e-Szignó Hitelesítés Szolgáltató

eIDAS rendelet szerinti minősített elektronikus archiválási szolgáltatás szolgáltatási szabályzat

ver. 2.0

Hatályba lépés: 2016-07-01

Azonosító	1.3.6.1.4.1.21528.2.1.1.88.2.0
Verzió	2.0
Első verzió hatálybalépése	2006-12-15
Biztonsági besorolás	NYILVÁNOS
Jóváhagyta	Vanczák Gergely
Jóváhagyás dátuma	2016-05-31
Hatálybalépés dátuma	2016-07-01

Microsec Számítástechnikai Fejlesztő zártkörűen működő Részvénytársaság

1031 Budapest, Záhony utca 7. D. épület

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	A fogyasztóvédelem elérhetőségének változása 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
2.0	Cégforma változás. Változás az archivált akták titkosításával kapcsolatban. OID: 1.3.6.1.4.1.21528.2.1.1.18.2.0	2012-05-01	Dr. Berta István Zsolt
2.0	eIDAS követelmények szerinti új archiválási szabályzat új OID azonosítóval. OID: 1.3.6.1.4.1.21528.2.1.1.88.2.0	2016-07-01	Dr. Szőke Sándor

Tartalomjegyzék

1. Bevezetés

Jelen dokumentum a Microsec Számítástechnikai Fejlesztő zrt. (továbbiakban: Microsec vagy *Minősített archiválási szolgáltató*) által üzemeltetett e-Szignó Hitelesítés Szolgáltató *minősített archiválási* szolgáltatásra vonatkozó *Minősített archiválási szolgáltatási szabályzat*a.

A *Minősített archiválási szolgáltató* szolgáltatásait a vele szerződéses viszonyban álló *Ügyfel*ek részére biztosítja.

Jelen *Minősített archiválási szolgáltatási szabályzat* a fenti szolgáltatások nyújtásának kereteit, a részletes eljárási és egyéb működési szabályokat tartalmazza.

A *Minősített archiválási szolgáltatási szabályzat* megfelel az eIDAS rendelet [1] által támasztott követelményeknek, az ezen szabályoknak megfelelően nyújtott szolgáltatás a rendelet szerinti EU minősített bizalmi szolgáltatás. A minősített bizalmi szolgáltatás nyújtásának és az "EU Trust Mark" feltüntetésének előfeltétele, hogy:

- a szolgáltatást vizsgálja meg egy eIDAS rendelet szerinti akkreditált független vizsgáló labor, a sikeres vizsgálatról állítson ki egy megfelelőségértékelési jelentést és egy tanúsítványt a *Minősített archiválási szolgáltató* részére;
- a *Minősített archiválási szolgáltató* nyújtsa be a megfelelőségértékelésről szóló tanúsítványt a Nemzeti Média- és Hírközlési Hatóságnak, mint ellenőrző hatósági szervezetnek;
- a Nemzeti Média- és Hírközlési Hatóság fogadja el a benyújtott megfelelőségértékelési tanúsítványt és jelentesse meg a szolgáltatást a nemzeti bizalmi listában.

1.1. Áttekintés

Jelen *Minősített archiválási szolgáltatási szabályzat* célja, hogy összefoglalja mindazokat az információkat, amelyeket a *Minősített archiválási szolgáltató*val kapcsolatba kerülő *Ügyfel*eknek tudniuk érdemes. Ezzel elő kívánja segíteni, hogy:

- *Ügyfel*ei és leendő *Ügyfel*ei minél könnyebben megismerhessék a *Minősített archiválási szolgáltató* által kínált szolgáltatások részleteit, feltételeit és a szolgáltatás nyújtásának gyakorlati hátterét;
- átláthassák a *Minősített archiválási szolgáltató* működését, és ennek révén minél könnyebben eldönthessék, hogy a szolgáltatások megfelelnek-e, illetve az egyes szolgáltatások melyik típusa felel meg igényeiknek, elvárásaiknak.

A végfelhasználóknak az igénybe vett szolgáltatással kapcsolatos tevékenységére vonatkozó előírásokat jelen *Minősített archiválási szolgáltatási szabályzat*on kívül a *Minősített archiválási rend*, az Általános szerződési feltételek, a szolgáltatóval kötött Szolgáltatási szerződés,

a *Minősített archiválási szolgáltató* által alkalmazott *Hitelesítési rend*ek (lásd: 1.2.1. fejezet), az *Időbélyegzési rend* [34] illetve egyéb, a *Minősített archiválási szolgáltató*tól független szabályzat illetve dokumentum is tartalmazhat.

1.2. Dokumentum neve és azonosítója

Kibocsátó	e-Szignó Hitelesítés Szolgáltató
Dokumentum címe	eIDAS rendelet szerinti minősített elektronikus archiválási szolgáltatás szolgáltatási szabályzat
Dokumentum verziószáma	2.0
Hatályba lépés ideje	2016-07-01

1.2.1. Archiválási rend

A *Minősített archiválási rend*et azonosító OID első hét száma a Microsec egyedi azonosítója az alábbiak szerint:

(1)	International Organization for Standardization (ISO)	Nemzetközi Szabványügyi Szervezet (ISO)
(3)	Organization identification schemes registered according to ISO/IEC 6523-2	Az ISO/IEC 6523-2 szerint regisztrált szervezeti azonosító rendszer
(6)	United States Department of Defense (DoD)	Amerikai Védelmi Minisztérium (DoD)
(1)	Internet	Internet
(4)	Private projects	Magán projektek
(1)	Private enterprises	Magán vállalatok
(21528)	MICROSEC Ltd.	Microsec zrt.

A további számok rendszerét a Microsec saját hatáskörben osztotta ki, értelmezésük az alábbiak szerinti:

(1.3.6.1.4.1.21528)	MICROSEC Ltd.
(2)	e-Szignó Hitelesítés Szolgáltató
(1)	dokumentumok
(1)	nyilvános dokumentumok
(x)	dokumentum egyedi azonosító sorszáma
(y)	dokumentum verziója
(z)	dokumentum alverziója

A jelen *Minősített archiválási szolgáltatási szabályzat* szerint nyújtott szolgáltatás megfelel az alábbi *Minősített archiválási rend* követelményeinek:

OID	MEGNEVEZÉS	RÖVID NÉV
1.3.6.1.4.1.21528.2.1.1.87.2.0	eIDAS rendelet szerinti minősített archiválási rend.	MAR

A felsorolt *Minősített archiválási rend*(ek) részletes követelményeit az " e-Szignó Hitelesítés Szolgáltató – eIDAS szerinti minősített elektronikus archiválási rend ver.2.0." [32] dokumentum tartalmazza.

1.2.2. Hatály

Tárgyi hatály

A *Minősített archiválási szolgáltatási szabályzat* az 1.3.1. fejezetben ismertetett szolgáltatások nyújtására és igénybevételére vonatkozik.

Időbeli hatály

A *Minősített archiválási szolgáltatási szabályzat* jelen verziója 2016-07-01-i hatálybalépési dátumtól visszavonásig hatályos. A hatályosság automatikusan megszűnik a szolgáltatások beszüntetésekor.

Személyi hatály

A *Minősített archiválási szolgáltatási szabályzat* személyi hatálya kiterjed az 1.3. alfejezetben azonosított közösség minden tagjára.

Területi hatály

A jelen *Minősített archiválási szolgáltatási szabályzat* a magyar jog alapján Magyarországon, elsősorban magyar *Ügyfel*ek részére, magyar nyelven nyújtott szolgáltatásokra vonatkozó konkrét követelményeket tartalmaz. A *Minősített archiválási szolgáltató* kiterjesztheti a szolgáltatás területi hatályát, ez esetben a magyar viszonyokra alkalmazható előírásoknak megfelelő, azoknál nem enyhébb követelményeket alkalmaz.

A jelen *Minősített archiválási szolgáltatási szabályzat* szerint nyújtott szolgáltatás az egész világon elérhető. A jelen *Minősített archiválási szolgáltatási 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 jelen *Minősített archiválási szolgáltatási szabályzat* szerint nyújtott szolgáltatás kizárólag a jelen dokumentumban, valamint a *Archiválási rend*ben leírtak szerint használható fel.

1.3. PKI szereplők

1.3.1. A Szolgáltató

A Szolgáltató adatai

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

Az ügyfélszolgálati iroda elérhetősége:

A szolgáltató egység neve:	e-Szignó Hitelesítés Szolgáltató
Ügyfélszolgálati iroda:	1031 Budapest, Záhony u. 7., Graphisoft Park, D épület
Ügyfélszolgálati iroda nyitvatartási ideje:	munkanapokon 8:30-16:30 között előzetes időpont egyeztetés alapján
Ügyfélszolgálati iroda telefonszáma:	(+36-1) 505-4444
Ügyfélszolgálati iroda e-mail címe:	`info@e-szigno.hu`
A szolgáltatással kapcsolatos információk elérése:	`https://www.e-szigno.hu`
Panaszok bejelentésének helye:	Microsec zrt. 1031 Budapest, Záhony u. 7., Graphisoft Park, D épület
Illetékes fogyasztóvédelmi felügyelőség:	Budapest Főváros Kormányhivatal Fogyasztóvédelmi Felügyelőség 1052 Budapest, Városház u. 7. 1364 Budapest, Pf. 144.

A Szolgáltató bemutatása

A Microsec zrt. a 910/2014/EU rendelet [1] (továbbiakban: eIDAS) szerinti EU minősített bizalmi szolgáltató.

A Microsec zrt. (illetve jogelődje, a Microsec Kft.) az elektronikus aláírással kapcsolatos szolgáltatásainak nyújtását a 2001. évi XXXV. törvény [2] (továbbiakban: Eat.) hatálya alatt indította el:

- 2002. május 30-tól kezdve nyújt az Eat. szerinti nem minősített elektronikus aláírás hitelesítés-szolgáltatást, időbélyegzés szolgáltatást és aláírás-létrehozó adat elhelyezése aláírás-létrehozó eszközön szolgáltatást (regisztrációs szám: MH 6834 1/2002);
- 2005. május 15-től kezdve nyújt az Eat. szerinti minősített hitelesítés-szolgáltatást, időbélyegzés szolgáltatást és aláírás-létrehozó adat elhelyezése aláírás-létrehozó eszközön szolgáltatást;
- 2007. február 1-től kezdve nyújt az Eat. szerinti minősített elektronikus archiválás szolgáltatást (a nyilvántartásba vételről szóló határozat ügyiratszáma: HL-3549- 2/2007).

2016. július 1-én az eIDAS és az azt kiegészítő 2015. évi CCXXII törvény [5] hatályba lépésével európai szinten egységesen megváltozott az elektronikus aláírással kapcsolatos szolgáltatások teljes rendszere. A Microsec folyamatosan állítja át szolgáltatásait az új eIDAS követelményrendszer szerint.

2016. július 1-től:

- elindítja természetes személyek számára az eIDAS rendelet szerinti minősített aláíró tanúsítványok kibocsátását;
- elindítja az eIDAS rendelet szerinti nem minősített aláíró, bélyegző és weboldal-hitelesítő tanúsítványok kibocsátását;
- az átmeneti rendelkezéseknek megfelelően a végső eIDAS tanúsítvány megszerzéséig nemzeti minősített szinten nyújtja a szervezetek számára aláíró tanúsítványok kibocsátását, az időbélyegzés és archiválás szolgáltatásokat.

Minőség és információbiztonság

A Microsec kiemelten fontosnak tartja *Ügyfel*ei elégedettségét. A magas színvonalú szolgáltatások fenntartása érdekében a *Minősített archiválási szolgáltató* ISO 9001 szabványnak megfelelő minőségirányítási rendszert üzemeltet 2002. január 23. óta. A szabványnak való megfelelést a Lloyd's Register Quality Assurance tanúsította.

A Microsec nagy figyelmet fordít az általa üzemeltetett rendszerek biztonságára, ezért fő tevékenységi területein a ISO/IEC 27001-nek megfelelő információbiztonság-irányítási rendszert (korábban BS 7799) üzemeltet 2003. május 19. óta. A szabványnak való megfelelést a Lloyd's Register Quality Assurance tanúsította.

Szolgáltatások

A *Minősített archiválási szolgáltató* az eIDAS rendelet [1] által meghatározott alábbi bizalmi szolgáltatásokat nyújthatja az *Előfizető* számára jelen *Minősített archiválási szolgáltatási szabályzat* keretében:

- minősített archiválási szolgáltatás

A *Minősített archiválási szolgáltató* a szolgáltatásokat jelen *Minősített archiválási szolgáltatási szabályzat* keretében minősített bizalmi szolgáltatóként nyújtja.

1.3.2. Ügyfelek

A *Minősített archiválási szolgáltató* által nyújtott szolgáltatások *Ügyfel*ei:

- *Előfizető*:
  - Szolgáltatási szerződést köt a *Minősített archiválási szolgáltató*val,
  - meghatározza a felhasználók körét,
  - felelős a szolgáltatás igénybevételével kapcsolatos díjak megfizetéséért.

1.3.3. Érintett felek

Az *Érintett fél* nem feltétlenül áll szerződéses viszonyban a *Minősített archiválási szolgáltató*val. A tevékenységére vonatkozó ajánlásokat a *Minősített archiválási szolgáltatási szabályzat* 8.6.3 és 8.9.3 fejezetei és az abban megnevezett egyéb szabályzatok tartalmazzák.

Az archiválás szolgáltatás során kibocsátott igazolásokat befogadó illetve felhasználó fél.

1.4. A dokumentum adminisztrálása

1.4.1. A dokumentum adminisztrációs szervezete

Jelen *Minősített archiválási szolgáltatási szabályzat* adminisztrációját ellátó szervezet adatai az alábbi táblázatban találhatók:

Szervezet neve	Microsec e-Szignó Hitelesítés Szolgáltató
Szervezet címe	Magyarország, H-1037 Budapest, Záhony utca 7. D épület

Telefonszám	+36 1 505-4444
Fax szám	+36 1 505-4445
E-mail cím	info@e-szigno.hu

1.4.2. Kapcsolattartó személy

Jelen *Minősített archiválási szolgáltatási szabályzat*tal kapcsolatos kérdésekben közvetlenül az alábbi személyhez lehet fordulni:

Kapcsolattartó	Folyamatszervezés részleg vezetője
Szervezet neve	Microsec zrt.
Szervezet címe	Magyarország, H-1037 Budapest, Záhony utca 7. D épület
Telefonszám	+36 1 505-4444
Fax szám	+36 1 505-4445
E-mail cím	info@e-szigno.hu

1.4.3. A Szolgáltatási szabályzat *Minősített archiválási rend*nek való megfelelőségéért felelős személy/szervezet

Egy *Minősített archiválási szolgáltatási szabályzat*nak a benne meghivatkozott *Minősített archiválási rend*nek való megfelelőségéért és az abban foglaltak szerinti szolgáltatás nyújtásáért az adott *Minősített archiválási szolgáltatási szabályzat*ot kibocsátó szolgáltató a felelős.

A *Minősített archiválási szolgáltatási szabályzat*ok és a szolgáltatások nyújtása feletti felügyeletet a Nemzeti Média- és Hírközlési Hatóság látja el. A Nemzeti Média- és Hírközlési Hatóság nyilvántartást vezet a követelményeknek megfelelő *Minősített archiválási rend*ekről valamint az ezeket alkalmazó *Minősített archiválási szolgáltató*król. A Nemzeti Média- és Hírközlési Hatóság a megfelelőség vizsgálatakor független megfelelőségértékelő szervezet megállapításaira támaszkodik.

1.4.4. A Szolgáltatási szabályzat elfogadási eljárása

A *Minősített archiválási szolgáltatási szabályzat* új verziójának illetve tetszőleges módosításának megírása, elfogadása és kibocsátása egységes folyamatok szerint – a 8.12.1 fejezetben részletezett módon – történik.

1.5. Fogalmak és rövidítések

1.5.1. Fogalmak

Adatközpont	Számítógépes rendszerek és a hozzájuk kapcsolódó komponensek elhelyezésére és üzemeltetésére kialakított létesítmény. Ezek a komponensek rendszerint magukba foglalják a távközlési rendszereket és kommunikációs kapcsolatokat, redundáns áramforrást, adattárolókat, légkondicionáló, tűzvédelmi és biztonsági rendszereket.
Bizalmi felügyelet	"A *Bizalmi szolgáltatás*ok felügyeletét ellátó hatóság a Nemzeti Média- és Hírközlési Hatóság." (2015. évi CCXXII. törvény [5] 91.§ 1. bekezdés)
Bizalmi szolgáltatás (Trust Service)	"Rendszerint díjazás ellenében nyújtott, az alábbiakból álló elektronikus szolgáltatások: • elektronikus aláírások, elektronikus bélyegzők vagy elektronikus időbélyegzők, ajánlott elektronikus kézbesítési szolgáltatások, valamint az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok létrehozása, ellenőrzése és érvényesítése; vagy • *Weboldal-hitelesítő tanúsítvány*ok létrehozása, ellenőrzése és érvényesítése; vagy • elektronikus aláírások, bélyegzők vagy az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok megőrzése; " (eIDAS [1] 3. cikk 16. pont)
Bizalmi szolgáltatási rend (Trust Service Policy)	"Olyan szabálygyűjtemény, amelyben egy *Bizalmi szolgáltató*, igénybe vevő vagy más személy valamely *Bizalmi szolgáltatás* használatának feltételeit írja elő igénybe vevők valamely közös biztonsági követelményekkel rendelkező csoportja vagy meghatározott alkalmazások számára. " (2015. évi CCXXII. törvény [5] 1. § 8. pont)

Bizalmi szolgáltató (Trust Service Provider)	"Egy vagy több *Bizalmi szolgáltatás*t nyújtó természetes vagy jogi személy; a *Bizalmi szolgáltató* lehet minősített vagy nem minősített *Bizalmi szolgáltató*." (eIDAS [1] 3. cikk 19. pont)
E-akta	Az elektronikus akta (e-akta) egy elektronikus aláírás konténer formátum. Egy e-akta dokumentumokat, illetve hozzájuk kapcsolódó profilokat (metaadatokat), aláírásokat, ellenjegyzéseket és időbélyegeket tartalmazhat.
Elektronikus dokumentum	"Elektronikus formában, különösen szöveg, hang-, képi vagy audiovizuális felvétel formájában tárolt bármilyen tartalom." (eIDAS [1] 3. cikk 35. pont)
Elektronikus időbélyegző (Electronic Time Stamp)	"Olyan elektronikus adatok, amelyek más elektronikus adatokat egy adott időponthoz kötnek, amivel igazolják, hogy utóbbi adatok léteztek az adott időpontban. " (eIDAS [1] 3. cikk 33. pont)
Előfizető (Subscriber)	A Szolgáltatóval valamely szolgáltatás igénybevétele érdekében Szolgáltatási szerződést kötő személy vagy szervezet.
Fájl	Általános értelemben olyan logikailag összetartozó adatállomány, amelyet egy elektronikus dokumentumban tárolunk és amely egy adott formátumban értelmezve egy meghatározott jelentés tartalommal (tipikusan szöveg, kép, hang, video ...) bír. A fájl fogalmát a jelen *Minősített archiválási szolgáltatási szabályzat*ban szűkebb értelemben, kizárólag az e-aktákban elhelyezett elektronikus dokumentumok megjelölésére használjuk.
Felfüggesztés	A *Tanúsítvány* érvényességének ideiglenes megszüntetése a *Tanúsítvány*ban is feltüntetett érvényességi idő lejárta előtt. A *Tanúsítvány* felfüggesztése nem végleges, a felfüggesztett *Tanúsítvány* érvényessége visszaállítható.

Gyökér tanúsítvány (Root Certificate)	Más néven legfelső szintű tanúsítvány. Önhitelesített *Tanúsítvány*, amelyet adott *Hitelesítő egység* saját maga számára bocsátott ki, azaz saját magánkulcsával van aláírva, így a saját – a tanúsítványban szereplő – nyilvános kulcsával ellenőrizhető.
Hardver kriptográfiai eszköz (HSM: Hardware Security Module)	Egy olyan hardver alapú biztonságos eszköz, mely előállítja, tárolja és védi a kriptográfiai kulcsokat, valamint biztonságos környezetet biztosít a kriptográfiai funkciók végrehajtására.
Hitelesítés-szolgáltató	Olyan *Bizalmi szolgáltató*, aki/amely a hitelesítés-szolgáltatás keretében azonosítja az igénylő személyét, *Tanúsítvány*t bocsát ki, nyilvántartásokat vezet, fogadja a *Tanúsítvány*okkal kapcsolatos változások adatait, valamint nyilvánosságra hozza a *Tanúsítvány*hoz tartozó szabályzatokat, és a *Tanúsítvány* aktuális állapotára (különösen esetleges visszavonására) vonatkozó információkat.
Hitelesítő egység	A *Hitelesítés-szolgáltató* rendszerének egy egysége, amely *Tanúsítvány*ok digitális aláírását végzi. Egy *Hitelesítő egység*hez mindig egy elektronikus aláírás vagy bélyegző létrehozásához használt adat (magánkulcs) tartozik. Előfordulhat, hogy egy *Hitelesítés-szolgáltató* egyszerre több *Hitelesítő egység*et is működtet.
Kompromittálódás	Egy kriptográfiai kulcs akkor kompromittálódott, ha illetéktelen személyek is hozzáférhettek.
Köztes hitelesítő egység	Olyan *Hitelesítő egység* amelynek *Tanúsítvány*át egy másik *Hitelesítő egység* bocsátotta ki.
Kriptográfiai kulcs (Key)	Olyan kriptográfiai transzformációt vezérlő egyedi digitális jelsorozat, amelynek ismerete titkosításhoz és dekódoláshoz, illetve digitális aláírás előállításához és ellenőrzéséhez szükséges.

