MICROSEC
Számítástechnikai Fejlesztő Kft.

e-Szignó Hitelesítés Szolgáltató – minősített elektronikus archiválás szolgáltatásra vonatkozó – szolgáltatási szabályzat

Azonosító:	1.3.6.1.4.1.21528.2.1.1.18.1.4
Verzió:	1.4
Első verzió hatálybalépése:	2006-12-15
Biztonsági besorolás:	NYILVÁNOS
Jóváhagyta:	Ellbogen András
Jóváhagyás dátuma:	2008-11-20
Hatálybalépés dátuma:	2008-12-20

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

Változáskövetés

Verzió	A változás leírása	Hatálybalépés	Készítette
1.0	Első változat OID: 1.3.6.1.4.1.21528.2.1.1.18	2006-12-15	Dr. Berta István Zsolt
1.1	Módosítás a Nemzeti Hírközlési Hatóság észrevételeinek megfelelően OID: 1.3.6.1.4.1.21528.2.1.1.18.1.1	2007-01-08	Dr. Berta István Zsolt
1.2	Megváltozott a fogyasztóvédelem elérhetősége. OID: 1.3.6.1.4.1.21528.2.1.1.18.1.2	2008-01-01	Dr. Berta István Zsolt
1.3	Nem lépett hatályba. OID: 1.3.6.1.4.1.21528.2.1.1.18.1.3	2008-10-01	Dr. Berta István Zsolt
1.4	Megfelelés az NHH által kibocsátott követelményrendszernek OID: 1.3.6.1.4.1.21528.2.1.1.18.1.4	2008-12-20	Dr. Berta István Zsolt

Tartalomjegyzék

1. Bevezetés

Jelen dokumentum a Microsec Számítástechnikai Fejlesztő Kft. (továbbiakban: Szolgáltató) által üzemeltetett e-Szignó Hitelesítés Szolgáltató minősített szolgáltatóként nyújtott elektronikus archiválás szolgáltatására vonatkozó Szolgáltatási Szabályzata (továbbiakban: Szabályzat).

A Szolgáltató szolgáltatásait a vele szerződéses viszonyban álló ügyfelek részére biztosítja.

Jelen Szabályzat az elektronikus archiválás szolgáltatás nyújtásának kereteit – a részletes eljárási és egyéb működési szabályokat – tartalmazza.

1.1. Áttekintés

1.1.1. A Szabályzat

Jelen Szabályzat célja, hogy összefoglalja mindazokat az információkat, amelyeket a Szolgáltatóval kapcsolatba kerülő ügyfeleknek tudniuk érdemes. Ezzel elő kívánja segíteni, hogy ügyfelei és leendő ügyfelei minél könnyebben megismerhessék a Szolgáltató által kínált szolgáltatások részleteit, feltételeit és a szolgáltatás nyújtásának gyakorlati hátterét; hogy átláthassák a Szolgáltató működését, és ennek révén minél könnyebben eldönthessék, hogy azok megfelelnek-e, illetve az egyes szolgáltatások melyik típusa felel meg igényeiknek, elvárásaiknak.

1.1.2. A Szabályzat hatálya

Tárgyi hatálya: A Szabályzat az 1.1.4. fejezetben ismertetett, minősített Szolgáltatóként nyújtott elektronikus archiválás szolgáltatás nyújtását és igénybevételét foglalja magában.

Időbeli hatálya: A Szabályzat jelen verziója a dokumentum címlapján feltüntetett hatálybalépési dátumtól határozatlan ideig hatályos. A hatályosság megszűnik a Szabályzat újabb verziójának hatályba lépésekor vagy a szolgáltatások beszüntetésekor.

Személyi hatálya: A Szabályzat hatálya a Szolgáltatóra és az Előfizetőre terjed ki.

Területi hatálya: A jelen Szabályzat szerint elektronikusan nyújtott szolgáltatások az egész világon elérhetőek. A jelen Szabályzat 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 [1] törvény teremtette meg.

1.1.3. A Szolgáltató

A Szolgáltató adatai

Név:	MICROSEC Számítástechnikai Fejlesztő Kft.
Cégjegyzék szám:	01-09-078353 a Fővárosi Bíróság, mint Cégbíróság
Székhely:	1022 Budapest, Marcibányi tér 9.
Telephely:	1031 Budapest, Záhony u. 7, Graphisoft Park, D épület
Telefonszám:	(+36-1) 505-4444
Telefax szám:	(+36-1) 505-4445
Internet cím:	`http://www.microsec.hu`, `http://www.e-szigno.hu`
Minősítések:	ISO 9001:2000, ISO 27001

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

A szolgáltató egység neve:	e-Szignó Hitelesítés Szolgáltató
Ügyfélszolgálati iroda:	1031 Budapest, Záhony u. 7., Graphisoft Park, D épület
Ügyfélszolgálati iroda nyitvatartási ideje:	munkanapokon 8:00-12:00 és 14-16:30 között
Ügyfélszolgálati iroda telefonszáma:	(+36-1) 505-4444
Ügyfélszolgálati iroda e-mail címe:	`info@e-szigno.hu`
A szolgáltatással kapcsolatos információk elérése:	`http://www.e-szigno.hu`
Panaszok bejelentésének helye:	MICROSEC Számítástechnikai Fejlesztő Kft. 1031 Budapest, Záhony u. 7., Graphisoft Park, D épület
Illetékes fogyasztóvédelmi felügyelőség:	NFH Közép-magyarországi Regionális Felügyelősége 1052 Budapest, Városház u. 7. 1364 Budapest, Pf. 270. tel.: +361 318 2681 fax: +361 318 1639

A Szolgáltató bemutatása

A Microsec Kft. 2002. május 30. óta szerepel a Nemzeti Hírközlési Hatóság (korábban Hírközlési Felügyelet) 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 Kft. 2005. május 15. óta minősített szolgáltatóként is szerepel a Nemzeti Hírközlési Hatóság nyilvántartásában elektronikus aláírás hitelesítés szolgáltatás, időbélyegzés és eszköz szolgáltatás vonatkozásában.

A Microsec Kft. minősített elektronikus archiválás szolgáltatást nyújtó szolgáltatóként is szerepel a Nemzeti Hírközlési Hatóság 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 Kft. kiemelten fontosnak tartja ügyfelei elégedettségét. A magas színvonalú szolgáltatások fenntartása érdekében a Szolgáltató ISO 9001:2000 szabványnak megfelelő minőségbiztosítási rendszert üzemeltet 2002. január 23. óta. A szabványnak való megfelelést a Lloyd's Register Quality Assurance ellenőrizte. A Microsec Kft. nagy figyelmet szentel az által üzemeltetett rendszerek biztonságára, ezért fő tevékenységi területein a MSZ/ISO/IEC 27001:2005-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.

1.1.4. Szolgáltatások

A szolgáltatási szerződés (a továbbiakban: *Szerződés*) keretében a Szolgáltató elektronikus archiválás szolgáltatást nyújt az Előfizető számára. A Szolgáltató a Szerződés keretében minősített szolgáltatóként nyújtja az elektronikus archiválás szolgáltatást. 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).

[1] Az itt szereplő fogalmakat (pl.: fájl, dokumentum, aláírás, e-akta) fogalmát az 1.7. fejezet definiálja.

- A Szolgáltató biztonságosan tárolja az e-aktákat (fájlokat és érvényességi láncokat), és biztosítja, hogy saját munkatársai nem férhetnek hozzájuk. 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. Ezek részleteit a 5. fejezet írja le.

