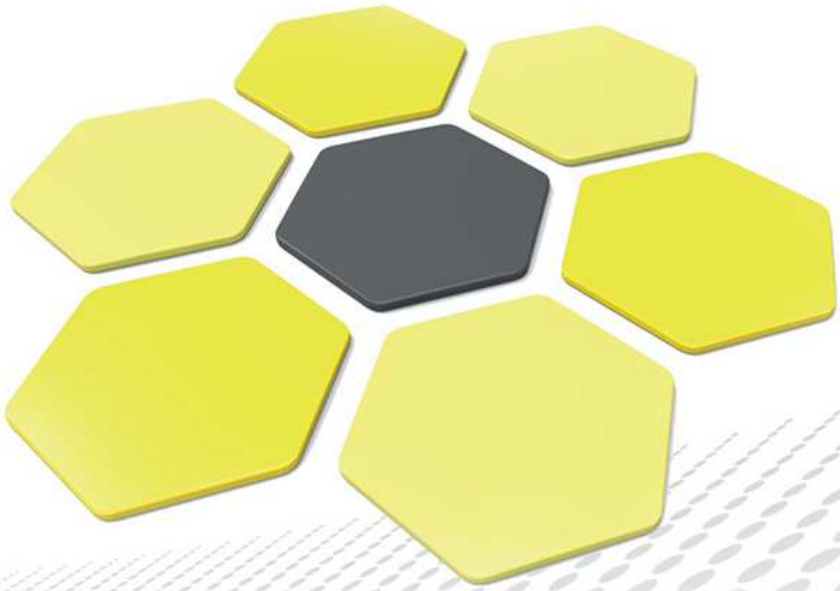
MICROSEC

e-Szignó Hitelesítés Szolgáltató

eIDAS rendelet szerinti minősített időbélyegzési rend

ver. 2.0

Hatályba lépés: 2016-07-01



Azonosító	1.3.6.1.4.1.21528.2.1.1.86.2.0
Verzió	2.0
Első verzió hatálybalépése	2005-04-01
Biztonsági besorolás	NYILVÁNOS
Jóváhagyta	Vanczák Gergely
Jóváhagyás dátuma	2016-05-31
Hatálybalépés dátuma	2016-07-01

Microsec Számítástechnikai Fejlesztő zártkörűen működő Részvénytársaság

1031 Budapest, Záhony utca 7. D. épület

Verzió	A változás leírása	Hatálybalépés	Készítette
1.0	Első változat OID: 1.3.6.1.4.1.21528.2.1.1.3	2005-04-01	Berta István Zsolt, Endrődi Csilla Belső auditor: Tóth Elemér
2.0	A belső auditor javaslatai alapján átdolgozott változat (azonos az 1.1-es verzióval)	2005-04-15	Berta István Zsolt, Belső auditor: Tóth Elemér
3.0	Apróbb javítások	2005-05-02	Berta István Zsolt, Belső auditor: Tóth Elemér
3.2	A hatósági szemlét követő módosítások	2005-08-08	Berta István Zsolt, Belső auditor: Tóth Elemér
4.0	Módosítás az általános szerződési feltételek megváltozása miatt	2006-11-19	Dr. Berta István Zsolt
4.1	Új OID hozzárendelése. OID: 1.3.6.1.4.1.21528.2.1.1.3.4.1	2006-12-04	Dr. Berta István Zsolt
4.2	A fogyasztóvédelem elérhetősége megváltozott. OID: 1.3.6.1.4.1.21528.2.1.1.3.4.2	2007-10-28	Dr. Berta István Zsolt
4.3	A fogyasztóvédelem elérhetősége ismét megváltozott. OID: 1.3.6.1.4.1.21528.2.1.1.3.4.3	2008-01-01	Dr. Berta István Zsolt
4.4	Nem lépett hatályba. OID: 1.3.6.1.4.1.21528.2.1.1.3.4.4	2008-10-01	Dr. Berta István Zsolt
4.5	Az időbélyegek naplózásának megszüntetése. OID: 1.3.6.1.4.1.21528.2.1.1.3.4.5	2008-12-20	Dr. Berta István Zsolt
5.0	Cégforma változás. OID: 1.3.6.1.4.1.21528.2.1.1.3.5.0	2012-05-01	Dr. Berta István Zsolt
5.1	Kisebb változtatások. OID: 1.3.6.1.4.1.21528.2.1.1.3.5.1	2013-08-01	Dr. Szőke Sándor
2.0	eIDAS szerinti követelményeknek megfelelő új rend új OID azonosítóval. OID: 1.3.6.1.4.1.21528.2.1.1.86.2.0	2016-07-01	Dr. Szőke Sándor

Tartalomjegyzék

1. Bevezetés

Jelen dokumentum a Microsec Számítástechnikai Fejlesztő zrt. (továbbiakban: *Időbélyegzés-szolgáltató*) által üzemeltetett e-Szignó Hitelesítés Szolgáltató által kidolgozott *Minősített időbélyegzési rend*et tartalmazza.

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

A minősített bizalmi szolgáltatás nyújtásának és az "EU Trust Mark" feltüntetésének előfeltétele, hogy:

- a szolgáltatást vizsgálja meg egy eIDAS rendelet szerinti akkreditált független vizsgáló labor, a sikeres vizsgálatról állítson ki egy megfelelőségértékelési jelentést és egy tanúsítványt az *Időbélyegzés-szolgáltató* részére;
- az *Időbélyegzés-szolgáltató* nyújtsa be a megfelelőségértékelésről szóló tanúsítványt a Nemzeti Média- és Hírközlési Hatóságnak, mint ellenőrző hatósági szervezetnek;
- a Nemzeti Média- és Hírközlési Hatóság fogadja el a benyújtott megfelelőségértékelési tanúsítványt és jelentesse meg a szolgáltatást a nemzeti bizalmi listában.

1.1. Áttekintés

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

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

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

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

1.2. Dokumentum neve és azonosítója

1.2.1. A dokumentum főbb azonosító adatai

Kibocsátó	e-Szignó Hitelesítés Szolgáltató
Dokumentum címe	eIDAS rendelet szerinti minősített időbélyegzési rend
Azonosító	1.3.6.1.4.1.21528.2.1.1.86
Dokumentum verziószáma	2.0
Hatályba lépés ideje	2016-07-01

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

1.2.2. Megfelelés

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

- ETSI EN 319 421 [14] szerinti
  BTSP: a best practices policy for time-stamp
  OID: itu-t(0) identified-organization(4) etsi(0)time-stamp-policy(2023)policy-identifiers(1) best-practices-ts-policy (1)

A követelményeknek való megfelelés kinyilatkoztatása érdekében az *Időbélyegzés-szolgáltató* két megoldás közül választhat:

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

1.2.3. Hatály

Jelen *Minősített időbélyegzési rend* 2016-07-01-i hatálybalépési dátumtól visszavonásáig hatályos.

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

Jelen *Minősített időbélyegzési rend* területi hatálya Magyarországra terjed ki. Az *Időbélyegzés-szolgáltató* működésére vonatkozóan a mindenkori magyar jogszabályok az irányadóak.

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

1.3. PKI szereplők

1.3.1. Szolgáltató

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

Jelen dokumentum előírásai vonatkoznak mindazon *Időbélyegzés-szolgáltató*kra, akik a *Minősített időbélyegzési szolgáltatási szabályzat*ukban vállalják a jelen dokumentumban szereplő *Minősített időbélyegzési rend*nek való megfelelést.

1.3.2. Ügyfelek

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

1.3.3. Érintett felek

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

1.4. Az időbélyegző felhasználhatósága

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

1.5. A dokumentum adminisztrálása

1.5.1. A dokumentum adminisztrációs szervezete

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

Szervezet neve	Microsec e-Szignó Hitelesítés Szolgáltató
Szervezet címe	Magyarország, H-1037 Budapest, Záhony utca 7. D épület
Telefonszám	+36 1 505-4444

Fax szám	+36 1 505-4445
E-mail cím	info@e-szigno.hu

1.5.2. Kapcsolattartó személy

Jelen *Minősített időbélyegzési rend*del kapcsolatos kérdésekben közvetlenül az alábbi személyhez lehet fordulni:

Kapcsolattartó	Folyamatszervezés részleg vezetője
Szervezet neve	Microsec zrt.
Szervezet címe	Magyarország, H-1037 Budapest, Záhony utca 7. D épület
Telefonszám	+36 1 505-4444
Fax szám	+36 1 505-4445
E-mail cím	info@e-szigno.hu

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

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

A *Minősített időbélyegzési szolgáltatási szabályzat*ok és a szolgáltatások nyújtása feletti felügyeletet a Nemzeti Média- és Hírközlési Hatóság látja el. A Nemzeti Média- és Hírközlési Hatóság nyilvántartást vezet a követelményeknek megfelelő *Minősített időbélyegzési rend*ekről valamint az ezeket alkalmazó *Időbélyegzés-szolgáltató*król. A Nemzeti Média- és Hírközlési Hatóság a megfelelőség vizsgálatakor független megfelelőségértékelő szervezet megállapításaira támaszkodik.

1.5.4. A Szolgáltatási szabályzat elfogadási eljárása

A jelen *Minősített időbélyegzési rend*nek való megfelelőséget kinyilatkoztató *Minősített időbélyegzési szolgáltatási szabályzat* elfogadási eljárását az *Időbélyegzés-szolgáltató*nak ismertetnie kell az adott *Minősített időbélyegzési szolgáltatási szabályzat*ban.

1.6. Fogalmak és rövidítések

1.6.1. Fogalmak

Adatközpont	Számítógépes rendszerek és a hozzájuk kapcsolódó komponensek elhelyezésére és üzemeltetésére kialakított létesítmény. Ezek a komponensek rendszerint magukba foglalják a távközlési rendszereket és kommunikációs kapcsolatokat, redundáns áramforrást, adattárolókat, légkondicionáló, tűzvédelmi és biztonsági rendszereket.
Bizalmi felügyelet	"A *Bizalmi szolgáltatás*ok felügyeletét ellátó hatóság a Nemzeti Média- és Hírközlési Hatóság." (2015. évi CCXXII. törvény [4] 91.§ 1. bekezdés)
Bizalmi szolgáltatás (Trust Service)	"Rendszerint díjazás ellenében nyújtott, az alábbiakból álló elektronikus szolgáltatások: • elektronikus aláírások, elektronikus bélyegzők vagy elektronikus időbélyegzők, ajánlott elektronikus kézbesítési szolgáltatások, valamint az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok létrehozása, ellenőrzése és érvényesítése; vagy • *Weboldal-hitelesítő tanúsítvány*ok létrehozása, ellenőrzése és érvényesítése; vagy • elektronikus aláírások, bélyegzők vagy az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok megőrzése; " (eIDAS [1] 3. cikk 16. pont)
Bizalmi szolgáltatási rend (Trust Service Policy)	"Olyan szabálygyűjtemény, amelyben egy *Bizalmi szolgáltató*, igénybe vevő vagy más személy valamely *Bizalmi szolgáltatás* használatának feltételeit írja elő igénybe vevők valamely közös biztonsági követelményekkel rendelkező csoportja vagy meghatározott alkalmazások számára. " (2015. évi CCXXII. törvény [4] 1. § 8. pont)