Kulcsgondozás (Key Management)	A kriptográfiai kulcsok előállítása, a felhasználókhoz történő eljuttatása vagy ennek algoritmikus megvalósítása, továbbá a kulcsok nyilvántartása, tárolása, archiválása, visszavonása, törlése, amely szoros kapcsolatban áll az alkalmazott biztonsági eljárásmóddal.
Magánkulcs	A Nyilvános kulcsú infrastruktúrában egy szereplőhöz tartozó aszimmetrikus kriptográfiai kulcspár azon eleme, amelyet az *Alany*nak szigorúan titokban kell tartania. A *Hitelesítés-szolgáltató* a *Tanúsítvány*ok kibocsátása során a *Hitelesítő egység* magánkulcsát használja arra, hogy a *Tanúsítvány*t védő elektronikus aláírást vagy bélyegzőt elhelyezze rajta.
Minősített bizalmi szolgáltatás (Qualified Trust Service)	"Olyan *Bizalmi szolgáltatás* amely megfelel az eIDAS rendeletben foglalt alkalmazandó követelményeknek." (eIDAS [1] 3. cikk 17. pont)
Minősített bizalmi szolgáltató (Qualified Trust Service Provider)	"Olyan *Bizalmi szolgáltató* amely egy vagy több *Minősített bizalmi szolgáltatás*t nyújt, és amelynek minősített státusát a felügyeleti szerv jóváhagyta. " (eIDAS [1] 3. cikk 20. pont)
Nyilvános kulcs	A Nyilvános kulcsú infrastruktúrában egy szereplőhöz tartozó aszimmetrikus kriptográfiai kulcspár azon eleme, amelyet nyilvánosságra kell hozni. A nyilvánosságra hozatal jellemzően egy *Tanúsítvány* formájában történik, amely összekapcsolja a szereplő nevét az ő nyilvános kulcsával. A *Tanúsítvány*ok hitelességét az őket kibocsátó *Hitelesítő egység* nyilvános kulcsa segítségével lehet ellenőrizni.
Nyilvános kulcsú infrastruktúra (Public Key Infrastructure, PKI)	Aszimmetrikus kulcsú kriptográfiára épülő infrastruktúra, beleértve a kriptográfiai algoritmusokat, kulcsokat, tanúsítványokat, a rájuk vonatkozó szabványokat és jogszabályokat, a mögöttes intézményrendszert, a különböző szolgáltatókat és eszközöket is.
Nyílt e-akta	Olyan e-akta, amely kódolatlan fájlokat, és rajta lévő elektronikus aláírásokat, elektronikus bélyegzőket tartalmaz. A nyílt e-akta az aláírt, bélyegzett fájlokat és az aláírásokat, bélyegzőket egyaránt nyíltan tartalmazza.

Rendkívüli üzemeltetési helyzet	Olyan, a *Minősített archiválási szolgáltató* üzemmenetében zavart okozó rendkívüli helyzet, amikor a *Minősített archiválási szolgáltató* rendes üzemmenetének folytatására ideiglenesen vagy véglegesen nincsen lehetőség.
Szervezet	Jogi személy.
Szolgáltatási szabályzat (Trust Service Practice Statement)	"A *Bizalmi szolgáltató* nyilatkozata az egyes *Bizalmi szolgáltatás*ok nyújtásával kapcsolatosan alkalmazott részletes eljárási vagy más működési követelményekről. " (2015. évi CCXXII. törvény [5] 1. § 41. pont)
Szolgáltatási szerződés	"A *Bizalmi szolgáltató* és a *Bizalmi szolgáltatás*i ügyfél között létrejött szerződés, amely a *Bizalmi szolgáltatás* nyújtására és a szolgáltatás igénybevételére vonatkozó feltételeket tartalmazza. " (2015. évi CCXXII. törvény [5] 1. § 42. pont)
Tanúsítvány (Certificate)	"Az elektronikus aláírás tanúsítvány, az elektronikus bélyegző tanúsítvány és a *Weboldal-hitelesítő tanúsítvány*, valamint mindazon, a *Bizalmi szolgáltatás* keretében a szolgáltató által kibocsátott elektronikus igazolás, amely tartalmazza a tanúsítványra vonatkozó érvényesítési adatot és a tanúsítvány használatához szükséges kapcsolódó adatokat, és amely elektronikus dokumentum megbízhatóan védve van a kibocsátáskor és az érvényességi ideje alatt rendelkezésre álló technológiákkal elkövetett hamisítás ellen. " (2015. évi CCXXII. törvény [5] 1. § 44.)
Tanúsítványtár	Különböző *Tanúsítvány*okat tartalmazó adattár. Tanúsítványtára van egy Szolgáltatónak is, amelyben az általa kibocsátott *Tanúsítvány*okat publikálja, de Tanúsítványtárnak nevezzük az *Érintett fél* számítógépén a használt alkalmazás számára elérhető *Tanúsítvány*okat tartalmazó rendszert is.

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.
Ügyfél	Az *Előfizető* és a szolgáltatás igénybe vevői, akik részére az Előfizető használati jogosultságot ad.
Visszavonás	A *Tanúsítvány* érvényességének megszüntetése a *Tanúsítvány*ban is feltüntetett érvényességi idő lejárta előtt. A *Tanúsítvány* visszavonása végleges, visszavont *Tanúsítvány* többet nem tehető érvényessé.
Visszavonási állapot nyilvántartás	A *Hitelesítés-szolgáltató* által vezetett nyilvántartás a felfüggesztett, illetőleg a visszavont *Tanúsítvány*okról, amelyek tartalmazzák legalább a felfüggesztés vagy visszavonás tényét, és a felfüggesztés vagy visszavonás időpontját.

1.5.2. Rövidítések

CRL	(Certificate Revocation List)	Tanúsítvány visszavonási lista
eIDAS	(electronic Identification, Authentication and Signature)	A 910/2014/EU rendelet általánosan használt hivatkozása
LDAP	(Lightweight Directory Access Protocol)	Protokoll címtár szolgáltatás eléréséhez
NMHH		Nemzeti Média- és Hírközlési Hatóság
OCSP	(Online Certificate Status Protocol)	Online tanúsítvány-állapot protokoll
OID	(Object Identifier)	Objektum azonosító
PKI	(Public Key Infrastructure)	Nyilvános kulcsú infrastruktúra
TSP	(Trust Service Provider)	Bizalmi szolgáltató

2. Közzététel és tanúsítványtár

2.1. Adatbázisok - tanúsítványtárak

A *Minősített archiválási szolgáltató* publikálja a működése alapjául szolgáló *Minősített archiválási rend*et, *Minősített archiválási szolgáltatási szabályzat*ot valamint a szerződési feltételeket tartalmazó egyéb dokumentumokat.

2.2. Az információ közzététele

2.2.1. Szolgáltatói információ közzététele

A *Minősített archiválási szolgáltató* nyilvánosságra hozza szerződéses feltételeit és szabályzatait a honlapján elektronikus formában.

A honlapon legalább 30 nappal a hatálybalépés előtt publikálásra kerülnek a bevezetésre váró új dokumentumok.

A honlapon az érvényben levő dokumentumokon kívül elérhető valamennyi dokumentum összes korábbi verziója is.

A szabályzatok és szerződési feltételek aktuális verziója nyomtatott formában olvasható a *Minősített archiválási szolgáltató* ügyfélszolgálati irodájában.

A *Minősített archiválási szolgáltató* a szerződéskötést követően tartós adathordozón bocsátja az *Ügyfél* rendelkezésére a *Minősített archiválási rend*et, a *Minősített archiválási szolgáltatási szabályzat*ot és a Szolgáltatási szerződést.

A *Minősített archiválási szolgáltató* értesíti *Ügyfel*eit az Általános szerződési feltételek változásáról.

2.3. A közzététel időpontja vagy gyakorisága

2.3.1. Kikötések és feltételek közzétételi gyakorisága

A *Minősített archiválási szolgáltatási szabályzat*tal kapcsolatos új verziók közzététele a 8.12. fejezetben ismertetett eljárásoknak megfelelően történik.

A *Minősített archiválási szolgáltató* szükség szerint hozza nyilvánosságra egyéb szabályzatait, szerződéses feltételeit, illetve azok újabb változatait.

A *Minősített archiválási szolgáltató* a rendkívüli információkat a jogszabályi előírásoknak megfelelően közzéteszi, külön rendelkezés hiányában pedig késedelem nélkül.

3. Elektronikus archiválási szolgáltatás

A *Minősített archiválási szolgáltató* a Szolgáltatási szerződés keretében az eIDAS szerinti minősített bizalmi szolgáltatóként nyújtja az elektronikus archiválási szolgáltatást az *Előfizető* részére. A szolgáltatás az alábbi főbb szolgáltatási elemeket tartalmazza:

- Az *Előfizető* elektronikus aktába (e-akta) foglalt elektronikusan aláírt elektronikus dokumentumokat (fájlokat) tölthet fel a *Minősített archiválási szolgáltató* által üzemeltetett

archívumba. Az e-akta befogadása során a *Minősített archiválási szolgáltató* ellenőrzi az e-aktán illetve az e-aktába foglalt fájlokon található elektronikus aláírás(oka)t vagy bélyegző(ke)t, kiegészíti vagy összeállítja az érvényességi lánco(ka)t, minden érvényességi láncon minősített elektronikus archív *Időbélyegző*t helyez el, majd eltárolja a befogadott e-aktát. (lásd 3.2. fejezet).

- A *Minősített archiválási szolgáltató* a befogadott e-aktákat – a benne foglalt fájlokat és érvényességi láncokat – biztonságosan tárolja és a tárolás teljes ideje alatt biztosítja, hogy
  - a tárolt adatokhoz kizárólag az arra jogosultak férhessenek hozzá;
  - a tárolt adatokhoz az arra jogosult *Előfizető* folyamatosan hozzáférjen;
  - a tárolt adatokat jogosulatlanul nem lehet módosítani, törölni.
- A *Minősített archiválási szolgáltató* gondoskodik az e-aktákon illetve az e-aktákban tárolt fájlokon elhelyezett elektronikus aláírások illetve bélyegzők hosszú távú érvényességének biztosításáról. A *Minősített archiválási szolgáltató* a megőrzés ideje alatt biztosítja az e-akták és meghatározott fájl formátumok esetén a bennük szereplő fájlok hosszú távú olvashatóságát. A megőrzési idő 50 év, kivéve ha a Szolgáltatási szerződés érvényessége ezen időtartam letelte előtt szűnik meg. (a részleteket lásd a 4. fejezetben).
- Az *Előfizető* a Szerződés időtartama alatt folyamatosan elérheti a *Minősített archiválási szolgáltató* archívumában az általa ott elhelyezett e-aktákat, elektronikus dokumentumokat, aláírásokat, bélyegzőket, illetve a hozzájuk tartozó érvényességi láncokat és azokat onnan letöltheti (lásd: 3.3).
- Az *Előfizető* kérésére a *Minősített archiválási szolgáltató* hiteles igazolást bocsát ki arról, hogy az egyes e-aktákat tárolja, és az e-aktán illetve az e-aktában tárolt egyes dokumentumokon az archívumba helyezés időpontjában érvényes elektronikus aláírás vagy bélyegző szerepelt (lásd: 3.4. fejezet).
- Az *Előfizető* kérésére a *Minősített archiválási szolgáltató* törli az e-aktákat az archívumából (lásd: 3.6. fejezet).

A *Minősített archiválási szolgáltató* minden esetben eltárolja az elektronikus aláírással vagy bélyegzővel ellátott elektronikus dokumentumot is, nem nyújtja az archiválási szolgáltatásnak a dokumentum tárolása nélküli változatát. Ez természetesen nem zárja ki, hogy az *Előfizető* a *Minősített archiválási szolgáltató*nak átadni bármilyen okból nem kívánt elektronikus dokumentumról maga készítsen egy kellően biztonságos lenyomatot és azt töltse fel egy e-aktában foglalt elektronikus dokumentumként az archívumba. Ilyen esetben az *Előfizető*nek kell gondoskodnia a megőrzés megújításáról például a használt lenyomatképző algoritmus ellenállóképességének gyengülése esetén.

A *Minősített archiválási szolgáltató* egyes meghatározott fájlformátumok esetén vállalja az archívumban tárolt elektronikus dokumentumok értelmezhetőségének, megjelenítésének biztosítását is.

A *Minősített archiválási szolgáltató* jelen szolgáltatás keretében elektronikus aláírások illetve bélyegzők érvényességének hosszú távú megőrzésével foglalkozik, így kizárólag csak a befogadás időpontjában érvényes elektronikus aláírással vagy bélyegzővel ellátott elektronikus dokumentumokat fogad be.

A *Minősített archiválási szolgáltató* csak olyan elektronikus aláírással illetve bélyegzővel ellátott elektronikus dokumentumokat fogad be, amelyek formátuma megfelel az ETSI EN 319 132-1 [10] előírásainak és található rajta *Időbélyegző*.

Az elektronikus aláírás vagy bélyegző létrehozásához használt *Tanúsítvány* és az *Időbélyegző*t kibocsátó egység *Tanúsítvány*a visszavezethető kell legyen egy a *Minősített archiválási szolgáltató* által megbízhatónak tekintett gyökér vagy szolgáltatói köztes *Tanúsítvány*ra.

Az archiválás időtartamát az *Előfizető* és a *Minősített archiválási szolgáltató* között kötendő Szolgáltatási szerződés határozza meg. A *Minősített archiválási szolgáltató* hosszú, akár 50-100 éves megőrzési időtartamra is vállal megbízást.

A *Minősített archiválási szolgáltató* a 4.8 fejezetben felsorolt formátumú fájlok hosszú távú olvashatóságát biztosítja az ott meghatározott módon, az ott leírt feltételek szerint.

3.1. Szolgáltatási szerződés kötése

A szolgáltatás igénybevétele előtt az *Előfizető*nek Szolgáltatási szerződést kell kötnie a *Minősített archiválási szolgáltató*val.

A *Minősített archiválási szolgáltatási szabályzat* illetve az abban hivatkozott egyéb szabályzatok egyértelműen meghatározzák a nyújtandó szolgáltatás részleteit, az igénybevételhez szükséges eszközöket.

A Szolgáltatási szerződés megkötésének folyamata:

1. Az *Előfizető* kapcsolatba lép a *Minősített archiválási szolgáltató* ügyfélszolgálati irodájával.
2. A *Minősített archiválási szolgáltató* ügyfélszolgálata tájékoztatást ad az elektronikus archiválás szolgáltatás jellemzőiről és a szolgáltatás megrendelésének módjáról. Az *Előfizető* a *Minősített archiválási szolgáltató* honlapján található információ alapján is tájékozódhat az elektronikus archiválás szolgáltatás felhasználásának módjáról, biztonsági fokáról, szolgáltatási szabályzatáról, a szerződés feltételeiről, valamint az alkalmazandó adatvédelmi szabályokról. Ezt a *Minősített archiválási szolgáltató* honlapján megtalálható Általános szerződési feltételek [35], *Minősített archiválási rend* [32], jelen *Minősített archiválási szolgáltatási szabályzat* [33], illetve a *Minősített archiválási szolgáltató* által készített ügyfél-tájékoztató dokumentum alapján teheti meg.

3. A *Minősített archiválási szolgáltató* a szerződéskötést megelőzően tájékoztatja az *Előfizető*t a *Minősített archiválási szolgáltatási szabályzat* elérhetőségéről és tartalmáról.

4. A Szolgáltatási szerződés megköthető írásban, papíralapon vagy elektronikus formában, legalább fokozott biztonságú elektronikus aláírással vagy bélyegzővel hitelesítve és minősített *Időbélyegző*vel ellátva.

5. A szolgáltatás igénybevételéhez az *Előfizető*nek szüksége van titkosító és autentikációs *Tanúsítvány*ra, amelyet részére az e-Szignó Hitelesítés Szolgáltató külön szolgáltatási szerződés keretében biztosíthat. A *Minősített archiválási szolgáltató* előírhatja, hogy más szolgáltató által kibocsátott titkosító illetve autentikációs *Tanúsítvány*ok esetén milyen feltételekkel nyújtja a szolgáltatást.

3.2. Dokumentum feltöltése

A *Minősített archiválási szolgáltató* kizárólag az *Előfizető* azonosságának megállapítása után, biztonságos eljárás keretében fogad be archiválandó e-aktákat. Az eljárás biztosítja az e-akták integritásának, bizalmasságának megőrzését.

A feltöltés tipikusan Interneten keresztül történik a *Minősített archiválási szolgáltató* által biztosított felület felhasználásával az alábbiak szerint:

1. Az *Előfizető* a kliens autentikációs *Tanúsítvány*a felhasználásával kölcsönös azonosításon alapuló TLS kapcsolatot létesít a *Minősített archiválási szolgáltató*val. A *Minősített archiválási szolgáltató* az *Előfizető*t az TLS kapcsolat felépítéséhez használt kliens autentikációs *Tanúsítvány*a alapján azonosítja. Az *Előfizető* az TLS kapcsolaton keresztül tölthet fel dokumentumokat a *Minősített archiválási szolgáltató* archívumába. Az *Előfizető* Dublin Core szerinti [24] metaadatokat is megadhat az egyes dokumentumokkal kapcsolatban. A metaadatokat elhelyezheti e-aktában is, de feltöltéskor is megadhatja őket.

2. A *Minősített archiválási szolgáltató* ellenőrzi, hogy a feltöltött e-akta megfelelő formátumú-e, azaz megfelel-e a *Minősített archiválási szolgáltató* honlapján közzétett e-akta specifikációnak [25]. A feltöltött e-akta egy vagy több elektronikus dokumentumot is tartalmazhat. Az e-akta tartalmazhat az egyes elektronikus dokumentumokon lévő aláírást vagy bélyegzőt, de lehet benne ún. keretaláírás is, amely az e-aktában lévő minden dokumentum, és a dokumentumokon lévő összes aláírás, bélyegző és *Időbélyegző* integritását biztosítja. Ha az e-akta tartalmaz keretaláírást, akkor a *Minősített archiválási szolgáltató* kizárólag a keretaláírásokat ellenőrzi (a belső aláírásokat, bélyegzőket nem). Ha az e-akta nem tartalmaz keretaláírást, akkor a *Minősített archiválási szolgáltató* az e-aktában foglalt egyes elektronikus dokumentumokon lévő elektronikus aláírásokat, bélyegzőket ellenőrzi. Ha az *Előfizető* mind a keretaláírások, mind a belső aláírások és bélyegzők hitelességét

biztosítani szeretné, akkor keretaláírásokkal is és keretaláírás nélkül is be kell küldenie az e-aktát.

Keretaláírás hiányában az e-aktában foglalt valamennyi elektronikus dokumentumon el kell helyezni legalább egy érvényes elektronikus aláírást vagy bélyegzőt.

A *Minősített archiválási szolgáltató* visszautasítja azon e-aktákat, amelyeken bármely a fentiek szerint ellenőrzött elektronikus aláírás vagy bélyegző hibás, vagy aláíratlan dokumentumokat is tartalmaznak.

3. Az egyes elektronikus aláírások vagy bélyegzők érvényességének ellenőrzése során a *Minősített archiválási szolgáltató* ellenőrzi, hogy az egyes aláírások vagy bélyegzők az adott dokumentumhoz tartoznak-e. Ezt követően megpróbálja visszavezetni az adott aláírást vagy bélyegzőt valamely általa elfogadott gyökér *Tanúsítvány*ra (lásd: 1.3.1 fejezet), és OCSP alapján ellenőrzi a tanúsítványlánc minden elemének visszavonási állapotát is. A befogadási folyamat csak akkor megy tovább, ha az e-aktában szereplő összes elektronikus aláírás, bélyegző és *Időbélyegző* érvényesnek bizonyult.

   Az aláírás ellenőrzéséhez a *Minősített archiválási szolgáltató* az e-Szignó aláírás-létrehozó és ellenőrző alkalmazást 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 [30] szerint ellenőrzi és ETSI TS 101 903 [14] szerinti formátumot hoz létre.

   A *Minősített archiválási szolgáltató* csak olyan adatok tekintetében nyújt archiválás szolgáltatást – azaz csak olyan e-aktákat fogad be – amelyeken legalább fokozott biztonságú elektronikus aláírás vagy bélyegző található. A *Minősített archiválási szolgáltató* az elektronikus aláírás, bélyegző vagy *Időbélyegző* vizsgálata során az érvényességi láncot visszavezeti egy elfogadott hitelesítés- (vagy időbélyegzés-) szolgáltató megbízható gyökértanúsítványára. Előfordulhat, hogy egy hitelesítés-szolgáltató olyan teszt *Tanúsítvány*t bocsát ki, amely saját megbízható gyökértanúsítványa alapján ellenőrizhető. Az ilyen *Tanúsítvány*t a *Minősített archiválási szolgáltató* nem tudja elkülöníteni a valódi – fokozott vagy minősített biztonságú elektronikus aláírás vagy bélyegző létrehozására alkalmas – *Tanúsítvány*októl, és az ebből adódó esetleges károkért nem vállal felelősséget.

   Amennyiben a *Minősített archiválási szolgáltató* nem fogadja be az e-aktát, 3 napig megőrzi mindazon információt, amely segíthet az elutasítás okának felderítésében. Ilyen információ többek között az e-aktában szerepelő elektronikus aláírás, bélyegző, az aláírói *Tanúsítvány*ok, ezek tanúsítványláncai, illetve az időbélyegző tanúsítványok és ezek tanúsítványláncai, illetve az ezekhez kapcsolódó esetleges metaadatok.

4. A *Minősített archiválási 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 *Minősített archiválási szolgáltató* a szükséges ellenőrzéseket a kivárási idők elteltével végzi el a vonatkozó szabványok és nemzetközi ajánlások szerint. A *Minősített archiválási szolgáltató* elutasítja az e-aktát, ha az ellenőrzést 3 nap alatt nem tudja elvégezni.

A *Minősített archiválási szolgáltató* felépíti az e-aktákban szereplő elektronikus aláírásokhoz, bélyegzőkhöz tartozó érvényességi láncokat, és minősített archív elektronikus *Időbélyegző*t helyez el rajtuk. Az így kapott érvényességi láncokat ETSI TS 101 903 [14] formátumú ún. archív aláírásként elhelyezi az e-aktában.

