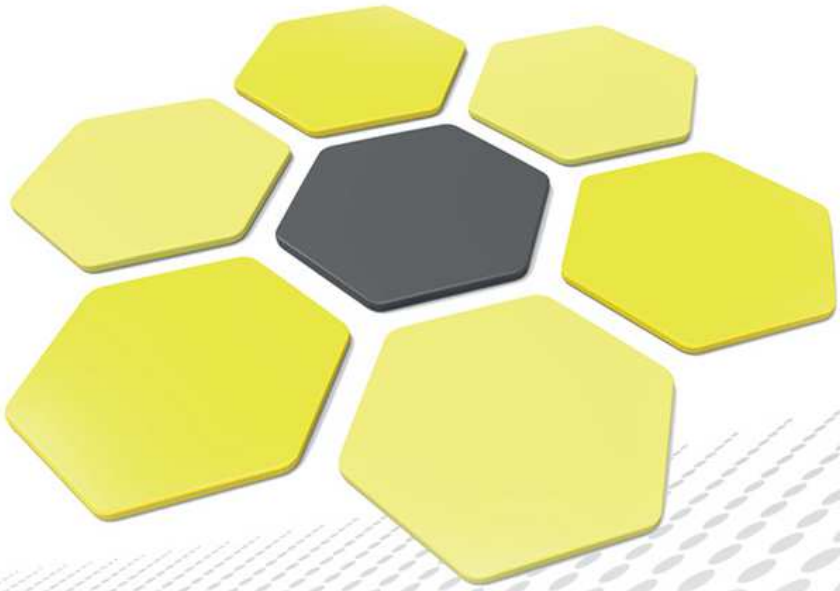
MICROSEC

e-Szignó Hitelesítés Szolgáltató

eIDAS rendelet szerinti minősített archiválási rend

ver. 2.2

Hatálybalépés: 2016-10-30



Azonosító	1.3.6.1.4.1.21528.2.1.1.87.2.2
Verzió	2.2
Első verzió hatálybalépése	2006-12-15
Biztonsági besorolás	NYILVÁNOS
Jóváhagyta	Vanczák Gergely
Jóváhagyás dátuma	2016-09-30
Hatálybalépés dátuma	2016-10-30

Microsec Számítástechnikai Fejlesztő zártkörűen működő Részvénytársaság

1031 Budapest, Záhony utca 7. D. épület

Verzió	A változás leírása	Hatálybalépés	Készítette
1.0	Első változat. OID: 1.3.6.1.4.1.21528.2.1.1.19	2006-12-15	Dr. Berta István Zsolt
1.1	Módosítás a Nemzeti Hírközlési Hatóság észrevételeinek megfelelően. OID: 1.3.6.1.4.1.21528.2.1.1.19.1.1	2007-01-08	Dr. Berta István Zsolt
1.2	A fogyasztóvédelem elérhetőségének változása. OID: 1.3.6.1.4.1.21528.2.1.1.19.1.2	2008-01-01	Dr. Berta István Zsolt
1.3	Nem lépett hatályba. OID: 1.3.6.1.4.1.21528.2.1.1.19.1.3	2008-10-01	Dr. Berta István Zsolt
1.4	Megfelelés az NHH által kibocsátott követelményrendszernek. OID: 1.3.6.1.4.1.21528.2.1.1.19.1.4	2008-12-20	Dr. Berta István Zsolt
2.0	Cégforma változás. Változás az archivált akták titkosításával kapcsolatban. OID: 1.3.6.1.4.1.21528.2.1.1.19.2.0	2012-05-01	Dr. Berta István Zsolt
2.0	eIDAS követelmények szerinti új archiválási rend új OID azonosítóval. OID: 1.3.6.1.4.1.21528.2.1.1.87.2.0	2016-07-01	Dr. Szőke Sándor
2.1	Módosítások az NMHH észrevételei alapján. OID: 1.3.6.1.4.1.21528.2.1.1.87.2.1	2016-09-05	Szomolya Melinda, Dr. Szőke Sándor
2.2	Módosítások a tanúsító észrevételei alapján.	2016-10-30	Dr. Szőke Sándor

Tartalomjegyzék

1. Bevezetés

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

A *Minősített archiválási rend* 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 nyújtásának és az "EU Trust Mark" feltüntetésének előfeltétele, hogy:

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

1.1. Áttekintés

A *Minősített archiválási rend* egy szabálygyűjtemény, amely a minősített elektronikus archiválási szolgáltatás felhasználhatóságát határozza meg egy közös biztonsági követelményekkel rendelkező közösség és/vagy alkalmazások egy osztálya számára.

A *Minősített archiválási rend* alapvető követelményeket fogalmaz meg elsősorban a *Minősített archiválási szolgáltató* számára a létesítendő minősített elektronikus archiválási szolgáltatással kapcsolatban.

A *Minősített archiválási rend* egyike a *Minősített archiválási szolgáltató* által kiadott azon dokumentumoknak, amelyek a *Minősített archiválási szolgáltató* által nyújtott szolgáltatások feltételeit együttesen szabályozzák. További dokumentumok például az Általános szerződési feltételek, a *Minősített archiválási szolgáltatási szabályzat*, a felhasználókkal és a partnerekkel kötött egyéb szerződések.

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 archiválási rend

Azonosító	1.3.6.1.4.1.21528.2.1.1.87
Dokumentum verziószáma	2.2
Hatálybalépés ideje	2016-10-30

1.2.1. Archiválási rend

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

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

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

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

Jelen dokumentum az alábbi *Minősített archiválási rend*(ek)et definiálja:

OID	MEGNEVEZÉS	RÖVID NÉV
1.3.6.1.4.1.21528.2.1.1.87.2.2	eIDAS rendelet szerinti minősített archiválási rend.	MAR

1.2.2. Hatály

Jelen *Minősített archiválási rend* 2016-10-30 -i hatálybalépési dátumtól visszavonásáig hatályos.

Jelen *Minősített archiválási rend*et és az ezen alapuló *Minősített archiválási szolgáltatási szabályzat*okat legalább évente felül kell vizsgálni, és gondoskodni kell az esetlegesen megváltozott követelményekhez illetve igényekhez igazodó módosításukról.

A *Minősített archiválási rend* hatálya kiterjed az 1.3. alfejezetben azonosított közösség minden egyes tagjára.

A jelen *Minősített archiválási rend* a magyar jog alapján Magyarországon, elsősorban magyar *Ügyfel*ek részére, magyar nyelven nyújtott szolgáltatásokra vonatkozó konkrét követelményeket tartalmaznak. A *Minősített archiválási szolgáltató* kiterjesztheti a szolgáltatás területi hatályát, ez esetben a magyar viszonyokra alkalmazható előírásoknak megfelelő, azoknál nem enyhébb követelményeket kell alkalmaznia. Ennek részleteit a *Minősített archiválási szolgáltatási szabályzat*ban kell rögzíteni.

1.3. PKI szereplők

1.3.1. A Szolgáltató

Az archiválási szolgáltató egy olyan *Bizalmi szolgáltató*, amely *Bizalmi szolgáltatás* keretében elektronikus aláírások, elektronikus bélyegzők, *Időbélyegző*k és az ezeket létrehozó *Tanúsítvány*ok érvényességének megőrzésével foglalkozik, opcionálisan beleértve az aláírt illetve bélyegzővel ellátott elektronikus dokumentum megőrzését is.

Jelen dokumentum előírásai vonatkoznak mindazon *Minősített archiválási szolgáltató*kra, akik a *Minősített archiválási szolgáltatási szabályzat*ukban vállalják a jelen dokumentumban szereplő *Minősített archiválási rend*(ek) valamelyikének való megfelelést.

1.3.2. Ügyfelek

Az *Előfizető* határozza meg a szolgáltatást igénybe vevő felhasználók körét és megfizeti az ezen szolgáltatások igénybevételével kapcsolatos szolgáltatási díjakat.

1.3.3. Érintett felek

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

1.4. A dokumentum adminisztrálása

1.4.1. A dokumentum adminisztrációs szervezete

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

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

1.4.2. Kapcsolattartó személy

Jelen *Minősített archiválási rend*del kapcsolatos kérdésekben közvetlenül az alábbi személyhez lehet fordulni:

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

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

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

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

1.4.4. A Szolgáltatási szabályzat elfogadási eljárása

A jelen *Minősített archiválási rend*nek való megfelelőséget kinyilatkoztató *Minősített archiválási szolgáltatási szabályzat* elfogadási eljárását a *Minősített archiválási szolgáltató*nak ismertetnie kell az adott *Minősített archiválási szolgáltatási szabályzat*ban.

1.5. Fogalmak és rövidítések

1.5.1. Fogalmak

Adatközpont	Számítógépes rendszerek és a hozzájuk kapcsolódó komponensek elhelyezésére és üzemeltetésére kialakított létesítmény. Ezek a komponensek rendszerint magukba foglalják a távközlési rendszereket és kommunikációs kapcsolatokat, redundáns áramforrást, adattárolókat, légkondicionáló, tűzvédelmi és biztonsági rendszereket.
Bizalmi felügyelet	"A *Bizalmi szolgáltatás*ok felügyeletét ellátó hatóság a Nemzeti Média- és Hírközlési Hatóság." (2015. évi CCXXII. törvény [4] 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 [4] 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.
Felfüggesztés	A *Tanúsítvány* érvényességének ideiglenes megszüntetése a *Tanúsítvány*ban is feltüntetett érvényességi idő lejárta előtt. A *Tanúsítvány* felfüggesztése nem végleges, a felfüggesztett *Tanúsítvány* érvényessége visszaállítható.
Gyökér tanúsítvány (Root Certificate)	Más néven legfelső szintű tanúsítvány. Önhitelesített *Tanúsítvány*, amelyet adott *Hitelesítő egység* saját maga számára bocsátott ki, azaz saját magánkulcsával van aláírva, így a saját – a tanúsítványban szereplő – nyilvános kulcsával ellenőrizhető.
Hardver kriptográfiai eszköz (HSM: Hardware Security Module)	Egy olyan hardver alapú biztonságos eszköz, mely előállítja, tárolja és védi a kriptográfiai kulcsokat, valamint biztonságos környezetet biztosít a kriptográfiai funkciók végrehajtására.
Hitelesítés-szolgáltató	Olyan *Bizalmi szolgáltató*, aki/amely a hitelesítés-szolgáltatás keretében azonosítja az igénylő személyét, *Tanúsítvány*t bocsát ki, nyilvántartásokat vezet, fogadja a *Tanúsítvány*okkal kapcsolatos változások adatait, valamint nyilvánosságra hozza a *Tanúsítvány*hoz tartozó szabályzatokat, és a *Tanúsítvány* aktuális állapotára (különösen esetleges visszavonására) vonatkozó információkat.
Hitelesítő egység	A *Hitelesítés-szolgáltató* rendszerének egy egysége, amely *Tanúsítvány*ok digitális aláírását végzi. Egy *Hitelesítő egység*hez mindig egy elektronikus aláírás vagy bélyegző létrehozásához használt adat (magánkulcs) tartozik. Előfordulhat, hogy egy *Hitelesítés-szolgáltató* egyszerre több *Hitelesítő egység*et is működtet.
Kompromittálódás	Egy kriptográfiai kulcs akkor kompromittálódott, ha illetéktelen személyek is hozzáférhettek.
Köztes hitelesítő egység	Olyan *Hitelesítő egység* amelynek *Tanúsítvány*át egy másik *Hitelesítő egység* bocsátotta ki.

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

Rendkívüli üzemeltetési helyzet	Olyan, a *Minősített archiválási szolgáltató* üzemmenetében zavart okozó rendkívüli helyzet, amikor a *Minősített archiválási szolgáltató* rendes üzemmenetének folytatására ideiglenesen vagy véglegesen nincsen lehetőség.
Szervezet	Jogi személy.
Szolgáltatási szabályzat (Trust Service Practice Statement)	"A *Bizalmi szolgáltató* nyilatkozata az egyes *Bizalmi szolgáltatás*ok nyújtásával kapcsolatosan alkalmazott részletes eljárási vagy más működési követelményekről. " (2015. évi CCXXII. törvény [4] 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 [4] 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 [4] 1. § 44.)
Tanúsítványtár	Különböző *Tanúsítvány*okat tartalmazó adattár. Tanúsítványtára van egy Szolgáltatónak is, amelyben az általa kibocsátott *Tanúsítvány*okat publikálja, de Tanúsítványtárnak nevezzük az *Érintett fél* számítógépén a használt alkalmazás számára elérhető *Tanúsítvány*okat tartalmazó rendszert is.
Titkosított e-akta	Ez az e-akta egy olyan XML fájl, amely egy másik (nyílt vagy titkosított) e-aktát (is) tartalmaz – az S/MIME specifikáció szerint titkosítva.
Ügyfél	Az *Előfizető* és a szolgáltatás igénybe vevői, akik részére az Előfizető használati jogosultságot ad.

Visszavonás	A *Tanúsítvány* érvényességének megszüntetése a *Tanúsítvány*ban is feltüntetett érvényességi idő lejárta előtt. A *Tanúsítvány* visszavonása végleges, visszavont *Tanúsítvány* többet nem tehető érvényessé.
Visszavonási állapot nyilvántartás	A *Hitelesítés-szolgáltató* által vezetett nyilvántartás a felfüggesztett, illetőleg a visszavont *Tanúsítvány*okról, amelyek tartalmazzák legalább a felfüggesztés vagy visszavonás tényét, és a felfüggesztés vagy visszavonás időpontját.

1.5.2. Rövidítések

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

2. Közzététel és tanúsítványtár

2.1. Adatbázisok - tanúsítványtárak

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

2.2. Az információ közzététele

2.2.1. Szolgáltatói információ közzététele

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

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

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

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

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

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

2.3. A közzététel időpontja vagy gyakorisága

2.3.1. Kikötések és feltételek közzétételi gyakorisága

A *Minősített archiválási rend*del kapcsolatos új verziók közzététele a 8.12. fejezetben ismertetett eljárásoknak megfelelően történik.

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

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

3. Elektronikus archiválási szolgáltatás

Az elektronikus archiválási szolgáltatás keretében az alábbi feladatokat kell ellátni:

- 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 3.2. 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 4. 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: 3.3).
- 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: 3.4. fejezet).
- Az *Előfizető* kérésére a *Minősített archiválási szolgáltató* törli az e-dokumentumokat az archívumából (lásd: 3.6. fejezet).

Az elektronikus archiválás szolgáltatás elsődleges feladata az e-dokumentumon elhelyezett elektronikus aláírás vagy bélyegző érvényességének hosszú távú megőrzése.

A *Minősített archiválási szolgáltató* az alapfeladat ellátása mellett további szolgáltatásokat is nyújthat az *Előfizető* részére, például:

- az elektronikus aláírással vagy bélyegzővel ellátott elektronikus dokumentum megőrzése,
- az archívumba feltöltött e-dokumentumok illetve az azokban foglalt elektronikus dokumentumok olvashatóságának, humán értelmezhetőségének biztosítása,
- az esetleg szükségessé váló fájlformátum konverziók elvégzése.

A jelen *Minősített archiválási rend* elektronikus aláírások és bélyegzők hosszú távú érvényességének biztosításával kapcsolatos követelményeket fogalmaz meg, így nem teszi lehetővé elektronikus aláírás illetve bélyegző nélküli e-dokumentumok befogadását és megőrzését.

A *Minősített archiválási szolgáltató* a *Minősített archiválási szolgáltatási szabályzat*ban meghatározhatja illetve korlátozhatja a befogadható elektronikus aláírások illetve bélyegzők formátumát, az elfogadott Hitelesítés-szolgáltatókat vagy bármilyen egyéb paramétert.

3.1. Szolgáltatási szerződés kötése

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

A *Minősített archiválási szolgáltatási szabályzat*nak illetve az abban hivatkozott egyéb szabályzatoknak egyértelműen meg kell határozniuk a nyújtandó szolgáltatás részleteit, az igénybevételhez szükséges eszközöket.

3.2. Dokumentum feltöltése

1. A *Minősített archiválási szolgáltató* kizárólag az *Előfizető* azonosságának megállapítása után, biztonságos eljárás keretében fogadhat be archiválandó e-dokumentumokat. Az eljárásnak biztosítania kell az e-dokumentumok integritásának, bizalmasságának megőrzését.
2. A *Minősített archiválási szolgáltatási szabályzat*ban egyértelműen meg kell határozni, hogy a *Minősített archiválási szolgáltató* milyen aláírás és fájlformátumokat fogad el, az elektronikus aláírásokat és bélyegzőket milyen módon ellenőrzi, és az e-dokumentumokat milyen feltételekkel fogadja be.

3. Az átvett e-dokumentumon található elektronikus aláírás(ok) vagy bélyegző(k) érvényességét a teljes érvényességi láncon ellenőrizni kell. Az ellenőrzés alapulhat az elektronikus aláírás(ok)hoz vagy bélyegző(k)höz csatolt részleges vagy teljes érvényességi láncon is. A teljes ellenőrzéshez esetlegesen még szükséges információt a *Minősített archiválási szolgáltató*nak be kell gyűjtenie és az e-dokumentumhoz kapcsolódóan el kell tárolnia. Az érvényességi láncok felépítése után a *Minősített archiválási szolgáltató* helyezzen el minden megőrzendő érvényességi láncon egy minősített archív *Időbélyegző*t.

4. A *Minősített archiválási szolgáltató* a befogadott az e-dokumentumot titkosított formában kell tárolja. A titkosításnak biztosítania kell, hogy az e-dokumentumok tartalmát arra jogosulatlan személyek nem ismerhetik meg. A titkosított e-dokumentum visszafejtésére kizárólag az elektronikus archiválás szolgáltatás nyújtásához szükséges esetekben, például letöltés (3.3. fejezet), felülhitelesítés (4.4. fejezet), illetve újra-titkosítás (4.5) esetén kerülhet sor.

5. A *Minősített archiválási szolgáltató* minél előbb, de legkésőbb a benyújtástól számított 3 napon belül vizsgálja meg az átvett e-dokumentumokat és küldjön visszaigazolást az *Előfizető*nek arról, hogy az érvényességi láncot sikeresen felépítette, és az e-dokumentumot befogadta. Ha a folyamat valahol megszakadt, a *Minősített archiválási szolgáltató* erről is értesítse az *Előfizető*t egy hibaüzenetben. A hibaüzenet alapján legyen egyértelműen megállapítható, hogy melyik e-dokumentumról van szó, és hogy mi volt az elutasítás oka.

   Ha az *Előfizető*höz a megadott határidőn belül nem érkezik meg az e-dokumentum befogadásáról szóló igazolás, akkor 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, bélyegzők hitelességének hosszú távú biztosításáért.

3.3. Érvényességi lánc elérhetőségének biztosítása - e-dokumentum letöltése

A *Minősített archiválási szolgáltató* biztosítsa, hogy az *Előfizető* a szolgáltatási szerződés érvényessége alatt letölthesse az archívumban tárolt e-dokumentumait és az azokhoz tartozó érvényességi láncokat.

1. Az *Előfizető* kizárólag biztonságos csatornán keresztül férhet hozzá a *Minősített archiválási szolgáltató* archívumában tárolt e-dokumentumokhoz és érvényességi láncokhoz.

2. A *Minősített archiválási szolgáltató*nak biztosítania kell, hogy minden *Előfizető* kizárólag azon e-dokumentumokhoz és érvényességi láncokhoz férhet hozzá, amelyekhez valóban jogosult hozzáférni.

3.4. 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 az *Előfizető* által bemutatott azonos lenyomatú e-dokumentummal.
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 fokozott biztonságú elektronikus aláírásával vagy bélyegzőjével hitelesített elektronikus igénylés benyújtásával kérheti az igazolás kiadását.

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

3.5. Dokumentum megjelenítése

A *Minősített archiválási szolgáltató* tegye lehetővé az *Előfizető* részére, hogy előre egyeztetett időpontban és helyszínen a *Minősített archiválási szolgáltató* szoftver és hardver eszközei segítségével megtekinthesse a *Minősített archiválási szolgáltató* archívumában lévő e-dokumentumait.

3.6. Dokumentum és érvényességi lánc törlése

A *Minősített archiválási szolgáltató* az *Előfizető* kérésére tegye lehetővé az archívumban tárolt e-dokumentumok és a hozzá tartozó valamennyi érvényességi lánc szelektív törlését. A 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 hajtsa végre, a törlés keretében az e-dokumentum minden mentett példányát semmisítse meg.

A *Minősített archiválási szolgáltató* a *Minősített archiválási szolgáltatási szabályzat*ban határozza meg a törlési kérelem benyújtásának és feldolgozásának módját és feltételeit.

3.7. A szolgáltatási szerződés megszűnése

A szolgáltatási szerződés megszűnése esetén a *Minősített archiválási szolgáltató* tegye lehetővé az *Előfizető* vagy az arra jogosult más személy részére az *Előfizető* megbízásából ott tárolt e-dokumentumok és érvényességi láncok letöltését.

A Szolgáltatási szerződés megszűnése után a *Minősített archiválási szolgáltató* törölje az archívumból az *Előfizető*höz tartozó e-dokumentumokat és érvényességi láncokat.

4. Műszaki biztonsági óvintézkedések

4.1. Biztonsági garanciák

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

Amennyiben a *Minősített archiválási szolgáltató* harmadik féltől bizalmi szolgáltatást vesz igénybe, ellenőriznie kell, hogy ezen harmadik fél eleget tesz-e minden szükséges kötelezettségének. A *Minősített archiválási szolgáltató* az archivált e-dokumentumokat fizikailag biztonságos környezetben, a 5. fejezetben leírt fizikai és eljárásbeli óvintézkedések mellett tárolja, amelynek biztonságát a *Minősített archiválási szolgáltató* belső biztonsági szabályzatai és a rendszeres belső és külső biztonsági felülvizsgálat garantálják. A *Minősített archiválási szolgáltató* biztosítja, hogy a tárolt e-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 3.6 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.

4.2. Számítógépes biztonsági óvintézkedések

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

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

4.3. Életciklusra vonatkozó műszaki óvintézkedések

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

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

4.4. Rendszeres felülhitelesítés

A *Minősített archiválási szolgáltató* az érvényességi láncokon 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.

4.5. Az archívum újra-titkosítása

Az archivált e-dokumentumokat titkosítva kell tárolni az archívumban. Biztosítani kell, hogy az archivált e-dokumentumok mindenkor biztonságos algoritmussal kerüljenek titkosításra.

Az e-dokumentumokat újra kell titkosítani, ha:

- a titkosításkor használt valamely algoritmusban megrendül a bizalom – ilyenkor a titkosítás időpontjában biztonságosnak ítélt algoritmussal kell újra titkosítani;
- a *Minősített archiválási szolgáltató* dekódoló kulcsának bizalmassága sérül;
- a *Minősített archiválási szolgáltatási szabályzat* vagy az *Előfizető*vel kötött szerződés így rendelkezik.

Az archivált e-dokumentumok újra titkosítása után a korábbi, már nem kellően biztonságosnak ítélt módon titkosított példányokat meg kell semmisíteni.

4.6. A technológia folyamatos figyelése

A *Minősített archiválási szolgáltató*nak folyamatosan figyelemmel kell kísérnie 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 értesítenie kell a Nemzeti Média- és Hírközlési Hatóságot és megkérni a kriptográfiai algoritmusokkal kapcsolatos határozat felülvizsgálatára.

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

4.7. Hitelesítés és időbélyegzés szolgáltatók elfogadása

A *Minősített archiválási szolgáltató* meghatározhatja, hogy az archiválás szolgáltatás keretében mely hitelesítés-szolgáltatók *Tanúsítvány*ait milyen feltételekkel fogadja el, valamint azt, hogy hitelesítés-szolgáltatók milyen feltételrendszer szerint kerülhetnek fel ezen listára, és le ezen listáról.

4.8. Az elektronikus dokumentumok olvashatóságának és értelmezhetőségének fenntartása

A *Minősített archiválási szolgáltató*nak egyértelműen meg kell határoznia a *Minősített archiválási szolgáltatási szabályzat*ban vagy a *Minősített archiválási szolgáltatási szabályzat*ban meghivatkozott más dokumentumban, hogy az archiválás szolgáltatás keretében mely formátumú fájlok, elektronikus dokumentumok olvashatóságát biztosítja

4.9. Az elektronikus archiválás szolgáltatás egyes elemeinek rendelkezésre állása

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

- az archivált e-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.

5. Elhelyezési, eljárásbeli és üzemeltetési előírások

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

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

A *Minősített archiválási szolgáltató*nak figyelemmel kell kísérnie a kapacitás igényeket és biztosítania kell, hogy megfelelő feldolgozási teljesítmény és tárolási kapacitás álljon rendelkezésre a szolgáltatás nyújtásához.

5.1. Fizikai követelmények

A *Minősített archiválási szolgáltató*nak gondoskodnia kell 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 kell megvalósítani.

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

5.1.1. A telephely elhelyezése és szerkezeti felépítése

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

5.1.2. Fizikai hozzáférés

A *Minősített archiválási szolgáltató*nak védenie kell a szolgáltatás nyújtásában részt vevő eszközeit és berendezéseit a jogosulatlan fizikai hozzáféréstől az eszközök manipulálásának megakadályozása érdekében. A *Minősített archiválási szolgáltató*nak biztosítania kell, 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 kell tartani;
- a bejelentkezett terminálokat nem szabad felügyelet nélkül hagyni;
- nem szabad olyan munkafolyamatot végezni, 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 fizikai biztonsági vizsgálatok rendszeres elvégzésére felelősöket kell kijelölni. A vizsgálatok eredményét megfelelő naplóbejegyzésekben kell rögzíteni.

5.1.3. Áramellátás és légkondicionálás

A *Minősített archiválási szolgáltató Adatközpont*jában olyan szünetmentes áramellátó rendszert kell alkalmazni, 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 szűrőrendszerrel kell biztosítani, amely kiszűri a levegőből a különféle szennyeződéseket (por, szennyező anyagok, korrozív anyagok, mérgező vagy gyúlékony anyagok). A szellőző rendszernek megfelelő szűrés mellett biztosítania kell az operátorok biztonságos munkavégzéséhez szükséges mennyiségű friss levegőt.

A levegő nedvességtartalmát az informatikai rendszerek által megkívánt szintre kell csökkenteni.

Megfelelő teljesítményű hűtőrendszert kell használni a szükséges üzemi hőmérséklet biztosítása, az informatikai eszközök túlhevülésének megakadályozása érdekében.

5.1.4. Beázás és elárasztódás veszély kezelése

A *Minősített archiválási szolgáltató Adatközpont*ját megfelelően védeni kell a vízbetöréstől és az elárasztódástól.

5.1.5. Tűz megelőzés és tűzvédelem

A *Minősített archiválási szolgáltató Adatközpont*ját füst- és tűzérzékelőkkel kell felszerelni, amelyek automatikusan riasztják a tűzoltóságot. Minden helyiségben jól látható helyen el kell helyezni a vonatkozó előírásoknak megfelelő típusú és mennyiségű kézi tűzoltó készüléket.

A gépteremben automatikus tűzoltó rendszert kell alkalmazni.

5.1.6. Adathordozók tárolása

A *Minősített archiválási szolgáltató*nak védenie kell valamennyi adathordozóját a jogosulatlan hozzáféréstől és a véletlen rongálódástól. Valamennyi napló és archív adatot duplikáltan kell létrehozni. A két példányt egymástól fizikailag elkülönítve kell tárolni, egymástól biztonságos távolságra lévő helyszíneken. A tárolt adathordozókat védeni kell a káros környezeti behatásoktól, mint pl. alacsony vagy magas hőmérséklet, szennyeződés, nedvesség, napfény, erős mágneses tér, erős sugárzás.

5.1.7. Hulladék megsemmisítése

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

Az ilyen eszközöket, adathordozókat a *Minősített archiválási szolgáltató* alkalmazottainak személyes felügyelete alatt, a széleskörűen elfogadott módszereknek megfelelően kell véglegesen törölni vagy használhatatlanná tenni.

5.1.8. A mentési példányok fizikai elkülönítése

A *Minősített archiválási szolgáltató*nak legalább heti rendszerességgel elő kell állítania olyan mentést, amiből meghibásodás esetén a teljes szolgáltatás helyreállítható. A mentéseket - legalább

az utolsó teljes mentést is beleértve - egy olyan külső helyszínen kell tárolni, amelynek a fizikai és működési védelme azonos az elsődleges helyszínével. Az elsődleges és a tartalék helyszínek között meg kell oldani az adatok biztonságos továbbítását.

5.2. Eljárásbeli előírások

A *Minősített archiválási szolgáltató*nak gondoskodnia kell 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 biztosítsa a jogszabályoknak és belső szabályzatainak megfelelő működést. Rendszerében minden rendszerelemhez és minden folyamathoz legyen egyértelműen hozzárendelhető az adott rendszerelemért, vagy folyamatért felelős személy. A *Minősített archiválási szolgáltató* rendszerében élesen különüljenek el egymástól a fejlesztési és üzemeltetési folyamatok. A rendszer megfelelő működését a független rendszervizsgáló és a *Minősített archiválási szolgáltató* belső folyamatainak rendszeres ellenőrzése biztosítsa.

5.2.1. Bizalmi szerepkörök

A *Minősített archiválási szolgáltató*nak feladatai ellátásához bizalmi szerepköröket kell létrehoznia. A jogosultságokat és funkciókat oly módon kell megosztani az egyes bizalmi szerepkörök között, hogy egyedül egyetlen felhasználó se legyen képes a biztonsági védelmi intézkedések megkerülésére.

A megvalósítandó bizalmi szerepkörök:

- a szolgáltató informatikai rendszeréért általánosan felelős vezető;
- biztonsági tisztviselő: a szolgáltatás biztonságáért általánosan felelős személy;
- rendszeradminisztrátor: az informatikai rendszer telepítését, konfigurálását, karbantartását végző személy;
- rendszerüzemeltető: az informatikai rendszer folyamatos üzemeltetését, mentését és helyreállítását végző személy;
- független rendszervizsgáló: a szolgáltató naplózott, illetve archivált adatállományát vizsgáló, a 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 vezetőjének formálisan ki kell nevezni 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 naprakész nyilvántartást kell vezetni, amit változás esetén haladéktalanul be kell jelenteni a Nemzeti Média- és Hírközlési Hatóságnak.

5.2.2. Az egyes feladatok ellátásához szükséges személyzeti létszámok

A *Minősített archiválási szolgáltató* biztonsági és üzemeltetési szabályzataiban elő kell írni, 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.

5.2.3. Az egyes szerepkörökben elvárt azonosítás és hitelesítés

A *Minősített archiválási szolgáltató* informatikai rendszerét kezelő felhasználóknak egyedi azonosító adatokkal kell rendelkezniük, 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 adatokat a felhasználói jogosultságok megszűnésekor haladéktalanul vissza kell vonni.

5.2.4. Egymást kizáró szerepkörök

A *Minősített archiválási szolgáltató* munkatársai egyidejűleg több bizalmi szerepkört is betölthetnek, de a *Minősített archiválási szolgáltató* köteles biztosítani, 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.

5.3. Személyzetre vonatkozó előírások

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

5.3.1. Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

A *Minősített archiválási szolgáltató* valamennyi dolgozójának rendelkeznie kell a munkaköre ellátásához szükséges végzettséggel, gyakorlattal és szakmai tapasztalattal. Már a munkaerő felvétel során a leendő dolgozók kiválasztásánál különös hangsúlyt kell fektetni a személyiségi jegyekre, csak megbízható személyek vehetők fel a bizalmi szerepkörbe.

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

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

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

5.3.2. Előélet vizsgálatára vonatkozó eljárások

A *Minősített archiválási szolgáltató* vezető munkakörben illetve bizalmi szerepkörben csak olyan alkalmazottakat foglalkoztathat, 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*nak a felvételi eljárás során ellenőriznie kell a jelentkező önéletrajzában megadott releváns információk valódiságát.

5.3.3. Képzési követelmények

A *Minősített archiválási szolgáltató* az újonnan felvett alkalmazottakat ki kell képezze, 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 kaphatnak hozzáférési jogosultságot.

5.3.4. Továbbképzési gyakoriságok és követelmények

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

Továbbképzést kell tartani, ha a *Minősített archiválási szolgáltató* folyamataiban vagy informatikai rendszerében változás áll be.

A továbbképzést megfelelően dokumentálni kell, amelyből egyértelműen megállapítható a továbbképzés tematikája és a résztvevő dolgozók köre.

5.3.5. Munkabeosztás körforgásának sorrendje és gyakorisága

Nincs előírás.

5.3.6. Felhatalmazás nélküli tevékenységek büntető következményei

A *Minősített archiválási szolgáltató*nak a dolgozókkal kötendő munkaszerződésben kell szabályoznia 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.

5.3.7. Szerződéses viszonyban foglalkoztatottakra vonatkozó követelmények

A *Minősített archiválási szolgáltató* által szerződéses viszonyban foglalkoztatott dolgozókra ugyanolyan szabályokat kell alkalmazni, mint a munkavállalókra.

A bizalmi szerepkört betöltő személynek munkaviszonyban kell állnia a *Minősített archiválási szolgáltató*val.

5.3.8. A személyzet számára biztosított dokumentációk

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

5.4. Naplózási eljárások

A *Minősített archiválási szolgáltató*nak a biztonságos informatikai környezet fenntartása érdekében a teljes informatikai rendszerét átfogó eseménynaplózó és ellenőrző rendszert kell megvalósítania és üzemeltetnie.

5.4.1. A tárolt események típusai

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

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

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

Naplózni kell minimálisan az alábbi eseményeket:

- ARCHIVÁLÁS

  - az e-akták feltöltésével és a bennük lévő aláírások ellenőrzésével kapcsolatos információk;
  - az adatok rendelkezésre állásának, sértetlenségének megőrzésével, hitelességének és letagadhatatlanságának megőrzésével, értelmezhetőségének fenntartásával és törlésével kapcsolatos információk;
  - az e-akták letöltésével, az igazolás-kérések teljesítésével, és az archívum más szolgáltatónak történő esetleges átadásával kapcsolatos információk;

- NAPLÓZÁS
  - a naplózó rendszer vagy egyes komponenseinek leállítása, újraindítása;
  - a naplózás bármilyen beállításának módosítása, mint pl. gyakoriság, riasztási küszöb érték, vizsgált esemény;
  - a tárolt naplózási adatok módosítása vagy törlése;
  - a naplózó rendszer hibája miatt végzett tevékenységek;
- RENDSZER BEJELENTKEZÉSEK
  - sikeres bejelentkezések, sikertelen bejelentkezési próbálkozások bizalmi szerepkörökbe;
  - jelszó alapú azonosítás esetén:
    * az engedélyezett sikertelen bejelentkezési próbálkozások számának megváltoztatása;
    * az engedélyezett sikertelen bejelentkezési próbálkozások számának elérése felhasználói bejelentkezéskor;
    * sikertelen bejelentkezések miatt zárolt felhasználó újbóli engedélyezése;
  - az azonosítási technika változtatása (például jelszó alapúról PKI alapúra);
- KULCSKEZELÉS
  - a szolgáltatói kulcsok teljes életciklusára vonatkozó valamennyi esemény (kulcsgenerálás, betöltés, elmentés stb.);
- TANÚSÍTVÁNY KEZELÉS
  - szolgáltatói *Tanúsítvány*ok kibocsátásával, állapotváltozásával kapcsolatos minden esemény;
- ADATMOZGÁSOK
  - bármilyen, a biztonság szempontjából kritikus adat manuális bevitele a rendszerbe;
  - a rendszer által fogadott, biztonsági szempontból fontos adatok, üzenetek;
- CA KONFIGURÁCIÓ
  - a CA tetszőleges komponensének átparaméterezése, a beállításon történt bármilyen változtatás;
  - felhasználók felvétele, törlése;

  - felhasználói szerepkörök, jogosultságok megváltoztatása;
  - a tanúsítvány profil megváltoztatása;
  - CRL profil megváltoztatása;
  - új CRL lista előállítása;
  - OCSP válasz generálása;
  - *Időbélyegző* generálása;
  - az előírt időpontossági küszöb túllépése;
- HSM
  - HSM installálása;
  - HSM eltávolítása;
  - HSM selejtezése, megsemmisítése;
  - HSM szállítása;
  - HSM tartalmának törlése (nullázás);
  - HSM feltöltése kulcsokkal, tanúsítványokkal;
- KONFIGURÁCIÓ VÁLTOZÁSA
  - hardver;
  - szoftver;
  - operációs rendszer;
  - javító csomag;
- FIZIKAI HOZZÁFÉRÉS, TELEPHELY BIZTONSÁG
  - személy belépése a CA komponenseket tartalmazó biztonsági területre és onnan kilépése;
  - hozzáférés egy CA rendszer komponenshez;
  - a fizikai biztonság ismert vagy gyanított megsértése;
  - tűzfal és router forgalmak;
- MŰKÖDÉSI RENDELLENESSÉGEK
  - rendszerösszeomlás, hardver hiba;
  - szoftveres hibák;
  - szoftverintegritás ellenőrzési hiba;
  - hibás vagy rossz helyre továbbított üzenetek;
  - hálózatot ért támadások, támadási kísérletek;
  - berendezés hiba;
  - elektromos hálózati üzemzavar;
  - szünetmentes tápegység hiba;
  - lényeges hálózati szolgáltatás hozzáférési hiba;

  - a *Minősített archiválási rend* vagy a *Minősített archiválási szolgáltatási szabályzat* megsértése;
  - operációs rendszer órájának törlése;

- EGYÉB ESEMÉNYEK
  - személy kinevezése biztonsági szerepkörbe;
  - operációs rendszer telepítése;
  - PKI alkalmazás telepítése;
  - rendszer elindítása;
  - belépési kísérlet a PKI alkalmazásba;
  - jelszó módosítási, beállítási kísérlet;
  - a belső adatbázis elmentése, visszaállítása mentésből;
  - fájl műveletek (pl. létrehozás, átnevezés, áthelyezés);
  - adatbázis hozzáférés.

5.4.2. A naplófájl feldolgozásának gyakorisága

A *Minősített archiválási szolgáltató*nak biztosítania kell a keletkezett naplóállományok rendszeres kiértékelését.

A keletkezett napi naplóállományokat lehetőség szerint a következő munkanapon, de legkésőbb 1 héten belül ki kell értékelni.

A naplóállományok kiértékelését csak a megfelelő szakértelemmel, jogosultságokkal és kinevezéssel rendelkező független rendszervizsgáló végezheti el.

A *Minősített archiválási szolgáltató* használhat automatizált eszközöket az elektronikus naplóállományok kiértékelésének segítésére.

A kiértékelés során meg kell győződni a vizsgált naplóállományok hitelességéről és sértetlenségéről.

A kiértékelés során elemezni kell a rendszerek által generált hibaüzeneteket.

Statisztikai módszerekkel elemezni kell a forgalmi adatokban bekövetkezett jelentős változásokat.

A vizsgálat tényét, a vizsgálat eredményeit és az esetleges feltárt hiányosságok elhárítása érdekében meghozott intézkedéseket megfelelően dokumentálni kell.

5.4.3. A naplófájl megőrzési időtartama

Az online rendszerből való kitörlés előtt a naplóállományokat archiválni kell és gondoskodni kell azok biztonságos megőrzéséről az 5.5.2 fejezetben meghatározott ideig.

5.4.4. A naplófájl védelme

A *Minősített archiválási szolgáltató*nak meg kell védenie a keletkezett naplóállományokat az előírt megőrzési ideig. A megőrzési idő teljes időtartama alatt biztosítania kell a naplóadatok:

- védelmét az illetéktelen felfedés ellen: a naplóállományokhoz csak az arra jogosultak – elsősorban a független rendszervizsgálók – férhessenek hozzá;

- rendelkezésre állását: a jogosultak számára biztosítani kell a naplóállományokhoz való hozzáférést;
- integritását: meg kell akadályozni a naplóállományokban bármilyen adat módosítását, törlését, bejegyzések sorrendjének megváltoztatását stb.

5.4.5. A naplófájl mentési eljárásai

Az üzemeltetés során az egyes rendszerekben folyamatosan keletkező naplóbejegyzésekből napi naplóállományokat kell előállítani.

A napi naplóállományokat a kiértékelés után 2 példányban archiválni kell és a példányokat egymástól fizikailag elkülönülő helyszíneken az előírt ideig meg kell őrizni.

A mentések pontos menetét a *Minősített archiválási szolgáltatási szabályzat*ban elő kell írni.

5.4.6. A naplózás adatgyűjtési rendszere

A *Minősített archiválási szolgáltató* a *Minősített archiválási szolgáltatási szabályzat*ában írja elő a naplózási folyamatainak működését.

A *Minősített archiválási szolgáltató* használhat automatikus vizsgáló és naplózó rendszereket is, amennyiben biztosítani tudja, hogy azok a rendszer indításakor már aktívak és a rendszer leállásáig folyamatosan működnek.

Amennyiben az automatikus vizsgáló és naplózó rendszerek működésében bármilyen rendellenesség lép fel, a *Minősített archiválási szolgáltató* működését fel kell függeszteni az üzemzavar elhárításáig.

5.4.7. Az eseményeket kiváltó alanyok értesítése

A feltárt hiba esetén a *Minősített archiválási szolgáltató* saját hatáskörében dönthet, hogy értesíti-e a hibáról az azt kiváltó személyt, szerepkört, eszközt vagy alkalmazást.

5.4.8. Sebezhetőség felmérése

A *Minősített archiválási szolgáltató*nak évente sebezhetőség vizsgálatot kell végeznie, amely segítségével feltérképezi a potenciális belső és külső fenyegetettségeket, amelyek jogosulatlan hozzáféréseket eredményezhetnek.

Fel kell térképezni továbbá az egyes fenyegetettségek bekövetkezésének valószínűségét és a bekövetkezés esetén várható kárt is.

Rendszeresen értékelnie kell az alkalmazott folyamatokat, védelmi intézkedéseket, informatikai rendszereket, hogy azok megfelelően képesek-e ellenállni a feltárt fenyegetettségeknek.

A feltárt hibák kiértékelése után szükség szerint módosítani kell a védelmi rendszereken, hogy a hasonló hibák a jövőben megakadályozhatók legyenek.

5.5. Adatok archiválása

5.5.1. Az archivált adatok típusai

A *Minősített archiválási szolgáltató*nak fel kell készülnie elektronikus és papíralapú dokumentumok megfelelően biztonságos, hosszú idejű archiválására.
A *Minősített archiválási szolgáltató*nak az alábbi jellegű információt kell archiválnia:

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

5.5.2. Az archívum megőrzési időtartama

A *Minősített archiválási szolgáltató* az archivált adatokat az alábbi időtartamokig köteles megőrizni:

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

5.5.3. Az archívum védelme

A *Minősített archiválási szolgáltató* köteles valamennyi archivált adatot két példányban, két egymástól fizikailag elkülönült helyszínen őrizni. Az egyetlen hiteles példányban rendelkezésre álló papíralapú dokumentumról hiteles papíralapú, vagy elektronikus másolat készíthető a vonatkozó jogszabályok betartásával.
A két helyszín mindegyikének teljesítenie kell az archiválással szemben támasztott biztonsági és egyéb követelményeket.
Az archivált adatok megőrzése során gondoskodni kell 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 kell ellátni.

5.5.4. Az archívum mentési folyamatai

Az archivált adatok másodpéldányát a *Minősített archiválási szolgáltató* telephelyétől fizikailag eltérő helyszínen kell tárolni az 5.1.8 fejezet előírásainak megfelelően.

5.5.5. Az adatok időbélyegzésére vonatkozó követelmények

Valamennyi elektronikus naplóbejegyzést el kell látni időjellel, amelyen legalább másodperc pontossággal fel van tüntetve a rendszer által szolgáltatott időpont.

A *Minősített archiválási szolgáltató*nak biztosítania kell, hogy a szolgáltatást nyújtó rendszerein a gépidő maximum 1 másodpercre térjen el a referenciaidőtől. Az időjel előállításához használt gépidőt naponta legalább egy alkalommal szinkronizálni kell az UTC időhöz.

A napi naplóállományokat minősített *Időbélyegző*vel kell ellátni.

Az archivált adatok megőrzése során szükség esetén (pl. algoritmusváltás, az eredeti *Időbélyegző* érvényességének lejárata) gondoskodni kell az adatok hitelességének megőrzéséről.

5.5.6. Az archívum gyűjtési rendszere

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

5.5.7. Archív információk hozzáférését és ellenőrzését végző eljárások

A *Minősített archiválási szolgáltató* a naplóállományok előállítását manuálisan vagy automatikusan is elvégezheti. Automatikus naplózó rendszer alkalmazása esetén a hitelesített naplóállományokat naponta kell előállítani.

Az archivált adatállományokat védeni kell a jogosulatlan hozzáféréstől.

Az arra jogosultaknak biztosítani kell az archivált adatokhoz való ellenőrzött hozzáférést:

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

5.6. Kompromittálódást és katasztrófát követő helyreállítás

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

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

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

5.6.1. Váratlan esemény és kompromittálódás kezelési eljárások

A *Minősített archiválási szolgáltató*nak rendelkeznie kell üzletmenet folytonossági tervvel.

A *Minősített archiválási szolgáltató*nak ki kell alakítania és fenn kell tartania 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*nak rendszeresen tesztelnie kell a tartalékrendszer működését és évente felül kell vizsgálnia az üzletmenet folytonossági terveit.

Katasztrófa esetén a lehető legrövidebb időn belül helyre kell állítani a szolgáltatások elérhetőségét.

5.6.2. Meghibásodott IT erőforrások, szoftverek és/vagy adatok

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

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

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

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

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

5.6.3. Működés folyamatosságának biztosítása katasztrófát követően

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

A katasztrófa bekövetkezése esetén haladéktalanul életbe kell léptetni a rendelkezéseket és meg kell kezdeni a károk elhárítását, a szolgáltatások helyreállítását.

A másodlagos szolgáltatási helyszínt az elsődleges telephelytől olyan távol kell elhelyezni, 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 állítsa helyre a katasztrófa során tönkrement eszközeit és az eredeti szolgáltatás biztonsági szintet.

5.7. Az Archiválási szolgáltatás leállítása

A *Minősített archiválási szolgáltató*nak a szolgáltatás megszüntetésekor teljesítenie kell a jogszabályokban megfogalmazott követelményeket.

A leállítás során kiemelten kezelendő feladatok:

- a tervezett leállásról időben értesíteni kell az *Érintett felek*et és az *Előfizető*ket;
- a *Minősített archiválási szolgáltató* tegyen meg mindent annak érdekében, hogy legkésőbb a szolgáltatás leállításáig egy másik szolgáltató átvegye nyilvántartásait és szolgáltatási kötelezettségeit;
- vissza kell vonni a szolgáltatói *Tanúsítvány*okat és meg kell semmisíteni a szolgáltatói magánkulcsokat;
- a szolgáltatás megszüntetése után egy teljes rendszermentést és archiválást kell végeznie;
- át kell adni az archivált adatokat a szolgáltatást átvállaló szolgáltatónak vagy a Nemzeti Média- és Hírközlési Hatóságnak.

6. Műszaki biztonsági óvintézkedések

A *Minősített archiválási szolgáltató*nak módosítás ellen védett, megbízható rendszereket és termékeket kell használnia a kriptográfiai kulcsok és aktivizáló adataik kezelésére a teljes életciklus alatt.

Folyamatosan nyomon kell követni a kapacitás igényeket és becsülni kell a jövőbeni várható kapacitást, hogy biztosítani lehessen a szükséges feldolgozási és tárolási igények rendelkezésre állását.

6.1. A magánkulcsok védelme

A *Minősített archiválási szolgáltató*nak gondoskodnia kell a birtokában lévő magánkulcsok biztonságos kezeléséről, meg kell akadályoznia a magánkulcsok felfedését, lemásolását, törlését, módosítását, jogosulatlan használatát. A *Minősített archiválási szolgáltató* csak addig őrizheti a magánkulcsokat, ameddig azt a szolgáltatás nyújtása feltétlenül megköveteli.

A *Hardver kriptográfiai eszköz*ök kezelése során a használatból kivont *Hardver kriptográfiai eszköz*ökben tárolt aláíró magánkulcsokat olyan módon kell törölni, hogy ne legyen lehetséges a kulcsok visszaállítása.

6.1.1. Kriptográfiai modulra vonatkozó szabványok és előírások

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

- megfelelnek az ISO/IEC 19790 [11] követelményeinek,
- vagy megfelelnek a FIPS 140-2 [12] 3-as, illetve annál magasabb szintű követelményeknek,
- vagy megfelelnek a CEN 14167-2 [13] munkacsoport egyezmény követelményeinek,

- vagy olyan megbízható rendszerek, amely az MSZ/ISO/IEC 15408 [10] 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 szolgáltatói magánkulcsok a *Hardver kriptográfiai eszköz*ön kívül csak kódolt formában tárolhatók. A kódoláshoz csak az Eüt. [4] 92. § (1) b) pontja szerinti aktuális Nemzeti Média- és Hírközlési Hatóság által kiadott algoritmusokkal kapcsolatos határozatban foglalt algoritmusok és kulcsparaméterek használhatók, amelyek várhatóan a kulcs teljes élettartama alatt képesek ellenállni a kriptográfiai támadásoknak.

A szolgáltatói magánkulcsokat kódolt formában is fizikailag biztonságos helyszínen kell tárolni, ahol azokhoz csak az arra jogosultak férhetnek hozzá.

A kriptográfiai algoritmusok vagy kulcsparaméterek gyengülése esetén a kódolt kulcsokat meg kell semmisíteni vagy erősebb védelmet biztosító algoritmus és kulcsparaméterek felhasználásával tovább kell kódolni.

6.1.2. Magánkulcs többszereplős (n-ből m) használata

A *Minősített archiválási szolgáltató*nak biztosítania kell, hogy a szolgáltatói magánkulcsaival végzett kritikus műveletek végrehajtásához legalább kettő, bizalmi szerepkört betöltő munkatárs egyidejű jelenlétére legyen szükség.

6.1.3. Magánkulcs letétbe helyezése

A *Minősített archiválási szolgáltató* nem helyezheti letétbe a szolgáltatói aláíró magánkulcsait.

6.1.4. Magánkulcs mentése

A *Minősített archiválási szolgáltató*nak biztonsági másolatokat kell készítenie szolgáltatói magánkulcsairól, ebből legalább egy példányt a szolgáltatás nyújtásától eltérő helyszínen kell tárolni.

A biztonsági másolatok készítése csak védett környezetben, legalább két bizalmi szerepkört betöltő személy együttes jelenlétében, más személyek kizárásával történhet.

A biztonsági másolatok kezelésére és megőrzésére legalább ugyanolyan szigorú biztonsági előírásokat kell alkalmazni, mint az éles rendszer üzemeltetésére.

6.1.5. Magánkulcs archiválása

A *Minősített archiválási szolgáltató* nem archiválhatja magánkulcsait.

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

A *Minősített archiválási szolgáltató* valamennyi szolgáltatói magánkulcsát a követelményeknek megfelelő *Hardver kriptográfiai eszköz*ben kell előállítani.

A magánkulcsok nem létezhetnek nyílt formában a *Hardver kriptográfiai eszköz*ön kívül.

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

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

6.1.7. Magánkulcs tárolása hardver kriptográfiai eszközben

A *Minősített archiválási szolgáltató*nak a jelen *Minősített archiválási rend*ek szerinti szolgáltatás nyújtásához használt magánkulcsait kriptográfiai modulban kell tartania.

A *Hardver kriptográfiai eszköz*ön belüli tárolási formára vonatkozóan nincs előírás.

6.1.8. A magánkulcs aktiválásának módja

A *Minősített archiválási szolgáltató* szolgáltatói magánkulcsait a felhasznált *Hardver kriptográfiai eszköz* felhasználói útmutatójában és a tanúsítási dokumentumokban megfogalmazott eljárásoknak, követelményeknek megfelelően kell aktiválni.

6.1.9. A magánkulcs deaktiválásának módja

A *Minősített archiválási szolgáltató* szolgáltatói magánkulcsait a felhasznált *Hardver kriptográfiai eszköz* felhasználói útmutatójában és a tanúsítási dokumentumokban megfogalmazott eljárásoknak, követelményeknek megfelelően kell deaktiválni.

6.1.10. A magánkulcs megsemmisítésének módja

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

A szolgáltatói magánkulcsok megsemmisítését a felhasznált *Hardver kriptográfiai eszköz* felhasználói útmutatójában és a tanúsítási dokumentumokban megfogalmazott eljárásoknak, követelményeknek megfelelően kell elvégezni.

A magánkulcsról készült minden mentett példányt dokumentált módon meg kell semmisíteni olyan módon, hogy annak visszaállítása, használata lehetetlenné váljon.

6.1.11. A hardver kriptográfiai eszközök értékelése

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

- rendelkezik ISO/IEC 19790 [11] szerinti tanúsítással,
- vagy rendelkezik FIPS 140-2 Level 3 [12] szerinti tanúsítással,
- vagy rendelkezik a CEN 14167-2 [13] munkacsoport egyezmény követelményeinek való megfelelést igazoló Common Criteria alapú tanúsítvánnyal,

- vagy rendelkezik a Nemzeti Média- és Hírközlési Hatóság által vagy az Európai Unió valamely tagállamában nyilvántartásba vett, elektronikus aláírási termékek értékelésére jogosult független tanúsító szervezet által erre a célra kiadott igazolással.

6.2. Aktivizáló adatok

6.2.1. Aktivizáló adatok előállítása és telepítése

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

Jelszó alapú aktivizáló adatok használata esetén a jelszavaknak kellően bonyolultnak kell lenniük a megkívánt védelmi szint biztosítása érdekében.

6.2.2. Az aktivizáló adatok védelme

A *Minősített archiválási szolgáltató* alkalmazottainak a magánkulcsok aktiválásához szükséges eszközöket, aktivizáló adatokat biztonságosan kell tárolniuk, a jelszavak csak kódolt formában tárolhatók.

6.2.3. Az aktivizáló adatok kezelésének egyéb szempontjai

Nincs megkötés.

6.3. Informatikai biztonsági előírások

6.3.1. Speciális informatikai biztonsági műszaki követelmények

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

- a rendszerhez vagy alkalmazáshoz való hozzáférés engedélyezése előtt a felhasználó azonosságát ellenőrizni kell;
- a felhasználókhoz szerepköröket kell rendelni és biztosítani kell, hogy minden felhasználó csak a szerepkörének megfelelő jogosultságokkal rendelkezzen;
- minden tranzakcióról naplóbejegyzést kell előállítani és a naplóbejegyzéseket archiválni kell;
- a biztonságkritikus folyamatok részére biztosítani kell, hogy a *Minősített archiválási szolgáltató* belső hálózati tartományai kellően védettek legyenek a jogosulatlan hozzáféréstől;
- megfelelő eljárásokat kell alkalmazni a kulcsvesztés vagy rendszerhiba után a szolgáltatás visszaállítása érdekében.

6.3.2. Az informatikai biztonság értékelése

Az informatikai biztonság és a szolgáltatás minőségének biztosítása érdekében a *Minősített archiválási szolgáltató* nemzetközileg elfogadott módszertanok szerinti irányítási rendszert kell alkalmazzon, ezek megfelelőségét független tanúsító szervezet által kiállított tanúsítvánnyal kell igazolnia.

6.4. Életciklusra vonatkozó műszaki előírások

6.4.1. Rendszerfejlesztési előírások

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

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

A beszerzést a hardver és szoftver komponensek módosítását kizáró módon kell elvégezni.

A szolgáltatás nyújtásához használt hardver és szoftver komponensek más célra nem használhatók.

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 ellenőrizni kell kártékony kódok után kutatva.

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

Megbízható, megfelelően képzett személyzetet kell alkalmazni a szoftverek és eszközök telepítése során.

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

A *Minősített archiválási szolgáltató*nak rendelkeznie kell egy változáskövető rendszerrel, amelyben minden változást dokumentálni kell.

A *Minősített archiválási szolgáltató* alkalmazzon eljárásokat a jogosulatlan változások észlelésére.

6.4.2. Biztonságkezelési előírások

A *Minősített archiválási szolgáltató* alkalmazzon eljárásokat a szolgáltatásban használt rendszerek telepítésének, konfigurációjának dokumentálására, üzemeltetésére, ellenőrzésére, monitorozására

és karbantartására, beleértve a módosításokat és továbbfejlesztéseket is. A változáskövető rendszernek észlelnie kell 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* győződjön meg róla, hogy a telepítendő program a megfelelő verziójú és mentes mindenféle jogosulatlan módosítástól. A *Minősített archiválási szolgáltató* ellenőrizze rendszeresen a szolgáltatói rendszereiben használt programok integritását.

6.4.3. Életciklusra vonatkozó biztonsági előírások

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

- Megfelelő tanúsítással rendelkező *Hardver kriptográfiai eszköz*t kell használnia.
- A *Hardver kriptográfiai eszköz* átvételekor meg kell róla győződni, hogy a szállítás során biztosították a *Hardver kriptográfiai eszköz*ök feltörés elleni védelmét.
- A tárolás során biztosítani kell a *Hardver kriptográfiai eszköz*ök feltörés elleni védelmét.
- Az üzemeltetés során folyamatosan be kell tartani a *Hardver kriptográfiai eszköz* biztonsági előirányzatában, használati útmutatójában és a tanúsítási jelentésben szereplő követelményeket.
- A használatból kivont *Hardver kriptográfiai eszköz*ökben tárolt magánkulcsokat olyan módon kell törölni, hogy lehetetlenné váljon a kulcsok visszaállítása.

6.5. Hálózati biztonsági előírások

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

A *Minősített archiválási szolgáltató* alkalmazzon megfelelő hálózatbiztonsági intézkedéseket, mint például

- tiltsa le a használaton kívüli hálózati portokat és szolgáltatásokat;
- csak az IT rendszer megfelelő működéséhez feltétlenül szükséges hálózati alkalmazásokat futtasson.

A *Minősített archiválási szolgáltató*nak sérülékenységvizsgálatot kell végeznie vagy végeztetnie 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 negyedévente egyszer.

6.6. Időbélyegzés

A *Minősített archiválási szolgáltató*nak valamely Európai Uniós tagállam bizalmi listáján szereplő minősített időbélyegzés-szolgáltató által biztosított *Időbélyegző*ket kell használnia a naplóbejegyzések és egyéb archiválandó elektronikus állományok hitelesítésére.

7. A megfelelőség vizsgálata

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

Az átvilágítás tematikája és módszertana feleljen meg 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; [9]
- ETSI EN 319 401 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [8]

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

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

A *Minősített archiválási szolgáltató* fenntartja a jogot, hogy a jelen *Minősített archiválási rend*(ek) alapján működő szolgáltatók tevékenységét tetszőleges időpontban független szakértő bevonásával átvizsgálja a követelmények betartásának ellenőrzése érdekében.

7.1. Az ellenőrzések körülményei és gyakorisága

A *Minősített archiválási szolgáltató* évente köteles elvégeztetni a megfelelőségértékelő vizsgálatot.

7.2. Az auditor és szükséges képesítése

A *Minősített archiválási szolgáltató* a belső auditokat a független rendszervizsgáló szerepkörrel felruházott alkalmazottai segítségével is elvégezheti.

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

7.3. Az auditor és az auditált rendszerelem függetlensége

A külső auditot csak olyan személy végezheti:

- 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;

7.4. Az auditálás által lefedett területek

Az átvizsgálásnak le kell fednie minimálisan az alábbi területeket:

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

7.5. A hiányosságok kezelése

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

- opcionálisan figyelembe vehető módosítási javaslatokat;

- kötelezően elhárítandó eltéréseket.

A független auditornak a feltárt súlyos eltéréseket haladéktalanul jelentenie kell a Nemzeti Média- és Hírközlési Hatóságnak, aki jogosult meghozni a szükséges intézkedéseket.
A *Minősített archiválási szolgáltató* köteles a független vizsgáló által felvetett problémákra írásban válaszolni, az elhárításukra tett intézkedésekről a következő hatósági szemle alkalmával beszámolni.
A független auditornak a vizsgálati jelentést minden esetben meg kell küldenie a Nemzeti Média- és Hírközlési Hatóságnak.

7.6. Az eredmények közzététele

A *Minősített archiválási szolgáltató* a vizsgálat eredményét összefoglaló jelentést köteles nyilvánosságra hozni. Nem köteles a független rendszervizsgálat során feltárt hiányosságok publikálására, azokat bizalmas információként kezelheti.

8. Egyéb üzleti és jogi kérdések

8.1. Díjak

A *Minősített archiválási szolgáltató* által alkalmazható díjakat a vonatkozó szabályozásnak megfelelően nyilvánosan közzé kell tenni.

8.1.1. Visszatérítési politika

Nincs megkötés.

8.2. Anyagi felelősségvállalás

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

8.2.1. Pénzügyi követelmények

A *Minősített archiválási szolgáltató* a szolgáltatási tevékenységének megszűnésével kapcsolatos költségek biztosítása és a megbízhatóság érdekében köteles az alábbi követelmények legalább egyikének megfelelni:

- A *Minősített archiválási szolgáltató* legalább huszonötmillió forint összegű, feltétel nélküli és visszavonhatatlan bankgaranciával rendelkezik.
- A *Minősített archiválási szolgáltató* a Nemzeti Média- és Hírközlési Hatóság mint jogosult javára pénzügyi intézménynél óvadékot tesz le. Az óvadék összege legalább huszonötmillió forint.

- A költségek megfizetéséért hitelesítés-szolgáltató esetén legalább százmillió forint jegyzett tőkéjű európai uniós vállalkozás készfizető kezességet vállal. A kezességvállalás mértéke legalább huszonötmillió forintig terjed.

8.2.2. Felelősségbiztosítás

- A *Minősített archiválási szolgáltató*nak a megbízhatóság biztosítása érdekében felelősségbiztosítással kell rendelkeznie.
- A felelősségbiztosítási szerződésnek ki kell terjednie 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 felelősségbiztosításnak a meghatározott összeg erejéig fedezetet kell nyújtania 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.

8.3. Bizalmasság

A *Minősített archiválási szolgáltató*nak az *Ügyfel*ek adatait a jogszabályoknak megfelelően kell kezelnie.

8.3.1. Bizalmas információk köre

A *Minősített archiválási szolgáltató*nak a *Minősített archiválási szolgáltatási szabályzat*ában pontosan meg kell határoznia, hogy mely adatok minősülnek bizalmas információnak.

8.3.2. Bizalmas információk körén kívül eső adatok

A *Minősített archiválási szolgáltató* nyilvánosnak tekinthet miden olyan adatot, amely nem szerepel a bizalmas adatok felsorolásában a *Minősített archiválási szolgáltatási szabályzat*ban.

8.3.3. Bizalmas információ védelme

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

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

A *Minősített archiválási szolgáltató Minősített archiválási szolgáltatási szabályzat*ában tételesen meg kell határozni azon eseteket, amikor a *Minősített archiválási szolgáltató* felfedheti a bizalmas adatokat.

8.4. Személyes adatok védelme

A *Minősített archiválási szolgáltató*nak gondoskodnia kell az általa kezelt személyes adatok védelméről. Működésének és szabályzatainak meg kell felelniük az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény [2] rendelkezéseinek.

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

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

8.4.1. Adatkezelési szabályzat

A *Minősített archiválási szolgáltató*nak rendelkeznie kell Adatkezelési szabályzattal, amely részletes előírásokat tartalmaz a személyes adatok kezelésére. Az Adatkezelési szabályzatot nyilvánosságra kell hozni a *Minősített archiválási szolgáltató* honlapján.

8.4.2. Személyes adatok

A *Minősített archiválási szolgáltató*nak védenie kell 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 gyűjthet személyes adatokat és csak olyan mértékben, ami a szolgáltatás nyújtásához szükséges.

8.4.3. Személyes adatnak nem minősülő adatok

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

8.4.4. Személyes adatok védelme

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

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

8.4.5. Személyes adatok felhasználása

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

8.4.6. Adatkezelés

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

8.4.7. Egyéb adatvédelmi követelmények

Nincs előírás.

8.5. Szellemi tulajdonjogok

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

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

A jelen *Minősített archiválási rend* 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 *Minősített archiválási szolgáltatási szabályzat*ban kell meghatározni.

8.6. Tevékenységért viselt felelősség és helytállás

8.6.1. A szolgáltató felelőssége és helytállása

A Szolgáltató felelőssége

A *Minősített archiválási szolgáltató* felel a jelen *Minősített archiválási rend*ben, a vonatkozó *Minősített archiválási szolgáltatási szabályzat*ban valamint az *Ügyfél*lel kötött Szolgáltatási szerződésben megfogalmazott valamennyi rá vonatkozó kötelezettség maradéktalan betartásáért, különösen a következő esetekben:

- a *Minősített archiválási szolgáltató* felelősséget vállal az általa támogatott *Minősített archiválási rend*(ek)ben leírt eljárásoknak való megfelelésért;
- a *Minősített archiválási szolgáltató* sajátjaként felel az alvállalkozói által a szolgáltatás nyújtása során okozott károkért;
- a *Minősített archiválási szolgáltató* a vele szerződéses jogviszonyban álló *Ügyfel*ekkel szemben a Polgári Törvénykönyv [3] 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 [3] általános felelősségi szabálya szerint felelős;
- a *Minősített archiválási szolgáltató* a felelősségi körén belül keletkezett, bizonyított károkért a szabályzataiban és az *Ügyfél*lel megkötött Szolgáltatási szerződésekben rögzített korlátozásokkal kártérítést fizet (lásd: Pénzügyi felelősség korlátozása 8.8. fejezet);

A Szolgáltató kötelezettsége

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

A *Minősített archiválási szolgáltató* alapvető kötelezettsége, hogy a szolgáltatásokat a *Minősített archiválási rend*del, a *Minősített archiválási szolgáltatási szabályzat*tal és egyéb nyilvános szabályzatokkal, a szerződéses feltételekkel, továbbá a vállalati és biztonsági belső szabályzatokkal összhangban nyújtsa. Ezen alapvető kötelezettségek a következők:

- a szolgáltatásnak megfelelő jogi-, szabályozási-, anyagi-, szerződéses stb. keretek megteremtése;
- magas színvonalú és biztonságos szolgáltatások nyújtása a vonatkozó szabályzatok szerint;
- a szolgáltatásokhoz kapcsolódó szervezetek (hitelesítő szervezet, ügyfélszolgálat stb.) folyamatos működtetése és ellenőrzése;
- a szabályzatokban előírt eljárások betartása és az esetleg bekövetkező helytelen működés elkerülése, illetve megszüntetése;
- a szolgáltatások biztosítása minden olyan igénylő számára, aki elfogadja a szabályzatokban rögzített feltételeket;
- a publikus nyilvántartások és saját szabályzatok karbantartása és folyamatos elérhetővé tétele bárki számára az interneten keresztül.

8.6.2. Az Ügyfél felelőssége és helytállása

Az *Előfizető* felelőssége

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

Az *Előfizető* kötelezettségei

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

Az *Előfizető* kötelezettségeit a jelen *Minősített archiválási rend*, a Szolgáltatási szerződés és annak mellékletei – különösen az Általános szerződési feltételek – és a *Minősített archiválási szolgáltatási szabályzat* írja le.

8.6.3. Az Érintett fél felelőssége

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

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

8.6.4. Egyéb szereplők tevékenységéért viselt felelősség és helytállás

Nincs megkötés.

8.7. Helytállás érvénytelenségi köre

A *Minősített archiválási szolgáltató* kizárja felelősségét, amennyiben:

- az Internet, vagy annak egy részének működési hibájából adódóan a tájékoztatás és egyéb kommunikációs kötelezettségeit nem tudja ellátni;
- a károkozás a Nemzeti Média- és Hírközlési Hatóság algoritmusokkal kapcsolatos határozat által elfogadott kriptográfiai algoritmusok hibájából, illetve gyengeségeiből ered.

8.8. A felelősség korlátozása

Nincs megkötés.

8.9. Kártérítési kötelezettség

8.9.1. A szolgáltató kártérítési kötelezettsége

A *Minősített archiválási szolgáltató* kártérítési kötelezettségének részletes szabályait a *Minősített archiválási szolgáltatási szabályzat*, a Szolgáltatási szerződés vagy az *Ügyfel*ekkel kötött szerződések tartalmazzák.

8.9.2. Az előfizető kártérítési kötelezettsége

A *Minősített archiválási szolgáltató* a *Minősített archiválási szolgáltatási szabályzat*ban és a Szolgáltatási szerződésben szabályozza az *Előfizető*kkel szemben támasztott kártérítési igényeit.

8.9.3. Az érintett felek kártérítési kötelezettsége

A *Minősített archiválási szolgáltató* a *Minősített archiválási szolgáltatási szabályzat*ban szabályozza az *Érintett felek*kel szemben támasztott kártérítési igényeit.

8.10. Érvényesség és megszűnés

8.10.1. Érvényesség

A *Minősített archiválási rend* adott verziója hatálybalépésének napja a dokumentum címlapján kerül meghatározásra.

8.10.2. Megszűnés

A *Minősített archiválási rend* visszavonásig hatályos időbeli korlátozás nélkül.

8.10.3. A megszűnés következményei

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

8.11. A felek közötti kommunikáció

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

8.12. Módosítások

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

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

8.12.1. Módosítási eljárás

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

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

A *Minősített archiválási szolgáltató* a közzétett új szabályzat tervezettel kapcsolatos észrevételeket a 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.

8.12.2. Értesítések módja és határideje

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

8.12.3. Az OID megváltoztatása

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

8.13. Vitás kérdések rendezése

A *Minősített archiválási szolgáltató* törekedjen a működése során felmerülő vitás kérdések békés, tárgyalásos rendezésére. A rendezés során a fokozatosság elvét kell követni.

8.14. Irányadó jog

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

8.15. Az érvényben lévő jogszabályoknak való megfelelés

A jelen *Minősített archiválási rend* megfelel az alábbi jogszabályoknak:

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

- 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól [4];
- 24/2016. (VI. 30.) BM rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről [5];
- 25/2016. (VI. 30.) BM rendelet a bizalmi felügyeletnek fizetendő igazgatási szolgáltatási díjak mértékéről [6];
- 26/2016. (VI. 30.) BM rendelet a bizalmi felügyelet által vezetett nyilvántartások tartalmáról és a bizalmi szolgáltatás nyújtásával kapcsolatos bejelentésekről [7];
- ETSI EN 319 401 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [8];
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról [2];
- 2013. évi V. törvény a Polgári Törvénykönyvről [3].

8.16. Vegyes rendelkezések

8.16.1. Teljességi záradék

Nincs megkötés.

8.16.2. Átruházás

A jelen *Minősített archiválási rend*nek megfelelően működő szolgáltatók csak a *Minősített archiválási szolgáltató* előzetes írásbeli engedélyével adhatják tovább jogosultságaikat és delegálhatják kötelezettségeiket harmadik félnek.

8.16.3. Részleges érvénytelenség

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

8.16.4. Igényérvényesítés

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

8.16.5. Vis maior

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

8.17. Egyéb rendelkezések

Nincs megkötés.

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

[3] 2013. évi V. törvény a Polgári Törvénykönyvről .

[4] 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól .

[5] 24/2016. (VI. 30.) BM rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről .

[6] 25/2016. (VI. 30.) BM rendelet a bizalmi felügyeletnek fizetendő igazgatási szolgáltatási díjak mértékéről .

[7] 26/2016. (VI. 30.) BM rendelet a bizalmi felügyelet által vezetett nyilvántartások tartalmáról és a bizalmi szolgáltatás nyújtásával kapcsolatos bejelentésekről .

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

[9] 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;.

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

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

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

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