- 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 [1] szerint definiált elektronikus archiválás szolgáltatásnak, amely szerint az Előfizető az aláírt 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 azoknak az időbélyegeknek a hosszú távú érvényességét biztosítja, amelyek ETSI TS 101 903 formátumú (például ún. XAdES-T) aláírásokban helyezkednek el.

A Szolgáltató az alábbi archiválási rend szerint nyújtja az elektronikus archiválás szolgáltatást:

- „e-Szignó Hitelesítés Szolgáltató – minősített elektronikus archiválás szolgáltatásra vonatkozó – archiválási rend” [2]

1.1.5. Archiválási szabályzat

Az archiválás időtartama az Előfizető és a Szolgáltató közötti Szerződés érvényességi ideje.

A Szolgáltató a 5.5. fejezetben felsorolt formátumú fájlok hosszú távú olvashatóságát biztosítja, az ott leírt módon, az ott leírt feltételek mellett.

1.2. Szabványok és előírások

A Szabályzat tartalmi vonatkozásokban eleget tesz a vonatkozó hazai jogszabályok előírásainak és ajánlásainak [1], [3].

A jelen Szabályzat 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 [4], illetve az RFC 3280 [5] specifikációnak, valamint a [6] specifikációnak megfelelő tanúsítványokat használ és fogad el.
- A Szolgáltatások nyújtása során felhasznált minősített időbélyeg megfelel az RFC 3161: Time-Stamp Protocol (TSP) ajánlásban megfogalmazottaknak. [7], valamint a [8] specifikációnak.
- A Szolgáltató az ETSI TS 101 903 (XAdES) [9] specifikációnak megfelelő elektronikus aláírásokat fogad el. Ennek megfelelően elfogadja a [10] specifikációnak megfelelő aláírásokat is.
- A Szolgáltató a CWA 14171 specifikáció [11] szerint ellenőrzi az elektronikus aláírásokat.
- A Szolgáltatások nyújtása során a Szolgáltató a Nemzeti Hírközlési Hatóság elektronikus aláírással kapcsolatos szolgáltatások nyújtása során alkalmazható biztonságos kriptográfiai algoritmusokról szóló [12] határozata szerinti algoritmusokat használ.
- A Szolgáltatásokat nyújtó rendszer megfelel at RFC 4810 (Long-Term Archive Service Requirements) specifikációnak. [13]
- A Szolgáltatásokat nyújtó rendszer megfelel a Nemzeti Hírközlési Hatóság által kibocsátott követelményekre vonatkozó ajánlásoknak is. [14], [15], [16]

1.3. Dokumentum neve és azonosítása

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

1.4. Közösség

- *Szolgáltató*: Az elektronikus archiválás szolgáltatást nyújtó fél (lásd: 1.1.3. 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.
- *Érintett fél*: Az elektronikus archiválás szolgáltatás során kibocsátott igazolásokat befogadó, illetve felhasználó fél.

1.5. Alkalmazhatóság

A jelen Szabályzat szerint nyújtott elektronikus archiválás szolgáltatás kizárólag az itt, valamint a szolgáltatási szerződésben leírtak szerint használható fel.

1.6. Kapcsolattartás

A Szolgáltatóval az ügyfelek a Szolgáltató ügyfélszolgálati irodáján keresztül tartják a kapcsolatot. Az ügyfélszolgálati iroda elérhetőségét az 1.1.3. fejezet tartalmazza.

1.7. Fogalmak meghatározása

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

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* ([17]) 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*.

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 bizonyos formátumú fájlok (lásd: 5.5. fejezet)

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 (nyílt vagy titkosított) e-aktát (is) 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 korábbi verziók is elérhetőek.

A Szolgáltató a következő dokumentumokat teszi közzé:

- „e-Szignó Hitelesítés Szolgáltató – minősített elektronikus archiválás szolgáltatásra vonatkozó – általános szerződési feltételek” [18],
- „e-Szignó Hitelesítés Szolgáltató – minősített elektronikus archiválás szolgáltatásra vonatkozó – szolgáltatási szabályzat” [19] (ez a dokumentum),
- „e-Szignó Hitelesítés Szolgáltató – minősített elektronikus archiválás szolgáltatásra vonatkozó – archiválási rend” [2].

A Szolgáltató a honlapján teszi közzé, hogy mely megbízható gyökér tanúsítványokra milyen feltételek szerint vállalja az érvényességi lánc felépítését. A Szolgáltató az Előfizetővel egyedi szerződést köt, a szolgáltatáshoz kapcsolódó árakat és díjakat e szerződés melléklete tartalmazza.

2.2. A közzététel gyakorisága

A Szabályzattal kapcsolatos új verziók közzététele a 2.1. fejezetben ismertetett eljárásoknak megfelelően történik. 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

Az Előfizető a következő módon veheti igénybe az elektronikus archiválás szolgáltatást:

1. Az Előfizető kapcsolatba lép a Szolgáltató ügyfélszolgálati irodájával.
2. A Szolgáltató tájékoztatja az Előfizetőt a Szolgáltatási Szabályzat tartalmáról és elérhetőségéről. A Szolgáltató ezen tájékoztatást a kapcsolatfelvétel során adja meg. A Szolgáltató honlapján egy külön erre szolgáló tájékoztató dokumentum is elérhető.
3. Az Előfizető a Szolgáltató honlapján keresztül tájékozódik az elektronikus archiválás szolgáltatás felhasználásának módjáról, biztonsági fokáról, szolgáltatási szabályzatáról, a szerződés feltételeiről, valamint az alkalmazandó adatvédelmi szabályokról. Ezt a Szolgáltató honlapján megtalálható általános szerződési feltételek [18], archiválási rend [2], jelen szolgáltatási szabályzat [19], illetve a Szolgáltató által készített ügyfél-tájékoztató dokumentum alapján teheti meg.
4. A Szolgáltató – külön szerződés keretében – biztosítja az Előfizetőnek a Szolgáltatás igénybe vételéhez szükséges titkosító és authentikációs tanúsítványokat. Felhasználónév és jelszó alapú authentikáció esetében meghatározásra kerülnek az Előfizetőhöz tartozó felhasználónév-jelszó párok.
5. A Szolgáltatási Szerződés kézzel írott vagy minősített elektronikus aláírással köthető meg. A Szolgáltatási Szerződés határozatlan időre szól, az archiválás időtartama a Szolgáltatási Szerződés érvényességének ideje.

3.2. Dokumentum feltöltése

Az Előfizető kizárólag biztonságos csatornán keresztül juttathatja el a dokumentumokat a Szolgáltató archívumába. Amennyiben ez elektronikusan, az Interneten keresztül történik, akkor a feltöltés a következő módon zajlik le:

1. Az Előfizető SSL kapcsolatot létesít a Szolgáltatóval. A Szolgáltató az Előfizetőt vagy az SSL kapcsolat felépítéséhez használt tanúsítványa vagy a jelszava alapján azonosítja.

   Az Előfizető az SSL kapcsolaton keresztül tölthet fel dokumentumokat a Szolgáltató archívumába. Az Előfizető Dublin Core szerinti [20] metaadatokat is megadhat az egyes dokumentumokkal kapcsolatban. A metaadatokat elhelyezheti e-aktában is, de feltöltéskor is megadhatja őket.

