Elektronikusan aláírta:
Péchy Gábor
Szigná

NOTARchiv

Minősített archiválási szolgáltatás archiválási rendje OID:1.3.6.1.4.1.54136.1.1.1.1.1.6

A dokumentum azonosítása angolul	Preservation Policy
A dokumentum rövid azonosítása	Archiválási rend
Kiadás dátuma	Időbélyeg szerint
Hatályba lépés dátuma	2025.08.01.

Jóváhagyta: _____ dátum: _____/_____/_____

Péchy Gábor, ügyvezető, NOTARchiv Kft.

© NOTARchiv Kft.
Minden jog fenntartva. A NOTARchiv Kft. előzetes írásos engedélye nélkül a jelen dokumentum egyetlen része sem reprodukálható, nem továbbítható semmilyen formában és semmilyen esetben, nem tárolható és nem helyezhető el adatbázisokban.

A DOKUMENTUM ADATAI

Cím	Archiválási rend
Biztonsági besorolás	PUBLIKUS
Kiadás dátuma	lásd: borító.

JÓVÁHAGYÓK

Név	Beosztás	Aláírás
Péchy Gábor	ügyvezető	lásd: borító.

© NOTARchiv Kft.
Minden jog fenntartva. A NOTARchiv Kft. előzetes írásos engedélye nélkül a jelen dokumentum egyetlen része sem reprodukálható, nem továbbítható semmilyen formában és semmilyen esetben, nem tárolható és nem helyezhető el adatbázisokban.

Tartalom

Tartalom 3

1 Bevezetés 9

1.1 Áttekintés 9

1.2 A dokumentum azonosítása 9

1.2.1 Hatály 9

1.3 Szereplők 10

1.3.1 A Minősített bizalmi szolgáltató 10

1.3.2 Az ügyfelek 11

1.3.3 Az érintett felek 11

1.4 A tanúsítványok alkalmazhatósága 11

1.5 A hitelesítési rend adminisztrációja 11

1.5.1 A dokumentum adminisztrálása 11

1.5.2 Kapcsolattartó személy 11

1.5.3 A szolgáltatási szabályzat megfelelőségéért felelős személy és/vagy szervezet 11

1.5.4 A szolgáltatási szabályzat elfogadási eljárása 11

1.6 Fogalmak és rövidítések 12

1.6.1 Fogalmak 12

1.6.2 Rövidítések 14

2 Közzététel 14

2.1 Szolgáltatási információ közzététele 14

2.2 A közzététel időpontja és gyakorisága 14

2.3 Információ hozzáférés biztosítása 14

3 Azonosítás és hitelesítés 15

4 Életciklus követelmények - Elektronikus archiválási szolgáltatás 15

4.1 A szolgáltatás igénylése - Szerződéskötés 15

4.2 Szolgáltatás nyújtása 15

4.2.1 Dokumentum befogadása és a visszaigazolás 15

4.2.2 Megőrzés, felülhitelesítés 15

4.2.3 Archivált objektum és érvényességi lánc elérhetőségének biztosítása 16

4.2.4 Igazolás kibocsátása 16

4.2.5 Dokumentum megjelenítése 16

4.3 Szolgáltatás elérhetősége 16

© NOTARchiv Kft.
Minden jog fenntartva. A NOTARchiv Kft. előzetes írásos engedélye nélkül a jelen dokumentum egyetlen része sem reprodukálható, nem továbbítható semmilyen formában és semmilyen esetben, nem tárolható és nem helyezhető el adatbázisokban.

4.4 A Szerződésmegszűnése 16
4.4.1 Dokumentum és érvényességi lánc törlése 16
5 Fizikai, eljárásbeli és üzemeltetési előírások 18
5.1 Fizikai követelmények 18
5.1.1 Telephelyek és szerkezeti felépítésük 18
5.1.2 A fizikai hozzáférés szabályozása 18
5.1.3 Áramellátás és légkondicionálás 19
5.1.4 Beázás és vízbetörés 19
5.1.5 Tűz megelőzés és tűzvédelem 19
5.1.6 Adathordozók tárolása 19
5.1.7 Hulladék megsemmisítése 19
5.1.8 A mentési példányok fizikai elkülönítése 19
5.2 Eljárásrendi előírások 20
5.2.1 Bizalmi szerepkörök 20
5.2.2 Az egyes feladatokhoz szükséges személyzeti létszámok 20
5.2.3 Az egyes szerepkörökhöz elvárt azonosítás és hitelesítés 20
5.2.4 Egymást kizáró szerepkörök 21
5.3 Személyzetre vonatkozó előírások 21
5.3.1 Képzettségre, gyakorlatra és megbízhatóságra vonatkozó követelmények 21
5.3.2 Biztonsági ellenőrzésre vonatkozó követelmények 22
5.3.3 Képzési követelmények 22
5.3.4 Továbbképzés gyakorisága 22
5.3.5 Munkabeosztás körforgása 22
5.3.6 Felhatalmazás nélküli tevékenységek szankciói 22
5.3.7 Szerződéses jogviszonyra vonatkozó követelmények 22
5.3.8 Működést támogató dokumentációk 22
5.4 A biztonsági naplózás folyamatai 22
5.4.1 A tárolt események típusai 23
5.4.2 A naplófájlok feldolgozásának gyakorisága 24
5.4.3 A naplófájl megőrzési időtartama 25
5.4.4 A naplófájl védelme 25
5.4.5 A naplófájl mentési eljárásai 25
5.4.6 A naplózás adatgyűjtési rendszere 25
5.4.7 Az eseményeket kiváltó Ügyfelek értesítése 25

© NOTARchiv Kft.
Minden jog fenntartva. A NOTARchiv Kft. előzetes írásos engedélye nélkül a jelen dokumentum egyetlen része sem reprodukálható, nem továbbítható semmilyen formában és semmilyen esetben, nem tárolható és nem helyezhető el adatbázisokban.

5.4.8 Sebezhetőség felmérése 25
5.5 Adatok archiválása 25
5.5.1 Az archiválandó adatok típusa 25
5.5.2 Adatok megőrzésének időtartama 25
5.5.3 Az archívum védelme 26
5.5.4 Az archívum mentési folyamatai 26
5.5.5 Az adatok időbélyegzésére vonatkozó követelmények 26
5.5.6 Az archívum gyűjtési rendszere 26
5.5.7 Archív információk hozzáférését és ellenőrzését végző eljárások 26
5.6 Kulcscsere 26
5.7 Katasztrófa helyzet kezelése 26
5.7.1 Váratlan esemény kezelési eljárások 27
5.7.2 Meghibásodott IT erőforrások és/vagy adatok 27
5.7.3 Magánkulcs kompromittálódása esetén követendő eljárás 27
5.7.4 Működés folyamatosságának biztosítása 27
5.8 A szolgáltatás megszűnése 28
6 Műszaki biztonsági óvintézkedések 29
6.1 Kulcspár generálás és telepítés 29
6.1.1 Kulcspár előállítása 29
6.1.2 Magánkulcs eljuttatása Végfelhasználóhoz 29
6.1.3 A nyilvános kulcs eljuttatása a tanúsítványkibocsátóhoz 29
6.1.4 A Minősített bizalmi szolgáltatói nyilvános kulcs közzététele 29
6.1.5 Kulcsméretek 29
6.1.6 A nyilvános kulcs paraméterek előállítása, a minőség ellenőrzése 29
6.2 A magánkulcsok védelme 30
6.2.1 Kriptográfiai modulra vonatkozó szabványok és előírások 30
6.2.2 Magánkulcs használata 30
6.2.3 Magánkulcs letétbe helyezése 30
6.2.4 Magánkulcs mentése 30
6.2.5 Magánkulcs archiválása 30
6.2.6 Magánkulcs import és export 30
6.2.7 Magánkulcs tárolása hardware kriptográfiai eszközben 30
6.2.8 Magánkulcs aktiválása 31
6.2.9 Magánkulcs deaktiválása 31

© NOTARchiv Kft.
Minden jog fenntartva. A NOTARchiv Kft. előzetes írásos engedélye nélkül a jelen dokumentum egyetlen része sem reprodukálható, nem továbbítható semmilyen formában és semmilyen esetben, nem tárolható és nem helyezhető el adatbázisokban.

