Magyar Telekom

Minősített Időbélyegzés

Szolgáltatási Szabályzata

Egyedi objektum-azonosító (OID): 1.3.6.1.4.1.17835.7.1.2.11.3.13.1.9

Verziószám: **1.9**

Hatályba lépés dátuma: ..... 2010.06.20.

Magyar Telekom

Változáskezelés

Verzió-szám	Dátum	A változás leírása
0.90	2003-10-10	Első változat (szakértői munkaanyagok)
0.91	2003-10-26	Javított tervezet (első változat)
0.92	2003-10-31	Javított tervezet (ellenőrzött változat)
0.93	2003-11-30	Javított tervezet (kiegészített és ellenőrzött harmadik változat)
0.94	2003-12-15	A kiviteli dokumentumokkal egyeztetett változat
0.95	2004-01-30	A tesztek és jogi ellenőrzések alapján módosított első változat
0.96	2004-03-05	A szolgáltatói ellenőrzések után javított változat
0,97	2004-03-11	Matáv Workshop utáni javított változat
1.0	2004-03-30	Hatósági kérelemben beadott szabályzat
1.1	2004-07-17	Hatósági szemlét követő változások átvezetése
1.2	2004-09-23	Hatóság részére átadott végső változat
1.3	2005-09-01	Magyar Telekom névváltásának és következményeinek módosítása
1,4	2005-11-15	Hatósági ellenőrzést követő változások átvezetése
1.5	2005-12-30	Hatósági és külső ellenőrzéseket követő változások átvezetése
1.6	2006-07-20	Nemzeti Hírközlési Hatóság Hivatalának észrevételei szerinti javítások
1.7	2006-12-18	Ket.-es fejlesztésekhez és a 2006. évi Hatósági szemléhez kapcsolódó módosítások
1.71	2007-03-10	Hatósági észrevételek szerint valamint az rfc 3647szerint módosított változat
1.8	2009.03.01	A Hatóság észrevételei szerinti módosítás (HL-923-1/2009)
1.9	2010. 06. 20.	Hitelesítés szolgáltatás kivezetésével beállt változások átvezetése

Módosítást készítette: Domokos Zoltán	Technológia/ IT üzemeltetési igazgatóság	Senior biztonsági szolgáltatási menedzser
Ellenőrizte: Dr. Barczy Gergely	Csoport Központ / Vállalati üzletágat támogató jogi osztály	Szakértő
Jóváhagyta: Hári Krisztián Péter	Technológia/ IT üzemeltetési igazgatóság	IT biztonsági osztály mb. vezetője

TARTALOMJEGYZÉK

1 Bevezetés

1.1 Áttekintés

1.1.1 A Szabályzat

Ez a szabályzat a **Magyar Telekom Nyrt.** (ebben a dokumentumban: Szolgáltató) minősített időbélyegzés szolgáltatás tevékenységével kapcsolatos részletes eljárási és működési szabályokat tartalmazza.

A Szabályzat célja, hogy összefogja azokat a dokumentumokat és információkat, melyeket a Szolgáltatóval valamilyen módon kapcsolatba kerülő feleknek (elsősorban a végfelhasználóknak) a minősített időbélyegzés szolgáltatással kapcsolatosan tudni érdemes. A Szabályzat biztosítja a Szolgáltató működésének átláthatóságát, s lehetővé teszi annak megállapítását, hogy a Szolgáltató gyakorlata, illetve az időbélyegzés szolgáltatás keretében kiadott időbélyeg mennyiben felel meg a felhasználói és törvényes elvárásoknak. A Szabályzat segítségével az időbélyegzés szolgáltatás megrendelői és elfogadói egyértelműen megállapíthatják az időbélyeg **kezelésének módját**, a garantált **biztonságot** és a szolgáltatásra vonatkozó műszaki, üzleti, pénzügyi **garanciák**at és jogi **felelősségvállalások**at.

A Szabályzatban meghatározott időbélyegzés szolgáltatást a jelen szabályzat, az ÁSZF ([11]), a vonatkozó Időbélyegzési Rend, valamint az előfizetővel megkötött szerződés ([12]) együttesen szabályozzák {ld. 1.7 Hivatkozások}. Amennyiben az Időbélyegzési Rend, az ÁSZF, valamint jelen szabályzat bármely vonatkozásban ellentmondással vagy eltérő kikötéssel élnének, akkor a vonatkozó Időbélyegzési Rend előírásai tekintendők irányadónak.

1.1.2 A Szabályzat hatályai

A Szabályzat tárgyi hatálya

A Szabályzat tárgyi hatálya az {1.1.4 **Szolgáltatások**} alfejezetben ismertetett **szolgáltatások** nyújtására és igénybevételére, illetve ezen szolgáltatásokkal kapcsolatos összes **objektum**ra és **tárgyi eszköz**re kiterjed.

A Szabályzat területi hatálya

A Szabályzat területi hatálya **Magyarország** teljes területe.

A Szabályzat időbeli hatálya

A Szabályzat határozatlan időre szól a címlapon feltüntetett jelen szabályzati verzióra érvényes **hatálybalépés dátumától** kezdődően. (A Szabályzat időbeli hatálya a szolgáltatás beszüntetésekor, illetve egy újabb szabályzati verzió hatályba lépésékor szűnik meg.)

A Szabályzat személyi hatálya

A Szabályzat személyi hatálya a teljes közösség {ld. **1.3 PKI szereplők**} minden egyes tagjára, természetes, jogi személyiségű illetve jogi személyiséggel nem rendelkező személyekre (szervezetekre) egyaránt kiterjed.

1.1.3 A szolgáltató

A Szabályzatban Szolgáltató alatt a Magyar Telekom Nyrt. által – a saját szervezetén belül – létrehozott **Magyar Telekom Időbélyegzés szolgáltatót** (időbélyegző szervezetet) kell érteni. A Szolgáltatót jogi értelemben a **Magyar Telekom Nyrt.** képviseli.

A Szolgáltató minősített szolgáltatókénti nyilvántartásba vételének napja: 2004. október 01.

A Szolgáltató (Magyar Telekom Nyrt.) adatai a következők:

Név:	Magyar Telekom Távközlési Nyilvánosan Működő Részvénytársaság
Cégjegyzékszám:	CG 01-10041928
Székhely:	1013 Budapest, Krisztina krt. 55.
Postacím:	1541 Budapest
Telefon:	+36-1-458 7346
Fax:	+36-1-458 7335
Honlap:	http://www.telekom.hu/

A Szolgáltató **alvállalkozókat** is megbízhat egyes feladatok elvégzésére. Az alvállalkozók tevékenységéért a Szolgáltató teljes felelősséggel tartozik.

1.1.4 Szolgáltatások

A Magyar Telekom Nyrt. tevékenységi köre – egyebek mellett – kiterjed az időbélyegzés szolgáltatásra és az ehhez kötődő fejlesztési és tanácsadási tevékenységekre.

Az **időbélyegzés-szolgáltatás** során a Szolgáltató az elektronikus dokumentumhoz időbélyegzőt kapcsol.

Az időbélyegzés-szolgáltatás bizonyítékot nyújt arról, hogy egy adatelem változatan formában létezett egy megadott időpontban (a **létezés** bizonyítéka). Ha az adatelemet az adatkérő azelőtt aláírta, mielőtt továbbította volna az időbélyegzés-szolgáltató számára, akkor az időbélyegzés-szolgáltatás bizonyítékul szolgál arra nézve, hogy az adott adatelem létezett és ezen entitás birtokában volt abban a bizonyos időpontban (a **birtoklás** bizonyítéka). Az időbélyegzés-szolgáltató, mint harmadik fél megbízhatóan gondoskodik az időbélyegzés-szolgáltatásról.

A Szolgáltató által nyújtott időbélyegzés-szolgáltatás hozzákapcsolható aláírással ellátott elektronikus dokumentumhoz, továbbá aláírással nem ellátott állományok esetében is használható.

1.1.5 Szabványok és előírások

A Szabályzat tartalmi vonatkozásokban eleget tesz az [1], [2], [3] és [4] szerinti hazai jogszabályok előírásainak, kapcsolódó rendeleteinek és ajánlásainak. {Id. 1.7 **Hivatkozások**}.

Jelen szabályzathoz kapcsolódó időbélyeg felhasználásának joghatásairól a minősített időbélyegzés szolgáltatásra vonatkozó **Általános Szerződési Feltételek** (ÁSzF) című dokumentum előírásai is rendelkeznek, amely megtalálható a Szolgáltató honlapján a http://www.t-systems.hu/nagyvallalatok/hitelesites_szolgaltatasok/idobelyegzes_szolgaltatas .

1.1.6 Időbélyegzés-szolgáltatás

Az Eat 2.§ 16. alapján az időbélyegző: elektronikus dokumentumhoz végérvényesen hozzárendelt vagy azzal logikailag összekapcsolt olyan adat, amely igazolja, hogy az elektronikus dokumentum az időbélyegző elhelyezésének időpontjában változatlan formában létezett

Az időbélyegzés szolgáltatás keretében Szolgáltató az elektronikusan aláírt elektronikus dokumentumhoz időbélyegzőt kapcsol.

Az időbélyegzés-szolgáltatás bizonyítékot nyújt arról, hogy egy adatelem változatlan formában létezett egy megadott időpontban (a **létezés** bizonyítéka). Ha az adatelemet az adatkérő azelőtt aláírta, mielőtt továbbította volna az időbélyegzés-szolgáltató számára, akkor az időbélyegzés-szolgáltatás bizonyítékul szolgál arra nézve, hogy az adott adatelem létezett és ezen entitás birtokában volt abban a bizonyos időpontban (a **birtoklás** bizonyítéka). Az-időbélyegzés-szolgáltató, mint harmadik fél megbízhatóan gondoskodik az időbélyegzés-szolgáltatásról.

A szolgáltatáshoz kétféle tevékenység köthető:

- maga az **időbélyegzés-szolgáltatás**, amelyet a Szolgáltató minősített időbélyegzés-szolgáltatásként (előfizetéses alapon) nyújt ügyfeleinek.
- a szolgáltatást biztosító menedzsment folyamatok - **időjel ellátás**

Az időbélyegek használata során **kétféle alapműveletet** kell elvégezni:

- **időbélyegzést** (folyamatot), amely az adatokat időértékekkel kapcsolja össze kriptográfiai eszközök segítségével és
- **időbélyeg-ellenőrzést** (folyamatot), amely kiértékeli ezeknek az összekötéseknek a megfelelőségét.

Az időbélyegzés-szolgáltatás során a Szolgáltató (bizonyíthatóan) nem ismeri meg az időbélyegzett dokumentum tartalmát, és csak az abból képzett lenyomatot kezeli.

A Szolgáltató két hozzáférési módot ajánl az időbélyegzés-szolgáltatáshoz:

- az első általában egyedi – dedikált – hozzáférés, melyen jellemzően a nagy forgalmú ügyfelek részére szolgáltat[1],
- a második az Internet alapú hozzáférés, mellyel a lehető legszélesebb felhasználói körre kiterjeszthető a szolgáltatás.

A Szolgáltató időbélyegző infrastruktúrája pontosság és biztonság tekintetében **megfelel** az Eat. valamint a 3/2005 IHM rendelet vonatkozó előírásainak.

1.2 A dokumentum neve és azonosítója

Jelen szabályzat neve: **A Magyar Telekom Minősített Időbélyegzés-szolgáltatás Szolgáltatási Szabályzata.**

A szabályzat rövid neve: **Magyar Telekom IBSzSz**, vagy egyszerűen csak IBSzSz, (ebben a dokumentumban még Szabályzat).

A **Szabályzat** az alábbi adatokkal azonosítható[2]:

Egyedi objektum-azonosító (OID): ..... a Szabályzat fedőlapján található

Verziószám: ..... a Szabályzat fedőlapján található

A hatályba lépés dátuma[3]: ..... a Szabályzat fedőlapján található

A Szabályzat hivatalos és aktuális verziója a Szolgáltató elektronikus aláírásával ellátva megtalálható és letölthető a Szolgáltató internetes honlapjának következő oldalról:

http://www.t-systems.hu/nagyvallalatok/hitelesites_szolgaltatasok/idobelyegzes_szolgaltatas

[1] Ez bizonyos technikai korlátozásokat jelent, például megkövetelheti a *bérelt vonali* kommunikációs csatornák vagy egyéb egyedi megoldásokhasználatát.

[2] A 3/2005. (III. 18.) IHM rendelet 1. számú mellékletének megfelelően

[3] A *Szabályzat* aktuális verziójára vonatkozik.

1.3 PKI szereplők

A **Szolgáltató** jelen szabályzatban tárgyalt szolgáltatásaihoz tartozó közösség (a továbbiakban: **Közösség**) az alábbiakból áll.

1.3.1 Időbélyegző szervezet

A Szolgáltató – a saját szervezetén belül, az IT Üzelmeltetési Igazgatóság keretében – időbélyegző szervezetet működtet (Időbélyegző Szervezet), melynek feladata a szolgáltatásokhoz kapcsolódó rendszerek üzemeltetése, az időbélyegzés szolgáltatások nyújtása.

A Szervezet a timestamp@telekom.hu elektronikus levélcímen érhető el.

Az Időbélyegző Szervezet feladatai az alábbiak:

- A minősített időbélyegző rendszer üzemeltetése,
- A Magyar Telekom Gyökér hitelesítő működtetése,
- Szolgáltatói tanúsítványok és visszavonási listák közzététele,
- ügyfélszolgálati teendők: a felhasználókkal való kapcsolattartás és további menedzsment feladatok ellátása.

Az Időbélyegző Szervezet a feladatait a Szabályzat előírásainak megfelelően végzi. Az aktuális ügyek kezelését interneten és telefonon keresztül, illetve (az ügyfélszolgálaton) személyes közreműködéssel látja el.

A Minősített Időbélyegző Szervezet elérési adatai a következők:

Név:	Magyar Telekom NyRt./ Minősített Időbélyegző Szervezet
Cím:	1117 Budapest Magyar tudósok körút 9.
Telefon:	+36-1- 481-7447
Fax:	+36-1- 481-7455
Postacím:	1541 Budapest
Honlap:	http://www.t-systems.hu/nagyvallalatok/hitelesites_szolgaltatasok/idobelyegzes_szolgaltatas
E-levélcím:	timestamp@telekom.hu

Az Időbélyegző Szervezet munkanapokon **8 és 16 óra között** tart nyitva, de egyes napokon ettől eltérő nyitvatartási időpont is lehetséges. Hibabejelentéssel, valamint időbélyegzés kérésre jogosító athentikációs tanúsítvány visszavonási szolgáltaással kapcsolatos szolgáltatás a fenti munkaidőn túl elérhető az alábbi telefon, ill. faxszámon:

24 órás ügyelet telefonszáma: +36-30-444-17-31

Az Időbélyegző Szervezet aktuális adatai a Szolgáltató fenti internetes honlapján megtekinthetők.