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

Hitelesítő egység	A *Hitelesítés-szolgáltató* rendszerének egy egysége, amely *Tanúsítvány*ok digitális aláírását végzi. Egy *Hitelesítő egység*hez mindig egy elektronikus aláírás vagy bélyegző létrehozásához használt adat (magánkulcs) tartozik. Előfordulhat, hogy egy *Hitelesítés-szolgáltató* egyszerre több *Hitelesítő egység*et is működtet.
Időbélyegzési rend	Olyan *Bizalmi szolgáltatási rend*, amelyben egy szolgáltató, igénybe vevő vagy más személy (szervezet) valamely *Időbélyegző* felhasználásának feltételeit írja elő az igénybe vevők valamely közös biztonsági követelményekkel rendelkező csoportja, illetőleg meghatározott alkalmazások számára.
Időbélyegzés-szolgáltató	Olyan *Bizalmi szolgáltató*, amely *Bizalmi szolgáltatás* keretében *Időbélyegző*ket bocsát ki, és ellátja az ehhez kapcsolódó feladatokat.
Időbélyegző egység	Az *Időbélyegzés-szolgáltató* rendszerének egy egysége, amely az *Időbélyegző*k aláírását vagy bélyegzését végzi. Egy időbélyegző egységhez mindig egy elektronikus aláírás vagy bélyegző létrehozáshoz használt adat tartozik. Előfordulhat, hogy egy *Időbélyegzés-szolgáltató* egyszerre több időbélyegző egységet is működtet.
Kompromittálódás	Egy kriptográfiai kulcs akkor kompromittálódott, ha illetéktelen személyek is hozzáférhettek.
Köztes hitelesítő egység	Olyan *Hitelesítő egység* amelynek *Tanúsítvány*át egy másik *Hitelesítő egység* bocsátotta ki.
Kriptográfiai kulcs (Key)	Olyan kriptográfiai transzformációt vezérlő egyedi digitális jelsorozat, amelynek ismerete titkosításhoz és dekódoláshoz, illetve digitális aláírás előállításához és ellenőrzéséhez szükséges.
Kulcsgondozás (Key Management)	A kriptográfiai kulcsok előállítása, a felhasználókhoz történő eljuttatása vagy ennek algoritmikus megvalósítása, továbbá a kulcsok nyilvántartása, tárolása, archiválása, visszavonása, törlése, amely szoros kapcsolatban áll az alkalmazott biztonsági eljárásmóddal.

Magánkulcs	A Nyilvános kulcsú infrastruktúrában egy szereplőhöz tartozó aszimmetrikus kriptográfiai kulcspár azon eleme, amelyet az *Alany*nak szigorúan titokban kell tartania. A *Hitelesítés-szolgáltató* a *Tanúsítvány*ok kibocsátása során a *Hitelesítő egység* magánkulcsát használja arra, hogy a *Tanúsítvány*t védő elektronikus aláírást vagy bélyegzőt elhelyezze rajta.
Minősített bizalmi szolgáltatás (Qualified Trust Service)	"Olyan *Bizalmi szolgáltatás* amely megfelel az eIDAS rendeletben foglalt alkalmazandó követelményeknek." (eIDAS [1] 3. cikk 17. pont)
Minősített bizalmi szolgáltató (Qualified Trust Service Provider)	"Olyan *Bizalmi szolgáltató* amely egy vagy több *Minősített bizalmi szolgáltatás*t nyújt, és amelynek minősített státusát a felügyeleti szerv jóváhagyta. " (eIDAS [1] 3. cikk 20. pont)
Nyilvános kulcs	A Nyilvános kulcsú infrastruktúrában egy szereplőhöz tartozó aszimmetrikus kriptográfiai kulcspár azon eleme, amelyet nyilvánosságra kell hozni. A nyilvánosságra hozatal jellemzően egy *Tanúsítvány* formájában történik, amely összekapcsolja a szereplő nevét az ő nyilvános kulcsával. A *Tanúsítvány*ok hitelességét az őket kibocsátó *Hitelesítő egység* nyilvános kulcsa segítségével lehet ellenőrizni.
Nyilvános kulcsú infrastruktúra (Public Key Infrastructure, PKI)	Aszimmetrikus kulcsú kriptográfiára épülő infrastruktúra, beleértve a kriptográfiai algoritmusokat, kulcsokat, tanúsítványokat, a rájuk vonatkozó szabványokat és jogszabályokat, a mögöttes intézményrendszert, a különböző szolgáltatókat és eszközöket is.
Rendkívüli üzemeltetési helyzet	Olyan, az *Időbélyegzés-szolgáltató* üzemmenetében zavart okozó rendkívüli helyzet, amikor az *Időbélyegzés-szolgáltató* rendes üzemmenetének folytatására ideiglenesen vagy véglegesen nincsen lehetőség.
Szervezet	Jogi személy.

Szolgáltatási szabályzat (Trust Service Practice Statement)	"A *Bizalmi szolgáltató* nyilatkozata az egyes *Bizalmi szolgáltatás*ok nyújtásával kapcsolatosan alkalmazott részletes eljárási vagy más működési követelményekről. " (2015. évi CCXXII. törvény [4] 1. § 41. pont)
Szolgáltatási szerződés	"A *Bizalmi szolgáltató* és a *Bizalmi szolgáltatás*i ügyfél között létrejött szerződés, amely a *Bizalmi szolgáltatás* nyújtására és a szolgáltatás igénybevételére vonatkozó feltételeket tartalmazza. " (2015. évi CCXXII. törvény [4] 1. § 42. pont)
Tanúsítvány (Certificate)	"Az elektronikus aláírás tanúsítvány, az elektronikus bélyegző tanúsítvány és a *Weboldal-hitelesítő tanúsítvány*, valamint mindazon, a *Bizalmi szolgáltatás* keretében a szolgáltató által kibocsátott elektronikus igazolás, amely tartalmazza a tanúsítványra vonatkozó érvényesítési adatot és a tanúsítvány használatához szükséges kapcsolódó adatokat, és amely elektronikus dokumentum megbízhatóan védve van a kibocsátáskor és az érvényességi ideje alatt rendelkezésre álló technológiákkal elkövetett hamisítás ellen. " (2015. évi CCXXII. törvény [4] 1. § 44.)
Tanúsítvány kérelem	Az *Igénylő* által, a Szolgáltató számára a *Tanúsítvány* kibocsátás érdekében benyújtott adatok és nyilatkozatok, amelyekben többek között az *Igénylő* megerősíti a *Tanúsítvány*ba kerülő adatok valódiságát.
Tanúsítványtár	Különböző *Tanúsítvány*okat tartalmazó adattár. Tanúsítványtára van egy Szolgáltatónak is, amelyben az általa kibocsátott *Tanúsítvány*okat publikálja, de Tanúsítványtárnak nevezzük az *Érintett fél* számítógépén a használt alkalmazás számára elérhető *Tanúsítvány*okat tartalmazó rendszert is.
Ügyfél	Az *Előfizető* másik elnevezése.

Visszavonás	A *Tanúsítvány* érvényességének megszüntetése a *Tanúsítvány*ban is feltüntetett érvényességi idő lejárta előtt. A *Tanúsítvány* visszavonása végleges, visszavont *Tanúsítvány* többet nem tehető érvényessé.
Visszavonási állapot nyilvántartás	A *Hitelesítés-szolgáltató* által vezetett nyilvántartás a felfüggesztett, illetőleg a visszavont *Tanúsítvány*okról, amelyek tartalmazzák legalább a felfüggesztés vagy visszavonás tényét, és a felfüggesztés vagy visszavonás időpontját.

1.6.2. Rövidítések

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

2. Közzététel és tanúsítványtár

2.1. Adatbázisok - tanúsítványtárak

Az *Időbélyegzés-szolgáltató* publikálja a működése alapjául szolgáló *Minősített időbélyegzési rend*et, *Minősített időbélyegzési szolgáltatási szabályzat*ot valamint a szerződési feltételeket tartalmazó egyéb dokumentumokat.

2.2. A tanúsítványokra vonatkozó információk közzététele

Az *Időbélyegzés-szolgáltató* tegye közzé a honlapján a szolgáltatói *Tanúsítvány*ait.

2.2.1. Szolgáltatói információ közzététele

Az *Időbélyegzés-szolgáltató* hozza nyilvánosságra szerződéses feltételeit és szabályzatait a honlapján elektronikus formában.

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

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

A szabályzatok és szerződési feltételek aktuális verziója legyen nyomtatott formában olvasható az *Időbélyegzés-szolgáltató* ügyfélszolgálati irodájában.

Az *Időbélyegzés-szolgáltató* a szerződéskötést követően tartós adathordozón bocsássa az *Ügyfél* rendelkezésére a *Minősített időbélyegzési rend*et, a *Minősített időbélyegzési szolgáltatási szabályzat*ot és a Szolgáltatási szerződést.

Az *Időbélyegzés-szolgáltató* értesítse *Ügyfel*eit az Általános szerződési feltételek változásáról.

2.3. A közzététel időpontja vagy gyakorisága

2.3.1. Kikötések és feltételek közzétételi gyakorisága

A *Minősített időbélyegzési rend*del kapcsolatos új verziók közzététele a 9.12. fejezetben ismertetett eljárásoknak megfelelően történik.

Az *Időbélyegzés-szolgáltató* szükség szerint hozza nyilvánosságra egyéb szabályzatait, szerződéses feltételeit, illetve azok újabb változatait.

Az *Időbélyegzés-szolgáltató* a rendkívüli információkat a jogszabályi előírásoknak megfelelően tegye közzé, külön rendelkezés hiányában pedig késedelem nélkül.

3. Az Időbélyegző egység tanúsítványa és az Időbélyegzés

3.1. A felhasználó azonosítása

Az *Időbélyegzés-szolgáltató* az *Időbélyegző*k kibocsátását a felhasználók előzetes azonosításához kötheti. Az azonosítás módját ismertetni kell a *Minősített időbélyegzési szolgáltatási szabályzat*ban.

3.2. Az Időbélyegző egység tanúsítványa

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

- az *Időbélyegző egység* nyilvános kulcsát közzé kell tenni *Tanúsítvány* formájában;
- az *Időbélyegző egység Tanúsítvány*át olyan *Hitelesítés-szolgáltató*nak kell kibocsátania, amely az ETSI EN 319 411-1 [8] szerinti szolgáltatást nyújt;
- a 910/2014/EU rendelet [1] szerinti minősített *Időbélyegző*ket kibocsátó *Időbélyegző egység Tanúsítvány*át olyan *Hitelesítés-szolgáltató*nak kell kibocsátania, amely az ETSI EN 319 411-2 [9] szerinti szolgáltatást nyújt;
- az *Időbélyegző egység* csak akkor bocsáthat ki *Időbélyegző*ket, ha már rendelkezik az *Időbélyegző*k ellenőrzésére szolgáló Tanúsítvánnyal, és annak aláírását ellenőrizte a megbízható *Hitelesítés-szolgáltató*ig visszavezetett teljes érvényességi láncon.

3.3. Az Időbélyegző

Az *Időbélyegző*re vonatkozó követelmények:

- az *Időbélyegző* feleljen meg az IETF RFC 3161 [19] és az ETSI EN 319 422 [15] szabványoknak;
- az *Időbélyegző*t biztonságos körülmények között kell kibocsátani és a helyes időt kell tartalmaznia;
- az *Időbélyegző egység*(ek) *Időbélyegző*k kibocsátásához használt belső órája visszavezethető kell legyen legalább egy UTC laboratórium által szolgáltatott pontos időre;
- az *Időbélyegző*ben megadott időpont meg kell feleljen az UTC által szolgáltatott időértéknek, az eltérés nem haladhatja meg az *Időbélyegzési rend*ben vagy az *Időbélyegző*ben magában megadott pontosság értéket;
- az *Időbélyegző egység* nem bocsáthat ki *Időbélyegző*t, amint észleli hogy a belső óra pontossága a megadott mértéknél jobban eltér a UTC szerinti pontos időtől;
- az *Időbélyegző*k hitelesítésére használt magánkulcsok más célra nem használhatók;
- az *Időbélyegző egység*nek vissza kell utasítania minden *Időbélyegző* kibocsátási kérelmet a kulcsok élettartamának lejárta után.

3.3.1. Időbélyegző kérés

Az időbélyegző kliens támogassa az IETF RFC 3161 [19] 2.4.1. fejezete szerinti *Időbélyegző* kéréseket. Ajánlott az alábbi mezők támogatása:

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

Az *Időbélyegzés-szolgáltató* támogassa mindegyik kiterjesztés használatát.

Az *Időbélyegzés-szolgáltató* az ETSI TS 119 312 [16] szerinti és az aktuális Nemzeti Média- és Hírközlési Hatóság algoritmusokkal kapcsolatos határozatban kijelölt lenyomatképző algoritmusokat fogadhat be az *Időbélyegző* kérésekben. A lenyomatképző algoritmusok kiválasztásánál figyelembe kell venni az *Időbélyegző* tervezett felhasználási idejét és a lenyomatképző függvény várható megfelelőségi időtartamát.

3.3.2. Időbélyegző válasz

Az *Időbélyegzés-szolgáltató* támogassa az IETF RFC 3161 [19] 2.4.2. fejezete szerinti *Időbélyegző* válaszokat az alábbi kiegészítésekkel:

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

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

Az *Időbélyegzés-szolgáltató* az ETSI TS 119 312 [16] szerinti és az aktuális Nemzeti Média- és Hírközlési Hatóság algoritmusokkal kapcsolatos határozatban kijelölt kriptográfiai algoritmuskészleteket és kulcshosszakat használhat az *Időbélyegző*k aláírására. A kriptográfiai algoritmuskészletek és kulcshosszak kiválasztásánál figyelembe kell venni az *Időbélyegző* tervezett felhasználási idejét.

3.4. Az Időbélyegzőben szereplő idő pontossága

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

- az *Időbélyegző egység* óráját védeni kell az olyan fenyegetéstől, amely lehetővé tenné az óra észrevétlen átállítását a vállalt pontossági tartományon kívüli értékre;

- az *Időbélyegzés-szolgáltató*nak észlelnie kell, ha az *Időbélyegző*kbe írandó belső idő a vállalt pontossági tartományon kívül esik;
- amint az *Időbélyegzés-szolgáltató* észleli, hogy az *Időbélyegző*kbe írandó belső idő a vállalt pontossági tartományon kívül esik, szüneteltetnie kell az *Időbélyegző*k kibocsátását;

3.5. Óraszinkronizálás

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

3.5.1. A szökőmásodpercek kezelése

Az *Időbélyegzés-szolgáltató*nak el kell végeznie az óraszinkronizációt az illetékes szervezet értesítése alapján szökőmásodperc előfordulásakor. A változtatást a kitűzött nap utolsó percében kell végrehajtani az ETSI 319 421 [14] C függelékében meghatározottak szerint az ITU-R TF.460-6 [23] ajánlásnak megfelelően.

3.5.2. Nyári időszámítás kezelése

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

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

3.6. Az Időbélyegző ellenőrzése

Az *Időbélyegző*n szereplő elektronikus aláírás vagy elektronikus bélyegző érvényességének ellenőrzése során az *Érintett fél*nek célszerű az ETSI EN 319 102-1 [5] specifikációban leírtak szerint eljárnia.

Az *Időbélyegző* ellenőrzése során:

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

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

3.7. A szolgáltatás rendelkezésre állása

Az *Időbélyegzés-szolgáltató*nak biztosítania kell a szolgáltatás, valamint az *Időbélyegzés-szolgáltató* által kibocsátott *Időbélyegző*k használatára vonatkozó kikötések és feltételek folyamatos elérhetőségét éves szinten legalább 99,9% -os rendelkezésre állás mellett, ahol az eseti szolgáltatáskiesések időtartama legfeljebb 3 óra.

3.8. Nem minősített időbélyegzők kibocsátása

A 910/2014/EU rendelet [1] szerinti minősített *Időbélyegző*ket kibocsátó *Időbélyegző egység* nem bocsáthat ki nem minősített *Időbélyegző*ket.
A külön *Időbélyegző egység* nem feltétlenül jelent különálló hardvert és szoftvert, de a különféle biztonsági szintű szolgáltatások elkülönítéséhez legalább:

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

3.9. Az Időbélyegző egység kulcshasználata

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

- csak olyan algoritmusokat és kulcsméreteket használhatnak az *Időbélyegző*k hitelesítésére, amelyek megfelelnek az alábbi követelményeknek:
  - ETSI TS 119 312 [16];
  - a 2015. évi CCXXII törvény [4] 92. § (1) b) szerint kiadott aktuális Nemzeti Média- és Hírközlési Hatóság algoritmusokkal kapcsolatos határozat.
- az aláíró vagy bélyegző létrehozó magánkulcsot lehetőleg ne importálják egyszerre több *Hardver kriptográfiai eszköz*be;
- amennyiben több *Hardver kriptográfiai eszköz* is ugyanazt az aláíró vagy bélyegző létrehozó magánkulcsot használja, akkor azoknak ugyanahhoz a *Tanúsítvány*hoz kell tartozniuk;
- egy *Időbélyegző egység*ben egyidőben csak egy *Időbélyegző* aláíró vagy bélyegző létrehozó magánkulcs lehet aktív;
- egy hardver-szoftver egység több különböző *Időbélyegző egység*et is kiszolgálhat a fenti követelmények betartása esetén.

3.10. Az Időbélyegző szolgáltatás elérési módjai

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

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

4. A tanúsítványok életciklusára vonatkozó követelmények

4.1. A kulcspár és a tanúsítvány használata

4.1.1. A magánkulcs és a tanúsítvány használata

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

4.1.2. Az Érintett felek nyilvános kulcs és tanúsítvány használata

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

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

Amennyiben az *Érintett fél* nem az ott leírtaknak megfelelően jár el, az ebből eredő károkért az *Időbélyegzés-szolgáltató* nem vállal felelősséget.

5. Elhelyezési, eljárásbeli és üzemeltetési előírások

Az *Időbélyegzés-szolgáltató*nak széles körben elismert szabványoknak megfelelő fizikai, eljárásbeli és személyzeti biztonsági óvintézkedéseket, valamint az ezeket érvényre juttató adminisztratív és irányítási eljárásokat kell alkalmaznia.

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

Az *Időbélyegzés-szolgáltató*nak figyelemmel kell kísérnie a kapacitás igényeket és biztosítania kell, hogy megfelelő feldolgozási teljesítmény és tárolási kapacitás álljon rendelkezésre a szolgáltatás nyújtásához.

5.1. Fizikai követelmények

Az *Időbélyegzés-szolgáltató*nak gondoskodnia kell arról, hogy a kritikus szolgáltatásokhoz történő fizikai hozzáférés ellenőrzött legyen és a kritikus szolgáltatások eszközeit érintő fizikai kockázatát minimalizálja.

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

A kritikus és érzékeny információt feldolgozó szolgáltatásokat biztonságos helyszíneken kell megvalósítani.

A biztosított védelem mértéke legyen megfelelő az *Időbélyegzés-szolgáltató* által végzett kockázatelemzésben megállapított fenyegetettség mértékének.

5.1.1. A telephely elhelyezése és szerkezeti felépítése

Az *Időbélyegzés-szolgáltató* informatikai rendszereit fizikai és logikai védelemmel ellátott, megfelelően biztonságos *Adatközpont*ban kell elhelyezni és üzemeltetni, amely megakadályozza az illetéktelen hozzáférést. Az *Adatközpont* elhelyezése és kialakítása során egymásra épülő és egymást támogató védelmi megoldásokat kell alkalmazni – mint pl. őrzés, biztonsági zárak, behatolás érzékelők, video megfigyelő rendszer, beléptető rendszer stb. – amelyek együttesen egy erős védelmi szintet biztosítanak a szolgáltatásban részt vevő informatikai rendszerek és a szolgáltató által tárolt bizalmas adatok megóvására.

5.1.2. Fizikai hozzáférés

Az *Időbélyegzés-szolgáltató*nak védenie kell a szolgáltatás nyújtásában részt vevő eszközeit és berendezéseit a jogosulatlan fizikai hozzáféréstől az eszközök manipulálásának megakadályozása érdekében. Az *Időbélyegzés-szolgáltató*nak biztosítania kell, hogy:

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

- az önálló jogosultsággal nem rendelkező személyek csak indokolt esetben, a szükséges ideig tartózkodhatnak a gépteremben megfelelő jogosultságú kísérő személyzettel;
- a belépési logokat folyamatosan archiválják és legalább hetente megvizsgálják.

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

Jogosulatlan személyek jelenlétében:

- a bizalmas adatokat tartalmazó adathordozókat fizikailag elzárva kell tartani;
- a bejelentkezett terminálokat nem szabad felügyelet nélkül hagyni;
- nem szabad olyan munkafolyamatot végezni, amely során bizalmas adat felfedésre kerülhet.

A gépterem elhagyásakor az adminisztrátornak ellenőriznie kell, hogy:

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

A fizikai biztonsági vizsgálatok rendszeres elvégzésére felelősöket kell kijelölni. A vizsgálatok eredményét megfelelő naplóbejegyzésekben kell rögzíteni.

5.1.3. Áramellátás és légkondicionálás

Az *Időbélyegzés-szolgáltató Adatközpont*jában olyan szünetmentes áramellátó rendszert kell alkalmazni, amely:

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

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

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

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

5.1.4. Beázás és elárasztódás veszély kezelése

Az *Időbélyegzés-szolgáltató Adatközpont*ját megfelelően védeni kell a vízbetöréstől és az elárasztódástól.

5.1.5. Tűz megelőzés és tűzvédelem

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

A gépteremben automatikus tűzoltó rendszert kell alkalmazni.

5.1.6. Adathordozók tárolása

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

5.1.7. Hulladék megsemmisítése

Az *Időbélyegzés-szolgáltató*nak a környezetvédelmi előírások betartásával kell gondoskodnia feleslegessé vált eszközeinek, adathordozóinak megsemmisítéséről.

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

5.1.8. A mentési példányok fizikai elkülönítése

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

5.2. Eljárásbeli előírások

Az *Időbélyegzés-szolgáltató*nak gondoskodnia kell arról, hogy rendszereit biztonságosan, szabályszerűen, a meghibásodás minimális kockázata mellett üzemeltesse.