6.2.10 Magánkulcs megsemmisítése ... 31
6.2.11 Kriptográfiai modulok értékelése ... 31
6.3 Kulcspárkezelés szempontjai ... 31
6.4 Aktivizáló adatok ... 31
6.4.1 Aktivizáló adatok előállítása és alkalmazása ... 31
6.4.2 Az aktivizáló adatok védelme ... 31
6.5 Informatikai biztonsági előírások ... 31
6.5.1 Speciális informatikai biztonsági műszaki követelmények ... 31
6.5.2 Az informatikai biztonság ellenőrzése ... 32
6.6 Életciklusra vonatkozó műszaki előírások ... 32
6.6.1 Rendszerfejlesztési előírások ... 32
6.6.2 Biztonságkezelési eljárások ... 32
6.7 Életciklusra vonatkozó biztonsági előírások ... 33
6.8 Hálózati biztonsági előírások ... 33
7 Tanúsítvány profil ... 34
8 A megfelelőség vizsgálata ... 34
8.1 Az ellenőrzések gyakorisága ... 34
8.2 Az auditorral szembeni elvárások ... 34
8.3 Az auditor és az auditált függetlensége ... 34
8.4 A vizsgálat által érintett területek ... 35
8.5 A hiányosságok kezelése ... 35
8.6 Az eredmények közzététele ... 35
9 Egyéb üzleti és jogi kérdések ... 36
9.1 Díjak ... 36
9.1.1 Archiválás szolgáltatás díjai ... 36
9.1.2 Visszatérítési politika ... 36
9.2 Pénzügyi felelősség ... 36
9.2.1 Biztosítási fedezet ... 36
9.2.2 Egyéb eszközök ... 36
9.2.3 Az Érintett felek számára elérhető biztosítások és garanciák ... 37
9.3 Bizalmasság, adatvédelem ... 37
9.3.1 Bizalmas információk köre ... 37
9.3.2 Bizalmas információk körén kívül eső adatok ... 37
9.3.3 Bizalmas információk védelme ... 37

© NOTARchiv Kft.
Minden jog fenntartva. A NOTARchiv Kft. előzetes írásos engedélye nélkül a jelen dokumentum egyetlen része sem reprodukálható, nem továbbítható semmilyen formában és semmilyen esetben, nem tárolható és nem helyezhető el adatbázisokban.

9.4 Személyes adatok védelme 37
9.4.1 Adatkezelési tájékoztató 37
9.4.2 Személyes adatok 37
9.4.3 Személyes adatnak nem minősülő adatok 38
9.4.4 Személyes adatok védelme 38
9.4.5 Személyes adatok felhasználása 38
9.4.6 Adatkezelés 38
9.4.7 Egyéb adatvédelmi követelmények 38
9.5 Szellemi tulajdonjogok 38
9.6 Felelősség és helytállás 38
9.6.1 A Minősített bizalmi szolgáltató felelőssége és helytállása 38
9.6.2 Az ügyfél felelőssége és helytállása 39
9.6.3 Az érintett fél felelőssége 39
9.6.4 Egyéb szereplők tevékenységéért viselt felelősség és helytállás 39
9.7 A helytállás érvénytelenségi köre 39
9.8 A felelősség korlátozása 39
9.9 Kártérítési kötelezettség 39
9.9.1 A Minősített bizalmi szolgáltató kártérítési kötelezettsége. 39
9.10 Érvényesség és megszűnés 39
9.10.1 Érvényesség 39
9.10.2 Megszűnés 39
9.10.3 A megszűnés következményei 39
9.11 A felek közötti kommunikáció 39
9.12 Módosítások 40
9.12.1 Módosítási eljárás 40
9.12.2 Értesítések módja és határideje 40
9.12.3 A hitelesítési rend azonosítójának megváltoztatása 40
9.13 Vitás kérdések rendezése 41
9.14 Irányadó jog 41
9.15 Az érvényben lévő jogszabályoknak való megfelelés 41
9.16 Vegyes rendelkezések 41
9.16.1 Teljességi záradék 41
9.16.2 Átruházás 41
9.16.3 Részleges érvénytelenség 41

© NOTARchiv Kft.
Minden jog fenntartva. A NOTARchiv Kft. előzetes írásos engedélye nélkül a jelen dokumentum egyetlen része sem reprodukálható, nem továbbítható semmilyen formában és semmilyen esetben, nem tárolható és nem helyezhető el adatbázisokban.

9.16.4 Igényérvényesítés 42

9.16.5 Vis major 42

9.17 Egyéb rendelkezések 42

10. Megfelelőségi vizsgálat, vizsgált követelmények, vizsgált rendek azonosítói (3.§ (3) f)) 42

© NOTARchiv Kft.

Minden jog fenntartva. A NOTARchiv Kft. előzetes írásos engedélye nélkül a jelen dokumentum egyetlen része sem reprodukálható, nem továbbítható semmilyen formában és semmilyen esetben, nem tárolható és nem helyezhető el adatbázisokban.

1 Bevezetés

Jelen dokumentum a NOTARchiv Kft. (továbbiakban: „Minősített bizalmi szolgáltató") által üzemeltetett minősített elektronikus archiválási szolgáltatására vonatkozó archiválási rendjét tartalmazza. Az eIDAS Rendelet (1) által meghatározott követelményeknek jelen dokumentum megfelel a rendeletben foglalt szabályoknak.
A dokumentum az RFC 3647 előírásai szerinti szerkezetet követi, az eIDAS, a DÁP. és releváns magyar jogszabályok és EN 319 401 és TS 119 511 szabványok elvárásait foglalja össze.

A szolgáltatási szabályzat és a kikötések együttesen meghatározzák a szolgáltatás paramétereit és az igénybevételhez szükséges részleteket, eszközöket.

1.1 Áttekintés

Az archiválási rend a minősített elektronikus archiválási szolgáltatás felhasználhatóságát definiálja egy kölcsönös biztonsági követelményekkel rendelkező közösség számára továbbá alapvető kritériumokat határoz meg főleg a Minősített bizalmi szolgáltató irányába a létesítendő minősített elektronikus archiválási szolgáltatás vonatkozásában.
Az archiválási rend egyike azon dokumentumoknak melyek a Minősített bizalmi szolgáltató által kiadott nyilvános biztonsági besorolással rendelkező szabályzatnak, és az archív szolgáltatást együtt hivatottak szabályozni.
A jelen dokumentum „Fogalmak és rövidítések" pontja különböző fogalmat magyaráz meg, amelyeket más területeken nem, vagy nem teljes értelmezésben használnak.

1.2 A dokumentum azonosítása

A dokumentum azonosítása a címlapon megadott adatokkal történik.
A dokumentum verzió száma egyben az OID száma is.

A Szolgáltató megfelel az ETSI TS 119511-nek, és Annex A fejezeteinek, így a policy azonosítása során jogosult a minősített megőrzési szolgáltatás policy azonosítóját is feltüntetni a policy dokumentáción, amely:
0.4.0.19511.1.2
itu-t(0) identified-organization(4) etsi(0) pres-service-policies(19511) policy-identifiers(1) qualified (2).

1.2.1 Hatály

Jelen dokumentum a hatálybalépési időpontjától annak visszavonásáig van érvényben. Jelen dokumentumban foglaltakat és a rá épülő Minősített archiválási szolgáltatási szabályzat tartalmát évente felül kell vizsgálni. A dokumentum hatálya kiterjed a „A Szereplők" pontban rögzített felekre. Jelen dokumentum a magyarországi és EU-s jogszabályok alapján, elsősorban magyar és EU-s Ügyfelek számára, nyújtott szolgáltatásokra fogalmazza meg a követelményeket.
A Minősített bizalmi szolgáltató a szolgáltatás területi hatályát kiterjesztheti, ez esetben legalább a magyar és EU-s viszonyokra alkalmazható előírásoknak megfelelő, azoknál nem alkalmazhat enyhébb követelményeket.
Ennek részleteit a minősített archiválási szolgáltatási szabályzatnak kell tartalmaznia.

© NOTARchiv Kft.
Minden jog fenntartva. A NOTARchiv Kft. előzetes írásos engedélye nélkül a jelen dokumentum egyetlen része sem reprodukálható, nem továbbítható semmilyen formában és semmilyen esetben, nem tárolható és nem helyezhető el adatbázisokban.