1.3.2 Előfizetők, érintett felek

A Szolgáltató által nyújtott szolgáltatások végfelhasználói az alábbiak lehetnek:

- előfizető, aki az időbélyegzés-szolgáltatást Szolgáltatóval kötött szerződés alapján igénybe veszi,
- az érintett fél.

Az **előfizető** olyan tetszőleges természetes vagy jogi személy, vagy jogi személyiséggel nem rendelkező szervezet lehet, aki/amely elfogadja a Szolgáltató szabályzataiban meghatározott kötelezettségeket, és aki (eltérő megállapodás hiányában) fizet a szolgáltatásért.

Az előfizető szerződéses viszonyban áll a Szolgáltatóval a vonatkozó Időbélyegzés Szolgáltatói Szerződésben (továbbiakban: ISzSz) [12], jelen IBSzSz, Magyar Telekom Időbélyegzés-szolgáltatás Általános Szerződési Feltételek (továbbiakban: ÁSZF) [11] és a TSP [13] dokumentumokban foglaltak szerint. A Szolgáltató az előfizetővel elsősorban az Időbélyegző Szervezeten keresztül tart kapcsolatot. Előfizető az időbélyegzés-szolgáltatást kizárólag a TSP-ben és ISzSz-ben meghatározott módon és célra veheti igénybe.

Az **érintett_fél** természetes vagy jogi személy, vagy jogi személyiséggel nem rendelkező szervezet lehet, a Közösség olyan tagja, aki az elektronikus dokumentum fogadója és egy hitelesített időpontra hagyatkozva jár el az aláírás és/vagy az időbélyeg hitelességének ellenőrzésekor.

A Szolgáltató szabályzatai semmilyen formában sem korlátozzák az érintett felek körét.

1.3.3 Egyéb szereplők

Egyéb szereplőként meg kell említeni:

- Magyar Telekom NyRt. / Technológia / Üzemeltetés és fenntartási ig. NGN alkalmazás üzemeltetési osztályát, mint az időjel ellátó rendszer üzemeltetőjét, aki ezt a tevékenységét az Időbélyegző Szervezet részére végzi
- A Szabályzat szerinti szolgáltatással kapcsolatban illetékes fogyasztóvédelmi felügyelőséget, melynek adatai a következők:

  NFH Közép-magyarországi Regionális Felügyelősége

  1052 Budapest, Városház u. 7.
  1364 Budapest, Pf. 270.
  tel.: +361 318 2681
  fax: +361 318 1639

1.4 A Szolgáltatási Szabályzat adminisztrálása

1.4.1 Adminisztrációért felelős szervezet és kapcsolattartó személy

A **Szolgáltató** – szervezetén belül – olyan szervezeti egységet működtet, amely az időbélyegzéssel kapcsolatos szolgáltatásokhoz elengedhetetlen szabályozási feladatokat látja el, beleértve elsősorban a jelen szabályzat valamint az egyéb nyílvános[4] szabályzatok (ÁSZF, Időbélyegzési Rend) el(ő)készít(tet)ésével, egyeztetésével, kiegészítésével, aktualizálásával, jóváhagyatásával és megjelentetésével kapcsolatos **összes feladatot**.

A **szabályozási szervezet** adatai, és azon belül a fenti tevékenységgel megbízott szolgáltatási menedzser elérési adatai a következők:

Név:	Magyar Telekom Nyrt. / Technológia / IT üzemeltetési igazgatóság IT biztonsági osztály
Cím:	1117 Budapest Magyar tudósok körút 9.
Telefon:	+36 1 481-7447
Mobil:	+36-30-444-17-31
e-Mail:	timestamp@telekom.hu
Fax:	+36 1 481-7455
Postacím:	1541 Budapest

A szabályzatokra vonatkozóan a hatósággal (NHH) történő hivatalos kapcsolattartás a Magyar Telekom Csoport Központ – Operatív szabályozási osztály feladata.

1.4.2 A Szolgáltatási Szabályzat elfogadási eljárása

A szabályozási tevékenységgel megbízott szolgáltatási menedzser összegyűjti a Szabályzatra (vagy az egyéb nyílvános szabályzatra) vonatkozó észrevételeket illetve változtatási igényeket, majd elkészít(tet)i a módosított szabályzattervezetet, melyet ezt követően elküld egyeztetésre. Az esetleges észrevételekkel kiegészített szabályzatot ellenőrzésre és jóváhagyásra megküldi az érintetteknek. Az ellenőrzések és jóváhagyások tényét az érintettek[5] aláírásukkal igazolják. Ezt követően a termékmenedzser eleget tesz a belső és külső (hatósági és ügyfelek érintő) tájékoztatási kötelezettségeknek, az 1.4.3 fejezet szerint.

A szabályzatok elrendelése és életbe léptetése a Szolgáltató felső vezetőségének jóváhagyásával, az erre vonatkozó belső utasítás alapján történik.

[4] A belső szabályozások kezelésével kapcsolatos felelősök külön belső utásításban vannak rögzítve

[5] Külön belső utasításban rögzítettek

Jelen szolgáltatási szabályzat Időbélyegzési Rendnek való megfelelőségét közzététel előtt Szolgáltató megvizsgálta. A vizsgálatot külső független szakértő is elvégzi évente rendszeresen végzett auditja során.

Ezen felül a Szabályzat megfelelőségét a vonatkozó törvények, jogszabályok, valamint szakmai előírások tekikntetében a Hatóság is megvizsgálja a szabályzat nyílvántartásba vételét (illetve hatályba lépését) megelőzően.

1.4.3 Szabályzat változtatási eljárások

Egy időszak alatt összegyűlt változási igényeket Szolgáltató kötegelve szerkeszti új szabályzati változattá, törekedve arra, hogy új szabályzatot csak a lehető legritkábban kelljen kibocsátania.

Értesítés nélkül, illetve értesítéssel változtatható elemek

A szabályzatok bármely részének (elemének) módosítása esetén az erről szóló értesítés és tájékoztatás a következő alfejezet szerint történik. Nincsenek olyan elemek, melyeket Szolgáltató értesítés nélkül változtatna meg jelen szabályzatában (illetve nyílvános szabályzataiban).

Szabályzati objektum-azonosítót vagy -mutatót változtató módosítások

Jelen szabályzat és az időbélyegzés szolgáltatással kapcsolatos egyéb nyílvános szabályzatok módosított változatai mindig új verziószámmal kerülnek nyilvánosságra. A szabályzatok módosítása a szabályzatok objektum-azonosítóját is módosítja.

A verziószám egy tizedes értékkel növekszik (pl. 1.6-ot követi az 1.7-es), az objektum-azonosítónak pedig az utolsó számjegye növekszik egy értékkel. (pl. 1.3.6.1.4.1.17835.7.1.2.8.2.1.13.3.4 –et követi az 1.3.6.1.4.1.17835.7.1.2.8.2.1.13.3.5).

- Közzétételi és tájékoztatási elvek

A szabályzat közzététele és nyílvántartásba vétele

Szolgáltató nyílvános szabályzatainak a változásokkal egybeszerkesztett új verzióját, annak hatályba lépését megelőzően **30 nappal** benyújtja azt a Hatóság részére, nyílvántartásba vétel céljából.

Amennyiben nem érkezik észrevétel, a szabályzatot Szolgáltató, mint hatályos dokumentumot helyezi el nyilvános internetes honlapján, ezzel egyidejűleg a korábbi változatot elhelyezi a „hatályát vesztett szabályzatok" közé.

A szabályzatban nem tárgyalt elemek

A Szolgáltató nyilvános szabályzataiban csak azon eljárásait hozza nyilvánosságra, melyek ismerete a szolgáltatás biztonságát nem veszélyezteti. Szolgáltató több belső biztonsági és egyéb szabályzattal, operatív szintű előírással rendelkezik, melyeket bizalmasan kezel (jelen szolgáltatási szabályzat több ilyet is megemlít). A 8 fejezetben leírt tanúsítási eljárások ezeket a dokumentumokat is vizsgálják.

1.5 Meghatározások

A Szolgáltató a dokumentumban szereplő fogalmakat az alábbi értelemben használja:

Fogalom	Meghatározás (magyarázat)
aktivizáló adatok	a kriptográfiai modul működtetéséhez szükséges adatok, melyeket védeni kell (pl. PIN kód, jelmondat vagy manuálisan birtokolt kulcs-részlet)
elektronikus dokumentum	elektronikus eszköz útján értelmezhető adategyüttes
előfizető	Időbélyegzés esetén maga az igénybevevő.
érintett fél	az elektronikus dokumentum fogadója, aki egy adott időbélyegzőrehagyatkozva jár el
fogadó fél (elfogadó fél)	az elektronikus dokumentum fogadója, aki egy adott időbélyegzőrehagyatkozva jár el
Időbélyegzés szolgáltatási szabályzat	Az Eat. [1] 6. § (1) bekezdése szerinti szolgáltató tevékenységével kapcsolatos részletes eljárási és egyéb működési szabályokat tartalmazó szabályzat
időbélyeg (időbélyegző)	elektronikus dokumentumhoz végérvényesen hozzárendelt, vagy azzal logikailag összekapcsolt olyan adat, amely igazolja, hogy az elektronikus dokumentum az időbélyegző elhelyezésének időpontjában változatlan formában létezett
időbélyegzés-szolgáltató	olyan szolgáltató, amely az időbélyegzés szolgáltatást végzi
kriptográfiai kulcs	olyan kriptográfiai transzformációt vezérlő egyedi jelsorozat, amelynek ismerete a kriptográfiai transzformáció elvégzéséhez, különösen az elektronikus aláírás előállításához vagy ellenőrzéséhez szükséges
tanúsítvány	Időbélyegzés szolgáltatás esetén az időbélyegzők szolgáltatói tanúsítv ányai.
tanúsítvány visszavonási állapot közzététele	Időbélyegzés szolgáltatás esetén információ nyújtása az elfogadó fél számára az időbélyegző tanúsítványok visszavonásáról. A szolgáltatás lehet valós idejű, vagy az információk előre meghatározott időközönkénti aktualizálásán kell alapulnia.
tanúsítvány visszavonási lista	Időbélyegzés szolgáltatás esetén valamely okból visszavont, azaz érvénytelenített időbélyegző tanúsítványok azonosítóit tartalmazó elektronikus lista, melyet a szolgáltató bocsát ki
Visszavonási nyilvántartások (tanúsítvány visszavonási	Időbélyegzés szolgáltatás esetén nyilvántartások a felfüggesztett, illetőleg a visszavont időbélyegző tanúsítványokról, amelyek tartalmazzák legalább a

nyilvántartás)	felfüggesztés vagy visszavonás tényét, és a felfüggesztés vagy visszavonás időpontját
időbélyegzési rend	olyan szabálygyűjtemény, amelyben egy szolgáltató, igénybe vevő vagy más személy (szervezet) valamely időbélyegző felhasználásának feltételeit írja elő igénybe vevők valamely közös biztonsági követelményekkel rendelkező csoportja, illetőleg meghatározott alkalmazások számára
végfelhasználó	az előfizető, az elfogadó fél, valamint az érintett fél

1.6 Rövidítések és jelölések.

A dokumentumban az alábbi jelölések és rövidítések szerepelnek:

- [ ] jelek között a dokumentumokra történő hivatkozások számai szerepelnek,
- { } jelek között egy dokumentum adott fejezetére / alfejezetére történő hivatkozások szerepelnek.

1.7 Hivatkozások

A Szolgáltató a jelen dokumentumban az alábbi dokumentumokra hivatkozik:

[1] 2001. évi XXXV. törvény az elektronikus aláírásról

[2] 2/2002. (IV. 26) MeHVM irányelve a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről

[3] 3/2005. (III.18.) IHM rendelet az elektronikus aláírásokkal kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről

[4] A Nemzeti Hírközlési Hatóság Hivatalának az elektronikus aláírással kapcsolatos szolgáltatások nyújtása során alkalmazható biztonságos kriptográfiai algoritmusok és paramétereik meghatározása tárgyában hozott HL-21917-12/2008 számú határozata.

[5] ISO 3166

[6] FIPS PUB 140-2 (1994. január 11.): "Kriptográfiai modulok biztonsági követelményei"

[8] International Telecommunication Union X.509 “Információ technológia – Nyílt rendszerek kapcsolódása - Könyvtár: Nyilvános kulcs és attribútum tanúsítvány keretrendszer”

[9] RFC 5280 (Internet X.509 Nyilvános kulcsú infrastruktúra – tanúsítvány és tanúsítvány visszavonási lista profil)

[10] RFC 3647 (Internet X.509 Nyilvános kulcsú infrastruktúra – Hitelesítési Rend és Szolgáltatási Szabályzat keretrendszer)

[11] Minősített Időbélyegzés szolgáltatások - Általános Szerződési Feltételek (ÁSzF)– Magyar Telekom Nyrt.

[12] Magyar Telekom Minősített Időbélyegzés szolgáltatás Szolgáltatói Szerződése – röviden Szolgáltatói Szerződés (ISzSz)

[13] Magyar Telekom Minősített Időbélyegzés-szolgáltatás Időbélyegzési Rendje – röviden (TSP)

2 Közzétételre és tárolásra vonatkozó felelősségek

A Szolgáltató a szolgáltatói tanúsítványokat –Gyökér hitelesítő és időbélyegző tanúsítványok- valamint a Gyökér hitelesítő visszavonási listáját nyilvánosan elérhető weblapján teszi elérhetővé. (http://www.t-systems.hu/nagyvallalatok/hitelesites_szolgaltatasok/idobelyegzes_szolgaltatas)

2.1 Adatbázisok

Adatbázisok alatt a Szolgáltató honlapján közzétett adatokat értjük. Itt a szolgáltatásokra vonatkozó kikötéseket, feltételeket, szabályzatokat; valamint a rendkívüli információkat is közzéteszik. A Szolgáltató weboldala HTTP lekérdezésekkel érhető el.

A **weboldal** elérhetőségét a Szolgáltató folyamatosan (az év minden napján, **0-24 óra** között) biztosítja, a karbantartáshoz szükséges idők kivételével. A Szolgáltató a tervezett karbantartásokat munkaidőn kívüli időszakokra ütemezi, és ezekről a karbantartás megelőzően **24 órával** értesítést tesz közzé a honlapján.[6]

2.2 Az időbélyegekre vonatkozó információk közzététele

Kikötések és feltételek közzététele

A Szolgáltató szerződéses feltételeit és szabályzatait – és ezek részeként az időbélyegzésre vonatkozó információkat - elektronikus formában (MS-Word és/vagy Adobe Acrobat formátumokban) hozza nyilvánosságra az internetes honlapjának oldalain.

