MICROSEC

Számítástechnikai Fejlesztő Kft.

Minősített e-Szignó Hitelesítés Szolgáltató

Időbélyegzési Rend

Azonosító:	1.3.6.1.4.1.21528.2.1.1.3
Verzió:	3.2
Első verzió hatályba lépése:	2005. április 1.
Kezelési mód:	**Nyilvános**
Jóváhagyta:	Ellbogen András
Jóváhagyás dátuma:	
Belső auditor:	Tóth Elemér
Hatálybalépés dátuma:	2005. augusztus 8.

MICROSEC Számítástechnikai Fejlesztő Kft.
1022 Budapest, Marcibányi tér 9.

Változáskövetés

Verzió	Dátum	A változás leírása	Hatálybalépés	Készítette
1.0	2005-04-01	Első változat	2005-04-01	Berta István Zsolt
2	2005-04-15	A belső auditor javaslatai alapján átdolgozott változat (azonos az 1.1-es verzióval)	2005-04-15	Berta István Zsolt
3	2005-05-02	Apróbb javítások	2005-05-02	Berta István Zsolt
3.2	2005-07-01	A hatósági szemlét követő módosítások	2005-08-08	Berta István Zsolt

Tartalomjegyzék

1. Bevezetés ... 5
1.1. Áttekintés ... 5
1.2. Azonosítás ... 5
1.3. Közösség és alkalmazhatóság ... 5
1.4. Kapcsolattartás ... 5
1.4.1. Szolgáltató ... 5
1.4.2. Ügyfélszolgálati iroda ... 6
1.4.3. Hitelesítő szervezet ... 6
2. Általános rendelkezések ... 6
2.1. Az időbélyegzés szolgáltatás komponensei ... 6
2.2. Időbélyegzés szolgáltató ... 6
2.3. Végfelhasználók ... 6
2.4. Az Időbélyegzési Rend és a Szolgáltatási Szabályzat ... 6
3. Időbélyegzés politika ... 7
3.1. Áttekintés ... 7
3.2. Azonosítás ... 7
3.3. Közösség és alkalmazhatóság ... 7
3.4. Megfelelőség ... 7
4. Kötelezettségek és felelősség ... 7
4.1. A Szolgáltató kötelezettségei ... 7
4.1.1. Általános kötelezettségek ... 7
4.1.2. Kötelezettségek az Ügyféllel szemben ... 8
4.2. Az Ügyfél kötelezettségei ... 8
4.3. Az Érintett fél kötelezettségei ... 8
4.4. Felelősség ... 8
5. Működésre vonatkozó követelmények ... 8
5.1. Az időbélyegzés szolgáltatás szabályozása és e szabályozás közzététele ... 8
5.1.1. Az időbélyegzés szolgáltatás szabályozása ... 8
5.1.2. Közzétételi nyilatkozat ... 8
5.2. Kulcsgondozás ... 9
5.2.1. Az időbélyegzés szolgáltató aláírókulcsának generálása ... 9
5.2.2. Az időbélyegzés szolgáltató magánkulcsának védelme ... 9
5.2.3. Az időbélyegzés szolgáltató nyilvános kulcsának közzététele ... 9
5.2.4. Az időbélyegzés szolgáltató tanúsítványának érvényessége ... 9
5.2.5. Az időbélyegzés szolgáltató aláírókulcsának használatának befejezése ... 9
5.2.6. Az alkalmazott kriptográfiai modul életciklusa ... 10
5.3. Időbélyegzés szolgáltatás ... 10
5.3.1. Időbélyeg ... 10
5.3.2. Óraszinkronizálás ... 10
5.4. Az időbélyegzés szolgáltatás üzemeltetése és menedzsmentje ... 10
5.4.1. Biztonsági intézkedések ... 10
5.4.2. Rendszerelemek biztonsági osztályba sorolása ... 10
5.4.3. Személyzeti biztonság ... 10
5.4.4. Fizikai biztonság ... 11
5.4.5. Üzemeltetés menedzsment ... 11
5.4.6. Hozzáférés-menedzsment ... 11
5.4.7. A rendszer telepítése és fejlesztése karbantartása ... 11

5.4.8. Üzletmenet folytonosság 12
5.4.9. A szolgáltatás leállítása 12
5.4.10. Jogszabályi megfelelőség 12
5.4.11. Időbélyegzés szolgáltatással kapcsolatos adatok naplózása 12
5.5. Szervezeti felépítés 13

1. Bevezetés

Jelen dokumentum a MICROSEC Számítástechnikai Fejlesztő Kft. (továbbiakban: Szolgáltató) által üzemeltetett minősített *e-Szignó Hitelesítés Szolgáltató* által támogatott időbélyegzési rendet tartalmazza. A dokumentum pontos megértéséhez szükségesek a használt fogalmak értelmezésének pontos ismerete, amelyek az A mellékletben találhatóak. Jelen Időbélyegzési Rend az ETSI TS 102 023 alapján készült, tartalmában és felépítésében követi annak előírásait.

1.1. Áttekintés

Az Időbélyegzési Rend az e-Szignó Hitelesítés Szolgáltató időbélyegzés szolgáltatására vonatkozó követelményeket tartalmazza. A szolgáltatás részletes szabályozását a „Minősített e-Szignó Hitelesítés Szolgáltató elektronikus aláírással kapcsolatos szolgáltatásaira vonatkozó Szolgáltatási Szabályzat" (a továbbiakban Szolgáltatási Szabályzat) című dokumentum tartalmazza.

1.2. Azonosítás

A dokumentum címe:	Minősített e-Szignó Hitelesítés Szolgáltató Időbélyegzési rend
OID:	1.3.6.1.4.1.21528.2.1.1.3
Verzió:	1.0
Hatálybalépés kelte:	2005. április 1.