2. Az Szolgáltató ellenőrzi, hogy a feltöltött e-akta megfelelő formátumú-e, azaz megfelel-e a Szolgáltató honlapján közzétett e-akta specifikációnak. [17] Visszautasítja azon e-aktákat, amelyek aláíratlan fájlokat is tartalmaznak.

3. A Szolgáltató ellenőrzi az e-aktákban szereplő elektronikus aláírásokat[2]. Ellenőrzi, hogy az egyes aláírások az aláírt fájlokhoz tartoznak-e. Ezt követően megpróbálja visszavezetni az aláírást valamely elfogadott gyökér tanúsítványra (lásd: 2.1. fejezet), és OCSP alapján ellenőrzi a tanúsítványlánc minden elemének visszavonási állapotát is. A folyamat csak akkor megy tovább, ha az e-aktában szereplő összes aláírás és időbélyeg érvényesnek bizonyult.

   Az aláírás ellenőrzéséhez a Szolgáltató az e-Szignó aláírás-létrehozó és ellenőrző programot használja. Az e-Szignó program 3-as változatának aláíró modulja a MATRIX Vizsgáló, Ellenőrző és Tanúsító Kft. által végzett tanúsítás szerint olyan minősített aláírás-létrehozó alkalmazás, amely az aláírásokat a CWA 14171 szerint ellenőrzi és ETSI TS 101 903 szerinti formátumot hoz létre.

   A Szolgáltató így biztosítja, hogy csak olyan adatok tekintetében nyújt archiválás szolgáltatást – azaz csak olyan e-aktákat fogad be – amelyeken legalább fokozott biztonságú elektronikus aláírás van. A Szolgáltató úgy győződik meg róla, hogy egy aláírás valóban fokozott biztonságú elektronikus aláírás (illetve egy időbélyeg valóban időbélyeg), hogy visszavezeti egy elfogadott hitelesítés (vagy időbélyegzés) szolgáltató megbízható gyökértanúsítványára. Előfordulhat, hogy egy hitelesítés szolgáltató olyan teszt tanúsítványt bocsátanak ki, amelyek saját megbízható gyökértanúsítványuk

[2] Az e-akta tartalmazhat az egyes fájlokon lévő aláírást is, de lehet benne ún. keretaláírás is, amely az e-aktában lévő minden fájl, és a fájlokon lévő összes aláírás és időbélyeg integritását biztosítja. Ha az e-akta tartalmaz keretaláírást, akkor a Szolgáltató kizárólag a keretaláírásokkal foglalkozik (a belső aláírásokat nem ellenőrzi). Ha az e-akta nem tartalmaz keretaláírást, akkor a Szolgáltató kizárólag a fájlokon lévő aláírásokkal foglalkozik. Ha az Előfizető mind a keretaláírások, mind a belső aláírások hitelességét biztosítani szeretné, akkor keretaláírásokkal is és keretaláírás nélkül is be kell küldenie az e-aktát.

alapján ellenőrizhető. Az ilyen tanúsítványokat a Szolgáltató nem tudja elkülöníteni a valódi, fokozott biztonságú aláírás létrehozására alkalmas tanúsítványoktól, és az ebből adódó károkért nem vállal felelősséget.

4. A Szolgáltató felépíti az e-aktákban szereplő elektronikus aláírásokhoz tartozó érvényességi láncokat, és minősített időbélyeget helyez el rajtuk. Az így kapott érvényességi láncokat ETSI TS 101 903 formátumú ún. archív aláírásként (XAdES-A) elhelyezi az e-aktában.

   A Szolgáltató OCSP szolgáltatás segítségével gyűjti össze a hiányzó visszavonási információkat. Amennyiben a tanúsítványláncban szereplő minden szolgáltató OCSP szolgáltatására vonatkozó kivárási idő 0, akkor a visszavonási információk rövid időn belül – akár másodpercek alatt – előállnak. Amennyiben valamely kivárási idő nem 0, akkor a Szolgáltató a szükséges ellenőrzéseket a kivárási idők elteltével végzi el a szabványok és nemzetközi ajánlások szerint. A Szolgáltató elutasítja az e-aktát, ha az ellenőrzést 3 nap alatt nem tudja elvégezni.

5. A Szolgáltató kizárólag titkosítva tárolja el az archiválandó nyílt e-aktát. A nyílt e-aktát a Szolgáltató a 3.6. fejezetben leírt biztonságos mechanizmus segítségével megsemmisíti. A Szolgáltató kizárólag a jelen Szolgáltatási Szabályzatban meghatározott esetekben, kizárólag egy különleges eljárás keretében, több bizalmi munkakört betöltő személy jelenlétében állíthatja vissza a nyílt e-aktát (lásd: 5.7. fejezet).

6. A Szolgáltató haladéktalanul, de a feltöltést követően legkésőbb 3 napon belül visszaigazolást küld az Előfizetőnek arról, hogy az e-aktát sikeresen befogadta. Ha a folyamat valahol megszakadt, a Szolgáltató erről is értesíti az Előfizetőt. Ilyenkor 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). A visszaigazolásokat és hibaüzeneteket a Szolgáltató elektronikus levélben vagy más, az Előfizetővel előre egyeztetett csatornán küldi ki.

   A visszaigazolás tartalmazza az archívumba beküldött e-akta lenyomatát, illetve azt, hogy az archívum befogadta-e az aktát. Ezen kívül, sikeres befogadás esetén tartalmazza

   - az archívumba befogadott – már XAdES-A aláírásokat tartalmazó – e-akta lenyomatát, amely egyedi azonosítóként is szolgál,
   - az archiválási rend azonosítóját,
   - annak az egyértelmű jelzését, hogy a szolgáltatás az Eat. hatálya alatt álló elektronikus archiválás szolgáltatás,
   - az archiválás időtartamát,
   - azt, hogy a Szolgáltató vállalja-e az olvashatóság és értelmezhetőség fenntartását az aktában lévő egyes fájlokkal kapcsolatban.

Ezen kívül egyéb információkat is tartalmazhat.

A visszaigazoláson – akár sikeres a befogadás, akár sikertelen – fokozott biztonságú elektronikus aláírás és minősített időbélyegző szerepel. Az Előfizetőnek meg kell győződnie róla, hogy a visszaigazolás valóban a feltöltött e-aktára vonatkozik (azaz a feltöltött e-akta lenyomata szerepel-e benne), és a visszaigazoláson lévő elektronikus aláírás érvényes. A visszaigazolás elektronikusan aláírt dokumentum, így ha az Előfizető hosszú távon is meg szeretné őrizni a visszaigazolás hitelességét, akkor az elektronikus aláírt dokumentumok archiválására vonatkozó jogszabályok szerint kell eljárnia.

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.

A Szolgáltató más biztonságos csatornán keresztül is biztosíthat feltöltési lehetőséget az Előfizető számára. Ilyenkor a feltöltött e-akták bizalmasságát nem az SSL kapcsolat, hanem ezen csatorna – például bérelt vonal – biztosítja. Ettől eltekintve a folyamat ekkor is a fenti elvek szerint zajlik le.

A Szolgáltatóval előre egyeztetett esetben az Előfizető nemcsak hálózaton keresztül, hanem valamely adathordozón, például optikai lemezen is juttathat el dokumentumokat a Szolgáltatónak. Az így kapott lemezek tartalmát a Szolgáltató a belső szabályzatainak megfelelően, szintén a fenti elvek szerint dolgozza fel.

3.3. Érvényességi lánc elérhetőségének biztosítása

Az Előfizető kizárólag biztonságos csatornán keresztül férhet hozzá a Szolgáltató archívumában lévő fájlokhoz, dokumentumokhoz, érvényességi láncokhoz. Amennyiben ez elektronikusan, az Interneten keresztül történik, akkor e folyamat a következő módon zajlik le:

1. Az Előfizető SSL kapcsolatot létesít a Szolgáltatóval. A Szolgáltató az Előfizetőt vagy az SSL kapcsolat felépítéséhez használt tanúsítványa vagy a jelszava alapján azonosítja.

2. A Szolgáltató megállapítja, hogy az Előfizető mely e-aktához kíván hozzáférni, és azt, hogy jogosult-e erre. Ekkor lehetősége van a dokumentumhoz kapcsolódó Dublin Core [20] szerinti metaadatok alapján keresni a fájlokra, e-aktákra.

3. Ha az Előfizető jogosult letölteni az e-aktát, akkor a Szolgáltató elküldi az Előfizetőnek a titkosított e-aktát. Ezen e-akta az Előfizető által felépített SSL kapcsolaton keresztül jut el az Előfizetőhöz.

A Szolgáltató megtagadja az e-akta letöltését, amennyiben az e-aktával kapcsolatban elbírált és hatályosult törlési kérelmet kapott.

4. Az Előfizető rendelkezik az archiválás szolgáltatás igénybe vételére szolgáló titkosító tanúsítványához tartozó magánkulccsal. Ezzel a kulccsal dekódolja az e-aktát, így hozzájut – az archiválás pillanatában létező – érvényességi lánchoz.

A Szolgáltatóval előre egyeztetett esetben az Előfizető nemcsak hálózaton keresztül, hanem valamely adathordozón, például optikai lemezen is átveheti a Szolgáltató archívumában szereplő fájljait, dokumentumait, érvényességi láncait. A hozzáférés ekkor is a fenti elvek szerint zajlik le, de ekkor az Előfizető (vagy írásban meghatalmazott képviselője) nem tanúsítvány, hanem valamely személyazonosításra alkalmas okmány alapján azonosítja magát.

A feltöltött e-akták az Előfizető tulajdonában vannak (lásd: 1.4. fejezet), így az Előfizető tölti be az adatgazda szerepét is. Amennyiben az e-aktához harmadik fél is hozzáfér, ő az Előfizető nevében jár el.

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[3] 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.

[3] 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.

Az igazolás igényléséhez az Előfizető (vagy meghatalmazottja) meg kell, hogy adja a lenyomatát vagy (a befogadáskor kiküldött visszaigazolásban is szereplő) egyedi azonosítóját annak a fájlnak vagy e-aktának, amelyikkel kapcsolatban az igazolást kéri. Ezen információkat a 3.3. fejezetben lévő keresőfelületről is kinyerheti. Az igazolást a Szolgáltató annak az Előfizetőnek adja ki, akihez az adott e-akta a Szolgáltató informatikai rendszere szerint tartozik. Harmadik félnek a Szolgáltató kizárólag a fent leírt meghatalmazás bemutatása esetén adja ki az igazolást.

A Szolgáltató az Előfizető rendelkezésére bocsátja azt a titkosított e-aktát is, amely azon nyílt e-aktát tartalmazza, amelyre az igazolás vonatkozik. Az e-akta az Előfizető titkosító tanúsítványához tartozó magánkulccsal visszafejthető.

Az igazolás kiállítása e-akta formában, az Informatikai és Hírközlési Minisztérium által kidolgozott, a közigazgatásban alkalmazható elektronikus aláírás formátumokra vonatkozó műszaki specifikációban meghatározott elektronikus aláírás formátumban történik. [10] Az Előfizető kérésére az igazolás más formátumban is kiállítható. A Szolgáltató az igazolás kiállításához olyan terméket használ, amely rendelkezik az Eat. szerint nyilvántartásba vett tanúsító szervezet által erre a célra kiállított igazolással.

A Szolgáltató megtagadja az igazolás kibocsátását, amennyiben az e-aktával kapcsolatban elbírált és hatályosult törlési kérelmet kapott.

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.

Amennyiben az Előfizető a Szolgáltató ügyfélszolgálati irodájában szeretné megtekinteni a dokumentumot, magával kell vinnie az archív szolgáltatás igénybe vételéhez szükséges titkosító tanúsítványához tartozó magánkulcsát, illetve a kulcsot tartalmazó intelligens kártyáját.

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.

Törlési kérelmet a Szolgáltató ügyfélszolgálati irodájának kell benyújtani, személyesen vagy minősített elektronikus aláírással ellátva. A törlést a Szolgáltató egy munkanapon belül bírálja el és hajtja végre. Törlési kérelem olyan módon is benyújtható, hogy a törlést a Szolgáltatónak nem haladéktalanul, hanem csak egy meghatározott napon kell végrehajtani.

A törlésről a Szolgáltató fokozott biztonságú elektronikus aláírással és minősített időbélyegzővel ellátott visszaigazolást küld az Előfizetőnek. A visszaigazolás tartalmazza a törölt e-akta egyedi azonosítóját, a törlés időpontját, valamint a törlést kérő benyújtó azonosítóját is.

3.7. A szolgáltatási szerződés megszűnése

A Szerződés megszűnése esetén a Szolgáltató az általános szerződési feltételekben [18] leírt eljárás szerint törli az Előfizetőhöz tartozó 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 a 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 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 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 jogszabályoknak és belső szabályzatainak megfelelő 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 Szolgáltató a következő bizalmi szerepköröket határozza meg az alábbi felelősségkörökkel:

Az e-Szignó Hitelesítés Szolgáltató igazgatója: A Szolgáltató – az e-Szignó Hitelesítés Szolgáltató – informatikai rendszeréért átfogóan felelős vezető.

Biztonságtechnikai főmunkatárs: Feladata és felelőssége a Szolgáltató – az e-Szignó Hitelesítés Szolgáltató – biztonsági szabályzatának betartatása a Szolgáltató alkalmazottaival.

Infrastruktúra adminisztrátor:
Feladata a Szolgáltató rendszereinek telepítése, konfigurálása, karbantartása. Felelős a rábízott rendszerelemek megbízható és folyamatos működéséért, valamint a technológia fejlődésének nyomon követéséért, az egyes rendszerelemekben való biztonsági rések felderítéséért és megoldási javaslatok kidolgozásáért.

Rendszervizsgáló: Feladata a biztonságos és funkcionálisan helyes működés ellenőrzése a naplófájlok és az archivált adatok alapján. Azért felelős, hogy a tőle elvárható legnagyobb mértékben felderítse a Szolgáltató rendszerében lévő működési rendellenességeket, valamint a biztonsági eseményeket, és jelentse őket az önálló üzleti egység vezetője, illetve a Szolgáltató felső vezetése felé.

Operátor: Feladata a napi archiválási feladatok elvégzése, azért felelős, hogy az archiválás valóban megtörténjen.

Archiválási tisztviselő: Amennyiben a Szolgáltatónak az archiválás szolgáltatás nyújtásához szüksége van a nyílt e-aktára, akkor az e-akták visszafejtésére szolgáló kulcsot több archiválási tisztviselő együttes jelenlétében fejti vissza, illetve kezeli. Az archiválási tisztviselő felel a nyílt kulcs és a nyílt e-akták biztonságos megsemmisítéséért is.

Archív igazolás kiállításáért felelős tisztviselő: Feladata az arcív igazolások kibocsátása, hitelesítése.

A fenti 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 a titkosított e-akták visszafejtésére szolgáló magánkulcs dekódolásához szükséges.

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 visszaélések 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.

Felvételi követelményként a Szolgáltató minden dolgozója számára legalább középfokú végzettséget ír elő, de a Szolgáltató a továbbiakban is gondot fordít arra, hogy dolgozói megfelelő képzésben részesüljenek. Közvetlenül a felvételt követően a Szolgáltató új dolgozóit képzésben kell részesíteni, melynek keretében el kell sajátítania a munkája elvégzéséhez szükséges ismereteket. A Szolgáltató általában támogatja a dolgozók szakmai fejlődését, de el is várja, hogy a dolgozók saját szakterületükön önállóan fejlesszék tudásukat. A Szolgáltató bizonyos dolgozóinak munkaköri kötelessége a technikai és üzleti újdonságok felderítése és összegyűjtése, rendszerezése, és ezen ismeretek megosztása munkatársaikkal.

4.3.1. Munkabeosztás körforgásának gyakorisága és sorrendje

Körforgás az egyes munkabeosztások között kötelezően nem valósul meg.

4.3.2. A felhatalmazás nélküli tevékenységek büntető következményei

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

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

Mindezek tartalmazzák azokat a munkajogi vagy büntető következményeket, melyek a különböző fegyelem-, munkaköri kötelezettség- vagy törvénysértést szankcionálják. Amennyiben egy munkatárs (gondatlanságból fakadóan vagy szándékosan) megsérti a fenti szabályokat, ellene büntető intézkedéseket hoznak (melyek az elkövetés módjától és következményétől függően a jutalom megvonástól fegyelmi eljárás indításán és kártérítésen át, egészen a hatósági feljelentésig terjedhet).

4.3.3. A szerződéses alkalmazottakra vonatkozó követelmények

A Szolgáltató bizalmi munkakörben csak vele munkaviszonyban álló személyt alkalmaz.

Az egyéb feladatok ellátására, alvállalkozói vagy megbízásos szerződésben foglalkoztatott szerződő személyeket (külső munkavállalókat és ideiglenes alkalmazottakat egyaránt) a Szolgáltató lehetőleg a korábban már minősített beszállítók listájáról választ. A beszállítókkal

a Szolgáltató olyan írásos szerződést köt, melyben beszállító elfogadta a Szolgáltató biztonságpolitikájának a beszállító tevékenységére vonatkozó részeit.

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

4.3.4. A személyzet számára biztosított dokumentációk

Minden bizalmi munkakört betöltő munkatárs írásban megkapja a következő dokumentumokat:

- Az e-Szignó Hitelesítés Szolgáltató biztonsági szabályzata,
- aláírt titoktartási nyilatkozat,
- egyéni munkaköri leírás,
- a tervezett és rendkívüli továbbképzések alkalmával megkapja az adott oktatási formához tartozó oktatási segédanyagokat is.

Az e-Szignó Hitelesítés Szolgáltató biztonsági szabályzatban bekövetkező változásokról írásos értesítők formájában mindenki tájékoztatást kap.

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 Szolgáltató pontos időt biztosító egysége 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, illetve az az esetleges hibaesemények. Mindenképpen naplózásra kerülnek

- a rendszer környezetében bekövetkező, illetve a kulcsok kezelésével kapcsolatos események,
- a naplózási funkció indítása, leállítása,
- a naplózási paraméterek megváltoztatása,
- a naplózás hibája miatt végzett tevékenységek,
- a rendszerhez való minden hozzáférési kísérlet,
- az e-akták feltöltésével és a bennük lévő aláírások ellenőrzésével kapcsolatos információk,
- a visszaigazolásokkal kapcsolatos információk,
- a hozzáférők jogosultságainak módosításaival kapcsolatos információk,
- az adatok rendelkezésre állásának, sértetlenségének megőrzésével, hitelességének és letagadhatatlanságának megőrzésével, értelmezhetőségének fenntartásával és törlésével kapcsolatos információk,
- az e-akták letöltésével, az igazolás-kérések teljesítésével, és az archívum más szolgáltatónak történő esetleges átadásával kapcsolatos információk.

4.4.2. A naplóállomány feldolgozásának gyakorisága

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 naplóállományokat 90 napig tárolják a keletkezésük helyén. Ezek után az adatokat egyszer írható médiára archiválják, és a naplóállományok archív adathordozóit 10 évig biztonságosan megőrzik.

4.4.4. A naplóállomány védelme

Szolgáltató rendszerének naplóbejegyzéseit a Szolgáltató időbélyeggel látja el, 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 naplóállományokat 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 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 Szolgáltatónak 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 7.3. fejezetben 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 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 egysége esik ki, a Szolgáltató 3 órán 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, Szolgáltató a másodlagos helyszínen is képes szolgáltatásainak beindítására.

Ilyen esetekben a Szolgáltató legfeljebb 3 órán 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 Nemzeti Hírközlési 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 [12] 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.

A Szolgáltató akkor is újra-titkosítja az adott Előfizetőhöz tartozó e-aktákat, ha az Előfizető titkosító tanúsítványa változik. Amennyiben az Előfizető titkosításra használt kulcspárjára és a hozzá kapcsolódó tanúsítványra vonatkozó valamely algoritmus avul el, akkor a Szolgáltató a titkosító tanúsítványokra vonatkozó szabályzatai [21] szerint visszavonja, majd lecseréli az érintett tanúsítványokat, és újra-titkosítja az érintett Előfizetők e-aktáit.

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 a 5.2., illetve 5.1. fejezetben szereplő műveleteket.

5.4. Hitelesítés és időbélyegzés szolgáltatók elfogadása

A Szolgáltató a honlapján teszi közzé, hogy mely hitelesítés szolgáltatók tanúsítványait és mely időbélyegzés szolgáltatók időbélyegeit milyen feltételekkel fogadja el. Az elfogadott szolgáltatók listája az alábbi címen érhető el:

`http://www.e-szigno.hu/?lap=dokszab_asz_elfogadott_szolgaltatok`

A Szolgáltató dokumentált eljárásrenddel rendelkezik, amely szerint az egyes hitelesítés szolgáltatók és időbélyegzés szolgáltatók tanúsítványait és időbélyegeit elfogadja, illetve nem fogadja el. Ezen eljárásrend többek között azt is meghatározza, hogy a Szolgáltató milyen intézkedéseket hajt végre egy korábban elfogadott hitelesítés szolgáltató, illetve időbélyegzés szolgáltató magánkulcsának kompromittálódása esetén.

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

A Szolgáltató gondoskodik róla, hogy az archiválás időtartama alatt bizonyos formátumú fájlok megjelenítéséhez szükséges szoftver és hardver eszközök folyamatosan rendelkezésére álljanak. A Szolgáltató ennek érdekében szabályozott és auditált belső folyamatokat alakított ki. A Szolgáltató belső szabályzatai kitérnek a fájlok megjelenítésére szolgáló mindenkori hardver és szoftver környezet rendelkezésre állásának biztosítására, a környezet rendszeres felülvizsgálatára és naprakészen tartására. Ezen szabályzatok szabályozzák az új adathordozókra történő mentések elvégzésének módját és gyakoriságát is. A Szolgáltató az

eredeti aláírt bitsorozat olvashatóságát, értelmezhetőségét biztosítja, így a Szolgáltató nem viszi át az aláírt fájlt más formátumba.