Elérhetőség: http://www.t-systems.hu/nagyvallalatok/hitelesites_szolgaltatasok/idobelyegzes_szolgaltatas

A dokumentumok korábban érvényben lévő változatai is megtalálhatóak itt az aktuális verziók mellett. A dokumentumok nyomtatott változatai semmilyen formában sem tekinthetők hivatalos példánynak vagy hiteles másolatnak.

Rendkívüli információk közzététele

A **Szolgáltató** a következő eseményekről hirdetést jelentethet meg egy országos terjesztésű napilapban:

- új szolgáltatás beindítása,
- valamely szolgáltatás tervezett beszüntetése vagy tartós (**24 órát** meghaladó) szüneteltetése,

[6] ld. [3] 17. §

- tevékenységének befejezése, ld. még 5.7 fejezetet.

Tanúsítványok nyilvánosságra hozatala

A Szolgáltató az általa működtetett **hitelesítő egységek és az időbélyegző eszközök tanúsítványait** a következő módszerekkel teszi közzé:

- Az időbélyeg aláíró kulcs tanúsítványát és a rá vonatkozó – Magyar Telekom gyökér Hitelesítő által kiadott - tanúsítvány visszavonási listát a honlapján keresztül teszi közzé.

A tanúsítványok visszavonásának és felfüggesztésének nyilvánosságra hozatala

A Szolgáltató az általa működtetett Időbélyegző egységek tanúsítványaival kapcsolatos **állapot-információ**kat a következő módszerel teszi közzé:

- Az Időbélyegző egységek tanúsítványainak állapotváltozását a Szolgáltató weboldalán hozza nyilvánosságra.

2.3 A közzététel gyakorisága

Kikötések és feltételek közzétételi gyakorisága

A Szabályzattal kapcsolatos új verziók közzététele az 1.4.3 alfejezetben ismertetett eljárásoknak megfelelően történik.

A Szolgáltató szükség szerinti gyakorisággal bocsátja ki az egyéb szabályzatait és szerződéses feltételeit, illetve az újabb változatokat.

Rendkívüli információk közzétételi gyakorisága

A Szolgáltató a rendkívüli információkat közzéteszi a jogszabályi előírásoknak megfelelően, illetve ennek hiányában akkor, amikor arra szükség van.

2.4 Az adatbázisok elérésének szabályozása

A Szolgáltató által közzétett kikötések és feltételek, a rendkívüli események, az időbélyegző szerver tanúsítványok és állapot információk nyilvános információk. Olvasás illetve lekérdezés céljából bárki korlátozás nélkül elérheti ezeket az információkat, a közzététel sajátosságainak megfelelően, Interneten keresztül.

A Szolgáltató által közölt információkat kizárólag csak a Szolgáltató egészítheti ki, törölheti vagy módosíthatja. A Szolgáltató különböző védelmi mechanizmusokat működtet az információk jogosulatlan módosításának.

3 Azonosítás és hitelesítés

3.1 Megnevezési konvenciók

3.1.1 Márkanevek elismerése, azonosításuk és szerepük

A Szolgáltató a szolgáltatása során bejegyzett védjegyet nem alkalmaz.

4 Működésre vonatkozó követelmények – időbélyegzés

A Szolgáltató minősített időbélyeg szolgáltatást jelen szabályzat előírásai alapján nyújt.

4.1 Időbélyeg szolgáltatás igénylése

Időbélyegzés szolgáltatásra vonatkozó igényt benyújthat, aki a Szolgáltató honlapján közzétett Általános Szerződési Feltételeket és jelen Szolgáltatási Szabályzatot meismeri és elfogadja, valamint az ott megjelentetett Megrendelő lapot kitölti és eljuttatja az Időbélyegzés Szolgálatás ügyfélszolgálat címére.

Amennyiben az igényelő kéri, a szolgáltatás nyilvános dokumentumainak helyszíni tanulmányozására is lehetősége van, valamint szóban történő tájékoztatást is kaphat a szolgáltatással kapcsolatban.

Az Időbélyegzés Szolgáltatási Szerződés és Megrendelőlap valamint a Szolgáltató szabályzatai és termékismertetői megtalálhatók a Szolgáltató honlapján is, így előzetesen is áttekinthetők és kitölthetők.

A szolgáltatási szerződés ezt követő aláírásával születik meg szolgáltató és igénylő között az előfizetői szerződés, az **Általános Szerződési Feltételek** (ÁSzF) rendelkezéseinek megfelelően.

Az igénylő aláírásával egyúttal nyilatkozik arról is, hogy Szolgáltató feltételei és kikötései, saját kötelezettségei vonatkozásában tájékoztatást kapott, azokat elfogadja.

Az **Időbélyegzés Szolgáltatási szerződés** és **Megrendelőlap tartalma** ezt követően Szolgáltató nyilvántartásába kerül mind elektronikus, mind papír formában.

Minősített időbélyeg-szolgáltatást természetes személy, vagy szervezet egyaránt igényelhet, személyesen a Szolgáltató székhelyén (Ld:1.5), telefonon, e-mail-ben, levélben.
Az igénybevételre két módon kerülhet sor:

- a Szolgáltatóval történő eseti megállapodás, vagy
- a Szolgáltató által nyújtott ajánlatok, csomagok elfogadott megrendelése keretében.

Az igénylés Szolgáltatóhoz való beérkezésétől számított 15 napon belül a Szolgáltató felveszi a kapcsolatot az igénylővel, s az ajánlatot elfogadja, az igénylőt felszólítja hiánypótlásra, pontosításra, vagy a Szolgáltató döntése szerint az ajánlatot visszautasítja, amennyiben az Igénylő a hiánypótlási, pontosítási felszólításnak 15 napon belül nem tesz eleget, a Szolgáltatóval szemben a Szolgáltatás korábbi igénybevételéből eredően díjtartozása van, vagy amennyiben a szolgáltatás nyújtásával más ügyfelek kiszolgálása veszélybe kerül.

4.2 Az időbélyeg szolgáltatás teljesítése

Szolgáltató az RFC 3161 szabványon alapuló időbélyeg kérelmeket fogad és időbélyeg válaszokat ad. Az időbélyeg kérelmek előállításához illetve az időbélyeg válaszok fogadásához, ellenőrzéséhez szükséges programokkal, program modulokkal, infrastruktúrával a Felhasználónak kell rendelkeznie.

A Szolgáltató a 3/2005 (III.18.) IHM rendelet 17.§ (1) alapján biztosítja az időbélyegzés szolgáltatás folyamatos rendelkezésre állását – éves szinten 99,5% rendelkezésre állást vállal. Az időbélyegzés szolgáltatás eseti szolgáltatás kiesése nem haladhatja meg a 3 óra időtartamot.

A Szolgáltató időbélyegzés-szolgáltatás nyújtása során biztosítja, hogy az időbélyeg válasz – az időbélyegzéssel összefüggésben hozzáadottaktól eltekintve – ugyanazokat az adatokat tartalmazza, amelyeket a kérelem tartalmazott. Az időbélyegzés szolgáltatás során a Szolgáltató - a technológia jellegéből adódóan - nem ismeri meg az időbélyeggel ellátott dokumentum tartalmát, csak az abból képzett lenyomatot.

Felhasználó vállalja a szolgáltatási díjak megfizetését, valamint elfogadja, hogy a szolgáltatás díjának megfizetését nem tagadhatja meg arra való hivatkozással, hogy érdekkörébe tartozó területen és eszközökön keresztül jogosulatlan személy vette igénybe a jelen szerződés tárgyát képező szolgáltatást.

4.3 Minősített Időbélyeg-szolgáltatás joghatása

Az [1] Törvény alapján, „*amennyiben az időbélyegzést olyan szolgáltató végezte, amely az időbélyegzéskor e szolgáltatás tekintetében a szolgáltatók nyilvántartásában minősítettként szerepelt és az időbélyegző ellenőrzésének eredményéből más nem következik, az ellenkező bizonyításáig vélelmezni kell, hogy a dokumentumban foglalt adatok az időbélyegző elhelyezése óta változatlan formában léteztek*”.

4.4 Az időbélyeg szolgáltatás igénybevételének vége

Amennyiben a szolgáltatásra vonatkozó szerződést Előfizető fel kívánja mondani a szerződés lejárata előtt, ezt írásban vagy faxon kell bejelenteni az Időbélyegző Szervezet részére.

5 Elhelyezési, irányítási és működtetési előírások

Szolgáltató gondoskodik arról, hogy kellő, az elismert szabványoknak megfelelő fizikai, eljárásbeli és személyzeti biztonsági óvintézkedések, valamint az ezeket érvényre juttató adminisztratív és irányítási eljárások kerüljenek alkalmazásra.

5.1 Fizikai előírások

Szolgáltató gondoskodik arról, hogy a kritikus szolgáltatásokhoz történő fizikai hozzáférés ellenőrzött legyen, és a kritikus szolgáltatások nyújtásához szükséges eszközök használatából eredő kockázatot minimalizálják.

A fizikai óvintézkedések célja a Szolgáltató információira és fizikai körleteire irányuló jogosulatlan hozzáférés, károkozás és illetéktelen behatolás megakadályozása.

A biztosított védelem arányban áll a Szolgáltató által végzett kockázat elemzésben megállapított kockázatokkal.

A leginkább veszélyeztetett szolgáltatásokat az Időbélyegző Szervezet védett számítógép termeiben valósítják meg. Ezek a számítógép termek speciálisan erre a célra lettek tervezve és kialakítva, és tervezésénél több különböző védelmi szempont (a telephely elhelyezése és szerkezeti felépítése, a fizikai hozzáférés /beléptetés ellenőrzése és felügyelete/, áramellátás, légkondicionálás, beázás és elárasztódás elleni védekezés, tűzmegelőzés és tűzvédelem, adathordozók tárolása, stb.) érvényesítésére is sor került.

Az Időbélyegző Szervezet valamennyi kritikus szolgáltatását biztonsági körletben valósítja meg, és az ehhez szükséges valamennyi eszközt a biztonsági körletek részét képező védett számítógép termekben helyezte el. A termek túlmelegedés elleni védelmére kialakításra kerül helyiségenként elektromos hőérzékelő berendezés mely a kritikus hőmérséklet elérése előtt riasztási jelzést továbbít a létesítmény épület-felügyeleti rendszeréhez. A helyiségekben gyengeáramú szükség-megvilágítás került telepítésre mely egyben a menekülési útvonalat is jelöli. A padló burkolata csúszásmentes, antisztatikus és terhelő nyomásnak ellenálló.

Az Időbélyegző Szervezet számítógép terme önálló biztonsági körletnek minősül. Ezen belül valósulnak meg a kritikus szolgáltatások, és itt került elhelyezésre az ezekhez szükséges valamennyi eszköz.

5.1.1 A telephely elhelyezése és szerkezeti felépítése

Az Időbélyegző Szervezet védett számítógép terme a befogadó épület területén elkülönítetten került kialakításra. Az elkülönített biztonsági körlet három egymásba nyíló, összesen egy bejárattal rendelkező ablaktalan helyiségből áll, melyben elhelyezésre kerültek a számítógépszerverek és az üzemeltetésükhöz szükséges teljes infrastruktúra.

5.1.2 Fizikai hozzáférés

Az Időbélyegző Szervezet védett számítógép terme úgy lett kialakítva, hogy illetéktelen személyek egyáltalán ne juthassanak be, a biztonsági őrség viszont rövid idő alatt meg tudja közelíteni riasztás esetén. A biztonsági körletnek nincs ablaka, a bejárati ajtón kívül csak falbontással lehet behatolni ide. A biztonsági körlet integráltan megvalósított behatolás jelző (riasztó) és beléptető (ujjlenyomat azonosító) rendszerrel van ellátva. A biztonság növelése érdekében egy falbontás érzékelő riasztó rendszer került telepítésre és beüzemelésre.

A védett számítógép termekbe az ott dolgozó bizalmi munkakört betöltő munkatársakon kívül más személyek (pl. karbantartók, takarítók) csak külön felhatalmazással és kísérettel léphetnek be.

5.1.3 Áramellátás, légkondicionálás

Áramellátás

Az Időbélyegző Szervezet védett számítógép termeinek zavartalan áramellátása kiemelten fontos a folyamatos üzemeltetés biztosítása érdekében. A helyiségek betáplálására 3x60 amper tápellátás áll rendelkezésre, fáziselosztással, bemeneti zavarszűrűvel és érintésvédelemmel.

A következő védelmi megoldások együttese biztosított:

- szünetmentes energia ellátás a gépekbe szerelt UPS-egységek által,
- villamos zavar, villám és túlfeszültség védelem,

Az alkalmazott üzemmód pedig az alábbi:

- az üzemi táp kimaradása vagy csökkenése esetén a rendszer átkapcsol a tartalék tápra,
- ha a tartalék táp sem használható, akkor a rendszer fokozatosan leállítja a szervereket,

Zárlati leoldásra szelektív áramkörök segítségével a gépteremben több egymástól független működésű rendszer lett kialakítva a folyamatos üzemeltetés támogatására. A villamos zavar, villám és túlfeszültség védelem szempontjából a gépterem nagy értékű, kritikus szolgáltatásokat biztosító berendezései védve vannak a különböző vezetett és sugárzott villamos zavarok, villámok miatt bekövetkező túlfeszültség hatásai ellen:

- a rendszert külön mechanizmusok védik a villámok által keltett elektromágneses impulzusok (EMI) hatása ellen,

- az üzemeltetett berendezések a sugárzott elektromágneses zavarás elleni védelem mindkét elvárását teljesítik: egyrészt védettek az üzemelési környezetükben jelen levő hatások ellen, másrészt nem bocsátanak ki olyan zavaró elektromágneses jeleket, amely a környezetükben üzemelő többi berendezés működését zavarhatná.

Külön akkumulátoros szünetmentes tápegységek biztosítják az alábbi berendezések áramellátását áramszünet esetén:

- tűzjelző berendezés (24 órás üzemképességgel teljes áramszünet esetén),
- telefonközpont (6 órás áramszüneti üzemképességgel).

Légkondicionálás

Az Időbélyegző Szervezet védett számítógép terme hűtésigényének kiszolgálását helyiségenkénti levegő hűtését egy ipari klíma illetve 3 db tartalékként létesített split klíma biztosítja. Mivel a létesítmény föld-alatti, a friss levegő utánpótlásról, illetve elszívásról egy központi rendszer gondoskodik.