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

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

5.2.1. Bizalmi szerepkörök

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

A megvalósítandó bizalmi szerepkörök:

- a szolgáltató informatikai rendszeréért általánosan felelős vezető;
- biztonsági tisztviselő: a szolgáltatás biztonságáért általánosan felelős személy;
- rendszeradminisztrátor: az informatikai rendszer telepítését, konfigurálását, karbantartását végző személy;
- rendszerüzemeltető: az informatikai rendszer folyamatos üzemeltetését, mentését és helyreállítását végző személy;

- független rendszervizsgáló: a szolgáltató naplózott, illetve archivált adatállományát vizsgáló, a szolgáltató által a szabályszerű működés érdekében megvalósított kontroll intézkedések betartásának ellenőrzéséért, a meglévő eljárások folyamatos vizsgálatáért és monitorozásáért felelős személy;

A bizalmi szerepkörök ellátására az *Időbélyegzés-szolgáltató* biztonságért felelős vezetőjének formálisan ki kell nevezni az *Időbélyegzés-szolgáltató* munkatársait.

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

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

5.2.2. Az egyes feladatok ellátásához szükséges személyzeti létszámok

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

- az *Időbélyegzés-szolgáltató* saját szolgáltatói kulcspárjának generálása;
- a szolgáltatói magánkulcs mentése;
- a szolgáltatói magánkulcs aktiválása;
- a szolgáltatói magánkulcs megsemmisítése.

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

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

5.2.3. Az egyes szerepkörökben elvárt azonosítás és hitelesítés

Az *Időbélyegzés-szolgáltató* informatikai rendszerét kezelő felhasználóknak egyedi azonosító adatokkal kell rendelkezniük, amely lehetővé teszi a felhasználók biztonságos azonosítását és hitelesítését.

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

Az azonosító és hitelesítő adatokat a felhasználói jogosultságok megszűnésekor haladéktalanul vissza kell vonni.

5.2.4. Egymást kizáró szerepkörök

Az *Időbélyegzés-szolgáltató* munkatársai egyidejűleg több bizalmi szerepkört is betölthetnek, de az *Időbélyegzés-szolgáltató* köteles biztosítani, hogy:

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

5.3. Személyzetre vonatkozó előírások

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

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

Az *Időbélyegzés-szolgáltató* egyúttal biztosítsa valamennyi munkakör betöltéséhez a szükséges közös, általános, illetve az egyes szerepkörök betöltéséhez szükséges speciális szakmai ismeretek megszerzését, illetve továbbfejlesztését.

5.3.1. Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

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

Az *Időbélyegzés-szolgáltató*nál bizalmi szerepkört csak olyan személy tölthet be, akinek a befolyásmentességét és szakértelmét az *Időbélyegzés-szolgáltató* igazolni tudja.

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

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

5.3.2. Előélet vizsgálatára vonatkozó eljárások

Az *Időbélyegzés-szolgáltató* vezető munkakörben illetve bizalmi szerepkörben csak olyan alkalmazottakat foglalkoztathat, akik:

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

Kinevezéskor az *Időbélyegzés-szolgáltató* vezető munkakört betöltő alkalmazottjának nyilatkozatával, bizalmi szerepkört betöltő alkalmazottjának 3 hónapnál nem régebbi erkölcsi bizonyítvánnyal kell igazolnia büntetlen előéletét.

Az *Időbélyegzés-szolgáltató*nak a felvételi eljárás során ellenőriznie kell a jelentkező önéletrajzában megadott releváns információk valódiságát.

5.3.3. Képzési követelmények

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

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

Az *Időbélyegzés-szolgáltató* éles informatikai rendszereihez csak a képzést sikeresen teljesítő alkalmazottak kaphatnak hozzáférési jogosultságot.

5.3.4. Továbbképzési gyakoriságok és követelmények

Az *Időbélyegzés-szolgáltató*nak gondoskodnia kell róla, hogy az alkalmazottak folyamatosan a megfelelő tudással rendelkezzenek, így szükség esetén továbbképzést, vagy ismétlő jellegű képzést kell tartani.

Továbbképzést kell tartani, ha az *Időbélyegzés-szolgáltató* folyamataiban vagy informatikai rendszerében változás áll be.

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

5.3.5. Munkabeosztás körforgásának sorrendje és gyakorisága

Nincs előírás.

5.3.6. Felhatalmazás nélküli tevékenységek büntető következményei

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

5.3.7. Szerződéses viszonyban foglalkoztatottakra vonatkozó követelmények

Az *Időbélyegzés-szolgáltató* által szerződéses viszonyban foglalkoztatott dolgozókra ugyanolyan szabályokat kell alkalmazni, mint a munkavállalókra.

A bizalmi szerepkört betöltő személynek munkaviszonyban kell állnia az *Időbélyegzés-szolgáltató*val.

5.3.8. A személyzet számára biztosított dokumentációk

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

5.4. Naplózási eljárások

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

5.4.1. A tárolt események típusai

Az *Időbélyegzés-szolgáltató*nak az általánosan elfogadott informatikai biztonsági gyakorlatnak megfelelően naplóznia kell minden olyan biztonsággal kapcsolatos eseményt, amely információt szolgáltathat az informatikai rendszerben vagy annak fizikai környezetében történt eseményekről, változásokról. Minden naplóbejegyzésnél el kell tárolni:

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

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

Naplózni kell minimálisan az alábbi eseményeket:

- IDŐBÉLYEGZÉS
  - az *Időbélyegző*k kibocsátásával kapcsolatos események;
  - az óra szinkronizációja az UTC időhöz, beleértve az üzemszerű újrakalibrálásokat is;
  - a szinkronizáció elvesztése;
- NAPLÓZÁS
  - a naplózó rendszer vagy egyes komponenseinek leállítása, újraindítása;
  - a naplózás bármilyen beállításának módosítása, mint pl. gyakoriság, riasztási küszöb érték, vizsgált esemény;
  - a tárolt naplózási adatok módosítása vagy törlése;
  - a naplózó rendszer hibája miatt végzett tevékenységek;
- RENDSZER BEJELENTKEZÉSEK
  - sikeres bejelentkezések, sikertelen bejelentkezési próbálkozások bizalmi szerepkörökbe;
  - jelszó alapú azonosítás esetén:
    - az engedélyezett sikertelen bejelentkezési próbálkozások számának megváltoztatása;
    - az engedélyezett sikertelen bejelentkezési próbálkozások számának elérése felhasználói bejelentkezéskor;

    - sikertelen bejelentkezések miatt zárolt felhasználó újbóli engedélyezése;
  - az azonosítási technika változtatása (például jelszó alapúról PKI alapúra);

- KULCSKEZELÉS
  - a szolgáltatói kulcsok teljes életciklusára vonatkozó valamennyi esemény (kulcsgenerálás, betöltés, elmentés stb.);

- TANÚSÍTVÁNY KEZELÉS
  - szolgáltatói *Tanúsítvány*ok kibocsátásával, állapotváltozásával kapcsolatos minden esemény;
  - az *Időbélyegző egység*ek *Tanúsítvány*ainak kibocsátásával, állapotváltozásával kapcsolatos minden esemény;

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

- CA KONFIGURÁCIÓ
  - a CA tetszőleges komponensének átparaméterezése, a beállításon történt bármilyen változtatás;
  - felhasználók felvétele, törlése;
  - felhasználói szerepkörök, jogosultságok megváltoztatása;
  - a tanúsítvány profil megváltoztatása;
  - CRL profil megváltoztatása;
  - új CRL lista előállítása;
  - OCSP válasz generálása;
  - *Időbélyegző* generálása;
  - az előírt időpontossági küszöb túllépése;

- HSM
  - HSM installálása;
  - HSM eltávolítása;
  - HSM selejtezése, megsemmisítése;

  - HSM szállítása;
  - HSM tartalmának törlése (nullázás);
  - HSM feltöltése kulcsokkal, tanúsítványokkal;

- KONFIGURÁCIÓ VÁLTOZÁSA
  - hardver;
  - szoftver;
  - operációs rendszer;
  - javító csomag;

- FIZIKAI HOZZÁFÉRÉS, TELEPHELY BIZTONSÁG
  - személy belépése a CA komponenseket tartalmazó biztonsági területre és onnan kilépése;
  - hozzáférés egy CA rendszer komponenshez;
  - a fizikai biztonság ismert vagy gyanított megsértése;
  - tűzfal és router forgalmak;

- MŰKÖDÉSI RENDELLENESSÉGEK
  - rendszerösszeomlás, hardver hiba;
  - szoftveres hibák;
  - szoftverintegritás ellenőrzési hiba;
  - hibás vagy rossz helyre továbbított üzenetek;
  - hálózatot ért támadások, támadási kísérletek;
  - berendezés hiba;
  - elektromos hálózati üzemzavar;
  - szünetmentes tápegység hiba;
  - lényeges hálózati szolgáltatás hozzáférési hiba;
  - a *Minősített időbélyegzési rend* vagy a *Minősített időbélyegzési szolgáltatási szabályzat* megsértése;
  - operációs rendszer órájának törlése;

- EGYÉB ESEMÉNYEK
  - személy kinevezése biztonsági szerepkörbe;
  - operációs rendszer telepítése;

- PKI alkalmazás telepítése;
- rendszer elindítása;
- belépési kísérlet a PKI alkalmazásba;
- jelszó módosítási, beállítási kísérlet;
- a belső adatbázis elmentése, visszaállítása mentésből;
- fájl műveletek (pl. létrehozás, átnevezés, áthelyezés);
- adatbázis hozzáférés.

5.4.2. A naplófájl feldolgozásának gyakorisága

Az *Időbélyegzés-szolgáltató*nak biztosítania kell a keletkezett naplóállományok rendszeres kiértékelését.

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

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

Az *Időbélyegzés-szolgáltató* használhat automatizált eszközöket az elektronikus naplóállományok kiértékelésének segítésére.

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

A kiértékelés során elemezni kell a rendszerek által generált hibaüzeneteket.

Statisztikai módszerekkel elemezni kell a forgalmi adatokban bekövetkezett jelentős változásokat.

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

5.4.3. A naplófájl megőrzési időtartama

Az online rendszerből való kitörlés előtt a naplóállományokat archiválni kell és gondoskodni kell azok biztonságos megőrzéséről az 5.5.2 fejezetben meghatározott ideig.

5.4.4. A naplófájl védelme

Az *Időbélyegzés-szolgáltató*nak meg kell védenie a keletkezett naplóállományokat az előírt megőrzési ideig. A megőrzési idő teljes időtartama alatt biztosítania kell a naplóadatok:

- védelmét az illetéktelen felfedés ellen: a naplóállományokhoz csak az arra jogosultak – elsősorban a független rendszervizsgálók – férhessenek hozzá;

- rendelkezésre állását: a jogosultak számára biztosítani kell a naplóállományokhoz való hozzáférést;
- integritását: meg kell akadályozni a naplóállományokban bármilyen adat módosítását, törlését, bejegyzések sorrendjének megváltoztatását stb.

5.4.5. A naplófájl mentési eljárásai

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

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

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

5.4.6. A naplózás adatgyűjtési rendszere

Az *Időbélyegzés-szolgáltató* a *Minősített időbélyegzési szolgáltatási szabályzat*ában írja elő a naplózási folyamatainak működését.

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

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

5.4.7. Az eseményeket kiváltó alanyok értesítése

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

5.4.8. Sebezhetőség felmérése

Az *Időbélyegzés-szolgáltató*nak évente sebezhetőség vizsgálatot kell végeznie, amely segítségével feltérképezi a potenciális belső és külső fenyegetettségeket, amelyek jogosulatlan hozzáféréseket eredményezhetnek.

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

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

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

5.5. Adatok archiválása

5.5.1. Az archivált adatok típusai

Az *Időbélyegzés-szolgáltató*nak fel kell készülnie elektronikus és papíralapú dokumentumok megfelelően biztonságos, hosszú idejű archiválására.

Az *Időbélyegzés-szolgáltató*nak az alábbi jellegű információt kell archiválnia:

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

5.5.2. Az archívum megőrzési időtartama

Az *Időbélyegzés-szolgáltató* az archivált adatokat az alábbi időtartamokig köteles megőrizni:

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

5.5.3. Az archívum védelme

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

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

Az archivált adatok megőrzése során gondoskodni kell az archivált adatok

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

- hitelességének megőrzéséről.

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

5.5.4. Az archívum mentési folyamatai

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

5.5.5. Az adatok időbélyegzésére vonatkozó követelmények

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

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

A napi naplóállományokat minősített *Időbélyegző*vel kell ellátni.

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

5.5.6. Az archívum gyűjtési rendszere

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

5.5.7. Archív információk hozzáférését és ellenőrzését végző eljárások

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

Az archivált adatállományokat védeni kell a jogosulatlan hozzáféréstől.

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

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

5.6. Szolgáltatói kulcs cseréje

Az *Időbélyegzés-szolgáltató* gondoskodjon arról, hogy az általa üzemeltetett *Időbélyegző egység*ek folyamatosan rendelkezzenek a működéshez szükséges érvényes kulccsal és Tanúsítvánnyal. Ennek érdekében a *Tanúsítvány*uk lejárta illetve a hozzájuk kapcsolódó kulcsok használati idejének lejárta előtt elegendő idővel generáljon új kulcspárt az *Időbélyegző egység* számára, és arról időben értesítse *Ügyfel*eit. Az új szolgáltatói kulcsot a jelen szabályzatnak megfelelően kell generálni és kezelni.

Amennyiben az *Időbélyegzés-szolgáltató* megváltoztatja az *Időbélyegző*ket kibocsátó bármely szolgáltatói *Tanúsítvány*ának kulcsait, be kell tartania az alábbi előírásokat:

- publikálnia kell az érintett *Tanúsítvány*ait és nyilvános kulcsait a 2.2 fejezetben meghatározott előírásoknak megfelelően;
- a szolgáltatói kulcscsere után a kibocsátandó *Időbélyegző*ket már csak az új szolgáltatói kulcsok felhasználásával írhatja alá;
- meg kell őriznie a régi szolgáltatói *Tanúsítvány*okat és nyilvános kulcsokat.

5.7. Kompromittálódást és katasztrófát követő helyreállítás

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

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

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

5.7.1. Váratlan esemény és kompromittálódás kezelési eljárások

Az *Időbélyegzés-szolgáltató*nak rendelkeznie kell üzletmenet folytonossági tervvel. Az üzletmenet folytonossági tervnek tartalmaznia kell az aláíró kulcs kompromittálódása, a kompromittálódás gyanúja és az *Időbélyegző egység* órájának elállítódása esetén követendő eljárásokat.

Kompromittálódás, kompromittálódás gyanúja vagy az *Időbélyegző egység* órájának elállítódása esetén az *Időbélyegzés-szolgáltató*nak közzé kell tennie az eseménnyel kapcsolatos információt valamint nem adhat ki *Időbélyegző*ket a veszélyhelyzet elhárításáig.

Kompromittálódás, kompromittálódás gyanúja vagy az *Időbélyegző egység* órájának elállítódása esetén az *Időbélyegzés-szolgáltató*nak közzé kell tennie az érintett *Időbélyegző*k beazonosításához szükséges információkat.

Az *Időbélyegzés-szolgáltató*nak ki kell alakítania és fenn kell tartania egy teljes értékű tartalékrendszert, amely az elsődleges helyszíntől biztonságos távolságra, földrajzilag különböző helyszínen található és önállóan is alkalmas a szolgáltatások teljes körű ellátására.

Az *Időbélyegzés-szolgáltató*nak rendszeresen tesztelnie kell a tartalékrendszer működését és évente felül kell vizsgálnia az üzletmenet folytonossági terveit.

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

5.7.2. Meghibásodott IT erőforrások, szoftverek és/vagy adatok

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

Az *Időbélyegzés-szolgáltató* naponta készítsen teljes mentést az adatbázisairól és a keletkezett naplózási eseményekről.

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

Az *Időbélyegzés-szolgáltató* üzletmenet folytonossági terve tartalmazzon pontos előírásokat a kritikus rendszerkomponensek meghibásodásának esetén végrehajtandó feladatokra.

Az *Időbélyegzés-szolgáltató* a hiba elhárítása és a rendszer integritásának helyreállítása után a lehető leghamarabb indítsa újra a szolgáltatásait.

5.7.3. Magánkulcs kompromittálódása esetén követendő eljárások

Az *Időbélyegzés-szolgáltató* magánkulcsának kompromittálódása vagy a kompromittálódás gyanúja esetén haladéktalanul meg kell tenni az alábbi lépéseket:

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

5.7.4. Működés folyamatosságának biztosítása katasztrófát követően

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

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

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

Az *Időbélyegzés-szolgáltató* a lehető legrövidebb időn belül köteles értesíteni az érintett felhasználókat a katasztrófa bekövetkezéséről.

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

5.8. Az Időbélyegzés-szolgáltató leállítása

Az *Időbélyegzés-szolgáltató*nak a szolgáltatás megszüntetésekor teljesítenie kell a jogszabályokban megfogalmazott követelményeket.

A leállítás során kiemelten kezelendő feladatok:

- a tervezett leállásról időben értesíteni kell az *Érintett felek*et és az *Előfizető*ket;
- az *Időbélyegzés-szolgáltató* tegyen meg mindent annak érdekében, hogy legkésőbb a szolgáltatás leállításáig egy másik szolgáltató átvegye nyilvántartásait és szolgáltatási kötelezettségeit;
- be kell szüntetni az új *Időbélyegző*k kiadását;
- vissza kell vonni a szolgáltatói *Tanúsítvány*okat és meg kell semmisíteni a szolgáltatói magánkulcsokat;
- a szolgáltatás megszüntetése után egy teljes rendszermentést és archiválást kell végeznie;
- át kell adni az archivált adatokat a szolgáltatást átvállaló szolgáltatónak vagy a Nemzeti Média- és Hírközlési Hatóságnak.

6. Műszaki biztonsági óvintézkedések

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

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

6.1. Kulcspár előállítása és telepítése

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

6.1.1. Kulcspár előállítása

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

- ETSI TS 119 312 [16];
- az Eüt. [4] 92. § (1) b) pontja szerinti aktuális Nemzeti Média- és Hírközlési Hatóság által kiadott algoritmusokkal kapcsolatos határozat.

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

- A szolgáltatói magánkulcs előállítását fizikailag védett környezetben (lásd 5.1 pont), két, bizalmi szerepkört (lásd 5.2.1 pont) betöltő, erre feljogosított személy együttes részvételével, más illetéktelen személyek jelenlétét kizárva végzi.
- A szolgáltatói magánkulcs előállítását olyan eszközön belül hajtja végre, amely:
  - megfelel az ISO/IEC 19790 [18] követelményeinek, vagy
  - megfelel a FIPS 140-2 [24] 3-as, illetve annál magasabb szintű követelményeinek, vagy
  - megfelel a CEN 14167-2 [25] munkacsoport egyezmény követelményeinek, vagy
  - olyan megbízható rendszer, amely az MSZ/ISO/IEC 15408 [17] szerint, illetve azzal egyenértékű biztonsági kritériumok szerint EAL 4-es vagy magasabb értékelési garancia szinten van értékelve. Az értékelésnek a jelen dokumentum követelményeinek megfelelő biztonsági rendszerterven, vagy biztonsági előirányzaton kell alapulnia.
- A szolgáltatói magánkulcs előállítását egy kulcsgenerálási forgatókönyv alapján végzi.

6.1.2. Kulcsméretek

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

- ETSI TS 119 312 [16];
- az Eüt. [4] 92. § (1) b) pontja szerinti aktuális Nemzeti Média- és Hírközlési Hatóság által kiadott algoritmusokkal kapcsolatos határozat.

6.1.3. A nyilvános kulcs paraméterek előállítása, a minőség ellenőrzése

A kulcsparaméterek előállítására vonatkozó követelményeket a 6.1.1. fejezet tartalmazza.

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

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

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

6.2. A magánkulcsok védelme

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

A *Hardver kriptográfiai eszköz*ök kezelése során a használatból kivont *Hardver kriptográfiai eszköz*ökben tárolt aláíró magánkulcsokat olyan módon kell törölni, hogy ne legyen lehetséges a kulcsok visszaállítása.

6.2.1. Kriptográfiai modulra vonatkozó szabványok és előírások

Az *Időbélyegzés-szolgáltató* *Időbélyegző*ket kibocsátó rendszerei az elektronikus aláírás vagy bélyegző létrehozásához használt magánkulcsokat olyan biztonságos hardver eszközökben kell tárolják, amelyek:

- megfelelnek az ISO/IEC 19790 [18] követelményeinek,
- vagy megfelelnek a FIPS 140-2 [24] 3-as, illetve annál magasabb szintű követelményeknek,

- vagy megfelelnek a CEN 14167-2 [25] munkacsoport egyezmény követelményeinek,
- vagy olyan megbízható rendszerek, amely az MSZ/ISO/IEC 15408 [17] szerint, illetve azzal egyenértékű biztonsági kritériumok szerint 4-es vagy magasabb értékelési garancia szinten vannak értékelve. Az értékelésnek a jelen dokumentum követelményeinek megfelelő biztonsági rendszerterven, vagy biztonsági előirányzaton kell alapulnia.

A szolgáltatói magánkulcsok a *Hardver kriptográfiai eszköz*ön kívül csak kódolt formában tárolhatók. A kódoláshoz csak az Eüt. [4] 92. § (1) b) pontja szerinti aktuális Nemzeti Média- és Hírközlési Hatóság által kiadott algoritmusokkal kapcsolatos határozatban foglalt algoritmusok és kulcsparaméterek használhatók, amelyek várhatóan a kulcs teljes élettartama alatt képesek ellenállni a kriptográfiai támadásoknak.

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

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

6.2.2. Magánkulcs többszereplős (n-ből m) használata

Az *Időbélyegzés-szolgáltató*nak biztosítania kell, hogy a szolgáltatói magánkulcsaival végzett kritikus műveletek végrehajtásához legalább kettő, bizalmi szerepkört betöltő munkatárs egyidejű jelenlétére legyen szükség.

6.2.3. Magánkulcs letétbe helyezése

Az *Időbélyegzés-szolgáltató* nem helyezheti letétbe a szolgáltatói aláíró magánkulcsait.

6.2.4. Magánkulcs mentése

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

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

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

6.2.5. Magánkulcs archiválása

Az *Időbélyegzés-szolgáltató* nem archiválhatja magánkulcsait.

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

Az *Időbélyegzés-szolgáltató* valamennyi szolgáltatói magánkulcsát a követelményeknek megfelelő *Hardver kriptográfiai eszköz*ben kell előállítani. A magánkulcsok nem létezhetnek nyílt formában a *Hardver kriptográfiai eszköz*ön kívül.

Az *Időbélyegzés-szolgáltató* a magánkulcsot csak biztonsági másolat készítése céljából exportálhatja a *Hardver kriptográfiai eszköz*ből.

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

6.2.7. Magánkulcs tárolása hardver kriptográfiai eszközben

Az *Időbélyegzés-szolgáltató*nak a jelen *Minősített időbélyegzési rend*ek szerinti szolgáltatás nyújtásához használt magánkulcsait kriptográfiai modulban kell tartania.

A *Hardver kriptográfiai eszköz*ön belüli tárolási formára vonatkozóan nincs előírás.

6.2.8. A magánkulcs aktiválásának módja

Az *Időbélyegzés-szolgáltató* szolgáltatói magánkulcsait a felhasznált *Hardver kriptográfiai eszköz* felhasználói útmutatójában és a tanúsítási dokumentumokban megfogalmazott eljárásoknak, követelményeknek megfelelően kell aktiválni.

6.2.9. A magánkulcs deaktiválásának módja

Az *Időbélyegzés-szolgáltató* szolgáltatói magánkulcsait a felhasznált *Hardver kriptográfiai eszköz* felhasználói útmutatójában és a tanúsítási dokumentumokban megfogalmazott eljárásoknak, követelményeknek megfelelően kell deaktiválni.

6.2.10. A magánkulcs megsemmisítésének módja

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

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

6.2.11. A hardver kriptográfiai eszközök értékelése

A 6.2.1 fejezet előírásaival összhangban az *Időbélyegzés-szolgáltató* valamennyi szolgáltatói magánkulcsát olyan *Hardver kriptográfiai eszköz*ben kell tárolni, amely:

- rendelkezik ISO/IEC 19790 [18] szerinti tanúsítással,
- vagy rendelkezik FIPS 140-2 Level 3 [24] szerinti tanúsítással,
- vagy rendelkezik a CEN 14167-2 [25] munkacsoport egyezmény követelményeinek való megfelelést igazoló Common Criteria alapú tanúsítvánnyal,
- vagy rendelkezik a Nemzeti Média- és Hírközlési Hatóság által vagy az Európai Unió valamely tagállamában nyilvántartásba vett, elektronikus aláírási termékek értékelésére jogosult független tanúsító szervezet által erre a célra kiadott igazolással.

6.3. A kulcspár kezelés egyéb szempontjai

6.3.1. A tanúsítványok és kulcspárok használatának periódusa

Az Időbélyegző egységek tanúsítványai

Az *Időbélyegzés-szolgáltató* által üzemeltetett *Időbélyegző egység*ek *Tanúsítvány*ainak érvényességi ideje:

- legfeljebb a kibocsátástól számított 12 év;
- nem haladhatja meg azt az időt, amely időpontig a felhasznált kriptográfiai algoritmusok a Nemzeti Média- és Hírközlési Hatóság algoritmusokkal kapcsolatos határozata szerint biztonságosan felhasználhatók;
- nem haladhatja meg a *Tanúsítvány*t kibocsátó szolgáltatói *Tanúsítvány* érvényességi idejét.

Az *Időbélyegzés-szolgáltató* minden év első negyedévében adjon ki új magánkulcso(ka)t és *Tanúsítvány*(oka)t az *Időbélyegző egység*ei számára. Az új *Időbélyegző egység Tanúsítvány*(ok) használatba vétele után a korábbi magánkulcso(ka)t meg kell semmisíteni.

Az Időbélyegző kulcsok életciklusa

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

- az *Időbélyegzés-szolgáltató*nak meg kell határoznia az *Időbélyegző egység*ekben használt magánkulcsok érvényességének végét;

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

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

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

6.4. Aktivizáló adatok

6.4.1. Aktivizáló adatok előállítása és telepítése

Az *Időbélyegzés-szolgáltató* a felhasznált *Hardver kriptográfiai eszköz* felhasználói útmutatójában és az eszköz tanúsítványban megfogalmazott eljárásoknak, követelményeknek megfelelő aktiváló módszereket kell alkalmazzon szolgáltatói magánkulcsainak védelmére.

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

6.4.2. Az aktivizáló adatok védelme

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

6.4.3. Az aktivizáló adatok kezelésének egyéb szempontjai

Nincs megkötés.

6.5. Informatikai biztonsági előírások

6.5.1. Speciális informatikai biztonsági műszaki követelmények

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

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

6.5.2. Az informatikai biztonság értékelése

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

6.6. Életciklusra vonatkozó műszaki előírások

6.6.1. Rendszerfejlesztési előírások

Az *Időbélyegzés-szolgáltató* az éles szolgáltatást nyújtó informatikai rendszereiben csak olyan eszközöket, alkalmazásokat használhat, amelyek:

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

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

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

Az *Időbélyegzés-szolgáltató* megfelelő védelmi intézkedésekkel megakadályozza, hogy kártékony szoftver kerülhessen a hitelesítés-szolgáltatás nyújtása körében használt eszközökbe.

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

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

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

Az *Időbélyegzés-szolgáltató* csak a szolgáltatás nyújtásához szükséges szoftvereket telepítheti a szolgáltatást nyújtó informatikai berendezéseire.

Az *Időbélyegzés-szolgáltató*nak rendelkeznie kell egy változáskövető rendszerrel, amelyben minden változást dokumentálni kell.

Az *Időbélyegzés-szolgáltató* alkalmazzon eljárásokat a jogosulatlan változások észlelésére.

6.6.2. Biztonságkezelési előírások

Az *Időbélyegzés-szolgáltató* alkalmazzon eljárásokat a szolgáltatásban használt rendszerek telepítésének, konfigurációjának dokumentálására, üzemeltetésére, ellenőrzésére, monitorozására és karbantartására, beleértve a módosításokat és továbbfejlesztéseket is. A változáskövető rendszernek észlelnie kell a rendszerben történt bármilyen jogosulatlan változtatást, adatbevitelt, amely érinti a szolgáltatásban használt rendszert, a tűzfalakat, routereket, programokat és egyéb komponenseket. A szolgáltatásban használt program telepítésekor az *Időbélyegzés-szolgáltató* győződjön meg róla, hogy a telepítendő program a megfelelő verziójú és mentes mindenféle jogosulatlan módosítástól. Az *Időbélyegzés-szolgáltató* ellenőrizze rendszeresen a szolgáltatói rendszereiben használt programok integritását.

6.6.3. Életciklusra vonatkozó biztonsági előírások

Az *Időbélyegzés-szolgáltató*nak gondoskodnia kell a felhasznált *Hardver kriptográfiai eszköz*ök védelméről azok teljes életciklusa alatt.

- Megfelelő tanúsítással rendelkező *Hardver kriptográfiai eszköz*t kell használnia.
- A *Hardver kriptográfiai eszköz* átvételekor meg kell róla győződni, hogy a szállítás során biztosították a *Hardver kriptográfiai eszköz*ök feltörés elleni védelmét.
- A tárolás során biztosítani kell a *Hardver kriptográfiai eszköz*ök feltörés elleni védelmét.

- Az üzemeltetés során folyamatosan be kell tartani a *Hardver kriptográfiai eszköz* biztonsági előirányzatában, használati útmutatójában és a tanúsítási jelentésben szereplő követelményeket.
- A használatból kivont *Hardver kriptográfiai eszköz*ökben tárolt magánkulcsokat olyan módon kell törölni, hogy lehetetlenné váljon a kulcsok visszaállítása.

6.7. Hálózati biztonsági előírások

Az *Időbélyegzés-szolgáltató* tartsa szigorú ellenőrzés alatt az alkalmazott IT rendszereinek konfigurációját, dokumentáljon minden változást, beleértve a legkisebb módosítást, fejlesztést, szoftverfrissítést is. Az *Időbélyegzés-szolgáltató* vezessen be megfelelő eljárásokat az IT rendszereiben bekövetkezett tetszőleges hardver vagy szoftver változás észlelésére, a rendszer telepítésére, karbantartására. Az *Időbélyegzés-szolgáltató* ellenőrizze minden szoftverkomponens első betöltésekor a komponens eredetiségét, integritását.
Az *Időbélyegzés-szolgáltató* alkalmazzon megfelelő hálózatbiztonsági intézkedéseket, mint például

- tiltsa le a használaton kívüli hálózati portokat és szolgáltatásokat;
- csak az IT rendszer megfelelő működéséhez feltétlenül szükséges hálózati alkalmazásokat futtasson.

6.8. Időbélyegzés

Az *Időbélyegzés-szolgáltató*nak valamely Európai Úniós tagállam bizalmi listáján szereplő minősített időbélyegzés-szolgáltató által biztosított *Időbélyegző*ket kell használnia a naplóbejegyzések és egyéb archiválandó elektronikus állományok hitelesítésére.

7. Tanúsítvány, CRL és OCSP profilok

7.1. Tanúsítvány profil

Az *Időbélyegzés-szolgáltató* által használt *Időbélyegző egység Tanúsítvány*ok illetve a szolgáltatás során használt szolgáltatói (gyökér és köztes) hitelesítő egységek *Tanúsítvány*ai feleljenek meg az alábbi ajánlásoknak, specifikációknak:

- ITU X.509 Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks [22];
- RFC 5280 [20];
- RFC 6818 [21];

- ETSI EN 319 412-1 [10];
- ETSI EN 319 412-2 [11] természetes személyek számára kibocsátott *Tanúsítvány*ok esetén;
- ETSI EN 319 412-3 [12] nem természetes személyek számára kibocsátott *Tanúsítvány*ok esetén;
- ETSI EN 319 412-5 [13].

7.1.1. Verzió szám(ok)

Az *Időbélyegzés-szolgáltató* által használt szolgáltatói (gyökér és köztes) hitelesítő egységek *Tanúsítvány*ai és az *Időbélyegzés-szolgáltató* által használt *Időbélyegző egység Tanúsítvány*ok legyenek az X.509 specifikáció [22] szerinti "v3" *Tanúsítvány*ok.

Az *Időbélyegzés-szolgáltató* által használt szolgáltatói (gyökér és köztes) hitelesítő egységek *Tanúsítvány*ai és az *Időbélyegzés-szolgáltató* által használt *Időbélyegző egység Tanúsítvány*ok alapmezői a következők:

- Verzió (Version)
  A *Tanúsítvány* az X.509 specifikáció [22] szerinti "v3" *Tanúsítvány*oknak felel meg, így a mezőbe a "2" érték kerül.
- Sorozatszám (Serial Number)
  A *Tanúsítvány*t kibocsátó hitelesítő egység által generált egyedi azonosító.

  A végfelhasználói *Tanúsítvány*ok esetében a "Serial Number" mezőnek legalább 8 bájt entrópiájú véletlen számot kell tartalmaznia.
- Algoritmus azonosító (Algorithm Identifier)
  A *Tanúsítvány*t hitelesítő elektronikus aláírás vagy bélyegző készítéséhez használt algoritmuskészlet azonosítója (OID).
- Aláírás (Signature)
  Az *Időbélyegzés-szolgáltató* által készített, a *Tanúsítvány*t hitelesítő elektronikus aláírás vagy bélyegző, amelyet az *Időbélyegzés-szolgáltató* az "Algoritmus azonosító" -ban megadott algoritmuskészlettel hozott létre.
- Kibocsátó (Issuer)
  A *Tanúsítvány*t kibocsátó *Hitelesítő egység* megkülönböztetett neve egyedi X.501 név formátum szerint.
- Érvényesség (Valid From & Valid To)
  A *Tanúsítvány* érvényességének kezdete és vége.

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

- Az *Alany* azonosítója (Subject)
  Az *Alany* megkülönböztetett neve egyedi X.501 név formátum szerint.
  Mindig kitöltésre kerül.
- Az *Alany* nyilvános kulcsának algoritmus-azonosítója (Subject Public Key Algorithm Identifier)
- Az *Alany* nyilvános kulcsa (Subject Public Key Value)
  Az *Alany* nyilvános kulcsa.
- Kibocsátó egyedi azonosító (Issuer Unique Identifier)
  Nem kitöltött.
- Az *Alany* egyedi azonosítója (Subject Unique Identifier)
  Nem kitöltött.

7.1.2. Tanúsítvány kiterjesztések

Az *Időbélyegzés-szolgáltató* az X.509 specifikáció [22] szerinti tanúsítvány kiterjesztéseket használhat, saját maga által definiált kritikus kiterjesztések használata nem megengedett.

A tanúsítvány kiterjesztéssel kapcsolatos konkrét előírások:

Időbélyegző egység tanúsítványa

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

  Használata kötelező.

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

Használata kötelező.

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

  Kitöltése opcionális.

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

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

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

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

  Az *Időbélyegző egység* számára kibocsátott *Tanúsítvány*okban kötelezően beállítandó és kizárólagosan megadandó érték: "nonRepudiation", "digitalSignature".

- Kulcshasználati időszak (PrivateKeyUsagePeriod) – nem kritikus
  OID: 2.5.29.16
  A magánkulcs engedélyezett használati időtartamának meghatározása.
  Használata opcionális. Amennyiben alkalmazásra kerül, a "notBefore" és "notAfter" értékek mindegyikét meg kell adni.

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

  Az *Időbélyegző egység* számára kibocsátott *Tanúsítvány*okban kötelezően beállítandó és kizárólagosan megadandó érték:

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

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

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

  - Az *Időbélyegzés-szolgáltató* a *Tanúsítvány*ok aktuális visszavonási állapotának gyors és pontos ellenőrizhetősége érdekében online tanúsítvány-állapot szolgáltatást kell nyújtson. Ennek elérhetőségét kell itt szerepeltetni.
  - A tanúsítványlánc felépítésének megkönnyítésére az *Időbélyegzés-szolgáltató* adja meg a *Tanúsítvány*t kibocsátó hitelesítési egység *Tanúsítvány*ának http protokollon keresztüli elérési helyét.

- Minősített tanúsítvánnyal kapcsolatos állítások (Qualified Certificate Statements) – nem kritikus
  OID: 1.3.6.1.5.5.7.1.3
  A mező a minősített *Tanúsítvány*okkal kapcsolatos állítások jelzésére szolgál. Az *Időbélyegző egység Tanúsítvány*ában szerepelniük kell a következő állításoknak:
  - a *Tanúsítvány* EU minősített *Tanúsítvány* – 'id-etsi-qcs 1' (10.4.0.1862.1.1);
  - a *Tanúsítvány*hoz kapcsolódó tranzakciós limit – más néven ügyleti érték vagy pénzügyi tranzakciós korlát – 'id-etsi-qcs 2' (0.4.0.1862.1.2);
  - azon kijelentés, hogy a Szolgáltató a *Tanúsítvány*hoz kapcsolódó regisztrációs adatokat a *Tanúsítvány* lejárta után 10 évig megőrzi – 'id-etsi-qcs 3' (0.4.0.1862.1.3);
  - az *Időbélyegző egység Tanúsítvány*ára vonatkozó Szolgáltatási szabályzat rövidített, kivonatolt változatát tartalmazó dokumentum elérhetősége – 'id-etsi-qcs 5' (0.4.0.1862.1.5);
  - annak jelzése, hogy a *Tanúsítvány* bélyegzés célra került kibocsátásra (a mező értéke 'id-etsi-qct-eseal')

Más tanúsítvány kiterjesztés nem kerülhet kitöltésre.

8. A megfelelőség vizsgálata

Az *Időbélyegzés-szolgáltató* tevékenységét az Európai Uniós szabályozással összhangban a Nemzeti Média- és Hírközlési Hatóság felügyeli. A Nemzeti Média- és Hírközlési Hatóság évente legalább egyszer átfogó helyszíni ellenőrzést tart az *Időbélyegzés-szolgáltató* telephelyén. A helyszíni ellenőrzés előtt az *Időbélyegzés-szolgáltató* köteles külső auditor igénybevételével átvilágíttatni üzemeltetését és az átvilágításról készült részletes megfelelőségértékelési jelentést annak kézhezvételétől számított három munkanapon belül a Nemzeti Média- és Hírközlési Hatóságnak benyújtani. Az átvizsgálás során azt kell megállapítani, hogy az *Időbélyegzés-szolgáltató* működése megfelel-e az eIDAS rendeletben [1] és a vonatkozó magyar jogszabályokban megállapított követelményeknek, valamint az alkalmazott *Minősített*

időbélyegzési rend(ek)ben és az ennek megfelelő *Minősített időbélyegzési szolgáltatási szabályzat*(ok)ban támasztott követelményeknek.

Az átvilágítás tematikája és módszertana feleljen meg az alábbi normatív dokumentumoknak:

- AZ EURÓPAI PARLAMENT ÉS A TANÁCS 910/2014/EU RENDELETE (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről [1];
- ETSI EN 319 403 V2.2.2 (2015-08) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers; [7]
- ETSI EN 319 401 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [6]
- ETSI EN 319 421 V1.1.1 (2016-03); Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps. [14]

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

A megfelelőségértékelési jelentés alapján kiállított megfelelőségi tanúsítványt közzé kell tenni az *Időbélyegzés-szolgáltató* honlapján.

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

8.1. Az ellenőrzések körülményei és gyakorisága

Az *Időbélyegzés-szolgáltató* évente köteles elvégeztetni a megfelelőségértékelő vizsgálatot.

8.2. Az auditor és szükséges képesítése

Az *Időbélyegzés-szolgáltató* a belső auditokat a független rendszervizsgáló szerepkörrel felruházott alkalmazottai segítségével is elvégezheti.

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

8.3. Az auditor és az auditált rendszerelem függetlensége

A külső auditot csak olyan személy végezheti:

- aki független a vizsgált *Időbélyegzés-szolgáltató* tulajdonosi körétől, vezetőségétől és üzemeltetésétől;
- aki független a vizsgált szervezettől, vagyis sem saját maga, sem közvetlen hozzátartozója nincs munkaviszonyban vagy üzleti kapcsolatban a *Időbélyegzés-szolgáltató*val;

8.4. Az auditálás által lefedett területek

Az átvizsgálásnak le kell fednie minimálisan az alábbi területeket:

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

8.5. A hiányosságok kezelése

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

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

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

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

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

8.6. Az eredmények közzététele

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

9. Egyéb üzleti és jogi kérdések

9.1. Díjak

Az *Időbélyegzés-szolgáltató* által alkalmazható díjakat a vonatkozó szabályozásnak megfelelően nyilvánosan elérhetővé kell tenni az *Előfizető*k részére.

9.1.1. Visszatérítési politika

Nincs megkötés.

9.2. Anyagi felelősségvállalás

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

9.2.1. Pénzügyi követelmények

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

- Az *Időbélyegzés-szolgáltató* legalább huszonötmillió forint összegű, feltétel nélküli és visszavonhatatlan bankgaranciával rendelkezik.

- Az *Időbélyegzés-szolgáltató* a Nemzeti Média- és Hírközlési Hatóság mint jogosult javára pénzügyi intézménynél óvadékot tesz le. Az óvadék összege legalább huszonötmillió forint.
- A költségek megfizetéséért hitelesítés-szolgáltató esetén legalább százmillió forint jegyzett tőkéjű európai uniós vállalkozás készfizető kezességet vállal. A kezességvállalás mértéke legalább huszonötmillió forintig terjed.

9.2.2. Felelősségbiztosítás

Az *Időbélyegzés-szolgáltató*nak megbízhatósága érdekében felelősségbiztosítással kell rendelkeznie.

9.3. Bizalmasság

Az *Időbélyegzés-szolgáltató*nak az *Ügyfel*ek adatait a jogszabályoknak megfelelően kell kezelnie.

9.3.1. Bizalmas információk köre

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

9.3.2. Bizalmas információk körén kívül eső adatok

Az *Időbélyegzés-szolgáltató* nyilvánosnak tekinthet miden olyan adatot, amely nem szerepel a bizalmas adatok felsorolásában a *Minősített időbélyegzési szolgáltatási szabályzat*ban.

9.3.3. Bizalmas információ védelme

Az *Időbélyegzés-szolgáltató* felelősséggel tartozik az általa kezelt bizalmas adatok védelméért.

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

Az *Időbélyegzés-szolgáltató Minősített időbélyegzési szolgáltatási szabályzat*ában tételesen meg kell határozni azon eseteket, amikor az *Időbélyegzés-szolgáltató* felfedheti a bizalmas adatokat.

9.4. Személyes adatok védelme

Az *Időbélyegzés-szolgáltató*nak gondoskodnia kell az általa kezelt személyes adatok védelméről. Működésének és szabályzatainak meg kell felelniük az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény [2] rendelkezéseinek.

Az *Időbélyegzés-szolgáltató* köteles az *Ügyfél*ről nyilvántartott személyes adatokat és információkat a jogszabályi előírásoknak megfelelően

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

9.4.1. Adatkezelési szabályzat

Az *Időbélyegzés-szolgáltató*nak rendelkeznie kell Adatkezelési szabályzattal, amely részletes előírásokat tartalmaz a személyes adatok kezelésére. Az Adatkezelési szabályzatot nyilvánosságra kell hozni az *Időbélyegzés-szolgáltató* honlapján.

9.4.2. Személyes adatok

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

Az *Időbélyegzés-szolgáltató* csak az *Előfizető*től közvetlenül, vagy annak egyértelmű előzetes hozzájárulásával gyűjthet személyes adatokat és csak olyan mértékben, ami a szolgáltatás nyújtásához szükséges.

9.4.3. Személyes adatnak nem minősülő adatok

Az *Időbélyegzés-szolgáltató* nem köteles bizalmasként kezelni az olyan személyes adatot, amely nyilvános adatforrásból elérhető.

9.4.4. Személyes adatok védelme

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

Az *Időbélyegzés-szolgáltató* általánosan felelős az Adatkezelési szabályzatában leírtak betartásáért, felelőssége kiterjed az alvállalkozói által végzett tevékenységekre is.

9.4.5. Személyes adatok felhasználása

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

9.4.6. Adatkezelés

Az *Időbélyegzés-szolgáltató* az *Ügyfél* értesítése nélkül is kiadhatja az *Ügyfél*ről tárolt személyes adatokat a vonatkozó jogszabályok által meghatározott esetekben.

9.4.7. Egyéb adatvédelmi követelmények

Nincs előírás.

9.5. Szellemi tulajdonjogok

Az *Időbélyegzés-szolgáltató* működése során nem sértheti meg harmadik személy szellemi tulajdonjogait.

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

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

Az *Időbélyegzés-szolgáltató* által a szolgáltatás igénybevételéhez biztosított szoftverek használatának szabályait a *Minősített időbélyegzési szolgáltatási szabályzat*ban kell meghatározni.

9.6. Tevékenységért viselt felelősség és helytállás

9.6.1. A szolgáltató felelőssége és helytállása

A Szolgáltató felelőssége

Az *Időbélyegzés-szolgáltató* felel a jelen *Minősített időbélyegzési rend*ben, a vonatkozó *Minősített időbélyegzési szolgáltatási szabályzat*ban valamint az *Ügyfél*lel kötött Szolgáltatási szerződésben megfogalmazott valamennyi rá vonatkozó kötelezettség maradéktalan betartásáért, különösen a következő esetekben:

- az *Időbélyegzés-szolgáltató* felelősséget vállal az általa támogatott *Minősített időbélyegzési rend*(ek)ben leírt eljárásoknak való megfelelésért;
- az *Időbélyegzés-szolgáltató* sajátjaként felel az alvállalkozói által a szolgáltatás nyújtása során okozott károkért;
- az *Időbélyegzés-szolgáltató* a vele szerződéses jogviszonyban álló *Ügyfel*ekkel szemben a Polgári Törvénykönyv [3] a szerződésszegésért való felelősség szabályai szerint felelős;

- az *Időbélyegzés-szolgáltató* a vele szerződéses jogviszonyban nem álló harmadik személlyel (ilyen az *Érintett fél*) szemben a Polgári Törvénykönyv [3] általános felelősségi szabálya szerint felelős;
- az *Időbélyegzés-szolgáltató* a felelősségi körén belül keletkezett, bizonyított károkért a szabályzataiban és az *Ügyfél*lel megkötött Szolgáltatási szerződésekben rögzített korlátozásokkal kártérítést fizet (lásd: Pénzügyi felelősség korlátozása 9.8. fejezet).

A Szolgáltató kötelezettségei az Előfizetővel szemben

Az *Időbélyegzés-szolgáltató* köteles:

- az *Előfizető*től érkező kérésre az ETSI EN 319 422 [15] specifikációnak megfelelő formátumú *Időbélyegző*t kibocsátani, amely a kérelemben szereplő lenyomatra vonatkozik és tartalmazza a kérelemben szereplő egyedi sorszámot;
- az *Időbélyegző* pontosságát 1 másodpercen belül tartani (az UTC-től való eltérés legfeljebb 1 másodperc lehet);
- a szolgáltatás megbízhatóságát és biztonságát a minősített időbélyegzés szolgáltatókra vonatkozó követelmények szerint biztosítani;
- naplózni a szolgáltatással kapcsolatos minden fontos eseményt, és e naplófájlokat a jogszabályi előírásoknak megfelelően megőrizni.

A Szolgáltató kötelezettsége

Az *Időbélyegzés-szolgáltató* köteles teljesíteni az eIDAS rendelet [1] 24. cikkének (2) bekezdésében foglalt követelményeket.

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

- a szolgáltatásnak megfelelő jogi-, szabályozási-, anyagi-, szerződéses stb. keretek megteremtése;
- magas színvonalú és biztonságos szolgáltatások nyújtása a vonatkozó szabályzatok szerint;
- a szolgáltatásokhoz kapcsolódó szervezetek (hitelesítő szervezet, ügyfélszolgálat stb.) folyamatos működtetése és ellenőrzése;

- a szabályzatokban előírt eljárások betartása és az esetleg bekövetkező helytelen működés elkerülése, illetve megszüntetése;
- a szolgáltatások biztosítása minden olyan igénylő számára, aki elfogadja a szabályzatokban rögzített feltételeket;
- a publikus nyilvántartások és saját szabályzatok karbantartása és folyamatos elérhetővé tétele bárki számára az interneten keresztül.

9.6.2. Az Ügyfél felelőssége és helytállása

Az *Előfizető* felelőssége

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

Az *Előfizető* kötelezettségei

Az *Előfizető* köteles az *Időbélyegzés-szolgáltató* szerződéses feltételeinek és szabályzatainak megfelelően eljárni a szolgáltatás igénybevétele során.
Az *Előfizető* kötelezettségeit a jelen *Minősített időbélyegzési rend*, a Szolgáltatási szerződés és annak mellékletei – különösen az Általános szerződési feltételek – és a *Minősített időbélyegzési szolgáltatási szabályzat* írja le.

9.6.3. Az Érintett fél felelőssége

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

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

9.6.4. Egyéb szereplők tevékenységéért viselt felelősség és helytállás

Nincs megkötés.

9.7. Helytállás érvénytelenségi köre

Az *Időbélyegzés-szolgáltató* kizárja felelősségét, amennyiben:

- az *Érintett fél* nem körültekintően jár el az *Időbélyegző*k felhasználása vagy ellenőrzése során, azaz nem a jelen *Minősített időbélyegzési rend*, a *Minősített időbélyegzési szolgáltatási szabályzat* vagy a hatályos jogszabályok szerint jár el;
- az *Érintett felek* vagy mások által kibocsátott szabályzatok nem felelnek meg a jelen *Minősített időbélyegzési rend*nek vagy a *Minősített időbélyegzési szolgáltatási szabályzat*nak;
- az Internet, vagy annak egy részének működési hibájából adódóan a tájékoztatás és egyéb kommunikációs kötelezettségeit nem tudja ellátni;
- a károkozás a Nemzeti Média- és Hírközlési Hatóság algoritmusokkal kapcsolatos határozat által elfogadott kriptográfiai algoritmusok hibájából, illetve gyengeségeiből ered.

9.8. A felelősség korlátozása

Az *Időbélyegzés-szolgáltató* korlátozhatja kártérítési felelősségét.

9.9. Kártérítési kötelezettség

9.9.1. A szolgáltató kártérítési kötelezettsége

Az *Időbélyegzés-szolgáltató* kártérítési kötelezettségének részletes szabályait a *Minősített időbélyegzési szolgáltatási szabályzat*, a Szolgáltatási szerződés vagy az *Ügyfel*ekkel kötött szerződések tartalmazzák.

9.9.2. Az előfizető kártérítési kötelezettsége

Az *Időbélyegzés-szolgáltató* a *Minősített időbélyegzési szolgáltatási szabályzat*ban és a Szolgáltatási szerződésben szabályozza az *Előfizető*kkel szemben támasztott kártérítési igényeit.

9.9.3. Az érintett felek kártérítési kötelezettsége

Az *Időbélyegzés-szolgáltató* a *Minősített időbélyegzési szolgáltatási szabályzat*ban szabályozza az *Érintett felek*kel szemben támasztott kártérítési igényeit.

9.10. Érvényesség és megszűnés

9.10.1. Érvényesség

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

9.10.2. Megszűnés

A *Minősített időbélyegzési rend* visszavonásig hatályos időbeli korlátozás nélkül.

9.10.3. A megszűnés következményei

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

9.11. A felek közötti kommunikáció

Az *Időbélyegzés-szolgáltató* az *Ügyfel*ekkel történő kapcsolattartás érdekében működtessen ügyfélszolgálati irodát.

9.12. Módosítások

Az *Időbélyegzés-szolgáltató* fenntartja magának a jogot, hogy a normatív szabályok, biztonsági követelmények, piaci környezet vagy egyéb körülmények változása esetén szabályozott módon megváltoztassa a *Minősített időbélyegzési rend*et.

Rendkívüli esetben (pl. kritikus biztonsági intézkedések meghozatalának szükségessége) a változások azonnali hatállyal is életbe léptethetők.

9.12.1. Módosítási eljárás

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

A jóváhagyott dokumentumot legalább 30 nappal a tervezett hatálybalépés előtt véleményezésre megküldi a Nemzeti Média- és Hírközlési Hatóság részére és publikálásra kerül a *Időbélyegzés-szolgáltató* honlapján.

Az *Időbélyegzés-szolgáltató* a közzétett új szabályzat tervezettel kapcsolatos észrevételeket a hatályba lépést megelőző 14. napig fogadja az alábbi címen:

`info@e-szigno.hu`

Érdemi változtatást igénylő észrevétel esetén a dokumentumot megváltoztatja.

A szabályzat észrevételekkel módosított változatát az *Időbélyegzés-szolgáltató* a hatályba lépést megelőző 7. napon zárja le és teszi közzé.

9.12.2. Értesítések módja és határideje

Az *Időbélyegzés-szolgáltató* a 9.12.1. pontban leírtak szerint értesíti az *Érintett felek*et az új dokumentum verziók kibocsátásáról.

9.12.3. Az OID megváltoztatása

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

9.13. Vitás kérdések rendezése

Az *Időbélyegzés-szolgáltató* törekedjen a működése során felmerülő vitás kérdések békés, tárgyalásos rendezésére. A rendezés során a fokozatosság elvét kell követni.

9.14. Irányadó jog

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

9.15. Az érvényben lévő jogszabályoknak való megfelelés

A jelen *Minősített időbélyegzési rend* megfelel az alábbi jogszabályoknak:

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

- 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól [4];

- ETSI EN 319 401 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [6];
- ETSI EN 319 421 V1.1.1 (2016-03); Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps. (Replaces ETSI TS 102 023) [14];
- ETSI EN 319 422 V1.1.1 (2016-03); Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles (Replaces ETSI TS 101 861) [15];
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról [2];
- 2013. évi V. törvény a Polgári Törvénykönyvről [3].

9.16. Vegyes rendelkezések

9.16.1. Teljességi záradék

Nincs megkötés.

9.16.2. Átruházás

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

9.16.3. Részleges érvénytelenség

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

9.16.4. Igényérvényesítés

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

9.16.5. Vis maior

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

9.17. Egyéb rendelkezések

Nincs megkötés.

10. Hivatkozások

Hivatkozások

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

[2] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról.

[3] 2013. évi V. törvény a Polgári Törvénykönyvről.

[4] 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól.

[5] ETSI EN 319 102-1 V1.1.1 (2016-05); Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation.

[6] ETSI EN 319 401 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

[7] ETSI EN 319 403 V2.2.2 (2015-08) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers;.

[8] ETSI EN 319 411-1 V1.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements .

[9] ETSI EN 319 411-2 v2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates; (Replaces ETSI TS 101 456).

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

[11] ETSI EN 319 412-2 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons; (Replaces ETSI TS 102 280).

[12] ETSI EN 319 412-3 V1.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons (Replaces ETSI TS 101 861).

[13] ETSI EN 319 412-5 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.

[14] ETSI EN 319 421 V1.1.1 (2016-03); Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps. (Replaces ETSI TS 102 023).

[15] ETSI EN 319 422 V1.1.1 (2016-03); Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles (Replaces ETSI TS 101 861).

[16] ETSI TS 119 312 V1.1.1 (2014-11); Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.

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

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

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

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

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

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

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

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

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