MICROSEC
Számítástechnikai Fejlesztő zrt.

e-Szignó Hitelesítés Szolgáltató nem minősített időbélyegzési rend

e-SZIGNÓ

Azonosító:	1.3.6.1.4.1.21528.2.1.1.23.2.0
Verzió:	2.0
Első verzió hatálybalépése:	2006-11-19
Biztonsági besorolás:	NYILVÁNOS
Jóváhagyta:	Ellbogen András
Jóváhagyás dátuma:	2012-03-30
Hatálybalépés dátuma:	2012-05-01

Microsec Számítástechnikai Fejlesztő zártkörűen működő Részvénytársaság
1031 Budapest, Záhony utca 7. D. épület

Változáskövetés

Verzió	A változás leírása	Hatálybalépés	Készítette
1.0	Első változat	2006-11-19	Dr. Berta István Zsolt
2.0	Új OID hozzárendelése. OID: 1.3.6.1.4.1.21528.2.1.1.23.1.1	2006-12-04	Dr. Berta István Zsolt
1.2	A fogyasztóvédelem elérhetősége megváltozott. OID: 1.3.6.1.4.1.21528.2.1.1.23.1.2	2007-10-28	Dr. Berta István Zsolt
1.3	A fogyasztóvédelem elérhetősége megváltozott. OID: 1.3.6.1.4.1.21528.2.1.1.23.1.3	2008-01-01	Dr. Berta István Zsolt
1.4	Nem lépett hatályba. OID: 1.3.6.1.4.1.21528.2.1.1.23.1.4	2008-10-01	Dr. Berta István Zsolt
1.5	Az időbélyegek naplózásának megszüntetése. OID: 1.3.6.1.4.1.21528.2.1.1.23.1.5	2008-12-20	Dr. Berta István Zsolt
2.0	Cégforma változás. OID: 1.3.6.1.4.1.21528.2.1.1.23.2.0	2012-05-01	Dr. Berta István Zsolt

Tartalomjegyzék

1. Bevezetés

Jelen dokumentum a Microsec Számítástechnikai Fejlesztő zrt. (továbbiakban: Szolgáltató) által üzemeltetett e-Szignó Hitelesítés Szolgáltató által támogatott nem minősített 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 [1] 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 „e-Szignó Hitelesítés Szolgáltató – nem minősített elektronikus aláírás hitelesítés szolgáltatásra és nem minősített időbélyegzés szolgáltatásra vonatkozó – szolgáltatási szabályzat" című dokumentum [2] tartalmazza.

1.2. Azonosítás

A dokumentum címe, azonosítója és verziószáma a dokumentum címlapján található. 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):

- Előfizető, 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 zártkörűen működő Részvénytársaság
Cégjegyzékszám:	01-10-047218 Fővárosi Törvényszék Cégbírósága
Székhely:	1031 Budapest, Záhony utca 7. D. épület
Telefonszám:	(+36-1) 505-4444
Telefax szám:	(+36-1) 505-4445
Internet cím:	`http://www.microsec.hu`, `http://www.e-szigno.hu`

1.4.2. Ügyfélszolgálati iroda

A Szolgáltató ügyfélszolgálati irodájának elérhetőségét, nyilvatartását és az illetékes fogyasztóvédelmi szerv elérhetőségét a Szolgáltatási Szabályzat tartalmazza.

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 [2] határozza meg.

2.2. Időbélyegzés szolgáltató

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

2.3. Végfelhasználók

Az időbélyegzés szolgáltatás végfelhasználói a következő felek lehetnek:

- Az Előfizető (ügyfél), aki előfizet a Szolgáltató által nyújtott időbélyegzés szolgáltatásra, és a szolgáltatás keretében időbélyegeket kér a Szolgáltatótól. Az Előfizető 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 az „e-Szignó Hitelesítés Szolgáltató – nem minősített elektronikus aláírás hitelesítés szolgáltatásra és nem minősített időbélyegzés szolgáltatásra vonatkozó – általános szerződési feltételek” (a továbbiakban Általános Szerződési Feltételek) című dokumentummal [3], 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 megfelelően. A szolgáltatás nyújtása során a Szolgáltató az ETSI TS 101 861 [1], illetve az RFC 3161 [4] specifikációknak megfelelő formátumú időbélyegeket nyújt az Előfizető 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 nem minősített időbélyegzés szolgáltatás nyújtó rendszere megfelel a vonatkozó jogszabályoknak. 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. [5] törvénynek és a hozzá kapcsolódó 3/2005 IHM rendeletnek az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről. [6]

E dokumentum megfelel a nemzetközi ajánlásoknak (ETSI TS 102 023 [7], ETSI TS 101 861 [1], RFC 3161 [4], CEN CWA 14167 [11]) 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 Előfizetővel kötött szolgáltatási szerződés, az Általános Szerződési Feltételek és a Szolgáltatási Szabályzat tartalmazzák.

4.1.2. Kötelezettségek az Előfizetővel szemben

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

- A Szolgáltató az Előfizetőtől érkező kérésekre időbélyegeket bocsát ki a ETSI TS 101 861 [1] 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 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 az időbélyegzés 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 Előfizető kötelezettségei

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

4.3. Az Érintett félre vonatkozó ajánlások

Az időbélyeget felhasználó Érintett félnek célszerű ellenőriznie az időbélyegen szereplő aláírást és az aláírókulcs érvényességét a Szolgáltatási Szabályzatban leírtak szerint. Ha az Érintett fél nem így jár el az időbélyeg felhasználásakor, a Szolgáltató nem vállal felelősséget a felmerülő károkért.

4.4. Felelősség

A Szolgáltató felelősségét a Szolgáltatási Szabályzat határozza meg.

Az Előfizető felelősségét a Szolgáltatási Szabályzat határozza meg.

Az Érintett fél felelősségét is a Szolgáltatási Szabályzat 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 biztonságos informatikai rendszeren nyújtja, amely megfelel a jogszabályok által előírt, időbélyegzés szolgáltatókra vonatkozó követelményeknek.

5.1.2. Közzétételi nyilatkozat

A Szolgáltató közzéteszi jelen Időbélyegzési Rend, valamint a Szolgáltatási Szabályzat 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 Nemzeti Hírközlési Hatóság által meghatározott biztonságos algoritmusokat 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) Jelen időbélyegzési rend területi hatálya Magyarország területe. A Szolgáltató működésére vonatkozóan a mindenkori magyar jogszabályok az irányadóak.

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

h) A szolgáltatás csak a felhasználó sikeres hitelesítését követően vehető igénybe.

i) Az időbélyegeket felhasználó az Érintett feleknek az időbélyegek felhasználása előtt célszerű meggyőződni az időbélyegen szereplő aláírás helyességéről, és az aláírásra használt tanúsítvány érvényességéről (a részleteket a Szolgáltatási Szabályzat tartalmazza).

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

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

l) Az esetleges jogi viták rendezése a Szolgáltatási Szabályzatban [2] leírtaknak megfelelően történik.

m) A Szolgáltató rendszeresen vizsgálja, hogy a szolgáltatás megfelel a jogszabályoknak, nemzetközi ajánlásoknak és saját belső szabályzatainak, melyeket a 3.4. fejezet ír le.

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 lehetnek jelen.

5.2.2. Az időbélyegzés szolgáltató magánkulcsának védelme

A magánkulcsot a Szolgáltató a FIPS 140-1 szabvány [8] 3. szintjén bevizsgált biztonságos hardvermodul segítségével védi. E védelem megfelel az időbélyegzés 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.

5.3. 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.
- 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 biztonságos 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 az időbélyegzés szolgáltatókra vonatkozó jogszabályi előírásoknak. E megfelelést a Szolgáltatási Szabályzat írja 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 védelemre, valamint a besugárzással szembeni védekezésre.

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.

5.4.5. Üzemeltetés menedzsment

A Szolgáltató üzemeltetési folyamatai megfelelnek az időbélyegzés szolgáltatókra vonatkozó követelményeknek. E folyamatokra érvényesek a Microsec zrt. 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 ISO 27001 szerint is.

5.4.6. Hozzáférés-menedzsment

A Szolgáltató által alkalmazott hozzáférés-menedzsment rendszer megfelel az időbélyegzés szolgáltatókra vonatkozó jogszabályi követelményeknek. Ennek megfelelően:

- A Szolgáltató belső hálózatát tűzfalakkal és más hálózatbiztonsági eszközökkel védi a jogosulatlan hozzáférésektől.
- A Szolgáltató gondoskodik arról, hogy munkatársai csak annyi jogosultsággal rendelkezzenek, amennyi a munkájuk ellátásához elengedhetetlenül szükséges; amennyiben munkakörük változik, a Szolgáltató gondoskodik a megfelelő jogosultságok megváltoztatásáról illetve visszavonásáról.
- A Szolgáltató gondoskodik arról, hogy a hozzáférések 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 azonosítaniuk kell magukat.
- 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, fejlesztése és karbantartása

A Szolgáltató a szolgáltatás nyújtásához megbízható termékeket és rendszereket használ. A Szolgáltató gondoskodik arról, 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 ellenőrizhető. 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, valamint 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, ezt követően minden e kulccsal kibocsátott időbélyeget visszamenőleg is érvénytelennek kell tekinteni. (Lásd: Szolgáltatási Szabályzat és RFC 3161, 4. fejezet, 2. pont) Vitás esetben az egyes időbélyegek érvényessége a Szolgáltató biztonságos naplófájljai segítségével bizonyítható.

A Szolgáltató az időbélyegző kulcsának kompromittálódása esetén a további időbélyegeket csak más kulccsal fogja 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 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. Megfelelőség

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

- Az EU 1999/93 direktíva [9] alapján kidolgozott 2001. évi XXXV. törvény (amely később módosításra került a 2004. évi LV. módosító törvény által) az elektronikus aláírásról. [5]
- 3/2005 IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről. [6]

- Jelen időbélyegzési rend megfelel az Informatikai és Hírközlési Minisztérium által közzétett, időbélyegzés formátumra vonatkozó követelményrendszerének. [10]

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 Előfizetővel történő szerződéskötés és az Előfizető jelszó-módosítási kérelmei.
- Az időbélyegzés szolgáltató kulcsával és tanúsítványával kapcsolatos események.
- A naplófájlok feldolgozásával kapcsolatos események.

Maguk az időbélyegek nem kerülnek naplózásra.

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

5.5. Szervezeti felépítés

A szolgáltatást a Microsec zrt. 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 Előfizetővel való kapcsolattartásért felelős.

A. Fogalmak

Aláírás-ellenőrző adat (Signature-Verification Data): Olyan egyedi adat (jellemzően kriptográfiai nyilvános kulcs), amelyet az elektronikusan aláírt elektronikus dokumentumot megismerő személy az elektronikus aláírás ellenőrzésére használ.

Aláírás-létrehozó adat (Signature-Creation Data): Olyan egyedi adat (jellemzően kriptográfiai magánkulcs), amelyet az aláíró az elektronikus aláírás létrehozásához használ.

Aláíró (Signatory): Az a természetes személy, aki az aláírás-létrehozó adat kizárólagos használatára jogosult.

Biztonságos aláírás-létrehozó eszköz (BALE): Az elektronikus aláírásról szóló törvény 1. számú mellékletében foglalt követelményeknek eleget tevő aláírás-létrehozó eszköz.

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

Fokozott biztonságú elektronikus aláírás (Advanced Electronic Signature): E lektronikus aláírás, amely megfelel a következő követelményeknek

- alkalmas az aláíró azonosítására és egyedülállóan hozzá köthető,
- olyan eszközzel hozták létre, amely kizárólag az aláíró befolyása alatt áll,
- a dokumentum tartalmához technikailag olyan módon kapcsolódik, hogy minden – az aláírás elhelyezését követően az iraton, illetve dokumentumon tett – módosítás érzékelhető.

Hardver kriptográfiai eszköz: 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.

Érintett fél (Relying Party): Az elektronikus dokumentum fogadója, aki egy adott tanúsítványra, illetve időbélyegre hagyatkozva jár el.

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

Hitelesítési rend: Olyan szabálygyűjtemény, amelyben a Szolgáltató valamely tanúsítvány felhasználásának feltételeit írja elő igénybe vevők valamely közös biztonsági követelményekkel rendelkező csoportja, illetőleg meghatározott alkalmazások számára.

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.

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.

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

Kriptográfiai Kulcs (Key): Olyan kriptográfiai transzformációt vezérlő egyedi digitális jelsorozat, amelynek ismerete titkosításához és dekódolásához, 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 hitelesítés-szolgáltató (Qualified Certification Service Provider): Az elektronikus aláírási törvény 3. számú mellékletében foglalt követelményeknek megfelelő, valamint ennek alapján nyilvántartásba vett hitelesítés-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.

Rendkívüli üzemeltetési helyzet: Olyan, a szolgáltató üzemmenetében zavart okozó rendkívüli helyzet, amikor a szolgáltató rendes üzemmenetének folytatására ideiglenesen vagy véglegesen nincsen lehetőség;

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

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

B. Rövidítések

CA: Certification Authority, Hitelesítés Szolgáltató
CRL: Certificate Revocation List, Tanúsítvány visszavonási lista
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

[1] ETSI TS 101 861: Time Stamping profile.

[2] e-Szignó Hitelesítés Szolgáltató – nem minősített elektronikus aláírás hitelesítés szolgáltatásra és nem minősített időbélyegzés szolgáltatásra vonatkozó – szolgáltatási szabályzat.

[3] e-Szignó Hitelesítés Szolgáltató – nem minősített elektronikus aláírás hitelesítés szolgáltatásra és nem minősített időbélyegzés szolgáltatásra vonatkozó – általános szerződési feltételek.

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

[5] 2001. évi XXXV. törvény az elektronikus aláírásról (a 2004. évi módosításokkal).

[6] 3/2005. (III.18.) IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről.

[7] ETSI TS 102 023: Policy requirements for time-stamping authorities.

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

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

[10] Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható időbélyegzés formátum műszaki specifikációjára, 2006.

[11] CEN 14167-1 munkacsoport egyezmény: "Biztonsági követelmények elektronikus aláírásokkal kapcsolatos tanúsítványokat kezelő rendszerek megbízható rendszereire".