MICROSEC
Számítástechnikai Fejlesztő zrt.

e-Szignó Hitelesítés Szolgáltató – minősített elektronikus archiválás szolgáltatásra vonatkozó – archiválási rend

e-SZIGNÓ

Azonosító:	1.3.6.1.4.1.21528.2.1.1.19.2.0
Verzió:	2.0
Első verzió hatálybalépése:	2006-12-15
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 OID: 1.3.6.1.4.1.21528.2.1.1.19	2006-12-15	Dr. Berta István Zsolt
1.1	Módosítás a Nemzeti Hírközlési Hatóság észrevételeinek megfelelően OID: 1.3.6.1.4.1.21528.2.1.1.19.1.1	2007-01-08	Dr. Berta István Zsolt
1.2	A fogyasztóvédelem elérhetőségének változása OID: 1.3.6.1.4.1.21528.2.1.1.19.1.2	2008-01-01	Dr. Berta István Zsolt
1.3	Nem lépett hatályba. OID: 1.3.6.1.4.1.21528.2.1.1.19.1.3	2008-10-01	Dr. Berta István Zsolt
1.4	Megfelelés az NHH által kibocsátott követelményrendszernek OID: 1.3.6.1.4.1.21528.2.1.1.19.1.4	2008-12-20	Dr. Berta István Zsolt
2.0	Cégforma változás. Változás az archivált akták titkosításával kapcsolatban. OID: 1.3.6.1.4.1.21528.2.1.1.19.2.0	2012-05-01	Dr. Berta István Zsolt

Tartalomjegyzék

1. Bevezetés

Jelen dokumentum a Microsec zrt. (továbbiakban: Szolgáltató) által üzemeltetett e Szignó Hitelesítés Szolgáltató által támogatott archiválási rendet tartalmazza.

1.1. Áttekintés

Az *archiválási rend* egy szabálygyűjtemény, amely az elektronikus archiválás szolgáltatás felhasználhatóságát határozza meg egy közös biztonsági követelményekkel rendelkező közösség és/vagy alkalmazások egy osztálya számára.

Az archiválási rend alapvető követelményeket fogalmaz meg az archiválás szolgáltatással kapcsolatban. Ezen követelmények teljesítésének módját, illetve az itt megnevezett eljárások részletes leírását az e-Szignó Hitelesítés Szolgáltató által kibocsátott „e-Szignó Hitelesítés Szolgáltató – minősített elektronikus archiválás szolgáltatásra vonatkozó – szolgáltatási szabályzat" [1] (a továbbiakban Szolgáltatási Szabályzat) határozza meg.

Jelen dokumentum az „e-Szignó Hitelesítés Szolgáltató – minősített elektronikus archiválás szolgáltatásra vonatkozó – archiválási rend" (OID: 1.3.6.1.4.1.21528.2.1.1.19) című archiválási rendet definiálja.

1.1.1. Hatály

Jelen archiválási rend a dokumentum címlapján feltüntetett hatálybalépési dátumtól határozatlan ideig hatályos. A hatályosság megszűnik jelen dokumentum újabb verziójának hatályba lépésekor vagy a dokumentum hatályon kívül helyezésekor.

Az archiválási rend hatálya a Szolgáltatóra és az Előfizetőre terjed ki.

Az archiválási rend szerint elektronikusan nyújtott szolgáltatások az egész világon elérhetőek. A jelen archiválási rend szerint archivált dokumentumok, érvényességi láncok, illetve a velük kapcsolatban kiállított igazolások érvényessége független attól, hogy mely földrajzi helyről küldték őket be az archívumba, illetve mely földrajzi helyről kérték le őket.

A Szolgáltató működésére vonatkozóan a mindenkori magyar jogszabályok az irányadóak. Az elektronikus archiválás szolgáltatás jogszabályi alapját az [2] törvény teremtette meg.

1.1.2. A Szolgáltató

A Szolgáltató adatai

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`

A Microsec zrt. az e-Szignó Hitelesítés Szolgáltató önálló üzleti egységhez rendeli az elektronikus aláírással kapcsolatos szolgáltatások – köztük az elektronikus archiválás szolgáltatás – nyújtását.

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

A Szolgáltató bemutatása

A Microsec 2002. május 30. óta szerepel a Hatóság (illetve annak jogelődje) nyilvántartásában nem minősített szolgáltatóként a 2001. évi XXXV. törvényben meghatározott elektronikus aláírás hitelesítés szolgáltatás, időbélyegzés és aláírás-létrehozó adat elhelyezése aláírás-létrehozó eszközön szolgáltatás (a továbbiakban eszköz szolgáltatás) vonatkozásában. Regisztrációs szám: MH 6834 1/2002.

A Microsec 2005. május 15. óta minősített szolgáltatóként is szerepel a Hatóság (illetve annak jogelődje) nyilvántartásában elektronikus aláírás hitelesítés szolgáltatás, időbélyegzés és eszköz szolgáltatás vonatkozásában.

A Microsec minősített elektronikus archiválás szolgáltatást nyújtó szolgáltatóként is szerepel a Hatóság (illetve annak jogelődje) nyilvántartásában. (A nyilvántartásba vételről szóló határozat ügyiratszáma: HL-3549-2/2007.) Az elektronikus archiválás szolgáltatás indításának időpontja 2007. február 1.

Minőség és információbiztonság

A Microsec kiemelten fontosnak tartja ügyfelei elégedettségét. A magas színvonalú szolgáltatások fenntartása érdekében a Szolgáltató ISO 9001 szabványnak megfelelő minőségbiztosítási rendszert üzemeltet 2002. január 23. óta. A szabványnak való megfelelést a Lloyd's Register Quality Assurance ellenőrizte. A Microsec nagy figyelmet szentel az általa

üzemeltetett rendszerek biztonságára, ezért fő tevékenységi területein a MSZ/ISO/IEC 27001-nek megfelelő információbiztonság-irányítási rendszert (korábban BS 7799) üzemeltet 2003. május 19. óta. A szabványnak való megfelelést a Lloyd's Register Quality Assurance ellenőrizte. A Szolgáltató önkéntes akkreditációs rendszer keretében nem lett tanúsítva, mert ilyen rendszer Magyarországon még nem működik.

1.1.3. Szolgáltatások

A Szolgáltató jelen archiválási rend keretében minősített szolgáltatóként nyújtja az elektronikus archiválás szolgáltatást a vele szerződést kötő Előfizető részére. Az elektronikus archiválás szolgáltatást a 2001. évi XXXV. törvény definiálja, és e szolgáltatás a következőket foglalja magában (a továbbiakban együttesen röviden *Szolgáltatások*):

- Az Előfizető elektronikusan aláírt fájlokat tölthet fel a Szolgáltató által üzemeltetett archívumba. A Szolgáltató ellenőrzi az elektronikus aláírást, összeállítja az érvényességi láncot, majd biztosítja az elektronikus aláírással ellátott e-aktákban (dokumentumokban[1]) elhelyezkedő elektronikus aláírások hosszú távú hitelességét (lásd: 3.2. fejezet).

- A Szolgáltató biztonságosan tárolja az e-aktákat (fájlokat és érvényességi láncokat), és biztosítja, hogy kizárólag arra az arra jogosultak férhetnek hozzájuk. (Lásd: 5. fejezet.) A Szolgáltató a megőrzés során biztosítja, hogy az e-aktákat utólag ne lehessen módosítani, és biztosítja, hogy az e-aktákhoz az arra jogosult Előfizető folyamatosan hozzáférjen. A Szolgáltató a megőrzés során kizárja a jogosulatlan hozzáférést, módosítást és törlést, és a megőrzés ideje alatt biztosítja az e-akták és a bennük szereplő fájlok hosszú távú olvashatóságát. A megőrzés a szolgáltatási szerződés időtartamára szól.

- Az Előfizető a Szerződés időtartama alatt folyamatosan elérheti a Szolgáltató archívumában szereplő fájlokat, dokumentumokat, aláírásokat, illetve a hozzájuk tartozó érvényességi láncokat (lásd: 3.3).

- Az Előfizető kérésére a Szolgáltató igazolást bocsát ki arról, hogy az egyes dokumentumokat tárolja, és az egyes dokumentumokon az archiválás pillanatában érvényes elektronikus aláírás szerepelt (lásd: 3.4. fejezet).

- Az Előfizető kérésére a Szolgáltató törli a dokumentumokat az archívumából (lásd: 3.6. fejezet).

A Szolgáltató kizárólag azt a változatát nyújtja az elektronikus aláírásról szóló törvény [2] szerint definiált elektronikus archiválás szolgáltatásnak, amely szerint az Előfizető az aláírt

[1] Az itt szereplő fogalmakat (pl.: fájl, dokumentum, aláírás, e-akta) a Fogalmak meghatározása című fejezet (1.7) definiálja.

fájlokat is feltölti az archívumba. Ez azt jelenti, hogy a Szolgáltató nem nyújtja az elektronikus archiválás szolgáltatás azon változatát, amely szerint az archiválás szolgáltató kizárólag az aláírt fájl lenyomatát kapja meg.

A Szolgáltató elektronikus aláírások hosszú távú érvényességének biztosításával foglalkozik. Nem fogad el olyan fájlokat, amelyeken kizárólag időbélyeg szerepel, és elektronikus aláírás nincsen rajta. A Szolgáltató archiválás szolgáltatása kizárólag olyan időbélyegek hosszú távú érvényességét biztosítja, amelyek ETSI TS 101 903 formátumú (például ún. XAdES-T) aláírásokban helyezkednek el.

A Szolgáltató a Szolgáltatási Szabályzatában meghatározza, hogy milyen formátumú fájlok hosszú távú olvashatóságát biztosítja.

1.2. Szabványok és előírások

Jelen archiválási rend tartalmi vonatkozásokban eleget tesz a vonatkozó hazai jogszabályok előírásainak és ajánlásainak [2], [3].

A jelen archiválási rend szerint nyújtott elektronikus archiválás szolgáltatás egyes elemei a következő szabványoknak és előírásoknak felelnek meg:

- Az archiválás szolgáltatást nyújtó rendszer az X.509 „Információ technológia – Nyílt rendszerek kapcsolódása – Könyvtár: Nyilvános kulcs és attribútum tanúsítvány keretrendszer” ajánlás 3. verziójának [18], illetve az RFC 3280 [4] specifikációnak, valamint a [5] specifikációnak megfelelő tanúsítványokat használ és fogad el.
- A Szolgáltatások nyújtása során felhasznált minősített időbélyeg megfelel az RFC 3161: Time-Stamp Protocol (TSP) ajánlásban megfogalmazottaknak [6], valamint a [7] specifikációnak.
- A Szolgáltató az ETSI TS 101 903 (XAdES) [8] specifikációnak megfelelő elektronikus aláírásokat fogad el. Ennek megfelelően elfogadja a [9] specifikációnak megfelelő aláírásokat is.
- A Szolgáltató a CWA 14171 specifikáció [10] szerint ellenőrzi az elektronikus aláírásokat.
- A Szolgáltatások nyújtása során a Szolgáltató a Nemzeti Média- és Hírközlési Hatóság elektronikus aláírással kapcsolatos szolgáltatások nyújtása során alkalmazható biztonságos kriptográfiai algoritmusokról szóló [11] határozata szerinti algoritmusokat használ.
- A Szolgáltatásokat nyújtó rendszer megfelel az RFC 4810 szerinti követelményrendszernek [12].

- A jelen archiválási rend keretében nyújtott elektronikus archiválás szolgáltatás megfelel a Nemzeti Hírközlési Hatóság által kibocsátott követelményekre vonatkozó ajánlásoknak. [13], [14], [15]

1.3. Dokumentum neve és azonosítása

A dokumentum egyértelmű azonosítására szolgáló adatok megtalálhatóak a dokumentum címlapján, a dokumentum hivatalos és aktuális verziója elérhető a Szolgáltató honlapján, de megtekinthető a Szolgáltató ügyfélszolgálati irodájában is.

1.4. Közösség

Jelen fejezet az archiválási rend hatálya alá tartozó közösséget határozza meg.

- *Szolgáltató*: Az elektronikus archiválás szolgáltatást nyújtó fél (lásd: 1.1.2. fejezet).
- *Előfizető*: Az elektronikus archiválás szolgáltatást igénybe vevő fél, aki a Szolgáltatásokkal kapcsolatos költségek ellenértékét megfizeti. Az Előfizető szolgáltatási szerződést köt a Szolgáltatóval. Az elektronikus archiválás szolgáltatás során feltöltött dokumentumok az Előfizető tulajdonát képezik, illetve az Előfizető rendelkezik felettük.
- *Érintett fél*: Az elektronikus archiválás szolgáltatás során kibocsátott igazolásokat befogadó, illetve felhasználó fél.

1.5. Alkalmazhatóság

A jelen archiválási rend szerint nyújtott elektronikus archiválás szolgáltatás kizárólag a jelen dokumentumban, valamint a Szolgáltatási Szabályzatban leírtak szerint használható fel.

1.6. Kapcsolattartás

A Szolgáltatóval az ügyfelek a Szolgáltató ügyfélszolgálati irodáján keresztül tartják a kapcsolatot. (Lásd: 1.1.2. fejezet.)

1.7. Fogalmak meghatározása

Az alábbiakban definiált fogalmakat az itt leírt jelentéssel használjuk jelen dokumentumban:

Aláírás, Elektronikus aláírás: Az ETSI TS 101 903 szabványnak megfelelő formátumú elektronikus aláírás. Ezen aláírások *e-aktákban* lévő *fájlokon* helyezkednek el.

Dokumentum: Lásd: *e-akta*.

E-Akta: Az elektronikus archiválás szolgáltatás keretében a Szolgáltató rendszere elektronikus aláírásokat tartalmazó *dokumentumokat*, ún. *e-aktákat* fogad be. Az e-akták egy vagy több *fájlt*, és rajtuk egy vagy több – az ETSI TS 101 903 szabványnak megfelelő formátumú – *elektronikus aláírást* tartalmazhatnak. Az e-akta tartalmazhatja a benne lévő aláírásokhoz tartozó érvényességi láncok egy részét, illetve a teljes érvényességi láncokat is. Megkülönböztetünk *nyílt e-aktát* és *titkosított e-aktát*. Az e-akta formátum specifikációja a `http://www.e-szigno.hu/?lap=eakta` oldalon érhető el. [16]

Előfizető: Az elektronikus archiválás szolgáltatást igénybe vevő fél (lásd: 1.4).

Érvényességi lánc: Olyan, az elektronikus aláírásról szóló törvény szerinti érvényességi lánc, amely az aláírt *fájlt* is tartalmazza.

Fájl: Olyan bitsorozat, amelyen *elektronikus aláírás* helyezkedhet el. A fájlok az archiválás szolgáltatás során *e-aktákban* jelennek meg. Az archiválás szolgáltató nem foglalkozik a fájlok tartalmával. A Szolgáltató a Szolgáltatási Szabályzatban meghatározott formátumú fájlok esetén vállalja, hogy a szolgáltatás időtartama alatt megőriz olyan szoftver és hardver eszközöket, amelyekkel a fájl megjeleníthető. Ezt leszámítva az archiválás szolgáltató nem foglalkozik a fájl tartalmával.

Nyílt e-akta: Olyan e-akta, amely közvetlenül fájlokat, és rajta lévő aláírásokat tartalmaz. A nyílt e-akta az aláírt fájlokat és az aláírásokat egyaránt nyíltan tartalmazza. (Maga az aláírt fájl természetesen tartalmazhat titkosított elemeket, sőt, akár maga is lehet titkosított fájl. Az archiválás szolgáltató az e-aktákban lévő fájlok tartalmával nem foglalkozik, az e-aktában lévő fájlokat titkosítatlan információnak tekinti, így szükség esetén titkosítja őket.)

Titkosított e-akta: Ez az e-akta egy olyan XML fájl, amely egy másik e-aktát tartalmaz – az S/MIME specifikáció szerint titkosítva.

2. Közzététel

2.1. A szolgáltatói információ közzététele

A Szolgáltató szerződéses feltételeit és szabályzatait elektronikus formában (PDF formátumban) hozza nyilvánosságra a honlapján. A honlapon az érvényben levő dokumentumokon kívül a korábban hatályos verziók is elérhetőek.

2.2. A közzététel gyakorisága

A Szolgáltató szükség szerint kibocsátja az egyéb szabályzatait és szerződéses feltételeit, illetve az újabb változatokat.

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

2.3. Hozzáférés-ellenőrzések

A Szolgáltató által közzétett kikötések, feltételek és rendkívüli információk nyilvános információk. Olvasás céljából bárki elérheti ezeket az információkat, a közzététel sajátosságainak megfelelően.

A Szolgáltató által közölt információkat kizárólag csak a Szolgáltató egészítheti ki, törölheti vagy módosíthatja. A Szolgáltató különböző védelmi mechanizmusokkal igyekszik megakadályozni az információk jogosulatlan módosítását.

3. Az elektronikus archiválás szolgáltatás nyújtása

3.1. Szolgáltatási szerződés kötése

A Szolgáltatási Szabályzat meghatározza, hogy az Előfizető milyen módon fizethet elő az elektronikus archiválás szolgáltatásra, valamint azt, hogy milyen eszközök szükségesek az elektronikus archiválás szolgáltatás igénybe vételéhez.

3.2. Dokumentum feltöltése

1. Az Előfizető kizárólag biztonságos csatornán keresztül juttathat el aláírt e-aktákat a Szolgáltató archívumába.

2. A Szolgáltatási Szabályzat meghatározza, hogy a Szolgáltató az e-aktákban milyen aláírásokat milyen módon ellenőriz, és milyen feltételekkel fogad el.

3. A Szolgáltató felépíti az e-aktákban szereplő elektronikus aláírásokhoz tartozó érvényességi láncokat, és minősített időbélyeget helyez el rajtuk.

4. A Szolgáltató titkosítja az e-aktát, és archívumában is ezen titkosított e-aktát tárolja el. Az e-akta visszafejtésére kizárólag az elektronikus archiválás szolgáltatás nyújtásához szükséges esetekben, például letöltés (3.3. fejezet), felülhitelesítés (5.1. fejezet), illetve újra-titkosítás (5.2) esetén kerül sor.