A Szolgáltató a dokumentumok megőrzését, tehát a dokumentumok olvashatóságának fenntartását is a szolgáltatási szerződés érvényességi idejéig vállalja.

A szolgáltatás leállításakor a Szolgáltató a 4.7. fejezetben leírtak szerint átadja a szolgáltatást egy másik szolgáltatónak. Ekkor a Szolgáltató az archivált e-akták mellett a fenti, támogatott formátumú fájlok megjelenítéséhez szükséges szoftver és hardver eszközökkel együtt a megjelenítés hosszú távú biztosításához szükséges ismereteket is átadja.

A Szolgáltató biztosítja az elektronikus ügyintézési eljárásban alkalmazható dokumentumok részletes technikai szabályairól szóló rendelet [22] 1. mellékletében felsorolt formátumú fájlok hosszú távú olvashatóságát és értelmezhetőségét. Ezen kívül más formátumú fájlok olvashatóságát és értelmezhetőségét is biztosíthatja. A Szolgáltató olyan formátumú fájlokat tartalmazó e-aktákat is befogad az archívumába, amelynek tekintetében nem biztosít olvashatóságot és értelmezhetőséget.

A Szolgáltató a következő fájlformátumok tekintetében biztosítja az olvashatóságot és értelmezhetőséget:

- ISO/IEC 646:1991 (7 bites karakterkészlet információcsere biztosításához, ASCII),
- ISO 8859-1:1998 (Latin-1, 8 bites grafikus karakterkészlet),
- ISO 8859-2:1999 (Latin-2), a magyar referenciakészletre vonatkozóan az MSZ 7795-3:1992 ASCII és ASCII/PC kód szerinti eltéréssel is,
- ISO 10646:2003 (Unicode v.4.0),
- Microsoft Rich Text Format 1.7. [23],
- Portable Document Format (PDF) 1.3. [24],
- PDF/A formátum (ISO 19005) [25],
- Microsec e-akta formátum [17],
- ETSI TS 101 903 v1.2.2 és v1.3.2 formátumú XAdES aláírások (amennyiben egy XML fájl XAdES aláírást tartalmaz, a Szolgáltató az aláírás értelmezhetőségét biztosítja),
- IETF RFC 2822 (Internet Message Format),
- IETF RFC 2045 (Multipurpose Internet Mail Extensions, MIME),
- Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható elektronikus aláírás formátumok műszaki specifikációjára [10],

- Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható végfelhasználói tanúsítványok szerkezetének és adattartalmának műszaki specifikációjára [6],
- Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható időbélyegzés formátum műszaki specifikációjára [8].
- Olyan XML formátumok, amelyekhez az Előfizető előzetesen benyújt a Szolgáltatónak egy, az adott XML formátum megjelenítésére szolgáló XSD sémadefiníciót és XSLT stíluslapot, és nyilatkozik, hogy adott névterekkel rendelkező XML-t ilyen módon kell megjeleníteni.

Amennyiben az Előfizető a fenti listában nem szereplő formátumra vonatkozóan is igényli, hogy a Szolgáltató biztosítsa az adott formátum olvashatóságát és értelmezhetőségét, és ezen igényét jelzi a Szolgáltatónak, a Szolgáltató erre vonatkozó eljárásrendje szerint megvizsgálja, hogy az adott formátum esetében ez megoldható-e, illetve milyen feltételekkel oldható meg. Amennyiben a Szolgáltató az Előfizető által kért formátumot felveszi az olvashatóság és értelmezhetőség tekintetében támogatott formátumok közé, az jelen Szabályzat módosítását jelenti.

A Szolgáltató kizárólag a fenti formátumok fent hivatkozott specifikációkban szereplő verzióit támogatja, az ettől eltérő (akár újabb) verziók szerinti fájlok olvashatóságát, megjeleníthetőségét nem garantálja. A Szolgáltató a *formátumok* olvashatóságát, értelmezhetőségét vállalja, tehát ha valamely alkalmazás hibásan, a fenti specifikációktól eltérően hozza létre vagy jeleníti meg a fájlokat, a Szolgáltató nem vállal felelősséget az ebből eredő károkért.

A Szolgáltató kizárólag a fent meghivatkozott specifikációkban leírt mértékig vállalja az egyes formátumok megjeleníthetőségét. Amennyiben egyes formátumok például beágyazott objektumokat is tartalmazhatnak, a Szolgáltató nem vállalja ezen beágyazott objektumok megjeleníthetőségének biztosítását. Mivel az e-mail formátum (RFC 2822) nem specifikálja az emailben szereplő karakterek kódolását, a Szolgáltató kizárólag olyan e-mailek megjelenítését vállalja, amelyekben az üzenet a fenti karakterkódolások egyikével szerepel. A MIME (RFC 2045) specifikáció szerint kódolt „csatolmányok" esetén a Szolgáltató kizárólag azon csatolmányok megjeleníthetőségét vállalja, amelyek a fenti formátumok egyikével rendelkeznek.

A Szolgáltató a *fájlok* olvashatóságát, megjeleníthetőségét vállalja, a fájl az 1.7. fejezetben szereplő definíciója szerint. Ez azt jelenti, hogy a Szolgáltató akkor biztosítja egy (fenti formátumú) fájl értelmezhetőségét, megjeleníthetőségét, ha az egy e-aktában az ETSI TS 101 903, illetve az e-Szignó program szerint beillesztve szerepel. A Szolgáltató nem vállalja az egyéb transzformációkkal (is) kódolt, különösen a titkosított fájlok olvashatóságának biztosítását. A fájlokon kívül a Szolgáltató e-akták olvashatóságát, megjeleníthetőségét is

vállalja. Ez az aláírások és időbélyegek ellenőrizhetőségéig, és az e-aktákban elhelyezett fájlok kinyeréséig terjed.

A Szolgáltató felhívja az ügyfelek figyelmét arra, hogy amennyiben egyes formátumok (különösen egyes nem karakterszintű formátumok) megengedik úgynevezett aktív elemek használatát, akkor előfordulhat, hogy egy ilyen formátumú fájl különböző időpontokban különböző módon jelenik meg a fenti specifikációk szerint is. A Szolgáltató azt tanácsolja ügyfeleinek, hogy lehetőleg ne helyezzenek el aláírást aktív elemeket tartalmazó fájlokon. A Szolgáltató az aktív elemeket is a fenti specifikációknak megfelelően jeleníti meg, az egyes fájlok különböző – de a fenti specifikációknak megfelelő – megjeleníthetőségéből eredő károkért nem vállal felelősséget.

A Szolgáltató alapvető ellenőrzést végez arra vonatkozóan, hogy a feltöltött e-akta tartalmaz-e olyan aktív kódot, ami a dokumentum megjelenítése során változást okozhat. Amennyiben ilyen aktív kódot talál, ennek tényét egyértelműen jelzi az Előfizetőnek. A Szolgáltató rendszere nem végez teljeskörű ellenőrzést, így a Szolgáltató nem vállal azért felelősséget, hogy rendszere minden aktív kódot megtalál.