A dokumentum aktuális változata a Szolgáltató honlapján, illetve a Szolgáltató ügyfélszolgálati irodájában érhető el.

1.3. Közösség és alkalmazhatóság

A Szolgáltató szervezetén belül az *e-Szignó Hitelesítés Szolgáltató*, mint önálló üzleti egység látja el az időbélyegzés szolgáltatással kapcsolatos feladatokat. Ezen önálló üzleti egység a következő két részből áll:

- Hitelesítő szervezet
- Ügyfélszolgálati iroda

A Szolgáltató által nyújtott időbélyegzés szolgáltatás végfelhasználói (lásd a 2.3. fejezetben):

- Ügyfél, aki előfizet a Szolgáltató által nyújtott időbélyegzés szolgáltatásra, és a szolgáltatás keretében időbélyegeket kér a Szolgáltatótól.
- Érintett fél, aki ellenőrzi és felhasználja a Szolgáltató által kibocsátott időbélyegeket.

1.4. Kapcsolattartás

1.4.1. Szolgáltató

Név: MICROSEC Számítástechnikai Fejlesztő Kft.
Cégjegyzék szám: 01-09-078353 a Fővárosi Bíróság mint Cégbíróság
Székhely: 1022 Budapest, Marcibányi tér 9.
Postacím: 1031 Budapest, Záhony utca 7, Graphisoft park
Központi telefonszám: (1) 505-4444
Központi telefax szám: (1) 505-4445
Internet cím: http://www.microsec.hu

1.4.2. Ügyfélszolgálati iroda

Név: e-Szignó Hitelesítés Szolgáltató Ügyfélszolgálati iroda

Cím: 1031 Budapest, Záhony u. 7.
Graphisoft Park, D épület

Postacím: 1031 Budapest, Záhony utca 7, Graphisoft park

Telefonszám: (+36-1) 505-4444

Telefax szám: (+36-1)

E-mail cím: info@e-szigno.hu

Internet cím: http://www.e-szigno.hu

1.4.3. Hitelesítő szervezet

A hitelesítő szervezet elérése az ügyfélszolgálati irodán keresztül történik.

2. Általános rendelkezések

2.1. Az időbélyegzés szolgáltatás komponensei

Az időbélyegzés szolgáltatás során a Szolgáltató a következő tevékenységeket végzi:

- Időbélyeg kibocsátás, melynek során a Szolgáltató időbélyegeket állít elő és bocsát ki ügyfelei részére.
- Időbélyegzés menedzsment, melynek során a Szolgáltató biztosítja és ellenőrzi az időbélyeg kibocsátás szolgáltatás a Szolgáltató által lefektetett követelményeknek megfelelő működését. Ezen követelményeket a Szolgáltató egyrészt jelen Időbélyegzési Rendben, másrészt a Szolgáltatási Szabályzatban határozza meg.
- Időjel ellátás, melynek során a Szolgáltató pontos időt szolgáltat a Microsec Kft. számára.

2.2. Időbélyegzés szolgáltató

Az időbélyegzés szolgáltatást, vagyis a 2.1. fejezetben leírt szolgáltatásokat a Microsec Kft. e-Szignó Hitelesítés Szolgáltató önálló üzleti egysége nyújtja.

2.3. Végfelhasználók

Az időbélyegzés szolgáltatás végfelhasználói a következő felek lehetnek:

- Az *Ügyfél*, aki előfizet a Szolgáltató által nyújtott időbélyegzés szolgáltatásra, és a szolgáltatás keretében időbélyegeket kér a Szolgáltatótól. Az Ügyfél lehet természetes vagy jogi személy, egy (jellemzően jogi személy) ügyfél nevében akár több természetes személy is kérhet időbélyegeket.
- *Érintett fél*, aki ellenőrzi és felhasználja a Szolgáltató által kibocsátott időbélyegeket. Az Érintett fél nem áll szerződéses kapcsolatban a Szolgáltatóval.

2.4. Az Időbélyegzési Rend és a Szolgáltatási Szabályzat

Jelen Időbélyegzési Rend a Szolgáltató által nyújtott időbélyegzés szolgáltatásra vonatkozó általános követelményeket tartalmazza. A Szolgáltatási Szabályzat azt írja le, hogy a Szolgáltató milyen módon teljesíti az Időbélyegzési Rendben megfogalmazott követelményeket.

Az Időbélyegzési Rend összhangban van a Szolgáltatási Szabályzattal és a „Minősített e-Szignó Hitelesítés Szolgáltató által nyújtott időbélyegzés és on-line tanúsítvány állapot szolgáltatásokra vonatkozó Általános Szerződési Feltételek” (a továbbiakban Általános Szerződési Feltételek) című dokumentummal, valamint a Szolgáltató belső biztonsági és üzemeltetési szabályzataival, és nem tartalmaz velük ellentétes szabályozást.

3. Időbélyegzés politika

3.1. Áttekintés

Jelen Időbélyegzési Rend az e-Szignó Hitelesítés Szolgáltató időbélyegzés szolgáltatására vonatkozó általános követelményeket tartalmazza. A követelményeknek való megfelelést a Szolgáltatási Szabályzat írja le.

A szolgáltatást a 2.3. fejezetben megnevezett Ügyfelek vehetik igénybe az Általános Szerződési Feltételeknek valamint az Ügyfél és a Szolgáltató közötti szerződés szerinti feltételekkel. A szolgáltatás nyújtása során a Szolgáltató az ETSI TS 101 861, illetve az RFC 3161 specifikációknak megfelelő formátumú időbélyegeket nyújt az Ügyfél által kért dokumentum-lenyomatra. Magát a dokumentumot a Szolgáltató a szolgáltatás nyújtása során nem ismeri meg. A Szolgáltató biztosítja az időbélyegek pontosságát; a kibocsátott időbélyegeken szereplő időpont legfeljebb 1 másodperccel térhet el az UTC (Coordinated Universal Time, ITU-R TF460-5 ajánlás szerinti időalap) referencia-időtől.

3.2. Azonosítás

Lásd a 1.2. fejezetben.

3.3. Közösség és alkalmazhatóság

Az 1.3. fejezet tartalmazza.

3.4. Megfelelőség

A Szolgáltató által nyújtott minősített időbélyegzés szolgáltatás nyújtó rendszere megfelel a vonatkozó jogszabályoknak, különösen a következőknek:

A Szolgáltató a 2001. évi XXXV. törvényben (amely később módosításra került a 2004. évi LV. módosító törvény által) meghatározott időbélyegzés szolgáltatást nyújtja. E szolgáltatás megfelel a 2001. évi XXXV. törvényben törvénynek és a kapcsolódó rendeleteknek:

- 3/2005 IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről (illetve a 16/2001 MeH irányelv az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről).
- 2/2002 MeH irányelv a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről.

E dokumentum megfelel a nemzetközi ajánlásoknak (ETSI TS 102 023, ETSI TS 101 861, RFC 3161, CEN CWA 14167) és a Szolgáltató belső szabályzatainak, a megfelelőséget rendszeres külső illetve belső audit, illetve a Nemzeti Hírközlési Hatóság rendszeres vizsgálatai ellenőrzik.

4. Kötelezettségek és felelősség

4.1. A Szolgáltató kötelezettségei

4.1.1. Általános kötelezettségek

A Szolgáltató alapvető kötelezettsége, hogy a szolgáltatást a Szolgáltatási Szabályzatban leírtaknak megfelelően nyújtsa. A Szolgáltató akkor is felelős ezen kötelezettségek betartásáért, ha bizonyos tevékenységeket alvállalkozók segítségével végez. A Szolgáltató részletes kötelezettségeit az Ügyféllel kötött szolgáltatási szerződés, az Általános Szerződési Feltételek és a Szolgáltatási Szabályzat tartalmazzák.

4.1.2. Kötelezettségek az Ügyféllel szemben

A Szolgáltató az Ügyféllel szemben a Magyar Köztársaság Polgári Törvénykönyvének a szerződésszegésért való felelősség szabályai szerint felelős. A Szolgáltató a következő kötelezettségeket vállalja az Ügyféllel szemben:

- A Szolgáltató az Ügyféltől érkező kérésekre időbélyegeket bocsát ki a ETSI TS 101 861 specifikációnak megfelelő formátumban. A kibocsátott időbélyeg a kérelemben szereplő lenyomatra vonatkozik, és tartalmazza a kérelemben szereplő egyedi sorszámot.
- Az Szolgáltató időbélyeget 1 másodperc pontossággal adja ki (az UTC-től való eltérés legfeljebb 1 másodperc lehet). Ennek megfelelően a Szolgáltató saját belső óráját 0,1 másodpercen belüli pontossággal szinkronizálja az UTC-hez, és e szinkronizációt naponta több, mint 4 alkalommal végzi el.
- A Szolgáltató nem ismeri meg az időbélyegzett dokumentum tartalmát.
- A Szolgáltató az időbélyegzés-szolgáltatás megbízhatóságát és biztonságát a minősített szolgáltatókra vonatkozó követelmények szerint biztosítja.
- A Szolgáltató naplózza az időbélyegzés szolgáltatással kapcsolatos minden fontos eseményt, és e naplófájlokat a jogszabályi előírásoknak megfelelően megőrzi.

4.2. Az Ügyfél kötelezettségei

Az Ügyfél kötelezettségeit a Szolgáltatóval szemben a Szolgáltató és az Ügyfél közötti szolgáltatási szerződés illetve az Általános Szerződési Feltételek és a Szolgáltatási Szabályzat tartalmazzák.

4.3. Az Érintett fél kötelezettségei

Az időbélyeget felhasználó Érintett fél kötelessége az időbélyegen szereplő aláírást és az aláírókulcs érvényességét ellenőrizni a Szolgáltatási Szabályzatban leírtak szerint.

4.4. Felelősség

A Szolgáltató felelősségét a Szolgáltatási Szabályzat 2.2. Felelősség című fejezete határozza meg.

Az Ügyfél felelősségét a Szolgáltatási Szabályzat 2.2. Felelősség című fejezete határozza meg.

Az Érintett fél felelősségét a Szolgáltatási Szabályzat 2.2. Felelősség című fejezete határozza meg.

5. Működésre vonatkozó követelmények

5.1. Az időbélyegzés szolgáltatás szabályozása és e szabályozás közzététele

5.1.1. Az időbélyegzés szolgáltatás szabályozása

A Szolgáltató az időbélyegzés szolgáltatást olyan informatikai rendszeren nyújtja, amely a Szolgáltató minősített hitelesítés szolgáltatásával közös fizikai környezetben működik. Ezen rendszer megfelel a jogszabályok által előírt időbélyegzés szolgáltatókra vonatkozó követelményeknek.

5.1.2. Közzétételi nyilatkozat

A Szolgáltató közzéteszi jelen Időbélyegzési Rendet, valamint a Szolgáltatási Szabályzatot mindenkori aktuális változatát. Ezen dokumentumok elérhetőek a Szolgáltató honlapján, valamint megtekinthetőek a Szolgáltató ügyfélszolgálati irodájában.

a) A Szolgáltató elérhetőségét a 1.4. fejezet tartalmazza.

b) A Szolgáltató az időbélyegző egység nyilvános kulcsát (tanúsítvány formájában) a honlapján közzéteszi.

c) Jelen Időbélyegzési Rend azonosítóit, köztük OID-jét a dokumentum fedőlapja, valamint a 1.2. fejezet tartalmazza.

d) Időbélyegzés során a Szolgáltató a MeHVM 2/2002 irányelv 1. mellékletében megnevezett SHA-1 algoritmust alkalmazza.

e) Az Időbélyeg érvényességi ideje megegyezik az időbélyegző szerver tanúsítványának érvényességi idejével, amely legfeljebb 10 év (a tanúsítvány visszavonása esetén kevesebb).

f) Az időbélyegben szereplő idő pontossága – a jogszabályi előírásoknak megfelelően – 1 másodpercen belül van.

g) Az időbélyegzés szolgáltatás Magyarországra terjed ki, a szolgáltatás csak a felhasználó sikeres hitelesítését követően vehető igénybe.

h) Az időbélyegek felhasználói (az Érintett felek) a felhasználás előtt kötelesek meggyőződni az időbélyegen szereplő aláírás helyességéről, és az aláírásra használt tanúsítvány érvényességéről (a részleteket a Szolgáltatási Szabályzat tartalmazza).

i) A Szolgáltató az időbélyegzés szolgáltatás során képződő naplóállományokat – a jogszabályi előírásoknak megfelelően – a keletkezésüktől legalább 10 évig megőrzi.

j) A Szolgáltató által nyújtott időbélyegzés szolgáltatás megfelel a hatályos jogszabályoknak, különösen a 5.4.10. fejezetben leírtaknak.

k) Az esetleges jogi viták rendezése az Általános Szerződési Feltételekben leírtaknak megfelelően történik.

l) A Szolgáltató rendszeresen vizsgálja, hogy a szolgáltatás megfelel a jogszabályoknak, nemzetközi ajánlásoknak és saját belső szabályzatainak, melyeket a 3.4. fejezet ír le. Ezen megfelelőséget a Nemzeti Hírközlési Hatóság is rendszeresen vizsgálja.

5.2. Kulcsgondozás

5.2.1. Az időbélyegzés szolgáltató aláírókulcsának generálása

A Szolgáltató az időbélyegzés szolgáltatás nyújtására használt magánkulcsát kriptográfiai hardvermodulban generálja az elektronikus aláírásról szóló törvény 18. §-ának megfelelő algoritmussal. Az alkalmazott hardvermodult az Európai Unióban tanúsították.

A Szolgáltató magánkulcsának generálásakor kizárólag bizalmi munkakört betöltő dolgozói voltak jelen.

5.2.2. Az időbélyegzés szolgáltató magánkulcsának védelme

A magánkulcsot a Szolgáltató a FIPS 140-1 szabvány 3. szintjén bevizsgált biztonságos hardvermodul segítségével védi. E védelem megfelel a minősített szolgáltatókra vonatkozó jogszabályi előírásoknak.

5.2.3. Az időbélyegzés szolgáltató nyilvános kulcsának közzététele

Az időbélyegzés szolgáltató nyilvános kulcsát tartalmazó tanúsítványt a Szolgáltató a honlapján közzéteszi. Ezen tanúsítványt a Szolgáltató által működtetett hitelesítési egység állította ki. Az ezen hitelesítési egységre vonatkozó előírásokat és a hitelesítési egység kulcsa közzétételének módját a Szolgáltatási Szabályzat tartalmazza.

5.2.4. Az időbélyegzés szolgáltató tanúsítványának érvényessége

Az időbélyegzés szolgáltató tanúsítványának érvényességi ideje 10 év.

5.2.5. Az időbélyegzés szolgáltató aláírókulcsának használatának befejezése

A Szolgáltató időbélyegzés szolgáltatásra használt magánkulcsa az érvényességének lejárta után megsemmisítésre kerül a Szolgáltatási Szabályzat szerint.

Amennyiben a magánkulcsa az érvényességi ideje alatt kompromittálódik, a Szolgáltató gondoskodik a kulcs visszavonásáról a Szolgáltatási Szabályzatban leírtak szerint.

5.2.6. Az alkalmazott kriptográfiai modul életciklusa

A Szolgáltató gondoskodik a kriptográfiai hardvermodul biztonságos kezeléséről a modul teljes életciklusa során. A modul telepítése, tárolása és szállítása és üzembe helyezése szigorú biztonsági feltételek szerint történt. A modul használata során a Szolgáltató a 5.4. fejezetben leírt biztonsági intézkedések szerint gondoskodik a modul védelméről. Amennyiben a modul kikerül a Szolgáltató rendszeréből, a Szolgáltató gondoskodik a modulban lévő kulcsok megsemmisítéséről.

5.3. Időbélyegzés szolgáltatás

5.3.1. Időbélyeg

A Szolgáltató által kibocsátott időbélyeg megfelel az RFC 3161-nek és a jelen Időbélyegzési Rendnek. Ennek megfelelően az időbélyeg:

- a kérelmező által küldött üzenetben szereplő lenyomatot tartalmazza.
- tartalmazza az Időbélyegzési Rend OID-jét.
- egyedi azonosítóval rendelkezik.
- az időbélyegben megadott időpontot a Szolgáltató belső órája adja, amelyet a Szolgáltató két egymástól független Stratum-1 UTC forrással szinkronizál; a Szolgáltató garantálja, hogy a kiadott időbélyegek pontossága legfeljebb 1 másodperccel tér el az UTC időalaptól (lásd Szolgáltatási Szabályzat). Ennek megfelelően a Szolgáltató saját belső óráját 0,1 másodpercen belüli pontossággal szinkronizálja az UTC-hez, és e szinkronizációt naponta több, mint 4 alkalommal végzi el. A Szolgáltató belső órájának pontosságát a Szolgáltató biztonsági bizottsága évente megvizsgálja.
- olyan kulccsal kerül aláírásra, amelyet a Szolgáltató más célra nem használ.

A Szolgáltató rendszeresen ellenőrzi belső órájának helyességét.

5.3.2. Óraszinkronizálás

A Szolgáltató az időbélyegzés szolgáltatás során használt belső óráját szinkronizálja az UTC-hez, a legnagyobb eltérés az UTC-től nem haladhatja meg az 1 másodpercet. Ennek biztosításához a Szolgáltató két független UTC forráshoz szinkronizálja belső óráját.

5.4. Az időbélyegzés szolgáltatás üzemeltetése és menedzsmentje

5.4.1. Biztonsági intézkedések

Az időbélyegzés szolgáltatást a Szolgáltató a minősített hitelesítés szolgáltatással azonos személyi, fizikai és szabályozási környezetben végzi.

5.4.2. Rendszerelemek biztonsági osztályba sorolása

A Szolgáltató kockázatelemzést végzett az időbélyegzés szolgáltatáshoz használt rendszerén. A rendszer egyes elemeit e kockázatelemzés alapján biztonsági osztályokba sorolta. Az egyes biztonsági osztályokba tartozó rendszerelemekre vonatkozó védelmi intézkedéseket olyan módon határozta meg, hogy az őket érintő kockázat elfogadható szintre csökkenjen.

5.4.3. Személyzeti biztonság

A Szolgáltató rendszerének személyzeti biztonsági követelményei megfelelnek a minősített hitelesítés szolgáltatókra vonatkozó jogszabályi előírásoknak. E megfelelést a Szolgáltatási Szabályzat 5.2. és 5.3. fejezetei írják le.

5.4.4. Fizikai biztonság

A Szolgáltató az időbélyegzés szolgáltatást nyújtó rendszerét fizikailag védett környezetben valósította meg. A rendszer megvalósítása során a Szolgáltató különös gondot fordított a tűz és az egyéb elemi károkkal szembeni védelemmel valamint a besugárzással szemben.

A Szolgáltató a rendszerében biztonsági zónákat jelölt ki, és úgy korlátozta alkalmazottai hozzáférését az egyes zónákhoz, hogy minden zónához csak azok az alkalmazottak férhessenek hozzá, akik esetében ez a munkakör ellátásához elengedhetetlenül szükséges. A fokozottan védett biztonsági zónákhoz történő hozzáféréseket olyan beléptető rendszer felügyeli, amely mindkét irányú áthaladásokat naplózza, és mind tudás, mind tulajdon, mind biometriai alapon azonosítja az áthaladó személyeket.

5.4.5. Üzemeltetés menedzsment

A Szolgáltató üzemeltetési folyamatai megfelelnek a minősített hitelesítés szolgáltatókra vonatkozó követelményeknek. E folyamatokra érvényesek a Microsec Kft. társasági szintű szabályozásai, amelyeket az e-Szignó Hitelesítés Szolgáltató belső szabályzatai tovább szigorítanak. A Szolgáltató ISO 9001:2000 minősítési rendszerrel rendelkezik, és emellett rendszeresen auditálják BS 7799 szerint is.

5.4.6. Hozzáférés-menedzsment

A Szolgáltató által alkalmazott hozzáférés-menedzsment rendszer megfelel a minősített hitelesítés szolgáltatókra vonatkozó jogszabályi követelményeknek. Ennek megfelelően:

- A Szolgáltató belső hálózatát tűzfalakkal és más hálózatbiztonsági eszközökkel védi a jogosulatlan hozzáférésektől.
- A Szolgáltató gondoskodik róla, hogy munkatársai csak annyi jogosultsággal rendelkezzenek, amely a munkájuk ellátásához elengedhetetlenül szükséges, amennyiben munkakörül változik, a Szolgáltató gondoskodik a megfelelő jogosultságok megváltoztatásáról illetve visszavonásáról.
- A Szolgáltató gondoskodik róla, hogy a hozzáférések a biztonsági szabályzatának megfelelően történjenek. A Szolgáltató biztonsági szabályzata a jogszabályi előírásoknak megfelelő bizalmi munkakörökbe sorolja be a Szolgáltató munkatársait, és gondoskodik e bizalmi munkakörök jogszabályi előírásoknak megfelelő szétválasztásáról.
- A Szolgáltató munkatársainak minden, az időbélyegzés szolgáltatás nyújtásával összefüggő kritikus művelet elvégzése előtt igazolni kell személyazonosságukat.
- A Szolgáltató minden, az időbélyegzés szolgáltatás nyújtásával összefüggő műveletet naplóz, és megőrzi, hogy mely műveletet mely munkatárs kezdeményezett. Ennek megfelelően a Szolgáltató munkatársai felelősségre vonhatóak a műveletekkel kapcsolatban.
- A Szolgáltató az időbélyegzés szolgáltatás nyújtásához szükséges berendezéseket fizikailag biztonságos környezetben tárolja, és konfigurációjukat rendszeresen ellenőrzi.
- A Szolgáltató riasztó és behatolásvédelmi rendszereket üzemeltet, amelyek azonnal jelzik az illetéktelen fizikai illetve logikai behatolási kísérleteket.

5.4.7. A rendszer telepítése és fejlesztése karbantartása

A Szolgáltató a szolgáltatás nyújtásához megbízható termékeket és rendszereket használ. A Szolgáltató gondoskodik róla, hogy e berendezések védettek legyenek a jogosulatlan módosításokkal szemben. A Szolgáltató kockázatmenedzsment rendszere meghatározza, hogy mely eszközök és termékek kritikusak a szolgáltatás nyújtásával kapcsolatban, és az egyes eszközök esetén milyen biztonsági garanciák szükségesek.

A Szolgáltató rendszerét telepíteni, fejleszteni, és karban tartani kizárólag a Szolgáltató szigorú előírásai mellett szabad. Minden rendszermódosítás elvégzéséhez az e-Szignó Hitelesítés Szolgáltató önálló üzleti egység felelős vezetőjének az engedélye szükséges. A Szolgáltató belső szabályzatai meghatározzák, hogy a rendszermódosítás elvégzése előtt a kockázatelemzést követően milyen tesztek és ellenőrzések szükségesek.

5.4.8. Üzletmenet folytonosság

A Szolgáltató a rendszerét úgy alakította ki, hogy az garantálja a jogszabályok által előírt rendelkezésre állást, valamint biztosítja, hogy a rendelkezésre állás minden pillanatban megállapítható. A Szolgáltató rendelkezik üzletmenet folytonossági tervvel, amely kiemelten foglalkozik a vészhelyzetek kezelésével. Vészhelyzet esetén az időbélyegzés szolgáltatást a Szolgáltató hidegtartalék rendszere is képes biztosítani. Üzletmenet folytonossági tervét és vészhelyzeti terveit a Szolgáltató rendszeresen karbantartja és teszteli.

A Szolgáltató gondoskodik róla, hogy a szolgáltatás biztonságának sérülése esetén minden érintett felhasználót értesít e tényről. Ennek pontos menetét a Szolgáltató belső üzletmenet-folytonossági terve szabályozza.

A Szolgáltató a szolgáltatás biztonságának sérülése esetén kivizsgálja, hogy mi okozta a sérülést, és a sérülés milyen mértékű. Az időbélyegek aláírására használt kulcs kompromittálódása esetén a Szolgáltató értesíti az érintett felhasználókat és ügyfeleket, és a Szolgáltató felfüggeszti az új időbélyegek kibocsátását egészen addig, amíg rendszere ismét biztonságosnak nem tekinthető. Ha az időbélyegek aláírására használt kulcs kompromittálódik, akkor a Szolgáltató az időbélyegző egység tanúsítványát haladéktalanul visszavonja, és minden e kulccsal kibocsátott időbélyeget visszamenőleg is érvénytelennek kell tekinteni. (Lásd: Szolgáltatási Szabályzat 2.1.5 és RFC 3161, 4. fejezet, 2. pont) Vitás esetben az egyes időbélyegek érvényessége a Szolgáltató biztonságos naplófájljai segítségével bizonyítható.

A Szolgáltató ekkor további időbélyegeket csak más kulccsal fog kibocsátani.

Amennyiben a Szolgáltató belső órájának pontossága sérül, a Szolgáltató értesíti az érintett ügyfeleket, és tájékoztatja őket arról, hogy a hibásan kibocsátott időbélyegek hogyan ismerhetőek fel.

5.4.9. A szolgáltatás leállítása

Az időbélyegzés szolgáltatást a Szolgáltató a Szolgáltatási Szabályzat 4.9.2. Az időbélyegzés szolgáltatás leállítása fejezete szerint végzi.

A Szolgáltató a szolgáltatás tervezett megszüntetése esetén legkevesebb 60 nappal a szolgáltatás leállítását megelőzően értesíti a végfelhasználókat és a Hatóságot.

A Szolgáltató az időbélyegzés szolgáltatási tevékenysége befejezésekor az informatikai rendszerében foglalt adatairól teljes körű, minősített időbélyegzővel ellátott mentést készít, és gondoskodik arról, hogy a jogszabályban előírt adatmegőrzési kötelezettségnek valamely megbízható fél eleget tegyen. A Szolgáltató gondoskodik róla, hogy a közzétételi kötelezettségeinek (például, az időbélyegek ellenőrzéséhez szükséges nyilvános kulcs közzététele) valamely megbízható fél eleget tegyen. A Szolgáltató gondoskodik az időbélyegzők aláírásához használt kulcsok megsemmisítéséről.

A szolgáltatás leállításakor az időbélyegző egység tanúsítványát vissza kell vonni. A Szolgáltató a tanúsítvány visszavonását 5 nappal megelőzően hirdetményt tesz közzé.

5.4.10. Jogszabályi megfelelőség

A Szolgáltató minősített időbélyegzés szolgáltatást nyújtó rendszere megfelel a vonatkozó jogszabályoknak, különösen a következőknek:

- Az EU 1999/93 direktíva alapján kidolgozott 2001. évi XXXV. törvény (amely később módosításra került a 2004. évi LV. módosító törvény által) az elektronikus aláírásról.
- 3/2005 IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről (illetve a 16/2001 MeH irányelv az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről).
- 2/2002 MeH irányelv a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről.

5.4.11. Időbélyegzés szolgáltatással kapcsolatos adatok naplózása

A Szolgáltató rendszere a következő eseményeket naplózza az időbélyegzés szolgáltatással kapcsolatosan:

- Az időbélyegek kibocsátása során bekövetkező események.
- Az Ügyféllel történő szerződéskötés és az Ügyfél jelszó-módosítási kérelmei.

- Az időbélyegzés szolgáltató kulcsával és tanúsítványával kapcsolatos események.
- A naplófájlok feldolgozásával kapcsolatos események.