5. A *Minősített archiválási szolgáltató* egy hosszú távon is biztonságosnak tartott kriptográfiai algoritmus és kulcsparaméter szerinti szolgáltatói kulccsal titkosítva tárolja el az archiválandó nyílt e-aktát. A befogadott e-akta titkosítatlan példányait a *Minősített archiválási szolgáltató* megsemmisíti olyan eljárás alkalmazásával, ami biztosítja hogy az e-aktát ne (vagy csak irreálisan nagy anyagi ráfordítás esetén) lehessen visszaállítani.

6. A *Minősített archiválási szolgáltató* a lehető leghamarabb, de a feltöltést követően legkésőbb 3 napon belül visszaigazolást küld az *Előfizető*nek arról, hogy az e-aktát sikeresen befogadta. Ha a folyamat valahol megszakadt, a *Minősített archiválási szolgáltató* erről is értesíti az *Előfizető*t. Ilyenkor az *Előfizető* olyan hibaüzenetet kap, amely arról tájékoztatja, hogy a *Minősített archiválási szolgáltató* nem tudta az e-aktát befogadni (például, mert nem tudta felépíteni az érvényességi láncot). A visszaigazolásokat és hibaüzeneteket a *Minősített archiválási szolgáltató* elektronikus levélben vagy más, az *Előfizető*vel 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 archív formátumú elektronikus aláírásokat, bélyegzőket tartalmazó – e-akta lenyomatát, amely a továbbiakban egyedi azonosítóként is szolgál,
   - a *Minősített archiválási rend* azonosítóját,
   - annak az egyértelmű jelzését, hogy a szolgáltatás az eIDAS-nak megfelelő, az Eüt. hatálya alatt álló elektronikus archiválás szolgáltatás,
   - az archiválás időtartamát,
   - azt, hogy a *Minősített archiválási szolgáltató* vállalja-e az olvashatóság és értelmezhetőség fenntartását az aktában lévő egyes elektronikus dokumentumokkal kapcsolatban.

   A visszaigazolás a fentieken kívül egyéb információt is tartalmazhat. A sikeres befogadásról szóló visszaigazolást minősített elektronikus bélyegző és minősített *Időbélyegző* hitelesíti.

Az *Előfizető*nek 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 bélyegző érvényes. A visszaigazolás elektronikusan bélyegzett dokumentum, így ha az *Előfizető* hosszú távon is meg szeretné őrizni a visszaigazolás hitelességét, akkor az elektronikusan bélyegzett dokumentumok érvényességének megőrzésére vonatkozó normatívák szerint kell eljárnia.

Ha az *Előfizető* a megadott határidőn belül nem kap pozitív visszaigazolást, azt úgy kell tekintenie, hogy a *Minősített archiválási szolgáltató* nem fogadta be az e-aktát. A *Minősített archiválási szolgáltató* kizárólag a pozitív visszajelzés elküldése esetén felel az e-akta megőrzéséért, és a benne szereplő elektronikus aláírások és bélyegzők hitelességének hosszú távú biztosításáért.

Az internet alapú feltöltésre a *Minősített archiválási szolgáltató* több lehetőséget is kínál, ezek például

- web oldali feltöltő felület a `https://archivmail.e-szigno.hu/arupload` címen;
- e-Szignó Archívum kliens feltöltő program;
- e-Szigno kliens programba épített archiválás feltöltő funkció a `https://archivmail.e-szigno.hu/submit` címen;
- más szolgáltatásokba integrált automatikus archiváló funkció.

A *Minősített archiválási 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 *Minősített archiválási szolgáltató*val egyedi esetben az *Előfizető* nemcsak hálózaton keresztül, hanem valamely adathordozón, például optikai lemezen is juttathat el dokumentumokat a *Minősített archiválási szolgáltató*nak. Az így kapott adathordozók tartalmát a *Minősített archiválási szolgáltató* a belső szabályzatainak megfelelően, szintén a fenti elvek szerint dolgozza fel. Az átvett adathordozót a *Minősített archiválási szolgáltató* nem őrzi meg, az adathordozón kapott adatállományok feldolgozása után az adathordozót a *Előfizető* kérésének megfelelően visszaszolgáltatja vagy biztonságos módon megsemmisíti.

3.3. Érvényességi lánc elérhetőségének biztosítása - e-akta letöltése

A *Minősített archiválási szolgáltató* biztosítja, hogy az *Előfizető* a szolgáltatási szerződés érvényességi ideje alatt letöltheti az archívumban tárolt e-aktáit és az azokhoz tartozó érvényességi láncokat.

Az *Előfizető* kizárólag biztonságos csatornán keresztül férhet hozzá a *Minősített archiválási szolgáltató* archívumában lévő e-aktákhoz és érvényességi láncokhoz. A letöltés tipikusan Interneten keresztül történik a *Minősített archiválási szolgáltató* által biztosított felület felhasználásával az alábbiak szerint:

1. Az *Előfizető* a kliens autentikációs *Tanúsítvány*a felhasználásával kölcsönös azonosításon alapuló SSL kapcsolatot létesít a *Minősített archiválási szolgáltató* szerverével. A *Minősített archiválási szolgáltató* az *Előfizető*t az SSL kapcsolat felépítéséhez használt kliens autentikációs *Tanúsítvány*a alapján azonosítja.

2. Az *Előfizető* megadja, hogy mely e-aktához kíván hozzáférni. A megfelelő e-akta kiválasztásához a web felületen lehetősége van a dokumentumhoz kapcsolódó Dublin Core [24] szerinti metaadatok alapján keresni az e-aktákra. A kiválasztás az e-aktát egyértelműen azonosító lenyomat (hash) alapú azonosító segítségével történik.

3. A *Minősített archiválási szolgáltató* megállapítja, hogy az *Előfizető* jogosult-e a kiválasztott e-aktához való hozzáférésre.

4. Megfelelő jogosultság esetén a *Minősített archiválási szolgáltató* a megadott hash alapú azonosító alapján előkeresi az archívumban titkosítottan tárolt e-aktát, átkódolja azt az *Előfizető* titkosító *Tanúsítvány*ához tartozó nyilvános kulccsal, majd az így újra titkosított e-aktát a védett SSL kapcsolaton keresztül eljuttatja az *Előfizető*höz.

   A *Minősített archiválási szolgáltató* megtagadja az e-akta letöltését, amennyiben az e-aktával kapcsolatban korábban már elbírált és hatályosult törlési kérelmet kapott.

5. Az *Előfizető* rendelkezik az archiválás szolgáltatás igénybevételére szolgáló titkosító *Tanúsítvány*ához tartozó magánkulccsal. Ezzel a kulccsal dekódolja az e-aktát, így hozzájut az érvényességi lánchoz illetve az e-aktában tárolt elektronikus dokumentumokhoz.

A *Minősített archiválási szolgáltató*val előre egyeztetett esetben az *Előfizető* valamely adathordozón, például optikai lemezen is átveheti a *Minősített archiválási szolgáltató* archívumában tárolt e-aktáit és érvényességi láncait. A hozzáférés ekkor is a fenti elvek szerint zajlik le, de ekkor az *Előfizető* (vagy írásban meghatalmazott képviselője) nem az autentikációs *Tanúsítvány*a, hanem valamely személyazonosításra alkalmas okmány alapján igazolja magát.

A feltöltött e-akták az *Előfizető* tulajdonában vannak (lásd: 1.3.2 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 e-aktákkal kapcsolatban a *Minősített archiválási szolgáltató* az *Előfizető* kérésére igazolást állít ki. Az igazolás a következőket tartalmazza:

1. Azt az állítást, hogy az adott e-aktán elhelyezett keretaláírás vagy keretaláírás hiányában az e-aktában foglalt fájlokon elhelyezett fokozott biztonságú vagy minősített elektronikus aláírások, bélyegzők, a rajtuk elhelyezkedő *Időbélyegző*k, és az ezekhez kapcsolódó *Tanúsítvány*ok az időbélyegzés és a feltöltés utáni ellenőrzés időpontjában érvényesek voltak.
2. Azt az állítást, hogy az adott e-akta adott lenyomattal rendelkezik, így megegyezik az *Előfizető* által bemutatott azonos lenyomatú e-aktával.
3. Azt az állítást, hogy keretaláírás esetén az adott e-aktán vagy keretaláírás hiányában az e-aktában foglalt fájlokon meghatározott személy vagy szervezet érvényes elektronikus aláírást vagy bélyegzőt helyezett el.
4. Azt az állítást, hogy keretaláírás esetén az adott e-aktán vagy keretaláírás hiányában az e-aktában foglalt fájlokon adott időpontban érvényes *Időbélyegző*t helyeztek el.

A *Minősített archiválási szolgáltató* az igazolást papír alapon, vagy minősített elektronikus aláírással ellátott e-aktában bocsátja ki. Az igazolást egy archív igazolás kiállításáért felelős tisztviselő készíti el, majd elektronikus igazolás esetében az igazolást minősített elektronikus aláírásával és minősített *Időbélyegző*vel látja el, papír alapú igazolás esetén a kinyomtatott igazolást kézzel írott aláírásával hitelesíti.

Az igazolás kibocsátásához nincs szükség az archivált e-akta ismeretére, az a nyílt e-akta nyíltan tárolt lenyomata alapján kerül kiállításra. A lenyomat értékből semmilyen információ nem nyerhető ki a tárolt e-akta tartalmára vonatkozóan. Az alkalmazott megoldás biztosítja, hogy az archív igazolás kiállításáért felelős tisztviselők az igazolás kiállítása kapcsán nem ismerhetik meg a nyílt e-akta tartalmát.

Az igazolás kibocsátása történhet olyan módon is, hogy az *Előfizető* bemutatja a *Minősített archiválási szolgáltató*nak a nyílt archivált e-aktát. Ekkor, feltéve, hogy a bemutatott nyílt e-aktával azonos lenyomatú e-akta szerepel a *Minősített archiválási szolgáltató* archívumában, a *Minősített archiválási szolgáltató* munkatársa az *Előfizető* által bemutatott e-aktára vonatkozóan állítja ki az igazolást.

Az *Előfizető* a *Minősített archiválási szolgáltató*hoz tetszőleges kézbesítési módon eljuttatott papír alapú, kézzel aláírt igénylés, vagy legalább fokozott biztonságú elektronikus aláírásával vagy bélyegzőjével hitelesített elektronikus igénylés benyújtásával kérheti az igazolás kiadását.

Az igazolás kiadását az *Előfizető* meghatalmazottja is kérheti, amennyiben ezt megelőzően bemutatta az *Előfizető* erre vonatkozó, teljes bizonyító erejű magánokiratba foglalt meghatalmazását.

Az igazolás igényléséhez az *Előfizető* (vagy meghatalmazottja) meg kell, hogy adja az e-akta lenyomatát vagy (a befogadáskor kiküldött visszaigazolásban is szereplő) egyedi azonosítóját, amelyikkel kapcsolatban az igazolást kéri. Ezen információkat a 3.3 fejezetben lévő keresőfelületről is kinyerheti. Az igazolást a *Minősített archiválási szolgáltató* annak az *Előfizető*nek adja

ki, akihez az adott e-akta a *Minősített archiválási szolgáltató* informatikai rendszere szerint tartozik. Harmadik félnek a *Minősített archiválási szolgáltató* kizárólag a fent leírt meghatalmazás bemutatása esetén adja ki az igazolást.

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. Az *Előfizető* kérésére az igazolás más formátumban is kiállítható. A *Minősített archiválási szolgáltató* az igazolás kiállításához olyan aláíró alkalmazást használ, amely rendelkezik egy független tanúsító szervezet által kiállított tanúsítvánnyal.

A *Minősített archiválási szolgáltató* megtagadja az igazolás kibocsátását, amennyiben az e-aktával kapcsolatban korábban már elbírált és hatályosult törlési kérelmet kapott.

3.5. Dokumentum megjelenítése

A *Minősített archiválási szolgáltató*val előre egyeztetett időpontban az *Előfizető* a *Minősített archiválási szolgáltató* szoftver és hardver eszközei segítségével megtekintheti a *Minősített archiválási szolgáltató* archívumában lévő dokumentumait a *Minősített archiválási szolgáltató* ügyfélszolgálati irodájában.

Az archívumban tárolt dokumentumok megtekintéséhez az *Előfizető* magával kell hozza az archív szolgáltatás igénybevételéhez szükséges titkosító *Tanúsítvány*ához tartozó magánkulcsát, illetve a kulcsot tartalmazó intelligens kártyáját.

3.6. Dokumentum és érvényességi lánc törlése

A *Minősített archiválási szolgáltató* az *Előfizető* kérésére törli az archivált e-aktát (dokumentumot) és a hozzá tartozó valamennyi 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 *Minősített archiválási szolgáltató* a teljes rendszerén végrehajtja, és a törlés keretében az e-akta minden mentett példányát megsemmisíti.

Törlési kérelmet a *Minősített archiválási szolgáltató* ügyfélszolgálati irodájának kell benyújtani írásban, papíralapon aláírt vagy elektronikus aláírással ellátott kérelem formájában. A törlést a *Minősített archiválási szolgáltató* egy munkanapon belül bírálja el és hajtja végre. Törlési kérelem olyan módon is benyújtható, hogy a törlést a *Minősített archiválási szolgáltató*nak nem haladéktalanul, hanem csak egy meghatározott napon kell végrehajtania.

A törlésről a *Minősített archiválási szolgáltató* visszaigazolást küld az *Előfizető*nek.

3.7. A szolgáltatási szerződés megszűnése

A Szolgáltatási szerződés megszűnése után még 60 napig a *Minősített archiválási szolgáltató* lehetővé teszi az *Előfizető* vagy az arra jogosult más személy részére az *Előfizető*höz tartozó e-akták és érvényességi láncok letöltését.

A határidő lejárta után a *Minősített archiválási szolgáltató* az archívumból kitörli az *Előfizető*höz tartozó e-aktákat és érvényességi láncokat.

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

4. Műszaki biztonsági óvintézkedések

4.1. Biztonsági garanciák

A *Minősített archiválási szolgáltató* módosítás ellen védett, megbízható rendszereket és termékeket használ. Megbízható, biztonságtechnikailag értékelt és minősített termékekből álló, egységes informatikai rendszert használ szolgáltatásai nyújtásához. A *Minősített archiválási szolgáltató* olyan megbízható rendszereket és termékeket használ, amelyek az illetéktelen módosítással szemben védettek. Mind a *Minősített archiválási szolgáltató*, mind a rendszert szállító és kivitelező vállalkozók hitelesítés-szolgáltatás kiépítésében jelentős tapasztalatokkal rendelkeznek és nemzetközileg elismert technológiát alkalmaznak.

Amennyiben a *Minősített archiválási szolgáltató* harmadik féltől bizalmi szolgáltatást vesz igénybe, ellenőriznie kell, hogy ezen harmadik fél eleget tesz-e minden szükséges kötelezettségének. A *Minősített archiválási szolgáltató* az archivált e-aktákat fizikailag biztonságos környezetben, a 5. fejezetben leírt fizikai és eljárásbeli óvintézkedések mellett tárolja, amelynek biztonságát a *Minősített archiválási szolgáltató* belső biztonsági szabályzatai és a rendszeres belső és külső biztonsági felülvizsgálat garantálják. A *Minősített archiválási szolgáltató* biztosítja, hogy a tárolt e-aktákat saját munkatársai sem olvashatják el. A *Minősített archiválási szolgáltató* az e-aktákat kizárólag akkor bocsátja harmadik fél (pl. hatóság) rendelkezésére, ha erre az *Előfizető* felhatalmazta, vagy ha ezt jogszabály írja elő.

A tárolt e-akták integritását az e-akták fizikai védelme, valamint az elektronikus aláírással kapcsolatos technológiák biztosítják. Az e-akták rendelkezésre állását a *Minősített archiválási 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 *Minősített archiválási szolgáltató* ezen eljárások, valamint ezek folyamatos külső és belső ellenőrzése és tesztelése segítségével kerüli el az üzemeltetés és a karbantartás során felmerülő hibákat. A *Minősített archiválási szolgáltató* két, egymástól távoli fizikai helyszínen tárolja az archivált e-aktákat.

A *Minősített archiválási szolgáltató* az archivált e-aktákat – az *Előfizető* kérése vagy a szerződés megszűnése esetén – a 3.6 fejezetben leírt feltételek mellett semmisíti meg. A *Minősített archiválási 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 *Minősített archiválási szolgáltató* szabályos időközönként cseréli. A *Minősített archiválási szolgáltató* figyelemmel kíséri a technológia fejlődését, és amennyiben azt észleli, valamely kulcs már nem biztonságos, illetve ha a Nemzeti Média- és Hírközlési Hatóság határozata szerint az adott algoritmus már nem használható, akkor haladéktalanul lecseréli az érintett kulcsot vagy kulcsokat.

A *Minősített archiválási szolgáltató* titkosítva tárolja az e-aktákat. A *Minősített archiválási szolgáltató* az e-aktákat mindig olyan algoritmussal titkosítja, amely a technológia adott állása szerint biztonságosnak minősül. Amennyiben ezen algoritmus biztonsága a technológia fejlődése során megsérül, a *Minősített archiválási szolgáltató* saját belső szabályzatai alapján gondoskodik az e-akta biztonságos algoritmussal történő újra-titkosításáról. A nyílt e-aktákat kizárólag az elektronikus archiválás nyújtásához kapcsolódó jogszabályi követelmények teljesítéséhez állítja vissza, azaz a 3.3., a 4.4. és 4.5. fejezetekben leírt esetekben.

4.2. Számítógépes biztonsági óvintézkedések

A *Minősített archiválási 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 visszaigazolásokat aláíró kulcsokat, az archivált adatok titkosításához/dekódoláshoz szükséges kulcsokat, valamint az infrastrukturális és rendszervezérlési kulcsokat hardveres kriptográfiai eszközben állítja elő.

A *Minősített archiválási szolgáltató* informatikai rendszerét többfokozatú tűzfalrendszerrel védi. Minden tűzfalból két példány működik, bármelyik kiesése esetén egy cluster segítségével a másik ugyanolyan egység átveszi a funkcióját.

4.3. Életciklusra vonatkozó műszaki óvintézkedések

Annak érdekében, hogy a *Minősített archiválási 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.

4.4. Rendszeres felülhitelesítés

A *Minősített archiválási szolgáltató* az érvényességi láncokon minősített elektronikus aláírást vagy bélyegzőt és minősített *Időbélyegző*t helyez el:

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

A minősített elektronikus aláírást vagy bélyegzőt és a minősített *Időbélyegző*t a *Minősített archiválási szolgáltató* a Nemzeti Média- és Hírközlési Hatóság mindenkori aktuális algoritmusokkal kapcsolatos határozata szerinti biztonságos algoritmusokkal hozza létre (a *Minősített archiválási szolgáltatási szabályzat* kibocsátásának idején [9]).

4.5. Az archívum újra-titkosítása

A *Minősített archiválási szolgáltató* az archivált e-aktákat titkosítva tárolja az archívumában. Biztosítja, hogy az archivált e-akták mindenkor biztonságos algoritmussal kerülnek titkosításra.

A *Minősített archiválási 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 *Minősített archiválási szolgáltató* dekódoló kulcsának bizalmassága sérül;
- a *Minősített archiválási szolgáltatási szabályzat* vagy az *Előfizető*vel kötött szerződés így rendelkezik.

Miután a *Minősített archiválási szolgáltató* biztonságos módon újra titkosította az archivált e-aktákat, megsemmisíti a korábbi, már nem kellően biztonságosnak ítélt módon titkosított példányokat.

4.6. A technológia folyamatos figyelése

A *Minősített archiválási szolgáltató* folyamatosan figyelemmel kíséri az elektronikus aláírással és kriptográfiával kapcsolatos technológia fejlődését. Amennyiben a *Minősített archiválási szolgáltató* értesülései szerint a Nemzeti Média- és Hírközlési Hatóság határozata szerinti, elfogadott, meghatározott paraméterekkel rendelkező kriptográfiai algoritmusok már nem biztonságosak, erről

értesíti a Nemzeti Média- és Hírközlési Hatóságot és megkéri a kriptográfiai algoritmusokkal kapcsolatos határozat felülvizsgálatára.

A *Minősített archiválási szolgáltató* bármikor szabadon dönthet a használt kriptográfiai algoritmuskészletek és paramétereik megváltoztatásáról a Nemzeti Média- és Hírközlési Hatóság algoritmusokkal kapcsolatos határozatában szereplő algoritmus és paraméter esetén.

4.7. Hitelesítés és időbélyegzés szolgáltatók elfogadása

A *Minősített archiválási szolgáltató* a honlapján teszi közzé, hogy mely *Hitelesítés-szolgáltató*k *Tanúsítvány*ait és mely *Időbélyegzés-szolgáltató*k *Időbélyegző*it milyen feltételekkel fogadja el. Az elfogadott szolgáltatók listája az alábbi címen érhető el:

`https://e-szigno.hu/hitelesites-szolgaltatas/archivalas-szolgaltatas/elfogadott-szolgaltatok.html`

A *Minősített archiválási szolgáltató* dokumentált eljárásrenddel rendelkezik, amely szerint az egyes *Hitelesítés-szolgáltató*k és *Időbélyegzés-szolgáltató*k *Tanúsítvány*ait és *Időbélyegző*it elfogadja, illetve nem fogadja el. Ezen eljárásrend többek között azt is meghatározza, hogy a *Minősített archiválási szolgáltató* milyen intézkedéseket hajt végre egy korábban elfogadott *Hitelesítés-szolgáltató*, illetve *Időbélyegzés-szolgáltató* magánkulcsának kompromittálódása esetén.

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

A *Minősített archiválási szolgáltató* gondoskodik róla, hogy az archiválás időtartama alatt bizonyos formátumú fájlok megjelenítéséhez szükséges szoftver és hardver eszközök folyamatosan rendelkezésére álljanak. A *Minősített archiválási szolgáltató* ennek érdekében szabályozott és auditált belső folyamatokat alakított ki. A *Minősített archiválási szolgáltató* belső szabályzatai kitérnek a fájlok megjelenítésére szolgáló mindenkori hardver és szoftver környezet rendelkezésre állásának biztosítására, a környezet rendszeres felülvizsgálatára és naprakészen tartására.

A *Minősített archiválási szolgáltató* az eredeti aláírt bitsorozat olvashatóságát, értelmezhetőségét biztosítja, így a *Minősített archiválási szolgáltató* nem transzformálja át az aláírt fájlt más formátumba.

A *Minősített archiválási szolgáltató* olyan formátumú fájlokat tartalmazó e-aktákat is befogad az archívumába, amelynek tekintetében nem biztosít olvashatóságot és értelmezhetőséget. A *Minősített archiválási szolgáltató* a dokumentumok megőrzését, tehát a dokumentumok olvashatóságának fenntartását is a szolgáltatási szerződés érvényességi idejéig vállalja. A szolgáltatás leállításakor a *Minősített archiválási szolgáltató* a 5.7 fejezetben leírtak szerint átadja a szolgáltatást egy másik szolgáltatónak. Ekkor a *Minősített archiválási 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 *Minősített archiválási szolgáltató* a következő fájlformátumok tekintetében biztosítja az olvashatóságot és értelmezhetőséget:

- ISO/IEC 646:1991 (7 bites karakterkészlet információcsere biztosításához, ASCII) [15],
- ISO 8859-1:1998 (Latin-1, 8 bites grafikus karakterkészlet) [16],
- ISO 8859-2:1999 (Latin-2) [17], a magyar referenciakészletre vonatkozóan az MSZ 7795-3:1992 [21] ASCII és ASCII/PC kód szerinti eltéréssel is,
- ISO 10646:2003 (Unicode v.4.0) [18],
- Microsoft Rich Text Format 1.7. [26],
- Portable Document Format (PDF) 1.3. [31],
- PDF/A formátum (ISO 19005) [27],
- Microsec e-akta formátum minden verziója [25],
- ETSI TS 101 903 v1.2.2, v1.3.2, v1.4.1 és v1.4.2 [14], formátumú XAdES aláírások (amennyiben egy XML fájl XAdES aláírást tartalmaz, a *Minősített archiválási szolgáltató* az aláírás értelmezhetőségét biztosítja),
- ETSI EN 319 132-1 [10] formátumú XAdES aláírások (amennyiben egy XML fájl XAdES aláírást tartalmaz, a *Minősített archiválási szolgáltató* az aláírás értelmezhetőségét biztosítja),
- ETSI EN 319 132-2 [11] formátumú XAdES aláírások (amennyiben egy XML fájl XAdES aláírást tartalmaz, a *Minősített archiválási szolgáltató* az aláírás értelmezhetőségét biztosítja),
- IETF RFC 2822 (Internet Message Format) [23],
- IETF RFC 2045 (Multipurpose Internet Mail Extensions, MIME) [22],
- Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható elektronikus aláírás formátumok műszaki specifikációjára [6]
- Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható végfelhasználói tanúsítványok szerkezetének és adattartalmának műszaki specifikációjára [7],
- Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható időbélyegzés formátum műszaki specifikációjára [8].
- Az elektronikus cégeljárásban használt XML formanyomtatványok [1],

[1] Ezek formátuma a `http://www.e-cegjegyzek.hu/e-cegeljaras/cegnyomtatvany.htm` címen érhető el.

- Olyan XML formátumok, amelyekhez az *Előfizető* előzetesen benyújt a *Minősített archiválási szolgáltató*nak 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 *Minősített archiválási szolgáltató* biztosítsa az adott formátum olvashatóságát és értelmezhetőségét, és ezen igényét jelzi a *Minősített archiválási szolgáltató*nak, a *Minősített archiválási szolgáltató* erre vonatkozó eljárásrendje szerint megvizsgálja, hogy az adott formátum esetében ez megoldható-e, illetve milyen feltételekkel oldható meg. Amennyiben a *Minősített archiválási szolgáltató* az *Előfizető* által kért formátumot felveszi az olvashatóság és értelmezhetőség tekintetében támogatott formátumok közé, az jelen *Minősített archiválási szolgáltatási szabályzat* módosítását jelenti.

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

A *Minősített archiválási szolgáltató* kizárólag a fent meghivatkozott specifikációkban leírt mértékig vállalja az egyes formátumok megjeleníthetőségét. Amennyiben egyes formátumok például beágyazott objektumokat is tartalmazhatnak, a *Minősített archiválási szolgáltató* nem vállalja ezen beágyazott objektumok megjeleníthetőségének biztosítását. Mivel az e-mail formátum (RFC 2822 [23]) nem specifikálja az e-mailben szereplő karakterek kódolását, a *Minősített archiválási szolgáltató* kizárólag olyan e-mailek megjelenítését vállalja, amelyekben az üzenet a fenti karakterkódolások egyikével szerepel. A MIME (RFC 2045 [22]) specifikáció szerint kódolt "csatolmányok" esetén a *Minősített archiválási szolgáltató* kizárólag azon csatolmányok megjeleníthetőségét vállalja, amelyek a fenti formátumok egyikével rendelkeznek.

A *Minősített archiválási szolgáltató* a fájlok olvashatóságát, megjeleníthetőségét vállalja, a fájl az 1.5. fejezetben szereplő definíciója szerint. Ez azt jelenti, hogy a *Minősített archiválási szolgáltató* akkor biztosítja egy (fenti formátumú) fájl értelmezhetőségét, megjeleníthetőségét, ha az egy e-aktában az ETSI TS 101 903 [14], (ETSI EN 319 132-1 [10]), illetve az e-Szignó program szerint beillesztve szerepel. A *Minősített archiválási szolgáltató* nem vállalja az egyéb transzformációkkal (is) kódolt, különösen a titkosított fájlok olvashatóságának biztosítását. A fájlokon kívül a *Minősített archiválási szolgáltató* e-akták olvashatóságát, megjeleníthetőségét is vállalja. Ez az aláírások, bélyegzők és *Időbélyegző*k ellenőrizhetőségéig, és az e-aktákban elhelyezett fájlok kinyeréséig terjed.

A *Minősített archiválási szolgáltató* felhívja az *Ügyfel*ek 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 *Minősített archiválási szolgáltató* azt tanácsolja *Ügyfel*einek, hogy lehetőleg ne helyezzenek el aláírást aktív elemeket tartalmazó fájlokon. A *Minősített archiválási 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 *Minősített archiválási 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 *Előfizető*nek. A *Minősített archiválási szolgáltató* rendszere nem végez teljeskörű ellenőrzést, így a *Minősített archiválási szolgáltató* nem vállal azért felelősséget, hogy rendszere minden aktív kódot megtalál. Amennyiben az *Előfizető*ben kétség merül fel arra vonatkozóan, hogy egy adott fájl esetén a *Minősített archiválási szolgáltató* milyen mértékig biztosítja a fájl olvashatóságát és értelmezhetőségét, a *Minősített archiválási szolgáltató* azt javasolja, hogy az *Előfizető* vegye igénybe a 3.5. fejezetben leírt szolgáltatást, és tekintse meg a fájlt a *Minősített archiválási szolgáltató* eszközei segítségével is.

Egy e-akta befogadásakor a *Minősített archiválási 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 *Minősített archiválási szolgáltató* nem garantálja. A befogadáskor elvégzett ellenőrzés nem teljes körű, a *Minősített archiválási szolgáltató* nem vállal felelősséget azért, hogy az ismeretlen formátumúnak nem tekintett fájlok támogatott formátummal rendelkeznek és szintaktikailag helyesek.

4.9. 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 *Minősített archiválási szolgáltató*), illetve korábbi időzített törlési kérelmek módosítása,

- információkérés a korábban elküldött kérések állapotára vonatkozóan.

A dokumentumok (e-akták) feltöltése szolgáltatást a *Minősített archiválási szolgáltató* jogosult szüneteltetni.

Az igazolások kibocsátását a *Minősített archiválási szolgáltató* a *Minősített archiválási szolgáltatási szabályzat*ban leírt módon, folyamatosan biztosítja, az igazolások kibocsátásának szolgáltatáskiesése nem haladhatja meg a 3 napot.

A *Minősített archiválási szolgáltató* ügyfélszolgálati irodája minden munkanapon, nyitvatartási időben fogad igazolás kibocsátására vonatkozó kérelmeket; az igazolások kibocsátása 3 nap alatt történik meg.

A *Minősített archiválási szolgáltató* ügyfélszolgálati irodájának nyitva tartását az 1.3.1. fejezet tartalmazza.

5. Elhelyezési, eljárásbeli és üzemeltetési előírások

A *Minősített archiválási szolgáltató* széles körben elismert szabványoknak megfelelő fizikai, eljárásbeli és személyzeti biztonsági óvintézkedéseket, valamint az ezeket érvényre juttató adminisztratív és irányítási eljárásokat alkalmaz.

A *Minősített archiválási szolgáltató* nyilvántartást vezet a szolgáltatás nyújtásával kapcsolatos rendszerelemekről és erőforrásokról, és ezekkel kapcsolatos kockázatelemzést végez. Az egyes elemekkel kapcsolatban a kockázatokkal arányos védelmi megoldásokat alkalmaz.

A *Minősített archiválási szolgáltató* figyelemmel kíséri a kapacitás igényeket és biztosítja, hogy megfelelő feldolgozási teljesítmény és tárolási kapacitás álljon rendelkezésre a szolgáltatás nyújtásához.

5.1. Fizikai követelmények

A *Minősített archiválási szolgáltató* gondoskodik arról, hogy a kritikus szolgáltatásokhoz történő fizikai hozzáférés ellenőrzött legyen és a kritikus szolgáltatások eszközeit érintő fizikai kockázatát minimalizálja.

A fizikai óvintézkedések célja a *Minősített archiválási szolgáltató* által birtokolt információra illetve fizikai zónáira irányuló jogosulatlan hozzáférés, károkozás és illetéktelen behatolás megakadályozása.

A kritikus és érzékeny információt feldolgozó szolgáltatásokat biztonságos helyszíneken valósítják meg a *Minősített archiválási szolgáltató* rendszerében.

A biztosított védelem mértéke megfelel a *Minősített archiválási szolgáltató* által végzett kockázatelemzésben megállapított fenyegetettség mértékének.

A megfelelő védelem biztosítása érdekében:

- A *Minősített archiválási szolgáltató* védett számítógéptermében valósítja meg a szigorúbban védendő szolgáltatásokat. Ez a számítógépterem speciálisan erre a célra lett tervezve és kialakítva, tervezésénél különböző védelmi szempontok [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 *Minősített archiválási szolgáltató* valamennyi kritikus szolgáltatását egy külön biztonsági zónában valósítja meg, az ehhez szükséges valamennyi eszközt egy – a biztonsági zóna részét képező – védett számítógépteremben helyezi el.

5.1.1. A telephely elhelyezése és szerkezeti felépítése

A *Minősített archiválási szolgáltató* informatikai rendszereit fizikai és logikai védelemmel ellátott, megfelelően biztonságos *Adatközpont*ban helyezte el és üzemelteti, amely megakadályozza az illetéktelen hozzáférést. Az *Adatközpont* elhelyezése és kialakítása során egymásra épülő és egymást támogató védelmi megoldásokat alkalmaz – őrzés, biztonsági zárak, behatolás érzékelők, video megfigyelő rendszer, beléptető rendszer stb. – amelyek együttesen egy erős védelmi szintet biztosítanak a szolgáltatásban részt vevő informatikai rendszerek és a szolgáltató által tárolt bizalmas adatok megóvására.

5.1.2. Fizikai hozzáférés

A *Minősített archiválási szolgáltató* védi a szolgáltatás nyújtásában részt vevő eszközeit és berendezéseit a jogosulatlan fizikai hozzáféréstől az eszközök manipulálásának megakadályozása érdekében. A *Minősített archiválási szolgáltató* biztosítja, hogy:

- az *Adatközpont*ba történő minden belépés regisztrálásra kerül;
- az *Adatközpont*ba csak két – bizalmi szerepkört betöltő, erre feljogosított – munkatárs egyidejű azonosítása után lehet belépni, legalább az egyik munkatársnak rendszeradminisztrátornak kell lennie;
- az önálló jogosultsággal nem rendelkező személyek csak indokolt esetben, a szükséges ideig tartózkodhatnak a gépteremben megfelelő jogosultságú kísérő személyzettel;
- a belépési logokat folyamatosan archiválják és legalább hetente megvizsgálják.

Az eszközök aktivizáló adatai (jelszavak, PIN kódok) a géptermen belül sem tárolhatók nyílt formában.

Jogosulatlan személyek jelenlétében:

- a bizalmas adatokat tartalmazó adathordozókat fizikailag elzárva tartják;
- a bejelentkezett terminálokat nem hagyják felügyelet nélkül;
- nem végeznek olyan munkafolyamatot, amely során bizalmas adat felfedésre kerülhet.

A gépterem elhagyásakor az adminisztrátornak ellenőriznie kell, hogy:

- az *Adatközpont* minden berendezése megfelelően biztonságos üzemállapotban van;
- egyetlen terminálon sem maradt bejelentkezve;
- a fizikai tároló eszközök megfelelően be lettek zárva;
- a fizikai védelmet biztosító rendszerek, berendezések megfelelően működnek;
- a riasztó rendszer aktiválva lett.

A rendszeres fizikai biztonsági vizsgálatokat kijelölt felelősök végzik. A vizsgálatok eredményét megfelelő naplóbejegyzésekben rögzítik.

5.1.3. Áramellátás és légkondicionálás

A *Minősített archiválási szolgáltató Adatközpont*jában olyan szünetmentes áramellátó rendszert alkalmaz, amely:

- megfelelő teljesítménnyel rendelkezik az adatközpont informatikai és a kisegítő létesítményi rendszerei áramellátásának biztosítására;
- megvédi az informatikai berendezéseket a külső hálózatból érkező feszültség ingadozások, feszültség kimaradások, tüskék és egyéb zavarok ellen;
- tartós áramszünet esetére saját áramtermelő berendezéssel rendelkezik, amely - üzemanyag utántöltést lehetővé téve - tetszőleges időtartamig képes a szükséges energia biztosítására.

Az *Adatközpont*ba nem juthat be közvetlenül a külső környezet levegője. Az *Adatközpont* levegőjének tisztaságát megfelelő szűrőrendszer alkalmazása biztosítja, amely kiszűri a levegőből a különféle szennyeződéseket (por, szennyező anyagok, korrozív anyagok, mérgező vagy gyúlékony anyagok). A szellőző rendszer megfelelő szűrés mellett biztosítja az operátorok biztonságos munkavégzéséhez szükséges mennyiségű friss levegőt.

A levegő nedvességtartalma az informatikai rendszerek által megkívánt szintre van csökkentve.

A *Minősített archiválási szolgáltató* megfelelő teljesítményű hűtőrendszert használ a szükséges üzemi hőmérséklet biztosítása, az informatikai eszközök túlhevülésének megakadályozása érdekében.

5.1.4. Beázás és elárasztódás veszély kezelése

A *Minősített archiválási szolgáltató* biztonsági zónájának kialakítása során fontos szempont volt a beázás és elárasztódás veszélyének minimalizálása. A biztonsági zóna teljes területe mentes a vizesblokkoktól, nincs a közelében sem csatorna sem vízvezeték. A biztonsági zóna teljes területét vízbetörés érzékelő rendszer felügyeli. A védett számítógépteremben a biztonságot tovább növeli az álpadló alkalmazása.

5.1.5. Tűz megelőzés és tűzvédelem

A *Minősített archiválási szolgáltató Adatközpont*jában az illetékes tűzoltóparancsnokság által jóváhagyott tűzvédelmi rendszer működik. A füst és tűzérzékelők vészhelyzet esetén automatikusan riasztják a tűzoltóságot. A gépteremben vízpára alapú, automatikus tűzoltó rendszer lett kialakítva, amely az emberi életre nem veszélyes és nem károsítja az informatikai eszközöket sem.

Minden helyiségben jól látható helyen található a vonatkozó előírásoknak megfelelő típusú és mennyiségű kézi tűzoltó készülék.

5.1.6. Adathordozók tárolása

A *Minősített archiválási szolgáltató* megvédi valamennyi adathordozóját a jogosulatlan hozzáféréstől és a véletlen rongálódástól. Minden napló és archív adatot legalább két példányban hoz létre. A példányokat egymástól fizikailag elkülönítve tárolja, egymástól biztonságos távolságra lévő helyszíneken. A tárolt adathordozókat védi a káros környezeti behatásoktól, mint pl. alacsony vagy magas hőmérséklet, szennyeződés, nedvesség, napfény, erős mágneses tér, erős sugárzás.

A *Minősített archiválási szolgáltató* az elsődleges adathordozókat kódzáras, tűzálló páncélszekrényekben tárolja a hitelesítő szervezet operátori helyiségében, a másolati példányokat páncélszekrényben az ügyfélszolgálati irodában.

5.1.7. Hulladék megsemmisítése

A *Minősített archiválási szolgáltató* a környezetvédelmi előírások betartásával gondoskodik feleslegessé vált eszközeinek, adathordozóinak megsemmisítéséről.

A *Minősített archiválási szolgáltató* a bizalmas minősítésű adatokat tartalmazó elektronikus adathordozókat még tartalmuk törlése után sem használja fel nem bizalmas minősítésű adatok tárolására, az ilyen eszközök nem vihetők ki a *Minősített archiválási szolgáltató* területéről. A *Minősített archiválási szolgáltató* a meghibásodott vagy bármely más okból használhatatlanná, feleslegessé vált, bizalmas minősítésű adatokat tartalmazó adathordozókat – a selejtezési szabályzatának megfelelően – fizikailag megsemmisíti:

- a papíralapú dokumentumokat iratmegsemmisítő géppel felaprítja;

- a merevlemezeket szétszereli és a kritikus alkatrészeket összetöri;
- az optikai lemezeket erre alkalmas iratmegsemmisítő géppel megsemmisíti.

5.1.8. A mentési példányok fizikai elkülönítése

A *Minősített archiválási szolgáltató* legalább heti rendszerességgel előállít olyan mentést, amiből meghibásodás esetén a teljes szolgáltatás helyreállítható. A mentéseket - legalább az utolsó teljes mentést is beleértve - egy olyan külső helyszínen tárolja, amelynek a fizikai és működési védelme azonos az elsődleges helyszínével. Az elsődleges és a tartalék helyszínek között biztosítja az adatok biztonságos továbbítását.

5.2. Eljárásbeli előírások

A *Minősített archiválási szolgáltató* gondoskodik arról, hogy rendszereit biztonságosan, szabályszerűen, a meghibásodás minimális kockázata mellett üzemeltesse.

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 környezetre és személyzetre vonatkozó óvintézkedések hatásosságát.

A *Minősített archiválási 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 *Minősített archiválási szolgáltató* rendszerében élesen elkülönülnek egymástól a fejlesztési és üzemeltetési folyamatok. A rendszer megfelelő működését a független rendszervizsgáló és a *Minősített archiválási szolgáltató* belső folyamatainak rendszeres ellenőrzése biztosítja.

5.2.1. Bizalmi szerepkörök

A *Minősített archiválási szolgáltató* feladatai ellátásához bizalmi szerepköröket hozott létre. A jogosultságok és funkciók oly módon lettek megosztva az egyes bizalmi szerepkörök között, hogy egyedül egyetlen felhasználó se legyen képes a biztonsági védelmi intézkedések megkerülésére.

A *Minősített archiválási szolgáltató* a következő bizalmi szerepköröket határozza meg az alábbi felelősségi körökkel:

A *Minősített archiválási szolgáltató* informatikai rendszeréért általánosan felelős vezető: Az informatikai rendszerért felelős személy.

Biztonsági tisztviselő: Biztonságtechnikai főmunkatárs, a szolgáltatás biztonságáért általánosan felelős személy.

Rendszeradminisztrátor: Infrastruktúra adminisztrátor. Feladata a *Minősített archiválási 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.

Operátor: Rendszerüzemeltető, az informatikai rendszer folyamatos üzemeltetését, mentését és helyreállítását végző személy.

Független rendszervizsgáló: A *Minősített archiválási szolgáltató* naplózott, illetve archivált adatállományát vizsgáló, a *Minősített archiválási szolgáltató* által a szabályszerű működés érdekében megvalósított kontroll intézkedések betartásának ellenőrzéséért, a meglévő eljárások folyamatos vizsgálatáért és monitorozásáért felelős személy.

Archiválási tisztviselő: Két archiválási tisztviselő együttes közreműködésével lehetőség van egy e-akta visszafejtésére. Az archiválási tisztviselők felelősek a visszafejtett e-akta biztonságos kezeléséért illetve a felhasználás utáni megsemmisítéséért.

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

A bizalmi szerepkörök ellátására a *Minősített archiválási szolgáltató* biztonságért felelős vezetője formálisan kinevezi a *Minősített archiválási szolgáltató* munkatársait.

Bizalmi szerepkört csak a *Minősített archiválási szolgáltató*val munkaviszonyban álló személyek láthatnak el, megbízási szerződés keretében a bizalmi szerepkörök nem láthatók el.

A bizalmi szerepkörökről a *Minősített archiválási szolgáltató* naprakész nyilvántartást vezet, a változásokat haladéktalanul bejelenti a Nemzeti Média- és Hírközlési Hatóságnak.

5.2.2. Az egyes feladatok ellátásához szükséges személyzeti létszámok

A *Minősített archiválási szolgáltató* biztonsági és üzemeltetési szabályzata előírja, hogy csak védett környezetben, kettő, bizalmi szerepkört betöltő munkatárs egyidejű fizikai jelenlétében végezhetők el az alábbi műveletek:

- a *Minősített archiválási szolgáltató* saját szolgáltatói kulcspárjának generálása;
- a szolgáltatói magánkulcs mentése;
- a szolgáltatói magánkulcs aktiválása;
- a szolgáltatói magánkulcs megsemmisítése.

A felsorolt műveleteket végrehajtó személyek közül legalább az egyiknek rendszeradminisztrátornak kell lennie és a másik személy nem lehet független rendszervizsgáló.

Két archiválási tisztviselő együttes közreműködése szükséges az archívumban titkosítottan tárolt e-akták visszafejtéséhez. Az archiválási tisztviselők felelősek a visszafejtett e-akta biztonságos kezeléséért illetve a felhasználás utáni megsemmisítéséért.

A felsorolt műveletek végrehajtása során illetéktelen személy nem lehet jelen a helyiségben.

5.2.3. Az egyes szerepkörökben elvárt azonosítás és hitelesítés

A *Minősített archiválási szolgáltató* informatikai rendszerét kezelő felhasználók egyedi azonosító adatokkal rendelkeznek, amely lehetővé teszi a felhasználók biztonságos azonosítását és hitelesítését.

A felhasználók a hitelesítés-szolgáltatás szempontjából kritikus informatikai rendszerekhez csak azonosítás és hitelesítés után férhetnek hozzá.

Az azonosító és hitelesítő adatok a felhasználói jogosultságok megszűnésekor haladéktalanul visszavonásra kerülnek.

Az informatikai rendszer minden felhasználója és az adminisztratív folyamatok minden szereplője személy szerint kerül azonosításra. A fizikai hozzáférés ellenőrzéséhez a *Minősített archiválási szolgáltató* RFID kártyára épülő beléptető rendszert használ, a logikai hozzáférés ellenőrzése *Elektronikus aláírást létrehozó eszköz*ön kiadott VPN *Tanúsítvány*ok segítségével történik. Sikeres hitelesítés nélkül egyetlen biztonsági szempontból kritikus feladatot sem lehet végrehajtani. A *Minősített archiválási szolgáltató* minden munkatársa annak megfelelő hozzáférési jogosultsággal rendelkezik, amely a feladatköre ellátásához elengedhetetlenül szükséges.

5.2.4. Egymást kizáró szerepkörök

A *Minősített archiválási szolgáltató* munkatársai egyidejűleg több bizalmi szerepkört is betölthetnek, de a *Minősített archiválási szolgáltató* biztosítja, hogy:

- a biztonsági tisztviselő és a regisztrációs felelős nem töltheti be a független rendszervizsgálói szerepkört;
- a rendszeradminisztrátor nem töltheti be a biztonsági tisztviselő és a független rendszervizsgálói szerepkört;
- az informatikai rendszerért általánosan felelős vezető nem láthatja el a biztonsági tisztviselő és a független rendszervizsgáló feladatkörét.

A fentieken túl a *Minősített archiválási szolgáltató* törekszik a bizalmi szerepkörök teljes szétválasztására.

5.3. Személyzetre vonatkozó előírások

A *Minősített archiválási szolgáltató* gondoskodik arról, hogy személyzeti politikája, illetve a munkatársak alkalmazására vonatkozó gyakorlata fokozza és támogassa a *Minősített archiválási szolgáltató* működésének megbízhatóságát. A személyzetre vonatkozó óvintézkedések célja az emberi hibák, lopás, csalás és a visszaélések kockázatának csökkentése.

A *Minősített archiválási szolgáltató* már a felvételi szakaszban foglalkozik a személyi biztonsággal, beleértve a szerződések megkötését, illetve azok alkalmazás során történő ellenőrzését. Valamennyi bizalmi szerepkör esetén a szerepkört betöltő személyeknek kinevezésükkor érvényes erkölcsi bizonyítvánnyal kell rendelkezniük. Minden bizalmi szerepkört betöltő alkalmazottnak és külső félnek – aki a *Minősített archiválási szolgáltató* szolgáltatásaival kapcsolatba kerül – titoktartási nyilatkozatot kell aláírnia.

A *Minősített archiválási szolgáltató* egyúttal biztosítja valamennyi munkakör betöltéséhez a szükséges közös, általános, illetve az egyes szerepkörök betöltéséhez szükséges speciális szakmai ismeretek megszerzését, illetve továbbfejlesztését.

5.3.1. Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

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

A *Minősített archiválási szolgáltató*nál bizalmi szerepkört csak olyan személy tölthet be, akinek a befolyásmentességét és szakértelmét a *Minősített archiválási szolgáltató* igazolni tudja.

Az informatikai rendszerért általánosan felelős vezető csak olyan személy lehet, aki rendelkezik:

- szakirányú felsőfokú végzettséggel (matematikusi, fizikusi egyetemi végzettség vagy a műszaki tudományterületre tartozó mérnöki szakon szerzett főiskolai vagy egyetemi végzettség);
- legalább három év, az informatikai biztonsággal összefüggésben szerzett szakmai gyakorlattal.

5.3.2. Előélet vizsgálatára vonatkozó eljárások

A *Minősített archiválási szolgáltató* vezető munkakörben illetve bizalmi szerepkörben csak olyan alkalmazottakat foglalkoztat, akik:

- büntetlen előélettel rendelkeznek és nincs ellenük folyamatban olyan eljárás, amely a büntetlenséget befolyásolhatja;
- nem állnak a bizalmi szolgáltatási tevékenység gyakorlását kizáró foglalkozástól eltiltás hatálya alatt.

Kinevezéskor a *Minősített archiválási szolgáltató* vezető munkakört betöltő alkalmazottjának nyilatkozatával, bizalmi szerepkört betöltő alkalmazottjának 3 hónapnál nem régebbi erkölcsi bizonyítvánnyal kell igazolnia büntetlen előéletét.

A *Minősített archiválási szolgáltató* a felvételi eljárás során ellenőrzi a jelentkező önéletrajzában megadott releváns információk valódiságát.

5.3.3. Képzési követelmények

A *Minősített archiválási szolgáltató* az újonnan felvett alkalmazottakat képzésben részesíti, amely során elsajátítják az adott munkakör ellátásához szükséges mértékben:

- a PKI alapismereteket;
- a *Minősített archiválási szolgáltató* informatikai rendszerének sajátosságait és kezelésének módját;
- a szerepkörük ellátásához szükséges speciális ismereteket;
- a *Minősített archiválási szolgáltató* nyilvános és belső szabályzataiban meghatározott folyamatokat, eljárásokat;
- az egyes tevékenységek jogi következményeit;
- az alkalmazandó informatikai biztonsági szabályokat;
- az adatvédelmi szabályokat.

A *Minősített archiválási szolgáltató* éles informatikai rendszereihez csak a képzést sikeresen teljesítő alkalmazottak kapnak hozzáférési jogosultságot.

5.3.4. Továbbképzési gyakoriságok és követelmények

A *Minősített archiválási szolgáltató* gondoskodik arról, hogy az alkalmazottak folyamatosan a megfelelő tudással rendelkezzenek, így szükség esetén továbbképzést, vagy ismétlő jellegű képzést kell tartani.

A *Minősített archiválási szolgáltató* továbbképzést tart, ha folyamataiban vagy informatikai rendszerében változás áll be.

A továbbképzés megfelelően dokumentálásra kerül, amelyből egyértelműen megállapítható a továbbképzés tematikája és a résztvevő dolgozók köre.

5.3.5. Munkabeosztás körforgásának sorrendje és gyakorisága

A *Minősített archiválási szolgáltató* nem alkalmaz kötelező jellegű körforgást az egyes munkabeosztások között.

5.3.6. Felhatalmazás nélküli tevékenységek büntető következményei

A *Minősített archiválási szolgáltató* a dolgozókkal kötendő munkaszerződésben szabályozza a dolgozók felelősségre vonásának lehetőségeit a dolgozó által elkövetett mulasztások, hibák, vétlen vagy szándékos károkozások esetére. Amennyiben egy munkatárs – szándékosan vagy gondatlanul – kötelezettségeit megsérti, vele szemben a *Minősített archiválási szolgáltató* szankciót alkalmazhat, amelyet az elkövetés módjára és következményeire tekintettel állapít meg. Szankcióként alkalmazható a jutalom megvonása, fegyelmi eljárás, elbocsátás, kinevezés visszavonása vagy büntetőjogi felelősségre vonás kezdeményezése.

Valamennyi bizalmi szerepkört betöltő munkatárs a szerepkörbe kinevezéskor a foglalkoztatási dokumentumok részeként:

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

A felsorolt dokumentumok tartalmazzák azokat a munkajogi következményeket és egyéb szankciókat, amelyek kötelezettségszegés esetén alkalmazhatóak.

5.3.7. Szerződéses viszonyban foglalkoztatottakra vonatkozó követelmények

A *Minősített archiválási szolgáltató* bizalmi munkakörben csak vele munkaviszonyban álló személyt alkalmaz.

Az egyéb feladatok ellátására alvállalkozói vagy megbízásos szerződésben foglalkoztatott szerződő személyeket a *Minősített archiválási szolgáltató* lehetőség szerint a korábban már minősített beszállítók listájáról választ. A beszállítókkal a *Minősített archiválási szolgáltató* a munkavégzést megelőzően írásban szerződést köt.

Valamennyi szerződő fél – még a tényleges munkavégzés megkezdése előtt – titoktartási nyilatkozatot ír alá, melyben vállalja, hogy a munkavégzés során későbbiekben megismert üzleti/vállalati titkokat illetéktelen személynek nem fedi fel, egyéb módon nem hasznosítja. A titoktartási nyilatkozat tartalmazza a megszegése esetén alkalmazandó szankciókat is. A szerződés alapján foglalkoztatott külső munkavállalókkal szemben elvárás a megfelelő szakismeret megléte, részükre a *Minősített archiválási szolgáltató* nem tart képzéseket.

5.3.8. A személyzet számára biztosított dokumentációk

A *Minősített archiválási szolgáltató* folyamatosan biztosítja a dolgozók részére a szerepkörük ellátásához szükséges aktuális dokumentációk, szabályzatok rendelkezésre állását.

Minden bizalmi munkakört betöltő munkatárs írásban megkapja a következő dokumentumokat:

- a *Minősített archiválási szolgáltató* szervezeti biztonsági szabályzata;
- aláírt titoktartási nyilatkozat;
- egyéni munkaköri leírás;
- a tervezett és rendkívüli továbbképzések alkalmával az adott oktatási formához tartozó oktatási segédanyagokat.

A szervezeti biztonsági szabályzatban bekövetkező változásokról írásos értesítő formájában minden dolgozó tájékoztatást kap.

5.4. Naplózási eljárások

A *Minősített archiválási szolgáltató* a biztonságos informatikai környezet fenntartása érdekében a teljes informatikai rendszerét átfogó eseménynaplózó és ellenőrző rendszert üzemeltet.

5.4.1. A tárolt események típusai

A *Minősített archiválási szolgáltató* az általánosan elfogadott informatikai biztonsági gyakorlatnak megfelelően naplóz minden olyan biztonsággal kapcsolatos eseményt, amely információt szolgáltathat az informatikai rendszerben vagy annak fizikai környezetében történt eseményekről, változásokról. Minden naplóbejegyzésnél eltárolja:

- az esemény időpontját;

- az esemény típusát;
- a végrehajtás sikerességét illetve sikertelenségét;
- a felhasználó vagy rendszer azonosítóját, aki/amely az eseményt kiváltotta.

Az összes lényeges naplóbejegyzést elérhetővé teszi a független rendszervizsgálók részére, akik a *Minősített archiválási szolgáltató* működésének megfelelőségét vizsgálják.

A *Minősített archiválási szolgáltató* naplózza minimálisan az alábbi eseményeket:

- ARCHIVÁLÁS
  - az e-akták feltöltésével és a bennük lévő aláírások ellenőrzésével 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;
- NAPLÓZÁS
  - a naplózó rendszer vagy egyes komponenseinek leállítása, újraindítása;
  - a naplózás bármilyen beállításának módosítása, mint pl. gyakoriság, riasztási küszöb érték, vizsgált esemény;
  - a tárolt naplózási adatok módosítása vagy törlése;
  - a naplózó rendszer hibája miatt végzett tevékenységek;
- RENDSZER BEJELENTKEZÉSEK
  - sikeres bejelentkezések, sikertelen bejelentkezési próbálkozások bizalmi szerepkörökbe;
  - jelszó alapú azonosítás esetén:
    - az engedélyezett sikertelen bejelentkezési próbálkozások számának megváltoztatása;
    - az engedélyezett sikertelen bejelentkezési próbálkozások számának elérése felhasználói bejelentkezéskor;
    - sikertelen bejelentkezések miatt zárolt felhasználó újbóli engedélyezése;
  - az azonosítási technika változtatása (például jelszó alapúról PKI alapúra);
- KULCSKEZELÉS

  - a szolgáltatói kulcsok teljes életciklusára vonatkozó valamennyi esemény (kulcsgenerálás, betöltés, elmentés stb.);

- TANÚSÍTVÁNY KEZELÉS
  - szolgáltatói *Tanúsítvány*ok kibocsátásával, állapotváltozásával kapcsolatos minden esemény;
- ADATMOZGÁSOK
  - bármilyen, a biztonság szempontjából kritikus adat manuális bevitele a rendszerbe;
  - a rendszer által fogadott, biztonsági szempontból fontos adatok, üzenetek;
- CA KONFIGURÁCIÓ
  - a CA tetszőleges komponensének átparaméterezése, a beállításon történt bármilyen változtatás;
  - felhasználók felvétele, törlése;
  - felhasználói szerepkörök, jogosultságok megváltoztatása;
  - a tanúsítvány profil megváltoztatása;
  - CRL profil megváltoztatása;
  - új CRL lista előállítása;
  - OCSP válasz generálása;
  - *Időbélyegző* generálása;
  - az előírt időpontossági küszöb túllépése;
- HSM
  - HSM installálása;
  - HSM eltávolítása;
  - HSM selejtezése, megsemmisítése;
  - HSM szállítása;
  - HSM tartalmának törlése (nullázás);
  - HSM feltöltése kulcsokkal, tanúsítványokkal;
- KONFIGURÁCIÓ VÁLTOZÁSA
  - hardver;
  - szoftver;

  - operációs rendszer;
  - javító csomag;

- FIZIKAI HOZZÁFÉRÉS, TELEPHELY BIZTONSÁG
  - személy belépése a CA komponenseket tartalmazó biztonsági területre és onnan kilépése;
  - hozzáférés egy CA rendszer komponenshez;
  - a fizikai biztonság ismert vagy gyanított megsértése;
  - tűzfal és router forgalmak;
- MŰKÖDÉSI RENDELLENESSÉGEK
  - rendszerösszeomlás, hardver hiba;
  - szoftveres hibák;
  - szoftverintegritás ellenőrzési hiba;
  - hibás vagy rossz helyre továbbított üzenetek;
  - hálózatot ért támadások, támadási kísérletek;
  - berendezés hiba;
  - elektromos hálózati üzemzavar;
  - szünetmentes tápegység hiba;
  - lényeges hálózati szolgáltatás hozzáférési hiba;
  - a *Minősített archiválási rend* vagy a *Minősített archiválási szolgáltatási szabályzat* megsértése;
  - operációs rendszer órájának törlése;
- EGYÉB ESEMÉNYEK
  - személy kinevezése biztonsági szerepkörbe;
  - operációs rendszer telepítése;
  - PKI alkalmazás telepítése;
  - rendszer elindítása;
  - belépési kísérlet a PKI alkalmazásba;
  - jelszó módosítási, beállítási kísérlet;
  - a belső adatbázis elmentése, visszaállítása mentésből;
  - fájl műveletek (pl. létrehozás, átnevezés, áthelyezés);
  - adatbázis hozzáférés.

5.4.2. A naplófájl feldolgozásának gyakorisága

A *Minősített archiválási szolgáltató* független rendszervizsgálói a keletkezett naplóbejegyzéseket minden munkanapon átvizsgálják.

A kiértékelés során meggyőződnek a vizsgált naplóállományok hitelességéről és sértetlenségéről, ellenőrzik a bejegyzésekben talált hibaüzeneteket, szükség esetén dokumentálják az eltérést és intézkedéseket hoznak az eltérés okának megszüntetése érdekében.

Az informatikai rendszerek ellenőrzésére a *Minősített archiválási szolgáltató* automatizált ellenőrző rendszereket is használ, amelyek előre beállított szempontok szerint folyamatosan figyelik a keletkező naplóbejegyzéseket és szükség esetén riasztják az üzemeltetés munkatársait.

A vizsgálat tényе, a vizsgálat eredményei és az esetleges feltárt hiányosságok elhárítása érdekében meghozott intézkedések megfelelően dokumentálásra kerülnek.

5.4.3. A naplófájl megőrzési időtartama

Az online rendszerből való kitörlés előtt a naplóállományokat a *Minősített archiválási szolgáltató* archiválja és gondoskodik azok biztonságos megőrzéséről az 5.5.2 fejezetben meghatározott ideig.

Ezen időtartamig a *Minősített archiválási szolgáltató* biztosítja az archivált adatok olvashatóságát, megőrzi az ehhez szükséges szoftver és hardver eszközöket.

5.4.4. A naplófájl védelme

A *Minősített archiválási szolgáltató* az előírt megőrzési ideig tárolja és védi a keletkezett naplóállományokat. A megőrzési idő teljes időtartama alatt biztosítja a naplóadatok:

- védelmét az illetéktelen felfedés ellen: a naplóállományokhoz csak az arra jogosultak – elsősorban a független rendszervizsgálók – férhetnek hozzá;
- rendelkezésre állását: a jogosultak számára biztosítja a naplóállományokhoz való hozzáférést;
- integritását: megakadályozza például a naplóállományokban bármilyen adat módosítását, törlését, bejegyzések sorrendjének megváltoztatását.

A *Minősített archiválási szolgáltató* a naplóbejegyzéseket minősített *Időbélyegző*vel 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 a *Minősített archiválási szolgáltató* gondoskodik az adatok bizalmas tárolásáról. A naplóállományokhoz való hozzáférésre csak azok jogosultak, akiknek erre munkakörük folytán feltétlenül szükségük van. A *Minősített archiválási szolgáltató* a hozzáféréseket biztonságos módon ellenőrzi. A naplóállományokat a *Minősített archiválási szolgáltató* biztonságos környezetben őrzi. Az állományokról a működés másodlagos helyszínén másolati példányokat is tart.

5.4.5. A naplófájl mentési eljárásai

Az üzemeltetés során az egyes rendszerekben folyamatosan keletkező naplóbejegyzésekből napi naplóállományok generálódnak.

A napi naplóállományokat a *Minősített archiválási szolgáltató* 2 példányban archiválja és a példányokat egymástól fizikailag elkülönülő helyszíneken az előírt ideig megőrzi.

A mentés operatív folyamatait a *Minősített archiválási szolgáltató* mentési szabályzatai írják le részletesen.

5.4.6. A naplózás adatgyűjtési rendszere

A naplóbejegyzéseket az egyes alkalmazások automatikusan gyűjtik és továbbítják a naplózó rendszer felé.

A naplózó funkciók automatikusan indulnak a rendszer indításakor és a rendszer működésének teljes időtartama alatt folyamatosan működnek.

Az automatikus vizsgáló és naplózó rendszerek működési rendellenessége esetén a *Minősített archiválási szolgáltató* felfüggeszti az érintett területek működését az üzemzavar elhárításáig.

5.4.7. Az eseményeket kiváltó alanyok értesítése

A hibaeseményt kiváltó személyeket, szervezeteket és alkalmazásokat a *Minősített archiválási szolgáltató* nem feltétlenül értesíti minden esetben, szükség esetén azonban bevonhatja őket az esemény kivizsgálásába. Az esemény kiváltásában érintett *Ügyfel*eknek ilyen esetben kötelességük a *Minősített archiválási szolgáltató*val való együttműködés a hiba feltárása érdekében.

5.4.8. Sebezhetőség felmérése

A naplóbejegyzések napi rendszerességgel végzett feldolgozásán túl a *Minősített archiválási szolgáltató* szakemberei havonta áttekintik a rendkívüli eseményeket és a sebezhetőségre vonatkozó elemzéseket végeznek, amely alapján a *Minősített archiválási szolgáltató* szükség esetén intézkedéseket hoz a rendszer biztonságának növelésére.

Minden nagyobb jelentőségű feltárt hiányosság vagy külső fenyegetettség esetén, de legalább évente egyszer a *Minősített archiválási szolgáltató* szakemberei átfogó sebezhetőség vizsgálatot végeznek, amely segítségével feltérképezik a potenciális belső és külső fenyegetettségeket, amelyek jogosulatlan hozzáféréseket eredményezhetnek.

A vizsgálat eredményei alapján a *Minősített archiválási szolgáltató* szükség esetén továbbfejleszti folyamatait, rendszereit a szolgáltatás általános biztonságának növelése érdekében.

5.5. Adatok archiválása

5.5.1. Az archivált adatok típusai

A *Minősített archiválási szolgáltató* felkészült elektronikus és papíralapú dokumentumok megfelelően biztonságos, hosszú idejű archiválására.

A *Minősített archiválási szolgáltató* minimálisan az alábbi jellegű információt archiválja:

- a *Minősített archiválási szolgáltató* akkreditációjával kapcsolatos valamennyi irat;
- a *Minősített archiválási rend*(ek) és *Minősített archiválási szolgáltatási szabályzat*(ok) valamennyi kibocsátott verziója;
- az Általános szerződési feltételek valamennyi kibocsátott verziója;
- a *Minősített archiválási szolgáltató* működésével kapcsolatos szerződések;
- valamennyi elektronikus és papíralapú naplóbejegyzés.

5.5.2. Az archívum megőrzési időtartama

A *Minősített archiválási szolgáltató* az archivált adatokat az alábbi időtartamokig őrzi meg:

- a *Minősített archiválási szolgáltatási szabályzat*ot a hatályon kívül helyezéstől számított 10 évig;

5.5.3. Az archívum védelme

A *Minősített archiválási szolgáltató* valamennyi archivált adatot két példányban, két egymástól fizikailag elkülönült helyszínen őrzi. Az egyetlen hiteles példányban rendelkezésre álló papíralapú dokumentumról hiteles papíralapú, vagy elektronikus másolatot készít a vonatkozó jogszabályok betartásával.

A két helyszín mindegyike teljesíti az archiválással szemben támasztott biztonsági és egyéb követelményeket.

Az archivált adatok megőrzése során a *Minősített archiválási szolgáltató* gondoskodik az archivált adatok

- sértetlenségének megőrzéséről;
- illetéktelen megismerés elleni védelméről;
- rendelkezésre állásáról;
- hitelességének megőrzéséről.

Az archivált elektronikus adatokat legalább fokozott biztonságú elektronikus aláírással vagy bélyegzővel és minősített *Időbélyegző*vel látja el.

5.5.4. Az archívum mentési folyamatai

A *Minősített archiválási szolgáltató* a papír alapú dokumentumokat egy eredeti példányban tárolja, a papíralapú eredetiről hiteles elektronikus másolatot készít a vonatkozó jogszabályok betartásával. Az elektronikus másolatokat a többi védendő elektronikus dokumentummal azonos szabályok szerint tárolja.

5.5.5. Az adatok időbélyegzésére vonatkozó követelmények

Valamennyi elektronikus naplóbejegyzés tartalmaz időjelzést, amelyen legalább másodperc pontossággal fel van tüntetve a rendszer által szolgáltatott időpont.

A *Minősített archiválási szolgáltató* biztosítja, hogy a szolgáltatást nyújtó rendszerein a gépidő maximum 1 másodpercre tér el a referenciaidőtől. Az időjel előállításához használt gépidőt naponta legalább négy alkalommal szinkronizálja az UTC időhöz.

A *Minősített archiválási szolgáltató* a napi naplóállományokat minősített *Időbélyegző*vel látja el.

Az archivált adatok megőrzése során szükség esetén (pl. algoritmusváltás, az eredeti *Időbélyegző* érvényességének lejárata) a *Minősített archiválási szolgáltató* gondoskodik az adatok hitelességének megőrzéséről.

5.5.6. Az archívum gyűjtési rendszere

A *Minősített archiválási szolgáltató* védett informatikai rendszerén belül keletkeznek a naplóbejegyzések, onnan csak az elektronikusan aláírt, minősített *Időbélyegző*vel védett naplóállományok kerülhetnek ki.

A szolgáltatás nyújtása során keletkezett papíralapú iratok egy eredeti példányát a *Minősített archiválási szolgáltató* az általa működtetett belső adattárban tárolja és őrzi.

5.5.7. Archív információk hozzáférését és ellenőrzését végző eljárások

A *Minősített archiválási szolgáltató* a naplóállományok előállítását automatikusan végzi, a hitelesített naplóállományokat naponta állítja elő.

Az archivált adatállományokat védi a jogosulatlan hozzáféréstől.

Az arra jogosultaknak biztosítja az archivált adatokhoz való ellenőrzött hozzáférést:

- az *Ügyfel*ek jogosultak a róluk tárolt adatok megtekintésére;
- jogi eljárásokban bizonyíték nyújtása céljából biztosítani kell a szükséges adatokat.

5.6. Kompromittálódást és katasztrófát követő helyreállítás

A *Minősített archiválási szolgáltató* katasztrófa esetén minden szükséges intézkedést meghoz annak érdekében, hogy a szolgáltatáskiesésből eredő károkat minimalizálja és a szolgáltatásokat a lehető legrövidebb időn belül helyreállítsa.

A bekövetkezett incidens kiértékelése alapján meghozza a szükséges módosító, javító intézkedéseket, hogy az incidens jövőbeli előfordulását megakadályozza.

A hiba elhárítása után az eseményt jelenti a Nemzeti Média- és Hírközlési Hatóságnak, mint felügyeleti szervnek.

5.6.1. Váratlan esemény és kompromittálódás kezelési eljárások

A *Minősített archiválási szolgáltató* rendelkezik üzletmenet folytonossági tervvel.

A *Minősített archiválási szolgáltató* kialakított és folyamatosan üzemben tart egy teljes értékű tartalékrendszert, amely az elsődleges helyszíntől biztonságos távolságra, földrajzilag különböző helyszínen található és önállóan is alkalmas a szolgáltatások teljes körű ellátására.

A *Minősített archiválási szolgáltató* folyamatosan teszteli a tartalékrendszer működését és évente felülvizsgálja az üzletmenet folytonossági terveit.

A *Minősített archiválási szolgáltató* megnövelt biztonságú eszközökkel és rendszerekkel rendelkezik a hardver- és szoftver meghibásodások valamint az adatsérülések okozta szolgáltatáskiesés minimalizálása érdekében. A szolgáltatások helyreállíthatóságát a *Minősített archiválási szolgáltató* háttérszerződései és saját tartalék eszközei garantálják.

A *Minősített archiválási szolgáltató* úgy alakította ki a minősített szolgáltatásokat nyújtó informatikai rendszerét, hogy bármely egy eszköz kiesése esetén képes zavartalanul folytatni a minősített szolgáltatások nyújtását.

5.6.2. Meghibásodott IT erőforrások, szoftverek és/vagy adatok

A *Minősített archiválási szolgáltató* informatikai rendszereit megbízható hardver és szoftver komponensekből építette fel. A kritikus funkciókat redundáns rendszerelemek alkalmazásával valósította meg úgy, hogy azok egy elem meghibásodása esetén is képesek legyenek a további működésre.

A *Minősített archiválási szolgáltató* naponta teljes mentést készít az adatbázisairól és a keletkezett naplózási eseményekről.

A *Minősített archiválási szolgáltató* olyan gyakorisággal készít teljes rendszermentést, amely biztosítja, hogy abból katasztrófa esetén a teljes szolgáltatás helyreállítható legyen.

A *Minősített archiválási szolgáltató* üzletmenet folytonossági terve pontos előírásokat tartalmaz a kritikus rendszerkomponensek meghibásodásának esetén végrehajtandó feladatokra.

A *Minősített archiválási szolgáltató* a hiba elhárítása és a rendszer integritásának helyreállítása után a lehető leghamarabb újraindítja a szolgáltatásait.

5.6.3. Működés folyamatosságának biztosítása katasztrófát követően

A *Minősített archiválási szolgáltató* üzletmenet folytonossági tervében meghatározta a természeti vagy egyéb katasztrófa miatt bekövetkezett szolgáltatás leállás esetén végrehajtandó feladatokat.

A katasztrófa bekövetkezése esetén haladéktalanul életbe lépteti a rendelkezéseket és megkezdi a károk elhárítását, a szolgáltatások helyreállítását.

A másodlagos szolgáltatási helyszín az elsődleges telephelytől olyan távolságra található, hogy egy valószínűsíthető katasztrófa ne érhesse mindkét helyszínt egyszerre.

A *Minősített archiválási szolgáltató* a lehető legrövidebb időn belül köteles értesíteni az érintett felhasználókat a katasztrófa bekövetkezéséről.

A szolgáltatások helyreállítása után a *Minősített archiválási szolgáltató* a lehető legrövidebb időn belül helyreállítja a katasztrófa során tönkrement eszközeit és az eredeti szolgáltatás biztonsági szintet.

5.7. Az Archiválási szolgáltatás leállítása

A *Minősített archiválási szolgáltató* a szolgáltatások valamelyikének tervezett megszüntetése esetén legkevesebb 60 nappal a szolgáltatás leállítását megelőzően értesíti a végfelhasználókat és a Nemzeti Média- és Hírközlési Hatóságot.

A *Minősített archiválási szolgáltató* a szolgáltatás leállítására vonatkozó bejelentéssel egyidejűleg leállítja a következő szolgáltatásait:

- Új e-akták befogadása az archívumba.

A *Minősített archiválási szolgáltató* a tervezett leállás előtt legalább 30 nappal felmondja a Szolgáltatási szerződéseket és felszólítja az *Előfizető*ket az archívumban tárolt e-aktáik letöltésére.
A *Minősített archiválási szolgáltató* a tervezett leállás előtt legalább 20 nappal leállítja a következő szolgáltatásait:

- Igazolások kiadása a tárolt e-aktákról

A leállás időpontjával egyidejűleg a *Minősített archiválási szolgáltató* a következő szolgáltatásokat állítja le:

- információ szolgáltatás,
- archívumban tárolt e-akták letöltése

A *Minősített archiválási szolgáltató* a tervezett megszűnés előtt tárgyalásokat kezd más vele azonos besorolású szolgáltatókkal szolgáltatásainak átvételéről. Nyilvántartásait a bizalmas felhasználói adatokkal együtt a 8.3 fejezet szerint mindenképpen átadja egy ilyen szolgáltatónak, vagy megállapodás hiányában a Nemzeti Média- és Hírközlési Hatóságnak, egyéb szolgáltatásait a tárgyalások eredményétől függően átadja vagy átadás nélkül megszünteti.

A szolgáltatás nyújtásához használt *Tanúsítvány*ok visszavonásáról (és a magánkulcsok megsemmisítéséről) – a tárgyalások eredményétől függően – a *Minősített archiválási szolgáltató* fokozatosan intézkedik a 60 napos időszakban.

A *Minősített archiválási szolgáltató* a tárgyalások végeredményéről tájékoztatja az *Ügyfel*eket és a Nemzeti Média- és Hírközlési Hatóságot. A *Minősített archiválási szolgáltató* az *Ügyfel*eket elektronikus levélben, az *Érintett felek*et a honlapján történő közzététel útján tájékoztatja.

A *Minősített archiválási szolgáltató* a szolgáltatás befejezésekor az informatikai rendszerében foglalt adatairól teljes körű, minősített *Időbélyegző*vel ellátott mentést készít.

A *Minősített archiválási 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 *Minősített archiválási szolgáltató* az *Előfizető*vel egyeztetett módon átadja az archivált fájlokat, aláírásokat, bélyegzőket és érvényességi láncokat az *Előfizető*nek, majd visszaállíthatatlan módon törli azokat az archívumából a 3.6. fejezetben leírt módon.

6. Műszaki biztonsági óvintézkedések

A *Minősített archiválási szolgáltató* módosítás ellen védett, megbízható, biztonságtechnikailag értékelt termékekből álló informatikai rendszereket használ szolgáltatásai nyújtásához. A *Minősített archiválási szolgáltató* a szolgáltatói kriptográfiai kulcsokat teljes életciklusuk alatt megfelelő tanúsítással rendelkező *Hardver kriptográfiai eszköz*ökben kezeli.

Mind a *Minősített archiválási szolgáltató*, mind a rendszert szállító és kivitelező vállalkozók jelentős tapasztalatokkal rendelkeznek hitelesítés-szolgáltatás kiépítésében és nemzetközileg elismert technológiát alkalmaznak.

A *Minősített archiválási szolgáltató* folyamatosan nyomon követi a kapacitás igényeket és a trendek felállításával becslést ad a jövőbeni várható kapacitás igényekre. Igény esetén gondoskodik a szűkös kapacitások bővítéséről, ezáltal biztosítja a szükséges feldolgozási és tárolási kapacitások folyamatos rendelkezésre állását.

6.1. A magánkulcsok védelme

A *Minősített archiválási szolgáltató* gondoskodik a birtokában lévő magánkulcsok biztonságos kezeléséről, megakadályozza a magánkulcsok felfedését, lemásolását, törlését, módosítását, jogosulatlan használatát. A *Minősített archiválási szolgáltató* csak addig őrzi a magánkulcsokat, ameddig azt a szolgáltatás nyújtása feltétlenül megköveteli.

A *Minősített archiválási szolgáltató* a használatból kivont *Hardver kriptográfiai eszköz*ökben tárolt magánkulcsokat kitörli az eszköz használati útmutatójában meghatározott módon, ami után gyakorlatilag lehetetlen a kulcsok visszaállítása.

6.1.1. Kriptográfiai modulra vonatkozó szabványok és előírások

A *Minősített archiválási szolgáltató* rendszerei a magánkulcsokat olyan biztonságos hardver eszközökben tárolják, amelyek:

- megfelelnek az ISO/IEC 19790 [20] követelményeinek,
- vagy megfelelnek a FIPS 140-2 [28] 3-as, illetve annál magasabb szintű követelményeknek,
- vagy megfelelnek a CEN 14167-2 [29] munkacsoport egyezmény követelményeinek,
- vagy olyan megbízható rendszerek, amely az MSZ/ISO/IEC 15408 [19] szerint, illetve azzal egyenértékű biztonsági kritériumok szerint 4-es vagy magasabb értékelési garancia szinten vannak értékelve. Az értékelésnek a jelen dokumentum követelményeinek megfelelő biztonsági rendszerterven, vagy biztonsági előirányzaton kell alapulnia.

A használt *Hardver kriptográfiai eszköz*ök megnevezése a 7. fejezetben található.

A *Minősített archiválási szolgáltató* a szolgáltatói magánkulcsokat a *Hardver kriptográfiai eszköz*ön kívül csak kódolt formában tárolja. A kódoláshoz csak az Eüt. [5] 92. § (1) b) szerint kiadott aktuális Nemzeti Média- és Hírközlési Hatóság határozat szerinti algoritmusokat és kulcsparamétereket használ, amelyek várhatóan a kulcs teljes élettartama alatt képesek ellenállni a kriptográfiai támadásoknak.

A *Minősített archiválási szolgáltató* a szolgáltatói magánkulcsokat kódolt formában is fizikailag biztonságos helyszínen tárolja az *Adatközpont* páncélszekrényében, ahol azokhoz csak az arra jogosultak férhetnek hozzá.

A *Minősített archiválási szolgáltató* a kriptográfiai algoritmusok vagy kulcsparaméterek gyengülése esetén a kódolt kulcsokat megsemmisíti vagy erősebb védelmet biztosító algoritmus és kulcsparaméterek felhasználásával tovább kódolja.

6.1.2. Magánkulcs többszereplős (n-ből m) használata

A *Minősített archiválási szolgáltató* alkalmazza az "n-ből m" ellenőrzést a magánkulcsokkal kapcsolatos kulcsgondozási funkciók aktivizálásánál. A paraméterek úgy lettek meghatározva, hogy a szolgáltatói magánkulcsaival végzett kritikus műveletek végrehajtásához legalább kettő, bizalmi szerepkört betöltő munkatárs egyidejű jelenlétére legyen szükség.

6.1.3. Magánkulcs letétbe helyezése

A *Minősített archiválási szolgáltató* nem helyezi letétbe saját szolgáltatói magánkulcsát.

6.1.4. Magánkulcs mentése

A *Minősített archiválási szolgáltató* minden szolgáltatói magánkulcsáról biztonsági másolatot készít még a magánkulcs használatbavételét megelőzően a 6.1.1. fejezetben leírtak szerint védett környezetben, legalább két bizalmi szerepkört betöltő személy együttes jelenlétében, más személyek kizárásával. A mentés során a magánkulcs titkosított formában hagyja el a modult, e titkosított kulcsot később másik modulba be lehet tölteni. Mind a mentés, mind a visszatöltés csakis a 6.1.2. fejezetben leírt védelmi mechanizmus mellett végezhető.

A *Minősített archiválási szolgáltató* a biztonsági másolatot legalább két példányban tárolja, ebből legalább az egyik példányt a szolgáltatás nyújtásától eltérő helyszínen.

A biztonsági másolatok kezelésére és megőrzésére ugyanolyan szigorú biztonsági előírások vonatkoznak, mint az éles rendszer üzemeltetésére.

6.1.5. Magánkulcs archiválása

A *Minősített archiválási szolgáltató* nem archiválja magánkulcsait.

6.1.6. Magánkulcs bejuttatása hardver kriptográfiai eszközbe, vagy onnan történő exportja

A *Minősített archiválási szolgáltató* valamennyi szolgáltatói magánkulcsát a követelményeknek megfelelő *Hardver kriptográfiai eszköz*ben állítja elő. A magánkulcsok nem léteznek nyílt formában a *Hardver kriptográfiai eszköz*ön kívül.

A *Minősített archiválási szolgáltató* a magánkulcsot csak biztonsági másolat készítése céljából exportálja a *Hardver kriptográfiai eszköz*ből.

A magánkulcs *Hardver kriptográfiai eszköz*ök közötti szállítása csak biztonsági másolat formájában engedélyezett.

A szolgáltatói magánkulcsok exportálása vagy betöltése minden esetben a 6.1.2. fejezetben leírt módon történik.

6.1.7. Magánkulcs tárolása hardver kriptográfiai eszközben

A *Minősített archiválási szolgáltató* a szolgáltatás nyújtásához használt magánkulcsait a 6.1.1. fejezet szerinti kriptográfiai modulokban tartja.

A *Hardver kriptográfiai eszköz*ben a magánkulcsokat az eszköz tanúsításában meghatározott módon tárolja és használja a vonatkozó kezelési utasítások maradéktalan betartásával.

6.1.8. A magánkulcs aktiválásának módja

A *Minősített archiválási szolgáltató* szolgáltatói magánkulcsait biztonságos *Hardver kriptográfiai eszköz*ben tárolja, a használat során betartja a *Hardver kriptográfiai eszköz* felhasználói útmutatójában és a tanúsítási dokumentumokban megfogalmazott követelményeket. A *Hardver kriptográfiai eszköz*t csak a hozzá tartozó operátori kártyákkal lehet aktiválni, a *Hardver kriptográfiai eszköz*ben lévő magánkulcsokat a modul aktiválása előtt nem lehet használni. A *Hardver kriptográfiai eszköz*höz tartozó operátori kártyákat a *Minősített archiválási szolgáltató* biztonságos környezetben tárolja és e kártyákat kizárólag a *Minősített archiválási szolgáltató* erre jogosult munkatársai érhetik el.

6.1.9. A magánkulcs deaktiválásának módja

A *Minősített archiválási szolgáltató* által használt hardver kriptográfia eszközök által kezelt magánkulcs akkor deaktiválódik, ha az eszköz (szabályos vagy szabálytalan módon) kikerül az aktív állapotból. Ez az alábbi esetekben következik be:

- a felhasználó deaktiválja a kulcsot,
- az eszköz áramellátása megszakad (kikapcsolás vagy tápellátási probléma),
- az eszköz hibaállapotba kerül.

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

6.1.10. A magánkulcs megsemmisítésének módja

A *Minősített archiválási szolgáltató* használatból kivont, lejárt érvényességű vagy kompromittálódott szolgáltatói magánkulcsait olyan módon semmisíti meg, amely lehetetlenné teszi a magánkulcs további használatát.

A *Minősített archiválási szolgáltató* a biztonságos *Hardver kriptográfiai eszköz*ében tárolt szolgáltatói magánkulcsok megsemmisítését a felhasznált *Hardver kriptográfiai eszköz* felhasználói útmutatójában és a tanúsítási dokumentumokban megfogalmazott eljárásoknak,

követelményeknek megfelelően végzi a *Minősített archiválási szolgáltató* két munkatársának (egy infrastruktúra adminisztrátor és egy biztonsági tisztviselő) együttes jelenlétében más személyek jelenlétének kizárásával.

6.1.11. A hardver kriptográfiai eszközök értékelése

A 6.1.1 fejezet előírásaival összhangban a *Minősített archiválási szolgáltató* valamennyi szolgáltatói magánkulcsát olyan *Hardver kriptográfiai eszköz*ben tárolja, amely:

- rendelkezik ISO/IEC 19790 [20] szerinti tanúsítással,
- vagy rendelkezik FIPS 140-2 Level 3 [28] szerinti tanúsítással,
- vagy rendelkezik a CEN 14167-2 [29] munkacsoport egyezmény követelményeinek való megfelelést igazoló Common Criteria alapú tanúsítvánnyal,
- vagy rendelkezik a Nemzeti Média- és Hírközlési Hatóság által vagy az Európai Unió valamely tagállamában nyilvántartásba vett, elektronikus aláírási termékek értékelésére jogosult független tanúsító szervezet által erre a célra kiadott igazolással.

6.2. Aktivizáló adatok

6.2.1. Aktivizáló adatok előállítása és telepítése

A *Minősített archiválási szolgáltató* a felhasznált *Hardver kriptográfiai eszköz* felhasználói útmutatójában és az eszköz tanúsítványban megfogalmazott eljárásoknak, követelményeknek megfelelő aktiváló módszereket alkalmaz szolgáltatói magánkulcsainak védelmére.

Jelszó alapú aktivizáló adatok használata esetén a jelszavak kellően bonyolultak a megkívánt védelmi szint biztosítása érdekében.

6.2.2. Az aktivizáló adatok védelme

A *Minősített archiválási szolgáltató* alkalmazottai a magánkulcsok aktiválásához szükséges eszközöket, aktivizáló adatokat biztonságosan kezelik, műszaki és szervezési intézkedések segítségével védik, a jelszavakat csak kódolt formában tárolják.

6.2.3. Az aktivizáló adatok kezelésének egyéb szempontjai

Nincs megkötés.

6.3. Informatikai biztonsági előírások

6.3.1. Speciális informatikai biztonsági műszaki követelmények

A *Minősített archiválási szolgáltató* informatikai rendszereinek konfigurálása és üzemeltetése során biztosítja az alábbi követelmények teljesülését:

- a rendszerhez vagy alkalmazáshoz való hozzáférés engedélyezése előtt a felhasználó azonosságát többfaktoros azonosítással ellenőrzi kártyán tárolt VPN tanúsítvány felhasználásával;
- a felhasználókhoz szerepköröket rendel és biztosítja, hogy minden felhasználó csak a szerepkörének megfelelő jogosultságokkal rendelkezzen;
- minden tranzakcióról naplóbejegyzést állít elő és a naplóbejegyzéseket archiválja;
- a biztonságkritikus folyamatok részére biztosítja, hogy a *Minősített archiválási szolgáltató* belső hálózati tartományai kellően védettek legyenek a jogosulatlan hozzáféréstől;
- megfelelő eljárásokat alkalmaz a kulcsvesztés vagy rendszerhiba után a szolgáltatás visszaállítása érdekében.

6.3.2. Az informatikai biztonság értékelése

A Microsec kiemelten fontosnak tartja *Ügyfel*ei elégedettségét. A magas színvonalú szolgáltatások fenntartása érdekében a Microsec e-Szignó Hitelesítés Szolgáltató ISO 9001 szabványnak megfelelő minőségirányítási rendszert üzemeltet 2002. január 23-a óta. A szabványnak való megfelelést a Lloyd's Register Quality Assurance tanúsította.

A Microsec nagy figyelmet szentel az általa üzemeltetett rendszerek biztonságára, ezért fő tevékenységi területein a ISO/IEC 27001-nek megfelelő információbiztonság-irányítási rendszert (korábban BS 7799) üzemeltet 2003. május 19. óta. A szabványnak való megfelelést a Lloyd's Register Quality Assurance tanúsította.

6.4. Életciklusra vonatkozó műszaki előírások

6.4.1. Rendszerfejlesztési előírások

A *Minősített archiválási szolgáltató* az éles szolgáltatást nyújtó informatikai rendszereiben csak olyan eszközöket, alkalmazásokat használ, amelyek:

- kereskedelmi dobozos szoftverek, amelyeket dokumentált tervezési módszertan szerint terveztek és fejlesztettek;

- a *Minősített archiválási szolgáltató* részére megbízható fél által kifejlesztett egyedi hardver és szoftver megoldások, amelyek tervezése során strukturált fejlesztési módszereket és ellenőrzött fejlesztési környezetet használtak;
- olyan nyílt forráskódú szoftverek, amelyek teljesítik a biztonsági követelményeket és amelyek megfelelőségét szoftver verifikáció, strukturált fejlesztés és életciklus menedzsment biztosítja.

Az informatikai eszközök beszerzése a hardver és szoftver komponensek módosítását kizáró módon történik, megbízható és rendszeresen minősített szállítók felhasználásával.

A *Minősített archiválási szolgáltató* a szolgáltatások nyújtásához használt kritikus informatikai eszközöket más célra nem használja.

A *Minősített archiválási szolgáltató* megfelelő védelmi intézkedésekkel megakadályozza, hogy kártékony szoftver kerülhessen a hitelesítés-szolgáltatás nyújtása körében használt eszközökbe.

A hardver és szoftver komponenseket az első használat előtt és azt követően rendszeresen ellenőrzi kártékony kódok után kutatva.

A *Minősített archiválási szolgáltató* a programfrissítések vásárlása vagy fejlesztése során ugyanolyan gondossággal jár el, mint az első verzió beszerzésekor.

A *Minősített archiválási szolgáltató* megbízható, megfelelően képzett személyzetet alkalmaz a szoftverek és eszközök telepítése során.

A *Minősített archiválási szolgáltató* csak a szolgáltatás nyújtásához szükséges szoftvereket telepíti a szolgáltatást nyújtó informatikai berendezéseire.

A *Minősített archiválási szolgáltató* rendelkezik változáskövető rendszerrel, amelyben az informatikai rendszer minden lényeges változtatása dokumentálásra kerül.

A *Minősített archiválási szolgáltató* a jogosulatlan változások észlelése érdekében automatikus monitorozó rendszert üzemeltet, amely rögzíti minden állomány változását és a figyelt állományok változása esetén naplóbejegyzést generál vagy figyelmeztető jelzést küld a rendszer üzemeltetőknek.

6.4.2. Biztonságkezelési előírások

A *Minősített archiválási szolgáltató* változáskövető rendszert használ a szolgáltatásban használt rendszerek telepítésének, konfigurációjának dokumentálására, üzemeltetésére, ellenőrzésére, monitorozására és karbantartására, beleértve a módosításokat és továbbfejlesztéseket is. A változáskövető rendszer alkalmas arra, hogy észleljen a rendszerben történt bármilyen jogosulatlan változtatást, adatbevitelt, amely érinti a szolgáltatásban használt rendszert, a tűzfalakat, routereket, programokat és egyéb komponenseket. A szolgáltatásban használt program telepítésekor a *Minősített archiválási szolgáltató* minden esetben meggyőződik arról, hogy a

telepítendő program a megfelelő verziójú és mentes mindenféle jogosulatlan módosítástól. A *Minősített archiválási szolgáltató* rendszeresen ellenőrzi a szolgáltatói rendszereiben használt programok integritását.

A *Minősített archiválási szolgáltató* által alkalmazott valamennyi *Hardver kriptográfiai eszköz* ellenőrzésre, bevizsgálásra és értékelésre került. A *Minősített archiválási szolgáltató* ellenőrzi a modulok sértetlenségét:

- az eszközök beszerzését követően az átvétel során,
- a használatbavételt közvetlenül megelőzően,
- rendszeresen az üzemeltetés során.

A használatból véglegesen vagy időlegesen kivont *Hardver kriptográfiai eszköz*ből a *Minősített archiválási szolgáltató* törli a szolgáltatói kulcsokat.

A *Minősített archiválási szolgáltató* a használaton kívüli *Hardver kriptográfiai eszköz*öket fizikailag védett helyszínen tárolja.

6.4.3. Életciklusra vonatkozó biztonsági előírások

A *Minősített archiválási szolgáltató* gondoskodik a felhasznált *Hardver kriptográfiai eszköz*ök védelméről azok teljes életciklusa alatt.

A szolgáltatások nyújtásához használt informatikai eszközök, rendszerek üzemeltetése során a *Minősített archiválási szolgáltató* figyelembe veszi az eszközök életciklusára vonatkozó biztonsági szempontokat, melyek szerint:

- megfelelő tanúsítással rendelkező *Hardver kriptográfiai eszköz*t használ rendszereiben;
- a *Hardver kriptográfiai eszköz* átvételekor a minőség ellenőrzése során meggyőződik róla, hogy a szállítás folyamán biztosították a *Hardver kriptográfiai eszköz*ök feltörés elleni védelmét;
- a *Hardver kriptográfiai eszköz*öket biztonságos helyen tárolja, a tárolás során biztosítja a *Hardver kriptográfiai eszköz*ök feltörés elleni védelmét;
- az üzemeltetés során folyamatosan betartja a *Hardver kriptográfiai eszköz* biztonsági előirányzatában, használati útmutatójában és a tanúsítási jelentésben szereplő követelményeket;
- a használatból kivont *Hardver kriptográfiai eszköz*ökben tárolt magánkulcsokat olyan módon törli, hogy lehetetlené válik a kulcsok visszaállítása.

6.5. Hálózati biztonsági előírások

A *Minősített archiválási szolgáltató* szigorú ellenőrzés alatt tartja az alkalmazott IT rendszereinek konfigurációját, minden változást dokumentál, beleértve a legkisebb módosítást, fejlesztést, szoftverfrissítést is. A *Minősített archiválási szolgáltató* megfelelő eljárásokat használ az IT rendszereiben bekövetkezett tetszőleges hardver vagy szoftver változás észlelésére, a rendszer telepítésére, karbantartására. A *Minősített archiválási szolgáltató* minden szoftverkomponens első betöltésekor ellenőrzi a komponens eredetiségét, integritását.

A *Minősített archiválási szolgáltató* megfelelő hálózatbiztonsági intézkedéseket alkalmaz, mint például:

- letiltja a használaton kívüli hálózati portokat és szolgáltatásokat;
- csak az IT rendszer megfelelő működéséhez feltétlenül szükséges hálózati alkalmazásokat futtat.

6.6. Időbélyegzés

A *Minősített archiválási szolgáltató* a naplóbejegyzések és egyéb archiválandó elektronikus állományok hitelesítésére az e-Szignó Hitelesítés Szolgáltató által kibocsátott minősített elektronikus *Időbélyegző*ket használja.

7. A megfelelőség vizsgálata

A *Minősített archiválási szolgáltató* tevékenységét az Európai Uniós szabályozással összhangban a Nemzeti Média- és Hírközlési Hatóság felügyeli. A Nemzeti Média- és Hírközlési Hatóság évente legalább egyszer átfogó helyszíni ellenőrzést tart a *Minősített archiválási szolgáltató* telephelyén. A helyszíni ellenőrzés előtt a *Minősített archiválási szolgáltató* külső auditor igénybevételével átvilágíttatja üzemeltetését és az átvilágításról készült részletes megfelelőségértékelési jelentést annak kézhezvételétől számított három munkanapon belül a Nemzeti Média- és Hírközlési Hatóságnak benyújtja. Az átvizsgálás során azt kell megállapítani, hogy a *Minősített archiválási szolgáltató* működése megfelel-e az eIDAS rendeletben [1] és a vonatkozó magyar jogszabályokban megállapított követelményeknek, valamint az alkalmazott *Minősített archiválási rend*(ek)ben és az ennek megfelelő *Minősített archiválási szolgáltatási szabályzat*(ok)ban támasztott követelményeknek.

Az átvilágítás tematikája és módszertana megfelel az alábbi normatív dokumentumoknak:

- AZ EURÓPAI PARLAMENT ÉS A TANÁCS 910/2014/EU RENDELETE (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről [1];

- ETSI EN 319 403 V2.2.2 (2015-08) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers; [13]
- ETSI EN 319 401 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [12]

A megfelelőségértékelési vizsgálat eredménye bizalmas dokumentum, csak az arra jogosultak számára hozzáférhető.

A megfelelőségértékelési jelentés alapján kiállított megfelelőségi tanúsítványt közzé kell tenni a *Minősített archiválási szolgáltató* honlapján.

A *Minősített archiválási szolgáltató* vizsgált és tanúsított elemeket (elektronikus aláírási termékeket, informatikai rendszerelemeket stb.) alkalmaz a szolgáltatásaihoz kapcsolódóan.

A *Minősített archiválási szolgáltató* az alábbi kriptográfiai modulokat használja szolgáltatói magánkulcsainak tárolására:

- nCipher nShield F3 PCI nC4032P-150, firmware verzió: 2.22.6-3;
- nChipher nShield F3 SCSI nC4032W-150, firmware verzió: 2.18.15-3;
- nChipher nShield F3 500e PCIe nC4033E-500, firmware verzió: 2.50.16-3 és 2.51.10-3.

A fenti eszközök FIPS 140-2 [28] Level 3 tanúsítással rendelkeznek.

A *Minősített archiválási szolgáltató* a szolgáltatások nyújtásához használt valamennyi rendszerelemet biztonsági osztályokba sorolta kockázatmenedzsment rendszere alapján. Ezen rendszerelemekről és a hozzájuk tartozó biztonsági besorolásról a *Minősített archiválási szolgáltató* a kockázatmenedzsment rendszere keretében nyilvántartást vezet.

A *Minősített archiválási szolgáltató* a külső auditon túl saját belső ellenőrzési rendszerrel is rendelkezik, amely segítségével rendszeresen vizsgálja a korábbi auditoknak való megfelelőséget és eltérés esetén megteszi a szükséges lépéseket.

A *Minősített archiválási szolgáltató* 2002 óta rendelkezik az ISO 9001 szabványnak megfelelő minőségirányítási, valamint 2003 óta a ISO/IEC 27001-nek (korábban BS 7799-nek) megfelelő információbiztonság-irányítási rendszerrel, amelyeket külső auditáló szervezet (Lloyd's Register Quality Assurance) auditál és vizsgál felül folyamatosan (lásd: 1.3.1. fejezet).

7.1. Az ellenőrzések körülményei és gyakorisága

A *Minősített archiválási szolgáltató* évente külső megfelelőségértékelési auditot hajt végre a szolgáltatások nyújtását végző informatikai rendszerén.

7.2. Az auditor és szükséges képesítése

A *Minősített archiválási szolgáltató* a belső auditokat a független rendszervizsgáló szerepkörrel felruházott alkalmazottai segítségével rendszeresen végzi.

Az eIDAS és ETSI követelményeknek való megfelelőséget igazoló vizsgálatot olyan szervezet végezheti el, amely rendelkezik egy EU tagállam nemzeti akkreditációs szervezete által kiadott erre feljogosító felhatalmazással.

7.3. Az auditor és az auditált rendszerelem függetlensége

A külső auditot olyan személy végzi:

- aki független a vizsgált *Minősített archiválási szolgáltató* tulajdonosi körétől, vezetőségétől és üzemeltetésétől;
- aki független a vizsgált szervezettől, vagyis sem saját maga, sem közvetlen hozzátartozója nincs munkaviszonyban vagy üzleti kapcsolatban a *Minősített archiválási szolgáltató*val;
- akinek díjazása nem függ az audit során végzett tevékenységének megállapításaitól.

7.4. Az auditálás által lefedett területek

Az átvizsgálás lefedi az alábbi területeket:

- hatályos jogszabályoknak való megfelelés;
- műszaki szabványoknak való megfelelés;
- *Minősített archiválási rend*(ek)nek és *Minősített archiválási szolgáltatási szabályzat*(ok)nak való megfelelés;
- az alkalmazott folyamatok megfelelősége;
- a dokumentálás;
- a fizikai biztonság;
- a személyi állomány megfelelősége;
- az IT biztonság;
- az adatvédelmi szabályok betartása.

7.5. A hiányosságok kezelése

A független auditor az átvizsgálás eredményét egy részletes átvilágítási jelentésben foglalja össze, amely kitér a vizsgált rendszerelemekre, folyamatokra, tartalmazza az átvilágítás során felhasznált bizonyítékokat és vizsgálói megállapításokat. A jelentésben külön fejezetben rögzíti a vizsgálat során feltárt eltéréseket és az elhárításukra kitűzött határidőket. A független auditor a vizsgálat során feltárt eltérések, hiányosságok súlyossága alapján a jelentésben rögzíthet:

- opcionálisan figyelembe vehető módosítási javaslatokat;
- kötelezően elhárítandó eltéréseket.

A független auditornak a feltárt súlyos eltéréseket haladéktalanul jelentenie kell a Nemzeti Média- és Hírközlési Hatóságnak, aki jogosult meghozni a szükséges intézkedéseket.

A *Minősített archiválási szolgáltató* köteles a független vizsgáló által felvetett problémákra írásban válaszolni, az elhárításukra tett intézkedésekről a következő hatósági szemle alkalmával beszámolni.

A független auditornak a vizsgálati jelentést minden esetben meg kell küldenie a Nemzeti Média- és Hírközlési Hatóságnak.

7.6. Az eredmények közzététele

A *Minősített archiválási szolgáltató* a vizsgálat eredményét összefoglaló jelentést nyilvánosságra hozza. A feltárt hiányosságok részleteit nem publikálja, azokat bizalmas információként kezeli.

8. Egyéb üzleti és jogi kérdések

8.1. Díjak

A szolgáltatási díjakat és árakat a *Minősített archiválási szolgáltató* a honlapján közzéteszi és kérelemre nyomtatott formában ügyfélszolgálati irodájában is biztosítja olvashatóságát.

A *Minősített archiválási szolgáltató* az árlistát egyoldalúan módosíthatja. Az árlista módosítását a hatályba lépése előtt 15 nappal a *Minősített archiválási szolgáltató* a honlapján közzéteszi. Az előre kifizetett szolgáltatások árát a módosítás nem érinti.

A díjak kifizetésével és visszatérítésével kapcsolatos rendelkezéseket a Szolgáltatási szerződés és mellékletei – különösen az Általános szerződési feltételek – tartalmazzák.

8.1.1. Visszatérítési politika

Lásd: 8.1. fejezet.

8.2. Anyagi felelősségvállalás

A *Minősített archiválási szolgáltató* megbízhatósága érdekében anyagi felelősséget vállal a jelen *Hitelesítési rend*ben, a vonatkozó *Minősített archiválási szolgáltatási szabályzat*ban valamint az *Ügyfél*lel kötött Szolgáltatási szerződésben megfogalmazott valamennyi rá vonatkozó kötelezettség maradéktalan betartásáért.

8.2.1. Pénzügyi követelmények

A *Minősített archiválási szolgáltató* pénzügyi felelőssége, valamint a megszűnésével kapcsolatos költségek biztosítása és a megbízhatóság érdekében a jogszabályi előírásoknak megfelelő óvadékkal rendelkezik.

8.2.2. Felelősségbiztosítás

A *Minősített archiválási szolgáltató* megbízhatósága érdekében felelősségbiztosítással rendelkezik.

8.3. Bizalmasság

A *Minősített archiválási szolgáltató* az *Ügyfel*ek adatait a jogszabályoknak megfelelően kezeli. A *Minősített archiválási szolgáltató* rendelkezik adatkezelési szabályzattal (lásd 8.4 fejezet), amely a személyes adatok kezelésével kiemelten foglalkozik.

Az *Ügyfél* a Szolgáltatási szerződés aláírásával hozzájárul ahhoz, hogy a személyes adatait a *Minősített archiválási szolgáltató* (az adatkezelési szabályzatnak megfelelő módon) tárolja és kezelje. A hozzájárulás vonatkozik a törvény által meghatározott és nyilvántartásba vett információk harmadik félhez történő továbbítására a *Minősített archiválási szolgáltató* szolgáltatásainak leállítása esetén, valamint – kizárólag a szolgáltatással összefüggő feladatok elvégzése céljából – a *Minősített archiválási szolgáltató* alvállalkozóinak való továbbításra. A *Minősített archiválási szolgáltató* az *Ügyfel*ek adatait kizárólag a szolgáltatásaival összefüggésben használja fel.

A *Minősített archiválási szolgáltató* a tudomására jutott adatokat a jogszabályi követelményeknek megfelelően, az előírt időtartamig megőrzi. A *Minősített archiválási szolgáltató* az adatok megőrzése során gondoskodik az információk sértetlenségéről, bizalmasságáról és biztonságos tárolásáról. Az információkhoz való hozzáférést csak azon személyeknek engedélyezi, akik feladata azt indokolja.

A *Minősített archiválási szolgáltató* az *Ügyfel*ek adatainak továbbítása során gondoskodik a nem nyilvános információk bizalmasságáról és sértetlenségéről.

8.3.1. Bizalmas információk köre

A *Minősített archiválási szolgáltató* bizalmas információként kezeli:

- az *Ügyfel*ek minden adatát, kivéve azokat, amelyeket a 8.3.2. fejezetben nem bizalmasnak tekintett információnak minősít;
- az *Ügyfel*ek adatain kívül:
  - az *Előfizető*k archívumban tárolt e-aktáita hozzájuk tartozó érvényességi láncokkal és egyéb meta adatokkal;
  - a tranzakciós és naplóadatokat;
  - a nem nyilvános szabályzatokat;
  - minden olyan adatot, amelynek nyilvánosságra hozatala a szolgáltatás biztonságát előnytelenül befolyásolná.

8.3.2. Bizalmas információk körén kívül eső adatok

A *Minősített archiválási szolgáltató* nyilvánosnak tekint miden olyan adatot, amely nyilvánosan elérhető forrásból beszerezhető, vagy amely nyilvánosságra hozatalához az *Előfizető* előzetesen írásban hozzájárult.

8.3.3. Bizalmas információ védelme

A *Minősített archiválási szolgáltató* felelősséggel tartozik az általa kezelt bizalmas adatok védelméért.

A *Minősített archiválási szolgáltató* szerződésben vagy titoktartási nyilatkozat aláírásával kötelezi alkalmazottait, alvállalkozóit, szerződött partnereit a bizalmas adatok védelmére.

A *Minősített archiválási szolgáltató* a birtokába jutott bizalmas adatokat az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény [3] rendelkezéseinek megfelelően kezeli, és kizárólag az alábbi esetekben fedi fel azokat:

- **Információszolgáltatás a hatóságok részére**

  A *Minősített archiválási szolgáltató* az Eüt. [5] 90. § (1) bekezdésének megfelelően az általa nyújtott bizalmi szolgáltatások felhasználásával elkövetett bűncselekmények felderítése vagy megelőzése céljából, illetőleg nemzetbiztonsági érdekből – az adatigénylésre külön törvényben meghatározott feltételek teljesülése esetén – a nyomozó hatóságnak és a nemzetbiztonsági szolgálatoknak díjmentesen továbbítja az

érintett személyazonosságát igazoló, valamint a *Minősített archiválási szolgáltató* által egyeztetett adatokat.

A *Minősített archiválási szolgáltató* rögzíti az adatátadás tényét, de arról nem tájékoztatja az érintett *Ügyfel*eket.

- **A tulajdonos kérésére történő felfedés**

  A *Minősített archiválási szolgáltató* az *Ügyfél* személyes kérése vagy az általa hivatalosan, írásban adott felhatalmazása alapján tárja fel a rá vonatkozó bizalmas felhasználói információkat harmadik fél részére.

8.4. Személyes adatok védelme

A *Minősített archiválási szolgáltató* gondoskodik az általa kezelt személyes adatok védelméről, működése és szabályzatai megfelelnek az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény [3] rendelkezéseinek.

A *Minősített archiválási szolgáltató* az *Ügyfél*ről nyilvántartott személyes adatokat és információkat a jogszabályi előírásoknak megfelelően

- megőrzi,
- azokat a megőrzési kötelezettség lejártával – amennyiben az *Ügyfél* erről másképpen nem rendelkezik – az ügyfél adatbázisból törli.

A *Minősített archiválási szolgáltató* nyilvántartásában azonosító adatokat, az *Előfizető*ről kizárólag a szolgáltatás igénybevételéhez, valamint a szerződéskötéshez és a számlázáshoz szükséges információkat tárolja.

A *Minősített archiválási szolgáltató* kizárólag olyan esetben adja át harmadik félnek az *Ügyfél* adatait, ha ezt jogszabály előírja vagy ha az *Ügyfél* ebbe írásban beleegyezett.

8.4.1. Adatkezelési szabályzat

A *Minősített archiválási szolgáltató* rendelkezik adatkezelési szabályzattal, amely részletes előírásokat tartalmaz a személyes adatok kezelésére. Az adatkezelési szabályzat megtalálható az e-Szignó Hitelesítés Szolgáltató honlapján az alábbi linken:

`https://e-szigno.hu/letoltesek/dokumentumok-es-szabalyzatok/`

8.4.2. Személyes adatok

A *Minősített archiválási szolgáltató* védi az érintettel kapcsolatba hozható, vagy az érintettre vonatkozó következtetést tartalmazó minden olyan személyes adatot, amely nem érhető el nyilvános adatforrásból.

A *Minősített archiválási szolgáltató* csak az *Előfizető*től közvetlenül, vagy annak egyértelmű előzetes hozzájárulásával gyűjt személyes adatokat és csak olyan mértékben, ami a szolgáltatás nyújtásához szükséges.

8.4.3. Személyes adatnak nem minősülő adatok

A *Minősített archiválási szolgáltató* nem köteles bizalmasként kezelni az olyan személyes adatot, amely nyilvános adatforrásból elérhető.

8.4.4. Személyes adatok védelme

A *Minősített archiválási szolgáltató* biztonságosan tárolja és védi az általa kezelt személyes adatokat. Az adatokat megfelelő intézkedésekkel védi különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, valamint nyilvánosságra hozatal ellen.

A *Minősített archiválási szolgáltató* általánosan felelős az Adatkezelési szabályzatában leírtak betartásáért, felelőssége kiterjed az alvállalkozói által végzett tevékenységekre is.

8.4.5. Személyes adatok felhasználása

A *Minősített archiválási szolgáltató* csak a szolgáltatás nyújtásához megkívánt mértékben, az *Ügyfél*lel való kapcsolattartás érdekében használja fel az *Ügyfél* személyes adatait.

8.4.6. Adatkezelés

A *Minősített archiválási szolgáltató* az *Ügyfél* értesítése nélkül is kiadhatja az *Ügyfél*ről tárolt személyes adatokat a vonatkozó jogszabályok által meghatározott esetekben.

8.4.7. Egyéb adatvédelmi követelmények

Nincs előírás.

8.5. Szellemi tulajdonjogok

A *Minősített archiválási szolgáltató* működése során nem sértheti meg harmadik személy szellemi tulajdonjogait.

A jelen *Minősített archiválási szolgáltatási szabályzat* a *Minősített archiválási szolgáltató* kizárólagos tulajdonát képezi. Az *Ügyfel*ek, *Igénylő*k és egyéb *Érintett felek* a dokumentumot csak a jelen *Minősített archiválási szolgáltatási szabályzat* előírásainak megfelelően jogosultak felhasználni, minden egyéb kereskedelmi vagy egyéb célú felhasználás szigorúan tilos.

A jelen *Minősített archiválási szolgáltatási szabályzat* szabadon terjeszthető, de csak változatlan formában, teljes terjedelemben és az eredet feltüntetésével.

A *Minősített archiválási szolgáltató* által a szolgáltatás igénybevételéhez biztosított szoftverek használatának szabályait a szoftver leírásában vagy magában a szoftverben elérhető illetve ott meghivatkozott helyen található felhasználói útmutató tartalmazza.

8.6. Tevékenységért viselt felelősség és helytállás

8.6.1. A szolgáltató felelőssége és helytállása

A Szolgáltató felelőssége

A *Minősített archiválási szolgáltató* felelősségét jelen *Minősített archiválási szolgáltatási szabályzat*, a vonatkozó *Minősített archiválási rend*, valamint az *Ügyfél*lel kötött Szolgáltatási szerződés és annak mellékletei tartalmazzák, melyek szerint:

- a *Minősített archiválási szolgáltató* felelősséget vállal az általa támogatott *Minősített archiválási rend*(ek)ben leírt eljárásoknak való megfelelésért;
- a *Minősített archiválási szolgáltató* sajátjaként felel az alvállalkozói által a szolgáltatás nyújtása során okozott károkért;
- a *Minősített archiválási szolgáltató* a vele szerződéses jogviszonyban álló *Ügyfel*ekkel szemben a Polgári Törvénykönyv [4] a szerződésszegésért való felelősség szabályai szerint felelős;
- a *Minősített archiválási szolgáltató* a vele szerződéses jogviszonyban nem álló harmadik személlyel (ilyen az *Érintett fél*) szemben a Polgári Törvénykönyv [4] általános felelősségi szabálya szerint felelős;
- a *Minősített archiválási szolgáltató* a felelősségi körén belül keletkezett, bizonyított károkért a szabályzataiban és az *Ügyfél*lel megkötött Szolgáltatási szerződésekben rögzített korlátozásokkal kártérítést fizet (lásd: Pénzügyi felelősség korlátozása 8.8. fejezet);
- ha egy biztosítási eseménnyel kapcsolatban több jogosult megalapozott kártérítési igénye meghaladja a károkra biztosítási eseményenként a felelősségbiztosítási szerződésben meghatározott összeget, akkor a kártérítési igények megtérítése az összes kártérítési igénynek a felelősségbiztosítási szerződésben meghatározott összeghez viszonyított arányában történik.

A *Minősített archiválási szolgáltató* nem felelős:

- az *Érintett felek* tanúsítvány ellenőrzési és felhasználási tevékenységeiért,
- az *Érintett felek* vagy mások által kibocsátott szabályzatokért.

A Szolgáltató kötelezettsége

A *Minősített archiválási szolgáltató* köteles teljesíteni az eIDAS rendelet [1] 24. cikkének (2) bekezdésében foglalt követelményeket.

A *Minősített archiválási szolgáltató* alapvető kötelezettsége, hogy a szolgáltatásokat a *Minősített archiválási rend*del, a *Minősített archiválási szolgáltatási szabályzat*tal és egyéb nyilvános szabályzatokkal, a szerződéses feltételekkel, továbbá a vállalati és biztonsági 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 szolgáltatásokhoz kapcsolódó szervezetek (hitelesítő szervezet, ügyfélszolgálat stb.) folyamatos működtetése és ellenőrzése;
- 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 publikus nyilvántartások és saját szabályzatok karbantartása és folyamatos elérhetővé tétele bárki számára az interneten keresztül.

8.6.2. Az Ügyfél felelőssége és helytállása

Az *Előfizető* felelőssége

Az *Előfizető* felelősségét a Szolgáltatási szerződés és annak mellékletei (köztük az Általános szerződési feltételek) határozzák meg.

Az *Előfizető* kötelezettségei

Az *Előfizető* köteles a *Minősített archiválási szolgáltató* szerződéses feltételeinek és szabályzatainak megfelelően eljárni a szolgáltatás igénybevétele során.

Az *Előfizető* kötelezettségeit a jelen *Minősített archiválási szolgáltatási szabályzat*, a Szolgáltatási szerződés és annak elválaszthatatlan részét képező Általános szerződési feltételek és egyéb dokumentumok, valamint a vonatkozó *Minősített archiválási rend* tartalmazzák.

Az *Előfizető* jogai

Az *Előfizető* jogosult:

- a szolgáltatások igénybevételére a jelen *Minősített archiválási szolgáltatási szabályzat*ban leírtak szerint;

8.6.3. Az Érintett fél felelőssége

Az *Érintett felek* saját belátásuk és/vagy szabályzataik alapján dönthetnek az egyes *Tanúsítvány*ok és *Időbélyegző*k elfogadásáról és a felhasználás módjáról. Az érvényesség vizsgálata során a *Minősített archiválási szolgáltató* által garantált biztonsági szint megtartásához szükséges, hogy az *Érintett fél* megfelelő körültekintéssel járjon el, ezért különös tekintettel javasolt:

- a *Minősített archiválási rend*ben és a *Minősített archiválási szolgáltatási szabályzat*ban megfogalmazott követelmények, előírások betartása;
- megbízható informatikai környezet és alkalmazások használata;
- visszavonási állapotának ellenőrzése az aktuális CRL vagy OCSP válasz alapján;
- felhasználására vonatkozó valamennyi korlátozás figyelembevétele, amely a jelen *Minősített archiválási rend*ben és a *Minősített archiválási szolgáltatási szabályzat*ban szerepel.

8.6.4. Egyéb szereplők tevékenységéért viselt felelősség és helytállás

Nincs megkötés.

8.7. Helytállás érvénytelenségi köre

A *Minősített archiválási szolgáltató* kizárja felelősségét, amennyiben:

- az *Érintett fél* nem körültekintően jár el a *Tanúsítvány*ok az *Időbélyegző*k felhasználása vagy ellenőrzése során, azaz nem a jelen *Minősített archiválási szolgáltatási szabályzat*, a *Minősített archiválási rend* vagy a hatályos jogszabályok szerint jár el;

- az *Érintett felek* vagy mások által kibocsátott szabályzatok nem felelnek meg a jelen *Minősített archiválási szolgáltatási szabályzat*nak vagy a *Minősített archiválási rend*nek;
- az Internet, vagy annak egy részének működési hibájából adódóan a tájékoztatás és egyéb kommunikációs kötelezettségeit nem tudja ellátni;
- a károkozás a Nemzeti Média- és Hírközlési Hatóság algoritmusokkal kapcsolatos határozat által elfogadott kriptográfiai algoritmusok hibájából, illetve gyengeségeiből ered.

8.8. A felelősség korlátozása

Nincs megkötés.

8.9. Kártérítési kötelezettség

8.9.1. A szolgáltató kártérítési kötelezettsége

A *Minősített archiválási szolgáltató* kártérítési kötelezettségének részletes szabályait jelen szabályzat (lásd: 8.8. fejezet), a Szolgáltatási szerződés és az *Ügyfel*ekkel kötött szerződések tartalmazzák.

8.9.2. Az előfizető kártérítési kötelezettsége

Az *Előfizető* kártérítési felelősséggel tartozik a *Minősített archiválási szolgáltató*nak azokért a veszteségekért és károkért, amelyeket kötelezettségei és a rá vonatkozó ajánlások be nem tartásával okoz számára.

8.9.3. Az érintett felek kártérítési kötelezettsége

Lásd: 8.8. fejezet

8.10. Érvényesség és megszűnés

8.10.1. Érvényesség

A *Minősített archiválási szolgáltatási szabályzat* adott verziója hatályba lépésének napja a dokumentum címlapján kerül meghatározásra.

8.10.2. Megszűnés

A *Minősített archiválási szolgáltatási szabályzat* visszavonásig hatályos időbeli korlátozás nélkül.

8.10.3. A megszűnés következményei

A *Minősített archiválási szolgáltatási szabályzat* visszavonása esetén a *Minősített archiválási szolgáltató* honlapján közzéteszi a visszavonás részletes szabályait és a visszavonás után is fennálló jogokat és kötelezettségeket.

A *Minősített archiválási szolgáltató* garantálja, hogy a *Minősített archiválási szolgáltatási szabályzat* visszavonása esetén is érvényben maradnak a bizalmas adatok védelmére vonatkozó előírások.

8.11. A felek közötti kommunikáció

A *Minősített archiválási szolgáltató* az *Ügyfel*ekkel történő kapcsolattartás érdekében ügyfélszolgálati irodát működtet.

Az *Ügyfel*ek jognyilatkozataikat a *Minősített archiválási szolgáltató* felé kizárólag írásban, aláírt módon tehetik meg. Szervezet képviseletében történő aláírás csak a képviseleti jogosultság igazolásával együtt érvényes.

Az e-Szignó Hitelesítés Szolgáltató elektronikus levélben tájékoztatja *Ügyfel*eit vagy tájékoztatását honlapján teszi közzé.

8.12. Módosítások

A *Minősített archiválási szolgáltató* fenntartja magának a jogot, hogy a normatív szabályok, biztonsági követelmények, piaci környezet vagy egyéb körülmények változása esetén szabályozott módon megváltoztassa a *Minősített archiválási szolgáltatási szabályzat*ot.

Rendkívüli esetben (pl. kritikus biztonsági intézkedések meghozatalának szükségessége) a változások azonnali hatállyal is életbe léptethetők.

8.12.1. Módosítási eljárás

A *Minősített archiválási szolgáltató* nyilvános szabályzataiban csak azon eljárásait hozza nyilvánosságra, melyek ismerete a szolgáltatások biztonságát nem veszélyezteti. A *Minősített archiválási szolgáltató* több belső biztonsági és egyéb szabályzattal, operatív szintű előírással rendelkezik, melyeket bizalmasan kezel (jelen *Minősített archiválási szolgáltatási szabályzat* több ilyet is megemlít). A 7.4. fejezetben leírt eljárások ezeket a dokumentumokat is vizsgálják.

A *Minősített archiválási szolgáltató* hitelesítő szervezetén belül működik egy olyan szervezeti egység, amely felelős a szabályzatok és dokumentációk karbantartásáért. A változtatási igényeket e csoport gyűjti, a módosításokat elvégzi, a belső és külső tájékoztatási kötelezettségeknek eleget tesz. A szabályzatot az e-Szignó Hitelesítés Szolgáltató igazgatója hagyja jóvá.

A változtatásokat gyűjtve a csoport belső, nem nyilvános munkaváltozatokat hoz létre a szabályzatokból, melyek a közzététel előtt belső felülvizsgálaton esnek át. A *Minősített archiválási szolgáltató* törekszik arra, hogy új szabályzatot csak a lehető legritkábban kelljen kibocsátania.

A *Minősített archiválási szolgáltató* évi rendszerességgel illetve rendkívüli változtatási igény esetén soron kívül átvizsgálja a *Minősített archiválási szolgáltatási szabályzat*ot és elvégzi a szükségesnek tartott változtatásokat. A dokumentum a legkisebb változtatás után is új verziószámot kap és az elfogadási procedúra időigényét figyelembe véve meghatározásra kerül a tervezett hatálybalépés időpontja is.

A jóváhagyott dokumentumot legalább 30 nappal a tervezett hatálybalépés előtt véleményezésre megküldi a Nemzeti Média- és Hírközlési Hatóság részére és publikálásra kerül a *Minősített archiválási szolgáltató* honlapján.

A *Minősített archiválási szolgáltató* a közzétett új szabályzat tervezettel kapcsolatos észrevételeket a hatályba lépést megelőző 14. napig fogadja az alábbi címen:

`info@e-szigno.hu`

Érdemi változtatást igénylő észrevétel esetén a dokumentumot megváltoztatja.

A szabályzat észrevételekkel módosított változatát a *Minősített archiválási szolgáltató* a hatályba lépést megelőző 7. napon zárja le és teszi közzé.

8.12.2. Értesítések módja és határideje

A *Minősített archiválási szolgáltató* a 8.12.1. pontban leírtak szerint értesíti az *Érintett felek*et az új dokumentum verziók kibocsátásáról.

8.12.3. Az OID megváltoztatása

A *Minősített archiválási szolgáltató* a *Minősített archiválási szolgáltatási szabályzat* legkisebb változtatása esetén is új verziószámot ad ki, ami része a dokumentum azonosítónak (OID), így a dokumentum minden változása az OID változását eredményezi, vagyis két eltérő tartalmú – hatályba léptetett – dokumentumnak nem lehet azonos OID azonosítója.

8.13. Vitás kérdések rendezése

A *Minősített archiválási szolgáltató* törekszik a működése során felmerülő vitás kérdések békés, tárgyalásos rendezésére. A rendezés során a fokozatosság elvét követi.

A *Minősített archiválási szolgáltató* és az *Ügyfél* kölcsönösen megállapodnak abban, hogy bármilyen vitás kérdés vagy panasz felmerülése esetén, a vita jogi útra való terelése előtt megkísérlik a békés úton, tárgyalással történő egyeztetést. A kezdeményező fél kötelessége, hogy minden érintett többi felet haladéktalanul értesítsen és teljes körűen tájékoztasson az ügy minden vonatkozását illetően.

A *Minősített archiválási szolgáltató* tevékenységével kapcsolatos kérdéseket, kifogásokat és panaszokat az ügyfélszolgálati iroda címére kell eljuttatni írásos formában. A bejelentés kézhezvételétől számított 3 munkanapon belül a *Minősített archiválási szolgáltató* értesíti a bejelentő felet az általa megadott címen a bejelentés fogadásáról és a kivizsgáláshoz szükséges időről. A megjelölt határidőig a *Minősített archiválási szolgáltató* köteles írásban válaszolni a bejelentőnek. A *Minősített archiválási szolgáltató* a válaszadáshoz szükséges információk megadását kérheti a bejelentőtől. A *Minősített archiválási szolgáltató* a panaszt 30 napon belül kivizsgálja, és az eredményekről értesíti a bejelentőt.

Amennyiben a választ a bejelentő nem tartja kielégítőnek, vagy az alapján nem sikerül a *Minősített archiválási szolgáltató* bevonása nélkül rendezni a felmerült vitát, akkor a bejelentő egyeztetést kezdeményezhet a *Minősített archiválási szolgáltató*val és az *Érintett felek*kel. Az egyeztetés minden résztvevőjét írásban értesíteni kell az egyeztetés időpontjáról azt megelőzően 10 munkanappal, és írásban meg kell számukra küldeni a bejelentést, a *Minősített archiválási szolgáltató* válaszát és egyéb szükséges információkat tartalmazó dokumentumokat.

Amennyiben az egyeztetés a panasz benyújtásától számított 30 napon belül nem vezet eredményre, akkor a bejelentő peres útra terelheti az ügyet. Az *Érintett felek* kölcsönösen alávetik magukat a Budapesti II. és III. Kerületi Bíróság, illetve a Fővárosi Törvényszék kizárólagos illetékességének.

8.14. Irányadó jog

A *Minősített archiválási szolgáltató* tevékenységét a mindenkor hatályos magyar jogszabályoknak megfelelően végzi. A *Minősített archiválási szolgáltató* szerződéseire és szabályzataira, azok teljesítésére a magyar jog az irányadó, s azok a magyar jog szerint értelmezendők.

8.15. Az érvényben lévő jogszabályoknak való megfelelés

A vonatkozó jogszabályok:

- AZ EURÓPAI PARLAMENT ÉS A TANÁCS 910/2014/EU RENDELETE (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről [1];
- 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól [5];
- ETSI EN 319 401 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [12];
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról [3];
- 2013. évi V. törvény a Polgári Törvénykönyvről [4].

8.16. Vegyes rendelkezések

8.16.1. Teljességi záradék

Nincs megkötés.

8.16.2. Átruházás

A jelen *Minősített archiválási szolgáltatási szabályzat* alapján nyújtott szolgáltatásokba bevont alvállalkozók vagy egyéb együttműködő partnerek csak a *Minősített archiválási szolgáltató* előzetes írásbeli engedélyével adhatják tovább jogosultságaikat és delegálhatják kötelezettségeiket harmadik félnek.

8.16.3. Részleges érvénytelenség

A jelen *Minősített archiválási szolgáltatási szabályzat* egyes rendelkezéseinek tetszőleges okból történő érvénytelenné válása esetén a többi rendelkezés változatlan formában érvényben marad.

8.16.4. Igényérvényesítés

A *Minősített archiválási szolgáltató* kártérítésre, az ügyvédi díjak megfizetésére tarthat igényt a partnerei által okozott károk, veszteségek, költségek megtérítése érdekében. Amennyiben a *Minősített archiválási szolgáltató* egy konkrét esetben nem él kártérítési igényével, az nem jelenti azt, hogy a jövőben hasonló esetben vagy a jelen *Minősített archiválási szolgáltatási szabályzat* más rendelkezésének megsértése esetén is lemondana a kártérítési igény érvényesítéséről.

8.16.5. Vis maior

A *Minősített archiválási szolgáltató* nem felelős a *Minősített archiválási rend*ben és a *Minősített archiválási szolgáltatási szabályzat*ban megfogalmazott kötelezettség hibás vagy késedelmes teljesítéséért, illetve nem teljesítéséért, amennyiben a hiba vagy késedelem oka a *Minősített archiválási szolgáltató* ellenőrzési körén kívül eső, előre nem látható elháríthatatlan külső ok.

8.17. Egyéb rendelkezések

Nincs megkötés.

9. Hivatkozások

Hivatkozások

[1] AZ EURÓPAI PARLAMENT ÉS A TANÁCS 910/2014/EU RENDELETE (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről.

[2] 2001. évi XXXV. törvény az elektronikus aláírásról (hatályát veszti 2016. július 1-én).

[3] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról.

[4] 2013. évi V. törvény a Polgári Törvénykönyvről.

[5] 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól.

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

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

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

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

[10] ETSI EN 319 132-1 V1.1.1 (2016-04) Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures.

[11] ETSI EN 319 132-2 V1.1.1 (2016-04) Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures.

[12] ETSI EN 319 401 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

[13] ETSI EN 319 403 V2.2.2 (2015-08) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers;.

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

[15] ISO/IEC 646:1991, Information technology – ISO 7-bit coded character set for information interchange.

[16] ISO/IEC 8859-1:1998, Information technology – 8-bit single-byte coded graphic character sets – Part 1: Latin alphabet No. 1.

[17] ISO/IEC 8859-2:1999, Information technology – 8-bit single-byte coded graphic character sets – Part 2: Latin alphabet No. 2.

[18] ISO/IEC 10646:2003, Information technology – Universal Multiple-Octet Coded Character Set (UCS) (withdrawn).

[19] MSZ/ISO/IEC 15408 Informatika. Biztonságtechnika. Az informatikai biztonságértékelés közös szempontjai, 2002 december .

[20] ISO/IEC 19790:2012: "Information technology – Security techniques – Security requirements for cryptographic modules".

[21] MSZ 7795-3:1992, Számítástechnikai karakterkódok. A grafikus karakterek magyar referenciakészlete.

[22] RFC 2045: Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies, November 1996.

[23] RFC 2822: Internet Message Format, April 2001.

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

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

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

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

[28] FIPS PUB 140-2 (2001 May 25): Security Requirements for Cryptographic Modules.

[29] CEN Workgroup Agreement CWA 14167-2: Cryptographic module for CSP signing operations with backup - Protection profile - CMCSOB PP.

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

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

[32] e-Szignó Hitelesítés Szolgáltató - eIDAS rendelet szerinti minősített elektronikus archiválási szolgáltatás - archiválási rend.

[33] e-Szignó Hitelesítés Szolgáltató - eIDAS rendelet szerinti minősített elektronikus archiválási szolgáltatás - archiválási szabályzat.

[34] e-Szignó Hitelesítés Szolgáltató - minősített időbélyegzési rend .

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