5. A Szolgáltató haladéktalanul, de legkésőbb 3 napon belül visszaigazolást küld az Előfizetőnek arról, hogy az érvényességi láncot sikeresen felépítette, és az e-aktát sikeresen befogadta. Ha a folyamat valahol megszakadt, a Szolgáltató erről is értesíti az Előfizetőt. Ekkor az Előfizető olyan hibaüzenetet kap, amely arról tájékoztatja, hogy

a Szolgáltató nem tudta az e-aktát befogadni (például, mert nem tudta felépíteni az érvényességi láncot).

Ha az Előfizető nem kap pozitív visszaigazolást, azt úgy kell tekintenie, hogy a Szolgáltató nem fogadta be az e-aktát. A Szolgáltató kizárólag a pozitív visszajelzés elküldése esetén felel az e-akta megőrzéséért, és a benne szereplő aláírások hitelességének hosszú távú biztosításáért.

3.3. Érvényességi lánc elérhetőségének biztosítása

1. Az Előfizető kizárólag biztonságos csatornán keresztül férhet hozzá a Szolgáltató archívumában tárolt fájlokhoz, dokumentumokhoz, érvényességi láncokhoz.

2. A Szolgáltató biztosítja, hogy az Előfizető kizárólag azon fájlokhoz, dokumentumokhoz, érvényességi láncokhoz férhet hozzá, amelyekhez jogosult hozzáférni.

3.4. Igazolás kibocsátása

A feltöltött fájlokkal, e-aktákkal (dokumentumokkal) kapcsolatban a Szolgáltató az Előfizető kérésére igazolást állít ki. Az igazolás a következőket tartalmazza a Szolgáltató archívumában szereplő fájllal vagy e-aktával kapcsolatban:

1. Azt az állítást, hogy az adott fájlon elhelyezett (illetve az e-aktában elhelyezkedő) fokozott biztonságú vagy minősített elektronikus aláírások, a rajtuk elhelyezkedő időbélyegzők, és az ezekhez kapcsolódó tanúsítványok az időbélyegzés és a feltöltés pillanatában érvényesek voltak.

2. Azt az állítást, hogy az adott fájl vagy e-akta adott lenyomattal[2] rendelkezik, így megegyezik az Előfizető által bemutatott azonos lenyomatú fájllal vagy e-aktával. Amennyiben a Szolgáltató fájllal kapcsolatban állítja ki az igazolást, akkor az igazolás a fájlt magában foglaló e-akta lenyomatát is tartalmazza.

3. Azt az állítást, hogy az adott fájlon (vagy az adott e-aktában elhelyezkedő egyes fájlokon) meghatározott személy érvényes elektronikus aláírást helyezett el.

4. Azt az állítást, hogy az adott fájlon (vagy az adott e-aktában elhelyezkedő egyes fájlokon) adott időpontban érvényes időbélyegzőt helyeztek el.

5. Azt, hogy az előző pontban szereplő elektronikus aláírást mely időpontban (pontosabban, mely időpont előtt) helyezték el.

[2] A lenyomat kiszámítására szolgáló algoritmus az igazolás kibocsátásának pillanatában biztonságos kell, hogy legyen.

6. Azt a legkésőbbi időpontot, ameddig az igazolás érvényes.

7. A kibocsátott igazoláshoz kapcsolódó pénzügyi felelősségvállalás mértékét.

A Szolgáltató papíron, vagy minősített elektronikus aláírással ellátott e-aktában bocsátja ki az igazolást. Az igazolást egy archív igazolás kiállításáért felelős tisztviselő készíti el, majd minősített aláírással és időbélyeggel látja el vagy (papíron kiállított igazolás esetén) kézzel írott aláírásával hitelesíti. Az igazolásban az Előfizetőhöz kapcsolódó díjcsomagra vonatkozó feltételek szerint feltüntetésre kerül az igazoláshoz kapcsolódó szolgáltatói felelősségvállalás mértéke (lásd: 7.2.4).

Az igazolás kibocsátásához nincsen szükség az archivált e-akta ismeretére, az a nyílt e-akta tárolt lenyomata szerint jön létre. A Szolgáltató így biztosítja, hogy az archív igazolás kiállításáért felelős tisztviselők sem ismerhetik meg a nyílt e-akta tartalmát.

Az igazolás kibocsátása történhet olyan módon is, hogy az Előfizető bemutatja a Szolgáltatónak a nyílt archivált e-aktát (vagy valamely benne szereplő fájlt). Ekkor, feltéve, hogy a bemutatott nyílt e-aktával (vagy fájllal) azonos lenyomatú e-akta vagy fájl szerepel a Szolgáltató archívumában, a Szolgáltató munkatársa az Előfizető által bemutatott e-aktára vagy fájlra vonatkozóan állítja ki az igazolást.

Az Előfizető postán vagy elektronikus levélben igényelheti az igazolást. A Szolgáltató az Előfizető meghatalmazottja számára akkor bocsát ki igazolást, ha a meghatalmazást az Előfizető teljes bizonyító erejű magánokiratba foglalta.

3.5. Dokumentum megjelenítése

A Szolgáltatóval előre egyeztetett időpontban az Előfizető a Szolgáltató szoftver és hardver eszközei segítségével is megtekintheti a Szolgáltató archívumában lévő dokumentumokat. Erre a Szolgáltató ügyfélszolgálati irodájában van lehetőség.

3.6. Dokumentum és érvényességi lánc törlése

A Szolgáltató az Előfizető kérésére törli az archivált e-aktát (dokumentumot) és az e-aktában szereplő összes aláíráshoz tartozó érvényességi láncot az archívumából. Ezen törlés a tárolt e-akta fizikai megsemmisítését, illetve olyan módon történő felülírását jelenti, hogy azt később az adathordozóról egyáltalán ne (vagy csak irreálisan nagy anyagi ráfordítás esetén) lehessen visszaállítani. A törlést a Szolgáltató a teljes rendszerén végrehajtja, és a törlés keretében az e-akta minden mentett példányát is megsemmisíti.

A Szolgáltatási Szabályzat meghatározza a törlési kérelem benyújtásának és feldolgozásának módját és feltételeit.

3.7. A szolgáltatási szerződés megszűnése

A szolgáltatási szerződés megszűnése esetén a Szolgáltató a Szolgáltatási Szabályzat szerint törli az Előfizetőhöz tartozó archivált dokumentumokat.

A Szolgáltató a szerződés megszűnésekor történő törlés esetén is a 3.6. fejezetben leírt módon biztosítja, hogy a törölt e-aktákat ne lehessen visszaállítani.

4. Fizikai, eljárásbeli és személyzeti biztonsági óvintézkedések

A Szolgáltató elismert szabványoknak megfelelő fizikai, eljárásbeli és személyzeti biztonsági óvintézkedéseket, valamint az ezeket érvényre juttató adminisztratív és irányítási eljárásokat alkalmaz.

Az archivált e-aktákat a Szolgáltató két, egymástól fizikailag elkülönített helyen, az elsődleges rendszeren és a háttérrendszeren tárolja. A háttérrendszer úgy lett kialakítva, hogy az elsődleges rendszer kiesése esetén képes legyen átvenni az elsődleges rendszer kritikus funkcióit.

4.1. Fizikai óvintézkedések

A Szolgáltató gondoskodik arról, hogy a kritikus szolgáltatásokhoz történő fizikai hozzáférés ellenőrzött legyen, és a kritikus szolgáltatások eszközeinek fizikai kockázatát minimalizálja.

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

A kritikus és érzékeny információt feldolgozó szolgáltatásokat biztonságos helyszíneken valósítják meg a Szolgáltató rendszerében. A biztosított védelem arányban áll a Szolgáltató által végzett kockázat elemzésben megállapított kockázatokkal.

- A Szolgáltató védett számítógép termében valósítják meg a leginkább veszélyeztetett szolgáltatásokat. Ez a számítógép terem speciálisan ilyen természetű szolgáltatások befogadására lett tervezve és kialakítva, s tervezésénél sok, 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.) egységes érvényesítésére került sor.
- A Szolgáltató ügyfélszolgálati irodája úgy lett kialakítva, hogy a fenti szempontoknak szintén megfeleljen, alacsonyabb kialakítási és fenntartási költségek mellett.

- A Szolgáltató valamennyi kritikus szolgáltatását egy külön biztonsági zónában valósítja meg, és az ehhez szükséges valamennyi eszközt egy a biztonsági zóna részét képező védett számítógép teremben helyezte el.

4.1.1. A telephely elhelyezése és szerkezeti felépítése

Az elektronikus archiválás szolgáltatást nyújtó egységek különleges biztonsági szempontok figyelembe vételével kialakított biztonsági zónában, ablaktalan helyiségben helyezkednek el. A zónát vastag és elektromágneses sugárzást át nem engedő falak veszik körül. A Szolgáltató másodlagos telephelye az elsődleges telephelytől távol helyezkedik el egy védett szervertermemben.

A Szolgáltató úgy alakította ki mind az elsődleges rendszerét, mind a háttérrendszerét, hogy egy a rendszerhez fizikailag hozzáférő (esetleg az egész rendszert elrabló) támadó ne okozhasson jelentős kárt, tehát ne sérthesse meg a tárolt fájlok és e-akták hitelességét, bizalmasságát.

4.1.2. Fizikai hozzáférés

A Szolgáltató védett számítógép terme úgy lett kialakítva, hogy illetéktelen személyek nehezen juthassanak be. A biztonsági zóna integráltan megvalósított behatolás jelző (riasztó) és beléptető rendszerrel van ellátva, a zónát 24 órás videó kamerás megfigyelő rendszer is védi. A védett számítógép terembe az ott dolgozó bizalmi munkakört betöltő munkatársakon kívül más személyek (pl. karbantartók, takarítók) csak külön felhatalmazással és felügyelet mellett léphetnek be.

Az ügyfélszolgálati irodába önállóan csak az erre feljogosított személyek léphetnek be, egy beléptető rendszer felügyelete alatt.

4.1.3. Áramellátás, légkondicionálás

A Szolgáltató védekezik a nem megfelelő hőmérsékletből vagy áramellátásból eredő hibák és adatvesztések ellen.

Áramellátás

A Szolgáltató védett számítógép termének zavartalan áramellátása kiemelten fontos a folyamatos üzemeltetés biztosítása érdekében.

Ez a következő – egységes tervezéssel megalapozott, a vonatkozó szabványoknak megfelelő – védelmi megoldások együttműködésével biztosított:

- akkumulátoros szünetmentes energia ellátás,

- dízelmotoros generátoregység,
- villamos zavar-, villám- és túlfeszültség védelem.

A háttérrendszeren működő szerverterem folyamatos áramellátását

- akkumulátoros szünetmentes energia ellátás és
- villamos zavar-, villám- és túlfeszültség védelem,

biztosítják.

Légkondicionálás

A Szolgáltató védett számítógép terme hűtésigényének kiszolgálását két klímaberendezés együttes működése biztosítja. A klímaberendezések elhelyezésének módja biztosítja, hogy azok karbantartása ne okozzon zavart gépterem működésében.

4.1.4. Beázás és elárasztás veszélyeztetettsége

A Szolgáltató biztonsági zónájának kialakítása során fontos szempont volt a beázás és elárasztódás veszélyének minimalizálása. A biztonsági zóna teljes területe mentes a vizesblokkoktól, illetve a közelben nincs sem csatorna sem vízvezeték. A védett számítógép teremben a fenti biztonságot tovább növeli az álpadló alkalmazása.

4.1.5. Tűzmegelőzés és tűzvédelem

A Szolgáltató védett számítógép termében tűzvédelmi rendszer működik, melyet az illetékes tűzoltó parancsnokság jóváhagyott.

4.1.6. Selejt kezelése és megsemmisítése

A Szolgáltató biztonsági zónájában a bizalmas minősítésű adatokat tartalmazó elektronikus adathordozókat még tartalmuk törlése után sem használják fel nem bizalmas minősítésű adatok tárolására. A feleslegessé vált, bizalmas minősítésű adatokat tartalmazó adathordozókat – a Szolgáltató selejtezési szabályzatának megfelelően – fizikailag megsemmisítik:

- a papíralapú dokumentumokat zúzógéppel felaprítják;
- a hajlékony lemezeket (házából való kibontás után) zúzógéppel felaprítják;
- a merev lemezeket összetörik;
- az optikai lemezeket összetörik.

4.1.7. Fizikailag elkülönítetten őrzött mentési példányok

A Szolgáltató biztonság-kritikus szolgáltatásaira vonatkozó adatok, valamint az archivált e-akták mentési példányait a háttérrendszer biztonsági zónájában tárolják.

4.2. Eljárásbeli óvintézkedések

A Szolgáltató gondoskodik arról, hogy rendszereit biztonságosan, szabályszerűen, a meghibásodás minimális kockázata mellett üzemeltessék.

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

A Szolgáltató belső irányítási rendszere biztosítja a Szolgáltató jogszabályoknak és belső szabályzatainak megfelelő és naprakész működést. Rendszerében minden rendszerelemhez és minden folyamathoz egyértelműen hozzárendelhető az adott rendszerelemért, vagy folyamatért felelős személy. A Szolgáltató rendszerében élesen elkülönülnek egymástól a fejlesztési és üzemeltetési folyamatok. A rendszer megfelelő működését a független rendszervizsgáló és a Szolgáltató belső ellenőrének ellenőrzési tevékenysége biztosítja.

4.2.1. Bizalmi szerepkörök

A Szolgáltatási Szabályzat megnevezi a szolgáltatás nyújtásában részt vevő bizalmi szerepköröket, és meghatározza az egyes szerepkörök alapvető felelősségét.

A bizalmi munkakörökben dolgozó személyek a Szolgáltatóval munkaviszonyban állnak, megbízhatóságukról
a Szolgáltató a biztonsági szabályzatában leírtak szerint bizonyosodott meg. A Szolgáltató biztonsági szabályzata meghatározza, hogy mely bizalmi szerepkörök olyanok, hogy egyazon dolgozó nem töltheti be őket. A bizalmi szerepkörök összeférhetetlenségével kapcsolatban a Szolgáltató teljesíti a 3/2005. IHM rendelet 7. § és 20. § (1) szerinti követelményeket, valamint törekszik a bizalmi szerepkörök teljes szétválasztására.

4.2.2. Az egyes feladatokhoz szükséges személyzeti létszámok

Általánosan teljesül a Szolgáltató egészére, hogy minden munkatárs csak a saját munkakörének megfelelő funkciókat aktivizálhatja. Több bizalmi munkakört betöltő személy együttes jelenléte szükséges a titkosított e-akták visszafejtésére szolgáló magánkulcs felülhitelesítés (5.1. fejezet), illetve újra-titkosítás (5.2) esetén történő használatához.

A Szolgáltató rendszerében minden bizalmi szerepkörhöz egyszerre legalább két munkatárs kell, hogy tartozzon.

4.2.3. Az egyes munkakörökben elvárt azonosítás és hitelesítés

Az informatikai rendszer minden felhasználója és az adminisztratív folyamatok minden szereplője személy szerint kerül azonosításra. Fizikai és logikai hozzáférés ellenőrzéshez a Szolgáltató intelligens kártyára épülő technológiát használ. Sikeres hitelesítés előtt egyetlen biztonság kritikus tevékenységet sem lehet végrehajtani. A Szolgáltató minden munkatársa pontosan annyi hozzáférési jogosultsággal rendelkezik, amennyi a feladatköre ellátásához elengedhetetlenül szükséges.

4.3. Személyzetre vonatkozó óvintézkedések

A Szolgáltató gondoskodik arról, hogy személyzeti politikája, illetve a munkatársak alkalmazására vonatkozó gyakorlatai fokozzák és támogassák a Szolgáltató működésének megbízhatóságát. A személyzetre vonatkozó óvintézkedések célja az emberi hibák, lopás, csalás és a lehetőségekkel való visszaélés kockázatának csökkentése.

Ennek érdekében a Szolgáltató a személyi biztonsággal már a felvételi szakaszban foglalkozik, beleértve a szerződések megkötését, illetve azok alkalmazás során történő ellenőrzését. Valamennyi bizalmi munkakör esetén a felvételire jelentkezőket biztonsági ellenőrzésnek vetik alá. Minden bizalmi munkakört betöltő alkalmazottnak és külső félnek, akik a Szolgáltató szolgáltatásaival kapcsolatba kerülnek, titoktartási nyilatkozatot kell aláírni.

A Szolgáltató egyúttal biztosítja a valamennyi munkakör betöltéséhez szükséges közös, általános, illetve az egyes munkakörök betöltéséhez szükséges speciális szakmai ismereteket megszerzését, illetve továbbfejlesztését. A Szolgáltató fontosnak tartja dolgozói folyamatos képzését. E képzés egy része az új szabványok, jogszabályok folyamatos tanulmányozása és nyomon követése, egy másik része formális képzés.

4.4. A biztonsági naplózás folyamatai

Szolgáltató rendszere széleskörű naplózási tevékenységet folytat a szolgáltatások nyújtásával kapcsolatos műveletek és az ezek során felhasznált adatok megőrzése érdekében. A naplóbejegyzések a bejegyzés pontos idejét, a tevékenység időpontját (ha az a bejegyzés idejétől eltér) és végrehajtóját is tartalmazzák. A pontos időt szolgáltató pontos idő egysége biztosítja, ami legfeljebb 1 másodperces eltérést engedélyez a valódi időhöz képest. Az esetleges ennél nagyobb eltérések szintén naplózásra kerülnek. A Szolgáltató egyéb rendszerei szintén naplóznak. E naplózások tulajdonságai az adott alkalmazások függvényei. A naplózások elemei elkülönülten keletkeznek a különböző modulokban. Operatív szinten az egyes rendszerek

üzemeltetési leírásai, valamint a Szolgáltató biztonsági szabályzata szabályozzák a napló adatok kezelését.

4.4.1. A tárolt események típusai

A Szolgáltató informatikai rendszerében naplózásra kerül:

- a szolgáltatások nyújtásával kapcsolatos valamennyi esemény,
- az esetleges hibaesemények.

4.4.2. A napló állomány feldolgozásának gyakorisága

A Szolgáltató naplóbejegyzéseinek átvizsgálása minden munkanapon megtörténik. A 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.

4.4.3. A naplóállomány 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 10 évig biztonságosan megőrzik.

4.4.4. A naplóállomány védelme

A rendszer naplóbejegyzéseit a Szolgáltató időbélyeggel látja el, így a naplóbejegyzések törlések és beszúrások észrevétlen végrehajtását kizáró módon kerülnek tárolásra.

A naplóállományt a véletlen és szándékos rongálások ellen biztonsági mentések védik. A személyes adatokat tartalmazó naplóbejegyzések esetében Szolgáltató gondoskodik az adatok bizalmas tárolásáról. A naplóállományokhoz való hozzáférésre csak azok jogosultak, akiknek erre munkakörük folytán szükségük van. A Szolgáltató a hozzáféréseket biztonságos módon ellenőrzi. A naplóllományokat a Szolgáltató biztonságos környezetben őrzi. Az állományokról a működés másodlagos helyszínén másolati példányokat is tart.

4.4.5. A naplóállomány mentési folyamatai

A naplóállományok minden munkanapon (az átvizsgálást megelőzően) mentésre kerülnek egyszer írható médiára, aláírt formában. A média elzárva és fizikailag is elkülönítetten megőrzésre kerül.

A mentés operatív folyamatait a Szolgáltató mentési szabályzatai írják le részletesen.

4.4.6. A napló gyűjtési rendszere

A naplóbejegyzéseket az alkalmazások automatikusan gyűjtik és tárolják a naplóállományokban. A mentett médiákat a Szolgáltató napi rendszerességgel begyűjti.

4.4.7. Az eseményeket kiváltó ügyfelek értesítése

A naplóbejegyzéseket kiváltó személyeket, szervezeteket és alkalmazásokat a Szolgáltató nem értesíti, szükség esetén azonban bevonhatja őket az esemény kivizsgálásába. Az esemény kiváltásában közreműködő Előfizetőnek ilyen esetben kötelessége a Szolgáltatóval való együttműködés.

Információbiztonsági esemény bekövetkeztekor a Szolgáltató értesíti az érintett adatot birtokló Előfizetőt, és teljeskörűen tájékoztatja az esemény bekövetkezéséről és hatásairól.

4.4.8. Sebezhetőség felmérése

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

4.5. Adatok archiválása

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

4.5.1. A tárolt események típusai

Szolgáltató ügyfélszolgálati irodája a Szolgáltató és az ügyfelek között megkötött valamennyi megállapodást tárol és megőriz.

4.5.2. Az archívum megőrzési időtartama

Szolgáltató valamennyi (papíralapú vagy elektronikus) iratot 10 évig, illetőleg velük kapcsolatban esetlegesen felmerült jogvita jogerős lezárásáig megőriz.

4.5.3. Az archívum védelme

Az iratok biztonságos megőrzéséről és tárolásáról a Szolgáltató olyan adattár segítségével gondoskodik, amelyhez a Szolgáltató meghatározott munkatársai rendelkeznek hozzáférési engedéllyel.

4.5.4. Az archívum mentési folyamatai

A Szolgáltató a papíron tárolt adatairól másodpéldányokat tárol, az eredeti példányétól különböző helyszínen, fizikailag elkülönítve.

4.5.5. Az archívum gyűjtési rendszere

Az ügyféllel való szerződéskötés során keletkezett papíralapú iratokat a Szolgáltató által működtetett adattárban tárolják és őrzik.

4.5.6. Archív információ hozzáférését és ellenőrzését végző eljárások

Az archívumhoz a Szolgáltató ügyfélszolgálatán keresztül biztosít hozzáférést. A hozzáférés az ügyfelek számára a rájuk vonatkozó adatokhoz lehetséges, más feleknek kizárólag a Bizalmasság című fejezetben (7.3. fejezet) leírtak szerint.

4.6. Helyreállítás rendkívüli üzemi helyzetek esetén

Szolgáltató katasztrófa elhárítási tervvel rendelkezik, mely részletesen szabályozza a különböző sérülések és katasztrófahelyzetek esetén követendő eljárásokat. A katasztrófa elhárítási terv a rendkívüli üzemi helyzetekre helyreállítási terveket tartalmaz. E terveket a Szolgáltató az adott esetekre rendszeresen teszteli. A következő fejezetekben e katasztrófa elhárítási terv irányelveit foglaljuk össze.

4.6.1. Sérült 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 a Szolgáltató háttérszerződései és saját tartalék eszközei garantálják.

A Szolgáltató úgy alakította ki az archivált e-akták tárolására szolgáló és az érvényességi láncot elérhetőségét biztosító informatikai rendszerét, hogy a rendszer bármely egy eszköz kiesése esetén képes zavartalanul folytatni a működését. Amennyiben a Szolgáltatónak egyszerre több eszköze esik ki, a Szolgáltató 3 napon belül képes háttér-rendszerének beindítására, amely képes biztosítani a fenti szolgáltatások folyamatos elérhetőségét.

4.6.2. Helyreállás természeti vagy más katasztrófát követően

A Szolgáltató elsődleges működési helyszínén kívül másodlagos helyszínnel is rendelkezik. Természeti vagy más katasztrófát követően, illetve a Szolgáltató berendezéseinek olyan mértékű meghibásodása esetén, mely az elsődleges rendszeren nem kezelhető, a Szolgáltató a másodlagos helyszínen is képes szolgáltatásainak beindítására.

Ilyen esetekben a Szolgáltató legfeljebb 3 napon belül vállalja az érvényességi láncok elérhetővé tételével kapcsolatos szolgáltatásának beindítását.

4.7. A szolgáltatások leállítása

A Szolgáltató az elektronikus archiválás szolgáltatás tervezett megszüntetése esetén legkevesebb 60 nappal a szolgáltatás leállítását megelőzően értesíti a végfelhasználókat és a Hatóságot. Ha a Szolgáltató ellen felszámolási vagy végelszámolási eljárás indult, haladéktalanul köteles tájékoztatni a Hatóságot e tényről, megnevezve az eljárást lefolytató szervezetet.

A Szolgáltató a szolgáltatás leállítására vonatkozó bejelentését követően nem fogad be további e-aktákat. A megszűnés időpontjával egyidejűleg a Szolgáltató a többi szolgáltatást is leállítja.

A Szolgáltató a tervezett megszűnés előtt tárgyalásokat kezd más vele azonos besorolású szolgáltatókkal a szolgáltatásainak átvételéről. Nyilvántartásait, a tárolt e-aktákkal, és a visszafejtésükre szolgáló magánkulccsal együtt mindenképpen átadja egy ilyen szolgáltatónak.

A Szolgáltató a tárgyalások végeredményéről tájékoztatja a végfelhasználókat és a Hatóságot. A Szolgáltató az Ügyfeleket elektronikus levélben, az Érintett feleket a honlapján történő közzététel útján tájékoztatja.

A Szolgáltató a szolgáltatás befejezésekor az informatikai rendszerében foglalt adatairól teljes körű, minősített időbélyegzővel ellátott mentést készít.

A Szolgáltató – annak érdekében, hogy adatait átadhassa egy másik szolgáltatónak – az adatokat az új szolgáltató által fogadóképes médián és formátumban helyezi el vagy biztosítja az új szolgáltató számára az adatok eredeti formátumban történő feldolgozásának lehetőségét, amelyekhez átadja a megfelelő eszközöket, dokumentációkat és ismereteket.

A szolgáltatás leállítását követően a Szolgáltató az Előfizetővel egyeztetett módon átadja az archivált fájlokat, aláírásokat és érvényességi láncokat az Előfizetőnek, majd visszaállíthatatlan módon törli őket az archívumából a 3.6. fejezetben leírt módon.

5. Műszaki biztonsági óvintézkedések

5.1. Rendszeres felülhitelesítés

A Szolgáltató az archivált e-aktákon (így a fájlokon, aláírásokon és az érvényességi láncokon) minősített időbélyeget és minősített elektronikus aláírást helyez el

- évente legalább egyszer;
- ha az elektronikus aláírásra, illetve időbélyegzésre használt valamely algoritmusban (többek között a lenyomatképző algoritmusban) megrendül a bizalom;
- ha a Nemzeti Hírközlési Hatóság ilyen határozatot hoz.

A minősített elektronikus aláírást és a minősített időbélyeget a Szolgáltató a Nemzeti Hírközlési Hatóság határozata [11] szerint biztonságos algoritmusokkal hozza létre.

5.2. Az archívum újra-titkosítása

A Szolgáltató az archivált e-aktákat titkosítva tárolja az archívumában. Biztosítja, hogy az archivált e-akták mindenkor biztonságos algoritmussal kerülnek titkosításra.

A Szolgáltató gondoskodik róla, hogy az e-akták újra-titkosításra kerüljenek, ha:

- A titkosításkor használt valamely algoritmusban megrendül a bizalom – ilyenkor a titkosítás időpontjában biztonságosnak ítélt algoritmussal kell újra titkosítani.
- A Szolgáltató dekódoló kulcsának bizalmassága sérül.
- A Szolgáltatási Szabályzat vagy az Előfizetővel kötött szerződés így rendelkezik.

Miután a Szolgáltató biztonságos módon titkosította az archivált e-aktákat, akkor megsemmisíti a korábbi, már elavult módon titkosított példányokat.

5.3. A technológia folyamatos figyelése

A Szolgáltató folyamatosan figyelemmel kíséri az elektronikus aláírással és kriptográfiával kapcsolatos technológia fejlődését, és ha valamely, a rendszerben használt algoritmus elavul, akkor a Szolgáltató elvégzi az újra-titkosításhoz (5.2. fejezet), illetve felülhitelesítéshez (5.1. fejezet) szükséges műveleteket.

Amennyiben a Szolgáltató felfedezi, hogy a Hatóság határozata szerinti, elfogadott, meghatározott paraméterekkel rendelkező kriptográfiai algoritmusok már nem biztonságosak, a Szolgáltató elvégzi a felülhitelesítést, és értesíti a Hatóságot.

5.4. Hitelesítés szolgáltatók elfogadása

A Szolgáltatási Szabályzat meghatározza, hogy a Szolgáltató mely hitelesítés szolgáltatók tanúsítványait milyen feltételekkel fogadja el, valamint azt, hogy hitelesítés szolgáltatók milyen feltételrendszer szerint kerülhetnek fel ezen listára, és le ezen listáról.

5.5. Az e-akták és a bennük lévő fájlok olvashatóságának és értelmezhetőségének fenntartása

A Szolgáltató biztosítja a Szolgáltatási Szabályzatban meghatározott formátumú fájlok, dokumentumok olvashatóságának fenntartását. Az ezzel kapcsolatos részleteket a Szolgáltatási Szabályzat tartalmazza.

5.6. Az elektronikus archiválás szolgáltatás egyes elemeinek rendelkezésre állása

Az elektronikus archiválás szolgáltatás következő elemeinek rendelkezésre állása éves szinten 99%, és az eseti szolgáltatás-kiesések nem haladhatják meg a 3 napot:

- az archivált e-akták és érvényességi láncok elektronikusan történő letöltése,
- keresés az archivált e-akták között,
- törlési kérelmek fogadása,
- időzített törlési kérelmek fogadása (amely segítségével az Előfizető meghatározhatja, hogy egy adott e-aktát mennyi ideig archivál a Szolgáltató), illetve korábbi időzített törlési kérelmek módosítása,
- információkérés a korábban elküldött kérések állapotára vonatkozóan.

A dokumentumok (e-akták) feltöltése szolgáltatást a Szolgáltató az elektronikus aláírásról szóló törvényben szereplő feltételek mellett jogosult szüneteltetni. [2]

Az igazolások kibocsátását a Szolgáltató a Szolgáltatási Szabályzatban leírt módon, folyamatosan biztosítja, az igazolások kibocsátása szolgáltatás kiesése nem haladhatja meg a három napot.

5.7. Biztonsági garanciák

A Szolgáltató módosítás ellen védett, megbízható rendszereket és termékeket használ. Megbízható, biztonságtechnikailag értékelt és minősített termékekből álló, egységes informatikai rendszert használ szolgáltatásai nyújtásához. A Szolgáltató olyan megbízható

rendszereket és termékeket használ, amelyek az illetéktelen módosítással szemben védettek. Mind a Szolgáltató, mind a rendszert szállító és kivitelező vállalkozók hitelesítés-szolgáltatás kiépítésében jelentős tapasztalatokkal rendelkeznek és nemzetközileg elismert technológiát alkalmaznak.

Amennyiben a Szolgáltató harmadik féltől bizalmi szolgáltatást vesz igénybe, ellenőriznie kell, hogy ezen harmadik fél eleget tesz-e minden szükséges kötelezettségének.

A Szolgáltató az archivált e-aktákat fizikailag biztonságos környezetben, a 4. fejezetben leírt fizikai és eljárásbeli óvintézkedések mellett tárolja, amelynek biztonságát a Szolgáltató belső biztonsági szabályzatai és a rendszeres belső és külső biztonsági felülvizsgálat garantálják.

A Szolgáltató biztosítja, hogy a tárolt dokumentumokat saját munkatársai sem olvashatják el. A Szolgáltató a dokumentumokat kizárólag akkor bocsátja harmadik fél (pl. hatóság) rendelkezésére, ha erre az Előfizető felhatalmazta, vagy ha ezt jogszabály írja elő.

A tárolt dokumentumok integritását a dokumentumok fizikai védelme, valamint az elektronikus aláírással kapcsolatos technológiák biztosítják. A dokumentumok rendelkezésre állását a Szolgáltató magas színvonalú informatikai rendszere, valamint a rendszer működését szabályzó belső szabályzatai, üzletmenet-folytonossági és vészhelyzet-kezelési eljárásai és egyéb rendkívüli üzemeltetési helyetek kezelésére szolgáló eljárásai biztosítják. A Szolgáltató ezen eljárások, valamint ezek folyamatos külső és belső ellenőrzése és tesztelése segítségével kerüli el az üzemeltetés és a karbantartás során felmerülő hibákat. A Szolgáltató két, egymástól távoli fizikai helyszínen tárolja az archivált dokumentumokat.

A Szolgáltató az archivált dokumentumokat – az Előfizető kérése vagy a szerződés megszűnése esetén – a 3.6. fejezetben leírt feltételek mellett semmisíti meg.

A Szolgáltató a visszaigazolások aláírására használt kulcsokat, az archivált e-akták titkosításához/dekódolásához használt kulcsokat, és az infrastrukturális és rendszervezérlési kulcsokat kriptográfiai hardver eszközben állítja elő. E kulcsokat a Szolgáltató szabályos időközönként cseréli. A Szolgáltató figyelemmel kíséri a technológia fejlődését, és amennyiben azt észleli, valamely kulcs már nem biztonságos, illetve ha a Hatóság határozata szerint az adott algoritmus már nem használható, akkor haladéktalanul lecseréli az érintett kulcsot vagy kulcsokat.

A Szolgáltató titkosítva tárolja a dokumentumokat. A Szolgáltató a dokumentumokat mindig olyan algoritmussal titkosítja, amely a technológia adott állása szerint biztonságosnak minősül. Amennyiben ezen algoritmus biztonsága a technológia fejlődése során megsérül, a Szolgáltató saját belső szabályzatai alapján gondoskodik a dokumentum biztonságos algoritmussal történő újra-titkosításáról.

5.8. Számítógépes biztonsági óvintézkedések

A Szolgáltató megbízható informatikai rendszereket és megoldásokat, technológiákat alkalmaz, és rendszerét redundánsan alakította ki. Minden, kritikus szolgáltatást biztosító rendszerelemből két példány üzemel, bármelyik elem kiesése esetén a másik elem átveszi a funkcióját.

A Szolgáltató a pontos időt három referencia időforrásból nyeri. Egyrészt GPS-re, másrészt hosszúhullámú pontos idő szolgáltatásra (DCF77) támaszkodik. A Szolgáltató két független Stratum-1 időforrással rendelkezik, és ezekhez 0,1 másodperc pontossággal szinkronizálja saját belső óráját. E szinkronizációt a Szolgáltató naponta több, mint négy alkalommal végzi el. A Szolgáltató belső órájának helyességét a Szolgáltató biztonsági bizottsága évente ellenőrzi.

A Szolgáltató informatikai rendszerét háromfokozatú tűzfalrendszerrel védi. Minden tűzfalból két példány működik, bármelyik kiesése esetén egy cluster segítségével a másik ugyanolyan egység átveszi a funkcióját.

5.9. Életciklusra vonatkozó műszaki óvintézkedések

Annak érdekében, hogy a Szolgáltató valamennyi rendszerfejlesztési projektjében a biztonsági követelmények magas színvonalon biztosítottak legyenek, a teljes fejlesztés során (már a tervezési és követelmény-meghatározási fázisban is) figyelembe kell venni a fokozott követelményeket.

A szolgáltatások nyújtásához használt termékek, életciklusukra vonatkozó biztonsági szempontok figyelembevételével kerültek alkalmazásra.

6. A megfelelőség vizsgálata

A Szolgáltató vizsgált és tanúsított elemeket (elektronikus aláírási termékeket, informatikai rendszerelemeket stb.) alkalmaz a szolgáltatásaihoz kapcsolódóan. A Szolgáltató a szolgáltatások nyújtásához használt valamennyi rendszerelemet biztonsági osztályokba sorolta kockázat-menedzsment rendszere alapján. Ezen rendszerelemekről és a hozzájuk tartozó biztonsági besorolásról a Szolgáltató a kockázatmenedzsment rendszere keretében nyilvántartást vezet.

A tanúsításhoz a Szolgáltató külső auditort vesz igénybe (lásd: 6.2. fejezet). A Szolgáltató e külső auditon túl saját belső ellenőrzési rendszerrel is rendelkezik, amely rendszeresen vizsgálja a korábbi tanúsításoknak való megfelelőséget, és eltérés esetén megteszi a szükséges lépéseket.

A Szolgáltató 2002 óta rendelkezik az ISO 9001 szabványnak megfelelő minőségirányítási, valamint 2003 óta a MSZ/ISO/IEC 27001-nek (korábban BS 7799-nek) megfelelő információbiztonság-irányítási rendszerrel, amelyeket külső auditáló szervezet auditál és vizsgál felül folyamatosan (lásd: 1.1.2. fejezet).

Az elektronikus aláírásról szóló törvény szerint hatósági felügyeleti ellenőrzési eljárás keretében további külső auditra kerül sor, amely a jogszabályoknak megfelelően legalább évente átfogó helyszíni ellenőrzéssel jár együtt.

6.1. Az ellenőrzések gyakorisága

A Szolgáltató évente külső megfelelőségi audit végrehajtásával bíz meg egy megfelelő szakembert a Szolgáltatások nyújtását végző informatikai rendszerével kapcsolatban.

6.2. Az auditor és szükséges képesítése

A rendszeres felülvizsgálatot a nyilvános kulcsú infrastruktúra területén többéves tapasztalattal rendelkező, a Nemzeti Hírközlési Hatóság által nyilvántartásba vett elektronikus aláírás szakértő végzi.

6.3. Az auditor függetlensége

A Szolgáltatóval kapcsolatban tanúsítást végző auditor a Szolgáltatótól függetlenül, és befolyástól mentesen végzik tevékenységüket. Az auditor díjazása nem függ a tanúsítás során tett megállapításaitól.

6.4. Az audit által érintett területek

Az audit az alábbi területeket fedi le:

- dokumentálás,
- folyamatok,
- fizikai biztonság,
- személyi állomány,
- műszaki biztonság,
- adatvédelem.

Az audit során megvizsgálásra kerül, hogy a Szolgáltató megfelel-e a hatályos jogszabályoknak – különösen az elektronikus aláírásról szóló [2] törvénynek és a [3] rendeletnek.

Az audit ezen kívül a Szolgáltató által támogatott jelen archiválási rendnek való megfelelőség vizsgálatára irányul.

6.5. Hiányosságok esetén végrehajtandó tevékenységek

A felügyeleti ellenőrzési eljárás vagy a rendszeres helyszíni ellenőrzések során feltárt esetleges hiányosságokat a Szolgáltató a Hatósággal megállapodott határidőn belül megszünteti a vizsgálatot végző Hatóságtól kapott információk és ajánlások alapján.

A Szolgáltató a külső vagy belső auditorai, illetve a saját belső ellenőrzése által feltárt hiányosságokat a lehető legrövidebb időn belül, a saját belső szabályzataiban dokumentált változás-kezelési eljárás szerint szünteti meg.

7. Üzleti és jogi tudnivalók

7.1. Díjak és árak

Az általános szerződési feltételek [17], illetve a szolgáltatási szerződés tartalmazzák.

7.2. Jogok, kötelezettségek és felelősség

7.2.1. A Szolgáltató kötelezettségei

A Szolgáltató alapvető kötelezettsége, hogy a Szolgáltatásokat a jelen archiválási rend, valamint a Szolgáltatási Szabályzat és általános szerződési feltételei [17] szerint nyújtsa.

7.2.2. Az Előfizető jogai

Az Előfizető jogosult az elektronikus archiválás Szolgáltatás igénybe vételére a Szolgáltatási Szabályzatban leírtak szerint.

7.2.3. Az Előfizető kötelezettségei

Az Előfizető kötelessége a Szolgáltatási Szabályzatnak, a Szolgáltató szerződéses feltételeinek és szabályzatainak megfelelően eljárni a Szolgáltatások felhasználása során.

7.2.4. A Szolgáltató felelőssége

A Szolgáltató felelősségét jelen archiválási rend, a Szolgáltatási Szabályzat, valamint az Előfizetővel kötött szerződés és annak mellékletei tartalmazzák.

- A Szolgáltató felelősséget vállal a jelen archiválási rendekben leírt eljárásoknak való megfelelésért, még abban az esetben is, amikor a Szolgáltató egyes tevékenységeit alvállalkozók végzik.

- A Szolgáltató a vele szerződéses jogviszonyban álló ügyfelekkel szemben a Magyar Köztársaság Polgári Törvénykönyvének a szerződésszegésért való felelősség szabályai szerint felelős.
- 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 a felelősségi körén belül keletkezett, bizonyított károkért a szabályzataiban és az Előfizetővel megkötött szolgáltatási szerződésekben rögzített korlátozásokkal kártérítést fizet.

Felelősség korlátozása

- A Szolgáltató nem felelős az olyan károkért, amelyek abból adódnak, hogy az Érintett fél az archiválás szolgáltatás során kibocsátott igazolások ellenőrzése és felhasználása során nem a hatályos jogszabályok és a Szolgáltató szabályzatai szerint járt el, illetve nem úgy járt el, ahogyan az az adott helyzetben elvárható.
- A Szolgáltató a szolgáltatásaival kapcsolatos szerződéses és szerződésen kívüli károkért harmadik személlyel szemben kizárólag kötelezettségei felróható megszegéséből bekövetkező, bizonyítható károkért tartozik helyt állni.
- A Szolgáltató nem felelős az abból adódó károkért, amikor az Internet, vagy annak egy részének működési hibájából adódóan a tájékoztatás és egyéb kommunikációs kötelezettségeit nem tudja ellátni.
- A Szolgáltató kizárólag azért vállal felelősséget, hogy a Szolgáltatásokat a jelen archiválási rendben, a Szolgáltatási Szabályzatban, illetve az abban meghivatkozott dokumentumokban leírtaknak, valamint saját belső szabályzatainak megfelelően nyújtja.
- A Szolgáltató az érvényességi lánc és az általa őrzött elektronikus dokumentumok, e-akták sérülése vagy megsemmisülése által más személynek okozott kár tekintetében a Szolgáltatási Szabályzat szerint korlátozza a felelősségét.

7.2.5. Az Érintett fél felelőssége

Amennyiben egy Érintett fél ésszerűen kíván az archiválás szolgáltatás során kibocsátott igazolásra (lásd 3.4. fejezet) hagyatkozni, akkor a jelen archiválási rendnek, és a Szolgáltatási Szabályzatnak megfelelően célszerű eljárnia.

Amennyiben az Érintett fél nem a Szolgáltatási Szabályzat szerint jár el az igazolás felhasználása során, a Szolgáltató nem vállal felelősséget a felmerülő károkért.

7.2.6. Pénzügyi felelősség

A Szolgáltató a megbízhatóság biztosítása érdekében a jogszabályi előírásoknak megfelelő felelősségbiztosítással is rendelkezik.

A Szolgáltató iránti kártérítés

Az Előfizető kártérítési felelősséggel tartozik a Szolgáltató iránt azokért a veszteségekért és károkért, amelyeket kötelezettségei és a rá vonatkozó ajánlások be nem tartásával okoz a Szolgáltató számára.

Adminisztratív folyamatok

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.

7.3. Bizalmasság

A Szolgáltató munkatársai nem ismerik meg sem az archiválásra került fájlokat, sem azok részeit.

A Szolgáltató a dokumentumokat kizárólag akkor bocsátja harmadik fél rendelkezésére, ha erre az Előfizető felhatalmazta, vagy ha ezt jogszabály írja elő.

A Szolgáltató az elektronikus archiválás szolgáltatás nyújtása során nem vesz igénybe más adatfeldolgozót. A Szolgáltató a feltöltött fájlokon és e-aktákon az elektronikus archiválás szolgáltatás ellátásán túl saját célra nem végez adatfeldolgozást.

Az Előfizető kizárólag olyan fájlokat, e-aktákat tölthet fel a Szolgáltató archívumába, amelyeket a hatályos adatvédelmi jogszabályok szerint adatfeldolgozónak átadhat. Ennek biztosításáról Előfizetőnek kötelessége gondoskodni.

7.4. Adatkezelési szabályzat

A Szolgáltatási Szabályzat tartalmazza.

7.5. Szellemi tulajdonjogok

Az Előfizető által feltöltött fájlok az Előfizető tulajdonát képezik, illetve az Előfizető rendelkezik felettük.

7.6. Értelmezés és érvényesítés

7.6.1. 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.

- 2001. évi XXXV. törvény az elektronikus aláírásról (a 2004. évi módosításokkal).
- 4/2006. (IV. 19.) IHM rendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással összefüggő nyilvántartással kapcsolatos tevékenységéért fizetendő díjakról.
- 3/2005. (III. 18.) IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről.
- 4/2006. (IV. 19.) IHM rendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással összefüggő nyilvántartással kapcsolatos tevékenységéért fizetendő díjakról.
- 114/2007. (XII. 29.) GKM rendelet a digitális archiválás szabályairól
- 7/2002. (IV. 26.) MeHVM rendelet az elektronikus aláírással kapcsolatos szolgáltatási szakértő nyilvántartásba vételéről.
- 45/2005 (III. 11) Kormányrendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással kapcsolatos feladat- és hatásköréről, valamint eljárásának részletes szabályairól.
- 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról.
- 1959. évi IV. törvény a Polgári Törvénykönyvről.

7.6.2. Érvénytelenség, megszűnés és értesítések

Érvénytelenség

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

Megszűnés

Jelen archiválási rend a Közösség című fejezetben (1.4. fejezet) leírt közösség valamennyi kötelezettségét, felelősségét és jogát tartalmazza vagy meghivatkozza. A Szolgáltatási

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. Jelen archiválási rend csak írott és hitelesített formában módosítható, a Hatóság által vezetett szabályzat-nyilvántartásban való átvezetés jelen archiválási rendben leírt módon történő kezdeményezése mellett.

Értesítések

Az Előfizető jognyilatkozatait a Szolgáltató felé kizárólag írásban, aláírt módon teheti meg. Szervezet képviseletében való aláírás csak a képviseleti jogosultság igazolásával együtt érvényes.

A Szolgáltató a honlapján történő közzététel útján vagy elektronikus levélben tájékoztatja ügyfeleit.

7.6.3. Vitás kérdések megoldására vonatkozó eljárások

A Szolgáltató és az Ügyfél kölcsönösen megállapodnak abban, hogy bármilyen vitás kérdés vagy panasz felmerülése esetén, a vita jogi útra való terelése előtt megkísérlik a békés úton, tárgyalással történő egyeztetést. A kezdeményező fél kötelessége, hogy minden érintett többi felet haladéktalan értesítsen és teljes körűen tájékoztasson az ügy minden vonatkozását illetően. A Szolgáltató tevékenységével vagy a kiadott tanúsítványok felhasználásával kapcsolatos kérdéseket, kifogásokat és panaszokat az Ügyfélszolgálati iroda címére kell eljuttatni írásos formában. A bejelentés kézhezvételétől számított 3 munkanapon belül a Szolgáltató értesíti a bejelentő felet az általa megadott címen a bejelentés fogadásáról és a kivizsgáláshoz szükséges időről. A megjelölt határidőig a Szolgáltató köteles írásban válaszolni a bejelentőnek. A Szolgáltató a válaszadáshoz szükséges információk megadását kérheti a bejelentőtől. A Szolgáltató a panaszt 30 napon belül kivizsgálja, és az eredményekről értesíti a bejelentőt. Amennyiben a választ a bejelentő nem tartja kielégítőnek, vagy az alapján nem sikerül a Szolgáltató bevonása nélkül rendezni a felmerült vitát, akkor a bejelentő egyeztetést kezdeményezhet a Szolgáltatóval és az érintett felekkel. Az egyeztetés minden résztvevőjét írásban értesíteni kell az egyeztetés időpontjáról azt megelőzően 10 munkanappal, és írásban meg kell számukra küldeni a bejelentést, a Szolgáltató válaszát és egyéb szükséges információkat tartalmazó dokumentumokat. Amennyiben az egyeztetés a panasz benyújtásától számított 30 napon belül nem vezet eredményre, akkor a bejelentő peres útra terelheti az ügyet. Az érintett felek kölcsönösen alávetik magukat a Budapesti II. és III. Kerületi Bíróság, illetve a Fővárosi Bíróság kizárólagos illetékességének.

7.7. Leírás-adminisztráció

A Szolgáltató működését nyilvános és belső dokumentumai, szabályzatai határozzák meg. A nyilvános dokumentumok mind a Szolgáltató honlapján, mind az ügyfélszolgálati irodájában elérhetőek.

7.7.1. Szabályzat-változtatási eljárások

Szolgáltató szervezetén belül olyan csoport működik, amely a szabályzatok és dokumentációk karbantartásáért felelős. A változtatási igényeket e csoport gyűjti, a módosításokat elvégzi, a belső és külső tájékoztatási kötelezettségeknek eleget tesz. A szabályzatokat és dokumentumokat az e-Szignó Hitelesítés Szolgáltató igazgatója hagyja jóvá.

A változtatásokat gyűjtve a csoport belső, nem nyilvános munkaváltozatokat hoz létre a dokumentumokból és szabályzatokból, melyek a közzététel előtt belső felülvizsgálaton esnek át. A Szolgáltató törekedik arra, hogy új szabályzatot csak a lehető legritkábban kelljen kibocsátania.

A nyilvános dokumentumok és szabályzatok módosított változatai mindig új verziószámmal és OID-del kerülnek nyilvánosságra.

7.7.2. Értesítés nélkül változtatható elemek

A Szolgáltató a jelen dokumentumban bekövetkező minden változást – a jogszabályi előírásoknak megfelelően – a változás életbe lépése előtt 30 nappal bejelent a Hatóságnak, és a megváltozott dokumentumok közzéteszi a weboldalán.

7.7.3. Értesítéssel változtatható elemek

Minden, a szolgáltatás biztonsági szintjét, felhasználhatóságát módosító változtatás értesítésköteles a 7.8 fejezet szerint.

7.7.4. Észrevételek kezelése

Az dokumentumok új verziójával kapcsolatos észrevételeket a Szolgáltató a hatályba lépést megelőző 14 napig fogadja az `info@e-szigno.hu` címen. A dokumentum észrevételekkel módosított változatát a Szolgáltató a hatályba lépést megelőző 7. nap zárja le és teszi közzé.

7.8. Közzétételi és tájékoztatási elvek

A jelen dokumentumban nem tárgyalt elemek

A Szolgáltató nyilvános dokumentumaiban csak azon eljárásait hozza nyilvánosságra, melyek ismerete a szolgáltatások biztonságát nem veszélyezteti. A Szolgáltató több belső biztonsági és egyéb szabályzattal, operatív szintű előírással rendelkezik, melyeket bizalmasan kezel (jelen dokumentum több ilyet is megemlít). A 6.4. fejezetben leírt tanúsítási eljárások ezeket a dokumentumokat is vizsgálják.

A nyilvános dokumentumok közzététele

A Szolgáltató nyilvános dokumentumainak (köztük jelen dokumentumnak) a változásokkal egybeszerkesztett új verzióját, annak hatályba lépését megelőzően 30 nappal közzéteszi web oldalain. A Szolgáltató alkalmanként ezt megelőzően is tájékoztatja a közösséget a tervezett változtatásairól.

Dokumentum jóváhagyási eljárások

Jelen dokumentum jogszabályoknak, szabványoknak, valamint egyéb mértékadó követelményeknek való megfelelőségét közzététel előtt a Szolgáltató megvizsgálta.

A jogszabályoknak való megfelelőséget a Hatóság is vizsgálja a dokumentumok hatályba lépését megelőzően. A nyilvános dokumentumok és szabályzatok változásokkal egybeszerkesztett új verzióját, azok hatályba lépését megelőzően 30 nappal a Szolgáltató átadja a Hatóság részére, akivel a Szolgáltató alkalmanként ezt megelőzően is konzultál a tervezett változtatásairól.

Hivatkozások

[1] e-Szignó Hitelesítés Szolgáltató – minősített elektronikus archiválás szolgáltatásra vonatkozó – szolgáltatási szabályzat.

[2] 2001. évi XXXV. törvény az elektronikus aláírásról (a 2004. évi módosításokkal).

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

[4] RFC 3280 (Internet X.509 Nyilvános kulcsú infrastruktúra - tanúsítvány és tanúsítvány visszavonási lista profil).

[5] Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható végfelhasználói tanúsítványok szerkezetének és adattartalmának műszaki specifikációjára, 2006.

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

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

[8] ETSI TS 101 903 XML Advanced Electronic Signatures (XAdES).

[9] Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható elektronikus aláírás formátumok műszaki specifikációjára, 2006.

[10] CEN CWA 14171: Procedures for Electronic Signature Verification.

[11] A Nemzeti Média- és Hírközlési Hatóság EF/26838-10/2011 számú, 2011. szeptember 27-én kelt határozata az elektronikus aláírással kapcsolatos szolgáltatások nyújtása során alkalmazható biztonságos kriptográfiai algoritmusokról és paramétereikről.

[12] RFC 4810 Long-Term Archive Service Requirements.

[13] Elektronikus archiválási szolgáltatással kapcsolatos hatósági tájékoztató, Nemzeti Hírközlési Hatóság Hivatala, 2008. június.

[14] Ajánlás eljárásrendi követelményekre elektronikus aláírás felhasználásával végzett elektronikus archiválási szolgáltatások szolgáltatói számára, Nemzeti Hírközlési Hatóság Hivatala, 2008. június.

[15] Ajánlás elektronikus archiválási szolgáltatások nyújtásához felhasznált megbízható rendszerekre vonatkozó biztonsági követelményekre, Nemzeti Hírközlési Hatóság Hivatala, 2008. június.

[16] Az e-akta formátum specifikációja, v1.2, Microsec zrt. `http://www.e-szigno.hu/?lap=eakta3/`.

[17] e-Szignó Hitelesítés Szolgáltató – minősített elektronikus archiválás szolgáltatásra vonatkozó – általános szerződési feltételek.

[18] ITU X.509 Information technology — Open Systems Interconnection — The Directory: Publickey and attribute certificate frameworks.