáról a Bizalmi Felügyeletet a következő helyszíni

ellenőrzés során tájékoztatni kell. Szolgáltató nem köteles a konkrét hiányosságot nyilvánosságra hozni.

9 EGYÉB ÜZLETI ÉS JOGI KÉRDÉSEK

9.1 Díjak

A szolgáltatási díjakat Szolgáltató a Szolgáltatás internetes honlapján teheti közzé, vagy ártájékoztatót küldhet az érdeklődők számára. Szolgáltató jogosult a díjakat egyoldalúan meghatározni, módosítani.

Az Előfizetőre vonatkozó szolgáltatási díjak a Szolgáltatási Szerződésben kerülnek rögzítésre.

9.1.1 Időbélyegzők díja

Szolgáltató az eSzemélyi tulajdonosok (állampolgárok) számára kiadott időbélyegzőkért díjat nem számít fel.

A közületi ügyfelek esetében Szolgáltató az időbélyegzők kibocsátásáért a Szolgáltatási Szerződésben meghatározott havi és/vagy tranzakciós díjat számítja fel.

9.1.2 Tanúsítványhozzáférés díja

Szolgáltató nem számít fel díjat az időbélyegző egységek tanúsítványai és az egyéb szolgáltatói tanúsítványoknak az eléréséért.

9.1.3 Visszavonási és állapot információ hozzáférés díja

Szolgáltató nem számít fel díjat a tanúsítványok visszavonási állapotára vonatkozó státusz információk (CRL és OCSP) szolgáltatásáért.

9.1.4 Egyéb szolgáltatások díja

Nincs kikötés.

9.1.5 Visszatérítési szabályzat

Visszatérítéssel kapcsolatos rendelkezéseket Szolgáltató nem állapít meg.

9.2 Anyagi felelősség

A Szolgáltató anyagi felelősségének mértékéről, illetve annak korlátairól a {D1} Általános Szerződési Feltételek rendelkezik.

9.2.1 Biztosítási fedezet

A Szolgáltató rendelkezik olyan felelősségbiztosítással, mely egyaránt kiterjed az elektronikus aláírással vagy bélyegzővel, az időbélyegzővel, illetve az ezzel ellátott elektronikus dokumentummal szerződésen kívül okozott károkra és szerződésszegéssel okozott károkra, és amely fedezetet biztosít az összes károsultnak okozott kárra, a {D1} Általános Szerződési Feltételekben rögzítettek szerint.

A felelősségbiztosítás ezen felül kiterjed az alábbiakra is:

- a {J2} DÁP tv. 92. §-ban foglalt kötelezettség nem teljesítése miatt a Bizalmi Felügyeletnél felmerült, a DÁP tv. 93. §-a szerinti költségekre;
- a {J1} eIDAS 17. cikk (4) bekezdés e) pontja alapján a Bizalmi Felügyelet által felkért megfelelőségértékelő szervezet eljárásainak költségeire, ha ezt a Bizalmi Felügyelet eljárási költségként érvényesíti.

A biztosítási szerződésben szereplő felelősségvállalási érték 3.000.000 Ft, vagy ennél esetenként magasabb összeg.

9.2.2 További követelmények

Szolgáltató rendelkezik a {J8} 24/2016 rendelet˙20. §-a szerint, huszonötmillió forint összegű, feltétel nélküli és visszavonhatatlan bankgaranciával.

9.2.3 Felelősségbiztosítás vagy garancia végfelhasználók számára

Nincs kikötés.

9.3 Üzleti információk bizalmassága

9.3.1 Bizalmasan kezelendő információk köre

Szolgáltató minden olyan adatot és információt bizalmasnak tekint, melyek nem kerültek felsorolásra a 9.3.2 fejezetben.

9.3.2 Nem bizalmasnak tekintett információk köre

Nem bizalmasnak tekintett információk az alábbiak:

- időbélyegző és egyéb szolgáltatói tanúsítványok és az azokban foglalt adatok;
- a Szolgáltatás igénybevételéhez a közületi Előfizetőknek kiadott autentikációs tanúsítvány
- a tanúsítványokhoz kapcsolódó visszavonási információk;
- a Szolgáltató internetes honlapján közzétett nyilvános információk, szabályzatok és egyéb dokumentumok;
- az olyan adatok, melyek nyilvános adatforrásból elérhetők.

9.3.3 Bizalmas információk védelmének felelőssége

Szolgáltató a bizalmas információkhoz való hozzáférést csak az arra feljogosított személyek és szervezetek számára teszi lehetővé. A bizalmas információk védelmét a személyzet megfelelő képzésével, továbbá a munkavállalókkal, szerződéses partnerekkel megkötött szerződésekkel juttatja érvényre.

9.4 Személyes adatok védelme

9.4.1 Adatvédelmi terv

Szolgáltató rendelkezik mind társasági szintű adatvédelmi tervvel ({D4}), mind pedig a Szolgáltatásra vonatkozó adatvédelmi tájékoztatóval, melyek nyilvános dokumentumok, és

elérhetők Szolgáltató internetes honlapján. Ezen dokumentumok összhangban vannak a nemzetközi és hazai vonatkozó jogszabályokkal.

Szolgáltató, mint adatkezelő, szerepel a Nemzeti Adatvédelmi és Információszabadság Hivatal Adatvédelmi Nyilvántartásában.

9.4.2 Bizalmasként kezelendő személyes adatok

Szolgáltató csak Előfizetőktől, illetve Előfizető Kapcsolattartójától közvetlenül, azok kifejezett írásos hozzájárulásával gyűjt személyes adatot és csak olyan mértékben, ami a Szolgáltatási Szerződés megkötéséhez, valamint a Szolgáltatás nyújtásához szükséges.

Szolgáltató bizalmasként kezelendő személyes adatnak tekinti:

- közületi Előfizető részéről a Szolgáltatói Szerződésben érintett személyek (pl. cégjegyzésre jogosult vezető, vagy Előfizető Kapcsolattartója) minden adatát;
- eSzemélyi esetén Előfizető minden adatát, mely a minősített aláíró tanúsítványában nem jelenik meg.

9.4.3 Bizalmasként nem kezelendő személyes adatok

Szolgáltató nem köteles bizalmasként kezelni az olyan személyes adatokat, melyek nyilvános adatforrásból elérhetők.

9.4.4 Személyes adatok védelmének felelőssége

Szolgáltató gondoskodik a személyes adatok védelméről, működése és szabályzatai megfelelnek a {J10} GDPR rendelkezéseinek.

9.4.5 Hozzájárulás a személyes adatok felhasználásához

Előfizetőnek a Szolgáltatási Szerződés aláírásával hozzá kell járulnia a szolgáltatási szerződés megkötéséhez és a Szolgáltatás nyújtásához szükséges adatok Szolgáltató által történő nyilvántartásba vételéhez, kezeléséhez és tárolásához.

Közületi Előfizető esetén Előfizető Kapcsolattartójának a regisztrációs űrlap kitöltésével és aláírásával hozzá kell járulnia az autentikációs tanúsítvány kiállításához szükséges adatok Szolgáltató által történő nyilvántartásba vételéhez, kezeléséhez és tárolásához.

9.4.6 Felfedés bírósági vagy polgári peres eljárás keretében

A Szolgáltató bűncselekmények felderítése vagy megelőzése céljából, illetve nemzetbiztonsági érdekből - az adatigénylésre meghatározott jogszabályi feltételek teljesülése esetén - a nyomozó hatóságnak és a nemzetbiztonsági szolgálatoknak haladéktalanul és egyéb feltételek nélkül feltárja a jogszabályban meghatározott bizalmas információkat. Szolgáltató rögzíti az adatátadás tényét, de arról nem tájékoztatja érintett Előfizetőt.

Szolgáltató az időbélyegző érvényességét érintő polgári peres, illetve nem peres eljárás során - az érintettség igazolása esetén - az ellenérdekű peres félnek vagy képviselőjének, valamint a megkereső bíróságnak feltárhatja a jogszabályban meghatározott bizalmas információkat. Szolgáltató rögzíti az adatátadás tényét, és arról tájékoztatja érintett Előfizetőt.

9.4.7 Egyéb, felfedést eredményező körülmények

Szolgáltató a szolgáltatási tevékenység, illetve a Szolgáltatás nyújtásának megszüntetése esetén Előfizetők, illetve a Kapcsolattartók adatait a jogszabályi kötelezettségeire tekintettel átadja harmadik félnek.

9.5 Szellemi tulajdonjogok

A Szolgáltató által a közületi ügyfelei részére kiadott, az Előfizető azonosításához szükséges tanúsítványok és az ahhoz tartozó kulcspár, illetve aktivizáló adat tulajdonosa az Előfizető.

A Szolgáltató tulajdonát képezik az időbélyegző egységek tanúsítványai és az egyéb szolgáltatói tanúsítványok, visszavonási információk, az Előfizető azonosításához használt tanúsítványokban szereplő, Szolgáltató által létrehozott azonosítók.

Szolgáltató kizárólagos tulajdonát képezik a szabályzatai, szerződéses feltételei és egyéb, a Szolgáltatás internetes honlapján közzétett dokumentumai. Ezen dokumentumok felhasználása csak és kizárólag a Szolgáltatás használatával összefüggésben engedélyezett, minden egyéb kereskedelmi vagy egyéb célú felhasználása szigorúan tilos.

9.6 Tevékenységért viselt felelősség és helytállás

9.6.1 Szolgáltató felelőssége és helytállása

Szolgáltató felel a bizalmi szolgáltatási rendben és jelen szolgáltatási szabályzatban, valamint az Előfizetővel megkötött Szolgáltatási Szerződésben megfogalmazott valamennyi kötelezettsége maradéktalan betartásáért, még akkor is, ha a Szolgáltatás nyújtásához kapcsolódó egyes feladatokat egyéb alvállalkozók végeznek.

Szolgáltató a vele szerződéses jogviszonyban nem álló harmadik személlyel szemben a {J5} Polgári Törvénykönyv 6:519. §-a szerint, a vele szerződéses jogviszonyban álló Előfizetővel szemben a szerződésszegésért való felelősség ({J5} Polgári Törvénykönyv 6:142. §) szabályai szerint felelős az elektronikus időbélyegzővel ellátott elektronikus dokumentummal okozott kárért, ha megszegte a bizalmi szolgáltatási rendben és a jelen szolgáltatási szabályzatban, valamint az Előfizetővel megkötött Szolgáltatási Szerződésben előírtakat, vagy az esemény időpontjában hatályos jogszabály szerinti, rá vonatkozó kötelezettségeket. E kötelezettségek megtartását kétség esetén Szolgáltatónak kell bizonyítania. Szolgáltató sajátjaként felel az egyéb alvállalkozók által a Szolgáltatás nyújtása során okozott kárért.

Szolgáltató a felelősségi körén belül keletkezett, bizonyított károkért az Előfizetővel megkötött Szolgáltatási Szerződésben és a 9.8 fejezetben foglalt korlátozásokkal kártérítést fizet.

Szolgáltató nem felel:

- az Előfizetők alábbi tevékenységeiért:
  - eSzemélyi ügyfél az eSzemélyi-vel kapcsolatos tevékenységeiért;
  - közületi ügyfél autentikációs tanúsítvánnyal és ahhoz kapcsolódó magánkulccsal kapcsolatos tevékenységeiért;
  - ha Előfizető nem a jelen szabályzat 4.2.1 fejezetében megadott címre (hanem például konkrét IP címre) küldi az időbélyegző kéréseket.
- az Érintett Felek időbélyeg ellenőrzési és felhasználási tevékenységeiért;
- az Érintett Felek vagy mások által kibocsátott szabályzatokért.

9.6.2 Szolgáltató kötelezettségei

Szolgáltató azzal, hogy kibocsát egy elektronikus időbélyegzőt – mely jelen szolgáltatás szabályzat hatálya alatt került kiadásra – arra vállal kötelezettséget, hogy a Szolgáltatás nyújtása során ő maga és a Szolgáltatás nyújtásában közreműködő egyéb alvállalkozói a jelen szabályzatban foglaltakat maradéktalanul betartják. Szolgáltató megteszi a szükséges és tőle telhető intézkedéseket ahhoz, hogy az Előfizetők is jelen szabályzat előírásainak megfelelően járjanak el.

Szolgáltató köteles a Szolgáltatás nyújtása során:

- a szerződéskötést megelőző tájékoztatást megadni;
- Szolgáltatási Szerződés megkötéséhez szükséges adatokat felvenni, továbbá a szerződést, a bizalmi szolgáltatási rendet és a szolgáltatási szabályzatot tartós adathordozón Előfizető rendelkezésére bocsátani;
- a közületi Előfizetőt ellátni az időbélyegzés hozzáféréshez szükséges autentikációs tanúsítvánnyal;
- az Előfizetőktől kapott időbélyegző kérésekre a 4.1 fejezetben leírt ellenőrzéseket elvégezni;
- az ellenőrzéseken meg nem felelt időbélyegző kéréseket visszautasítani;
- az ellenőrzéseken megfelelt időbélyegző kérésre a 4.4 fejezetben leírt tartalmú, megfelelő időbélyegző választ kiadni, melyet a 4.5 fejezetben leírtaknak megfelelően hitelesített;
- az időbélyegzők pontosságát a 4.6 fejezetben megadott időtartamon belül tartani;
- a Szolgáltatás megbízhatóságát és biztonságát a minősített időbélyegzés szolgáltatásra vonatkozó követelményeknek megfelelően biztosítani;
- naplózni a Szolgáltatással kapcsolatos minden fontos esemény, a naplóállományokat a jogszabályi előírásoknak megfelelően megőrizni.

9.6.3 Előfizető felelőssége és helytállása

Előfizető jogai

Előfizető jogosult:

- a Szolgáltatás igénybevételére a jelen szabályzatban, a Szolgáltatási Szerződésben és a {D1} Általános Szerződési Feltételekben leírtak szerint;
- a kiadott időbélyegzőket a jelen szabályzatban leírt módon felhasználni.

Előfizető felelőssége

Az Előfizető felelős:

- a szolgáltatási szerződés megkötése során megadott adatainak valódiságáért, pontosságáért és érvényességéért;
- közületi Előfizető esetén az autentikációs tanúsítvány igényléséért;
- közületi Előfizető esetén az autentikációs tanúsítvány időben történő megújításáért, ha a Szolgáltatást továbbra is igénybe kívánja venni;
- az adataikban bekövetkezett változás haladéktalan bejelentéséért;
- a Szolgáltatás igénybevételéhez szükséges, számára kiadott azonosítók (tanúsítvány és kapcsolódó magánkulcs) biztonságos kezeléséért;
- az időbélyegző kérésnek a 4.1 fejezetben megadott követelményeknek megfelelő összeállításáért;
- a kapott időbélyegző válaszra a 4.7 fejezetben előírt ellenőrzéseknek az elvégzéséért;
- az időbélyegző szabályzatoknak megfelelő felhasználásáért;
- a Szolgáltató haladéktalan értesítéséért és teljes körű tájékoztatásáért vitás ügyek esetén;
- általában, a jelen szabályzatban előírt kötelezettségei betartásáért.

Ezen túlmenően Előfizető felelősségét a Szolgáltatási Szerződés és a {D1} Általános Szerződési Feltételek határozzák meg.

Előfizető kötelezettségei:

Előfizető kötelessége a Szolgáltató szabályzatainak és szerződéses feltételeinek megfelelően eljárni a Szolgáltatás használata során, beleértve az időbélyegzők kérését és felhasználását. Az Előfizető kötelezettségeit a szolgáltatási szabályzat, a Szolgáltatási Szerződés és annak {D1} Általános Szerződési Feltételek melléklete tartalmazzák.

Ezen túlmenően Előfizető köteles:

- a Szolgáltatás használata előtt megismerni a szolgáltatási szabályzatot;
- a Szolgáltató által kért, a Szolgáltatás igénybevételéhez szükséges adatokat hiánytalanul és a valóságnak megfelelően megadni;
- olyan megbízható informatikai rendszert (számítógépes programot) használni, amely képes időbélyegzőket kérni és fogadni a 4. fejezetben leírt módon;
- a Szolgáltatást kizárólag a jogszabályok által megengedett vagy nem tiltott célokra, a jelen szabályzatban és a hivatkozott dokumentumokban foglaltaknak megfelelően használni;
- adatváltozás (különösen az értesítéshez szükséges adatok) esetén haladéktalanul írásban értesíteni erről Szolgáltatót;
- biztosítani, hogy a Szolgáltatás igénybevételéhez szükséges adatokhoz és eszközökhöz (különösen az időbélyegzés hozzáférés titkos adataihoz) illetéktelen személy ne férhessen hozzá;
- haladéktalanul, írásban értesíteni Szolgáltatót, ha az időbélyegzővel vagy az annak felhasználásával kapcsolatban jogvita indul.

9.6.4 Érintett felek felelőssége és helytállása

Az Érintett Felek a saját belátásuk és/vagy szabályzataik szerint dönthetnek az egyes időbélyegzők elfogadásáról és a felhasználás módjáról. Az időbélyegző érvényességének elbírálása során az Érintett Félnek megfelelő körültekintéssel kell eljárnia, ezért különös tekintettel javasolt:

- a szolgáltatási szabályzatban foglalt követelmények és előírások betartása, különösen az időbélyegző hitelességének ellenőrzése a 4.7 fejezetben leírt módon;
- megbízható informatikai környezet és alkalmazások használata;
- az időbélyegző felhasználására vonatkozó valamennyi korlátozás figyelembevétele, amely a tanúsítványban vagy a szolgáltatási szabályzatban szerepel;
- a tőle elvárható magatartás tanúsítása az időbélyegzők ellenőrzésekor.

Szolgáltató kizárja a felelősségét (9.8 fejezet), amennyiben az Érintett Fél az időbélyegző elfogadásakor nem körültekintően, vagy nem a tőle elvárható gondossággal jár el.

9.6.5 Egyéb felek felelőssége és helytállása

Nincs kikötés.

9.7 Helytállás érvénytelenségi köre

Szolgáltató kizárja felelősségét, amennyiben:

- az Érintett Fél nem körültekintően jár el az időbélyegzők ellenőrzése és felhasználásra során, azaz nem jelen szolgáltatási szabályzatnak vagy a hatályos jogszabályoknak megfelelően jár el;

- az Érintett Felek vagy mások által kibocsátott szabályzatok nem felelnek meg jelen szabályzatnak;
- az Internet, vagy annak egy részének működési hibájából fakadóan tájékoztatási vagy egyéb kommunikációs kötelezettségeit nem tudja ellátni;
- Előfizető, illetve Előfizető kapcsolattartója által megadott értesítési email cím időközben megváltozott vagy megszűnt, és ebből fakadóan Szolgáltató nem tudja őket értesíteni;
- az Előfizető nem tesz eleget a szolgáltatási szabályzatban előírt kötelezettségeinek;
- a károkozás a Bizalmi Felügyelet Szolgáltatónak kiadott, hatályos határozatában közölt kriptográfiai algoritmusok hibájából, illetve gyengeségeiből ered.

9.8 Felelősség korlátozása

Szolgáltató nem felelős az olyan károkért, melyek abból adódnak, hogy az Érintett Fél a időbélyegzők ellenőrzése és felhasználása során nem a hatályos jogszabályok és a mérvadó műszaki szabványok szerint járt el, illetve nem tanúsította a tőle elvárható gondosságot.

A Szolgáltató pénzügyi felelősségének korlátját a Szolgáltatási Szerződés, illetve a {D1} Általános Szerződési Feltételek határozza meg. Ha egy biztosítási eseménnyel kapcsolatban több jogosult megalapozott kártérítési igénye meghaladja ezt az összeget, akkor az egyes kártérítési igények megtérítése az összes kártérítési igénynek a megadott összeghez viszonyított arányában történik.

9.9 Kártérítések

A kártérítésekről a jelen szabályzat 9.8 fejezetében leírtakon túl a Szolgáltatási Szerződés és a {D1} Általános Szerződési Feltételek rendelkeznek.

9.10 Hatályosság és megszűnés

9.10.1 Hatályosság

Időbeli hatály

A szolgáltatási szabályzat egy adott verziójának időbeli hatálya a címlapon feltüntetett hatálybalépés dátumával kezdődik és határozatlan időre szól. Az időbeli hatály megszűnik a szolgáltatási szabályzat újabb verziójának hatályba lépésével vagy a Szolgáltatás befejezésekor.

Tárgyi hatály

A szolgáltatási szabályzat tárgyi hatálya kiterjed a Szolgáltatás nyújtására és igénybevételére.

Személyi hatály

A szolgáltatási szabályzat személyi hatálya kiterjed Szolgáltatónak a Szolgáltatás nyújtásában közreműködő munkatársaira, továbbá az Előfizetőkre:

- eSzemélyi ügyfelek esetén a személyazonosító igazolvány tulajdonosára;
- közületi ügyfelek esetén Előfizető Kapcsolattartójára, valamint Előfizető szervezetén belül az egyes elektronikus időbélyegzők felhasználásáért felelős személyekre.

9.10.2 Megszűnés

A bizalmi szolgáltatási szabályzat a Szolgáltató szolgáltatási tevékenységének befejezésével tekintendő megszűntnek.

9.10.3 Megszűnés után is hatályban maradó rendelkezések

A megszűnés után is hatályban maradó rendelkezéseket – amennyiben ilyenek vannak – a {D1} Általános Szerződési Feltételek és a Szolgáltatási Szerződés tartalmazza.

9.11 Egyéni hirdetmények és kommunikáció a részvevőkkel

9.11.1 eSzemélyi ügyfelek esetén

Azokban az esetekben, melyekre jelen szolgáltatási szabályzat nem rendelkezik a felek közötti értesítésről, illetve annak joghatást kiváltó módjáról, a Szolgáltató értesítése elektronikus aláírással hitelesítve az ekozig@1818.hu email címre beküldéssel történik. Az elektronikus értesítés csak a Szolgáltató általi visszaigazolást követően tekinthető kézbesítettnek. Szolgáltató a megkeresésekre 30 napon belül válaszol elektronikus aláírással ellátott válasz üzenetben.

9.11.2 Közületi ügyfelek esetén

Azokban az esetekben, melyekre jelen szolgáltatási szabályzat nem rendelkezik a felek közötti értesítésről, illetve annak joghatást kiváltó módjáról, a Szolgáltató értesítése írásban vagy emailben, Előfizető kapcsolattartója saját kezű vagy elektronikus aláírásával hitelesítve az Ügyfélkapcsolati Iroda elérhetőségeire való beküldéssel történik. Az elektronikus értesítés csak a Szolgáltató általi visszaigazolást követően tekinthető kézbesítettnek. Szolgáltató a megkeresésekre 30 napon belül válaszol elektronikus aláírással vagy bélyegzővel ellátott válasz üzenetben.

9.12 Módosítások

9.12.1 Módosítás eljárása

A szolgáltatási szabályzat módosítása az 1.5.3 és 1.5.4 fejezetekben leírt szabályok szerint történik. A szolgáltatási szabályzat módosulását a verziószám megfelelő változása jelzi.

9.12.2 Értesítés módszere és időtartama

A Szolgáltatás jelentős vagy lényeges változása esetén Szolgáltató internetes honlapján közleményt tesz közzé és emailben tájékoztatást küld Előfizetőknek, a hatályba lépést megelőzően kellő időben ahhoz, hogy az érintett a felek a változásokra felkészülhessenek.

9.12.3 OID megváltozását előidéző körülmények

A szolgáltatási szabályzat OID-ja nem változik.

9.13 Vitás kérdések rendezése

Bármely vitás kérdés felmerülése előtt az Előfizetőnek kötelessége a Szolgáltató haladéktalan értesítése és teljes körű tájékoztatása a kérdés minden vonatkozását illetően, a vita jogi útra terelése előtt.

Az eSzemélyi ügyfelek a panaszt a Kormányzati Ügyfélvonal 1.5.2.1 fejezetben megadott elérhetőségein terjeszthetik elő.

A közületi ügyfelek a panaszt írásban vagy személyesen, az Ügyfélkapcsolati Iroda elérhetőségein tudják előterjeszteni. A panaszt a Szolgáltató az előterjesztéstől számított 30 napon belül kivizsgálja és ennek eredményéről a panaszost írásban tájékoztatja.

A jogviták esetén követendő eljárást a {D1} Általános Szerződési Feltételek tartalmazza.

Bármely vitás kérdés felmerülése esetén az esetleges bírósági eljárást megelőzően a jogszabályok szerinti fogyasztónak lehetősége van békéltető testülethez fordulni. Az illetékes békéltető testület megnevezését és elérhetőségeit jelen szabályzat 1.5.2 fejezete tartalmazza.

9.14 Irányadó jog

Szolgáltató szerződéseire, szabályzataira és azok teljesítésére a magyar jog az irányadó és azokat a magyar jog szerint kell értelmezni.

9.15 Hatályos jognak megfelelés

Szolgáltató tevékenységét a mindenkor hatályos Európai Uniós, illetve magyar jogszabályoknak megfelelően köteles végezni.

9.16 Vegyes rendelkezések

Nincs kikötés.

9.16.1 Teljességi záradék

Nincs kikötés.

9.16.2 Átruházás

Nincs kikötés.

9.16.3 Részleges érvénytelenség

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

9.16.4 Igényérvényesítés

Szolgáltató kártérítésre, az ügyvédi díjak megfizetésére tarthat igényt a partnerei által okozott károk, veszteségek, költségek megtérítése érdekében. Amennyiben Szolgáltató egy konkrét esetben nem él kártérítési igényével, az nem jelenti azt, hogy a jövőben hasonló esetben a szolgáltatási

szabályzat más rendelkezésének megsértése esetén is lemondana a kártérítési igény érvényesítéséről.

9.16.5 Force Majeure (Vis maior)

Vis maior: Az olyan – a Szolgáltató akaratától, cselekedeteitől és személyétől függetlenül bekövetkező és érdekkörén kívül eső elháríthatatlan – esemény (pl. sztrájk, háború, polgári felkelés, természeti katasztrófa, a Felek bármelyikének partnerénél felmerülő elháríthatatlan fizikai vagy jogi akadály vagy más elháríthatatlan szükséghelyzet) minősül vis maiornak, amely megakadályozza vagy lehetetlenné teszi a jelen szolgáltatási szabályzatban foglalt követelmény teljesítését, feltéve, hogy ezen körülmények a jelen szolgáltatási szabályzat hatálybalépését követően keletkeznek, illetőleg azt megelőzően következtek be, ám a jelen szolgáltatási szabályzat teljesítésére kiható következményeik az említett időpontban még nem voltak előre láthatóak.

Szolgáltató nem felelős a vis maior esetekből fakadó károkért.

9.17 Egyéb rendelkezések

Szolgáltató a Szolgáltatást és ennek keretében alkalmazott végfelhasználói termékeket hozzáférhetővé teszi a fogyatékossággal élő személyek számára, amennyiben az lehetséges.

TSA Közzétételi Nyilatkozat (TDS)

Teljességi záradék

Jelen közzétételi nyilatkozat nem tartalmazza a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. (a továbbiakban: Szolgáltató) időbélyegzés szolgáltatásra vonatkozó teljes szabályzatát.

Az „*Időbélyegzés Bizalmi Szolgáltatási Szabályzat*" (IBSZ) dokumentum a Szolgáltató internetes honlapján érhető el.

Szolgáltató elérhetősége eSzemélyi ügyfelek számára

Az időbélyegzés szolgáltatást igénybe vevő eSzemélyi ügyfelek a Kormányzati Ügyfélvonalon vehetik fel Szolgáltatóval a kapcsolatot.

Telefon:	1818 Kormányzati Ügyfélvonal, külföldről: +36 1 550-1858
Email:	ekozig@1818.hu
Postacím:	Kormányzati Ügyfélvonal, 1389 Budapest, Pf: 133

Az időbélyegzés szolgáltatást igénybe vevő eSzemélyi tulajdonosok a Kormányzati Ügyfélvonal 1818 hívószámán telefonon, vagy emailben az ekozig@1818.hu címre küldve, továbbá írásban a 1389 Budapest, Pf: 133 postacímre terjeszthetik elő a panaszt Szolgáltató részére.

Szolgáltató elérhetősége közületi ügyfelek számára

Ügyfélkapcsolati Iroda

Az ügyfelekkel való kapcsolattartás érdekében a Szolgáltató Ügyfélkapcsolati Irodát tart fenn, mely egyben a Szolgáltatásért illetékes szervezeti egység, és amelyet az ügyfelek személyesen, illetve telefonon a nyitvatartási időkben kereshetnek fel. A mindenkori nyitvatartási időket a Szolgáltató a Szolgáltatás internetes honlapján teszi közé.

Cím:	1097 Budapest, Vaskapu u.30/b.
Telefon:	+36 1 795-7200
Email:	info@hiteles.gov.hu
Szolgáltatás internetes honlapja	https://hiteles.gov.hu/

Telefonos Ügyfélszolgálat

A Szolgáltatás nyújtásához felhasznált rendszerrel kapcsolatos műszaki hibák bejelentésére a Szolgáltató folyamatos (7x24 órás) ügyfélszolgálatot (Help Desk) biztosít.

Telefon:	+36 1 795-7300
Email:	helpdesk@nisz.hu

Illetékes fogyasztóvédelmi felügyelőség

Budapest Főváros Kormányhivatala, Fogyasztóvédelmi Főosztály

Cím:	1051 Budapest, Sas u.19.
Telefon:	+36 1 450-2598
Email:	fogyved_kmf_budapest@bfkh.gov.hu

Illetékes békéltető testület

Budapesti Békéltető Testület
Cím: 1016 Budapest, Krisztina krt. 99. I. em.111.
Levelezési cím: 1253 Budapest, Pf.:10.
Telefon: +36 1 488 2131
Email: bekelteto.testulet@bkik.hu

Időbélyegzők alkalmazhatósága

Az szolgáltatásban kiadott időbélyegzők az Európai Parlament és a Tanács 910/2014/EU Rendeletének (eIDAS) 42. cikke szerinti minősített elektronikus időbélyegzők, melyek alkalmasak az időbélyegzett adatok sértetlenségének és bélyegzés dátumának és időpontjának bizonyítására.

A minősített elektronikus időbélyegző joghatását az Európai Parlament és a Tanács 910/2014/EU Rendeletének (eIDAS) 41. cikke határozza meg. E szerint, a minősített elektronikus időbélyegzőt bírósági eljárásokban bizonyítékként el kell fogadni és vélelmezni kell az általa feltüntetett dátum és időpont pontosságát, valamint az adott dátumhoz és időponthoz kapcsolt adatok sértetlenségét.

A Szolgáltató által kiadott időbélyegzők azonosíthatók azáltal, hogy azokat az időbélyegző egységek olyan elektronikus bélyegzés célú tanúsítvánnyal hitelesítik, melyben szerepel a Szolgáltató közhiteles nyilvántartás szerinti teljes neve és közösségi adószáma.

Időbélyegzők pontossága

Az időbélyegzőkben szereplő időpontok pontossága 1 másodpercen belüli.

Az időbélyegzés szolgáltatással kapcsolatos események naplóinak megőrzési ideje az időbélyegző kiadásától számított 10 év.

Előfizetők kötelezettségei

Az Előfizetők kötelesek az „*Időbélyegzés Bizalmi Szolgáltatási Szabályzat*” (IBSZ), a szolgáltatási szerződés és annak mellékletei szerint eljárni az időbélyegzők kérése és felhasználása során.

Ajánlások az Érintett Felek számára

Az időbélyegző érvényességének elbírálása során az Érintett Félnek megfelelő körültekintéssel kell eljárnia, ezért különös tekintettel javasolt:

- az időbélyegző hitelességének ellenőrzése:
  - Szolgáltató időbélyegzőn elhelyezett elektronikus bélyegzőjének kriptográfiai ellenőrzésével;
  - az időbélyegzőt hitelesítő tanúsítvány érvényességének ellenőrzésével, az RFC 5280 6. fejezete szerinti tanúsítási útvonal felépítésével és érvényesítésével;
  - az időbélyegzőt hitelesítő tanúsítvány visszavonási állapotának ellenőrzésével, a tanúsítványban feltüntetett elérhetőségről letöltött CRL vagy megkért OCSP válasz alapján;
  - az olyan felhasználási célok esetén, ahol jogszabályi vagy egyéb követelmény minősített időbélyegző használatát írja elő:
    - ellenőrizni, hogy az időbélyegző tartalmaz `QcStatements` kiterjesztést és abban a `tst-EuQcCompliance`[13] nyilatkozatot; és/vagy
    - ellenőrizni azt, hogy az időbélyegzőt kibocsátó szolgáltatás - a bélyegzett időpontra vonatkoztatva - szerepel-e EU minősített szolgáltatásként és megfelelő státusszal és az Európai Parlament és a Tanács 910/2014/EU Rendeletének (eIDAS) 22. cikke szerinti Bizalmi Listán.

[13] OID: 0.4.0.19422.1.1

- ellenőrizni, hogy a bélyegzett dokumentum összetartozik-e a kapott időbélyegzővel (azaz az időbélyegző `messageImprint` mezőjében szereplő lenyomat és a dokumentumra kiszámított lenyomat egyező);
- ellenőrizni, hogy az időbélyegzőben szereplő pontosság, a szabályzatokban vállalt felelősségvállalás az adott célra megfelelő-e;
- archiválás céljára történő felhasználás esetén ellenőrizni, hogy időbélyegzőben szereplő lenyomatok és aláírási algoritmusok megfelelően erősek-e a tervezett megőrzési időtartamra;
    - figyelembe venni és betartani minden olyan korlátozást, ami az időbélyegzőben és az időbélyeget hitelesítő tanúsítvány által hivatkozott szabályzatokban szerepel.
- megbízható informatikai környezet és alkalmazások használata;

Felelősség kizárása

Szolgáltató kizárja a felelősségét, amennyiben az Érintett Fél az időbélyegző elfogadásakor nem körültekintően, vagy nem a tőle elvárható gondossággal jár el.

Időbélyegzési Bizalmi Szolgáltatási Rend

Az „*Időbélyegzési Bizalmi Szolgáltatási Rend*” (IBR) elérhető a Szolgáltató internetes honlapján.

Az IBR megfelel az EN 319 421 szabvány 5.2 fejezet a) pontjában meghatározott BTSP időbélyegzési rendnek:

```
BTSP : a best practices policy for time-stamp.
itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023)
policy-identifiers(1) best-practices-ts-policy (1)
```

A Szolgáltatás keretében kiadott időbélyegzők tartalmazzák az IBR objektumazonosítóját.

Személyes adatok védelme

Szolgáltató, mint adatkezelő, szerepel a Nemzeti Adatvédelmi és Információszabadság Hivatal (NAIH) nyilvántartásában. Az adatbiztonsági szabályzat a Szolgáltató internetes honlapján érhető el.

Visszatérítési szabályzat

Visszatérítéssel kapcsolatos rendelkezéseket Szolgáltató nem állapít meg.

Bizalmi jegy, audit

A Szolgáltató 910/2014/EU rendelet 20. cikke szerinti megfelelőségértékelésére vonatkozó adatok:

- a megfelelőségértékelő szerv neve: Hunguard Kft.
- a megfelelőségértékelési jelentés azonosítója: HUNG-T-ESIGN-R-032-2025

Szolgáltató jogosult a 910/2014/EU rendelet 23. cikke szerinti „uniós bizalmi jegy” használatára.

A Bizalmi Lista elérhetősége (amelyen a Szolgáltatás EU minősített státusza feltüntetésre került):

http://www.nmhh.hu/tl/pub/HU_TL.xml (géppel feldolgozható formátum)
http://www.nmhh.hu/tl/pub/HU_TL.pdf (ember által olvasható formátum)