A Szolgáltató a naplófájlokat napi rendszerességgel elemzi. A Szolgáltató a naplófájlokat a jogszabályi előírásoknak megfelelő módon és időtartamig megőrzi.

5.5. Szervezeti felépítés

A minősített időbélyegzés szolgáltatást a Microsec Kft. önálló üzleti egysége, az e-Szignó Hitelesítés Szolgáltató végzi. Az e-Szignó Hitelesítés Szolgáltatón belül a hitelesítő szervezet végzi a 2.1. fejezetben leírt szolgáltatásokat, míg az ügyfélszolgálati iroda az Ügyféllel való kapcsolattartásért felelős.

A. FOGALMAK

Elektronikus aláírás (Electronic Signature)
Elektronikusan aláírt elektronikus dokumentumhoz azonosítás céljából logikailag hozzárendelt vagy azzal elválaszthatatlanul összekapcsolt elektronikus adat.

Elektronikus aláírás ellenőrzése (Electronic Signature Validation)
Az elektronikus dokumentum aláíráskori, illetve ellenőrzéskori tartalmának összevetése, továbbá az aláíró személyének azonosítása a dokumentumon szereplő, illetve a Szolgáltató által közzétett aláírás-ellenőrző adat, valamint a tanúsítvány felhasználásával.

Elektronikus aláírás felhasználása
Elektronikus adat elektronikus aláírással történő ellátása, illetve elektronikus aláírás ellenőrzése.

Elektronikusan történő aláírás
Elektronikus aláírás hozzárendelése, illetve logikailag való hozzárendelése az elektronikus adathoz.

Elektronikus dokumentum
Elektronikus eszköz útján értelmezhető adat, mely elektronikus aláírással van ellátva.

Érintett fél (Relying Party)
Az időbélyeg felhasználója, aki az időbélyegre hagyatkozva jár el.

Hardver kriptográfiai eszköz, biztonságos hardvermodul, kriptográfiai hardvermodul
Egy olyan hardver alapú biztonságos eszköz, mely előállítja, tárolja és védi a kriptográfiai kulcsokat, valamint biztonságos környezetet biztosít a kriptográfiai funkciók végrehajtására. Megjegyzés: Lehetséges példák ilyen eszközre: PC bővítő kártya, intelligens kártya, USB token.

Hatóság

Az elektronikus aláírással kapcsolatos szolgáltatásokat nyújtó szolgáltatókat felügyelő hatóság, a Nemzeti Hírközlési Hatóság.

Hitelesítő egység
A hitelesítés szolgáltató rendszerének egy egysége, amely tanúsítványok aláírását végzi. Egy hitelesítő egységhez mindig egy aláírókulcs tartozik. Előfordulhat, hogy egy szolgáltató egyszerre több hitelesítő egységet is működtet.

Kriptográfiai magánkulcs
Egy kriptográfiai kulcspár egyik kulcsa. A titkos kulcsot titokban kell tartani, mert például aláírásra szolgáló kulcspár esetén a magánkulcs birtokában bárki aláírhat a kulcs tulajdonosa nevében. Ezért a magánkulcsokat (más néven aláíráslétrehozó adatot) biztonságos aláíráslétrehozó eszközön szokás tárolni.

Kriptográfiai nyilvános kulcs
Egy kriptográfiai kulcspár egyik kulcsa. A nyilvános kulcsot nem szükséges titokban tartani, aláírásra szolgáló kulcspár esetén a nyilvános kulcs szolgál az aláírás ellenőrzésére (lásd: aláíráslétrehozó adat).

Időbélyegző (Time Stamp)
Egy elektronikus dokumentumhoz hozzárendelt vagy azzal logikailag összekapcsolt adat, amely segítségével igazolható, hogy a dokumentum változatlan az időbélyegző elhelyezésének időpontjában létező állapothoz képest.

Időbélyegzési rend
Olyan szabálygyűjtemény, amelyben a Szolgáltató az általa kibocsátott időbélyegzők felhasználásának feltételeit írja elő igénybe vevők valamely közös biztonsági követelményekkel rendelkező csoportja, illetőleg meghatározott alkalmazások számára.

Informatikai rendszer
A szolgáltató által a szolgáltatói kulcspár kezeléséhez, az aláírás létrehozó adat előállításához, a tanúsítványok kibocsátásához, a kibocsátott tanúsítványt tartalmazó nyilvántartáshoz, a visszavonási nyilvántartásokhoz és a visszavonás kezelési szolgáltatáshoz, valamint e tevékenységek informatikai védelméhez használt, az Eat. 3. számú mellékletének f) pontja szerinti megbízható rendszerek és termékek.

Kompromittálódik
Egy kriptográfiai kulcs akkor kompromittálódik, ha illetéktelen személyek is megismerik.

Kriptográfiai Kulcs (Key)
Olyan kriptográfiai transzformációt vezérlő egyedi digitális jelsorozat, amelynek ismerete rejtjelezéshez és visszaállításhoz, specifikusan az elektronikus aláírás előállításához, illetőleg ellenőrzéséhez szükséges.

Kulcsgondozás (Key Management)
A kriptográfiai kulcsok előállítása, a felhasználókhoz történő eljuttatása vagy ennek algoritmikus megvalósítása, továbbá a kulcsok nyilvántartása, tárolása, archiválása, visszavonása, törlése, szoros kapcsolatban az alkalmazott biztonsági eljárásmóddal.

Minősített elektronikus aláírás (Qualified Electronic Signature)
Olyan fokozott biztonságú elektronikus aláírás, amely biztonságos aláírás létrehozó eszközzel készült és amelynek hitelesítése céljából minősített tanúsítványt bocsátottak ki.

Minősített hitelesítési rend(Qualified Certificate Policy)
Olyan tanúsítványtípus, amely megfelel az elektronikus aláírási törvény 2. és 3. mellékletében foglalt követelményeknek.

Minősített Szolgáltató (Qualified Certification Service Provider)
Az elektronikus aláírási törvény 3. számú mellékletében foglalt követelményeknek megfelelő, valamint ennek alapján nyilvántartásba vett Szolgáltató.

Minősített tanúsítvány (Qualified Certificate)
Az elektronikus aláírási törvény 2. számú mellékletében foglalt követelményeknek megfelelő olyan tanúsítvány, amelyet minősített szolgáltató bocsátott ki.

Nyilvános (publikus) kulcsú infrastruktúra (Public Key Infrastructure, PKI)
Az elektronikus aláírás létrehozására, ellenőrzésére, kezelésére szolgáló, aszimmetrikus kulcspárt alkalmazó infrastruktúra, beleértve a mögöttes intézményrendszert, a különböző szolgáltatókat és eszközöket is.

Szolgáltatási szabályzat (Certificate Practice Statement)
A Szolgáltató tevékenységével kapcsolatos részletes eljárási és egyéb működési szabályokat tartalmazó szabályzat.

Szolgáltatási Szerződés
Olyan szerződés, melynek keretében az Aláíró és az Aláíró Szervezete hitelesítés szolgáltatást (Hitelesítés Szolgáltatási Szerződés) vagy egyéb szolgáltatást rendel meg a Szolgáltatótól.

Szolgáltató
Jelen dokumentumban a MICROSEC Kft., amely az Elektronikus aláírás törvényben [1] foglaltaknak megfelelő a hitelesítés-szolgáltatást, az aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatást és időbélyegzés szolgáltatást minősített szolgáltatóként nyújtja.

Szolgáltatói magánkulcs (CA private key)
Olyan kriptográfiai magánkulcs, amelyet a Szolgáltató vagy az időbélyegzést nyújtó szolgáltató saját elektronikus aláírási szolgáltatásának igazolására, így különösen a tanúsítvány kibocsátására, a visszavonási nyilvántartásokra, az időbélyegzésre, a naplózáshoz, az archiváláshoz használ.

Szolgáltatói nyilvános kulcs (CA public key)
Olyan kriptográfiai nyilvános kulcs, amelyet a szolgáltatói magánkulcs használatával létrehozott elektronikus aláírás ellenőrzésére használnak.

Tanúsítvány (Certificate)
A Szolgáltató által kibocsátott igazolás, amely az aláírás-ellenőrző adatot egy meghatározott személyhez kapcsolja, akinek személyazonosságáról meggyőződött.

Visszavonási nyilvántartások
Nyilvántartások a felfüggesztett, illetőleg a visszavont tanúsítványokról, amelyek tartalmazzák legalább a felfüggesztés vagy visszavonás tényét, és a felfüggesztés vagy visszavonás időpontját.

Visszavonási állapot közzététele (Revocation status service)
Információ nyújtása az érintett (fogadó) fél számára a tanúsítványok visszavonásáról. A szolgáltatás lehet valós idejű, vagy az információk előre meghatározott időközönkénti aktualizálásán kell alapulnia.

B. RÖVIDÍTÉSEK

CA: Certification Authority, Hitelesítés Szolgáltató
CRL: Certificate Revocation List, Tanúsítvány visszavonási lista
OCSP: On-line Certificate Status Response, On-line tanúsítvány állapot válasz
NHH: Nemzeti Hírközlési Hatóság
RA: Registration Authority, Regisztráló szervezet
TSA: Time Stamping Authority, Időbélyegzés Szolgáltató
CP: Certificate Policy, Tanúsítványtípus, Hítelesítési Rend
CPS: Certificate Practice Statement, Hitelesítés Szolgáltatási Szabályzat
UTC: Coordinated Universal Time

C. HIVATKOZÁSOK

Jelen dokumentum 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] 16/2001. (IX. 1.) MeHVM rendelet az elektronikus aláírásokkal kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről.

[4] 3/2005 IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről.

[6] FIPS PUB 140-1 (1994. január 11): "Kriptográfiai modulok biztonsági követelményei"

[7] ETSI TS 101 456 Minősített tanúsítványokat kibocsátó Szolgáltatókra vonatkozó szabályozási követelmények

[8] ETSI TS 101 862 Minősített tanúsítvány profil

[9] CEN 14167-1 munkacsoport egyezmény: „Biztonsági követelmények elektronikus aláírásokkal kapcsolatos tanúsítványokat kezelő rendszerek megbízható rendszereire”

[10] MSZ ISO/IEC 15408:2002 Az információbiztonság értékelésének közös szempontrendszere (Common Criteria for Information Technology Security Evaluation version 2.1):

[11] EU Directive 1999/93/EC of the European Parliament and the council of 13 December 1999 on a Community framework for electronic signatures;

[12] Minősített e-Szignó Hitelesítés Szolgáltató elektronikus aláírással kapcsolatos szolgáltatásaira vonatkozó Szolgáltatási Szabályzat, Microsec Kft., e-Szignó Hitelesítés Szolgáltató, 1.3.6.1.4.1.21528.2.1.1.1

[13] e-Szignó Hitelesítés Szolgáltató által nyújtott időbélyegzés és on-line tanúsítvány állapot szolgáltatásokra vonatkozó Általános Szerződési Feltételek, OID: 1.3.6.1.4.1.21528.2.1.1.5

[14] RFC 3161: Time-Stamp Protocol (TSP)

[15] ETSI TS 102 023 EU szabvány: Policy requirements for time-stamping authorities

[16] ETSI TS 101 861: Time Stamping profile

[17] 3/2005 IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről