NISZ

Nemzeti Infokommunikációs Szolgáltató Zrt.

Időbélyegzés
Bizalmi Szolgáltatási Rend
(IBR)

Verziószám	1.5
OID	0.2.216.1.200.1100.100.42.3.3.14.1.5
Hatályba lépés dátuma	2024.01.02.
Dokumentum besorolása	nyilvános

Adorján István

Digitálisan aláírta: Adorján István
Dátum: 2023.12.22 16:58:26 +01'00'

Változáskövetés

verzió	dátum	a változás leírása	készítette	ellenőrizte	jóváhagyta
1.0[1]	2016.12.29	Első, eIDAS megfelelőségértékeléshez elkészített változat	Polysys Kft.	Kővári Ferenc	Ferencz Attila
1.1[2]	2017.04.28	Megfelelőségértékelő szervezet észrevételei alapján módosított változat	Polysys Kft. Kővári Ferenc	Kővári Ferenc	Ferencz Attila
1.2	2017.05.31.	Hatályba lépés dátumának pontosítása	Papp Eszter	Kővári Ferenc	Ferencz Attila
1.3	2019.03.25	EN szabványok változásainak követése, egyéb frissítések	Polysys Kft.	Kővári Ferenc	Ferencz Attila
1.4.	2023.03.20.	A tanúsítványok alkalmazhatósági szabályainak módosítása	Nagy Benjámin	Kővári-Szabó Zoltán	Adorján István
1.5	2024.01.02	Székhelyváltozás átvezetése	Kővári-Szabó Zoltán	Nagy Benjámin	Adorján István

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

Tartalomjegyzék

1 BEVEZETÉS

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

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

Jelen IBR hatálya alatt a Szolgáltató a Szolgáltatást két ügyfélcsoport számára nyújtja:

a) a {J7} 84/2012 Korm. rendelet 7/C. § pontja szerinti kijelölés alapján, azon állampolgárok számára, akik az elektronikus tároló elemmel ellátott állandó személyazonosító igazolványuk e-aláírás funkciójához kapcsolódó szolgáltatások igénybe vételére szolgáltatási szerződést kötöttek (továbbiakban: eSzemélyi[3] ügyfelek);

b) a {J7} 84/2012 Korm. rendelet 4. § g) pontja szerint kormányzati hitelesítés-szolgáltatás keretében, jogi személy vagy jogi személyiség nélküli szervezetek számára (továbbiakban: közületi ügyfelek).

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

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

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

1.1 Áttekintés

Az IBR egy olyan szabálygyűjtemény, amely a Szolgáltatás használatának feltételeit írja elő igénybe vevők valamely közös biztonsági követelményekkel rendelkező csoportja vagy meghatározott alkalmazások számára, valamint meghatározza a Szolgáltatásban kiadott időbélyegzők felhasználhatóságát.

Jelen bizalmi szolgáltatási rend az {Sz1} RFC 3647 nemzetközi ajánlás alapján készült, felépítésében és tartalmában követi annak előírásait.

Jelen bizalmi szolgáltatási rend előírja az időbélyegzőkkel kapcsolatos, a Szolgáltatás nyújtása során teljesíteni szükséges összes követelményt, melyeket az alábbi nemzetközi szabványok határoznak meg:

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

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

Ezen követelmények teljesítésének módját, illetve az itt megnevezett eljárások részletes leírását a „Időbélyegzés Bizalmi Szolgáltatási Szabályzat” (IBSZ) dokumentum tartalmazza.

A jelen bizalmi szolgáltatási rendnek megfelelően kibocsátott időbélyegzők tartalmazzák jelen dokumentum objektum azonosítóját, mely alapján az érintett felek képesek meghatározni az adott időbélyegző alkalmazhatóságát és megbízhatóságát.

1.2 Dokumentum neve és azonosítása

Jelen bizalmi szolgáltatási rend teljes neve: NISZ Zrt. „Időbélyegzés Bizalmi Szolgáltatási Rend”.

A bizalmi szolgáltatási rend rövid neve: IBR.

A bizalmi szolgáltatási rend objektum azonosítója és verziószáma a címlapon található.

A jelen IBR hatálya alatt kiadott időbélyegzők kibocsátására és felhasználására vonatkozó részletes szabályokat az IBSZ szolgáltatási szabályzat tartalmazza.

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

1.2.1 Hitelesítési rendek

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

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

1.3 PKI közösség

1.3.1 Hitelesítő szervezet

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

A Szolgáltató saját szervezetén kívül más szervezetek is közreműködhetnek a Szolgáltatás nyújtásában, azonban a Szolgáltató teljes körű felelősséggel tartozik azért, hogy a jelen szabályzatban foglalt követelmények teljesülnek.

Produktív hitelesítő központ

Szolgáltatónak a Szolgáltatási Szabályzatban azonosítania kell azt a produktív hitelesítő központot, mely a kiadott időbélyegzők hitelesítésére alkalmas tanúsítványokat (4.5.1 fejezet) bocsátja ki az időbélyegző egységek részére.

Időbélyegző egységek (TSU)

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

Hitelesítési Rend és Szabályozási Csoport

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

1.3.2 Ügyfélkapcsolati Iroda

A Szolgáltató – saját szervezetén belül – ügyfélkapcsolati irodát működtet.

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

Az eSzemélyi ügyfelekkel való kapcsolattartás módját, a szolgáltatási szerződés megkötésének eljárását a BSZ-ESZIG szabályzat tartalmazza.

1.3.3 Előfizetők

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

Előfizető:

a) a {J7} 84/2012 Korm. rendelet 7/C. § pontja szerinti kijelölés alapján az állampolgár, aki az elektronikus tároló elemmel ellátott állandó személyazonosító igazolványa e-aláírás funkciójához kapcsolódó szolgáltatások igénybe vételére szolgáltatási szerződést kötött (eSzemélyi ügyfél); vagy

b) a {J7} 84/2012 Korm. rendelet 4. § g) pontja szerint kormányzati hitelesítés-szolgáltatás keretében a jogi személy vagy jogi személyiség nélküli szervezet, aki a Szolgáltatás igénybe vételére Szolgáltatóval szolgáltatási szerződést kötött (közületi ügyfél).

A szolgáltatási szerződés megkötése során a közületi Előfizető kapcsolattartó személyt kell kijelöljön, aki a Szolgáltatás eléréséhez szükséges autentikációs tanúsítványt megigényli, illetve Szolgáltatótól átveszi, a kapcsolódó PIN-borítékkal együtt.

Az Előfizetők felelősségeit a 9.6.3 fejezet tartalmazza.

1.3.4 Érintett felek

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

1.3.5 Egyéb felek

Bizalmi Felügyelet

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

kriptográfiai algoritmusokat, és az azok meghatározott paraméterekkel történő alkalmazására vonatkozó követelményeket.

1.4 Az elektronikus időbélyegző alkalmazhatósága

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

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

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

1.4.1 Engedélyezett időbélyegző használat

Az eSzemélyi ügyfelek a Szolgáltatást csak és kizárólag az elektronikus tároló elemmel rendelkező személyazonosító igazolványuk e-aláírás funkciójának felhasználásával történő elektronikus aláíráshoz kapcsolódóan jogosultak igénybe venni, magáncélra. Ezek használata bármilyen üzleti, munkahelyi vagy ilyen jellegű szakmai tevékenység céljából nem megengedett; kivételt képez a BSZ-ESZIG 1.4.2. pontjában foglalt esetek. Az eSzemélyi ügyfél által igényelhető időbélyegzők számát Szolgáltató jogosult korlátozni; az erre vonatkozó részleteket a szolgáltatási szabályzat (IBSZ) tartalmazza.

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

1.4.2 Tiltott időbélyegző használat

Nincs kikötés.

1.5 Szabályzat adminisztráció

1.5.1 Szabályzatot karbantartó szervezet

A Szolgáltatónak szervezetén belül Hitelesítési Rend és Szabályozási Csoportot kell működtetnie, amely többek között jelen bizalmi szolgáltatási rend karbantartásáért is felelős.

1.5.2 Kapcsolat

A Szolgáltatóval való kapcsolattartás módját, az elérhetőségeket és az illetékes fogyasztóvédelmi szerv elérhetőségét a szolgáltatási szabályzat tartalmazza.

1.5.3 Szabályzat alkalmasságának meghatározása

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

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

1.5.4 Szabályzat jóváhagyásának eljárása

Szolgáltatónak rendelkeznie kell a szabályzatainak jóváhagyására és kiadására vonatkozó eljárásrenddel, melyet a szolgáltatási szabályzatában ismertetnie kell. Az eljárásrendben meg kell jelölni az eljárásért felelős személyt, valamint az egyéb fontos részleteket (pl. hatályba lépés napja).

1.6 Fogalmak, rövidítések és hivatkozások

1.6.1 Fogalmak

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

Az ezen felül alkalmazott fogalmak meghatározása az alábbiakban olvasható.

Előfizető Kapcsolattartója: a szolgáltatási szerződés megkötése során a közületi Előfizető kapcsolattartó személyt kell kijelöljön, aki a Szolgáltatás eléréséhez szükséges autentikációs tanúsítványt megigényli, illetve Szolgáltatótól átveszi, a kapcsolódó PIN-borítékkal együtt.

1.6.2 Rövidítések

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

1.6.3 Hivatkozások

1.6.3.1 Jogszabályi hivatkozások

{J1}	910/2014/EU Európai Parlament és a Tanács rendelete a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről (továbbiakban: eIDAS)
{J2}	2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól (továbbiakban: E-ügyintézési tv.)
{J3}	1992. évi LXVI. törvény a polgárok személyi adatainak és lakcímének nyilvántartásáról (továbbiakban: Nytv.)
{J4}	2016. évi CXXX. törvény a polgári perrendtartásról (továbbiakban: Pp.)
{J5}	2013. évi V. törvény a Polgári Törvénykönyvről (továbbiakban: Ptk.)
{J6}	451/2016. (XII. 19.) Korm. rendelet az elektronikus ügyintézés részletszabályairól
{J7}	84/2012. (IV. 21.) Korm. rendelet egyes, az elektronikus ügyintézéshez kapcsolódó szervezetek kijelöléséről
{J8}	24/2016 (VI. 30.) BM rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről
{J9}	137/2016 (VI. 13.) Korm. rendelet az elektronikus ügyintézés céljára felhasználható elektronikus aláíráshoz és bélyegzőhöz kapcsolódó követelményekről
{J10}	679/2016/EU Európai Parlament és Tanács rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (továbbiakban: GDPR)

1.6.3.2 Szabványok és műszaki-technikai specifikációk

{Sz1}	RFC 3647	Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework
{Sz2}	EN 319 401	General policy requirements for Trust Service Providers
{Sz3}	EN 319 411-1	Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
{Sz4}	EN 319 412-1	Certificate Profiles; Part 1: Overview and common data structures
{Sz5}	EN 319 412-2	Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
{Sz6}	EN 319 412-3	Certificate Profiles; Part 3: Certificate profile for certificates issues to legal persons
{Sz7}	EN 319 412-5	Certificate Profiles; Part 5: QCStatements

{Sz8}	RFC 5280	Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile
{Sz9}	ITU-T X.520	Information technology - Open Systems Interconnection - The Directory: Selected attribute types
{Sz10}	RFC 4514	Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names
{Sz11}	ITU-T X.509	Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate framework
{Sz12}	RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
{Sz13}	EN 319 411-2	Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
{Sz14}	EN 319 421	Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
{Sz15}	EN 319 422	Time-Stamping protocol and time-stamp token profiles
{Sz16}	RFC 3161	Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)
{Sz17}	RFC 5816	ESSCertIDV2 update to RFC 3161
{Sz18}	ETSI TS 119 312	Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
{Sz19}	MSZ/ISO/IEC 15408	ISO/IEC 15408 (parts 1 to 3): Information technology – Security techniques – Evaluation criteria for IT security
{Sz20}	ISO/IEC 19790	ISO/IEC 19790:2012: Information technology – Security techniques – Security requirements for cryptographic modules
{Sz21}	FIPS 140-2	FIPS PUB 140-2 (2001): Security Requirements for Cryptographic Modules
{Sz22}	RFC 2616	Hypertext Transfer Protocol – HTTP/1.1

1.6.3.3 Hivatkozott dokumentumok

{D1}	ÁSZF-GOVCA	Általános Szerződési Feltételek a NISZ Zrt. kormányzati hitelesítés szolgáltatásaihoz
{D2}	SZSZ	Szolgáltatási Szerződés
{D3}		NISZ Zrt. Szervezeti és Működési Szabályzata
{D4}		NISZ Zrt. Adatvédelmi és adatbiztonsági előírásai
{D5}		NISZ Zrt. PKI szolgáltatások informatikai biztonságpolitikája
{D6}		NISZ Zrt. PKI szolgáltatások biztonsági szabályzata

{D7}		NISZ Zrt. PKI szolgáltatások üzletmenet-folytonossági terve
{D8}		NISZ eIDAS tanúsítványprofilok
{D9}		Tanúsítvány megrendelő és regisztrációs űrlap
{D10}	BSZ-ESZIG	Bizalmi Szolgáltatási Szabályzat a személyazonosító igazolványokhoz kibocsátott minősített tanúsítványokhoz

2 KÖZZÉTÉTEL ÉS TANÚSÍTVÁNYTÁR

2.1 Szabályzatok elérhetősége

A Szolgáltatónak gondoskodnia kell arról, hogy a Szolgáltatással kapcsolatos szabályzatok, valamint az egyéb közérdekű szolgáltatói információk az Előfizetők és Érintett Felek részére folyamatosan, napi 24 órában, heti hét napban rendelkezésre álljanak. A Szolgáltatónak mindent meg kell tennie annak érdekében, hogy az információk elérhetetlensége ne haladhassa meg a szolgáltatási szabályzatban meghatározott időtartamot.

2.2 A szolgáltatói információ közzététele

A Szolgáltató a szolgáltatói tanúsítványokat (beleértve az időbélyegző egységek tanúsítványait), valamint a Szolgáltatással kapcsolatos szabályzatokat és egyéb közérdekű szolgáltatói információkat internetes honlapján közzé kell tegye.

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

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

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

2.3 A közzététel gyakorisága

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

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

2.4 Hozzáférés-ellenőrzések

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

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

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

3 AZONOSÍTÁS

A Szolgáltató az időbélyegzők kiadását a felhasználók előzetes azonosításához köti.

A Szolgáltatás igénylésének eljárását és a használat során alkalmazott azonosítás és jogosultságellenőrzés módját a szolgáltatási szabályzatban kell ismertetni.

4 Az időbélyegzés szolgáltatás

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

Szolgáltató a jelen bizalmi szolgáltatási rendjének hatálya alatt minősített időbélyegzés szolgáltatást nyújt, melyről a legfontosabb információkat tartalmazó, TSA Közzétételi Nyilatkozatot (TDS) kell készítenie és közzé tennie. A TDS egyaránt lehet önálló dokumentum (melynek elérhetőségét a szolgáltatás szabályzatban meg kell adni), vagy elkészíthető a szolgáltatási szabályzat mellékleteként.

Az elektronikus időbélyegző kérésének és felhasználásának folyamata röviden az alábbi:

- Előfizető – egy erre alkalmas számítógépes programmal – kiszámítja az időbélyegzővel ellátandó elektronikus dokumentum lenyomatát és azzal szabványos időbélyegző kérést állít elő;
- Előfizető számítógépes programja az időbélyegző kérést Interneten elküldi Szolgáltatónak;
- Szolgáltató azonosítja Előfizetőt és elbírálja jogosultságát;
- Szolgáltató ellenőrzi az időbélyegző kérés formai és tartalmi megfelelőségét, illetve azt, hogy időbélyegző válasz kiadható-e;
- sikeres ellenőrzést követően Szolgáltató szabványos időbélyegző választ állít elő és küld vissza Interneten keresztül Előfizető számára;
- Előfizető számítógépes programja ellenőrzi a kapott időbélyegző választ;
- sikeres ellenőrzést követően Előfizető számítógépes programja az időbélyegzőt:
    - hozzákapcsolja az adott elektronikus dokumentumhoz; vagy
    - elhelyezi abban az elektronikus aláírásban vagy bélyegzőben, melyet az adott elektronikus dokumentum hitelesítésére hoztak létre.
- a későbbiekben, Előfizető vagy bármely Érintett Fél az elektronikus időbélyegzőt felhasználhatja arra, hogy bizonyítsa:
    - az elektronikus dokumentum, amelyhez az időbélyegzőt hozzákapcsolták, létezett az időbélyegben szereplő időpontban és az elektronikus dokumentum az időbélyegző hozzákapcsolását követően nem változott meg; vagy
    - az elektronikus aláírás vagy bélyegző - melyet az adott elektronikus dokumentum hitelesítése céljára hoztak létre, és amelyben az elektronikus időbélyegző szerepel – biztosan az időbélyegzőben jelzett időpontot megelőzően került létrehozásra.

4.1 Időbélyegző kérés

Előfizetőnek olyan számítógépes programot kell használnia az időbélyegző kéréséhez, amely képes az {Sz16} RFC 3161 szabvány 2.4.1 fejezetének megfelelő időbélyegző kérést előállítani.

A kérés által tartalmazott lenyomat (`messageImprint`) algoritmusa meg kell egyezzen valamely, az {Sz18} ETSI TS 119 312 szabványban javasolt, és a Bizalmi Felügyelet algoritmus határozatában szereplő lenyomatképző algoritmussal. Ennek megfelelően Szolgáltató csak SHA256 lenyomatképző algoritmussal előállított időbélyegző kérést fogad be az Előfizetőtől.

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

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

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

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

4.2 Időbélyegzés szolgáltatás elérhetősége és rendelkezésre állása

Szolgáltatónak a szolgáltatási szabályzatában meg kell adnia a Szolgáltatás elérhetőségét (azt a webcímet, URI-t) ahová az időbélyegző kérések elküldése kell történjen.

A Szolgáltatás kizárólag csak biztonságos HTTPS protokollon vehető igénybe.

Szolgáltatónak biztosítania kell, hogy a Szolgáltatás az Előfizetők részére folyamatosan – 99,9 %-os szinten rendelkezésre álljon, és egy eseti szolgáltatáskiesés időtartama nem haladhatja meg a három órát.

4.3 Időbélyegző kérés elfogadása vagy visszautasítása

Szolgáltatónak ellenőriznie kell a kapott időbélyegző kérés formai és tartalmi megfelelőségét.

Szolgáltató visszautasítja az időbélyegző kérést, ha:

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

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

4.4 Időbélyegző válasz

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

Jelen bizalmi szolgáltatási rend hatálya alatt, a Szolgáltatás keretében csak és kizárólag minősített időbélyegzők adhatók ki.

Az időbélyegző válasznak tartalmaznia kell:

- a verziószámot „1” értékkel (a `version` mezőben);
- jelen IBR objektum azonosítóját (a `policy` mezőben);
- a kérésben levő lenyomatot (a `messageImprint` mezőben);
- az időbélyegző egyedi sorszámát (a `serialNumber` mezőben);
- a dátumot és pontos időpontot a vállalt pontossággal (a `genTime` mezőben);
- a vállalt pontosságot (az `accuracy` mezőben);
- a `nonce` véletlenszámot, ha a kérésben szerepelt olyan
- az adott időbélyegző ellőállítását végző időbélyegző egység azonosítóit (a `tsa` mezőben);
- annak jelzését, hogy az időbélyegző EU minősített bizalmi szolgáltatásban került kiadásra (a `QcStatements` kiterjesztésben a `tst-EuQcCompliance`[4] nyilatkozattal);
- az időbélyegző egység által az időbélyegző hitelesítésére használt tanúsítványt (a `SignedData` / `certificates` mezőben).

Az időbélyegző nem tartalmazhat:

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

4.5 Időbélyegző válasz hitelessége

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

Az időbélyegző hitelesítésére használt elektronikus bélyegző algoritmusa meg kell egyezzen az {Sz18} ETSI TS 119 312 szabványban javasolt, és a Bizalmi Felügyelet algoritmus határozatában szereplő algoritmusok egyikével.

4.5.1 Időbélyegző egységek tanúsítványa

Az időbélyegzők hitelesítésére használt magánkulcshoz tartozó nyilvános kulcsot tanúsítvánnyal kell hitelesíteni és azt közzé kell tenni a Szolgáltató internetes honlapján elérhető nyilvános tanúsítványtárban.

Az időbélyegzők hitelesítésére olyan tanúsítvány kell használni:

- melynek kiadása egy olyan, a Szolgáltató által működtetett, minősített elektronikus bélyegzés célú tanúsítvány kibocsátására irányuló szolgáltatásban történt, amely a bizalmi

[4] OID: 0.4.0.19422.1.1

szolgáltatási rendjében felvállalja az {Sz5} EN 319 412-2 szabvány követelményeinek teljesítését;

- a tanúsítványhoz kapcsolódó magánkulcs előállítása csak és kizárólag időbélyegző aláírása céljára történt (ezt a tanúsítvány kritikus `extendedKeyUsage` kiterjesztésében az `id-kp-timeStamping`[5] jelzi);

4.5.2 Időbélyegző egységek magánkulcsa és kriptográfiai modulja

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

A magánkulcs használati időtartamát az adott algoritmushoz és kulcshosszhoz tartozó, az {Sz18} ETSI TS 119 312 szabványban javasolt, illetve a Bizalmi Felügyelet algoritmus határozatában megjelölt időtartamokra kell korlátozni, a 6.3.2 fejezetben leírt eljárásokkal.

Az időbélyegző egységek tanúsítványhoz kapcsolódó magánkulcsát olyan HSM modulban kell tárolni és használni, ami megfelel a 6.2.1 fejezetben leírt előírásoknak.

Az időbélyegző egység magánkulcsát csak és kizárólag időbélyegzők hitelesítésére lehet használni.

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

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

Az időbélyegző egységek által használt HSM modulokat meg kell védeni a meghamisítás ellen szállítás és tárolás során.

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

Az időbélyegző egység által használt HSM modulnak a használatból történő kivonásakor a rajta levő magánkulcsokat a 6.2.10 fejezetben leírt módon kell megsemmisíteni, hogy a további használatuk gyakorlatilag lehetetlenné váljon.

4.6 Az időbélyegzőben szereplő időpont

Az időbélyegzőben szereplő időpont pontossága 1 másodpercen belüli kell legyen.

4.6.1 Óraszinkronizálás

Az időbélyegző egységek belső óráját egy olyan pontos idővel kell szinkronizálni, amely visszavezethető legalább egy, UTC laboratórium által szolgáltatott, pontos időre.

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

[5] OID: 1.3.6.1.5.5.7.3.8

4.6.2 Időbélyegző egység belső órájának védelme

Szolgáltatónak az időbélyegző egységeket meg kell védenie minden olyan támadástól vagy behatástól, ami a belső óra kalibrációjának észrevétlen elvesztését eredményezhetné.

A Szolgáltatónak folyamatosan vizsgálnia és észlelnie kell az időbélyegző egység belső órája pontos UTC idővel való szinkronizációja sikertelenségét vagy a kalibráció elvesztését.

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

4.6.3 Szökőmásodpercek kezelése

Szökőmásodperc előfordulásakor a Szolgáltatónak el kell végeznie az óra szinkronizációt az illetékes szervezet értesítése alapján.

A szökőmásodperc miatti óraátállítást a szökőmásodperc előfordulására kitűzött napon, a nap utolsó percében kell elvégezni.

4.6.4 Nyári időszámítás kezelése

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

Az UTC időpont értelmezésével kapcsolatos lehetséges problémákról a szolgáltatási szabályzatban tájékoztatni kell az Előfizetőket és Érintett Feleket.

4.7 Időbélyegző válasz hitelességének ellenőrzése

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

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

- az időbélyegző hitelességének ellenőrzése (az azon elhelyezett elektronikus bélyegző kriptográfiai ellenőrzése);
- az időbélyegzőt hitelesítő tanúsítványra az {Sz8} RFC 5280 6. fejezete szerinti tanúsítási útvonal felépítés és érvényesítés elvégzése;
- az időbélyegzőt hitelesítő tanúsítvány visszavonási állapotának ellenőrzése a 4.8 fejezetben ismertetett visszavonási állapot szolgáltatások használatával;
- azokban az alkalmazásokban, ahol jogszabályi vagy egyéb követelmény minősített időbélyegző használatát írja elő:
    - ellenőrizni, hogy az időbélyegző tartalmaz `QcStatements` kiterjesztést és abban a `tst-EuQcCompliance`[6] nyilatkozatot; és/vagy
    - ellenőrizni azt, hogy az időbélyegzőt kibocsátó szolgáltatás - a bélyegzett időpontra vonatkoztatva - szerepel-e EU minősített szolgáltatásként és megfelelő státusszal a {J1} eIDAS 22. cikke szerinti Bizalmi Listán.

[6] OID: 0.4.0.19422.1.1

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

4.8 Visszavonási állapot szolgáltatások

4.8.1 Működési jellemzők

Szolgáltatónak az időbélyegző egységek tanúsítványaihoz, valamint az egyéb szolgáltatói tanúsítványokhoz kapcsolódó visszavonási információkat mind CRL, mind OCSP formájában biztosítania kell.

Szolgáltatónak biztosítania kell, hogy a visszavonási állapot információ változása mind a CRL, mind az OCSP szolgáltatásban azonosan, konzisztens módon megjelenjen, figyelembe véve az egyes szolgáltatásokban eltérő frissítési időket is.

CRL

A Szolgáltató által kibocsátott CRL meg kell feleljen az {Sz8} RFC 5280 szabványnak.

A CRL elérhetőségét a tanúsítvány `cRLDistributionPoint` kiterjesztése kell tartalmazza.

A CRL minden esetben tartalmazza a következő kibocsátás időpontját (`nextUpdate`). A záró CRL (az adott hitelesítő központ által kiadott utolsó CRL) esetén a `nextUpdate` mező tartalma a „99991231235959Z” RFC 5280 {Sz8} szerinti speciális időpont. Szolgáltatónak biztosítania kell, hogy az új CRL kibocsátása a `nextUpdate` mezőben jelzett időpont előtt minden esetben megtörténjen.

A CRL-nek tartalmaznia kell minden olyan visszavont tanúsítványt, amelynek érvényessége a CRL kibocsátásának időpontjában nem járt még le.

OCSP

A Szolgáltató által biztosított OCSP szolgáltatás meg kell feleljen az {Sz12} RFC 6960 szabványnak.

Az OCSP szolgáltatás elérhetőségét a tanúsítvány `authorityInformationAccess` kiterjesztésében, az `ocsp` / `accessLocation` mezőnek kell tartalmaznia.

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

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

Az OCSP válaszadó számára minimum 4 és maximum 21 óránként új, 24 órás érvényességű tanúsítvány kerül kiadásra, annak érdekében, hogy az OCSP választ aláíró tanúsítvány

visszavonási állapotát ne kelljen ellenőrizni, ennek jelzésére az OCSP válaszadó tanúsítványában szerepel az `id-pkix-ocsp-nocheck` kiterjesztés.

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

4.8.2 Szolgáltatás rendelkezésre állása

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

4.8.3 Opcionális funkciók

Nincs kikötés.

5 FIZIKAI, ELJÁRÁSBELI ÉS SZEMÉLYZETI BIZTONSÁGI ÓVINTÉZKEDÉSEK

Szolgáltatónak gondoskodnia kell arról, hogy kellő, az irányadó szabványoknak megfelelő fizikai, eljárásbeli és személyzeti biztonsági óvintézkedések, illetve az ezeket érvényre juttató adminisztratív és irányítási eljárások kerüljenek alkalmazásra.

5.1 Fizikai óvintézkedések

5.1.1 Telephely elhelyezése és szerkezeti felépítése

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

5.1.2 Fizikai hozzáférés

Szolgáltatónak védenie kell a Szolgáltatás nyújtásában közreműködő eszközeit és berendezéseit a jogosulatlan fizikai hozzáféréstől az eszközök manipulálásának megakadályozása érdekében.

Ehhez biztosítania kell az alábbiakat:

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

5.1.3 Áramellátás és légkondicionálás

Szolgáltató a gépteremben olyan szünetmentes áramellátó rendszert kell biztosítson, amely:

- megfelelő teljesítménnyel rendelkezik a gépterem informatikai és kisegítő létesítményi berendezései áramellátásának biztosítására;

- megvédi az informatikai berendezéseket a külső hálózat feszültség ingadozásai, feszültség kimaradásai és egyéb zavarok ellen;
- tartós áramszünet esetére saját áramellátó berendezés biztosítja - üzemanyag utántöltéssel - tetszőlegesen hosszú időtartamig az áramellátást.

Szolgáltatónak a gépteremben olyan légkondicionáló berendezést kell alkalmazni, mely biztosítja az alábbiakat:

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

5.1.4 Beázás és elárasztás veszélyeztetettség

Szolgáltatónak a géptermet meg kell védenie a beázástól, víz betöréstől és elárasztástól.

5.1.5 Tűzmegelőzés és tűzvédelem

Szolgáltatónak a géptermet füst- és tűzérzékelőkkel kell felszerelni, melyek automatikusan riasztják az illetékes személyzetet. Minden helyiségben jól látható helyen kell elhelyezni a vonatkozó előírásoknak megfelelő típusú és mennyiségű kézi tűzoltó készüléket. A gépteremben automatikus tűzoltó rendszert kell kialakítani, amely emberi egészségre nem veszélyes és nem károsítja az informatikai eszközöket.

5.1.6 Adathordozók tárolása

Szolgáltatónak meg kell védenie valamennyi adathordozóját a jogosulatlan hozzáféréstől, a megsemmisüléstől vagy véletlen rongálódástól.

5.1.7 Selejt kezelése és megsemmisítése

Szolgáltatónak a környezetvédelmi előírások betartásával kell gondoskodnia feleslegessé vált eszközeinek, adathordozóinak megsemmisítéséről. A felesleges eszközöket és adathordozókat az erre kijelölt munkatárs személyes felügyelete mellett, széleskörűen elfogadott módszerekkel használhatatlanná kell tenni vagy visszaállíthatatlan módon törölni kell.

5.1.8 Fizikailag elkülönítetten őrzött mentési példányok

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

Szolgáltatónak biztosítania kell, hogy az adatmentést vagy abból a helyreállítást csak rendszerüzemeltető bizalmi munkakört betöltő személy végezze el.

5.2 Eljárásbeli előírások

Szolgáltatónak gondoskodnia kell arról, hogy informatikai rendszereit biztonságosan, szabályszerűen, a meghibásodás minimális kockázata mellett üzemeltessék. Szolgáltató

személyzete a feladatokat olyan eljárásbeli előírások alapján kell végezze, melyek szinkronban vannak a jogszabályi, szabványi és belső biztonsági előírásokkal.

5.2.1 Bizalmi munkakörök

Szolgáltatónak egyértelműen azonosítania kell azokat a munkaköröket, amelyektől a Szolgáltatás biztonsága függ. Ezeket a bizalmi munkaköröket és felelősségeket dokumentálni kell. A jogosultságokat és funkciókat olyan módon kell megosztani az egyes bizalmi munkakörök között, hogy egyedül egyetlen felhasználó se legyen képes a biztonsági védelmi intézkedések megkerülésére. Szolgáltatónak biztosítania kell, hogy minden bizalmi munkakör betöltésre kerüljön.

A bizalmi munkakört betöltő személynek munkaviszonyban kell állnia Szolgáltatóval. Bizalmi munkakörbe a Szolgáltató felső vezetősége kell kinevezze a munkatársakat.

5.2.2 Az egyes feladatokhoz szükséges személyzeti létszámok

Szolgáltató biztonsági szabályzataiban elő kell írni, hogy csak védett környezetben, legalább kettő, bizalmi munkakört betöltő munkatárs egyidejű fizikai jelenlétében végezhetők el az alábbi műveletek:

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

5.2.3 Bizalmi munkakörökben elvárt azonosítás és hitelesítés

A bizalmi munkaköröket betöltő személyeket azonosítani és hitelesíteni kell, mielőtt a Szolgáltatás nyújtásában érintett, kritikus informatikai rendszerekhez hozzáférnének.

5.2.4 Egymást kizáró munkakörök

A Szolgáltatónak biztosítania kell, hogy a bizalmi munkakörök vonatkozásában:

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

5.3 Személyzetre vonatkozó előírások

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

5.3.1 Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

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

5.3.2 Biztonsági háttér ellenőrzés eljárásai

A Szolgáltató vezetői munkakörben, illetve bizalmi munkakörben csak olyan alkalmazottakat foglalkoztathat, akik:

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

5.3.3 Képzési követelmények

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

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

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

5.3.4 Továbbképzési gyakoriságok és követelmények

Szolgáltatónak gondoskodnia kell arról, hogy a munkatársak folyamatosan a megfelelő tudással rendelkezzenek, szükség esetén továbbképzést vagy ismétlő jellegű képzést kell tartania.

Legalább évente egyszer továbbképzést kell biztosítani az újonnan ismertté vált sebezhetőségekről, az IT biztonság aktuális gyakorlatáról, a munkatársak saját szakterületét érintően.

5.3.5 Munkabeosztás körforgásának gyakorisága és sorrendje

Nincs kikötés.

5.3.6 Felhatalmazás nélküli tevékenységek büntető következményei

Szolgáltatónak a dolgozókkal kötendő munkaszerződésben szabályoznia kell a dolgozó felelősségre vonásának lehetőségét a dolgozó által elkövetett mulasztások, vétlen vagy szándékos károkozás esetére.

5.3.7 Szerződéses munkavállalókra vonatkozó követelmények

Szolgáltató bizalmi munkakörben csak munkaviszonyban álló személyt foglalkoztathat.

Az egyéb feladatok ellátására, vállalkozási vagy megbízási szerződésben foglalkoztatott személyeket Szolgáltató csak előzetes biztonsági ellenőrzést követően foglalkoztathatja. Az ellenőrzött személyekkel írásos megállapodást kell kötni, melyben rögzíteni kell az esetleges biztonsági szabályokat és a titoktartásra vonatkozó kikötéseket.

5.3.8 A személyzet számára biztosított dokumentációk

Szolgáltatónak folyamatosan biztosítania kell a személyzet részére a munkakörük ellátásához szükséges dokumentációk és szabályzatok rendelkezésre állását.

5.4 A biztonsági naplózás folyamatai

5.4.1 Naplózott esemény típusok

Szolgáltatónak minden, az informatikai rendszerével és a Szolgáltatás nyújtásával kapcsolatos eseményt naplóznia kell. A naplózott adatállománynak a Szolgáltatás nyújtásának teljes folyamatát át kell fognia, és lehetővé tennie, hogy a valós helyzetek megítéléséhez a szükséges mértékben minden, a Szolgáltatással kapcsolatos eseményt rekonstruálni lehessen.

5.4.2 Naplóállomány feldolgozásának gyakorisága

Szolgáltatónak biztosítania kell a naplóállományok rendszeres ellenőrzését és kiértékelését.

5.4.3 Naplóállomány megőrzési időtartama

A naplóállományokat archiválni kell és gondoskodni azok biztonságos megőrzéséről az 5.5.2 fejezetben előírt időtartamig.

5.4.4 Naplóállomány védelme

A naplóállomány minden bejegyzését védeni kell a módosítástól, illetve biztosítani kell, hogy a napló tartalmához csak arra feljogosított személyek férhessenek hozzá.

A naplóállományok kezelését olyan módon kell megoldani, hogy kizárható legyen a napló megsemmisülése, a napló bejegyzések törlése, módosítása, a bejegyzések sorrendjének bármilyen módon történő megváltoztatása.

5.4.5 Naplóállomány mentési folyamatai

A naplóállományokról rendszeres mentést kell készíteni.

5.4.6 Naplózás gyűjtési rendszere

A naplóbejegyzések gyűjtését belső komponenssel kell megoldani. A naplóbejegyzések gyűjtésének meg kell kezdődnie rendszer indításkor és rendszer leállításig folyamatosan működnie kell, és közben biztosítania kell a gyűjtött bejegyzések integritását és rendelkezésre állását, szükség esetén a bizalmasságát is.

A naplóbejegyzések gyűjtési rendszerének működési rendellenessége esetén Szolgáltatónak fel kell függesztenie az érintett területek működését az üzemzavar elhárításáig.

5.4.7 Rendellenes eseményeket kiváltó alanyok értesítése

Nincs kikötés.

5.4.8 Sebezhetőség értékelések

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

Szolgáltatónak folyamatosan figyelemmel kell kísérnie az újonnan ismertté vált, kritikus sebezhetőségeket, és a szükséges ellenintézkedéseket lehetőség szerint 48 órán belül meg kell tennie. Bármely olyan sebezhetőség esetén, melynek kihatása lehet a Szolgáltatás nyújtására, Szolgáltatónak vagy cselekvési tervet kell készítenie és végrehajtania annak érdekében, hogy a sebezhetőség ne legyen kihasználható illetve annak hatása elhanyagolható legyen, vagy dokumentálnia kell annak ténybeli alapját, hogy az adott sebezhetőség nem igényel intézkedést.

5.5 Adatok archiválása

5.5.1 A tárolt adatok típusai

Szolgáltatónak gondoskodnia kell arról, hogy megőrzésre kerüljön minden olyan információ, amely szükséges ahhoz, hogy egy elektronikus időbélyegző érvényessége bizonyítható legyen, továbbá amely a Szolgáltató és a rendszereinek megfelelő működését alátámasztja.

Ehhez legalább az alábbi információkat tárolja papír alapon vagy elektronikusan:

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

5.5.2 Archívum megőrzési időtartama

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

5.5.3 Archívum védelme

Szolgáltatónak biztosítania kell valamennyi archivált adatra azok sértetlenségét és hitelességét, a rendelkezésre állását és a bizalmasságát.

5.5.4 Archívum mentési eljárásai

Szolgáltatónak biztosítania kell az iratok, dokumentumok, elektronikus állományok biztonságos, hosszú távú megőrzését, illetve tárolását, továbbá az elektronikus formában archivált állományok adathordozóinak elavulás elleni védelmét a megőrzési időn belül.

5.5.5 Az adatok időbélyegzésére vonatkozó követelmények

Valamennyi naplóbejegyzést el kell látni olyan időjellel, melyben legalább egy másodperc pontossággal fel van tüntetve a rendszer által szolgáltatott időpont.

Az elektronikus formában archivált adatokon legalább fokozott biztonságú elektronikus aláírást vagy bélyegzőt, valamint minősített időbélyeget kell elhelyezni

Az archivált adatok megőrzése során szükség esetén (pl. algoritmus váltás) gondoskodni kell az elektronikus aláírások vagy bélyegzők, valamint az időbélyegzők hitelességének fenntartásáról.

5.5.6 Archívum gyűjtési rendszere

A naplóállományokat és az egyéb elektronikusan keletkezett adatokat a Szolgáltató védett informatikai rendszerén belül kell gyűjteni. A védett informatikai rendszerből történő kimozgatás során az adatokat minősített időbélyegzőt tartalmazó elektronikus aláírással vagy bélyegzővel kell ellátni.

A papíralapú iratokat Szolgáltató dokumentumtárában kell tárolni.

5.5.7 Archívum hozzáférés és ellenőrzés eljárásai

Szolgáltatónak az archivált adatokat meg kell védenie a jogosulatlan hozzáféréstől. A jogosult hozzáféréseket naplózni kell.

5.6 Kulcs átállás

Szolgáltatónak biztosítania kell, hogy az időbélyegző egységek folyamatosan rendelkezzenek a működésükhöz szükséges, megfelelően erős algoritmusú és kulcshosszú, érvényes kulccsal és tanúsítvánnyal.

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

5.7 Helyreállítás rendkívüli üzemi helyzetek esetén

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

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

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

5.7.1 Rendkívüli események és kompromittálódás kezelésének eljárásai

Szolgáltatónak rendelkeznie kell üzletmenet folytonossági tervvel.

Rendkívüli üzemeltetési helyzetben Szolgáltatónak dokumentálnia kell az eseményeket, azok körülményeit, az elhárításukra megtett intézkedéseket.

A rendkívüli üzemeltetési helyzetben Szolgáltatónak a lehető legrövidebb időn belül tájékoztatást kell közzé tennie internetes honlapján, valamint - lehetőség szerint - elektronikus levélben kell értesítenie azokat a személyeket, akiket az esemény érint.

5.7.2 Sérült számítási erőforrások, szoftverek és/vagy adatok

Szolgáltatónak olyan megbízható rendszert kell működtetni, mely a rendszerben bekövetkezett hiba esetén is biztosítja a Szolgáltatás működtetését és elérhetőségét.

5.7.3 Időbélyegző egység magánkulcsának kompromittálódása esetén követendő eljárás

Az időbélyegző egység magánkulcsának kompromittálódása esetén haladéktalanul meg kell tenni a szükséges lépéseket:

- megszüntetni az érintett időbélyegző egység és így az érintett magánkulcs használatát;
- visszavonni az érintett magánkulcshoz tartozó tanúsítványt;
- új időbélyegző kulcspárt és tanúsítványt hozni létre;
- értesíteni a Bizalmi Felügyeletet;
- intézkedni valamennyi érintett fél értesítéséről;
- közzé tenni azt az információt, ami alapján egyértelműen meg lehet határozni az érintett időbélyegzők körét.

5.7.4 Üzletmenet folytonosság helyreállás katasztrófát követően

Szolgáltatónak rendelkeznie kell tartalék helyszínnel és informatikai rendszerrel, továbbá megtervezett eljárásokkal az áttelepülésre.

5.8 A szolgáltatási tevékenység megszüntetése

Szolgáltatónak rendelkeznie kell a szolgáltatási tevékenység megszüntetésére vonatkozó, aktualizált tervvel.

A szolgáltatási tevékenység megszüntetésére vonatkozó tervnek tartalmaznia kell legalább az alábbiakat:

- Előfizetők és Érintett Felek értesítésének módja;
- a Szolgáltatással kapcsolatos azon kötelezettségeknek átadása egy másik minősített bizalmi szolgáltatónak, melyek arra vonatkoznak, hogy bizonyítékot szolgáltassanak a Szolgáltató működésével kapcsolatban - különösen az 5.5.1 fejezetben meghatározott adatoknak a megőrzése az 5.5.2 fejezetben megjelölt időtartamig;
- időbélyegzők kiadásának beszüntetése;
- az összes. a Szolgáltatásban érintett időbélyegző egységek által valaha használt tanúsítvány visszavonása;
- időbélyegző egységek magánkulcsainak és azok mentései megsemmisítésének módja;
- Szolgáltató informatikai rendszerében foglalt adatokról teljes körű mentés készítése.

Szolgáltatónak rendelkeznie kell olyan bankgaranciával, mely fedezi a szolgáltatási tevékenység megszüntetésének költségeit abban az esetben, ha Szolgáltató csődeljárás alá kerül vagy más okból kifolyólag nem képes önmaga fedezni a költségeket.

6 MŰSZAKI BIZTONSÁGI ÓVINTÉZKEDÉSEK / TECHNICAL SECURITY CONTROLS

6.1 Kulcspár előállítás és telepítés

6.1.1 Kulcspár előállítás

Szolgáltató maga kell előállítsa az időbélyegző egységek által a kiadott időbélyegző hitelesítésére használandó kulcspárokat fizikailag védett környezetben, kriptográfiai modulban (HSM), legalább két bizalmi munkakört betöltő személy együttes részvételével, illetéktelen személy jelenlétének kizárásával. A kriptográfiai modulnak meg kell felelnie a 6.2.1 fejezet szerinti követelményeknek. Az időbélyegző egység magánkulcsai teljes életciklusuk alatt abban kriptográfiai modulban kell maradjanak, amelyben az előállításuk történt, más modulba nem importálhatók.

Az időbélyegző egység kulcspárjának generálása a Szolgáltató által előkészített ún. „kulcs ceremónia” forgatókönyv szerint kell történjen.

Egy időbélyegző egységnek egy időben csak egy aktív kulcspárja lehet.

6.1.2 Magánkulcs eljuttatása a tulajdonoshoz

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

6.1.3 Nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz

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

6.1.4 Időbélyegző egységek nyilvános kulcsának közzététele

Szolgáltatónak biztosítania kell, hogy az időbélyegző egységek nyilvános kulcsa a kicserélésen alapuló támadás (substitution attack) ellen védett módon legyen eljuttatva az Érintett Felekhez.

6.1.5 Kulcs méretek

A Szolgáltatónak a Szolgáltatás nyújtása során - mind a produktív hitelesítő központok, mind az időbélyegző egységek kulcsainak tekintetében - a Bizalmi Felügyelet vonatkozó határozatának megfelelő szabványos algoritmusokat, paramétereket és kulcshosszakat kell használnia.

6.1.6 A nyilvános kulcs paraméterek előállítása és megfelelőségének ellenőrzése

Az időbélyegző egységek kulcspárjainak előállítása a 6.1.1 fejezet szerint védett környezetben és tanúsított HSM modulban, legalább két bizalmi munkakört betöltő személy együttes részvételével, illetéktelen személy jelenlétét kizárva kell történjen. A kulcspárok generálása során Szolgáltatónak be kell tartania a HSM modul tanúsítási jelentésében foglalt előírásokat is.

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

Szolgáltatónak az időbélyegző egységek tanúsítványaiban a `KeyUsage` és `ExtendedKeyUsage` kiterjesztésekben az {Sz11} ITU-T X.509 v3 és a {Sz15} EN 319 422 szabványnak megfelelően kell jeleznie a kulcs használat célját.

Az időbélyegző egység magánkulcsa csak és kizárólag időbélyegzők hitelesítésére használható.

6.2 Magánkulcs védelme és kriptográfiai modul műszaki szabályozások

6.2.1 Kriptográfiai modul szabványok és műszaki szabályozások

Szolgáltató az időbélyegző egységek magánkulcsainak előállítására, tárolására és használatára csak olyan kriptográfiai modult (HSM) alkalmazhat, amely:

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

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

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

6.2.3 Magánkulcs letét

Szolgáltató az időbélyegző egységek magánkulcsait nem teszi letétbe.

6.2.4 Magánkulcs visszaállítása

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

6.2.5 Magánkulcs mentése

Az időbélyegző egységek magánkulcsai biztonsági okokból mentésre kell kerüljenek. A mentést fizikailag biztonságos helyszínen, legalább kettő bizalmi munkakört betöltő személy részvételével titkosított formában, speciális eszközök alkalmazásával kell megvalósítani, megfelelő biztonsági óvintézkedések és eljárási szabályok betartásával, melyek garantálják a magánkulcs sértetlenségét és bizalmasságát.

A mentett példányokat titkosított formában, fizikailag biztonságos környezetben kell megőrizni.

6.2.6 Magánkulcs bejuttatása a kriptográfiai modulba

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

6.2.7 Magánkulcs kriptográfiai modulban történő tárolásának módja

Az időbélyegző egységek magánkulcsainak a tárolása a kulcsok teljes életciklusa alatt a 6.2.1 fejezetben leírt, tanúsítással rendelkező HSM modulban kell történjen.

6.2.8 Magánkulcs aktiválásának módja

Az időbélyegző egységek magánkulcsainak aktiválását Szolgáltató a HSM modul gyártói dokumentációjában előírtak szerint kell végezze.

6.2.9 Magánkulcs aktív állapotának megszüntetési módja

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

6.2.10 Magánkulcs megsemmisítésének módja

Az időbélyegző egységek magánkulcsát visszaállíthatatlan módon meg kell semmisíteni, amikor használatuk már nem szükséges, vagy a magánkulcs használati időtartama (6.3.2 fejezet), vagy a kapcsolódó tanúsítvány lejárt vagy visszavonásra került. A magánkulcsot és az aktiválásához szükséges minden adatot olyan módon kell megsemmisíteni, hogy annak végrehajtása után a magánkulcs semmilyen része ne legyen kikövetkezhető vagy levezethető.

6.2.11 Kriptográfiai modul értékelése

A 6.2.1 fejezet tartalmazza.

6.3 Kulcspár gondozás egyéb szempontjai

6.3.1 Nyilvános kulcs archiválása

Szolgáltató köteles minden időbélyegző egység által valaha használt nyilvános kulcsot az általa kibocsátott tanúsítvánnyal hitelesített formában, a tanúsítványba foglalva archiválni és az érvényesség lejártától – vagy a kapcsolódó magánkulcs használatának végétől - számított tíz évig megőrizni.

6.3.2 Tanúsítvány érvényességi időszaka és kulcspár felhasználás időtartama

A Szolgáltatónak meg kell határoznia az időbélyegző egységek által használt magánkulcsok használati időtartamának végét, amit vagy a tanúsítvány `privateKeyUsagePeriod` kiterjesztésében kell jelezzen, vagy egyéb operatív és/vagy technológiai intézkedésekkel (pl. az időbélyegző egység által használt HSM modul megfelelő paraméterezésével) kell biztosítson.

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

Az időbélyegző egység magánkulcsa nem használható a használati időtartam lejártát követően, azt és annak minden mentett példányát meg kell semmisíteni a 6.2.10 fejezetben leírt módon.

6.4 Aktivizáló adatok

6.4.1 Aktivizáló adatok előállítása és telepítése

Szolgáltató az aktivizáló adatok előállítását és telepítését az időbélyegző egységben használt HSM modul felhasználói útmutatójában leírt eljárásokkal kell végezze, melynek során be kell tartania a HSM modul tanúsítási jelentésében foglalt előírásokat is.

6.4.2 Aktivizáló adatok védelme

Az időbélyegző egységek magánkulcsainak aktivizáló eszközeit, aktivizáló kódokat biztonságosan kell tárolni és használni.

6.4.3 Aktivizáló adatok egyéb szempontjai

Nincs kikötés.

6.5 Informatikai biztonsági óvintézkedések

6.5.1 Informatikai biztonsági műszaki követelmények meghatározása

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

Ennek alapján Szolgáltatónak olyan megbízható informatikai rendszert (beleértve a redundáns kiépítést) és technikákat kell kialakítania és üzemeltetnie, melyek biztosítják a Szolgáltató megbízható működését a Szolgáltatás nyújtásához. Ennek ismertetését Szolgáltató részben a szolgáltatási szabályzatában (IBSZ), részben a belső biztonsági szabályzataiban írja le.

6.5.2 Informatikai biztonsági értékelés

Szolgáltatónak az informatikai rendszerek biztonsági értékelését az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény rendelkezései szerint kell elvégeznie.

6.6 Életciklusra vonatkozó műszaki óvintézkedések

6.6.1 Rendszerfejlesztési óvintézkedések

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

Szolgáltatónak folyamatosan vizsgálnia kell az időbélyegző egységek informatikai eszközeinek terheltségét és kihasználtságát, ez alapján meg kell határoznia a várható kapacitás igényeket és ennek megfelelően időben meg kell tennie a szükséges intézkedéseket ahhoz, hogy a Szolgáltatás jövőbeni nyújtásához megfelelő számítási teljesítmény és tároló kapacitás rendelkezésre álljon.

6.6.2 Biztonságkezelési óvintézkedések

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

A biztonságkezelési szabályokat a Szolgáltató belső társasági szintű és rendszer szintű információbiztonsági szabályzata tartalmazza.

6.6.3 Életciklus biztonsági óvintézkedések

Szolgáltatónak a szolgáltatási szabályzatban meghatározott rendszeres időközönként el kell végeznie a Szolgáltatást megvalósító, megbízható informatikai rendszereinek konfigurációs beállításai, az operációs rendszer beállítások, a hálózati konfigurációs beállítások, továbbá az alkalmazott biztonsági mechanizmusok sértetlenségének és helyes működésének ellenőrzését.

6.7 Hálózatbiztonsági óvintézkedések

A hálózati védelmi intézkedéseket a Szolgáltató belső biztonsági szabályzatában meghatározott követelményeknek megfelelően kell megvalósítani, figyelembe véve az {Sz2} EN 319 411-1 szabvány 6.5.7 fejezetében és az {Sz14} EN 319 421 szabvány 7.10 fejezetében leírt követelményeket is.

Az időbélyegző egységeket kiemelten biztonságos zónában kell elhelyezni, amelyhez csak a bizalmi munkaköröket betöltő személyeknek lehet logikai vagy fizikai hozzáférése.

Az időbélyegző egységek informatikai rendszereit úgy kell konfigurálni, hogy minden, a Szolgáltatás nyújtásához nem szükséges felhasználó és jogosultság, alkalmazás, protokoll, port vagy hálózati szolgáltatás letiltásra vagy eltávolításra kerüljön.

6.8 Időforrások

Az időbélyegző egységek által használt időforrásnak visszavezethetőnek kell lennie legalább egy UTC laboratórium által szolgáltatott, pontos időforrásra.

7 TANÚSÍTVÁNY, CRL ÉS OCSP PROFILOK

7.1 Tanúsítvány profil

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

7.2 CRL profil

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

7.3 OCSP profil

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

8 MEGFELELŐSÉG VIZSGÁLAT ÉS EGYÉB ÉRTÉKELÉSEK

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

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

8.1 Vizsgálatok gyakorisága és körülményei

Szolgáltatónak megfelelőségi vizsgálatokat és értékeléseket kell elvégeznie, illetve elvégeztetnie annak érdekében, hogy a Szolgáltatással kapcsolatos folyamatai, személyzete, eszközei és környezete mindenkor megfeleljen a vonatkozó jogszabályi és szakmai követelményeknek.

Szolgáltató legalább 24 havonta egyszer megfelelőségértékelést és 12 havonta egyszer felülvizsgálatot kell végeztessen a {J1} eIDAS, illetve a {J2} E-ügyintézési tv. követelményeinek való megfelelés tárgykörben. Szolgáltató köteles az elkészült megfelelőségértékelés jelentést annak kézhezvételétől számított három munkanapon belül benyújtani a Bizalmi Felügyeletnek.

8.2 Auditor azonosítása és képesítése

A megfelelőségértékelés előkészítésére, illetve az információbiztonsági rendszer ellenőrzésére Szolgáltató külső rendszervizsgálót alkalmazhat.

A külső rendszervizsgáló által végzett auditokra Szolgáltató olyan szakértőt vagy szakértői szolgáltatásokat nyújtó szervezetet kell megbízzon, aki független Szolgáltatótól, illetve az ellenőrzött rendszertől, területtől, és szakértelmét biztosítani tudja a PKI és az informatikai biztonság, valamint az ezen területekre vonatkozó technikai, technológiai, jogi, szabályzati ismeretek és auditálási módszertanok vonatkozásában.

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

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

8.3 Auditor függetlensége

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

8.4 Audit során vizsgált területek

Az audit az alábbi területeket fedi le:

- szabályzatok és dokumentációk;
- irányítási és ellenőrzési követelmények;
- személyzeti biztonsági követelmények;

- a szolgáltatói kulcspár kezeléséhez kapcsolódó követelmények;
- üzemeltetési és hozzáférési biztonság;
- fizikai és környezeti biztonság;
- folyamatos szolgáltatás biztosítása;
- adatbiztonság és archiválás.

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

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

8.5 Hiányosságok esetén végrehajtandó tevékenységek

Az üzemszerű ellenőrzések, belső és külső auditok, szakértői elemzések által feltárt hiányosságok, hibás gyakorlatok kezelésére Szolgáltató intézkedési tervet kell készítsen. A hiányosságokat köteles késlekedés nélkül orvosolni, az intézkedéseket dokumentálni és ellenőrizni.

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

8.6 Eredmény kommunikációja

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

9 EGYÉB ÜZLETI ÉS JOGI KÉRDÉSEK

9.1 Díjak

A Szolgáltatás díjaival kapcsolatos információkat a szolgáltatási szabályzat kell tartalmazza.

Szolgáltató nem számíthat fel díjat a tanúsítványok visszavonási állapotára vonatkozó státusz információk szolgáltatásáért, valamint a nyilvános tanúsítványtárban közzétett időbélyegző egységek által használt és egyéb szolgáltatói tanúsítványoknak az eléréséért.

9.2 Anyagi felelősség

Szolgáltatónak az anyagi felelősség mértékéről, illetve annak korlátairól a szolgáltatási szabályzatban rendelkeznie kell.

9.2.1 Biztosítási fedezet

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

A felelősségbiztosítási szerződésnek meg kell felelnie a {J8} 24/2016 rendelet előírásainak is.

9.2.2 További követelmények

Szolgáltatónak teljesítenie kell a {J8} 24/2016 rendelet 19. §-a szerint pénzügyi követelményeket is.

9.2.3 Felelősségbiztosítás vagy garancia végfelhasználók számára

Nincs kikötés.

9.3 Üzleti információk bizalmassága

9.3.1 Bizalmasan kezelendő információk köre

Szolgáltatónak a szolgáltatási szabályzatban meg kell adnia a bizalmasan kezelendő információk körét.

9.3.2 Nem bizalmasnak tekintett információk köre

Nincs kikötés.

9.3.3 Bizalmas információk védelmének felelőssége

Szolgáltatónak meg kell védenie a bizalmas információkat. A bizalmas információk védelmét a személyzet megfelelő képzésével, továbbá a munkavállalókkal, szerződéses partnerekkel megkötött szerződésekkel kell érvényre juttatni.

9.4 Személyes adatok védelme

9.4.1 Adatvédelmi terv

Szolgáltató rendelkezik mind társasági szintű adatvédelmi tervvel ({D4}), mind pedig a Szolgáltatásra vonatkozó adatvédelmi tájékoztatóval, melyek nyilvános dokumentumok, és elérhetők Szolgáltató internetes honlapján. Ezen dokumentumok összhangban vannak a nemzetközi és hazai vonatkozó jogszabályokkal.

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

9.4.2 Bizalmasként kezelendő személyes adatok

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

Szolgáltató bizalmasként kezelendő személyes adatnak tekinti:

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

9.4.3 Bizalmasként nem kezelendő személyes adatok

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

9.4.4 Személyes adatok védelmének felelőssége

Szolgáltatónak gondoskodnia kell a személyes adatok védelméről, működése és szabályzatai meg kell feleljenek a {J10} GDPR rendelkezéseinek.

9.4.5 Hozzájárulás a személyes adatok felhasználásához

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

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

9.4.6 Felfedés bírósági vagy polgári peres eljárás keretében

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

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

9.4.7 Egyéb, felfedést eredményező körülmények

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

9.5 Szellemi tulajdonjogok

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

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

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

9.6 Tevékenységért viselt felelősség és helytállás

9.6.1 Szolgáltató felelőssége és helytállása

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

9.6.2 Szolgáltató kötelezettségei

Szolgáltató köteles a Szolgáltatás nyújtása során:

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

- naplózni a Szolgáltatással kapcsolatos minden fontos esemény, a naplóállományokat a jogszabályi előírásoknak megfelelően megőrizni.

9.6.3 Előfizető felelőssége és helytállása

Előfizető jogai

Előfizető jogosult:

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

Előfizető felelőssége

Előfizető felelős:

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

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

Előfizető kötelezettségei

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

Ezen túlmenően Előfizető köteles:

- a Szolgáltatás használata előtt megismerni a szolgáltatási szabályzatot;
- a Szolgáltatás igénybe vételéhez szükséges adatokat hiánytalanul és a valóságnak megfelelően megadni Szolgáltató kérésére;
- olyan megbízható informatikai rendszert (számítógépes programot) használni, amely képes időbélyegzőket kérni és fogadni a 4. fejezetben leírt módon;
- a Szolgáltatást kizárólag a jogszabályok által megengedett vagy nem tiltott célokra, a jelen szabályzatban és a hivatkozott dokumentumokban foglaltaknak megfelelően használni;
- adat változás (különösen az értesítéshez szükséges adatok) esetén haladéktalanul írásban értesíteni erről Szolgáltatót;

- biztosítani, hogy a Szolgáltatás igénybe vételéhez szükséges adatokhoz és eszközökhöz (különösen az időbélyegzés hozzáférés titkos adataihoz) illetéktelen személy ne férhessen hozzá;
- haladéktalanul, írásban értesíteni Szolgáltatót, ha az időbélyegzővel vagy az annak felhasználásával kapcsolatban jogvita indul.

9.6.4 Érintett felek felelőssége és helytállása

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

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

9.6.5 Egyéb felek felelőssége és helytállása

Nincs kikötés.

9.7 Helytállás érvénytelenségi köre

A helytállás érvénytelenségi körét a szolgáltatási szabályzatban meg kell határozni.

9.8 Felelősség korlátozása

Szolgáltató korlátozhatja a kártérítési felelősségét; erről a szolgáltatási szabályzatban kell rendelkeznie.

9.9 Kártérítések

A kártérítésekről a szolgáltatási szabályzatban kell rendelkezni.

9.10 Hatályosság és megszűnés

9.10.1 Hatályosság

Időbeli hatály

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

Tárgyi hatály

A bizalmi szolgáltatási rend tárgyi hatálya kiterjed a Szolgáltatás nyújtására és igénybe vételére.

Személyi hatály

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

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

9.10.2 Megszűnés

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

9.10.3 Megszűnés után is hatályban maradó rendelkezések

A megszűnés után is hatályban maradó rendelkezéseket a szolgáltatási szabályzatban meg kell határozni.

9.11 Egyéni hirdetmények és kommunikáció a részvevőkkel

A szolgáltatási szabályzatban rendelkezni kell a felek és részvevők közötti kommunikáció joghatást kiváltó módjairól.

9.12 Módosítások

9.12.1 Módosítás eljárása

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

9.12.2 Értesítés módszere és időtartama

A Szolgáltatás jelentős vagy lényeges változása esetén Szolgáltatónak internetes honlapján közleményt kell közzé tennie, a hatályba lépést megelőzően kellő időben ahhoz, hogy az érintett felek a változásokra felkészülhessenek.

9.12.3 OID megváltozását előidéző körülmények

A bizalmi szolgáltatási rend új verziójával az OID verziószámot jelentő része megfelelően változik.

9.13 Vitás kérdések rendezése

A vitás kérdések rendezéséről a szolgáltatási szabályzatban kell rendelkezni.

9.14 Irányadó jog

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

9.15 Hatályos jognak megfelelés

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

9.16 Vegyes rendelkezések

Nincs kikötés.

9.16.1 Teljességi záradék

Nincs kikötés.

9.16.2 Átruházás

Nincs kikötés.

9.16.3 Részleges érvénytelenség

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

9.16.4 Igényérvényesítés

Szolgáltató kártérítésre, az ügyvédi díjak megfizetésére tarthat igényt a partnerei által okozott károk, veszteségek, költségek megtérítése érdekében. Amennyiben Szolgáltató egy konkrét esetben nem él kártérítési igényével, az nem jelenti azt, hogy a jövőben hasonló esetben a bizalmi szolgáltatási rend más rendelkezésének megsértése esetén is lemondana a kártérítési igény érvényesítéséről.

9.16.5 Force Majeure (Vis maior)

A szolgáltatási szabályzat tartalmazza.

9.17 Egyéb rendelkezések

A Szolgáltatást és az ennek keretében alkalmazott végfelhasználói termékeket hozzáférhetővé kell tenni a fogyatékossággal élő személyek számára, amennyiben az lehetséges.