Egy e-akta befogadásakor a Szolgáltató automata segítségével megvizsgálja, hogy az adott e-aktában lévő fájlok rendelkezhetnek-e a támogatott formátumok valamelyikével. Amelyek nem rendelkeznek támogatott formátummal, azok esetén elutasítja az olvashatóság fenntartását. A 3.2. fejezetben leírt visszaigazolás tartalmazza, hogy mely fájl formátuma ismeretlen – az ilyen fájlok olvashatóságát a Szolgáltató nem garantálja. A befogadáskor elvégzett ellenőrzés nem teljes körű, a Szolgáltató nem vállal felelősséget azért, hogy az ismeretlen formátumúnak nem tekintett fájlok támogatott formátummal rendelkeznek és szintaktikailag helyesek.

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. [1]

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

A Szolgáltató ügyfélszolgálati irodája minden munkanapon, nyitvatartási időben fogad igazolás kibocsátására vonatkozó kérelmeket, az igazolások kibocsátása 3 nap alatt történik meg. A Szolgáltató ügyfélszolgálati irodájának nyitva tartását az 1.1.3. fejezet tartalmazza.

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 a harmadik fél, amely számára bizalmi szolgáltatásokat nyújt, 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 garantálja.

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 az 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.

A Szolgáltató a titkosított dokumentumokat olyan módon tárolja, hogy a titkosított dokumentumok visszafejtéséhez szükséges dekódoló kulcs a dokumentummal egy fizikai helyszínen nincs jelen. A nyílt dokumentumokat kizárólag az elektronikus archiválás nyújtásához kapcsolódó jogszabályi követelmények teljesítéséhez állítja vissza a 5.1. és 5.2. fejezetekben leírt esetekben. A dekódoló kulcs visszaállítására különleges eljárás keretében kerül sor, amelyhez több bizalmi munkakört betöltő (archiválási tisztviselő) munkatárs szükséges. Ezen archiválási tisztviselők felügyelik a dekódoló kulcs visszaállítását, használatát és megsemmisítését. A Szolgáltató törekedik rá, hogy a dekódoló kulcsot csak a lehető legritkábban kelljen használni, és a titkosított e-aktákat csak a lehető legritkábban kelljen dekódolni. A Szolgáltató titkosítás, illetve az itt leírt szabályozással biztosítja, hogy az archivált e-aktákat saját munkatársai sem ismerhetik meg.

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. Ezen időforrásból származó időbélyeg szerepel a Szolgáltató elektronikus nyilvántartásain, naplófájljain is.

A visszaigazolásokat aláíró kulcsokat, az archivált adatok titkosításához/dekódoláshoz

szükséges kulcsokat, valamint az infrastrukturális és rendszervezérlési kulcsokat hardveres kriptográfiai eszközben kell előállítani.

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.

Amennyiben a Szolgáltató munkatársai minősített aláírást hoznak létre, azt mindig biztonságos aláírás-létrehozó eszköz segítségével teszik. A Szolgáltató által alkalmazott biztonságos aláírás-létrehozó eszköz P8WE5032v0G mikrochipből, STARCOS SPK 2.3 v7.0 operációs rendszerből, valamint a StarCert v2.2 digitális aláírás alkalmazásból álló intelligens kártya, amely rendelkezik az Eat. 7 § (5) -(6) szerinti igazolással. A Szolgáltató minősített hitelesítés szolgáltatást és minősített eszköz szolgáltatást is nyújt [26], a fenti eszközt saját eszköz szolgáltatása segítségével bocsátja ki, és az eszközre saját hitelesítés szolgáltatása keretében bocsát ki tanúsítványt.

Az aláírások ellenőrzéséhez a Szolgáltató az e-Szignó aláírás-létrehozó és ellenőrző programot használja. Az e-Szignó program 3-as változatának aláíró modulja a MATRIX Vizsgáló, Ellenőrző és Tanúsító Kft. által végzett tanúsítás szerint olyan minősített aláírás-létrehozó alkalmazás, amely az aláírásokat a CWA 14171 szerint ellenőrzi és ETSI TS 101 903 szerinti formátumot hoz létre.

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 9001:2000 szabványnak megfelelő minőségirányítási, valamint 2003 óta a MSZ/ISO/IEC 27001:2005-nek (korábban BS 7799-nek) megfelelő információbiztonság-irányítási rendszerrel, amelyeket külső auditáló szervezet auditál és vizsgál felül folyamatosan (lásd: 1.1.3. 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 [1] törvénynek és a [27] rendeletnek.

Az audit ezen kívül a Szolgáltató által támogatott archiválási rendeknek 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 [18], 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 Szolgáltatási Szabályzattal és egyéb nyilvános szabályzatokkal, különösen az alkalmazott archiválási renddel, a szerződéses feltételekkel, továbbá a vállalati belső szabályzatokkal összhangban nyújtsa; ezen alapvető kötelezettségek a következők:

- a szolgáltatásnak megfelelő jogi-, szabályozási-, anyagi-, szerződéses stb. keretek megteremtése,
- magas színvonalú és biztonságos szolgáltatások nyújtása a vonatkozó szabályzatok szerint,
- a szabályzatokban előírt eljárások betartása és az esetleg bekövetkező helytelen működés elkerülése, illetve megszüntetése,
- a Szolgáltatások biztosítása minden olyan igénylő számára, aki elfogadja a szabályzatokban rögzített feltételeket,
- a saját szabályzatok karbantartása és a nyilvános dokumentumok folyamatos elérhetővé tétele bárki számára az Interneten keresztül.

7.2.2. Az Előfizető jogai

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

Az Előfizető további jogait és kötelezettségeit az „e-Szignó Hitelesítés Szolgáltató – minősített archiválás szolgáltatásra vonatkozó – általános szerződési feltételek" [18] című dokumentumban szereplő általános szerződési feltételek tartalmazzák.

7.2.3. Az Előfizető kötelezettségei

Az Előfizető kötelessége a Szolgáltató szerződéses feltételeinek és szabályzatainak megfelelően eljárni a Szolgáltatások felhasználása során. Amennyiben a Szolgáltatást az Előfizető nevében harmadik fél veszi igénybe, az Előfizető köteles tudatosítani e harmadik félben, hogy a Szolgáltató szerződéses feltételeit be kell tartania.

Amennyiben az Előfizető elektronikus archiválás szolgáltatás igénybevételéhez szükséges valamely – különösen titkosító vagy authentikációs – tanúsítványához tartozó magánkulcs illetéktelen kezekbe kerül, az Előfizető köteles erről haladéktalanul értesíteni a Szolgáltatót, és haladéktalanul köteles kezdeményezni az érintett tanúsítvány felfüggesztését vagy visszavonását. Amennyiben az Előfizető ezek bármelyikét elmulasztja, akkor az ebből eredő károkért a Szolgáltató nem vállal felelősséget.

7.2.4. A Szolgáltató felelőssége

A Szolgáltató felelősségét jelen szolgáltatási szabályzat, a vonatkozó archiválási rendek, valamint az Ügyféllel kötött szerződés és annak mellékletei tartalmazzák.

- A Szolgáltató felelősséget vállal az általa támogatott 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 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 következő módon korlátozza felelősségét:
  - A Szolgáltató az Előfizetővel szemben a Szolgáltatási Szerződésben - a szerződés mellékletében, vagy a Szolgáltató honlapján szereplő árlistában meghatározott díjcsomagban - korlátozza felelősségét az okozott kár tekintetében.
  - A Szolgáltató felelősségvállalása nem lehet nagyobb, mint az archivált e-aktában szereplő aláírásokhoz tartozó aláírói tanúsítványban, illetve az aláíró tanúsítványtól a gyökértanúsítványig tartó érvényességi lánc egyes elemeiben lévő legkisebb tranzakciós limit, illetve az adott (aláírói vagy szolgáltatói) tanúsítványhoz kapcsolódó szolgáltatói felelősségvállalás mértéke.
  - A Szolgáltató által a 3.4. fejezet szerint elektronikusan kibocsátott igazolásokkal kapcsolatos felelősségvállalás nem lehet nagyobb, mint az igazolás aláírásakor használt minősített tanúsítványban szereplő tranzakciós limit mértéke. Papír alapú igazolás esetén ezen korlátozás az igazolás szövegében tüntethető fel. Az Előfizető által választott díjcsomag, illetve a szolgáltatási szerződés határozzák meg ezen korlátozás mértékét.

7.2.5. Az Érintett fél felelőssége

Amennyiben egy Érintett fél ésszerűen kíván az archiválás szolgáltatás során kibocsátott igazolásra (lásd 3.4. fejezet) támaszkodni, a jelen Szolgáltatási Szabályzatnak megfelelően

célszerű eljárnia. Ez az alábbiak mérlegelését jelenti:

- Az Érintett félnek célszerű meggyőződnie róla, hogy a kibocsátott igazolás valóban egy adott dokumentumhoz, e-aktához tartozik-e. Ezt úgy teheti meg, hogy összehasonlítja az igazolásban szereplő lenyomat-értéket a dokumentum lenyomatával.
- Az Érintett félnek célszerű meggyőződnie a kibocsátott igazolás hitelességéről. Ehhez az igazoláson szereplő kézzel írott vagy elektronikus aláírást kell ellenőrizni. Minősített elektronikus aláírással hitelesített igazolások esetén ez az aláírás és az aláíráshoz kapcsolódó tanúsítvány érvényességének ellenőrzését jelenti a tanúsítványra vonatkozó hitelesítési rend szerint.

  Az igazolás mindaddig hiteles, amíg az aláírás létrehozására szolgáló technológia, és az aláírt igazolásban szereplő lenyomat létrehozására szolgáló algoritmus biztonságosnak minősül, illetve ha a vonatkozó jogszabályoknak megfelelően kerül megőrzésre.
- Az Érintett félnek célszerű meggyőződnie róla, hogy az igazoláshoz kapcsolódó szolgáltatói felelősségvállalás mértéke (7.2.4. fejezet) megfelel-e a kívánt célra.

Amennyiben az Érintett fél nem a fent leírtak szerint jár el, a Szolgáltató nem vállal felelősségét az ebből eredő kárért.

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 kötelezettségeik és a rájuk vonatkozó ajánlások be nem tartásával okoznak 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 munkatársai kizárólag a fájlok lenyomatával találkoznak. A Szolgáltató informatikai rendszerét úgy alakította ki, hogy az archivált e-aktákat és fájlokat a rendszer kizárólag az arra jogosult feleknek továbbítja, és kizárólag titkosított formában.

A Szolgáltató a dokumentumokat kizárólag akkor bocsátja harmadik fél rendelkezésére, ha erre az Előfizető felhatalmazta, vagy ha ezt jogszabály írja elő. Ilyenek különösen az Eat. 11. § (2) és (3) bekezdésében, illetve a 3/2005. IHM rendelet 6. § (1) bekezdésében leírt esetek. A Szolgáltató haladéktalanul teljesíti ezen adatszolgáltatást, és a 3/2005. IHM rendelet 6. § (1) szerinti esetben nem köti azt sem díjhoz, sem egyéb feltételhez.

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 Szolgáltató az archiválás szolgáltatás nyújtásához kizárólag a szerződéskötéshez szükséges adatokat tartja nyilván ügyfeleiről, ezen túl nem kezel személyes adatokat. Az Előfizető kérésére – amennyiben ezt jogszabály nem tiltja – a Szolgáltató haladéktalanul törli ezen adatokat nyilvántartásából.

Az adatok bizalmas kezelésére vonatkozó rendelkezéseket a 7.3. fejezet 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 a Szolgáltatási Szabályzat valamely pontja érvénytelen lenne, az a Szolgáltatási Szabályzat egészének és más pontjainak érvényességét nem érinti.

Megszűnés

A Szolgáltatási Szabályzat az 1.4. fejezetben leírt közösség valamennyi kötelezettségét, felelősségét és jogát tartalmazza vagy meghivatkozza. A Szolgáltatási Szabályzat egyetlen pontja sem értelmezhető az abban foglalt értelmezéstől eltérően, bármely más szerződés vagy szabályzat, írott vagy szóbeli kommunikáció következtében, beleértve a Szolgáltató és más szervezet jövőbeli esetleges összeolvadásának esetét is. A Szolgáltatási Szabályzat csak írott és hitelesített formában módosítható, a Hatóság által vezetett szabályzat-nyilvántartásban való átvezetés jelen Szolgáltatási Szabályzatban 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 Előfizető 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 kapcsolatos kérdéseket, kifogásokat és panaszokat az Ügyfélszolgálati iroda címére kell eljuttatni írásos formában. A panaszokat a Szolgáltató 30 napon belül kivizsgálja. Ennek keretében, 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 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 Budai Központi Kerületi bíróság, illetve a Fővárosi Bíróság kizárólagos illetékességének.

7.7. Leírás-adminisztráció

A Szolgáltató működését nyilvános és belső dokumentumai, szabályzatai szabályozzák. 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 Nemzeti Hírközlési 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] 2001. évi XXXV. törvény az elektronikus aláírásról (a 2004. évi módosításokkal).

[2] e-Szignó Hitelesítés Szolgáltató – minősített elektronikus archiválás szolgáltatásra vonatkozó – archiválási rend.

[3] 114/2007. (XII. 29.) GKM rendelet a digitális archiválás szabályairól.

[4] ITU X.509 "Információ technológia - Nyílt rendszerek kapcsolódása - Könyvtár: Nyilvános kulcs és attribútum tanúsítvány keretrendszer" ajánlás 3. verzió.

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

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

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

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

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

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

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

[12] A Nemzeti Hírközlési Hatóság HL2191713/2008 ügyiratszámú határozata az elektronikus aláírással kapcsolatos szolgáltatások nyújtása során alkalmazható biztonságos kriptográfiai algoritmusok és paramétereik meghatározása.

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

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

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

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

[17] Az e-akta formátum specifikációja, v1.0, Microsec Kft. `http://www.e-szigno.hu/?lap=eakta3/`.

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

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

[20] Dublin Core Metadata Element Set, Version 1.1, `http://dublincore.org/documents/2006/12/18/dces/`.

[21] e-Szignó Hitelesítés Szolgáltató – nem elektronikus aláírásra szolgáló tanúsítványok kibocsátására vonatkozó – szolgáltatási szabályzat.

[22] 12/2005. (X. 27.) IHM rendelet az elektronikus ügyintézési eljárásban alkalmazható dokumentumok részletes technikai szabályairól.

[23] Rich Text Format (RTF) Specification, RTF Version 1.7, Microsoft Technical Support, 2001.

[24] PDF Reference, second edition – Adobe Portable Document Format, Version 1.3, Addison-Wesley, ISBN 0-201-61588-6, 2000.

[25] ISO 19005-1:2005 – Document management – Electronic document file format for long-term preservation – Part 1: Use of PDF 1.4 (PDF/A-1).

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

[27] 3/2005. IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről.