MICROSEC

e-Szignó Hitelesítés Szolgáltató

eIDAS Rendelet szerinti minősített elektronikus archiválási szolgáltatás szolgáltatási szabályzat

ver. 2.19

Hatálybalépés: 2020-12-28

Azonosító	1.3.6.1.4.1.21528.2.1.1.188.2.19
Verzió	2.19
Első verzió hatálybalépése	2006-12-15
Biztonsági besorolás	NYILVÁNOS
Jóváhagyta	Vanczák Gergely
Jóváhagyás dátuma	2020-12-11
Hatálybalépés dátuma	2020-12-28

Microsec Számítástechnikai Fejlesztő zártkörűen működő Részvénytársaság

1033 Budapest, Ángel Sanz Briz út 13.

Verzió	Hatálybalépés	A változás leírása
1.0	2006-12-15	Első változat. OID: 1.3.6.1.4.1.21528.2.1.1.18
1.1	2007-01-08	Módosítás a Nemzeti Hírközlési Hatóság észrevételeinek megfelelően. OID: 1.3.6.1.4.1.21528.2.1.1.18.1.1
1.2	2008-01-01	A fogyasztóvédelem elérhetőségének változása. OID: 1.3.6.1.4.1.21528.2.1.1.18.1.2
1.3	2008-10-01	Nem lépett hatályba. OID: 1.3.6.1.4.1.21528.2.1.1.18.1.3
1.4	2008-12-20	Megfelelés az NHH által kibocsátott követelményrendszernek. OID: 1.3.6.1.4.1.21528.2.1.1.18.1.4
2.0	2012-05-01	Cégforma változás. Változás az archivált akták titkosításával kapcsolatban. OID: 1.3.6.1.4.1.21528.2.1.1.18.2.0
2.0	2016-07-01	eIDAS követelmények szerinti új archiválási szabályzat új OID azonosítóval. OID: 1.3.6.1.4.1.21528.2.1.1.88.2.0
2.1	2016-09-05	Módosítások az NMHH észrevételei alapján.
2.2	2016-10-30	Módosítások a tanúsító észrevételei alapján.
2.4	2017-09-30	Éves felülvizsgálat.
2.6	2018-03-24	Teljes felülvizsgálat. Kisebb módosítások.
2.7	2018-09-15	Éves felülvizsgálat.
2.8	2018-12-14	Változások az auditor javaslatai alapján.
2.11	2019-09-25	Éves felülvizsgálat.
2.13	2020-03-05	Hatály. HSM követelmények. Kisebb pontosítások.
2.14	2020-05-26	Kisebb pontosítások.
2.17	2020-10-28	Átírás az ETSI TS 119 511 követelményei szerint. | Pontosítások az auditor és a felügyelő hatóság észrevételei alapján. | Kisebb pontosítások.
2.19	2020-12-28	Kisebb módosítások.

Tartalomjegyzék

1. Bevezetés

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

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

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

A *Minősített elektronikus 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 archiválási szolgáltató* a bizalmi szolgáltatás nyújtását 2016. július 1-jén jelentette be a Nemzeti Média- és Hírközlési Hatóságnak.

A minősített bizalmi szolgáltatás megfelelőségértékelését független vizsgáló szervezetként a TÜV Informationstechnik GmbH (továbbiakban TÜViT) végezte.

A sikeres megfelelőség értékelési vizsgálat alapján a Nemzeti Média- és Hírközlési Hatóság 2016. december 20-án nyilvántartásba vette és a magyar bizalmi listában [57] publikálta a bejegyzett minősített bizalmi szolgáltatást.

A minősített bizalmi szolgáltatás megfelelőségértékelését független vizsgáló szervezetként 2020. októberétől a Hunguard Kft (továbbiakban Hunguard) végzi.

A *Minősített archiválási szolgáltató* az *Ügyfel*ek részére legfontosabb információkat egy Szolgáltatási kivonat formájában is rendelkezésre bocsátja. A Szolgáltatási kivonat a 2.1 fejezetben leírtak szerint kerül publikálásra.

1.1. Áttekintés

Jelen *Minősített elektronikus 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 elektronikus archiválási szolgáltatási szabályzat*on kívül a *Minősített elektronikus archiválási rend*, [60] az Általános Szerződési Feltételek, a szolgáltatóval kötött Szolgáltatási szerződés, illetve egyéb, a *Minősített archiválási szolgáltató*tól független szabályzat illetve dokumentum is tartalmazhat.

A jelen dokumentum 1.5 fejezete számos fogalmat definiál, amelyeket más területeken nem, vagy nem teljesen ilyen értelmezésben használnak. Az ilyen értelemben használandó fogalmakat a dokumentumban minden esetben nagy kezdőbetűvel írva, döntött betűk használatával jelöljük.

1.2. Dokumentum neve és azonosítója

Kibocsátó	e-Szignó Hitelesítés Szolgáltató
Dokumentum címe	eIDAS Rendelet szerinti minősített elektronikus archiválási szolgáltatás szolgáltatási szabályzat
Azonosító	1.3.6.1.4.1.21528.2.1.1.188
Dokumentum verziószáma	2.19
Hatálybalépés ideje	2020-12-28

1.2.1. Megfelelés

A *Minősített archiválási szolgáltató* támogatja az alábbi ETSI arhiválási rendet:

- az ETSI TS 119 511 [35] specifikációban támasztott követelmények, beleértve az A Függelék követelményeit is:
  OID: itu-t(0) identified-organization(4) etsi(0) pres-service-policies(19511) policy-identifiers(1) qualified (2)

A *Minősített archiválási szolgáltató* a saját rend azonosító OID értékét használja a szolgáltatás nyújtása során, az ETSI követelményeknek való megfelelés a jelen *Minősített elektronikus archiválási szolgáltatási szabályzat* révén vállalja fel.

1.2.2. Archiválási rend

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

OID	MEGNEVEZÉS	RÖVID NÉV
1.3.6.1.4.1.21528.2.1.1.187.2.19	eIDAS Rendelet szerinti minősített archiválási rend.	MAR

A részletes követelményeket az " e-Szignó Hitelesítés Szolgáltató – eIDAS szerinti minősített elektronikus archiválási rend
ver.2.19." [58] dokumentum tartalmazza.

1.2.3. Hatály

Tárgyi hatály

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

Időbeli hatály

A *Minősített elektronikus archiválási szolgáltatási szabályzat* jelen verziója 2020-12-28 -i hatálybalépési dátumtól visszavonásig hatályos. A hatályosság automatikusan megszűnik a szolgáltatások beszüntetésekor vagy a *Minősített elektronikus archiválási szolgáltatási szabályzat* újabb verziójának hatályba lépésekor.

Személyi hatály

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

A *Minősített archiválási szolgáltató* elsősorban az Európai Unió állampolgárai és az Európai Unió területén bejegyzett szervezetek részére nyújtja bizalmi szolgáltatásait, de nem zárja ki szolgáltatásaiból más országok természetes és jogi személyeit sem, amennyiben azok elfogadják a *Minősített archiválási szolgáltató* által követett szabályrendszert és a szolgáltatások nyújtásához szükséges ellenőrzések kellően biztonságosan és gazdaságosan megvalósíthatók.

Fogyatékkal élők

A *Minősített archiválási szolgáltató* törekszik arra, hogy az általa nyújtott szolgáltatásokhoz a lehető legmagasabb színvonalon biztosítsa az egyenlő esélyű hozzáférést.

A szolgáltatás esélyegyenlőségének megteremtése érdekében minden lehetséges és ésszerű eszköz alkalmazásával törekszik arra, hogy szolgáltatásai akadálymentesen elérhetőek legyenek a fogyatékkal élő személyek számára is. Különösen fontos számára, hogy a fogyatékkal élő ügyfelek a fogyatékossággal nem érintett ügyfelekkel azonos minőségű, speciális igényeikhez igazodó szolgáltatásban részesülhessenek.

A *Minősített archiválási szolgáltató* az ügyfelekkel együttműködve, a *Minősített elektronikus archiválási szolgáltatási szabályzat* által meghatározott keretek között törekszik a személyes igényeknek leginkább megfelelő ügyintézési forma biztosítására.

Területi hatály

A jelen *Minősített elektronikus archiválási szolgáltatási szabályzat* az Európai Uniós jogon alapulva a magyar jog alapján Magyarországon nyújtott szolgáltatásokra vonatkozó konkrét követelményeket is tartalmaz.

A *Minősített archiválási szolgáltató* kiterjesztheti a szolgáltatás területi hatályát, ez esetben a *Minősített elektronikus archiválási szolgáltatási szabályzat* előírásainak megfelelő, azoknál nem enyhébb követelményeket alkalmaz. A külföldi *Ügyfel*ek számára nyújtott szolgáltatások *Minősített elektronikus archiválási szolgáltatási szabályzat*tól eltérő részletes feltételeit egyedi Szolgáltatási szerződésben szabályozhatja.

A jelen *Minősített elektronikus archiválási szolgáltatási szabályzat* szerint nyújtott szolgáltatás az egész világon elérhető. A jelen *Minősített elektronikus 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 elektronikus 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 *Minősített archiválási szolgáltató* adatai

Név:	Microsec Számítástechnikai Fejlesztő zártkörűen működő Részvénytársaság
Cégjegyzékszám:	01-10-047218 Fővárosi Törvényszék Cégbírósága
Székhely:	1033 Budapest, Ángel Sanz Briz út 13.
Telefonszám:	(+36-1) 505-4444
Telefax szám:	(+36-1) 505-4445
Internet cím:	`https://www.microsec.hu`, `https://www.e-szigno.hu`

Ügyfélszolgálati iroda

A szolgáltató egység neve:	e-Szignó Hitelesítés Szolgáltató
Ügyfélszolgálati iroda:	
	1033 Budapest, Ángel Sanz Briz út 13., Graphisoft Park Déli Terüet, C épület
Ügyfélszolgálati iroda nyitvatartási ideje:	munkanapokon 8:30-16:30 között előzetes időpont egyeztetés alapján
Ügyfélszolgálati iroda telefonszáma:	(+36-1) 505-4444
Ügyfélszolgálati iroda email címe:	`info@e-szigno.hu`
Visszavonási kérelmek fogadása:	`visszavonas@e-szigno.hu`
A szolgáltatással kapcsolatos információk elérése:	`https://www.e-szigno.hu`
Panaszok bejelentésének helye:	Microsec zrt.
	1033 Budapest, Ángel Sanz Briz út 13., Graphisoft Park Déli Terület, C épület
Illetékes fogyasztóvédelmi felügyelőség:	Budapest Főváros Kormányhivatal Fogyasztóvédelmi Felügyelőség 1052 Budapest, Városház u. 7. 1364 Budapest, Pf. 144.
Illetékes békéltető testület elérhetősége:	Budapesti Békéltető Testület 1016 Budapest, Krisztina krt. 99. III. em. 310. Levelezési cím: 1253 Budapest, Pf.: 10.

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 [3] (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 [6] hatálybalépésével európai szinten egységesen megváltozott az elektronikus aláírással kapcsolatos szolgáltatások teljes rendszere.

A Microsec 2016. július 1-jétől nyújtja eIDAS Rendelet szerinti nem minősített bizalmi szolgáltatásait, valamint elindította természetes személyek számára az eIDAS Rendelet szerinti minősített aláíró tanúsítványok kibocsátását.
A Microsec 2016. december 20-ától nyújtja az alábbi eIDAS Rendelet szerinti minősített bizalmi szolgáltatásait:

- minősített elektronikus bélyegző tanúsítványok kibocsátása
- minősített elektronikus időbélyegzés
- minősített elektronikus archiválás.

Microsec 2019. január 2-ától nyújtja az alábbi eIDAS Rendelet szerinti minősített bizalmi szolgáltatást:

- minősített weboldal hitelesítő tanúsítvány kibocsátás.

Microsec 2020. május 29-étől nyújtja az alábbi eIDAS Rendelet szerinti minősített bizalmi szolgáltatás komponenst

- minősített elektronikus aláírás/bélyegző létrehozására alkalmas távoli kulcsmenedzsment szolgáltatás.

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.

A minőségirányítási rendszer és az információbiztonság-irányítási rendszer hatóköre kiterjed a Microsec által nyújtott bizalmi szolgáltatásokra is.

A Microsec kétszintű kockázatelemzése az információ technológiai kockázatokon túlmenően kiterjed a teljes szervezetre és az üzleti kockázatokra is. A kockázatelemzés legalább évente felülvizsgálatra kerül. A kockázatelemzés eredménye alapján a *Minősített archiválási szolgáltató*

- intézkedéseket hoz a feltárt sérülékenységek megszüntetésére, és/vagy
- elfogadja az azonosított maradvány kockázatokat a döntés indokainak rögzítésével.

A *Minősített archiválási szolgáltató* honlapján minden érintett fél számára elérhetővé teszi Információbiztonsági Politikáját az alábbi linken:

`https://www.microsec.hu/hu/biztonsagi-garanciak`

Az Információbiztonsági politika minden változása ily módon kerül publikálásra a web oldalon keresztül.

A *Minősített archiválási szolgáltató* a szükséges mértékben tájékoztatja a harmadik feleket az Információbiztonsági politika változásairól, beleértve az előfizetőket, az érintett feleket, a tanúsító szervezeteket, a felügyelő és egyéb hatóságokat.

A *Minősített archiválási szolgáltató* azok bizalmas jellege miat nem hozza nyilvánosságra belső Biztonsági szabályzatait. Alvállalkozót, szerződéses partnereit és az egyéb érintett feleket a szerződés megkötésekor a szükséges mértékben tájékoztatja a rájuk vonatkozó biztonsági szabályokról.

Hitelesítés-szolgáltatást nyújtó üzletág

A Microsec szervezetén belül önálló üzleti egységként működő e-Szignó Hitelesítés Szolgáltató látja el a bizalmi szolgáltatások nyújtásával kapcsolatos feladatokat.

Szolgáltatások

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

- minősített elektronikus archiválási szolgáltatás

A *Minősített archiválási szolgáltató* a szolgáltatásokat jelen *Minősített elektronikus 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
  - elfogadja az Általános Szerződési Feltételeket,
  - meghatározza a felhasználók körét,
  - kijelölhet *Szervezeti ügyintéző*ket,
  - 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 elektronikus archiválási szolgáltatási szabályzat* 9.6.3 és 9.9.3 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 elektronikus archiválási szolgáltatási szabályzat* adminisztrációját ellátó szervezet adatai az alábbi táblázatban találhatók:

Szervezet neve	Microsec e-Szignó Hitelesítés Szolgáltató
Szervezet címe	Magyarország, H-1033 Budapest, Ángel Sanz Briz út 13.
Telefonszám	+36 1 505-4444
Fax szám	+36 1 505-4445
Email cím	info@e-szigno.hu

1.4.2. Kapcsolattartó személy

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

Kapcsolattartó	Folyamatszervezés részleg vezetője
Szervezet neve	Microsec zrt.
Szervezet címe	Magyarország, H-1033 Budapest, Ángel Sanz Briz út 13.
Telefonszám	+36 1 505-4444
Fax szám	+36 1 505-4445
Email cím	info@e-szigno.hu

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

A jelen *Minősített elektronikus archiválási szolgáltatási szabályzat*nak a benne meghivatkozott *Minősített elektronikus archiválási rend*nek való megfelelőségéért felelős személy:

Felelős	Folyamatszervezés részleg vezetője
Szervezet neve	Microsec zrt.
Szervezet címe	Magyarország, H-1033 Budapest, Ángel Sanz Briz út 13.
Telefonszám	+36 1 505-4444
Fax szám	+36 1 505-4445
Email cím	info@e-szigno.hu

A *Minősített elektronikus 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 elektronikus archiválási rend*ekről valamint az ezeket alkalmazó *Minősített archiválási szolgáltató*król.

1.4.4. A Szolgáltatási szabályzat elfogadási eljárása

A *Minősített elektronikus archiválási szolgáltatási szabályzat* új verziójának illetve tetszőleges módosításának megírása, elfogadása és kibocsátása egységes folyamatok szerint – a 9.12.1 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.
Archiválási bizonyíték	Az archiválási szolgáltatás által előállított bizonyíték, mely alkalmas annak igazolására, hogy egy vagy több archiválási cél elérésre került egy adott archivált dokumentumot tekintve.
Archiválási bizonyíték kibővítés	Adat hozzáadása létező archiválási bizonyítékhoz annak érdekében, hogy a bizonyíték érvényességi időtartama meghosszabbításra kerüljön.
Archiválási cél	A következő célkitűzések egyikének elérése az archiválási időkereten belül: elektronikus aláírás és bélyegző érvényességének hosszú időperiódusra való kiterjesztése, adat(ok) létezésére való bizonyítékok szolgáltatása hosszú időperióduson keresztül, vagy külsőleg szolgáltatott archiválási bizonyítékok kibővítése.
Archiválási profil	Egy archiválási tárolási modell és egy vagy több archiválási cél szempontjából releváns egyedileg azonosított implementációs adathalmaz, amely meghatározza az archiválási bizonyítékok előállításának és ellenőrzésének milyenségét.
Archiválási séma	Egy archiválási tárolási modell és egy vagy több archiválási cél szempontjából releváns általános eljárások és szabályzatok, melyek felvázolják, hogyan történik az archiválási bizonyítékok előállítása és ellenőrzése.
Archiválási szolgáltatás	Olyan bizalmi szolgáltatás, mely lehetőséget nyújt elektronikus aláírások és bélyegzők érvényességi állapotának meghosszabbítására és/vagy hosszú időtartamon keresztül az adatok létezéséről való bizonyítékok biztosítására.
Archiválási szolgáltató	Bizalmi szolgáltató, amely archiválási szolgáltatást nyújt.
Bizalmi felügyelet	"A *Bizalmi szolgáltatás*ok felügyeletét ellátó hatóság a Nemzeti Média- és Hírközlési Hatóság." (2015. évi CCXXII. törvény [6] 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 [6] 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, az e-dokumentum egy fajtája. Egy e-akta dokumentumokat, illetve hozzájuk kapcsolódó profilokat (metaadatokat), aláírásokat, ellenjegyzéseket és időbélyegeket tartalmazhat.
E-dokumentum	Az e-dokumentum egy olyan elektronikus dokumentum, amely legalább egy PKI alapú elektronikus aláírást vagy bélyegzőt tartalmaz. Az e-dokumentum típusától függően tartalmazhat további elektronikus dokumentumokat, illetve hozzájuk kapcsolódó profilokat (metaadatokat), aláírásokat, ellenjegyzéseket és időbélyegzőket.
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.
Export-import csomag	Az archiválási szolgáltatásból kiadásra kerülő olyan információ (elektronikusan aláírt dokumentum, archiválási bizonyíték, metaadat stb.), amely az archiválási célok elérése érdekében az importálást lehetővé teszi más archiválási szolgáltatás számára.
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 elektronikus aláírását vagy bélyegzését 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.
Hosszú táv	Időperiódus, amely alatti technológiai változások problémát jelenthetnek az elektronikus aláírás érvényességének ellenőrízhetőségében.

Hosszú távú archiválás	Egy elektronikus aláírás és bélyegző érvényességének hosszú időperiódusra való kiterjesztése és/vagy adat(ok) létezésére való bizonyítékok szolgáltatása hosszú időperióduson keresztül, az alkalmazott kriptográfiai technológia elavulása ellenére is.
Kompromittálódás	Egy kriptográfiai kulcs abban az esetben tekintendő kompromittálódottnak, ha vélelmezhető, hogy illetéktelen személynek is hozzáférése van hozzá.
Köztes hitelesítő egység	Olyan *Hitelesítő egység* amelynek *Tanúsítvány*át egy másik *Hitelesítő egység* bocsátotta ki.
Kriptográfiai kulcs (Cryptographic Key)	Olyan – kriptográfiai transzformációt vezérlő – egyedi digitális jelsorozat, amelynek ismerete szükséges titkosításhoz és dekódoláshoz, illetve elektronikus aláírás vagy bélyegző előállításához és ellenőrzéséhez.
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 [6] 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 [6] 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 [6] 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 belső nyilvántartás a felfüggesztett, illetőleg a visszavont *Tanúsítvány*okról, amelyek tartalmazzák legalább a felfüggesztés vagy visszavonás tényét, és a felfüggesztés vagy visszavonás időpontját másodperc pontossággal.

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 adattár felelősségek

2.1. Adattárak

A *Minősített archiválási szolgáltató* nyilvánosságra hozza szerződéses feltételeit és szabályzatait a honlapján elektronikus formában az alábbi linken:

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

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

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 weboldalán publikálva teszi letölthetővé elektronikusan aláírt PDF fájl formájában az *Ügyfél* részére az Általános Szerződési Feltételeket, a *Szolgáltatási kivonat*ot, a *Minősített elektronikus archiválási rend*et és a *Minősített elektronikus archiválási szolgáltatási szabályzat*ot. A *Minősített archiválási szolgáltató* az egyedi Szolgáltatási szerződést papír alapon kézi aláírással és pecséttel hitelesítve, vagy minősített elektronikus aláírással ellátott PDF formátumú elektronikus dokumentum formájában bocsátja az *Ügyfél* rendelkezésére.

A *Minősített archiválási szolgáltató* értesíti *Ügyfel*eit az Általános Szerződési Feltételek változásáról.

2.2. A közzététel időpontja vagy gyakorisága

2.2.1. Kikötések és feltételek közzétételi gyakorisága

A szolgáltatás szempontjából leglényegesebb kikötéseket és feltételeket tartalmazza az *Ügyfél* által a szerződéskötés során aláírandó szolgáltatási szerződés, vagy az abban meghivatkozott Általános Szerződési Feltételek [61] dokumentum.

A *Minősített archiválási szolgáltató* évi rendszerességgel illetve rendkívüli változtatási igény esetén soron kívül átvizsgálja az Általános Szerződési Feltételek dokumentumot 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 *Minősített archiválási szolgáltató* a jóváhagyott dokumentumot legalább 30 nappal a tervezett hatálybalépés előtt véleményezésre megküldi a Nemzeti Média- és Hírközlési Hatóság részére és publikálja honlapján.

A *Minősített archiválási szolgáltató* a közzétett új Általános Szerződési Feltételek tervezettel kapcsolatos észrevételeket a hatálybalépést megelőző 14. napig fogadja az alábbi címen:

`info@e-szigno.hu`

Érdemi változtatást igénylő észrevétel esetén a dokumentumot megváltoztatja.

Az Általános Szerződési Feltételek észrevételekkel módosított változatát a *Minősített archiválási szolgáltató* a hatálybalépést megelőző 7. napon lezárja és közzé teszi.

3. Elektronikus archiválási szolgáltatás

3.1. Archiválási rendszer

3.1.1. Azonosító

Az archiválási rendszert az aláírás-kibővítéssel és a tárolással együtt a következő URI azonosítja:

`http://uri.etsi.org/19512/scheme/pds+wst+aug`

Az archiválási rendszer Microsec azonosítója:

HU	Microsec archiválási rendszer dokumentum tárolással és aláírás kibővítéssel 2007
EN	Microsec preservation scheme with signature augmentation and with storage 2007
OID	1.3.6.1.4.1.21528.2.1.1.209.2007

3.1.2. Archiválási célkitűzések

A jelen archiválási rendszer az alábbi archiválási célkitűzéseket támogatja:

- **Az elektronikus aláírások és bélyegzők megőrzése (Preservation of Digital Signatures (PDS))**

  hosszú ideig kiterjeszti az elektronikus aláírás vagy bélyegző érvényesítésének, érvényességi állapotának megőrzésére és a kapcsolódó aláírt adatok meglétének igazolására vonatkozó képességét, amelyet az alábbi URI jelöl:

  `http://uri.etsi.org/19512/goal/pds`

- **Aláírások kiegészítése (Augmentation (AUG))**

  az archiválási szolgáltatás támogatja a benyújtott megőrzési igazolások kibővítését, amelyet az alábbi URI jelöl:

  `http://uri.etsi.org/19512/goal/aug`

3.1.3. Archiválás tárolási modell

A jelen archiválási rendszer a "Archiválás tárolással (Preservation with storage (WST))" archiválási tárolási modellt támogatja az ETSI TS 119 512 [36]) 4.3.1 fejezete szerint.

3.1.4. Támogatott műveletek

Feltöltés - Elektronikusan aláírt dokumentum átadása az archiválási szolgáltatónak megőrzésre.

Letöltés - Korábban a szolgáltatónak megőrzésre átadott dokumentum és a hozzá tartozó igazolások letöltése.

Törlés - Korábban a szolgáltatónak megőrzésre átadott dokumentum és a hozzá tartozó metaadatok törlése a szolgáltató nyilvántartásából.

Lekérdezés - Tárolási esemény információ letöltése az archiválás szolgáltatásból, amely információkat tartalmaz a vonatkozó eseményekkel kapcsolatban, amelyek egy megőrzési szolgáltatáson belül történtek egy adott tárolt dokumentumra.

Ellenőrzés - A szolgáltató által archivált elektronikus dokumentumon lévő aláírás érvényességének ellenőrzése.

Keresés - A kliens által elérhető archivált dokumentumok közötti keresés.

3.1.5. A tárolási bizonyítékok gyűjtése és ellenőrzése

A jelenlegi archiválási rendszer kiegészíti az aláírás formátumának megfelelő aláírást, amelyet a Profile / EvidenceFormat elemben jelentenek a következő URI-kkal:

- `http://uri.etsi.org/ades/CAdES/archive-time-stamp-v3`
- `http://uri.etsi.org/ades/XAdES/ArchiveTimeStamp`
- `http://uri.etsi.org/ades/PAdES/document-time-stamp`

A jelen archiválási rendszer csak az alábbi esetet támogatja:

- az aláírandó adat és az aláírás ugyanabban az objektumban található;

Az archiválás szolgáltatás ellenőrzi, hogy az aláírás érvényesítéséhez szükséges összes érvényesítési adat elérhető-e, hozzáadja ezt az aláíráshoz, és egy adott aláírás formátumának megfelelő minősített időbélyegzővel védi. A szolgáltatás a technika állásának megfelelő lenyomatképző algoritmust választ ki az érvényesítési adatok, az aláírás és az aláírt adatok védelmére.

A bizonyítékokat az aláírás tartalmazza.

Az aláírási formátumra jellemző szabvány meghatározza, hogyan kell érvényesíteni a megfelelő bizonyítékokat.

3.1.6. A megőrzési bizonyítékok kiegészítése

A *Minősített archiválási szolgáltató* folyamatosan figyeli a használt kriptográfiai algoritmusok megfelelőségét az alábbi normatívákban megfogalmazott követelmények alapján:

- ETSI TS 119 312 [34];
- az Eüt. [6] 92. § (1) b) pontja szerinti aktuális Nemzeti Média- és Hírközlési Hatóság által kiadott algoritmusokkal kapcsolatos határozat.

A megfigyelési eredmények alapján a *Minősített archiválási szolgáltató* az aláírás kibővítését hajtja végre új archív *Időbélyegző* elhelyezésével a e-dokumentumon a konkrét aláírás formátumnak megfelelően, mielőtt a kriptográfiai algoritmus gyengévé válna.

3.1.7. Támogatott archiválási profil

A szolgáltató az alábbi archiválási profilt használja a jelen archiválisi rendszerben:

HU	Microsec archiválási profil dokumentum tárolással és aláírás kibővítéssel 2007
EN	Microsec preservation profile with signature augmentation and with storage 2007
OID	1.3.6.1.4.1.21528.2.1.1.210.2007

3.2. Archiválási profil

A támogatott archiválási profilt jelen *Minősített elektronikus archiválási szolgáltatási szabályzat* jelen fejezete határozza meg.

3.2.1. Az archiválisi profil azonosítója

Az archiválási profil Microsec azonosítója:

HU	Microsec archiválási profil dokumentum tárolással és aláírás kibővítéssel 2007
EN	Microsec preservation profile with signature augmentation and with storage 2007
OID	1.3.6.1.4.1.21528.2.1.1.210.2007

3.2.2. Archiválási célkitűzések

A jelen archiválási rend az alábbi archiválási célkitűzéseket támogatja:

- **Az elektronikus aláírások és bélyegzők megőrzése (Preservation of Digital Signatures (PDS))**

  hosszú ideig kiterjeszti az elektronikus aláírás vagy bélyegző érvényesítésének, érvényességi állapotának megőrzésére és a kapcsolódó aláírt adatok meglétének igazolására vonatkozó képességét,

- **Aláírások kiegészítése (Augmentation (AUG))**

  az archiválási szolgáltatás támogatja a benyújtott megőrzési igazolások kibővítését,

3.2.3. Archiválás tárolási modell

A jelen archiválási profil az "Archiválás tárolással (Preservation with storage (WST))" archiválási tárolási modellt támogatja az ETSI TS 119 512 [36]) 4.3.1 fejezete szerint.

3.2.4. Támogatott műveletek

Feltöltés - Elektronikusan aláírt dokumentum átadása az archiválási szolgáltatónak megőrzésre.

Letöltés - Korábban a szolgáltatónak megőrzésre átadott dokumentum és a hozzá tartozó igazolások letöltése.

Törlés - Korábban a szolgáltatónak megőrzésre átadott dokumentum és a hozzá tartozó metaadatok törlése a szolgáltató nyilvántartásából.

Lekérdezés - Tárolási esemény információ letöltése az archiválás szolgáltatásból, amely információkat tartalmaz a vonatkozó eseményekkel kapcsolatban, amelyek egy megőrzési szolgáltatáson belül történtek egy adott tárolt dokumentumra.

Ellenőrzés - A szolgáltató által archivált elektronikus dokumentumon lévő aláírás érvényességének ellenőrzése.

Keresés - A kliens által elérhető archivált dokumentumok közötti keresés.

3.2.5. Műszaki rendek

A *Minősített elektronikus archiválási szolgáltatási szabályzat* jelenlegi verziója csak emberi olvasásra alkalmas formátumban érhető el, a *Minősített archiválási szolgáltató* jelenleg nem támogatja automatikus gépi feldolgozásra alkalmas formátumú rendek kezelését.

3.2.6. Érvényességi idő

A *Minősített archiválási szolgáltató* által nyújtott szolgáltatás a szolgáltatás 2007-es indítása óta megfelel a jelen *Minősített elektronikus archiválási szolgáltatási szabályzat*ban új formába öntött követelmény rendszernek, de az archiválási profil ebben a formában először a *Minősített elektronikus archiválási szolgáltatási szabályzat* 2.16 verziójában került publikálásra.

Az archiválási profil érvényességének nincs előre tervezett érvényesség vége ideje, annak érvényességét a *Minősített archiválási szolgáltató* a szolgáltatás teljes ideje alatt fenntartja.

3.2.7. A tárolási bizonyítékok formátuma

Az archiválási profil minősített időbélyegzőket használ a bizonyítékok érvényességének védelmére, amelyet az aláírás formátumának függvényében az alábbi URI értékek határoznak meg:

- `http://uri.etsi.org/ades/CAdES/archive-time-stamp-v3`
- `http://uri.etsi.org/ades/XAdES/ArchiveTimeStamp`
- `http://uri.etsi.org/ades/PAdES/document-time-stamp`

3.2.8. Emberi érthető formátum

A jelen *Minősített elektronikus archiválási szolgáltatási szabályzat*ban található archiválási profil emberek által értelmezhető formátumban készült, nem célja az automatikus gépi feldolgozás támogatása.

3.2.9. A támogatott archiválási profilok nyilvánosságra hozatala

A támogatott archiválási profilok a jelen *Minősített elektronikus archiválási szolgáltatási szabályzat* részeként kerülnek publikálásra a 2.1. fejezetben ismertetett módon.

3.2.10. Az archiválási profil élettartama

A teljes megőrzési idő alatt ugyanaz az archiválási profil van érvényben.

Az archiválási profil időben állandó, minden változó paraméter az archiválási profilon kívül kerül meghatározásra az archiválási bizonyíték rend vagy az aláírás ellenőrzési rend részeként.

Az alkalmazott archiválási bizonyíték rend vagy az aláírás ellenőrzési rend az idők során megváltozhat. Adott archiválási profilhoz tartozó valamennyi rend verzió nyilvánosan elérhető, és egyértelmű, hogy mikor melyik változat a hatályos.

3.2.11. Támogatott archiválási bizonyíték rend

A *Minősített archiválási szolgáltató* az alábbi archiválási bizonyíték rendet használja a jelen archiválisi profilban:

HU	Microsec archiválási bizonyíték rend 2007
EN	Microsec preservation evidence policy 2007
OID	1.3.6.1.4.1.21528.2.1.1.211.2007

3.2.12. Támogatott aláírás ellenőrzési rend

A *Minősített archiválási szolgáltató* az alábbi aláírás ellenőrzési rendet használja a jelen archiválisi profilban:

HU	Microsec aláírás ellenőrzési rend 2007
EN	Microsec signature validation policy 2007
OID	1.3.6.1.4.1.21528.2.1.1.212.2007

3.3. Archiválási bizonyíték rend

3.3.1. Az archiválisi bizonyíték rend azonosítója

Az archiválási bizonyíték rend Microsec azonosítója:

HU	Microsec archiválási bizonyíték rend 2007
EN	Microsec preservation evidence policy 2007
OID	1.3.6.1.4.1.21528.2.1.1.211.2007

3.3.2. Archiválási bizonyíték rend formátuma

Az archiválási bizonyíték rend jelen *Minősített elektronikus archiválási szolgáltatási szabályzat* részeként csak emberi olvasásra alkalmas formátumban érhető el, a *Minősített archiválási szolgáltató* jelenleg nem támogatja automatikus gépi feldolgozásra alkalmas formátumú archiválási bizonyíték rendek kezelését.

3.3.3. Archiválási bizonyítékok létrehozása

A *Minősített archiválási szolgáltató* az elektronikus aláírások érvényességének hosszú idejű megőrzését a tárolt elektronikus aláírások rendszeres kibővítésével (augmentation) valósítja meg. Az érvényesség kibővítése során az elektronikus aláíráson egy archív *Időbélyegző*t helyez el, amely további évekre biztosítja a megőrzött eredeti elektronikus aláírás érvényességének ellenőrízhetőségét.

Az archiválási bizonyíték létrehozása során a *Minősített archiválási szolgáltató* ellenőrzi az adott elektronikus aláírás, elektronikus bélyegző vagy időbélyegző érvényességét.

A *Minősített archiválási szolgáltató* az elektronikus aláírás, bélyegző vagy *Időbélyegző* vizsgálata során az érvényességi láncot visszavezeti egy általa elfogadott hitelesítés- (vagy időbélyegzés-) szolgáltató megbízható gyökér- vagy szolgáltatói köztes *Tanúsítvány*ára (lásd: 1.3.1 fejezet).

A *Minősített archiválási szolgáltató* OCSP szolgáltatás segítségével gyűjti össze az érvényességi lánc minden elemére a visszavonási állapot információt. Amennyiben a tanúsítványláncban szereplő minden szolgáltató OCSP szolgáltatására vonatkozó kivárási idő 0, akkor a szükséges valamennyi visszavonási információ rövid időn belül – akár másodpercek alatt – előáll. 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 kezdeti ellenőrzés során a *Minősített archiválási szolgáltató* elutasítja az e-dokumentumot, ha az ellenőrzést 3 nap alatt nem tudja elvégezni. Ez a későbbiekben az e-dokumentum kibővítésekor nem fordulhat elő, mert a *Minősített archiválási szolgáltató* által használt időbélyegzés szolgáltató 0 kivárási idejű OCSP szolgáltatást nyújt.

A *Minősített archiválási szolgáltató* felépíti az e-dokumentumokban szereplő elektronikus aláírásokhoz, bélyegzőkhöz vagy *Időbélyegző*khöz tartozó érvényességi láncokat, és minősített archív elektronikus *Időbélyegző*t helyez el rajtuk. Az így kapott érvényességi láncokat az e-dokumentum formátumának megfelelő formátumú ún. archív aláírásként elhelyezi az e-dokumentumban.

A *Minősített archiválási szolgáltató* az archiválási bizonyítékok létrehozásához a saját fejlesztésű e-Szignó minősített aláírás-létrehozó és ellenőrző alkalmazást használja.

3.3.4. Felhasznált kriptográfiai algoritmusok

A *Minősített archiválási szolgáltató* folyamatosan figyeli a használt kriptográfiai algoritmusok megfelelőségét az alábbi normatívákban megfogalmazott követelmények alapján:

- ETSI TS 119 312 [34];
- az Eüt. [6] 92. § (1) b) pontja szerinti aktuális Nemzeti Média- és Hírközlési Hatóság által kiadott algoritmusokkal kapcsolatos határozat.

A *Minősített archiválási szolgáltató* csak olyan kriptográfiai algoritmusokat használ az archiválási bizonyítékok létrehozása, amelyek megfelelnek a hatályos követelményeknek, és előreláthatóan még évekig biztosítják az archiválási bizonyítékok érvényességét.

A *Minősített archiválási szolgáltató* jelenleg kizárólag csak a 256 bites ECC kulcs használatán alapuló *Időbélyegző*ket használ az archiválási bizonyítékok létrehozására.

A *Minősített archiválási szolgáltató* által jelenleg tárolt e-dokumentumok mindegyike legalább 2048 bites RSA kulcsot vagy 256 bites ECC kulcsot tartalmazó *Időbélyegző*vel védett.

A *Minősített archiválási szolgáltató* legkésőbb 2022-12-31-ig az akkori követelményeknek megfelelő új *Időbélyegző*t helyez el valamennyi e-dokumentumon, amelyen a legutolsó *Időbélyegző* RSA kulcsot használ.

3.3.5. Más bizalmi szolgáltatások használata

A *Minősített archiválási szolgáltató* a szolgáltatás nyújtása során az alábbi módokon használja fel más bizalmi vagy hitelesítés szolgáltatók szolgáltatásait:

- az archiválási bizonyítékok hitelesítése során a Microsec zrt. "Minősített időbélyegző szolgáltatás" által kibocsátott minősített *Időbélyegző*ket használja az archív *Időbélyegző*k előállítására,

- az érvényességi lánc felépítése során a *Tanúsítvány* Szolgáltatói információ elérése (AIA) kiterjesztésében található kibocsátó hitelesítési egység *Tanúsítvány* URI felhasználásával gyűjti be a kibocsátó CA *Tanúsítvány*át,
- a *Tanúsítvány* visszavonási állapotának ellenőrzése során a *Tanúsítvány* Szolgáltatói információ elérése (AIA) kiterjesztésében megadott OCSP szolgáltatás elérési URI felhasználásával szerzi be az OCSP válaszokat.

3.3.6. Archiválási bizonyítékok érvényességének ellenőrzése

Az archiválási bizonyíték érvényességének ellenőrzése során a *Minősített archiválási szolgáltató* ellenőrzi az adott minősített *Időbélyegző* érvényességét.
Az általános aláírás ellenőrző lépéseken túlmenően a *Minősített archiválási szolgáltató* ellenőrzi, hogy

- az *Időbélyegző*t hitelesítő *Időbélyegző egység Tanúsítvány*a szerepel a magyar bizalmi listán
- az *Időbélyegző egység Tanúsítvány*a érvényes volt az *Időbélyegző* által igazolt időpontban
- az *Időbélyegző egység Tanúsítvány*a érvényes az ellenőrzés időpontjában
- az *Időbélyegző egység Tanúsítvány*a egy aktív státuszú minősített időbélyegzés szolgáltatáshoz tartozik
- a kibocsátott *Időbélyegző* minősített

A *Minősített archiválási szolgáltató* OCSP szolgáltatás segítségével ellenőrzi a visszavonási állapot információt. Mivel az OCSP szolgáltatására vonatkozó kivárási idő 0, a szükséges visszavonási információ rövid időn belül – másodpercek alatt – előáll.

3.3.7. A bizonyítékok frissítése

A *Minősített archiválási szolgáltató* folyamatosan figyeli a használt kriptográfiai algoritmusok megfelelőségét az alábbi normatívákban megfogalmazott követelmények alapján:

- ETSI TS 119 312 [34];
- az Eüt. [6] 92. § (1) b) pontja szerinti aktuális Nemzeti Média- és Hírközlési Hatóság által kiadott algoritmusokkal kapcsolatos határozat.

A megfigyelési eredmények alapján a *Minősített archiválási szolgáltató* az aláírás kibővítését hajtja végre új archív *Időbélyegző* elhelyezésével az e-dokumentumon a konkrét aláírás formátumnak megfelelően, mielőtt a kriptográfiai algoritmus gyengévé válna.

3.3.8. Archiválási bizonyítékok formátuma

A *Minősített archiválási szolgáltató* az archiválási bizonyítékokat archív *Időbélyegző* formájában állítja elő, amelyet az e-dokumentum kibővítéseként az e-dokumentumon helyez el annak elválaszthatatlan részeként.
Az archiválási bizonyítékok szabványos PKI elemeket tartalmaznak az alábbiak szerint:

- az érvényességi láncban található ITU X.509 [49] formátumú szolgáltatói gyökér és köztes CA *Tanúsítvány*ok
- az érvényességi láncban található *Tanúsítvány*ok érvényességét igazoló IETF RFC 6960 [48] szerinti OCSP válaszok
- opcionálisan az OCSP válaszok érvényességét igazoló további szabványos elemek (tanúsítványok, visszavonási állapot információk)
- az archiválási bizonyítékokat és az e-dokumentumot védő IETF RFC 3161 [47] szerinti *Időbélyegző*

3.3.9. Bizonyíték hivatkozása az archiválás szolgáltatóra

A *Minősített archiválási szolgáltató* szabványos PKI elemeket alkalmaz archiválási bizonyítékként, amely elemek nem tartalmaznak hivatkozást a *Minősített archiválási szolgáltató*ra.

3.4. Aláírás ellenőrzési rend

3.4.1. Aláírás ellenőrzési rend azonosítója

Az aláírás ellenőrzési rend Microsec azonosítója:

HU	Microsec aláírás ellenőrzési rend 2007
EN	Microsec signature validation policy 2007
OID	1.3.6.1.4.1.21528.2.1.1.212.2007

3.4.2. Aláírás ellenőrzési rend formátuma

Az aláírás ellenőrzési rend jelen *Minősített elektronikus archiválási szolgáltatási szabályzat* részeként csak emberi olvasásra alkalmas formátumban érhető el, a *Minősített archiválási szolgáltató* jelenleg nem támogatja automatikus gépi feldolgozásra alkalmas formátumú aláírás ellenőrzési rendek kezelését.

3.4.3. Nyelvi verziók

A *Minősített archiválási szolgáltató* nyilvános szabályzatai két nyelvi verzióban készülnek, magyar és angol változatban.

Az elsődleges verzió a magyar nyelvű szabályzat.

Az angol nyelvű verzió a magyar nyelvű fordítása. A *Minősített archiválási szolgáltató* törekszik rá, hogy az angol nyelvű verzió teljesen megfeleljen a magyar nyelvű verziónak, de a nyelvi sajátosságok és esetleges fordítási hibák következtében a két verzióban előfordulhatnak kisebb eltérések. Ilyen jellegű eltérés esetén ellenkező értelmű megállapodás hiányában a magyar nyelvű verzióban foglaltak az irányadók.

3.4.4. Validálási információk összegyűjtése

A *Minősített archiválási szolgáltató* ellenőrzi, hogy az aláírás érvényesítéséhez szükséges összes érvényesítési adat elérhető-e, a hiányzó érvényesítési adatokat összegyűjti, hozzáadja ezt az aláíráshoz, és egy adott aláírás formátumának megfelelő minősített archív *Időbélyegző*vel védi.

A bizonyítékokat az aláírt e-dokumentum tartalmazza.

Az aláírási formátumra jellemző szabvány meghatározza, hogyan kell érvényesíteni a megfelelő bizonyítékokat.

A *Minősített archiválási szolgáltató* az aláírások érvényességének ellenőrzése során a kagyló modellt követi, vagyis az érvényességi lánc minden *Tanúsítvány*ának érvényességi ideje befoglalva kell legyen az azt kibocsátó szolgáltatói *Tanúsítvány* érvényességi idejében.

3.5. Kriptográfiai előírások

3.5.1. Időbélyegzők

A *Minősített archiválási szolgáltató* a Microsec e-Szignó Hitelesítés Szolgáltató által nyújtott "eIDAS Rendelet szerinti minősített időbélyegzés-szolgáltatás" által kibocsátott minősített *Időbélyegző*ket használja az archív *Időbélyegző*k létrehozására.

Az igénybe vett időbélyegző szolgáltatás megfelel az ETSI EN 319 421 [20] és az ETSI EN 319 422 [21] követelményeknek és minősített időbélyegzés szolgáltatásként jegyzett a magyar bizalmi listán [57].

Az *Időbélyegzés-szolgáltató* által használt *Időbélyegző Tanúsítvány*ok visszavonási állapota ellenőrizhető az *Időbélyegzés-szolgáltató* által biztosított CRL és OCSP szolgáltatás alapján. Az *Időbélyegzés-szolgáltató* által nyújtott visszavonási állapot információ az *Időbélyegző Tanúsítvány* visszavonása esetén tartalmazza a visszavonás okát ("reason code").

3.5.2. Kriptográfiai algoritmusok változáskövetése

A *Minősített archiválási szolgáltató* folyamatosan figyeli a használt kriptográfiai algoritmusok megfelelőségét az alábbi normatívákban megfogalmazott követelmények alapján:

- ETSI TS 119 312 [34];
- az Eüt. [6] 92. § (1) b) pontja szerinti aktuális Nemzeti Média- és Hírközlési Hatóság által kiadott algoritmusokkal kapcsolatos határozat.

Minden támogatott aktív megőrzési profilnál a *Minősített archiválási szolgáltató* figyelemmel kíséri minden, a profilhoz kapcsolódó kriptográfiai algoritmus erősségét. Ha úgy gondolja, hogy valamely alkalmazott kriptográfiai algoritmus vagy paraméter kevésbé biztonságos, akkor vagy frissíti a kapcsolódó archiválási bizonyíték rendet, vagy új archiválási profilt hoz létre az újonnan benyújtott e-dokumentumok kezelésére.

A *Minősített archiválási szolgáltató* a teljes megőrzési idő alatt figyelemmel kíséri az egyes e-dokumentumokon elhelyezett legutolsó archív *Időbélyegző* alkalmasságát az elektronikus aláírás érvényességének megőrzésére. A *Minősített archiválási szolgáltató* az aktuális archiválási bizonyíték rendnek megfelelő új archív *Időbélyegző*t helyez el az adott e-dokumentumon, amennyiben:

- az utolsó *Időbélyegző* előállításához használt bármely kriptográfiai algoritmus vagy paraméter biztonsága csökken, vagy használatát megtiltják a vonatkozó kriptográfiai követelmények;
- az utolsó *Időbélyegző* hitelesítéséhez használt *Tanúsítvány* érvényességi ideje végéhez közeledik.

3.6. A megőrzési bizonyítékok bővítése

A *Minősített archiválási szolgáltató* folyamatosan figyeli a használt kriptográfiai algoritmusok megfelelőségét az alábbi normatívákban megfogalmazott követelmények alapján:

- ETSI TS 119 312 [34];
- az Eüt. [6] 92. § (1) b) pontja szerinti aktuális Nemzeti Média- és Hírközlési Hatóság által kiadott algoritmusokkal kapcsolatos határozat.

A megfigyelési eredmények alapján a *Minősített archiválási szolgáltató* az aláírás kibővítését hajtja végre új archív *Időbélyegző* elhelyezésével a e-dokumentumon a konkrét aláírás formátumnak megfelelően, mielőtt a kriptográfiai algoritmus gyengévé válna.

3.7. Export-import csomag

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

Az *Előfizető* kizárólag biztonságos csatornán keresztül férhet hozzá a *Minősített archiválási szolgáltató* archívumában lévő e-dokumentumokhoz és archiválási bizonyítékokhoz. A letöltés tipikusan Interneten keresztül történik a *Minősített archiválási szolgáltató* által biztosított felület felhasználásával a 4.3. fejezetben részletesen leírtak szerint.

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

Az e-dokumentumok átadása minden esetben az átvevő azonosságának és jogosultságának ellenőrzése után történik. Minden *Előfizető* alapesetben csak az általa feltöltött e-dokumentumokhoz fér hozzá, további hozzáférések csak írásbeli meghatalmazás alapján állíthatók be.

Internet alapú lekérdezés esetében a jogosultság ellenőrzése authentikációs *Tanúsítvány* alapján történik.

A személyes átadás során az átvevő személyazonosságát a *Minősített archiválási szolgáltató* személyazonosításra alkalmas hatósági igazolvány alapján ellenőrzi.

A *Minősített archiválási szolgáltató* minden adatátadást naplóz a 6.4. fejezetben leírtak szerint. A napló adatok többek között tartalmazzák az esemény időpontját, az átadott e-dokumentumok azonosítóit.

3.8. Archiválási protokoll

3.8.1. Hozzáférés a tárolt dokumentumokhoz

Az *Előfizető* a kliens autentikációciós *Tanúsítvány*a felhasználásával kölcsönös azonosításon alapuló SSL/TLS kapcsolatot létesít a *Minősített archiválási szolgáltató* szerverével.

A *Minősített archiválási szolgáltató* az *Előfizető*t az SSL/TLS kapcsolat felépítéséhez használt kliens autentikációciós *Tanúsítvány*a alapján azonosítja.

A *Minősített archiválási szolgáltató* biztosítja, hogy az *Előfizető* a szolgáltatási szerződés érvényességi ideje alatt letöltheti az archívumban tárolt összes korábban feltöltött e-dokumentumát és az azokhoz tartozó archiválási bizonyítékokat.

A *Minősített archiválási szolgáltató* többféle lehetőséget kínál egy vagy több e-dokumentum feltöltésére a szolgáltatásba. Az *Előfizető* Dublin Core szerinti [50] metaadatokat is megadhat az egyes elektronikus dokumentumokkal kapcsolatban. A részletek jelen *Minősített elektronikus archiválási szolgáltatási szabályzat* 4.2. fejezetében találhatók.

A *Minősített archiválási szolgáltató* a feltöltött e-dokumentum típusától függően ellenőrzi az e-dokumentum megfelelőségét.

Az e-dokumentumban lévő elektronikus aláírások és elektronikus bélyegzők érvényességének ellenőrzése után a *Minősített archiválási szolgáltató* a lehető leghamarabb, de a feltöltést követően 3 napon belül visszaigazolást küld az *Előfizető*nek arról, hogy az e-dokumentumot sikeresen befogadta. A visszaigazolás egyebek között tartalmazza az e-dokumentum lenyomatát, ami a későbbiekben az e-dokumentum azonosítójaként használható különféle műveletekben.

Egy tetszőleges művelet elvégzéséhez az *Előfizető*nek először meg kell adnia, hogy mely e-dokumentumokhoz kíván hozzáférni. A megfelelő e-dokumentum kiválasztásához a web felületen lehetősége van a dokumentumhoz kapcsolódó Dublin Core [50] szerinti metaadatok alapján megadható szűrőkkel keresni az e-dokumentumokra. A kiválasztás az e-dokumentumot egyértelműen azonosító lenyomat (hash) alapú azonosító segítségével történik.

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

3.8.2. A tárolt dokumentumok törlése

A *Minősített archiválási szolgáltató* az *Előfizető* kérésére törli az archivált e-dokumentumot és a hozzá tartozó valamennyi archiválási bizonyítékot az archívumából. Részleteket lásd a 4.6. fejezetben.

Törlési kérelem csak a Szolgáltatási szerződés érvényességi ideje alatt, a megőrzési idő vége előtt nyújtható be.

Az e-dokumentum benyújtásakor kapott dokumentum azonosító használható a törlendő e-dokumentum kiválasztására.

3.9. Ügyfél értesítések

A *Minősített archiválási szolgáltató* a nyújtott szolgáltatás keretében minden *Előfizető* részére biztosít egy levelező postafiókot, amelyet a *Minősített archiválási szolgáltató* saját informatikai rendszerében üzemeltet.

Az *Előfizető*k POP3 protokollon keresztül érhetik el leveleiket felhasználónév és jelszó alapú azonosítást követően.

A *Minősített archiválási szolgáltató* az *Előfizető* részére küldött személyes értesítéseket minden esetben ebbe a postafiókba küldi, pl. a feltöltött e-dokumentumok befogadásáról kiállított igazolásokat.

Az általános jellegű információkat a *Minősített archiválási szolgáltató* a honlapján teszi közzé.

A nyilvános szabályzatok változásáról a *Minősített archiválási szolgáltató* a weboldalán keresztül tájékoztatja *Előfizető*it a 2.1 fejezetben leírt módon.

A *Minősített archiválási szolgáltató Minősített elektronikus archiválási szolgáltatási szabályzat*a tartalmazza az összes információt a használt archiválási profilokról és az azokban meghivatkozott szolgáltatási rendekről.

3.10. Tárolás folyamata

3.10.1. Megőrzési bizonyítékok

A *Minősített archiválási szolgáltató* a Microsec e-Szignó Hitelesítés Szolgáltató által nyújtott "eIDAS Rendelet szerinti minősített időbélyegzés-szolgáltatás" által kibocsátott minősített *Időbélyegző*ket használja az archív *Időbélyegző*k létrehozására.

Az igénybe vett időbélyegző szolgáltatás minősített időbélyegzés szolgáltatásként jegyzett a magyar bizalmi listán [57], és megfelel az alábbi követelményeknek:

- IETF RFC 3161 [47]
- ETSI EN 319 421 [20]
- ETSI EN 319 422 [21]

3.10.2. Elektronikus aláírás és bélyegző megőrzése

A *Minősített archiválási szolgáltató* csak érvényes elektronikus aláírással vagy bélyegzővel rendelkező e-dokumentumot fogad be. A feltöltött e-dokumentum opcionálisan tartalmazhat az *Előfizető* által beszerzett bizonyítékokat az elektronikus aláírás vagy bélyegző érvényességéről.

Az archiválandó e-dokumentum megérkezésekor a *Minősített archiválási szolgáltató* mindent megtesz annak érdekében, hogy az érvényesítési adatokat az archiválási profil által támogatott aláírás ellenőrzési rend szerint begyűjtse és ellenőrizze a 4.2. szakaszban leírtak szerint.

A *Minősített archiválási szolgáltató* felhasználhatja az *Előfizető* által feltöltött bizonyítékokat, de ilyen esetben meggyőződik róla, hogy a biztosított bizonyíték megfelel az archiválási profil által támogatott aláírás ellenőrzési rend követelményeinek.

Az elektronikus aláírás és bélyegző érvényesíthetőségének és az érvényességének fenntartása érdekében a *Minősített archiválási szolgáltató* archív *Időbélyegző*t helyez az elektronikus aláírásra vagy bélyegzőre.

Az archív *Időbélyegző* egyrészt bizonyítja az elektronikus aláírás és bélyegző és az elektronikus aláírás és bélyegző érvényesítéséhez szükséges érvényesítési adatok meglétét, másrészt pedig bizonyítja az aláírt adatok meglétét.

3.11. Hálózati biztonság

3.11.1. Hozzáférés a tárolt dokumentumokhoz

Az *Előfizető*k a szolgáltatás keretében csak a *Minősített archiválási szolgáltató* által biztosított felhasználói felületen keresztül férnek hozzá a szolgáltatásban tárolt e-dokumentumokhoz.

Az *Előfizető*knek sem az e-dokumentumokhoz, sem pedig az azokhoz kapcsolódó archiválási bizonyítékokhoz nincs közvetlen hozzáférésük.

3.12. Bizalmi szolgáltatás leállítása, szolgáltatás leállítási terv

3.12.1. Tárolt dokumentumok a leállás után

A *Minősített archiválási szolgáltató* részletes szolgáltatás leállítási tervvel rendelkezik, amely meghatározza a szolgáltatás tervezett megszüntetése során elvégzendő feladatokat.

A jelen *Minősített elektronikus archiválási szolgáltatási szabályzat* 6.7. fejezete ismerteti a szolgáltatás leállításával kapcsolatos főbb tudnivalókat, beleértve a tárolt e-dokumentumok kezelésének módját.

3.13. Archiválás szolgáltatás szabályai

3.13.1. Támogatott archiválási rendek

A *Minősített elektronikus archiválási szolgáltatási szabályzat* 1.2. fejezete tartalmazza a támogatott archiválási rendek megnevezését.

3.13.2. Támogatott archiválási profilok

A *Minősített elektronikus archiválási szolgáltatási szabályzat* 3.1.7. fejezete tartalmazza a támogatott archiválási profilok megnevezését.

3.13.3. Archiválási célkitűzések megvalósítása

A *Minősített archiválási szolgáltató* az archivált e-dokumentumokon található elektronikus aláírások és bélyegzők érvényességének hosszú távú megőrzését az elektronikus aláírások és bélyegzők szükséges időnkénti kiegészítésével biztosítja archív *Időbélyegző* elhelyezésével.

3.13.4. Az archivált dokumentumok elérhetősége

A *Minősített elektronikus archiválási szolgáltatási szabályzat* 5.9. fejezete tartalmazza az archivált dokumentumokelérhetőségét.

3.13.5. Az archiválási szolgáltatást támogató összes külső szervezet kötelezettségei

A *Minősített archiválási szolgáltató* a szolgáltatás nyújtása során igénybe veheti külső szervezetek közreműködését, de az *Előfizető* felé minden közreműködő teljesítéséért sajátjaként felel. A közreműködők kötelezettségeit a közreműködővel kötött együttműködési szerződés szabályozza.

3.13.6. Adatok fel- illetve letöltésének igénylése

A *Minősített elektronikus archiválási szolgáltatási szabályzat* 4.2. és 4.3. fejezetei tartalmazzák az adatok fel- illetve letöltésének lehetőségeit.

3.13.7. Az archivált adatok kezelése a megőrzési idő lejárta után

A *Minősített archiválási szolgáltató* a Szolgáltatási szerződés érvényességi idejének végéig biztosítja a feltöltött e-dokumentumokon elhelyezett elektronikus aláírások és bélyegzők érvényességének ellenőrízhetőségét. A Szolgáltatási szerződés érvényességének végével a tárolt e-dokumentumok és a hozzájuk tartozó archiválási bizonyítékok véglegesen törlésre kerülnek a 4.7. fejezetben részletezett módon.

3.14. Minősített archiválás szolgáltatás

3.14.1. Időbélyegző szolgáltató

A *Minősített archiválási szolgáltató* a Microsec e-Szignó Hitelesítés Szolgáltató által nyújtott "eIDAS Rendelet szerinti minősített időbélyegzés-szolgáltatás" által kibocsátott minősített *Időbélyegző*ket használja az archív *Időbélyegző*k létrehozására.

3.14.2. Szolgáltatás azonosító

A szolgáltatás regisztrálva van a magyar bizalmi listán minősített archiválás szolgáltatásként, a szolgáltatás kódja "PSES/Q".

A szolgáltatás azonosítására az a minősített bélyegző *Tanúsítvány* szolgál, amelyet a *Minősített archiválási szolgáltató* a feltöltött e-dokumentumok befogadásáról küldött visszaigazolás hitelesítésére használ. A minősített *Tanúsítvány*ok 2 éves magyarországi érvényességi korlátja miatt a használt *Tanúsítvány*t a *Minősített archiválási szolgáltató* rendszeresen megújítja, de a bizalmi listán a jelenlegi mellett megtalálható az összes korábbi *Tanúsítvány* is.

A jelenleg használatban lévő *Tanúsítvány* főbb adatai:

Subject Common Name	e-Szignó Archívum
Issuer Common Name	Qualified e-Szigno QCP CA 2012
Serial number	01:1d:d1:0e:a7:52:51:ca:5a:1a:c7:00:e0:0a
Subject Key identifier	81:ed:df:1b:95:9b:d2:8b:07:5c:47:b4:6e:db:bf:21:12:fe:86:09
SHA-1 lenyomat	4b:1d:23:6d:4b:90:86:8c:bf:4b:35:4e:f5:95:19:4d:7a:22:82:28

4. Az archiválás szolgáltatás folyamatainak leírása

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* elektronikusan aláírt e-dokumentumokat tölthet fel a *Minősített archiválási szolgáltató* által üzemeltetett archívumba. Az e-dokumentum befogadása során a *Minősített*

archiválási szolgáltató ellenőrzi az e-dokumentumon illetve az e-dokumentumba 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-dokumentumot. (lásd 4.2. fejezet).

- A *Minősített archiválási szolgáltató* a befogadott e-dokumentumokat – 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-dokumentumokon illetve az e-dokumentumokban tárolt fájlokon elhelyezett elektronikus aláírások illetve bélyegzők hosszú távú érvényességének biztosításáról. A *Minősített archiválási szolgáltató* a megőrzés ideje alatt biztosítja az e-dokumentumok és meghatározott fájlformátumok 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 5. fejezetben).
- Az *Előfizető* a Szerződés időtartama alatt folyamatosan elérheti a *Minősített archiválási szolgáltató* archívumában az általa ott elhelyezett e-dokumentumokat, aláírásokat, bélyegzőket, illetve a hozzájuk tartozó érvényességi láncokat és azokat onnan letöltheti (lásd: 4.3).
- Az *Előfizető* kérésére a *Minősített archiválási szolgáltató* hiteles igazolást bocsát ki arról, hogy az egyes e-dokumentumokat tárolja, és az e-dokumentumon illetve az e-dokumentumban tárolt egyes dokumentumokon az archívumba helyezés időpontjában érvényes elektronikus aláírás vagy bélyegző szerepelt (lásd: 4.4. fejezet).
- Az *Előfizető* kérésére a *Minősített archiválási szolgáltató* törli az e-dokumentumokat az archívumából (lásd: 4.6. 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-dokumentumban 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 e-dokumentumokat fogad be.

A *Minősített archiválási szolgáltató* csak olyan elektronikus aláírással illetve bélyegzővel ellátott e-dokumentumokat fogad be,

- amelyekben minden megőrzendő érvényességű elektronikus aláírást vagy elektronikus bélyegzőt *Időbélyegző*vel láttak el;
- amelyekben az elektronikus aláírás vagy elektronikus bélyegző formátuma megfelel az alábbi formátumok valamelyikének:
  - XAdES ETSI TS 101 903 [24] [25] [26] [27]
  - PAdES PDF/A format (ISO 19005) [51]
  - ASiC (Associated Signature Containers) ETSI TS 102 918 [32]
  - CAdES ETSI EN 319 122 [10], [11]
  - XAdES ETSI EN 319 132 [12], [13]
  - PAdES ETSI EN 319 142 [14], [15]
  - ASiC ETSI EN 319 162 [16], [17]

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. Egyéb értelmű megállapodás hiányában az alapértelmezett megőrzési időtartam 50 év.

A *Minősített archiválási szolgáltató* a 5.8 fejezetben felsorolt formátumú fájlok hosszú távú olvashatóságát biztosítja az ott meghatározott módon, az ott leírt feltételek szerint.

4.1. Szolgáltatási szerződés kötése

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

A *Minősített elektronikus 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 [62], *Minősített elektronikus archiválási rend* [58], jelen *Minősített elektronikus archiválási szolgáltatási szabályzat* [59], 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 elektronikus 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 autentikációciós *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 autentikációciós *Tanúsítvány*ok esetén milyen feltételekkel nyújtja a szolgáltatást.

4.2. Dokumentum feltöltése

A *Minősített archiválási szolgáltató* kizárólag az *Előfizető* azonosságának megállapítása után, biztonságos eljárás keretében fogad be archiválandó e-dokumentumokat. Az eljárás biztosítja az e-dokumentumok 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 autentikációciós *Tanúsítvány*a felhasználásával kölcsönös azonosításon alapuló SSL/TLS kapcsolatot létesít a *Minősített archiválási szolgáltató*val. A *Minősített archiválási szolgáltató* az *Előfizető*t az SSL/TLS kapcsolat felépítéséhez használt kliens autentikációciós *Tanúsítvány*a alapján azonosítja. Az *Előfizető* az SSL/TLS kapcsolaton keresztül tölthet fel e-dokumentumokat a *Minősített archiválási szolgáltató* archívumába. Az *Előfizető* Dublin Core szerinti [50] metaadatokat is megadhat az egyes elektronikus dokumentumokkal kapcsolatban. A metaadatokat elhelyezheti az e-dokumentumban, de feltöltéskor is megadhatja őket.

2. A *Minősített archiválási szolgáltató* a feltöltött e-dokumentum típusától függően ellenőrzi az e-dokumentum megfelelőségét az alábbiak szerint:

    - e-akta esetén 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 [52]. 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 úgynevezett keretaláírás is, amely az e-aktában lévő minden elektronikus dokumentum és az elektronikus 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 elektronikus dokumentumokat is tartalmaznak.

- PAdES formátumú e-dokumentum esetén a *Minősített archiválási szolgáltató* ellenőrzi, hogy a feltöltött PAdES formátumú e-dokumentum formátuma megfelel-e a támogatott formátumok valamelyikének. A PAdES formátumú e-dokumentum tartalmazhat további elektronikus dokumentumokat is, de az ezeken esetleg található elektronikus aláírások, bélyegzők érvényességét a *Minősített archiválási szolgáltató* nem vizsgálja. A PAdES formátumú e-dokumentum több egymásba ágyazott elektronikus aláírást vagy bélyegzőt is tartalmazhat. A *Minősített archiválási szolgáltató* valamennyi elektronikus aláírás vagy bélyegző érvényességét vizsgálja, de csak a legutolsó, külső szintű aláírás vagy bélyegző érvényességének megőrzését biztosítja. A *Minősített archiválási szolgáltató* megköveteli, hogy a feltöltött PAdES formátumú e-dokumentumon érvényes elektronikus aláírás vagy bélyegző és belső *Időbélyegző* legyen. Az elektronikus aláírást vagy bélyegzőt nem tartalmazó, az *Időbélyegző* nélküli, vagy külső *Időbélyegző*vel ellátott e-dokumentumokat a *Minősített archiválási szolgáltató* nem fogadja be az archívumba.
- ASiC formátumú e-dokumentum esetén a *Minősített archiválási szolgáltató* ellenőrzi, hogy a feltöltött e-dokumentum formátuma megfelel-e a támogatott formátumok valamelyikének. A feltöltött e-dokumentum egy vagy több elektronikus dokumentumot is tartalmazhat. Az e-dokumentum tartalmazhat további e-dokumentumokat is, de az ezekben található további elektronikus aláírások, bélyegzők érvényességét a *Minősített archiválási szolgáltató* nem vizsgálja. A *Minősített archiválási szolgáltató* az e-dokumentumban foglalt egyes elektronikus dokumentumokhoz rendelt külső elektronikus aláírások, bélyegzők mindegyikét ellenőrzi. Az e-dokumentumban foglalt külső elektronikus aláírások vagy bélyegzők egyike sem tartalmazhat másik aláírásra vagy bélyegzőre való hivatkozást, vagyis aláírást nem lehet újra aláírni. Az e-dokumentumban tárolt valamennyi elektronikus dokumentumnak érvényes aláírással vagy bélyegzővel és *Időbélyegző*vel kell rendelkeznie. A feltételek bármelyikét nem teljesítő e-dokumentum befogadását a *Minősített archiválási szolgáltató* megtagadja.

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-dokumentumban szereplő összes vizsgálandó 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 [56] szerint ellenőrzi és ETSI TS 101 903 [24] [25] [26] [27] szerinti formátumot hoz létre.

   A *Minősített archiválási szolgáltató* csak olyan adatok tekintetében nyújt archiválás szolgál-

tatást – azaz csak olyan e-dokumentumokat fogad be – amelyeken legalább fokozott biztonságú, PKI alapú 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-dokumentumot, 3 napig megőrzi mindazon információt, amely segíthet az elutasítás okának felderítésében. Ilyen információ többek között az e-dokumentumban 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-dokumentumot, ha az ellenőrzést 3 nap alatt nem tudja elvégezni.

   A *Minősített archiválási szolgáltató* felépíti az e-dokumentumokban szereplő elektronikus aláírásokhoz, bélyegzőkhöz tartozó érvényességi láncokat, és minősített archív elektronikus *Időbélyegző*t helyez el rajtuk. Az így kapott archiválási bizonyítékokat az e-dokumentum formátumának megfelelő formátumú ún. archív aláírásként elhelyezi az e-dokumentumban.

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-dokumentumot egy titkosított e-aktában. A befogadott e-dokumentum titkosítatlan példányait a *Minősített archiválási szolgáltató* megsemmisíti olyan eljárás alkalmazásával, ami biztosítja hogy az e-dokumentumot 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-dokumentumot 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-dokumentumot 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-dokumentum lenyomatát, illetve azt, hogy az archívum befogadta-e a dokumentumot. Ezen kívül sikeres befogadás esetén tartalmazza

   - az archívumba befogadott – már archív formátumú elektronikus aláírásokat, bélyegzőket tartalmazó – e-dokumentum lenyomatát, amely a továbbiakban egyedi

azonosítóként is szolgál,

- a *Minősített elektronikus 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 e-dokumentumban 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-dokumentumra vonatkozik (azaz a feltöltött e-dokumentum 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-dokumentumot. A *Minősített archiválási szolgáltató* kizárólag a pozitív visszajelzés elküldése esetén felel az e-dokumentum 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-dokumentumok bizalmasságát nem az SSL/TLS 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.

4.3. Érvényességi lánc/archiválási bizonyítékok elérhetőségének biztosítása - e-dokumentum letöltése

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

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

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

2. Az *Előfizető* megadja, hogy mely e-dokumentumokhoz kíván hozzáférni. A megfelelő e-dokumentum kiválasztásához a web felületen lehetősége van a dokumentumhoz kapcsolódó Dublin Core [50] szerinti metaadatok alapján keresni az e-dokumentumokra. A kiválasztás az e-dokumentumot egyértelműen azonosító lenyomat (hash) alapú azonosító segítségével történik.

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

4. Megfelelő jogosultság esetén a *Minősített archiválási szolgáltató* a megadott hash alapú azonosító alapján előkeresi az archívumban titkosított e-aktában tárolt e-dokumentumot, majd az e-dokumentum típusától függő módon eljuttatja azt az *Előfizető*höz az alábbiak szerint:

   - e-akta esetén átkódolja azt az *Előfizető* titkosító *Tanúsítvány*ához tartozó nyilvános kulccsal, majd az így újra titkosított e-aktát a védett SSL/TLS kapcsolaton keresztül eljuttatja az *Előfizető*höz.
   - PADES formátumú e-dokumentum esetén a visszafejtett e-dokumentumot nyílt formában, a védett SSL/TLS kapcsolaton keresztül eljuttatja az *Előfizető*höz.
   - ASiC formátumú e-dokumentum esetén a visszafejtett e-dokumentumot nyílt formában, a védett SSL/TLS kapcsolaton keresztül eljuttatja az *Előfizető*höz.

   A *Minősített archiválási szolgáltató* nem garantálja az e-dokumentum letölthetőségét, amennyiben az *Előfizető* az e-dokumentummal kapcsolatban korábban már törlési kérelmet nyújtott be.

   Egyes előfizetés típusok esetében a *Minősített archiválási szolgáltató* megtagadhatja az e-dokumentum letöltését, amennyiben az *Előfizető* már meghaladta a részére az adott időszakban rendelkezésre álló letöltési méret limitet.

5. Az e-akta formátumú tárolás esetén az *Előfizető* rendelkezik az archiválás szolgáltatás igénybevételére szolgáló titkosító *Tanúsítvány*ához tartozó magánkulccsal. Ezzel a kulccsal dekódolja az e-aktát, így hozzájut az archiválási bizonyítékokhoz 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-dokumentumait és archiválási bizonyítékait. 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.

Az adathordozó átadása történhet személyes találkozó keretében a *Minősített archiválási szolgáltató* megfelelő bizalmi szerepkört betöltő munkatársa által, vagy az *Előfizető* által előzetesen benyújtott ilyen irányú írásbeli kérelme alapján megbízható harmadik fél igénybe vételével.

A feltöltött e-dokumentumok az *Előfizető* tulajdonában vannak (lásd: 1.3.2 fejezet), így az *Előfizető* tölti be az adatgazda szerepét is. Amennyiben az e-dokumentumhoz harmadik fél is hozzáfér, ő az *Előfizető* nevében jár el.

4.4. Igazolás kibocsátása

A feltöltött e-dokumentumokkal kapcsolatban a *Minősített archiválási szolgáltató* az *Előfizető* kérésére igazolást állít ki. Az igazolás a következőket tartalmazza:

1. Azt az állítást, hogy az adott e-dokumentumon 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. Az e-dokumentum lenyomatát, az *Előfizető* nevét és azonosítóját.
3. Azt az állítást, hogy az adott e-dokumentum adott lenyomattal rendelkezik, így megegyezik azzal, amelynek a lenyomatát az *Előfizető* bemutatta vagy a *Minősített archiválási szolgáltató* segítségével előállította.
4. Az e-dokumentum archívumba fogadásának idejét.

A *Minősített archiválási szolgáltató* az igazolást papír alapon, vagy minősített elektronikus aláírással ellátott e-dokumentumban 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-dokumentum ismeretére, az a nyílt e-dokumentum nyíltan tárolt lenyomata alapján kerül kiállításra. A lenyomat értékből semmilyen információ nem nyerhető ki a tárolt e-dokumentum tartalmára vonatkozóan. Az alkalmazott megoldás biztosítja, hogy az archív igazolás kiállításáért felelős tisztviselők az igazolás kiállítása kapcsán nem ismerhetik meg a nyílt e-dokumentum tartalmát.

Az igazolás kibocsátása történhet olyan módon is, hogy az *Előfizető* bemutatja a *Minősített archiválási szolgáltató*nak a nyílt archivált e-dokumentumot. Ekkor, feltéve, hogy a bemutatott nyílt e-dokumentummal azonos lenyomatú e-dokumentum szerepel a *Minősített archiválási szolgáltató* archívumában, a *Minősített archiválási szolgáltató* felelős tisztviselője az *Előfizető* által bemutatott e-dokumentumra vonatkozóan állítja ki az igazolást.

Az *Előfizető* a *Minősített archiválási szolgáltató*hoz tetszőleges kézbesítési módon eljuttatott papíralapú, kézzel aláírt igénylés, vagy legalább minősített tanúsítványon alapuló 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, a meghatalmazott aláírását is tartalmazó meghatalmazását.

Az igazolás igényléséhez az *Előfizető* (vagy meghatalmazottja) meg kell, hogy adja az e-dokumentum lenyomatát amelyikkel kapcsolatban az igazolást kéri. Ezt az információt a 4.3 fejezetben lévő keresőfelületről is kinyerheti. Az igazolást a *Minősített archiválási szolgáltató* annak az *Előfizető*nek adja ki, akihez az adott e-dokumentum 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.

4.5. 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 e-dokumentumait a *Minősített archiválási szolgáltató* ügyfélszolgálati irodájában.

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

4.6. Dokumentum és érvényességi lánc/archiválási bizonyítékok törlése

A *Minősített archiválási szolgáltató* az *Előfizető* kérésére törli az archivált e-dokumentumot és a hozzá tartozó valamennyi archiválási bizonyítékot az archívumából. Ezen törlés a tárolt e-dokumentum 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-dokumentum minden mentett példányát megsemmisíti.

Törlési kérelem csak a Szolgáltatási szerződés érvényességi ideje alatt, a megőrzési idő vége előtt nyújtható be. Törlési kérelmet a *Minősített archiválási szolgáltató* ügyfélszolgálati irodájának kell benyújtani írásban, papíralapon aláírt vagy legalább fokozott biztonságú 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.

4.7. 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-dokumentumok és archiválási bizonyítékok letöltését.

A határidő lejárta után a *Minősített archiválási szolgáltató* az archívumból kitörli az *Előfizető*höz tartozó e-dokumentumokat és archiválási bizonyítékokat.

A *Minősített archiválási szolgáltató* a szerződés megszűnésekor történő törlés esetén is a 4.6. fejezetben leírt módon biztosítja, hogy a törölt e-dokumentumokat ne lehessen visszaállítani.

5. Műszaki biztonsági óvintézkedések

5.1. 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-dokumentumokat fizikailag biztonságos környezetben, a 6. 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-dokumentumokat saját munkatársai sem olvashatják el. A *Minősített archiválási szolgáltató* az e-dokumentumokat kizárólag akkor bocsátja harmadik fél (pl. hatóság) rendelkezésére, ha erre az *Előfizető* felhatalmazta, vagy ha ezt jogszabály írja elő.

A tárolt e-dokumentumok integritását az e-dokumentumok fizikai védelme, valamint az elektronikus aláírással kapcsolatos technológiák biztosítják. Az e-dokumentumok 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-dokumentumokat.

A *Minősített archiválási szolgáltató* az archivált e-dokumentumokat – az *Előfizető* kérése vagy a szerződés megszűnése esetén – a 4.6 fejezetben leírt feltételek mellett semmisíti meg. A *Minősített archiválási szolgáltató* a visszaigazolások aláírására használt kulcsokat, az archivált e-dokumentumok 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* titkosított e-aktában tárolja az e-dokumentumokat. A *Minősített archiválási szolgáltató* az e-dokumentumokat 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-dokumentum biztonságos algoritmussal történő újra-titkosításáról. A nyílt e-dokumentumokat kizárólag az elektronikus archiválás nyújtásához kapcsolódó jogszabályi követelmények teljesítéséhez állítja vissza, azaz a 4.3., a 5.4. és 5.5. fejezetekben leírt esetekben.

5.2. 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.

5.3. 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.

5.4. Rendszeres felülhitelesítés

A *Minősített archiválási szolgáltató* az érvényességi láncokon köteles minősített szolgáltató által kibocsátott időbélyegzőt elhelyezni vagy elhelyeztetni az alábbi esetekben:

- ha a Nemzeti Média- és Hírközlési Hatóság ilyen határozatot hoz;
- a Nemzeti Média- és Hírközlési Hatóságnak a *Minősített archiválási szolgáltató* elleni végelszámolási eljárás megindításáról vagy felszámolásának elrendeléséről megküldött kötelező tájékoztatást követően.

5.5. Az archívum újra-titkosítása

A *Minősített archiválási szolgáltató* az archivált e-dokumentumokat titkosított e-aktában tárolja az archívumában. Biztosítja, hogy az archivált e-dokumentumok mindenkor biztonságos algoritmussal kerülnek titkosításra.

A *Minősített archiválási szolgáltató* a titkosításhoz jelenleg AES 256 algoritmust használ e-aktánként egyedi kulccsal. Az egyedi szimmetrikus titkosító kulcsot a *Minősített archiválási szolgáltató* 2048 bites RSA alapú titkosító kulcsa védi.

A *Minősített archiválási szolgáltató* gondoskodik róla, hogy az e-dokumentumok 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 elektronikus archiválási szolgáltatási szabályzat* vagy az *Előfizető*vel kötött szerződés így rendelkezik.

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

5.6. 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.

5.7. 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/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.

5.8. Az elektronikus dokumentumok 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* a műszaki értelemben vett olvashatóságot biztosítja, így nem vállal felelősséget a fájlok tartalmának értelmezhetőségéért (pl. hibás szkennelés következtében feltöltött üres, de szabályos formátumú .PDF fájl.)

A *Minősített archiválási szolgáltató* olyan formátumú fájlokat tartalmazó e-dokumentumokat is befogad az archívumába, amelynek tekintetében nem biztosít olvashatóságot és értelmezhetőséget. A *Minősített archiválási szolgáltató* az elektronikus dokumentumok megőrzését, tehát a elektronikus dokumentumok olvashatóságának fenntartását is a szolgáltatási szerződés érvényességi idejéig vállalja. A szolgáltatás leállításakor a *Minősített archiválási szolgáltató* a 6.7 fejezetben leírtak szerint átadja a szolgáltatást egy másik szolgáltatónak. Ekkor a *Minősített archiválási szolgáltató* az archivált e-dokumentumok 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) [38],
- ISO 8859-1:1998 (Latin-1, 8 bites grafikus karakterkészlet) [39],
- ISO 8859-2:1999 (Latin-2) [40], a magyar referenciakészletre vonatkozóan az MSZ 7795-3:1992 [44] ASCII és ASCII/PC kód szerinti eltéréssel is,
- ISO 10646:2003 (Unicode v.4.0) [41],
- Microsoft Rich Text Format 1.7. [53],
- Microsec e-akta formátum minden verziója [52],
- XAdES ETSI TS 101 903 v1.2.2 [24], v1.3.2 [25], v1.4.1 [26] and v1.4.2 [27], formátumú XAdES aláírások (amennyiben egy XML fájl XAdES aláírást tartalmaz, a *Minősített archiválási szolgáltató* az aláírás értelmezhetőségét biztosítja),
- XAdES Baseline Profile ETSI TS 103 171 v2.1.1 [33],
- CAdES ETSI TS 101 733 v1.8.1 [22],
- CAdES Baseline Profile ETSI TS 101 733 v2.1.1 [23],
- ASiC ETSI TS 102 918 v1.3.1 [32],
- PAdES ETSI TS 102 778 -1 v1.1.1 [28], -2 v1.2.1 [29], -3 v1.1.2 [30], -4 v1.1.2 [31],
- ETSI EN 319 122-1 [10] formátumú CAdES aláírások
- ETSI EN 319 122-2 [11] formátumú CAdES aláírások

- ETSI EN 319 132-1 [12] formátumú XAdES aláírások
- ETSI EN 319 132-2 [13] formátumú XAdES aláírások
- ETSI EN 319 142-1 [14] formátumú PAdES aláírások
- ETSI EN 319 142-2 [15] formátumú PAdES aláírások
- ETSI EN 319 162-1 [16] formátumú ASiC aláírások
- ETSI EN 319 162-2 [17] formátumú ASiC aláírások
- IETF RFC 2822 (Internet Message Format) [46],
- IETF RFC 2045 (Multipurpose Internet Mail Extensions, MIME) [45],
- Az elektronikus cégeljárásban használt XML formanyomtatványok [1],
- 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 elektronikus 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 [46]) 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 [45]) 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*

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

akkor biztosítja egy (fenti formátumú) fájl értelmezhetőségét, megjeleníthetőségét, ha az egy e-dokumentumban 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-dokumentumok olvashatóságát, megjeleníthetőségét is vállalja. Ez az aláírások, bélyegzők és *Időbélyegző*k ellenőrizhetőségéig, és az e-dokumentumokban elhelyezett fájlok kinyeréséig terjed.

A fájl formátumok meghatározása az e-dokumentumban foglalt "mimeType" érték alapján történik, ennek hiányában a *Minősített archiválási szolgáltató* az adott elektronikus dokumentum formátumát ismeretlennek tekinti és nem biztosítja az elektronikus dokumentum értelmezhetőségét. A *Minősített archiválási szolgáltató* csak az alábbi listában szereplő "mimeType" értékek használatát támogatja:

- text/txt
- application/xml
- text/xml
- text/plain
- application/pdf
- application/eszigno3
- application/vnd.eszigno3+xml
- application/octet-stream(dosszie)
- application/octet-stream(es3)
- application/nldossier2
- application/octet-stream(xml)
- application/octet-stream(pdf)

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* nem végez ellenőrzést végez arra vonatkozóan, hogy a feltöltött e-dokumentum tartalmaz-e olyan aktív kódot, ami a dokumentum megjelenítése során változást okozhat.

Egy e-dokumentum befogadásakor a *Minősített archiválási szolgáltató* automata segítségével megvizsgálja, hogy az adott e-dokumentumban lévő fájlok rendelkezhetnek-e a támogatott formátumok valamelyikével. Amelyek nem rendelkeznek támogatott formátummal, azok esetén elutasítja az olvashatóság fenntartását. A 4.2. 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.

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

Az e-dokumentumok feltöltése szolgáltatást a *Minősített archiválási szolgáltató* jogosult szüneteltetni.

A *Minősített archiválási szolgáltató* ügyfélszolgálati irodája minden munkanapon, nyitvatartási időben fogad igazolás kibocsátására vonatkozó kérelmeket; az igazolások kibocsátása 5 munkanap alatt történik meg.

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

6. 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.

6.1. 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 szigorúban 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.

6.1.1. 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, videó 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.

6.1.2. 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.

6.1.3. 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.

6.1.4. 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.

6.1.5. 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.

6.1.6. 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.

6.1.7. 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.

6.1.8. 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.

A mentett állományokból legalább évente szúrópróbaszerű kiválasztással jegyzőkönyvezett helyreállítási tesztet végez.

6.2. 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.

6.2.1. 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 elektronikus dokumentum visszafejtésére. Az archiválási tisztviselők felelősek a visszafejtett elektronikus dokumentum 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.

6.2.2. 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 elektronikus dokumentumok visszafejtéséhez. Az archiválási tisztviselők felelősek a visszafejtett elektronikus dokumentum biztonságos kezeléséért illetve a felhasználás utáni megsemmisítéséért.

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

6.2.3. 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.

6.2.4. 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.

6.3. 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.

6.3.1. 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. A bizalmi szerepkört betöltő személyeknek mentesnek kell lenniük az összeférhetetlenségtől, amely veszélyeztethetné a *Minősített archiválási szolgáltató* tevékenységének pártatlanságát.

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.

6.3.2. 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, úgy mint előző munkahely, szakmai referenciák, legfontosabb képzettség.

6.3.3. 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.

6.3.4. 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 képzési anyag legalább 12 havonta felülvizsgálatra kerül, és tartalmazza az új fenyegetéseket és biztonsági megoldásokat.

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

6.3.5. Munkabeosztás körforgásának sorrendje és gyakorisága

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

6.3.6. 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.

6.3.7. 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.

6.3.8. 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;
- aláírandó 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.

6.4. Naplózási eljárások

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

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

Minden új naplóbejegyzés hozzáadódik a korábban elmentett bejegyzésekhez, az egyszer már elmentett bejegyzés nem kerülhet módosításra vagy törlésre.

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:

- BELSŐ ÓRA
  - a belső óra szinkronizációja az UTC időhöz, beleértve az üzemszerű újrakalibrálásokat is;
  - a szinkronizáció elvesztése;
- 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, elmentés, betöltés, megsemmisítés stb.);
- TanúsítványY KEZELÉS
- ADATMOZGÁSOK
  - bármilyen, a biztonság szempontjából kritikus adat manuális bevitele a rendszerbe;
  - a rendszer által fogadott, biztonsági szempontból fontos adatok, üzenetek;
- *HSM eszköz*
  - *HSM eszköz* installálása;
  - *HSM eszköz* eltávolítása;
  - *HSM eszköz* selejtezése, megsemmisítése;
  - *HSM eszköz* szállítása;
  - *HSM eszköz* tartalmának törlése (nullázás);
  - *HSM eszköz* feltöltése kulcsokkal, tanúsítványokkal;
- KONFIGURÁCIÓ VÁLTOZÁSA
  - hardver;
  - szoftver;
  - operációs rendszer;
  - javító csomag;
- FIZIKAI HOZZÁFÉRÉS, TELEPHELY BIZTONSÁG
  - személy belépése a bizalmi szolgáltatást nyújtó rendszer komponenseket tartalmazó biztonsági területre és onnan kilépése;
  - hozzáférés egy bizalmi szolgáltatást nyújtó 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 elektronikus 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.

6.4.2. 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. Az automatizált ellenőrző rendszerekből kapott értesítéseket az IT üzemeltetés munkatársai 24 órán belül feldolgozzák és az eredményeket kiértékelik.

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

6.4.3. A naplófájl megőrzési időtartama

Az online rendszerből való kitörlés előtt a naplóállományokat a *Minősített archiválási szolgáltató* archiválja és gondoskodik azok biztonságos megőrzéséről az 6.5.2 fejezetben meghatározott ideig, de legalább a keletkezésüktől számított 10 évig.

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

6.4.4. 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.

6.4.5. 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.

6.4.6. 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.

6.4.7. 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.

6.4.8. Sebezhetőség felmérése

A naplóbejegyzések napi rendszerességgel végzett feldolgozásán túl a *Minősített archiválási szolgáltató* szakemberei figyelik a nyilvánosan elérhető információt a lehetséges sérülékenységekről, szoftver javító csomagokról. Elemzik a gyűjtött információt, osztályba sorolják a sérülékenységet és szükség esetén értesítik a vezetőséget az eredményről és intézkedési tervet javasolnak a rendszer biztonságának növelésére.

Minden nagyobb jelentőségű feltárt hiányosság vagy külső fenyegetettség esetén az észlelésétől számított 48 órán belül, 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*

- intézkedési tervet hoz létre és hajt végre a sérülékenységek megszüntetése érdekében, vagy
- dokumentálja a döntés alapjául szolgáló tényeket, elfogadja a maradvány kockázatokat és nem hoz intézkedési tervet a sérülékenység megszüntetésére.

Az új program verziókat vagy program javító csomagokat a *Minősített archiválási szolgáltató* először a teszt rendszeren telepíti és csak a sikeres tesztek elvégzése után kerülnek telepítésre a szolgáltatásokat nyújtó éles rendszeren.

Az új szoftver verziók vagy javító csomagok nem kerülnek bevezetésre az éles rendszeren, amennyiben olyan további sérülékenységet vagy instabilitást okoznak a rendszer működésében, ami nagyobb gondot eredményez az alkalmazásukból származó előnynél. Az alkalmazás mellőzésének okát a *Minősített archiválási szolgáltató* dokumentálja.

6.5. Adatok archiválása

6.5.1. 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 elektronikus archiválási rend*(ek) valamennyi kibocsátott verziója;
- a *Minősített elektronikus 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.

6.5.2. Az archívum megőrzési időtartama

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

- a *Minősített elektronikus archiválási rend*et a hatályon kívül helyezéstől számított legalább 10 évig;
- a *Minősített elektronikus archiválási szolgáltatási szabályzat*ot a hatályon kívül helyezéstől számított legalább 10 évig;
- Általános Szerződési Feltételeket a hatályon kívül helyezéstől számított legalább 10 évig;
- minden egyéb archiválandó dokumentomot a keletkezésétől számított legalább 10 évig.

6.5.3. 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.

6.5.4. Az archívum mentési folyamatai

A *Minősített archiválási szolgáltató* a papír alapú dokumentumok eredeti példányáról hiteles elektronikus másolatot készít a vonatkozó jogszabályok betartásával.

Az elektronikus másolatokat a többi védendő elektronikus dokumentummal azonos szabályok szerint tárolja.

A *Minősített archiválási szolgáltató* a hiteles elektronikus másolatok archiválása után az eredeti papír alapú dokumentumokat megsemmisítheti.

6.5.5. Az adatok időbélyegzésére vonatkozó követelmények

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

Az időpontot a *Minősített archiválási szolgáltató* belső órája adja, amelyet a *Minősített archiválási szolgáltató* két egymástól független Stratum-1 UTC referencia időforrással szinkronizál:

- az egyik pontos idő forrás a műhold alapú GPS jelet használja;
- a másik pontos idő forrás a hosszúhullámú pontos idő szolgáltatásra (DCF77) támaszkodik.

A *Minősített archiválási szolgáltató* a fenti két független Stratum-1 időforráshoz 0,1 másodperc pontossággal szinkronizálja saját belső óráját. E szinkronizációt a *Minősített archiválási szolgáltató* naponta legalább négy alkalommal elvégzi.

A *Minősített archiválási szolgáltató* a belső óra pontosságának ilyen szinten tartásával garantálja, hogy valamennyi időjelzés pontossága legfeljebb 1 másodperccel tér el az UTC időalaptól.

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.

6.5.6. 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.

6.5.7. 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.

6.6. 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.

6.6.1. 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 bizalmi szolgáltatásokat nyújtó informatikai rendszerét, hogy bármely egy eszköz kiesése esetén képes zavartalanul folytatni a bizalmi szolgáltatások nyújtását.

6.6.2. 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.

6.6.3. 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.

6.7. Az Archiválási szolgáltatás leállítása

A *Minősített archiválási szolgáltató* a szolgáltatás 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 elektronikus dokumentumok 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 elektronikus dokumentumaik letöltésére.

A *Minősített archiválási szolgáltató* a tervezett leállás előtt legalább 20 nappal, de az *Ügyfel*ek értesítését követően legalább 14 nappal leállítja a következő szolgáltatásait:

- Igazolások kiadása a tárolt elektronikus dokumentumokról

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

- archívumban tárolt elektronikus dokumentumok letöltése,
- műszaki segítségnyújtás,
- információ szolgáltatás.

A *Minősített archiválási szolgáltató* a tervezett megszűnés előtt tárgyalásokat kezd más vele azonos besorolású bizalmi szolgáltatókkal szolgáltatásainak átvételéről. Nyilvántartásait a bizalmas felhasználói adatokkal együtt a 9.3 fejezet szerint mindenképpen átadja egy ilyen bizalmi 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 bizalmi szolgáltatónak – az adatokat az új bizalmi szolgáltató által fogadni képes médián és formátumban helyezi el vagy biztosítja az új bizalmi 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 4.6. fejezetben leírt módon.

7. 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 magánkulcsokat teljes életciklusuk alatt megfelelő tanúsítással rendelkező *HSM eszköz*ökben kezeli.

Mind a *Minősített archiválási szolgáltató*, mind a rendszert szállító és kivitelező vállalkozók jelentős tapasztalatokkal rendelkeznek PKI alapú rendszerek és bizalmi szolgáltatások 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.

7.1. 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.

7.1.1. Kriptográfiai modulra vonatkozó szabványok és előírások

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

- megfelelnek az ISO/IEC 19790 [43] követelményeinek,
- vagy megfelelnek a FIPS 140-2 [54] 3-as, illetve annál magasabb szintű követelményeknek,
- vagy megfelelnek a CEN 14167-2 [55] munkacsoport egyezmény követelményeinek,
- vagy megfelelnek a CEN 419 221-5 [37] követelményeinek,
- vagy olyan megbízható rendszerek, amely az MSZ/ISO/IEC 15408 [42] 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 *Minősített archiválási szolgáltató* a szolgáltatói magánkulcsokat a *HSM eszköz*ön kívül csak kódolt formában tárolja. A kódoláshoz csak az Eüt. [6] 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.

7.1.2. 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.

7.1.3. Magánkulcs letétbe helyezése

A *Minősített archiválási szolgáltató* a szolgáltatói magánkulcsait nem helyezi letétbe.

7.1.4. Magánkulcs mentése

A *Minősített archiválási szolgáltató* biztonsági másolatot készít minden szolgáltatói magánkulcsáról még a magánkulcs használatbavételét megelőzően a 7.1.1. 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 7.1.2. fejezetben leírt védelmi mechanizmus mellett végezhető.

A *Minősített archiválási szolgáltató* a biztonsági másolatot 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.

7.1.5. Magánkulcs archiválása

A *Minősített archiválási szolgáltató* nem archiválja magánkulcsait.

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

A *Minősített archiválási szolgáltató* valamennyi szolgáltatói magánkulcsát a követelményeknek megfelelő *HSM eszköz*ben állítja elő.

A magánkulcsok nem léteznek nyílt formában a *HSM eszköz*ön kívül.

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

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

A szolgáltatói magánkulcsok exportálása vagy betöltése minden esetben a 7.1.2. fejezetben leírt módon történik.

7.1.7. Magánkulcs tárolása hardver kriptográfiai eszközben

A *Minősített archiválási szolgáltató* a szolgáltatás nyújtásához használt magánkulcsait a 7.1.1. fejezet szerinti kriptográfiai modulokban tartja.

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

7.1.8. A magánkulcs aktiválásának módja

A *Minősített archiválási szolgáltató* szolgáltatói magánkulcsait biztonságos *HSM eszköz*ben tárolja, a használat során betartja a *HSM eszköz* felhasználói útmutatójában és a tanúsítási dokumentumokban megfogalmazott követelményeket. A *HSM eszköz*t csak a hozzá tartozó operátori kártyákkal lehet aktiválni, a *HSM eszköz*ben lévő magánkulcsokat a modul aktiválása előtt nem lehet használni. A *HSM 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.

7.1.9. A magánkulcs deaktiválásának módja

A *Minősített archiválási szolgáltató* által használt hardver kriptográfia eszközök által kezelt szolgáltatói 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.

7.1.10. 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 *HSM eszköz*ében tárolt szolgáltatói magánkulcsok megsemmisítését a felhasznált *HSM 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.

A *Minősített archiválási szolgáltató* dokumentált módon megsemmisíti a magánkulcsról készült minden mentett példányt olyan módon, hogy annak visszaállítása, használata lehetetlenné váljon.

7.1.11. A hardver kriptográfiai eszközök értékelése

A 7.1.1 fejezet előírásaival összhangban a *Minősített archiválási szolgáltató* valamennyi szolgáltatói magánkulcsát olyan *HSM eszköz*ben tárolja, amely rendelkezik:

- ISO/IEC 19790 [43] szerinti tanúsítvánnyal,
- vagy FIPS 140-2 Level 3 [54] szerinti tanúsítvánnyal,
- vagy a CEN 14167-2 [55] munkacsoport egyezmény követelményeinek való megfelelést igazoló legalább EAL-4 szintű Common Criteria alapú tanúsítvánnyal,
- vagy a CEN 419 221-5 [37] követelményeinek való megfelelést igazoló legalább EAL-4 szintű Common Criteria alapú tanúsítvánnyal,
- vagy 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.

7.2. Aktivizáló adatok

7.2.1. Aktivizáló adatok előállítása és telepítése

A *Minősített archiválási szolgáltató* a felhasznált *HSM 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.

7.2.2. 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.

7.2.3. Az aktivizáló adatok kezelésének egyéb szempontjai

Nincs megkötés.

7.3. Informatikai biztonsági előírások

7.3.1. 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.

7.3.2. Az informatikai biztonság értékelése

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.

A minőségirányítási rendszer és az információbiztonság-irányítási rendszer hatóköre kiterjed a Microsec által nyújtott bizalmi szolgáltatásokra is.

A Microsec kétszintű kockázatelemzése az információ technológiai kockázatokon túlmenően kiterjed a teljes szervezetre és az üzleti kockázatokra is. A kockázatelemzés legalább évente felülvizsgálatra kerül. A kockázatelemzés eredménye alapján a *Minősített archiválási szolgáltató*

- intézkedéseket hoz a feltárt sérülékenységek megszüntetésére, és/vagy
- elfogadja az azonosított maradvány kockázatokat a döntés indokainak rögzítésével.

7.4. Életciklusra vonatkozó műszaki előírások

7.4.1. 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* saját maga által kifejlesztett egyedi hardver és szoftver megoldások, amelyek tervezése során strukturált fejlesztési módszereket és ellenőrzött fejlesztési környezetet használt;
- 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.

7.4.2. 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 *HSM 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 *HSM eszköz*ből a *Minősített archiválási szolgáltató* törli a szolgáltatói kulcsokat.
A *Minősített archiválási szolgáltató* a használaton kívüli *HSM eszköz*öket fizikailag védett helyszínen tárolja.

7.4.3. Életciklusra vonatkozó biztonsági előírások

A *Minősített archiválási szolgáltató* gondoskodik a felhasznált *HSM 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 *HSM eszköz*öket használ rendszereiben;
- a *HSM eszköz*ök átvételekor a minőség ellenőrzése során meggyőződik róla, hogy a szállítás folyamán biztosították a *HSM eszköz*ök feltörés elleni védelmét;
- a *HSM eszköz*öket biztonságos helyen tárolja, a tárolás során biztosítja a *HSM eszköz*ök feltörés elleni védelmét;
- az üzemeltetés során folyamatosan betartja a *HSM eszköz*ök biztonsági előirányzatában, használati útmutatójában és a tanúsítási jelentésben szereplő követelményeket;
- a használatból kivont *HSM eszköz*ökben tárolt magánkulcsokat olyan módon törli, hogy lehetetlené válik a kulcsok visszaállítása;
- a használatból kivont *HSM eszköz*öket a biztonsági előirányzatában, használati útmutatójában és a tanúsítási jelentésben szereplő követelményeknek megfelelően kezeli és semmisíti meg.

7.5. 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:

- IT rendszereit jól elválasztott biztonsági zónákra osztja;
- elkülöníti az IT rendszer üzemeltetését támogató rendszereit az éles szolgáltatást nyújtó rendszereitől;
- elkülöníti az éles szolgáltatást nyújtó rendszereit a fejlesztésre és tesztelésre szolgáló rendszerektől;
- az elkülönített megbízható rendszerek között csak olyan megbízható kommunikációs csatornákon keresztül létesít kapcsolatot, amelyek logikailag el vannak választva más kommunikációs csatornáktól, megbízható végponti azonosítást használnak és védik a csatornákon küldött adatokat a módosítástól és a felfedéstől;
- az éles szolgáltatást nyújtó IT rendszereit biztonságos hálózati zónában üzemelteti;
- a zónákhoz való hozzáférést és a zónák közötti kommunikációt csak a szolgáltatás nyújtásához szükségesre korlátozza;
- letiltja a nem használt protokollokat és felhasználókat;
- letiltja a használaton kívüli hálózati portokat és szolgáltatásokat;
- csak az IT rendszer megfelelő működéséhez feltétlenül szükséges hálózati alkalmazásokat futtat.
- a használt szabályrendszert rendszeresen felülvizsgálja.

A *Minősített archiválási szolgáltató* sérülékenységvizsgálatot végez vagy végeztet a *Minősített archiválási szolgáltató* nyilvános és privát IP címein:

- a CA/Browser Forum kérésétől számított egy héten belül;
- a *Minősített archiválási szolgáltató* által jelentősnek minősített rendszer vagy hálózati változtatás után;
- legalább minden három (3) hónapban.

A *Minősített archiválási szolgáltató* legalább 3 havonta ellenőrzi a helyi hálózati eszközök (pl. router) konfigurációjának megfelelőségét a *Minősített archiválási szolgáltató* által meghatározott követelményeknek.

A *Minősített archiválási szolgáltató* évente illetve az informatikai rendszerén történt minden jelentős változás után sebezhetőségvizsgálatot végeztet egy külső, független szakemberrel, aki rendelkezik az ilyen vizsgálat elvégzéséhez szükséges képességekkel, szakértelemmel, eszközökkel és etikai kódexekkel.

7.6. 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.

8. 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 elektronikus archiválási rend*(ek)ben és az ennek megfelelő *Minősített elektronikus 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; [19]
- ETSI EN 319 401 V2.2.1 (2018-04); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [18]
- ETSI TS 119 511 V1.1.1 (2019-06); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques [35]

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

A megfelelőségértékelési jelentés alapján kiállított megfelelőségi tanúsítványt a *Minősített archiválási szolgáltató* honlapján közzéteszi.

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

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).

8.1. Az ellenőrzések körülményei és gyakorisága

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

8.2. 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 végzi el, amely rendelkezik egy EU tagállam nemzeti akkreditációs szervezete által kiadott erre feljogosító felhatalmazással.

8.3. 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.

8.4. Az auditálás által lefedett területek

Az átvizsgálás lefedi az alábbi területeket:

- hatályos jogszabályoknak való megfelelés;
- műszaki szabványoknak való megfelelés;
- *Minősített elektronikus archiválási rend*(ek)nek és *Minősített elektronikus 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.

8.5. 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.

8.6. Az eredmények közzététele

A *Minősített archiválási szolgáltató* a vizsgálat eredményét összefoglaló jelentést nyilvánosságra hozza honlapján az alábbi linken:

`https://e-szigno.hu/eidas/`

A feltárt hiányosságok részleteit nem publikálja, azokat bizalmas információként kezeli.

9. Egyéb üzleti és jogi kérdések

9.1. 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 hatálybalépése előtt 30 nappal a *Minősített archiválási szolgáltató* a honlapján közzéteszi. Az *Ügyfél* számára kedvező változások a 30 naposnál rövidebb határidővel is bevezethetők. 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.

9.1.1. Visszatérítési politika

Lásd: 9.1. fejezet.

9.2. Anyagi felelősségvállalás

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

9.2.1. Pénzügyi követelmények

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

9.2.2. Felelősségbiztosítás

- A *Minősített archiválási szolgáltató* a megbízhatóság biztosítása érdekében felelősségbiztosítással rendelkezik.
- A felelősségbiztosítási szerződés kiterjed az alábbi, a *Minősített archiválási szolgáltató* által a szolgáltatások nyújtásával összefüggésben okozott károkra:
  - a bizalmi szolgáltatási *Ügyfél*nek a Szolgáltatási szerződés megszegésével összefüggésben okozott károkra;
  - a bizalmi szolgáltatási *Ügyfél*nek és harmadik személynek szerződésen kívüli okozott károkra;
  - a Nemzeti Média- és Hírközlési Hatóságnak a bizalmi szolgáltatási tevékenységet befejező *Minősített archiválási szolgáltató* által okozott költségekre;
  - az eIDAS Rendelet [1] 17. cikk (4) bekezdés e) pontja alapján a Nemzeti Média- és Hírközlési Hatóság által felkért megfelelőségértékelő szervek eljárásának költségeire, ha azt a Nemzeti Média- és Hírközlési Hatóság eljárási költségként érvényesíti.
- A biztosítási szerződésben szereplő felelősségvállalási érték káreseményenként legalább 3.000.000 forint. Több azonos okból bekövetkezett, időben összefüggő káresemény egy biztosítási eseménynek minősül.
- A felelősségbiztosítás a meghatározott összeg erejéig fedezetet nyújt a károsultnak a szolgáltató károkozó magatartásával összefüggésben keletkező teljes kárára, függetlenül attól, hogy a kárt szerződésszegéssel vagy szerződésen kívül okozták.
- 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.

9.3. Bizalmasság

A *Minősített archiválási szolgáltató* az *Ügyfel*ek adatait a jogszabályoknak megfelelően kezeli. A *Minősített archiválási szolgáltató* rendelkezik adatkezelési szabályzattal (lásd 9.4 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.

9.3.1. Bizalmas információk köre

A *Minősített archiválási szolgáltató* bizalmas információként kezeli:

- az *Ügyfel*ek minden adatát, kivéve azokat, amelyeket a 9.3.2. fejezetben nem bizalmasnak tekintett információnak minősít;
- az *Ügyfel*ek adatain kívül:
  - az *Előfizető*k archívumban tárolt elektronikus dokumentumait a 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.

9.3.2. 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.

9.3.3. 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 [4] rendelkezéseinek megfelelően kezeli, és kizárólag az alábbi esetben fedi fel azokat:

- **Információszolgáltatás a hatóságok részére**

  A *Minősített archiválási szolgáltató* az Eüt. [6] 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.

9.4. 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 [4] és a 2016/679 EU általános adatvédelmi rendelet [2] 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.

9.4.1. Adatkezelési terv

A *Minősített archiválási szolgáltató* rendelkezik Adatvédelmi Szabályzattal és Adatkezelési Tájékoztatóval, amelyek részletes előírásokat tartalmaznak a személyes adatok kezelésére.

Az Adatvédelmi Szabályzat megtalálható az e-Szignó Hitelesítés Szolgáltató honlapján az alábbi linken:

`https://e-szigno.hu/minden-dokumentum.html`

Az Adatkezelési Tájékoztató megtalálható az e-Szignó Hitelesítés Szolgáltató honlapján az alábbi linken:

`https://e-szigno.hu/adatkezelesi-tajekoztato.html`

9.4.2. 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.

9.4.3. Személyes adatnak nem minősülő adatok

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

9.4.4. 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.

9.4.5. 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.

9.4.6. Adatkezelés

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

9.4.7. Egyéb adatvédelmi követelmények

Nincs előírás.

9.5. Szellemi tulajdonjogok

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

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

A jelen *Minősített elektronikus 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.

9.6. Tevékenységért viselt felelősség és helytállás

9.6.1. A szolgáltató felelőssége és helytállása

A Szolgáltató felelőssége

A *Minősített archiválási szolgáltató* felelősségét jelen *Minősített elektronikus archiválási szolgáltatási szabályzat*, a vonatkozó *Minősített elektronikus 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 elektronikus 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 [5] 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 [5] 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 9.8. 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 szolgáltatást a *Minősített elektronikus archiválási rend*del, a *Minősített elektronikus archiválási szolgáltatási szabályzat*tal, az Általános Szerződési 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 (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.

9.6.2. 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 elektronikus archiválási szolgáltatási szabályzat*, a Szolgáltatási szerződés és annak elválaszthatatlan részét képező Általános Szerződési Feltételek, valamint a vonatkozó *Minősített elektronikus archiválási rend* tartalmazzák.

Az *Előfizető* jogai

Az *Előfizető* jogosult:

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

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

9.6.4. Egyéb szereplők tevékenységéért viselt felelősség és helytállás

Nincs megkötés.

9.7. Helytállás érvénytelenségi köre

A *Minősített archiválási szolgáltató* kizárja felelősségét, amennyiben:

- 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.

9.8. A felelősség korlátozása

Nincs megkötés.

9.9. Kártérítési kötelezettség

9.9.1. A szolgáltató kártérítési kötelezettsége

A *Minősített archiválási szolgáltató* kártérítési kötelezettségének részletes szabályait jelen szabályzat (lásd: 9.8. fejezet), a Szolgáltatási szerződés és az *Ügyfel*ekkel kötött szerződések tartalmazzák.

9.9.2. 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.

9.9.3. Az érintett felek kártérítési kötelezettsége

Lásd: 9.8. fejezet

9.10. Érvényesség és megszűnés

9.10.1. Érvényesség

A *Minősített elektronikus archiválási szolgáltatási szabályzat* adott verziója hatálybalépésének napja a dokumentum címlapján kerül meghatározásra.

9.10.2. Megszűnés

A *Minősített elektronikus archiválási szolgáltatási szabályzat* visszavonásig illetve a *Minősített elektronikus archiválási szolgáltatási szabályzat* újabb verziójának hatályba lépéséig hatályos időbeli korlátozás nélkül.

9.10.3. A megszűnés következményei

A *Minősített elektronikus 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 elektronikus archiválási szolgáltatási szabályzat* visszavonása esetén is érvényben maradnak a bizalmas adatok védelmére vonatkozó előírások.

9.11. 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.

9.12. 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 elektronikus archiválási szolgáltatási szabályzat*ot.

9.12.1. 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 elektronikus archiválási szolgáltatási szabályzat* több ilyet is megemlít). A 8.4. fejezetben leírt eljárások ezeket a dokumentumokat is vizsgálják.

A *Minősített archiválási szolgáltató* 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 elektronikus 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.

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

A *Minősített archiválási szolgáltató* a közzétett új szabályzat tervezettel kapcsolatos észrevételeket a hatálybalépést 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 hatálybalépést megelőző 7. napon zárja le és teszi közzé.

9.12.2. Értesítések módja és határideje

A *Minősített archiválási szolgáltató* a 9.12.1. pontban leírtak szerint értesíti az *Érintett felek*et az új dokumentum verziók kibocsátásáról.

9.12.3. Az OID megváltoztatása

A *Minősített archiválási szolgáltató* a *Minősített elektronikus 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.

9.13. 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.

Az *Ügyfél* vitás kérdés felmerülése esetén jogosult az esetleges bírósági eljárást megelőzően a Budapesti Békéltető Testülethez fordulni.

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.

9.14. 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.

9.15. 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];
- 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];
- 24/2016. (VI. 30.) BM rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről [7];
- 25/2016. (VI. 30.) BM rendelet a bizalmi felügyeletnek fizetendő igazgatási szolgáltatási díjak mértékéről [8];
- 470/2017. (XII. 28.) Kormányrendelet a bizalmi felügyelet által vezetett nyilvántartások tartalmáról és a bizalmi szolgáltatás nyújtásával kapcsolatos bejelentésekről [9];

9.16. Vegyes rendelkezések

9.16.1. Teljességi záradék

Nincs megkötés.

9.16.2. Átruházás

A jelen *Minősített elektronikus 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.

9.16.3. Részleges érvénytelenség

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

9.16.4. 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 elektronikus archiválási szolgáltatási szabályzat* más rendelkezésének megsértése esetén is lemondana a kártérítési igény érvényesítéséről.

9.16.5. Vis maior

A *Minősített archiválási szolgáltató* nem felelős a *Minősített elektronikus archiválási rend*ben és a *Minősített elektronikus 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.

9.17. Egyéb rendelkezések

Nincs megkötés.

A. 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] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) .

[3] 2001. évi XXXV. törvény az elektronikus aláírásról (hatályon kívül helyezve 2016. július 1-től) .

[4] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról .

[5] 2013. évi V. törvény a Polgári Törvénykönyvről .

[6] 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól .

[7] 24/2016. (VI. 30.) BM rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről .

[8] 25/2016. (VI. 30.) BM rendelet a bizalmi felügyeletnek fizetendő igazgatási szolgáltatási díjak mértékéről .

[9] 470/2017. (XII. 28.) Korm. rendelet a bizalmi felügyelet által vezetett nyilvántartások tartalmáról és a bizalmi szolgáltatás nyújtásával kapcsolatos bejelentésekről .

[10] ETSI EN 319 122-1 V1.1.1 (2016-04) Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures.

[11] ETSI EN 319 122-2 V1.1.1 (2016-04) Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures.

[12] 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.

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

[14] ETSI EN 319 142-1 V1.1.1 (2016-04) Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures.

[15] ETSI EN 319 142-2 V1.1.1 (2016-04) Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles.

[16] ETSI EN 319 162-1 V1.1.1 (2016-04) Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers.

[17] ETSI EN 319 162-2 V1.1.1 (2016-04) Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 2: Additional ASiC containers.

[18] ETSI EN 319 401 V2.2.1 (2018-04); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

[19] 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;.

[20] ETSI EN 319 421 V1.1.1 (2016-03); Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.

[21] ETSI EN 319 422 V1.1.1 (2016-03); Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.

[22] ETSI TS 101 733 V1.8.1 (2009-11) Technical Specification Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES).

[23] ETSI TS 101 733 V2.1.1 (2012-03) Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES).

[24] ETSI TS 101 903 V1.2.2 (2004-04) Technical Specification XML Advanced Electronic Signatures (XAdES).

[25] ETSI TS 101 903 V1.3.2 (2006-03) Technical Specification XML Advanced Electronic Signatures (XAdES).

[26] ETSI TS 101 903 V1.4.1 (2009-06) Technical Specification XML Advanced Electronic Signatures (XAdES).

[27] ETSI TS 101 903 V1.4.2 (2010-12) Technical Specification Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES).

[28] ETSI TS 102 778-1 V1.1.1 (2009-07) Technical Specification Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview - a framework document for PAdES.

[29] ETSI TS 102 778-2 V1.2.1 (2009-07) Technical Specification Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic - Profile based on ISO 32000-1.

[30] ETSI TS 102 778-3 V1.1.2 (2009-12) Technical Specification Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles.

[31] ETSI TS 102 778-4 V1.1.2 (2009-12) Technical Specification Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term - PAdES-LTV Profile.

[32] ETSI TS 102 918 V1.3.1 (2013-06) Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC).

[33] ETSI TS 103 171 V2.1.1 (2012-03) Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile.

[34] ETSI TS 119 312 V1.3.1 (2019-02); Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.

[35] ETSI TS 119 511 V1.1.1 (2019-06); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques.

[36] ETSI TS 119 512 V1.1.1 (2020-01); Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services.

[37] CEN 419 221-5; Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services.

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

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

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

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

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

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

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

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

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

[47] IETF RFC 3161: Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP), August 2001.

[48] IETF RFC 6960: X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol (OCSP), June 2013.

[49] ITU X.509 Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.

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

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

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

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

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

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

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

[57] Magyarország (Hungary): Trusted List (http://www.nmhh.hu/tl/pub/HU_TL.pdf).

[58] e-Szignó Hitelesítés Szolgáltató - eIDAS rendelet szerinti minősített archiválási rend.

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

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

[61] e-Szignó Hitelesítés Szolgáltató - Általános Szerződési Feltételek .

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