5.1.4 Beázás és elárasztás veszélyeztetettsége

Az Időbélyegző Szervezet biztonsági körleteinek kialakítása során figyelembe vették az elárasztás veszélyének minimalizálását. A biztonsági körletek teljes területe mentes a vizesblokkoktól, illetve a közelben nincs sem csatorna, sem vízvezeték. A biztonság növelése érdekében egy nedvességérzékelő riasztó rendszer került telepítésre és beüzemelésre.

5.1.5 Tűzmegelőzés és tűzvédelem

Az Időbélyegző Szervezet géptermét befogadó épületben a helyiségek védelmére kiépített tűzvédelmi rendszer működik.

A helyiségek tűzvédelmét egy tűzjelző és oltóközpont biztosítja. A tűzvédelmi jelzések az épület felügyeleti rendszerre kerültek beintegrálásra, mely a jelzéseket a Magyar Telekom Nyrt. 24 órás diszpécserszolgálatához továbbítja, ahol a szükséges intézkedéseket megteszik. Tűzriasztás esetén az épület-felügyeleti rendszer a légbefújást automatikusan leállítja.

A helyiségek bejáratát tűzgátló ajtó választja el a létesítménytől, így a kialakított termek önálló tűzszakaszt képeznek.

A kiépített tűzvédelmi rendszert (melynek fő elemei: füstérzékelő- és tűzjelző rendszerek, oltókapszulák) az illetékes tűzoltó parancsnokság engedélyezte.

5.1.6 Adathordozók tárolása

Az Időbélyegző Szervezet biztonsági körletében egy kódzáras tűzbiztos szekrény szolgál az adathordozók biztonságos tárolására. A szekrényben az Időbélyegző Szervezet mentési példányait tárolják {ld. 5.1.8 **A mentési példányok fizikai elkülönítése**}. Itt kerülnek elhelyezésre adminisztrálásához, üzemeltetéséhez szükséges adathordozók, ill. az üzemeltetési dokumentációk elektronikus formában.

5.1.7 Hulladék megsemmisítése és selejtezés

Az Időbélyegző Szervezet biztonsági körleteiben a bizalmas minősítésű adatokat tartalmazó elektronikus adathordozókat, még tartalmuk törlése után sem használják fel nem minősített adatok tárolására. A feleslegessé vált, bizalmas minősítésű adatokat tartalmazó adathordozókat fizikailag megsemmisítik:

- a papíralapú dokumentumokat zúzógéppel felaprítják,
- a hajlékony lemezeket (házából való kibontás után) zúzógéppel felaprítják,
- a merev lemezeket (a befogadó épületben központilag biztosított célberendezés felhasználásával) demagnetizálás után fizikailag összetörik.

5.1.8 A mentési példányok fizikai elkülönítése

Az Időbélyegző Szervezet biztonság-kritikus szolgáltatásaira vonatkozó adatok mentési példányait az Időbélyegző Szervezet biztonsági körletében és a Magyar Telekom Központi Katasztrófa adattárában (a továbbiakban: megőrzési hely) tárolják.

5.2 Eljárásbeli óvintézkedések

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

5.2.1 Bizalmi munkakörök

Szolgáltató a következő bizalmi munkaköröket határozza meg az alábbi felelősségkörökkel:

- biztonsági tisztviselő,
- rendszer (vagy központi) adminisztrátor,
- rendszeroperátor (rendszerüzemeltető),

- rendszervizsgáló,
- szolgáltató informatikai rendszeréért általánosan felelős vezető.

Az **Időbélyegző Szervezettel munkaviszonyban** álló, változó helyszínen dolgozó **biztonsági tisztviselők** általánosan felelnek:

- a különböző biztonsági óvintézkedések kidolgozásáért,
- a különböző biztonsági óvintézkedések rendszeres felülvizsgálatáért, a szükségessé váló módosítások kezdeményezéséért,
- a biztonsági óvintézkedések érvényre jutásáért, betartatásáért,
- az informatikai rendszerek biztonsági szintjének megőrzéséért (rendszeres auditok szervezésével).

Az **Időbélyegző Szervezettel munkaviszonyban** álló, változó helyszínen dolgozó **biztonsági tisztviselők** közreműködnek (egy másik, bizalmi munkakört betöltő társuk jelenlétében) az alábbi tevékenységeknél:

- a Szolgáltató időbélyegző szerver kulcsainak generálásánál,
- a Szolgáltató időbélyegző szerver kulcsainak (és annak összes másodpéldányának) megsemmisítésénél,

Az **Időbélyegző Szervezettel munkaviszonyban** álló **rendszeradminisztrátorok**:

- telepítik, konfigurálják és karbantartják az Időbélyegző Szervezet védett számítógép termében üzemeltetett megbízható rendszereket,
- beállítják a fenti megbízható rendszerek kezdeti hálózati konfigurációját,
- kezelik az Időbélyegző Szervezet állományába tartozó rendszeroperátorok vonatkozásában a rendszerhez való hozzáféréseket (account felvétele, jogosultságok beállítása, módosítása, kezdeti jelszó beállítása, a távozó, illetve munkakört váltó rendszeroperátorok hozzáférési jogainak azonnali megszüntetése),
- letöltik és installálják a felügyeletük alatt üzemeltetett operációs rendszerre és adatbázisra kiadott biztonsági javítócsomagokat, ezen keresztül gondoskodnak az informatika biztonsági szint folyamatos megőrzéséről,
- rendszeres időnként ellenőrzik az Időbélyegző Szervezet védett géptermében üzemeltetett informatikai rendszernek és információinak a sértetlenségét,
- gondoskodnak a rendszeroperátorok által végzett rendszermentések, illetve az Időbélyegző Szervezet rendszermentés másolatainak biztonságos tárolásáról,
- gondoskodnak a rendszermentésekről készített, elkülönítetten őrzendő másolati példányok megőrzési helyre történő szállításáról {ld. **5.1.8 A mentési példányok fizikai elkülönítése**} ,

- elvégzik az Időbélyegző Szervezet védett számítógép termében üzemeltetett megbízható rendszer hálózati konfigurációjának kezdeti beállítását,
- ellenőrzik (áttekintik és kiértékelik) és karbantartják (archiválják és törlik) az általuk felügyelt tűzfalak, behatolást detektáló rendszerek biztonsági naplóit,
- közreműködik az időbélyegző tanúsítványok generálásánál,
- authentikációs tanúsítványokat generál(tat)nak az előfizetők számára,
- gondoskodnak a tűzfalakra, behatolást detektáló rendszerekre kiadott biztonsági javítócsomagok letöltéséről, installálásáról, ezen keresztül a biztonsági szint naprakész megőrzéséről.

Az **Időbélyegző Szervezettel munkaviszonyban** álló **rendszeroperátorok** folyamatosan üzemeltetik az Időbélyegző Szervezet védett számítógép termében működő megbízható rendszereket, melynek során:

- authentikációs tanúsítványokat generál(tat)nak az előfizetők számára,
- közreműködik az időbélyegző tanúsítványok generálásánál,
- tanúsítványokat generál(tat)nak az Időbélyegző Szervezet számára,
- negyedévente archiválást végeznek,
- szükség esetén helyreállításokat hajtanak végre.

Az **Időbélyegző Szervezet állományába** tartozó **rendszervizsgáló**:

- ellenőrzi (áttekinti) és karbantartja (archiválja és törli) az Időbélyegző Szervezet védett számítógép termében működő megbízható rendszer biztonsági naplóit,
- szükség esetén az általa készített archívumokban keresést végez.

Valamennyi fent megnevezett bizalmi munkakört a munkaköri leírások dokumentálják.

A bizalmi munkakörökbe az Adatgazda nevezi ki Szolgáltató munkatársait, a biztonsági alapellenőrzés sikeres befejezése után {ld. **5.3.1 pont**}.

5.2.2 Az egyes feladatokhoz szükséges személyzeti létszámok

Általánosan teljesül a Szolgáltató egészére, hogy minden munkatárs csak a saját munkakörének megfelelő funkciókat aktivizálja.

Az Időbélyegző Szervezetnél az alábbi kettős felügyeletet igénylő **munkafolyamatok** vannak, amelyhez két bizalmi munkakört betöltő személy együttes jelenléte (és előzetes, sikeres hitelesítése) szükséges:

- a Szolgáltató TrustedTimeStamp szerverei HSM-jében használt nyilvános kulcsait tartalmazó **adathordozóknak** a Gyökér Hitelesítő Egységhez való továbbításánál, illetve az erre, a Gyökér Hitelesítő Egység által kibocsátott tanúsítvány visszaszállításánál. (megjegyzés: a szerverből két példány van, két külön HSM modullal).

Szolgáltató vonatkozó belső szabályzata meghatározza az egyes feladatokhoz szükséges személyzeti létszámokat is.

5.2.3 Az egyes munkakörökben elvárt azonosítás és hitelesítés

Az Időbélyegző Szervezet valamennyi bizalmi munkakört betöltő munkatársának azonosítása és hitelesítése a Magyar Telekom hatályos szabályzataiban rögzített eljárásokkal történik. Sikeres hitelesítés előtt egyetlen biztonság kritikus tevékenységet sem lehet végrehajtani.

5.2.4 Egymást kizáró munkakörök

Szolgáltató gyakorlatában a bizalmi munkakörök között **személyi átfedések nincsenek**, minden személy csak egy bizalmi munkakört tölt be, az erre vonatkozó jogszabályi[7] előírásoknak megfelelően.

5.3 Személyzetre vonatkozó előírások

A személyzetre vonatkozó óvintézkedések célja az emberi hibák, lopás, csalás és a lehetőségekkel való visszaélés kockázatának csökkentése.

Ennek érdekében Szolgáltató külön a személyzetre vonatkozó belső előírással rendelkezik, és ezek szerint jár el, így a személyi biztonsággal már a felvételi szakaszban foglakozik, beleértve a szerződések megkötését, illetve azok alkalmazás során történő ellenőrzését.

Valamennyi bizalmi munkakör esetén a felvételre jelentkezőket biztonsági ellenőrzésnek vetik alá. Minden bizalmi munkakört betöltő alkalmazottnak és külső félnek, akik Szolgáltató szolgáltatásaival kapcsolatba kerülnek, titoktartási nyilatkozatot kell aláírni.

Szolgáltató egyúttal biztosítja a valamennyi munkakör betöltéséhez szükséges közös, általános, illetve az egyes munkakörök betöltéséhez szükséges speciális szakmai ismereteket megszerzését, illetve továbbfejlesztését.

Ennek érdekében Szolgáltató egy két lépcsős (tájékoztatás + továbbképzés) képzési rendszert valósít meg:

[7] 3/2005-ös IHM rendelet

- a tájékoztatás valamennyi, a Szolgáltató szolgáltatásaival és az érintett informatikai rendszerével kapcsolatba kerülő munkatárs számára egységes {ld. 5.3.3 pont},
- a továbbképzés moduláris, és az egyes bizalmi munkakörök szerint eltérő felépítésű tananyag szerint történik, a személyre szóló éves továbbképzési terveknek megfelelően {ld. 5.3.4 pont}.

5.3.1 Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

Az Időbélyegző Szervezet minden bizalmi munkakörére jelölt személyének (emberi megbízhatóságuk és szakmai alkalmasságuk ellenőrzése céljából) egy kezdeti ellenőrzésen (biztonsági alapellenőrzésen) kell keresztülmennie.

A biztonsági alapellenőrzés során az ellenőrzést végző szakemberek, az életrajzban megadott adatokat (életrajzi elemek, referenciák, szakmai előmenetel, stb.) ellenőrzik. Ennek során:

- a képzettségre vonatkozó adatokat egybevetik a jelölt által benyújtandó bizonyítványokkal, diplomákkal,
- a gyakorlati tapasztalatra vonatkozó állításokat személyes referenciákon keresztül, publikációkra alapozva, illetve egyéb úton igazolják.

A bizalmi munkakört betöltő (vagy arra jelölt) személyek és a vezető tisztségviselők esetén büntetlen előélet igazolása (hatósági erkölcsi bizonyítvány beszerzése és bemutatása) is szükséges.

Az egyes bizalmi munkakörök betöltéséhez szükséges képzettség és gyakorlat a következő.

- Informatikai rendszerért általánosan felelős vezető:

- szakirányú felsőfokú végzettség, valamint
- legalább három év informatika biztonsággal összefüggésben szerzett szakmai gyakorlat.

- biztonsági tisztviselő, rendszer (vagy központi) adminisztrátor, rendszervizsgáló, rendszeroperátor,:

- középfokú szakirányú végzettség vagy szakképesítés és legalább öt év informatika biztonsággal összefüggésben szerzett szakmai gyakorlat, vagy
- szakirányú felsőfokú végzettség vagy felsőfokú szakképesítés és legalább három év informatika biztonsággal összefüggésben szerzett szakmai gyakorlat.

- adattár-felelős:

- középiskolai végzettség,
- legalább két év, hasonló munkakörben szerzett szakmai gyakorlat.

Az informatika biztonsággal kapcsolatos valamennyi bizalmi munkakört[8] betöltő munkatársra nézve **továbbképzési terv** készül, melyet évente áttekintenek (egyúttal az időközben elvégzett továbbképzési, oktatási anyagokkal kiegészítenek), illetve az adott munkakörhöz tartozó szakmai ismeretek megújulása, változása függvényében aktualizálnak.

5.3.2 Előélet vizsgálatára és biztonsági háttér ellenőrzésekre vonatkozó eljárások

Valamennyi bizalmi munkakört betöltő munkatárs biztonsági alapellenőrzésen esik túl {ld. 5.3.1}, emellett mindenkinek időszakos biztonsági ellenőrzéseken is át kell esniük.

Nem tölthet be bizalmi munkakört az a személy, aki akár az alap, akár egy időszakos biztonsági ellenőrzésen a "elfogadhatatlanul nagy biztonsági kockázat" minősítést kapja[9].

Az időszakos biztonsági ellenőrzésre rendszeres időnként kerül sor:

- a biztonsági tisztviselők esetében **3 évente**,
- egyéb bizalmi munkakörök esetében **5 évente**.

Az ellenőrzés során vizsgálják a munkatárs erkölcsi bizonyítványát és olyan körülményeket, melyek kockázati tényezőt jelentenek. E mellett figyelembe veszik a közvetlen vezetők véleményét is.

5.3.3 Kiképzési követelmények

Az Időbélyegző Szervezet területén dolgozó valamennyi munkatárs felvételét követően, a saját munkakörének betöltéséhez szükséges elméleti és gyakorlati alapkiképzésben vesz részt.

Valamennyi munkakörbe való végleges kinevezésnek feltétele az alapkiképzésen való részvétel, s az ezt követő írásos teszten legalább "megfelelő" eredmény elérése.

Egyesített tematika keretében minden munkatárs egy egységes informatika biztonsági alapkiképzésben is részesül. Ennek az (egynapos, intenzív) képzési formának a fő célja az egész időbélyegzés szolgáltatásra vonatkozó szervezet biztonságpolitika megismerése, megértése, az ezen alapuló aktuális eljárások és követelmények megismerése és a későbbi helyes alkalmazása érdekében.

Rendszeroperátori munkakörben kinevezett (véglegesített) munkatárs a kinevezést követő **két hétig** megfelelő gyakorlattal rendelkező kollégával közösen van beosztva (nem lehetséges, hogy a két egyszerre szolgálatban lévő rendszeroperátor mindegyike az adott munkahelyen kezdő).

[8] Ez a meghatározás az *adattár-felelős* munkakör kivételével az összes többi munkakörre vonatkozik

[9] Ilyen esetekben Szolgáltató gondoskodik a megfelelő személy kijelöléséről.

5.3.4 Továbbképzési gyakoriságok és követelmények

Minden bizalmi munkakört betöltő munkatárs esetében továbbképzési terv készül. (Ez tartalmazza az arra az évre beütemezett szervezett belső továbbképzéseket, illetve külső tanfolyamokon, egyéb továbbtanulási formákban való ismeretszerzést.) A személyes továbbképzési tervet a humánpolitikai részleg bevonásával, a közvetlen vezető évente áttekinti, értékeli és (az érintett munkatárs beleegyezésével) aktualizálja.

Abban az esetben, amikor az időbélyegzés szolgáltatásban jelentős változás következik be, valamennyi munkatárs, az őt érintő mélységben továbbképzésben részesül, illetve megkapja a számára szükséges dokumentációkat.

Kisebb változások bekövetkezése előtt a munkatársak írásos tájékoztatást kapnak a változásokról.

5.3.5 Munkabeosztás körforgásának gyakorisága és sorrendje

Körforgás az egyes munkabeosztások között a Szervezet nem tervez.

5.3.6 A felhatalmazás nélküli tevékenységek büntető következményei

Valamennyi bizalmi munkakört betöltő munkatárs esetén, a munkakörbe kinevezéskor a foglalkoztatási dokumentumok részeként

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

Mindezek tartalmazzák azokat a munkajogi vagy büntető következményeket, melyek a különböző fegyelem- munkaköri kötelezettség- illetve törvénysértést szankcionálják.

Amennyiben egy munkatárs (gondatlanságból fakadóan vagy szándékosan) megsérti a fenti szabályokat, ellene büntető intézkedéseket hoznak (melyek az elkövetés módjától és következményétől függően a jutalom megvonástól fegyelmi eljárás indításán és kártérítésen át, egészen a hatósági feljelentésig terjedhet).

5.3.7 A szerződéses alkalmazottakra vonatkozó követelmények

Szolgáltató bizalmi munkakörben csak vele (vagy az Időbélyegző Szervezettel) munkaviszonyban álló személyt alkalmaz.

Szolgáltató az egyéb feladatok ellátására, alvállalkozói vagy megbízásos szerződésben foglalkoztatott szerződő személyeket (külső munkavállalókat és ideiglenes alkalmazottakat egyaránt) csak az "ellenőrzött beszállítók" listájáról választ. Az ellenőrzött beszállítókkal az Időbélyegző Szervezet előzetesen írásos megállapodást köt, melyben vállalta Szolgáltató **biztonságpolitikájának** elfogadását.

Valamennyi szerződő fél – még a tényleges munkavégzés megkezdése előtt – titoktartási nyilatkozatot ír alá, melyben vállalja, hogy a munkavégzés során későbbiekben megismerendő üzleti/vállalati titkokat illetéktelen személynek fel nem fedi, s egyéb módon sem hasznosítja. A titoktartási nyilatkozat záró része tartalmazza a megszegése esetén alkalmazandó szankciókat is.

A külső munkavállalók és ideiglenes alkalmazottak szakmai kiképzésben nem részesülnek, erre nem kötelezettek[10].

5.3.8 A személyzet számára biztosított dokumentációk

Minden bizalmi munkakört betöltő munkatárs megkapja a következő dokumentumokat:

- a **kinevezés**i eljárás, illetve az alapkiképzés során:
  - Szolgáltató szervezeti „Biztonsági kódex",
  - aláírt titoktartási nyilatkozat,
  - egyéni munkaköri leírás.
- a tervezett és rendkívüli **továbbképzés**ek alkalmával:
  - az adott oktatási formához tartozó oktatási segédanyagok.
- egyéb esetekben:
  - személyes továbbképzési terv (évenkénti aktualizálása után),
  - a munkavégzést érintő kisebb változások leírása (a változások előtt),
  - módosított biztonsági politika (a bekövetkező változások előtt).

A szervezeti biztonságpolitikában bekövetkező változásokról írásos értesítők formájában mindenki tájékoztatást kap {ld. **5.3.4 Továbbképzési gyakoriságok és követelmények**} az említett továbbképzés előtt.

[10] A külső munkavállalókat eleve úgy választják meg, hogy az adott munkafeladathoz minden szakmai ismerettel és gyakorlattal rendelkezzenek. Az ideiglenes alkalmazottak olyan jellegű munkát végeznek, melyhez nincs szükség ki- és továbbképzésre.

5.4 Naplózási eljárások

Szolgáltató időbélyegző rendszere széleskörű naplózási tevékenységet folytat. A naplóbejegyzések a bejegyzés pontos idejét, a tevékenység időpontját (ha az a bejegyzés idejétől eltér) és végrehajtóját is tartalmazzák. A pontos időt Szolgáltató pontosidő-egysége biztosítja, ami legfeljebb **1 másodperces** eltérést engedélyez a valódi időhöz képest. Az eltérések szintén naplózásra kerülnek.

5.4.1 A tárolt események típusai

A időbélyegzési rendszer által az egységekhez történő valamennyi hozzáférés és tevékenység naplózásra kerül. Így naplózásra kerül:

- a rendszerbe történő belépések és az operációs rendszer szempontjából fontos üzenetek rögzítése,
- a rendszer komponensek konfigurálására, a rendszer módosítására, beavatkozásra vonatkozó események rögzítése,
- helyi és külső időforrásokkal való kapcsolatfelvétel és időeltérés.

5.4.2 A napló állomány feldolgozásának gyakorisága

Szolgáltató naplóbejegyzéseinek átvizsgálása különböző gyakorisággal, belső üzemeltetési utasításban rögzített rendszerességgel megtörténik. Szolgáltató hálózati védelmi riasztás funkciókkal is rendelkeznek az erőforrásokhoz történő jogosulatlan hozzáférés észlelésének jelzésére. Ilyen riasztási esetekben a naplóbejegyzéseket soron kívül átvizsgálják. Rendellenességek észleléskor, reklamáció esetén, vagy egyéb megkeresések kapcsán szintén sor kerülhet a napló adatok rendkívüli átvizsgálására.

5.4.3 A napló-állomány megőrzési időtartama

A napló-állományokat 90 napig tárolják a keletkezésük helyén. Ezek után az adatokat egyszer írható médiára archiválják, és a napló-állományok archív adathordozóit biztonságosan megőrzik a velük kapcsolatba hozható tanúsítványok érvényességének lejártától számított 10 évig, illetőleg a velük kapcsolatban esetleg felmerült jogvita jogerős lezárásáig.[11]

[11] ld. [1] törvény 9. § (7)

5.4.4 A napló állomány védelme

A napló állományt a véletlen és szándékos rongálások ellen biztonsági mentések védik (ld. 5.4.5 pont). A személyes adatokat tartalmazó naplóbejegyzések esetében Szolgáltató gondoskodik az adatok bizalmas tárolásáról. A napló állományokhoz való hozzáférésre csak azok jogosultak, akiknek erre munkakörük folytán szükségük van. Szolgáltató a hozzáféréseket biztonságos módon ellenőrzi.

Szolgáltató a keletkezett naplóadatok védelme érdekében helyi és valós idejű központi naplógyűjtést is végez. A központi naplógyűjtő hozzáférés szabályozása garantálja a naplóadatok sértetlenségét.

5.4.5 A napló állomány mentési folyamatai

A naplóállományokat a rendzservizsgáló negyedévente archiválja egyszer írható médiára aláírt formában. A mentési médiák a Magyar Telekom Központi Katasztrófa Adattárában kerülnek megőrzésre.

A mentések operatív folyamatait Szolgáltató erre vonatkozó belső szabályzatai írják le részletesen.

5.4.6 A napló gyűjtési rendszere

A naplóbejegyzéseket az alkalmazások automatikusan gyűjtik és tárolják a napló állományokban. A médiákat Szolgáltató saját munkatársai szállítják a megőrzési helyre.

5.4.7 Log-elemzés

A naplóbejegyzések feldolgozása során Szolgáltató naplóadat elemzéseket végez. A napi rendszerességgel végzett feldolgozáson túl Szolgáltató szakemberei **havonta áttekintik** a rendkívüli eseményeket és ezek alapján elemzéseket végeznek. Ezen elemzések alapján Szolgáltató lépéseket tesz a rendszer biztonságának javítására.

5.5 Adatok archiválása

Szolgáltató informatikai rendszerének biztonsági és egyéb naplózási folyamatait ugyanazon rendszerek végzik, ugyanazon módszerek segítségével. Jelen fejezetben csak Szolgáltató ettől eltérő papír alapú és egyéb speciális archiválási rendszerét ismertetjük.

5.5.1 Az archivált adatok típusai

Szolgáltató szervezete a szerződéskötési eljárás során keletkező iratot tárol és megőriz. Így tárolják:

- a Szolgáltatóhoz benyújtott valamennyi papír alapú kérelmet,
- Szolgáltató és az előfizető között megkötött valamennyi megállapodást.

5.5.2 Az archívum megőrzési időtartama

Szolgáltató valamennyi (papíralapú vagy elektronikus) iratot az előfizetői szerződés megszűnésének idejétől számított **10 évig**, illetőleg velük kapcsolatban esetlegesen felmerült jogvita jogerős lezárásáig megőrzi.[12]

5.5.3 Az archívum védelme

Az iratok biztonságos megőrzéséről és tárolásáról Szolgáltató egy **Adattár** segítségével gondoskodik, amelyhez a Szolgáltatónak a meghatározott munkatársai rendelkeznek hozzáférési engedéllyel (adattár felelős).

A Szolgáltató az időbélyegzés szolgáltatás során elektronikus formában tárolt archivált adatállományt **legalább fokozott biztonságú aláírás**sal és minősített **időbélyegző**vel látja el.

5.5.4 Az archívum mentési folyamatai

Az elektronikus másolati példányban létező iratokat (amennyiben keletkeznek ilyenek) egyszer írható médiára rendszeresen mentik.

5.5.5 Archív információ hozzáférését és ellenőrzését végző eljárások

Az archívumhoz Szolgáltató ügyfélszolgálatán keresztül biztosít hozzáférést. A hozzáférés előfizetőnek a rá vonatkozó adatokhoz lehetséges, más feleknek a 9.4.3, 9.4.4 és 9.4.5 alfejezetek szerint. Szolgáltató a jogosultságot minden esetben ellenőrzi, és azt naplózza.

[12] ld. [1] törvény 9. § (7)

5.6 Kompromittálódást és katasztrófát követő helyreállítás

5.6.1 Váratlan esemény és kompromittálódás kezelési eljárások

Rendkívüli üzemeltetési helyzet bekövetkezése esetén a szolgáltató haladéktalanul értesíti a Hatóságot a rendkívüli üzemeltetési helyzet bekövetkezéséről, annak hatásáról, várható időtartamáról, a rendkívüli üzemeltetési helyzet elhárítása érdekében tett és tervezett intézkedésekről, valamint a rendkívüli üzemeltetési helyzet megszűnéséről. A Szolgáltató a rendkívüli üzemeltetési helyzetről értesíti a szolgáltatást igénybe vevő azon szerződött ügyfeleit, akiket a rendkívüli üzemeltetési helyzet érint, valamint az erről szóló tájékoztatást az interneten elérhetővé teszi.

A Szolgáltató Katasztrófa elhárítási tervben (DRP) részletesen szabályozza a különböző sérülések és katasztrófahelyzetek (beleértve valamely szolgáltatói magánkulcs kompromittálódását, vagy kritikus hardver/szoftver elem meghibásodását is) esetén követendő eljárásokat. A következő fejezetekben e **katasztrófa elhárítási irányelveket** foglaljuk össze.

Kompromittálódás esetén az 5.6.3 alfejezetben írtak kerülnek alkalmazásra.

5.6.2 Meghibásodott számítási erőforrások, szoftverek és/vagy adatok

Szolgáltató **megnövelt biztonságú eszközökkel és rendszerekkel rendelkezik**, a hardver- és szoftver-meghibásodások valamint az adatsérülések minimalizálása érdekében. A szolgáltatások helyreállíthatóságát Szolgáltató háttérszerződései és saját tartalékeszközei garantálják. Szolgáltató rendszeres mentései és tranzakció naplózása biztosítja az adatok visszaállíthatóságát valamely adattároló eszköz kiesésének esetére. Ez a rendszer a legrosszabb esetben az előző napi adatok helyreállítására képes.

Szolgáltató katasztrófa elhárítási terve eseményjelentési előírásokkal rendelkezik valamennyi eszköze meghibásodása, illetve rendellenes működése tekintetében (ezek egy része automatizált, más része a kezelőszemélyzet felelőssége). A jelentéseket szakértő személyzet értékeli ki, és válaszadás eljárásokat foganatosítva minimalizálja az esetleges károkat és szolgáltatás kieséseket.

5.6.3 Egy szolgáltatói egység kulcsának kompromitálódása

Szolgáltató katasztrófa elhárítási terve a szolgáltatói magánkulcsok[13] kompromittálódása esetére akciótervvel rendelkezik. Az akcióterv a szolgáltatói nyilvános kulcs visszavonása mellett feltárja a kompromittálódás körülményeit, intézkedik az ez által érintett valamennyi fél értesítéséről, megteszi a szükséges lépéseket a kompromittálódás megismétlődése ellen és szükség esetén új kulccsal látja el a szolgáltatói egységet.

5.6.4 Működés folyamatosságának biztosítása katasztrófát követően

Szolgáltató **elsődleges működési helyszín**ein kívül másodlagos helyszínekkel is rendelkezik. Természeti vagy más katasztrófát követően, illetve Szolgáltató berendezéseinek olyan mértékű meghibásodását illetően, mely a fentiek szerint nem kezelhető, Szolgáltató a másodlagos helyszínen is képes szolgáltatásainak beindítására.

A szolgáltatások elindítását Szolgáltató **3 órán belül** vállalja.

5.7 Időbélyeg szolgáltató vagy szervezet leállítása

A Szolgáltató a szolgáltatás tervezett megszűntetése esetén legkevesebb 30 nappal a szolgáltatás leállítását megelőzően értesíti az előfizetőtket és a Hatóságot. Szolgáltató a tervezett megszűnés előtt legalább **20 nappal** leállítja az időbélyegzés szolgáltatást.

[13] Ide nem csak az időbélyegző egységek tartoznak, de egyéb – az időbélyegzés szolgáltatásban részt vevő - alkalmazások és személyek kulcsai is.

6 Műszaki biztonsági óvintézkedések

A Szolgáltató, biztonságtechnikailag értékelt és minősített termékekből álló, megbízható informatikai rendszert használ szolgáltatásai nyújtásához.

6.1 Kulcspár előállítás és telepítés

Szolgáltató gondoskodik valamennyi általa (saját maga, egyes szervezeti egységei) generált magánkulcs biztonságos és az ipari szabványoknak megfelelő generálásáról.

6.1.1 Kulcspár előállítás

Az időbélyegző szolgáltatás kulcspárjait saját maga generálja, a saját HSM-ekben. A generált magánkulcsok teljes életciklusuk alatt a kriptográfiai hardverekben maradnak, megsemmisítésükig azt sehová nem kell továbbítani.

Az Időbélyegző Szervezet az alábbi **kulcspárt** használja:

- Időbélyeget aláíró kulcs (TrustedTimeStamp szerverek kulcsai).

6.1.2 A szolgáltatói nyilvános kulcs közzététele

Az Időbélyegző Szervezet mindenki számára elérhetővé teszi a szolgáltatói nyilvános kulcsokat tartalmazó tanúsítványokat a Címtárban, valamint a Szolgáltató honlapján.

6.1.3 Kulcs méretek

az Időbélyegző szerverek aláíró kulcsának mérete: ..... 2048 bit

6.1.4 A nyilvános kulcs paraméterek előállítása és ellenőrzése

Az Időbélyegző Szervezet digitális aláírásra az RSA algoritmust használja.

Az RSA algoritmussal van aláírva a rendszer által kibocsátott **időbélyeg**, és ezt az algoritmust használják a rendszeren belül is a letagadhatatlanság biztosítására.

A kulcsgenerálás paramétereinek megfelelőségét két szempontból ellenőrzi a rendszer:

- a paraméterekhez felhasznált véletlenszám generálás megfelelőségének ellenőrzése (statisztikailag kellőképpen véletlenszerű-e a generálás),
- a paraméterekre vonatkozó feltételek, összefüggések teljesülésének ellenőrzése.

A **véletlenszám generálás** megfelelőségének ellenőrzése:

- A rendszerben használt valamennyi kriptográfiai hardver modul képes az általa generált bitsorozat egyenletességének és függetlenségének statisztikai tesztelésére. A modulok lehetővé teszik a tesztek meghívását egy szabványos interfészen keresztül. A modulokat az ezzel megbízott bizalmi munkakört betöltő munkatársak rendszeres időközönként tesztelik.
- A külső interfészen meghívható tesztelési utasításon kívül a hardver modulok is folyamatosan tesztelik saját véletlenszám generálásukat.

A **paraméterekre** vonatkozó feltételek, összefüggések teljesülésének ellenőrzése:

- A rendszerben használt valamennyi kriptográfiai hardver modul a kulcsgenerálás során generált paraméterekre ellenőrzi, hogy azok a rájuk vonatkozó korlátok közé esnek-e, illetve teljesülnek-e az egymás közötti, kötelező összefüggések.

6.1.5 A kulcs használat célja (az X.509 v3 kulcs használati mező tartalmának megfelelően)

A "kulcs használati" mezők lehetséges (egyúttal kötelezően kitöltendő) értékei az alábbiak:

Kulcs megnevezése	A "kulcs használati" mező értéke	Kritikus / Nem kritikus
az időbélyegző központ aláíró kulcsai	*NonRepudiation*	K
	az „Extended Key Usage" mezőbe: *timeStamping*	K

6.2 A Szolgáltatói magánkulcsok védelme és a kriptográfiai modulokkal kapcsolatos előírások

6.2.1 Kriptográfiai modulra vonatkozó szabványok

A Szolgáltató Időbélyegző szervezete a kriptográfiai kulcsok gondozását külön hardver modulban valósítja meg.

Az Időbélyegző Szervezet kulcsainak generálása nCipher nShield F3 500 (hw: nC4033P-500) **hardver** eszközzel történik amely FIPS 140-2 szabvány[14] szerint 3. szinten bevizsgált HSM. Az eszköz rendelkezik a Hatóság által nyilvántartásba vett, tanúsításra jogosult szervezet által erre a célra kiadott kiadott igazolással.

Az Időbélyegző Szervezet kulcsainak előállítása **On-board hardver** generálással történik.

Fentiek során a Nemzeti Hírközlési Hatóság által a [4] dokumentumban jelzett algoritmusokat használata megengedett.

6.2.2 A több-szereplős ("n-ből m") magánkulcs visszaállítás ellenőrzése

Szolgáltató a szolgáltatói magánkulcsot nem állítja helyre, új kulcspárt generál indokolt esetben.

6.2.3 Magánkulcs mentése

A **Szolgáltató**nál az Időbélyegző Szervezet magánkulcsai nem kerülnek mentésre, azokat nCipher nShield F3 500 (hw: nC4033P-500) kriptográfiai hardver (FIPS 140-2 level3) modulja **maga generálja**, és a magánkulcs semmilyen körülmények között nem hagyja el a modult.

Ha a fenti aláíró magánkulcsok megsemmisülnek, akkor helyettük új kulcsok kerülnek generálásra.

6.2.4 Magánkulcs archiválása

A **Szolgáltató**nál **magánkulcsokat** nem archiválnak.

6.2.5 Magánkulcs bejuttatása a kriptográfiai modulba

Az Időbélyegző Szervezet magánkulcsait az nCipher nShield F3 500 (hw: nC4033P-500) kriptográfiai hardver modulja **maga generálja**, és a magánkulcs semmilyen körülmények között nem hagyja el a modult. /Következésképpen soha nem kell kívülről bejuttatni azt./ Ha a magánkulcsok megsemmisülnek, akkor helyettük új kulcsok kerülnek generálásra.

6.2.6 Magánkulcs tárolása a kriptográfiai modulba

A szolgáltatói magánkulcsok tárolása külön kriptográfiai modulban történik, a hozzáfáérés-ellenőrzésekkel együtt az előző alfejezeteknek megfelelően.

[14] Ld. [6] hivatkozás

6.2.7 A magánkulcs aktiválásának módja

A HSM kriptográfiai hardver modulok magánkulcsa csak aktív állapotban használható. A modul automatikusan aktiválódik az operációs rendszer indításakor. Az így aktivált magánkulcs mindaddig használható, amíg a modul aktív állapotban marad.

6.2.8 A magánkulcs aktív állapotának megszüntetési módja

A nCipher nShield F3 500 (hw: nC4033P-500) HSM kriptográfiai hardver modul magánkulcsa akkor deaktiválódik, ha a modul (szabályos vagy szabálytalan módon) kikerül az aktív állapotból. Ez az alábbi esetben következik be:

- a jogosult adminisztrátor törli a kulcsot,
- a kripto modul áramellátása megszakad (kikapcsolás vagy tápellátási probléma),
- a kripto modul hibaállapotba kerül.

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

6.2.9 A magánkulcs megsemmisítésének módja

Az Időbélyegző Szervezet HSM kriptográfiai hardver moduljaiban tárolt magánkulcsok megsemmisítése a Biztonsági tisztviselő, a rendszer adminisztrátor és rendszer operátor együttes jelenlétében sikeres hitelesítésük után, a szükséges kulcsmegsemmisítő funkciók kiváltásával történhet.

6.2.10 A kriptográfiai modulok értékelése

A 6.2.1 ponttal összhangban az alábbi táblázat tartalmazza a Szolgáltató által alkalmazott kriptográfiai hardver modulokra nézve, az ezek ellenőrzése, bevizsgálása és értékelése során megállapított legfontosabb tényeket, tulajdonságokat:

Kriptográfiai modul	HSM nChiper/nShield
A modul fizikai konfigurációja	• Önálló modul

Szolgáltatások	• kriptográfiai műveletek (kódolás, dekódolás, üzenet sértetlenség, digitális aláírás generálás, digitális aláírás ellenőrzés) • kulcsmenedzsment (kulcs generálás, védett kulcstárolás, kulcs klónozás, „n-ből m” aktivizálás, kulcs nullázás) • kriptográfiai menedzsment funkciók (naplózási paraméterek bevitele és beállítása, alarm kezelés és visszaállítás/resetelés/) • felhasználó által választható ön-tesztek végrehajtása (kriptográfiai algoritmus tesztek, szoftver/förmver tesztek, a kritikus funkciók tesztjei, statisztikus véletlenszám generátor teszt) • "státusz kijelzés" (a következőket jelzik ki: aktív szerepkör, a modul kriptográfiai státusza /nullázott, beavatkozás következményeként fellépő, betöltött, inicializált/, hiba kód (ha a modul hiba állapotban van)
Az operációs rendszer biztonsága	A modulok nem nyújtanak olyan eszközt, amelynek segítségével egy operátor a modul hatáskörébe nem tartozó szoftvereket / förmvereket tölthet be és hajthat végre. Ezért ez a kérdéskör jelen modulokra nem releváns.
Kriptográfiai kulcskezelés	A modulok védik a tárolt titkos és magánkulcsokat a jogosulatlan felfedéssel, módosítással és helyettesítéssel szemben. A modulok védik a tárolt nyilvános kulcsokat a jogosulatlan módosítással és kicseréléssel szemben. A kulcsgenerálás és a kulcs megsemmisítésének módszere szabványos és biztonságos
Kriptográfiai algoritmusok	A modulok FIPS által jóváhagyott illetve a Nemzeti Hírközlési Hatóság által a [4] dokumentumban jelzett algoritmusokat alkalmaznak.
Öntesztek	A modulok képesek öntesztek végrehajtására, annak kimutatására, hogy megfelelően működnek
Értékelési szint	FIPS 140-2 szabvány szerint 3. szinten bevizsgált

6.3 A kulcspár kezelésének egyéb szempontjai

6.3.1 A tanúsítványok és a kulcspárok használatának periódusa

Az Időbélyegző Szervezet időbélyeget aláíró kulcsához tartozó tanúsítvány érvényességi ideje: **5 év**

Az Időbélyegző Szervezet magán kulcsainak érvényességi ideje: **5 év**

6.4 Informatikai biztonsági óvintézkedések

6.4.1 Speciális informatikai biztonsági műszaki követelmények

Szolgáltató a Minősített Időbélyegzés Szolgáltatásban alkalmazott időbélyegző egységeit a Magyar Telekom Gyökér Hitelesítő (továbbikaban: Magyar Telekom Root CA) egységében hitelesíti. A Magyar Telekom Root CA-t a Magyar Telekom IT biztonsági osztálya (Időbélyegző Szervezet) működteti, önálló megbízható környezetben. A Magyar Telekom Root CA off-line CA, hálózati kapcsolattal nem rendelkezik. A Szolgáltató a Magyar Telekom Root CA magán kulcsát FIPS 140-2 3 szinten tanúsított és az NHH által nyilvántartott nCipher nShield F3 500 (hw: nC4033P-500) HSM-ben kezeli.

A Magyar Telekom Root CA az általa kibocsátott tanúsítvány visszavonását követően azonnal, de legalább 30 naponta tanúsítvány visszavonási listát (CRL) ad ki, melyet a folyamatosan elérhetővé tesz a

http://www.t-systems.hu/nagyvallalatok/hitelesites_szolgaltatasok/idobelyegzes_szolgaltatas

lapon.

Az Időbélyegző Szervezet olyan megbízható informatikai rendszereket alkalmaz, mely az alábbi termékeken alapul:

nCipher Document Sealing Engine (DSE 200)

Az időbélyegző rendszerbe DSE200 eszközök kerültek beépítésre. Egy DSE200 1024 bites kulcshossz esetén másodpercenként 150, **2048 bites kulcshossz esetén** másodpercenként **90** időbélyeg előállítására képes.

- Windows 2003 alapú szerver(ek),
- A szerver modul a host rendszer számára is biztosítja a megbízható időt, és garantálja, hogy 100 milliszekundumon belül marad az UTC időhöz képest,
- A DSE200 képes elektronikusan aláírni az időbélyeget,
- A telepített szerverek a TCP és HTTP alapú kommunikációt (RFC 3161) támogatják.

Nyilvános LDAP szerviz (HA gép-pár)

- Operációs rendszer [GNU/Linux + HA (HeartBeat HA szoftver)],
- Kernel verzió: folyamatosan frissített stabil verzió.

Tűzfal ALF (HA gép-pár)

- Operációs rendszer [GNU/Linux + HA (HeartBeat HA szoftver)],
- Kernel verzió: folyamatosan frissített stabil verzió,
- ALF alkalmazásszintű tűzfal szoftver.
- Timestamp gateway

Az operációs rendszerek által megvalósított biztonsági funkciók az alábbiak:

- **biztonsági naplózás** (a központi adminisztrátori hozzáférések és tevékenységek rögzítése, a biztonsági napló védelme, az ahhoz való hozzáférés rendszervizsgáló szerepkörre korlátozása),
- a felhasználói adatok védelme (a **hozzáférés ellenőrzési** szabályok alapjainak érvényre juttatása /rendszer fájlok védelme, a felhasználói adatok csak alkalmazáson keresztüli elérésének biztosítása/, a tárolt adatok sértetlenségének védelme /beleértve a vírusok, káros és engedély nélküli szoftverek elleni védekezés támogatását is/, a maradvány információ védelmének megvalósítása),
- **azonosítás és hitelesítés** (a központi adminisztrátorok azonosítása és hitelesítése, az operációs rendszer által biztosított funkciók elérésének sikeres hitelesítéshez kötése),
- **biztonságkezelés** (a biztonsági szerepkörök kezelése, a hozzáférési jogosultságok szerepkörök szerinti beállítása, módosítása),
- **biztonsági funkciók** megbízható **védelme** (alap biztonsági tesztelés végrehajtása, biztonságos állapot megőrzése hiba esetén, a hozzáférés ellenőrzés megkerülhetetlenségének biztosítása, a különböző alkalmazói folyamatok által használt tartományok elkülönítése).

Az alkalmazások által megvalósított biztonsági funkciók az alábbiak:

- **biztonsági naplózás** (a rendszeroperátori hozzáférések és tevékenységek rögzítése),
- **biztonságos kommunikáció** (az Időbélyegző Szervezet és az előfizető közötti kommunikáció bizalmasságának, sértetlenségének és hitelességének biztosítása,
- **felhasználói adatok védelme** (a hozzáférés ellenőrzési szabályok érvényre juttatása /az elindított alkalmazások csak a jogosultságnak megfelelő funkciók elérhetőségét biztosítják/, a maradvány információ védelmének támogatása),
- **azonosítás és hitelesítés** (a rendszeroperátorok azonosítása, hitelesítése, az alkalmazások által biztosított funkciók elérésének sikeres hitelesítéshez kötése).

A **kriptográfiai hardver modulok** által megvalósított biztonsági funkciók részletesen az nCipher nShiel/payShield User/Administration Guide /Windows/ dokumentációkban találhatók.

A **tűzfal** által megvalósított biztonsági funkciók az alábbiak:

- **biztonsági naplózás** (a hálózati kommunikáció naplózása, a biztonsági napló védelme, az ahhoz való hozzáférés rendszervizsgáló szerepkörre korlátozása, a napló folyamatos elemzése: biztonsági riasztások és automatikus válaszok megvalósítása),
- **felhasználói adatok védelme** (az információ áramlás ellenőrzési szabályok érvényre juttatása /szűrés, a tiltott információ áramlás megakadályozása, megfigyelése,)
- **azonosítás és hitelesítés** (központi adminisztrátorok/ azonosítása, hitelesítése, a tűzfal funkciók elérésének sikeres hitelesítéshez kötése),
- **biztonsági funkciók** megbízható **védelme** (az információ áramlás ellenőrzés megkerülhetetlenségének biztosítása).

6.4.2 Informatikai biztonsági minősítés

Az Időbélyegző Szervezet olyan megbízható informatikai rendszert alkalmaz, mely az alábbi komponenseken alapul:

- (tűzfal) operációs rendszer GNU/Linux,
- (időbélyegző alkalamazás) operációs rendszer Windows Server 2003,
- alkalmazászintű és csomagszűrő tűzfalat működtet.

Az Időbélyegző Szervezet informatikai rendszerében alkalmazott kriptográfiai hardver modulok minősítésére vonatkozóan lásd a {**6.2.1 Kriptográfiai modulra vonatkozó szabványok**} és {6.2.10 **A kriptográfiai modul értékelése**} alfejezeteket.

6.5 Életciklusra vonatkozó műszaki óvintézkedések

6.5.1 Rendszerfejlesztési óvintézkedések

Annak érdekében, hogy az Időbélyegző Szervezet valamennyi rendszerfejlesztési projektjében a biztonság követelményeit magas színvonalon biztosítsák, a teljes fejlesztés során (már a tervezési és követelmény-meghatározási fázisban is) figyelembe veszik a különös követelményeket.

6.5.2 Biztonságkezelési óvintézkedések

Az Időbélyegző Szervezet szolgáltatásai nyújtásához olyan termékeket használ, amely a helyes konfigurációt megalapozó megfelelő útmutató dokumentációk használatával, valamint a helytelen használat lehetőségének és egyéb sebezhetőségek vizsgálata útján biztosítja az elvárt működést.

6.5.3 Az életciklusra vonatkozó biztonság osztályozása

Az Időbélyegző Szervezet által a szolgáltatások nyújtásához használt termékek, életciklusra vonatkozó biztonsági szempontok figyelembevételével kerültek alkalmazásra.

6.6 Hálózatbiztonsági óvintézkedések

Az Időbélyegző Szervezet és az előfizetők közötti kommunikáció védett a bizalmasság, sértetlenség és letagadhatatlanság elvesztése ellen. A magas szintű védelmet titkosítással és digitális aláírással biztosítják.

7 Tanúsítvány profil

Szolgáltató által használt Időbélyegzői tanúsítvány alap mezői a következők:

Mezőnév	Érték vagy szabály
Verzió *Version*	A tanúsítvány a [8] ajánlásban leírt X509 3-as verziójú tanúsítványnak felel meg {ld. **1.7 Hivatkozások**}. Ebbe a mezőbe az „**x.509v3**" adat kerül a tanúsítványokon.
Sorozatszám *Serial Number*	A tanúsítványok sorozatszáma: egyedi szám, amelyet a *Hitelesítő Egység* ad ki.
Algoritmus azonosító *Signature Algorithm Identifier*	Ez a szám a *Szolgáltató* **tanúsítványokat hitelesítő elektronikus aláírás**ának algoritmusát azonosítja {ld. 7.3}.
Aláírás *Signature*	A *Szolgáltató* tanúsítványt hitelesítő **elektronikus aláírása**, amelyet a [9] szerint generál és kódol.
Kibocsátó *Issuer*	A tanúsítványt kibocsátó *Időbélyegző Szervezet* egyedi tulajdonos azonosítója {ld.7.4}.
Érvényesség *Valid From & Valid To*	A tanúsítvány érvényességének kezdete és vége[15], amely UCT szerinti érték a [9] szerinti kódolással.
Aláíró (tulajdonos) **azonosító** *Subject*	Az *aláíró* (tulajdonos) egyedi neve {ld. 7.4}.
Aláíró nyilvános kulcsának algoritmus-azonosítója *Subject Public Key Algorithm Identifier*	Ebbe a mezőbe az aláírói nyilvános kulcs algoritmusának azonosítója kerül {ld. 7.3}.
Aláíró nyilvános kulcsa *Subject Public Key Value*	Az aláíró nyilvános kulcsa.
Kibocsátó kulcs azonosító *Authiority Key Identifier*	Kibocsátó kulcsára vonatkozó információ
Aláíró kulcs azonosító *Subject Key Identifier*	Alany kulcsára vonatkozó információ

7.1 Verzió szám(ok)

Szolgáltató a [8] ajánlásban szereplő X509 3. verziónak megfelelő szolgáltatói tanúsítványokat használ.

7.2 Tanúsítvány-kiterjesztések

Szolgáltató által használt Időbélyegzői tanúsítvány **kiterjesztései** a következők:

[15] A két időpont közötti időtartam 5 év

Mezőnév	Érték vagy szabály	Kritikus
Tanúsítvány irányelv *Certificate Policies*	Policy Identifier=1.3.6.1.4.1.17835.7.1.2.8.2.1.12.1.2.1 {Id. 7.6}	Nem
Alapvető megkötések *Basic Constraints*	Subject Type=End Entity Path Length Constraint=None	Igen
Kulcshasználat *Key Usage*	Digital Signature, Non-Repudiation (c0)	Igen
Kiterjesztett Kulcshasználat ***Enhanced Key Usage***	Time Stamping (1.3.6.1.5.5.7.3.8)	Igen
CRL szétosztási pont *CRL Distribution Points*	[1] CRL elérési helye URL=http://eszigno.t-systems.magyartelekom.hu/download_crl?issuer=Magyar%20Telekom%20Root%20CA [2] CRL elérési helye URL=ldap://trustcenter.magyartelekom.hu:389/cn=Magyar%20Telekom%20Root%20CA,c=HU?certificateRevocationList?base?objectClass=certificationAuthority	Nem

7.3 Az algoritmus objektum-azonosítója

Szolgáltató által használt Időbélyegzői tanúsítvány aláírásakor az **SHA-1** RSA algoritmus használatos.

7.4 Elnevezési formák

Szolgáltató által használt Időbélyegzői tanúsítvány **kibocsátó azonosító** és az **aláíró-azonosító** esetében az egyedi X.500 név formátumot alkalmazza, jelen alfejezet szerint a kibocsátó-azonosító (Kibocsátó/Issuer) esetében.

Az Időbélyegzési Rendben meghatározott időbélyegző tanúsítványok kibocsátó azonosítója (a „Kibocsátó” mező tartalma) a következő:

Jelölés	Jelentés	Adat
CN	a tanúsítvány kibocsátását végző szervezet neve (*Common name*)	Magyar Telekom Root CA
OU	a szolgáltató szervezeti egység neve (*Organizational* unit)	Magyar Telekom Trust Center
O	a szolgáltató szervezet neve (*Organization*)	Magyar Telekom Rt.
L	a szervezet székhelye - városnév (*Locality*)	Budapest

C	ország név (*Country*)	HU

Az Időbélyegzési Rendben meghatározott időbélyegző tanúsítványok azonosítója (a „Tulajdonos” mező tartalma) a következő:

Jelölés	Jelentés	Adat
CN	a tanúsítvány kibocsátását végző szervezet neve (*Common name*)	Magyar Telekom Root CA
OU	a szolgáltató szervezeti egység neve (*Organizational* unit)	nCipher DSE ESN:XXXX-XXXX-XXXX (= nChipher HSM ESN (=elektronikus sorozat szám) egy 12 jegyű egyedi azonosító))
OU	a szolgáltató szervezeti egység neve (*Organizational* unit)	TTI
O	a szolgáltató szervezet neve (*Organization*)	Magyar Telekom
L	a szervezet székhelye - városnév (*Locality*)	Budapest
C	ország név (*Country*)	HU

7.5 Elnevezésre vonatkozó korlátozások

Szolgáltató ilyen korlátozást nem alkalmaz.

7.6 Az Időbélyegzési Rend objektum-azonosítója

Szolgáltató által használt Időbélyegzői tanúsítványok a vonatkozó **Időbélyegzési Rend** egyedi objektum-azonosítóját tartalmazzák {ld. 7.2 **Tanúsítvány-kiterjesztések**}.

7.7 A „Hitelesítési Rend korlátozás” kiterjesztés használata

Szolgáltató ezt a kiterjesztést nem használja.

7.8 Szabályzatminősítő szintaxis és szemantika

Szolgáltató által használt Időbélyegzői tanúsítványok a szolgáltatási szabályzat internetcímét, valamint figyelmeztető szöveget nem tartalmazzák {ld. 7.2 **Tanúsítvány-kiterjesztések**}.

7.9 A kritikus Időbélyegzési Rend kiterjesztés feldolgozása

Szolgáltató által használt Időbélyegzői tanúsítványokban alkalmazott Tanúsítvány-irányelv kiterjesztés nem kritikus. Mindazonáltal **Szolgáltató** előírásainak és kikötéseinek figyelmen kívül hagyásáért a végfelhasználók a felelősek.

7.10 Időbélyeg profil

Az időbélyeg profil leírását az Időbélyegzési Rend dokumentum [13] 5.3.1 fejezete tartalmazza.

8 Megfelelőségi audit és egyéb ellenőrzések

8.1 Az ellenőrzések körülményei és gyakorisága

A Szolgáltató vizsgált és tanúsított **elemeket** (elektronikus aláírási termékeket, informatikai rendszerelemeket stb.) alkalmaz az időbélyegzés szolgáltatásaihoz kapcsolódóan, úgymint:

- az időbélyeg előállítására, valamint magánkulcsainak tárolására használt kriptográfiai hardver modult (nShield F3 500 hw: nC4033P-500 hardver kriptográfiai modul),

A kriptográfiai hardver modulok tanúsítására a használatba vételt megelőzően kerül sor. A tanúsítás érvényessége 3 év, melynek lejártával a megfelelőség-vizsgálatot meg kell ismételni.

A tanúsításhoz és vizsgálatokhoz a Szolgáltató alapvetően külső szervezete(ke)t vesz igénybe {ld. 8.2 **Az auditor és szükséges képesítése**}. A Szolgáltató e külső tanúsításokon túl saját belső központi ellenőrzési szervezettel is rendelkezik, mely rendszeresen vizsgálja a korábbi tanúsításoknak való megfelelőséget, és eltérés esetén megteszi a szükséges lépéseket. Ezen felül Szolgáltató informatikai szervezetében saját belső szakértői csoport tevékenykedik, mely az Időbélyegző Szervezet tevékenységét eseti és / vagy tervezett jelleggel megvizsgálja.

8.2 Az auditor és szükséges képesítése

A kriptográfiai hardver modulok tanúsítását egy erre feljogosított tanúsító szervezet végezte. A tanúsított elektronikus aláírási terméket a Hatóság nyilvántartásba vette.

A minősített időbélyegzést kiszolgáló rendszerek és módszerek megfelelőségének vizsgálatára külső, független, a Hatóság által nyilvántartásba vett elektornikus aláírás szakértő által, valamint Szolgáltató erre a célra létrehozott belső központi ellenőrzési szervezetének auditorai által kerül sor.

Emellett a Szolgáltató mind belső, mind pedig külső, független rendszervizsgáló(ka)t is megbíz a minőségirányítási és információbiztonsági rendszerek ellenőrzésére. Ezen szakemberek többéves szakmai gyakorlattal valamint megfelelő végzettséggel és szakképesítéssel rendelkeznek.

Mindezeken felül a Szolgáltatónál a Hatóság is helyszíni szemlét és ellenőrzést tart, évente legalább egyszer.

8.3 Az auditor és az auditált rendszer függetlensége

A Szolgáltatóval kapcsolatban tanúsítást végző szervezetek a Szolgáltatótól függetlenek, és befolyástól mentesen végzik tevékenységüket. A vizsgálatot végző külső, független szervezet nem rendelkezik tulajdonrésszel vagy érdekeltséggel a Szolgáltatót illetően, és Szolgáltató nem tulajdonosa közvetlenül vagy közvetve a vizsgálatot végző szervezetnek. A tanúsító szervezetek díjazása nem függ a tanúsítás során végzett tevékenységük megállapításaitól.

8.4 Az auditálás által lefedett területek

A vizsgálatok által lefedett területek a következők:

- A kriptográfiai hardver modulok tanúsítása, mely a [2] harmadik részének 1. fejezetében maghatározott követelményeknek való megfelelőség vizsgálatára irányul.
- A minősített időbélyegzést kiszolgáló rendszerek és módszerek tanúsítása (beleértve a dokumentálásra, folyamatokra, fizikai és műszaki biztonságra, az érintett személyzetre, valamint az adatvédelemre) mely a vonatkozó jogszabályok[16] előírásainak, a jelen Szabályzatban rögzített Időbélyegzési Rend dokumentumoknak valamint Szolgáltató egyéb szabályzatainak való megfelelőség vizsgálatára irányul.
- Szolgáltató minőségirányítási és információbiztonsági irányítási rendszere, mely a külső és belső szabványok, ajánlások és leírások követelményei végrehajtásának megfelelőségére irányul.

8.5 A hiányosságok kezelése

A vizsgálatok vagy a rendszeres helyszíni ellenőrzések során feltárt esetleges hiányosságokat a Szolgáltató az előírt határidőre megszünteti a vizsgálatot végző szervezettől kapott információ és ajánlások alapján.

8.6 Az eredmények közzététele

A Szolgáltató a tanúsítások illetve vizsgálatok végeredményét saját honlapján közzéteszi, amennyiben ezek a pubikus szabályzatait és dokumentumait érintik. Ez nem vonatkozik a tanúsítási eljárás során feltárt, az eljárás végeredményét nem befolyásoló hiányosságokra és részeredményekre.

[16] [1], [3], [22] és kacsolódó rendeletei és vonatkozó ajánlások

9 Egyéb üzleti és jogi kérdések

9.1 Díjak

A Szolgáltató meghirdetett díjait előzetes értesítés nélkül bármikor módosíthatja. Bármilyen költség számlázására csak közvetlenül a Szolgáltató jogosult.

Időbélyegzés szolgáltatási díjak. A Szolgáltató az időbélyegzés szolgáltatásért díjat számol fel a vonatkozó Szolgáltatói Szerződésben (ISzSz) foglaltak szerint.

Díjvisszatérítésre jogosult előfizető a Szolgáltatási Szerződésben vállalt szolgáltatási szint nem teljesítése esetén, az abban foglaltak szerint.

9.2 Anyagi felelősségvállalalás, felelősségbiztosítás.

A Szolgáltató a megbízhatóság biztosítása érdekében teljes körű felelősségbiztosítással is rendelkezik a Lloyds biztosítótársaságnál. A felelősségbiztosítási szerződés kiterjed a Szolgáltató által a szolgáltatások nyújtásával összefüggésben okozott valamennyi kárra. A **biztosítás** egy biztosítási esemény vonatkozásában káreseményenként[17] és összességében **évente 27.000.000** Ft (Huszonhétmillió forint) összegig **fedezetet** biztosít az összes károsultnak okozott károkra. Több azonos okból bekövetkezett, időben összefüggő káresemény egy biztosítási eseménynek minősül.

Ha egy biztosítási eseménnyel kapcsolatban több jogosult megalapozott kártérítési igénye meghaladja a károkra biztosítási eseményenként a felelősségbiztosítási szerződésben meghatározott összeget, akkor a kártérítési igények megtérítése az összes kártérítési igénynek a felelősségbiztosítási szerződésben meghatározott összeghez viszonyított arányában történik.[18]

További információkat a 9.8 és 9.9 fejezetek tartalmaznak.

A **Szolgáltató** a vagyoni felelősségre vonhatóság, az általa okozott károkkal kapcsolatos saját felelősség, illetve a neki okozott károkért járó kártérítés megállapíthatósága, dokumentálása és bizonyíthatósága érdekében naplózza tevékenységeit, védi a naplóbejegyzések sértetlenségét és hitelességét, valamint hosszú távon megőrzi (archiválja) a naplóadatokat.

9.3 Az üzleti információk bizalmassága

Szolgáltató az általános alapszabályokon túlmenően nem alkalmaz egyedi szabályt erre vonatkozóan.

[17] ld. a [3] 11. § (3)

[18] ld. [3] 11. § (5)

9.4 A személyes adatok védelme

A Szolgáltató az előfizető adatait a jogszabályoknak megfelelően kezeli. A Szolgáltató társasági szintű **adatkezelési szabályzat**tal rendelkezik, mely a személyes adatok kezelésével kiemelten foglalkozik, és amely általánosságban vonatkozik az időbélyegzéssel kapcsolatos szolgáltatásokra is. A szolgáltatásokra vonatkozó speciális adatkezelést jelen szabályzat valamint Szolgáltató belső (nem nyilvános) szabályzatai operatív szinten tárgyalják.

Az előfizető a Szolgáltatási Szerződés aláírásával hozzájárul ahhoz, hogy a személyes adatait a Szolgáltató (az adatkezelési szabályzatnak megfelelő módon) tárolja és kezelje. A Szolgáltató az előfizetői adatokat kizárólag csak az időbélyegzés szolgáltatással összefüggésben használja fel.

A Szolgáltató a tudomására jutott adatokat a jogszabályi követelményeknek megfelelően, az előírt időtartamig megőrzi, majd a bizalmasnak számító információkat vissza nem állítható módon megsemmisíti.

A Szolgáltató a felhasználói adatok megőrzése során gondoskodik az információk **sértetlenség**éről, **bizalmasság**áról és **biztonságos tárolás**áról. Az információkhoz való hozzáférést csak azon személyeknek engedélyezi, akik feladata azt indokolja. Így például a felhasználói adatok papír alapú eredeti példányát (felhasználói szerződés) az adott megrendelésben részt vevő tisztviselő kezeli, másnak át nem adja, másoktól elzárt módon tárolja, majd a megrendelés lezártával a **Magyar Telekom IT üzemeltetési igazgatóság Katasztrófa Adattárában** (ebben a dokumentumban Adattár) helyezi el végső megőrzésre. Az elektronikus rendszerekben csak azon adatok kerülnek rögzítésre, amelyek az időbélyegzés igénybevételéhez szükségesek (authentikációs tanúsítvány). A hozzáférések és jogosultságok kezelésére Szolgáltató külön belső szabályzattal rendelkezik (Rendszer Biztonsági Megfelelőség dokumentum), melynek alapján a rendszerek megfelelőségét és a jogosultságkezelési szabályok betartását mind belső, mind pedig külső független auditorok és a Hatóság (NHH) ellenőrzik rendszeresen.

A Szolgáltató gondoskodik a nem nyilvános információk **bizalmasság**áról és **sértetlenség**éről a felhasználói adatok továbbítása során, továbbá – megbízható rendszerek alkalmazásával és az adatok rendszeres archiválásával – a megfelelő **rendelkezésre állás**ról.

9.4.1 Bizalmasan kezelendő információ-típusok

a) A Szolgáltató bizalmas információként kezeli az előfizető minden adatát, kivéve azokat, amelyeket a 9.4.2 alfejezet tárgyal.

b) A Szolgáltató a birtokába jutott bizalmas információt a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény rendelkezéseinek megfelelően kezeli, s csak a 9.4.3 – 9.4.5 alfejezetekben említett esetekben és személyek/szervezetek részére fedi fel őket.

c) A Szolgáltató bizalmas információként kezeli a következő adatokat és dokumentumokat az előbbieken kívül:

- magánkulcsok és aktivizáló kódok,
- szolgáltatási szerződések,
- tranzakciós és napló adatok,
- nem nyilvános szabályzatok,
- minden olyan adat, amelynek nyilvánosságra kerülése a szolgáltatás biztonságát előnytelenül befolyásolná.

9.4.2 Nem bizalmasnak tekintett információ típusok

A Szolgáltató nem bizalmas információként kezeli mindazon adatokat, melyet a szolgáltatás igénybevételéhez kiadott authentikációs tanúsítványba belefoglal[19].

9.4.3 Információszolgáltatás a hatóságok részére

a) A Szolgáltató az elektronikus aláírás felhasználásával elkövetett bűncselekmények felderítése vagy megelőzése céljából, illetőleg 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 az [1] törvény[20] 11.§ (2) bekezdése szerinti körben.

b) A Szolgáltató rögzíti az a) pontbeli adatátadás tényét, de arról nem tájékoztatja az előfizetőt.

c) A Szolgáltató olyan esetben is szolgáltathat információt, amikor egyéb jogszabály(ok) ezt előírják.

9.4.4 Információszolgáltatás polgári eljárás keretében

a) A Szolgáltató a tanúsítvány 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 felhasználói információkat, illetőleg azokat közölheti a megkereső bírósággal az [1] törvény 11.§ (3) bekezdése szerinti körben.

b) A Szolgáltató rögzíti az a) pontbeli adatátadás tényét, és arról tájékoztatja az előfizetőt.

[19] Függetlenül attól, hogy az előfizető hozzájárul-e (az alany nevében) a tanúsítvány nyilvánosságra hozásához.

[20] 2001. évi XXXV. törvény az elektronikus aláírásról

9.4.5 A tulajdonos kérésére történő felfedés

A **Szolgáltató** az **előfizető** hivatalos – írásban adott – felhatalmazása alapján tárja fel a rájuk vonatkozó bizalmas felhasználói információkat **harmadik fél** részére.

9.5 Szellemi tulajdonjogok

a) A Szolgáltató szabályzatai, szerződéses feltételei Szolgáltató tulajdonát képezik.

b) A **visszavonási információ** a Szolgáltató tulajdonát képezi.

9.6 Tevékenységért viselt felelősség és helytállás

A Szolgáltató általános felelőssége:

a) A Szolgáltató felelősséget vállal az Időbélyegzési Rend dokumentumban leírt eljárásoknak való megfelelőségért, még abban az esetben is, amikor a Szolgáltató egyes tevékenységeit alvállalkozók végzik[21].

b) A Szolgáltató a vele szerződéses jogviszonyban álló felekkel (előfizető) szemben a Magyar Köztársaság Polgári Törvénykönyvének a szerződésszegésért való felelősség szabályai szerint felelős.

c) A Szolgáltató a vele szerződéses jogviszonyban nem álló harmadik féllel (ilyen az érintett fél) szemben a Magyar Köztársaság Polgári Törvénykönyvének a szerződésen kívüli károkozásról szóló szabályai (Ptk. 339. §) szerint felelős.

A **Szolgáltató** feladata az Időbélyegző Szervezet és a címtár működtetése. A **Szolgáltató**nak szolgáltatásait a hatályos jogi szabályozással, szolgáltatási szabályzatával és egyéb nyilvánosságra hozott szabályzataival, szerződéses feltételeivel összhangban kell nyújtania. A Szabályzat keretei között végzett szolgáltatói tevékenységekért (beleértve az esetlegesen igénybe vett alvállalkozókét is) a **Magyar Telekom Nyrt. a felelős.**

9.6.1 Az időbélyegzés szolgáltató felelőssége és helytállása

a) Az Időbélyegző Szervezet **felelős**:
   - a kiadott időbélyeg szabványoknak történő megfeleléséért,
   - az időbélyegben szereplő időért,
   - általában a kötelezettségei betartásáért.

b) Az Időbélyegző Szervezet **nem felelős**:

[21] Az időbélyegzés-szolgáltató általánosan felelős az időbélyegző szervezet, valamint a címtár kötelezettségeiért, tevékenységeiért.

- az előfizetők időbélyeg felhasználással kapcsolatos tevékenységeiért,
- az előfizetők, érintett felek, és mások által kibocsátott szabályzatokért.

9.6.2 Az előfizető felelőssége és helytállása

Az előfizető felelős:

- a Szolgáltatási Szerződés betartásáért,
- a számára kibocsátott authentikációs tanúsítványok és az ehhez tartozó kulcspár tulajdonosi kötelezettségeiért,
- a Szolgáltató haladéktalan értesítéséért és teljes körű tájékoztatásáért vitás ügyekben,
- az időbélyegzés szolgáltatás díja(i)nak szerződés szerinti kifizetéséért, azaz a számlákon szereplő összegek megjelölt időpontig történő kifizetéséért (eltérő megállapodás hiányában),
- általában a kötelezettségei betartásáért.

9.6.3 Az érintett fél felelőssége

Az érintett fél felelős a jogszabályokban írt kötelezettségek betartásáért és az adott helyzetben általában elvárható magatartás tanúsításáért, különösen az elektronikus aláírás, az időbélyeg ellenőrzéséért, illetve a tanúsítványok elfogadása során tanúsított körültekintő eljárásért.

9.7 Helytállás érvénytelenségi köre

Szolgáltató nem alkalmaz különleges szabályokat erre vonatkozóan.

9.8 Felelősségi korlátozások

A Szolgáltató nem felelős az olyan károkért, mely abból adódott, hogy az érintett fél a tanúsítványok ellenőrzése és felhasználása során nem a hatályos jogszabályok és szolgáltatói szabályzatai szerint járt el, illetve nem úgy járt el, ahogyan az adott helyzetben elvárható.

Pénzügyi felelősség korlátozása

A **Szolgáltató** a kártérítés felső határát összességében korlátozza. A **Szolgáltató** pénzügyi felelősségével kapcsolatos további részleteket az **ÁSzF** dokumentum tartalmazza.

9.9 Kártérítési kötelezettségek

A Szolgáltató a felelősségi körén belül keletkezett, bizonyított károkért a szabályzataiban és az előfizetővel megkötött szolgáltatási szerződésekben valamint az előző pontban rögzített korlátozásokkal kártérítést fizet.

A Szolgáltató a szolgáltatásaival kapcsolatos szerződéses és szerződésen kívüli károkért harmadik személlyel szemben kizárólag kötelezettségei felróható megszegéséből bekövetkező, bizonyítható károkért tartozik helyt állni.

Az előfizető kártérítési felelősséggel tartoznak a Szolgáltatóval szemben azokért a veszteségekért és károkért, melyeket kötelezettségeik be nem tartásával okoznak számára.

9.10 Érvényesség

Jelen szabályzat időbeli hatályát az 1.1.2 pont tartalmazza.

Amennyiben a Szabályzat valamely pontja érvénytelen lenne, az a Szabályzat egészének és más pontjainak érvényességét nem érinti.

A Szabályzat a Közösség valamennyi kötelezettségét, felelősségét és jogát tartalmazza. A Szabályzat egyetlen pontja sem értelmezhető a jelen dokumentumba foglalt értelmezéstől eltérően, bármely más szerződés vagy szabályzat, írott vagy szóbeli kommunikáció következtében, beleértve a Szolgáltató és más szervezet jövőbeli esetleges összeolvadásának esetét is. A Szabályzat csak írott és hitelesített formában módosítható, a Hatóság által vezetett szabályzat-nyilvántartásban való átvezetés mellett.

9.11 A felek közötti kommunikációra vonatkozó előírások

Az előfizető jognyilatkozatait Szolgáltató felé kizárólag írásban, hivatalosan aláírt módon teheti meg. Az előfizető egyéb esetekben a Szolgáltatót írásban, elektronikus levél vagy fax formájában is értesítheti. A Szolgáltató értesítési címei jelen szabályzat 1.1.3 és 1.3.1 alfejezetében találhatóak.

9.12 Kiegészítések

Szolgáltató nem alkalmaz különleges szabályokat erre vonatkozóan.

9.13 Vitás kérdések megoldása

A szolgáltatással kapcsolatos bármely vitás kérdés vagy panasz felmerülése esetén a vita jogi útra terelése előtt az előfizetőnek kötelessége a Szolgáltató haladéktalan értesítése és teljes körű tájékoztatása az ügy minden vonatkozását érintően. A felek vitáikat mindenkor megkísérlik békés, tárgyalásos úton rendezni.

A Szolgáltató (beleértve az Időbélyegző Szervezetet is) tevékenységével kapcsolatos kérdéseket, kifogásokat és panaszokat az.1.3.1alfejezetben rögzített Időbélyegző Szervezetre vonatkozó elérhetőségeken lehet megtenni.

Az eljárás további részleteit az ÁSZF dokumentum 12.pontja tartalmazza.

9.14 Irányadó jog

A Szolgáltató tevékenységét a mindenkor hatályos magyar jogszabályoknak megfelelően végzi. A 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 megfelelőség

A legfontosabb jogszabályok felsorolását az Időbélyegzési Rend tartalmazza.