1.2.1.1 Dokumentum verziók

Azonosító	Kiadás	Leírás	Készítette
1.3.6.1.4.1.54136. 1.1.1.1.1.0	lásd: borító	első kiadás (v1.0)	Bajusz Balázs
1.3.6.1.4.1.54136. 1.1.1.1.1.1	lásd: borító	- Kisebb pontosítások. (v1.1)	Bajusz Balázs
1.3.6.1.4.1.54136. 1.1.1.1.1.2	lásd: borító	Kisebb pontosítások.	Bajusz Balázs
1.3.6.1.4.1.54136. 1.1.1.1.1.3	lásd: borító	Kisebb pontosítások. Minősítettség feltüntetése a dokumentumban	Bajusz Balázs
1.3.6.1.4.1.54136. 1.1.1.1.1.4	lásd: borító	Kisebb pontosítások. 10. pont kiegészítés a Szolgáltatási szabályzat kivonata vonatkozásában	Bajusz Balázs
1.3.6.1.4.1.54136. 1.1.1.1.1.5	lásd: borító	Kisebb pontosítások, javítások hatályba lépő DÁP jogszabály és szabványok vonatkozásában	Bajusz Balázs
1.3.6.1.4.1.54136. 1.1.1.1.1.6	lásd: borító	Kisebb javítások, pontosítások.	Bajusz Balázs

1.3 Szereplők

1.3.1 A Minősített bizalmi szolgáltató

A szolgáltatást nyújtó Szolgáltató adatai a következők:

Kapcsolati adatok	
Minősített bizalmi szolgáltató teljes neve	NOTARchiv Korlátolt felelősségű társaság
Minősített bizalmi szolgáltató rövid neve	NOTARchiv Kft.
Minősített bizalmi szolgáltató székhelye	1087 Stróbl Alajos utca 3/b
Postázási cím:	1087 Stróbl Alajos utca 3/b
Cégjegyzékszám:	01-09328760
Adószám:	26497611-2-42
Elérhetőségek	
Telefonszám:	+36 (30) 158 5185, +36 (30) 158 5170
Weboldal:	notarchiv.hu
Kikötések és feltételek közzététele:	notarchiv.hu/docs.html
Ügyfélkapcsolati e-mail:	info@notarchiv.hu
Ügyfélfogadás / Nyitva tartás	Hétköznap 9:00-12:00

Jelen archiválási rendben találhatóak a követelmények a minősített archiválás szolgáltatás nyújtásához.

A Szolgáltató minősített szolgáltatást csak felügyeleti nyilvántartásba felvételt és a bizalmi listán feltüntetést követően végezhet.

A felügyelet nyilvántartásának elérhetősége:
http://webpub-ext.nmhh.hu/esign2016/szolgParams/init.do?tipus=mi
A bizalmi lista elérhetőségei:
http://nmhh.hu/tl/pub/HU_TL.pdf
http://nmhh.hu/tl/pub/HU_TL.xml

© NOTARchiv Kft.
Minden jog fenntartva. A NOTARchiv Kft. előzetes írásos engedélye nélkül a jelen dokumentum egyetlen része sem reprodukálható, nem továbbítható semmilyen formában és semmilyen esetben, nem tárolható és nem helyezhető el adatbázisokban.

1.3.2 Az ügyfelek

A minősített elektronikus archiválási szolgáltatást igénybe vevő fél (Ügyfél), aki Szolgáltatási szerződést köt a Minősített bizalmi szolgáltatóval és az igénybe vett szolgáltatással kapcsolatos költségek ellenértékét rendezi. Az elektronikus archiválási szolgáltatás során az Ügyfél által feltöltött dokumentumok az Ügyfél tulajdonát képezik mely(ek) felett az Ügyfél rendelkezhet.

1.3.3 Az érintett felek

A minősített elektronikus archiválási szolgáltatás során kibocsátott igazolásokat befogadó, illetve felhasználó fél.

1.4 A tanúsítványok alkalmazhatósága

A rendszer aláíró/bélyegző tanúsítványai kizárólag a szolgáltatás céljaira (felülhitelesítés, értesítés, igazolás) használhatók.

1.5 A hitelesítési rend adminisztrációja

1.5.1 A dokumentum adminisztrálása

Jelen dokumentum adminisztrációját ellátó szervezet adatai:

Szervezet neve	NOTARchiv Kft.
Szervezet címe	1087 Stróbl Alajos utca 3/b
Telefonszám	+36 (30) 158 5185 +36 (30) 158 5170
email címe	info@notarchiv.hu
Web oldala	www.notarchiv.hu

1.5.2 Kapcsolattartó személy

Jelen dokumentum adminisztrációját ellátó szervezet adatai:

Kapcsolattartó	Ügyfélszolgálat
Szervezet neve	NOTARchiv Kft.
Szervezet címe	1087 Stróbl Alajos utca 3/b
Telefonszám	+36 (30) 158 5185 +36 (30) 158 5170
email címe	info@notarchiv.hu
Web oldala	www.notarchiv.hu

1.5.3 A szolgáltatási szabályzat megfelelőségéért felelős személy és/vagy szervezet

A minősített szolgáltatás szolgáltatási szabályzatnak és az archiválási rendnek való megfeleléséért és az abban leírtak szerinti szolgáltatás nyújtásáért a szabályzatot kibocsátó Minősített bizalmi szolgáltató a felelős.

1.5.4 A szolgáltatási szabályzat elfogadási eljárása

A mindenkori hatályos archiválási rendnek való megfelelőséget kinyilatkoztató archiválás szolgáltatási szabályzat elfogadási eljárását az Minősített bizalmi szolgáltatónak ismertetnie kell a mindenkor hatályos archiválás szolgáltatási szabályzatában.

© NOTARchiv Kft.
Minden jog fenntartva. A NOTARchiv Kft. előzetes írásos engedélye nélkül a jelen dokumentum egyetlen része sem reprodukálható, nem továbbítható semmilyen formában és semmilyen esetben, nem tárolható és nem helyezhető el adatbázisokban.

1.6 Fogalmak és rövidítések

1.6.1 Fogalmak

Befogadott elektronikus dokumentum	Az Ügyfél által archiválás céljából feltöltött olyan elektronikus dokumentum, amely az archívumba történő befogadás részleteiről az Ügyfél elektronikus igazolást kapott.
Felügyelet	Nemzeti Média- és Hírközlési Hatóság röviden NMHH
E-akta	Egy e-akta az elektronikus dokumentumok egy fajtája, amely a hozzájuk kapcsolódó profilokat (metaadatokat), aláírásokat, ellenjegyzéseket és időbélyegeket tartalmaz
Elektronikus aláírás	minősített, vagy fokozott biztonságú aláírás.
Elektronikus bélyegző	minősített, vagy fokozott biztonságú bélyegző
Érintett fél	Természetes vagy jogi személy, aki Minősített bizalmi szolgáltatóval nem kerül szerződéses viszonyba, de annak valamely szolgáltatását vagy valamely szolgáltatás egyes funkcióit jellemzően térítésmentesen igénybe veszi.
Evidencia	Megőrzés szolgáltatásban ez az az adatcsomag, ami az archivált állomány sértetlenségét biztosítja. Az alkalmazott PKI technológia tekintetében az Evidencia maga az aláírás és/vagy időbélyeg, amely a támogatott formátumoknak integráns része.
Export-import folyamat	A megőrzött adat evidenciával közös rendszerbe betöltése, vagy abból kivétele. Az alkalmazott PKI technológia és formátumok tekintetében az Evidencia és a Dokumentum egymástól függetlenül nem létezhet, így a folyamat egyezik a hagyományos fel vagy letöltéssel.
Felülhitelesítés	Megőrzésre átadott dokumentum a hosszútávú megőrzés céljából történő aláírása és/vagy időbélyegzése a megfelelő formátumban. Az alkalmazott PKI technológia és formátumok tekintetében ez jellemzően a hosszú távú archív formátumra (LTA) bővítést jelenti.
Fokozott biztonságú elektronikus aláírás	olyan elektronikus aláírás, amely megfelel az eIDAS rendelet 26 cikkben meghatározott követelményeknek.
Fokozott biztonságú elektronikus bélyegző	olyan elektronikus bélyegző, amely megfelel az eIDAS rendelet 36. cikkben meghatározott követelményeknek.
HSM hardver kriptográfiai eszköz	Olyan hardver alapú biztonságos kriptográfiai eszköz, mely előállítja, tárolja és védi a titkosító és aláíró kulcsokat.
Időbélyegző	„olyan elektronikus adatok, amelyek más elektronikus adatokat egy adott időponthoz kötnek, amivel igazolják, hogy utóbbi adatok léteztek az adott időpontban” (910/2014 eIDAS rendelet 3 cikk 33.)
Kriptográfiai kulcs	Az elektronikus adaton olyan matematikai transzformációt vezérlő egyedi jelsorozat, amelynek ismerete szükséges kódoláshoz és dekódoláshoz.
Magánkulcs	Egy azon aszimmetrikus kulcspár fele, amelyet titokban kell tartani és kizárólag annak gazdája használhatja.

© NOTARchiv Kft.
Minden jog fenntartva. A NOTARchiv Kft. előzetes írásos engedélye nélkül a jelen dokumentum egyetlen része sem reprodukálható, nem továbbítható semmilyen formában és semmilyen esetben, nem tárolható és nem helyezhető el adatbázisokban.

Meghatalmazott	Az ügyfél által írásban szerződéskötéskor vagy köz/magán okiratban meghatalmazott természetes személy.
Minősített elektronikus aláírás	olyan, fokozott biztonságú elektronikus aláírás, amelyet minősített elektronikus aláírást létrehozó eszközzel állítottak elő, és amely elektronikus aláírás minősített tanúsítványán alapul (910/2014 eIDAS rendelet 3 cikk 12.)
Minősített elektronikus bélyegző	olyan, fokozott biztonságú elektronikus bélyegző, amelyet minősített elektronikus bélyegzőt létrehozó eszközzel állítottak elő, és amely elektronikus bélyegző minősített tanúsítványán alapul (910/2014 eIDAS rendelet 3 cikk 27.)
Nyilvános kulcs vagy PKI infrastruktúra	A PKI infrastruktúra minden szereplője két kulccsal rendelkezik: magánkulccsal és nyilvános kulccsal. A magánkulcsát mindenki titkokban tartja, míg a nyilvános kulcsát – például tanúsítvány formájában – nyilvánosságra hozza.
Nyilvános kulcs	A Nyilvános kulcsú infrastruktúrában egy szereplőhöz tartozó aszimmetrikus kriptográfiai kulcspár azon eleme, amelyet nyilvánosságra kell hozni. Jellemzően nyilvánosságra hozatala egy tanúsítvány formájában történik.
Regisztráció	Kezdeti azonosítási eljárás, amelyet a Minősített bizalmi szolgáltató az Előfizető személyazonosságának megállapítására, eljárási joguk ellenőrzésére, valamint adatainak felvételére végez.
Rendkívüli üzemeltetési helyzet	A Minősített bizalmi szolgáltató üzemmenetében zavart okozó rendkívüli helyzet, amikor a Minősített bizalmi szolgáltató normál üzemmenetének folytatására ideiglenesen nincsen lehetőség.
Szervezet	Az archiválás szolgáltatás előfizetője tekintetében: jogi személyek, jogi személyiség nélküli gazdasági társaságok a velük kötött Szolgáltatási szerződés alapján.
Szolgáltatás	Jelen szabályzat keretén belül Minősített bizalmi szolgáltató archiválási szolgáltatásai.
Szolgáltatási Szabályzat	Minősített bizalmi szolgáltató archiválási szolgáltatási tevékenységével kapcsolatos részletes eljárás és további működési szabályokat tartalmazó szabályzat.
Szolgáltatási Szerződés	Megkötése a szolgáltatás igénybevételének előfeltétele. Minősített bizalmi szolgáltató és Ügyfél között létrejött szerződés, amely az archiválási szolgáltatás nyújtására és igénybevételére vonatkozó feltételeket tartalmazza.
Minősített bizalmi szolgáltató	A NOTARchiv Kft.
Tanúsítvány	"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." 2023. évi CIII. törvény 8. § 46.
Ügyfél	A Minősített bizalmi szolgáltatóval szerződésben lévő előfizető.

© NOTARchiv Kft.
Minden jog fenntartva. A NOTARchiv Kft. előzetes írásos engedélye nélkül a jelen dokumentum egyetlen része sem reprodukálható, nem továbbítható semmilyen formában és semmilyen esetben, nem tárolható és nem helyezhető el adatbázisokban.

1.6.2 Rövidítések

eIDAS	electronic Identification, Authentication and Signature (A 910/2014/EU rendelet általánosan használt hivatkozása)
IP	Internet protokoll
IT	Information techology
HSM	Hardwer security modul (Hardver kriptográfiai eszköz)
OID	Objektum azonosító
PKI	Nyilvános kulcsú infrastruktúra

2 Közzététel

2.1 Szolgáltatási információ közzététele

A Minősített bizalmi szolgáltató a minősített archiválási szolgálatatás szerződés feltételei és szabályzatai Minősített bizalmi szolgáltató honlapján elektronikus formában teszi elérhetővé nyilvános hozzáféréssel. Legalább 30 nappal a hatálybalépésük előtt kerülnek kommunikálásra az új vagy módosított dokumentumok. Az érvényben levő dokumentumokon felül a honlapon elérhető a hatályon kívüli dokumentumok valamennyi korábbi verziója is.

2.2 A közzététel időpontja és gyakorisága

Az archiválási rend vonatkozásában az újabb verziójú dokumentumok publikálása a jelen dokumentum „Módosítások” pontjában leírt folyamatnak megfelelően történik. A Minősített bizalmi szolgáltató szükség szerint nyilvánosságra hozza további szabályzatait, a szolgáltatási szerződéskötéshez szükséges feltételeit, illetve azok újabb verziót is. A Minősített bizalmi szolgáltató a rendkívülinek minősített információkat a jogszabályi előírásoknak megfelelően késedelem nélkül teszi közzé.

2.3 Információ hozzáférés biztosítása

Az információk elérése bárki számára biztosított.
Az archiválási szolgáltatási szabályzatok és szerződési feltételek aktuális verziója a Minősített bizalmi szolgáltató ügyfélszolgálati irodájában is megtalálható.

© NOTARchiv Kft.
Minden jog fenntartva. A NOTARchiv Kft. előzetes írásos engedélye nélkül a jelen dokumentum egyetlen része sem reprodukálható, nem továbbítható semmilyen formában és semmilyen esetben, nem tárolható és nem helyezhető el adatbázisokban.

3 Azonosítás és hitelesítés

A Szolgáltatónak ellenőriznie kell az ügyfél adatait megfelelő, megbízható forrás segítségével.

4 Életciklus követelmények - Elektronikus archiválási szolgáltatás

4.1 A szolgáltatás igénylése - Szerződéskötés

A minősített szolgáltatás igénybevétele előtt a leendő Ügyfélnek Szolgáltatási szerződést kell kötniük a NOTARchiv Kft.-vel mint Minősített bizalmi szolgáltatóval továbbá az minősített archiválási Szolgáltatási Szabályzatnak, illetve az abban hivatkozott egyéb szabályzatoknak egyértelműen definiálniuk kell a nyújtandó szolgáltatás részleteit, a szükséges eszközöket az archiválási szolgáltatás igénybevételhez.

4.2 Szolgáltatás nyújtása

4.2.1 Dokumentum befogadása és a visszaigazolás

A Minősített bizalmi szolgáltató kizárólag az Ügyfél személyazonosságának megállapítása és biztonsági eljárás elvégezése után fogadhat be elektronikusan aláírt dokumentumokat. Az eljárásnak biztosítania kell az elektronikusan aláírt dokumentumok integritásának, bizalmasságának megőrzését és az Ügyfél számára történő befogadott elektronikusan aláírt dokumentumainak elérhetőségi szolgáltatás rendelkezésre állását.

A szolgáltatási szabályzatban egyértelműsíteni kell, hogy a Minősített bizalmi szolgáltató milyen fájl formátumokat fogad be, továbbá a fájlokban szereplő az elektronikus aláírásokat és bélyegzőket milyen módon ellenőrzi, és a dokumentumokat milyen feltételekkel fogadja be.

A minősített bizalmi szolgáltató ezt követően 3 napon belül be kell, hogy szerezze a hosszú távú megőrzéshez szükséges adatokat, amennyiben ez nem lehetséges meg kell tagadnia a befogadást.

Dokumentum befogadása esetén a felhasználó részére vissza kell igazolni az alábbi adatokat:

- a befogadás sikeressége vagy sikertelensége
- a befogadás egyedi azonosítója
- a benyújtó azonosítója
- a befogadott fájl neve
- a befogadott fájl SHA256 algoritmussal számított hash lenyomata

Amennyiben a dokumentumról 3 napig nem érkezett visszajelzés, azt sikertelennek kell tekinteni.

4.2.2 Megőrzés, felülhitelesítés

A Minősített bizalmi szolgáltató az archiválásra befogadott fájlokat titkosított formában kell tárolnia. A Minősített bizalmi szolgáltató titkosítás által védi a fájlokat a jogosulatlan hozzáférését. A titkosított dokumentum visszafejtésére kizárólag az elektronikus archiválás szolgáltatás nyújtásához szükséges esetekben, például

- letöltés,
- felülhitelesítés,
- újra-titkosítás esetén kerülhet sor.

© NOTARchiv Kft.
Minden jog fenntartva. A NOTARchiv Kft. előzetes írásos engedélye nélkül a jelen dokumentum egyetlen része sem reprodukálható, nem továbbítható semmilyen formában és semmilyen esetben, nem tárolható és nem helyezhető el adatbázisokban.

4.2.3 Archivált objektum és érvényességi lánc elérhetőségének biztosítása

A Szerződés érvényessége alatt a Minősített bizalmi szolgáltató biztosítsa, hogy az Ügyfél letölthesse az archívumban tárolt elektronikus dokumentumait és az azokhoz tartozó érvényességi láncokat.
- Az Ügyfél csak is biztonságos csatornán keresztül férhet hozzá az archívumában tárolt elektronikus dokumentumokhoz és érvényességi láncokhoz.
- Minden Ügyfél kizárólag azon elektronikus dokumentumokhoz férhet hozzá, amelyekhez valóban jogosult.

4.2.4 Igazolás kibocsátása

A befogadott dokumentumokkal kapcsolatban a Minősített bizalmi szolgáltató az Ügyfél írásos kérésére igazolást állít ki. Megőrzött dokumentum lekérése esetén a dokumentum és a hitelességhez szükséges adatok vagy a befogadási igazolás HTML link segítségével válnak letölthetővé a felhasználó számára. A dokumentumot az Ügyfél a Minősített bizalmi szolgáltató által aláírt igazolás kiadásával együtt is letöltheti a felhasználó, a saját kulcsával titkosított formában.
A Minősített bizalmi szolgáltató az igazolást elektronikus aláírással ellátott elektronikus dokumentumban bocsátja ki az Ügyfél részére. Az alkalmazott megoldás biztosítja, hogy az archiválási igazolás kiállításáért felelős tisztviselők az igazolás kiállítása kapcsán nem ismerhetik meg a dokumentum tartalmát.
Az igazolás kiadását az Ügyfél meghatalmazottja is kérheti, amennyiben ezt megelőzően az Ügyfél elvégezte az erre vonatkozó meghatalmazását.

4.2.5 Dokumentum megjelenítése

A Minősített bizalmi szolgáltató tegye lehetővé az Ügyfél számára, hogy egyeztetett időpontban és helyszínen a Minősített bizalmi szolgáltató szoftver-es és hardver-es eszközein keresztül az Ügyfél megtekinthesse a Minősített bizalmi szolgáltató archívumában lévő befogadott dokumentumait.

4.3 Szolgáltatás elérhetősége

A Szolgáltató a tevékenységét 7/24 kell biztosítsa, a befogadást kivéve, melyet szüneteltethet.
A szolgáltatás esetében biztosítani kell:

- éves szinten a 99%-os rendelkezésre állást
- az egyszeri kimaradás hossza nem haladhatja meg a három napot (NMHH ajánlás)[1]
- a dokumentum befogadását 3 nap alatt fel kell dolgoznia.

A szolgáltatás elérhetősége időben korlátozás mentes, azonban a szolgáltatás túlhasználat esetén a szolgáltatás rendelkezésre állásának védelmében korlátozható.

4.4 A Szerződésmegszűnése

A szolgáltatási szerződés megszűnése esetén Minősített bizalmi szolgáltató tegye lehetővé az Előfizető vagy az arra jogosult más személy részére az Előfizető megbízásából ott tárolt adatállományok letöltését.
A Szolgáltatási szerződés megszűnése után a Minősített bizalmi szolgáltató törölje az archívumból az Előfizetőhöz tartozó adatállományokat.

4.4.1 Dokumentum és érvényességi lánc törlése

Az archiválási szolgálatás által tárolt dokumentumok törlését a szolgáltatási szerződésben foglalt esetekben biztosítani kell. Törlésre csak kivételesen, szerződésben meghatározott esetekben kerül sor.
A Minősített bizalmi szolgáltató a törlés a teljes rendszerén hajtsa végre, a törlés keretében a dokumentum minden mentett példányát semmisítse meg.

© NOTARchiv Kft.
Minden jog fenntartva. A NOTARchiv Kft. előzetes írásos engedélye nélkül a jelen dokumentum egyetlen része sem reprodukálható, nem továbbítható semmilyen formában és semmilyen esetben, nem tárolható és nem helyezhető el adatbázisokban.

A törlésre történő részleteket a Minősített bizalmi szolgáltató a szolgáltatási szabályzatban határozza meg.

© NOTARchiv Kft.
Minden jog fenntartva. A NOTARchiv Kft. előzetes írásos engedélye nélkül a jelen dokumentum egyetlen része sem reprodukálható, nem továbbítható semmilyen formában és semmilyen esetben, nem tárolható és nem helyezhető el adatbázisokban.

5 Fizikai, eljárásbeli és üzemeltetési előírások

A Minősített bizalmi szolgáltatónak széles kiterjedésű szabványoknak megfelelő fizikai, eljárásbeli és személyzeti biztonsági óvintézkedéseket, valamint az ezeket érvényre juttató adminisztratív és irányítási eljárásokat kell alkalmaznia.

Az információbiztonsági szabályozást és vagyonnyilvántartást rendszeres időközönként, vagy ha jelentős változás történik, felül kell vizsgálni, hogy biztosított legyen azok folyamatos alkalmazhatósága, megfelelősége és eredményessége.

A Minősített bizalmi 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 bizalmi szolgáltatónak 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 bizalmi szolgáltató gondoskodjon arról, hogy a kritikus szolgáltatásokhoz történő fizikai hozzáférés ellenőrzött legyen és a kritikus szolgáltatások eszközeit érintő fizikai kockázatát minimalizálja.

A Minősített bizalmi szolgáltató biztosítsa az értékek elvesztésének, sérülésének, és kompromittálódásának, valamint a működési tevékenységek megzavarásának elkerülését.

A Minősített bizalmi szolgáltató óvintézkedéseket valósítson meg annak elkerülése érdekében, hogy az információ és az információ feldolgozó berendezések kompromittálódjanak, illetve eltulajdonításra kerüljenek.

5.1.1 Telephelyek és szerkezeti felépítésük

A telephelyek kiépítése a környezeti biztonság kezelése során Minősített bizalmi szolgáltatónak figyelembe kell venni a tűz és vízvédelemre, a folyamatos elektromos áramellátásra, a légkondicionálásra, a fizikai behatolás megakadályozására, a biztonságos zónák kialakítására és a telekommunikációs hálózatok elérhetőségére és a sugárzás elleni védelemre vonatkozó ajánlásokat és előírásokat.

Az Adatközpont kialakítása során alkalmazott védelmi megoldásokat kell alkalmazni – mint pl. őrzés, biztonsági zárak, behatolás érzékelők, video megfigyelő rendszer, beléptető rendszer stb. – amelyek együttesen egy erős védelmi szintet biztosítanak az elektronikus archívumban tárolt bizalmas adatok megóvására.

5.1.2 A fizikai hozzáférés szabályozása

A Minősített bizalmi szolgáltató biztosítson egy meghatározott és fizikailag lehatárolt biztonsági területet a biztonságos működés kritikus komponensei számára, amelyet a behatolás ellen fizikailag is megvéd, ahova a bejutást ellenőrzi, észleli az illetéktelen behatolást és riasztással is el van látva. Ugyanezen biztonsági területen belül más tevékenységek kizárólag abban az esetben végezhetők, ha a területre belépési jogosultsággal rendelkezők azt el tudják végezni.

A Szolgáltatónak biztosítani kell az alábbiak teljesülését:

• a biztonsági területre történő belépés naplózásra kerül;
• az Adatközpontba legalább két ember a négy szem elvet betartva tartózkodhat;
• indokolt esetben egyéb jogosultsággal rendelkező személyek csak a szükséges ideig tartózkodhatnak a gépteremben megfelelő jogosultságú személyzet kíséretében;
• a belépési napló fájlokat folyamatosan a szolgáltaónak archiválnia kell, melyek heti revízióra kerülnek.

Jogosulatlan személyek jelenlétében:

• az archív dokumentumokat tartalmazó adattároló fizikailag elzárva kell tartani;
• nem szabad felügyelet nélkül hagyni a bejelentkezett munkaállomásokat;

© NOTARchiv Kft.
Minden jog fenntartva. A NOTARchiv Kft. előzetes írásos engedélye nélkül a jelen dokumentum egyetlen része sem reprodukálható, nem továbbítható semmilyen formában és semmilyen esetben, nem tárolható és nem helyezhető el adatbázisokban.

• megfelelő elzárásra kerültek a fizikai adattároló eszközök;
• berendezések és a fizikai védelmet biztosító rendszerek megfelelően működnek;
• a riasztó rendszer aktív riasztási állapotba kerül.

A Minősített bizalmi szolgáltatónak felelősöket kell kijelölnie a fizikai biztonsági vizsgálatok elvégzésére. A Minősített bizalmi szolgáltatónak naplóznia kell a vizsgálatok eredményét.

5.1.3 Áramellátás és légkondicionálás

A Minősített bizalmi szolgáltatónak a kiszolgáló helyszíneire olyan szünetmentes áramellátási eszközöket kell biztosítani, amely megfelelő hatékonyságot nyújt a rendszerek áramellátásához, rövid idejű elektromos áram kimaradás, és akár tartós áramszünet esetén áramtermelő funkció segítségével biztosítja a rendszerek további rendelkezésre állását.

A légkondicionáló rendszer teljesítménye képesnek kell lennie a megfelelő üzemelési hőfokot biztosítani az adatközpont hardverei számára.

5.1.4 Beázás és vízbetörés

A Minősített bizalmi szolgáltató az adatközpont helyszínei beázástól és vízbetörés veszélyétől védenie kell.

5.1.5 Tűz megelőzés és tűzvédelem

A Minősített bizalmi szolgáltató az adatközpont helyszínein az aktuális tűzvédelmi előírásoknak megfelelő eljárással kell védeni. Megfelelő füst- és tűzérzékelőket kell felszerelni, jól látható helyen el kell helyezni a menekülési útvonalat és megfelelő típusú és mennyiségű tűzoltóság által hitelesített kézi tűzoltó készüléket.

Az adatközpontban automatikusan üzemelő tűzoltó rendszert kell alkalmazni.

5.1.6 Adathordozók tárolása

A Minősített bizalmi szolgáltatónak adathordozóit meg kell védenie valamennyi jogosulatlan hozzáféréstől és esetleges megrongálódástól. A napló és archív fájlokat duplikáltan kell létrehozni és tárolni. Egymástól fizikailag elkülönítve kell tárolni, egymástól biztonságos távolságra lévő helyszíneken. A káros környezeti körülményektől a tárolt adathordozókat védeni kell, mint pl. alacsony vagy magas hőmérséklet, szennyeződés, nedvesség, napfény, erős mágneses tér, erős sugárzás stb.

5.1.7 Hulladék megsemmisítése

A mindenkori környezetvédelmi előírások betartásával a Minősített bizalmi szolgáltatónak gondoskodnia kell feleslegessé vált eszközeinek, adathordozóinak selejtezéséről és megsemmisítéséről. A feleslegessé és leselejtezett eszközöket, adathordozókat a Minősített bizalmi szolgáltató munkatársának személyes jelenléte és felügyelete alatt, az elfogadott módszereknek megfelelően kell véglegesen törölni vagy alap funkcióját tekintve használhatatlanná tenni.

5.1.8 A mentési példányok fizikai elkülönítése

Az üzemmenet folytonosság fenntartása és az adatvesztés elkerülése érdekében a Minősített bizalmi szolgáltató rendszerein mentéseket kell eszközölnie, és biztosítania kell szükség esetén való az archiváló rendszer egészének a helyreállíthatóságát. A mentéseket védeni kell a jogosulatlan módosítástól, törléstől, megsemmisüléstől és a jogosulatlan hozzáféréstől esetleges megrongálódástól. A vészhelyzetekre való felkészülés tartalmazza a kidolgozott tervek adott esetekre történő alkalmazását és tesztelését is.

A Minősített bizalmi szolgáltatónak a mentéseket, amely az utolsó teljes mentést is beleértve egy olyan külső helyszínen kell tárolni, amelynek a fizikai és működési védelme azonos az elsődleges helyszínével.

© NOTARchiv Kft.
Minden jog fenntartva. A NOTARchiv Kft. előzetes írásos engedélye nélkül a jelen dokumentum egyetlen része sem reprodukálható, nem továbbítható semmilyen formában és semmilyen esetben, nem tárolható és nem helyezhető el adatbázisokban.

5.2 Eljárásrendi előírások

Az archiválási rendszerek szabályszerű, biztonságos és a meghibásodás minimális kockázati üzemeltetéséről a Minősített bizalmi szolgáltatónak kell gondoskodnia. A biztonságos működés érdekében elegendő számú és megfelelő képzettséggel, műszaki tudással, tapasztalattal rendelkező munkavállalókat kell foglalkoztatnia

A Minősített bizalmi szolgáltató naprakész belső szabályzati és ellenőrzési eljárásrendet kell működtessen. A Minősített bizalmi szolgáltató független rendszervizsgáló ellenőrzési tevékenységgel biztosítja az archiválási rendszer megfelelő működését.

Az archiválási szolgáltatás folyamatában kezelt adatot kockázatelemzés alapján biztonsági osztályba kell sorolni azokat, amely a jogszabályok és a szolgáltatási szabályzatban rögzítettek, és gondoskodnia kell:

megfelelő nyilvántartásáról,
ellenőrzéséről,
védelméről.

5.2.1 Bizalmi szerepkörök

A Minősített bizalmi szolgáltatónak a jogszabályban rögzítettek alapján bizalmi munkakört betöltő személyeket szükséges foglalkoztatnia. Bizalmi pozíciót csak olyan személy tölthet be, akinek a bizalmi munkakör betöltéséhez szükséges

- befolyásmentességét,
- szakértelmét szakmai gyakorlattal,
- végzettséggel és szakképesítéssel tudja igazolni.

Az általánosan felelős munkakört olyan személynek kell betöltenie, aki szakirányú felsőfokú végzettséggel és legalább három év, az informatikai biztonsággal összefüggésben szerzett szakmai gyakorlattal rendelkezik.

A szolgáltatás nyújtó és támogató személy(ek) a szükséges és megfelelően naprakész tudással rendelkeznie.

Bizalmi munkakörök a következők:

-Biztonsági tisztviselő: A szolgáltatás biztonságáért általánosan felelős személy.

-Rendszeradminisztrátor: A Minősített bizalmi szolgáltató informatikai rendszer telepítését, konfigurálását, karbantartását végző személy.

-Általánosan felelős vezető: A Minősített bizalmi szolgáltató informatikai rendszeréért általánosan felelős személy.

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

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

5.2.2 Az egyes feladatokhoz szükséges személyzeti létszámok

A Minősített bizalmi szolgáltatónak a szolgáltatási szabályzatban elő kell írnia, hogy az archiválási szolgáltatás vonatkozásában az elvégzendő műveletek közül melyek azok, amelyek kizárólag két bizalmi munkakört betöltő munkatárs együttes fizikai jelenlétével és/vagy egy fizikailag védett környezetben és/vagy más személyek jelenlétét kizárva végezhető el.

5.2.3 Az egyes szerepkörökhöz elvárt azonosítás és hitelesítés

A Minősített bizalmi szolgáltató az elektronikus informatikai rendszerét kezelő személyzetnek egyedi azonosító adatokkal kell rendelkezzenek, melyek az egyes felhasználók biztonságos azonosítását

© NOTARchiv Kft.
Minden jog fenntartva. A NOTARchiv Kft. előzetes írásos engedélye nélkül a jelen dokumentum egyetlen része sem reprodukálható, nem továbbítható semmilyen formában és semmilyen esetben, nem tárolható és nem helyezhető el adatbázisokban.

és hitelesítését teszi lehetővé. A felhasználók az archív szolgáltatás vonatkozásában a kritikus informatikai rendszerekhez csak azonosítás után férhetnek hozzá. Az azonosító adatokat és felhasználói jogosultságokat munkaviszony megszűnés miatt haladéktalanul vissza kell vonni.

5.2.4 Egymást kizáró szerepkörök

A jogszabályi követelmények megfelelően a Minősített bizalmi szolgáltató egyes munkatársai egyidőben akár több bizalmi szerepkört is betölthetnek, de egyben köteles a Minősített bizalmi szolgáltató biztosítani, hogy:

- a biztonsági tisztviselő 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 bizalmi szolgáltatónak gondoskodni kell arról, hogy szolgáltatások megbízhatóságát munkavállalói és szállítói támogassák. A bizalmi munkakörben foglalkoztatott egyéneknek minden olyan összeférhetetlenségtől menteséget a Minősített bizalmi szolgáltatónak biztosítani kell.

A személyzetnek a biztonsági szabályzatban rögzített eljárásokkal összhangban kell végrehajtani a vezetési és adminisztratív eljárásokat.

Az információbiztonsági szabályzatban dokumentálni kell a biztonsági munkaköröket és felelősségeket munkaköri leírásokban vagy más az érintett felek számára elérhető dokumentációban. A bizalmi munkakörök elvégzéséhez kapcsolódó tevékenységeket világosan definiálni kell,
melyet a vezetésnek és az érintett személynek egyaránt el kell fogadnia.

A munkavállalóknak (egyaránt beletartoznak az állandóan és ideiglenesen alkalmazottak is) olyan munkaköri leírásokkal kell rendelkezni, legkevesebb jogosultság elvéből indulnak ki, ezért a feladatok szétválasztása és az egyes pozíciók bizalmas jellege a feladatok, a hozzáférési szintek, a háttér szűrés és az alkalmazott képzése és tudatossága pontos meghatározása alapján történik.

5.3.1 Képzettségre, gyakorlatra és megbízhatóságra vonatkozó követelmények

A Minősített bizalmi szolgáltató valamennyi alkalmazottjának kell rendelkeznie releváns végzettséggel, gyakorlattal és szakmai tapasztalattal, melyek a betöltött munkakör ellátásához szükséges. Már a toborzás során a leendő dolgozók kiválasztásánál különös hangsúlyt kell fektetni arra, hogy csak megbízható személyek vehetők fel a bizalmi szerepkörbe.

A Minősített bizalmi szolgáltatónál csak olyan személy tölthet be bizalmi szerepkört, akinek a szakértelmét a Minősített bizalmi szolgáltató igazolni tudja.

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

- szakirányú felsőfokú végzettséggel;
- legalább három év, az informatikai biztonsággal összefüggésben szerzett szakmai gyakorlattal.

A Minősített bizalmi szolgáltató bizalmi munkakörben csak büntetlen előélettel rendelkező alkalmazottakat foglalkoztathat, melyet a felvételi eljárás során erkölcsi bizonyítvánnyal igazolni kell.

A Minősített bizalmi szolgáltató bizalmi munkakört betöltő munkatársak befolyásmentességét tudnia kell igazolni.

© NOTARchiv Kft.
Minden jog fenntartva. A NOTARchiv Kft. előzetes írásos engedélye nélkül a jelen dokumentum egyetlen része sem reprodukálható, nem továbbítható semmilyen formában és semmilyen esetben, nem tárolható és nem helyezhető el adatbázisokban.

5.3.2 Biztonsági ellenőrzésre vonatkozó követelmények

A Szolgáltatónak a bizalmi munkakörök betöltéséhez szükséges feltételeket ellenőriznie kell. Az ellenőrzések lefolyását megelőzően nem kaphatnak privilegizált hozzáférést a bizalmi rendszerekhez.

5.3.3 Képzési követelmények

A Minősített bizalmi szolgáltató új belépőit ki kell képezze, amely során elsajátítják az adott munkakör ellátásához szükséges kompetenciát:

- a PKI kriptográfiai alapismereteket;
- biztonsági és adatvédelmi szabályzatot;
- a szerepkörük ellátásához szükséges speciális ismereteket;
- általános fenyegetések az információhitelesítési eljárásokat (beleértve az adathalász és egyéb social engineering taktikákat);
- az egyes tevékenységek jogi következményeit;
- jelen szolgáltatási rend, a szolgáltatási szabályzat és egyéb szabályzatok előírásait;
- az informatikai rendszerének sajátosságait és kezelésének módjait.

A Minősített bizalmi szolgáltató éles informatikai rendszereihez hozzáférési jogosultságot csak a képzést sikeresen abszolváló munkavállalók kapnak.

5.3.4 Továbbképzés gyakorisága

Továbbképzést kell tartani abban az esetben, ha a Minősített bizalmi szolgáltatói rendszereiben a használatot jelentősen megváltozott változás történik.

Egyébként a Szolgáltató legalább 12 havonta tájékoztatja a munkatársait, az elmúlt időszakban megváltozott eljárásokról, szabályokról.

5.3.5 Munkabeosztás körforgása

Nem értelmezett

5.3.6 Felhatalmazás nélküli tevékenységek szankciói

A Minősített bizalmi szolgáltatónak megfelelő fegyelmi eljárásokat kell alkalmazni az archiválást kiszolgáló rendszerének engedélytelen használata vagy a szolgáltatás nyújtása közben esetlegesen elkövetett hibák, mulasztások, károkozások vonatkozásában az előidéző alkalmazottak vagy közreműködő jogi és/vagy természetes személyek esetében. A lehetséges fegyelmi intézkedésről a Minősített bizalmi szolgáltató és az előidéző és/vagy közreműködő jogi és/vagy természetes személyek kötött szerződésben rendelkezni kell.

5.3.7 Szerződéses jogviszonyra vonatkozó követelmények

A Minősített bizalmi szolgáltató által szerződéses viszonyban közreműködő jogi és természetes személyekre ugyanúgy vonatkoznak a szabályzatok és előírások rendelkezései, mint az alkalmazottjaira.

5.3.8 Működést támogató dokumentációk

A dokumentációk, szabályzatok rendelkezésre állását a Minősített bizalmi szolgáltató által folyamatosan biztosítania kell az alkalmazottak irányába a munkakörük ellátásához.

5.4 A biztonsági naplózás folyamatai

A Minősített bizalmi szolgáltatónak az informatikai környezet fenntartása és biztonságos működés érdekében átfogó eseménynaplózó és ellenőrző rendszert kell megvalósítania és üzemeltetnie.

© NOTARchiv Kft.
Minden jog fenntartva. A NOTARchiv Kft. előzetes írásos engedélye nélkül a jelen dokumentum egyetlen része sem reprodukálható, nem továbbítható semmilyen formában és semmilyen esetben, nem tárolható és nem helyezhető el adatbázisokban.

A Minősített bizalmi szolgáltatónak minden lényeges naplóbejegyzést elérhetővé kell tenni a független rendszervizsgálók részére revízió céljából.
Minden naplóbejegyzésnél el kell tárolni esemény vonatkozásában:

- annak időpontját;
- típusát;
- a végrehajtási műveletek sikerességét, illetve sikertelenségét.

A napló fájloknak továbbá el kell tudniuk tárolni felhasználó vagy rendszer azonosítóját, aki/amely az eseményt kiváltotta.

A Minősített bizalmi szolgáltatónak tudnia kell dokumentálnia a naplózott információk elérésének módjait és megőrzési idejét.

Az archiválási szolgáltatás kapcsán naplózni kell a következő eseményeket:

- Archiválásra szánt dokumentumok feltöltésével és a rajtuk elhelyezett aláírások, bélyegzők ellenőrzésével kapcsolatos információkat;
- Dokumentumok felülhitelesítésével kapcsolatos információkat;
- Dokumentumok törlésével kapcsolatos információkat;
- Dokumentumok letöltésével és igazolás-kérések teljesítésével kapcsolatos információkat.

A Minősített bizalmi szolgáltatónak rögzíteni és folyamatosan hozzáférhetővé kell tenni egy meghatározott ideig - a tevékenységének megszűnése utáni időszakban is a lényeges információkat szolgáltatásfolyamatosság biztosítása és a megfelelőségértékelés érdekében.

Amennyiben komoly rendellenesség lép fel a naplózó rendszer működésében, a Minősített bizalmi szolgáltató működését fel kell függeszteni az üzletmenet helyreállításáig.

5.4.1 A tárolt események típusai

Az automatikusan és manuálisan rögzített naplóállományokban az alábbi eseményeket el kell tárolni:

1. Biztonsági események
   a. Rendszer indítása és leállítása,
   b. Biztonsági profil változások,
   c. Tűzfal és router tevékenységek,
   d. Minősített bizalmi szolgáltatói rendszer hozzáférési kísérletek eredménye (sikeres és/vagy sikertelen),
   e. Minősített bizalmi szolgáltatói létesítménybe történő belépések és kilépések.
2. Minősített bizalmi szolgáltatói rendszer beállításai
   a. Rendszer telepítése,
   b. Rendszerkonfiguráció változásai (pl. frissítések, beállítások),
   c. Rendszer vagy rendszeradatok mentése és visszaállítása.
3. Pontos időt érintő események
   a. Óraszinkronizációs események,
   b. Előírt időpontossági küszöb túllépése.
4. Naplózási események
   a. Naplózó rendszer leállítása, újraindítása,
   b. Naplózási beállítás módosítása,
   c. Naplózási adatok archiválása-törlése.
5. Felhasználómenedzsment műveletek
(Minősített bizalmi szolgáltatói rendszerek tekintetében)
   a. Felhasználók felvétele, törlése,

© NOTARchiv Kft.
Minden jog fenntartva. A NOTARchiv Kft. előzetes írásos engedélye nélkül a jelen dokumentum egyetlen része sem reprodukálható, nem továbbítható semmilyen formában és semmilyen esetben, nem tárolható és nem helyezhető el adatbázisokban.

b. Szerepkörök vagy jogosultságok kiosztása, visszavonása,
c. Státuszváltozások (pl. zárolás, tiltás, engedélyezés),
d. Előírt azonosítási módszer beállításai,
e. Hitelesítési adat (pl. jelszó) cseréje.

6. Rendellenes vagy veszélyt jelentő események
   a. Rendszerösszeomlás és a hardver hibák,
   b. Bármilyen szoftverművelet hibája,
   c. Szoftverintegritás hiba,
   d. Hálózati támadási kísérletek,
   e. Elektromos hálózati üzemzavar,
   f. Szünetmentes tápegység hiba,
   g. Kommunikációs üzemzavar.

7.Tanusítány kezelés
   - A tanúsítvány kezelése vonatkozásában minden fontos művelet.

8. HSM
   a. HSM installálása,
   b. HSM eltávolítása,
   c. HSM selejtezése, megsemmisítése,
   d. HSM szállítása,
   e. HSM tartalmának törlése (nullázás),
   f. HSM feltöltése kulcsokkal, tanúsítványokkal.

9. Konfigurációs elem változása a rendszerben
   a. hardver,
   b. szoftver,
   c. operációs rendszer,
   d. javító csomag.

5.4.2 A naplófájlok feldolgozásának gyakorisága

A Minősített bizalmi szolgáltatónak biztosítania kell a keletkezett naplóállományok rendszeres kiértékelését. A naplóállományokban rögzített bejegyzéseket a keletkezésüktől számított legkésőbb 1 héten belül ki kell értékelni a megfelelő szakértelemmel és jogosultságokkal rendelkező Független rendszervizsgálónak.

- A kiértékeléshez szoftvereszközök is igénybe vehetők.
- A kiértékelés során meg kell győződni a vizsgált naplóállományok hitelességéről és sértetlenségéről.
- A kiértékelés során elemezni kell
  - a rendszerek által generált hibaüzeneteket,
  - a forgalmi adatokban bekövetkezett jelentős változásokat,
  - a szokványostól eltérő bármilyen rendkívüli mintákat,
  - gyanús aktivitásokat.

A kiértékelés tényét, eredményeit és az esetlegesen feltárt problémák és kockázatok elhárítása érdekében meghozott intézkedéseket dokumentálni kell.
Az automatikus kiértékelő eljárásoknak riasztani kell a személyzetet a biztonság technikailag kritikusnak tűnő események észlelése esetén.

© NOTARchiv Kft.
Minden jog fenntartva. A NOTARchiv Kft. előzetes írásos engedélye nélkül a jelen dokumentum egyetlen része sem reprodukálható, nem továbbítható semmilyen formában és semmilyen esetben, nem tárolható és nem helyezhető el adatbázisokban.

5.4.3 A naplófájl megőrzési időtartama

A naplófájlok információit legalább 10 évig meg kell őrizni és a független rendszervizsgáló számára bármikor elérhetővé kell tenni a naplókban tárolt információkat.

5.4.4 A naplófájl védelme

A Minősített bizalmi szolgáltatónak gondoskodni kell arról, hogy a naplófájlok, illetve a benne rögzített információk egyszerűen ne legyenek törölhetők vagy megsemmisíthetők.

- A rögzített információk bizalmasságát és integritását kell tartani a megőrzési idő végéig.
- A naplóállományokhoz csak az arra jogosultak – elsősorban a Független rendszervizsgálók – férhessenek hozzá.
- Jogi eljárás esetén az érintett információkat elérhetővé kell tenni az eljárásban érintett és erre feljogosított személyek számára.

5.4.5 A naplófájl mentési eljárásai

A naplóállományokat kiértékelés után 2 példányban, fizikailag elkülönülő helyeken kell tárolni az előírt időpontig.

5.4.6 A naplózás adatgyűjtési rendszere

Nincs előírás.

5.4.7 Az eseményeket kiváltó Ügyfelek értesítése

Nincs előírás.

5.4.8 Sebezhetőség felmérése

A Szolgáltatónak negyedévente sebezhetőség felmérést kell végeznie, évente pedig penetrációs teszteket is végrehajtania.

5.5 Adatok archiválása

A Minősített bizalmi szolgáltató a szolgáltatással kapcsolatosan rendelkezésére álló adatokat - ideértve a személyes adatokat is köteles megőrizni (időtartamot lásd az 5.5.2 fejezetben).

5.5.1 Az archiválandó adatok típusa

A Szolgáltatónak a szolgáltatás rendelkezésére állással kapcsolatos információkat és az ahhoz kapcsolódó személyes adatokat meg kell őriznie. Melyek:

- a szolgáltatás igénylése során beszerzett információkat, dokumentumok;
- a jelen archiválási rend szerint naplózott információk.

5.5.2 Adatok megőrzésének időtartama

A szolgáltatási szabályzatot a hatályon kívül helyezéstől számított 10 évig a Minősített bizalmi szolgáltató köteles megőrizni.

Az egyéb adatokat a keletkezésüktől számított 10 évig a Minősített bizalmi szolgáltató köteles megőrizni.

© NOTARchiv Kft.
Minden jog fenntartva. A NOTARchiv Kft. előzetes írásos engedélye nélkül a jelen dokumentum egyetlen része sem reprodukálható, nem továbbítható semmilyen formában és semmilyen esetben, nem tárolható és nem helyezhető el adatbázisokban.

5.5.3 Az archívum védelme

A Minősített bizalmi szolgáltató köteles valamennyi archivált adatot két példányban egymástól fizikailag elkülönített helyszínen őrizni. Az archivált adatok megőrzése során gondoskodni kell az archivált adatok:

- sértetlenségének megőrzéséről;
- illetéktelen hozzáféréstől;
- rendelkezésre állásáról;
- hitelességének megőrzéséről.

Olyan papír alapú dokumentumokat melyeknek csak egyetlen hiteles példánya létezik, a Minősített bizalmi szolgáltatónak szkennelt és digitálisan aláírt hiteles elektronikus formában rögzíteni és tárolni kell jelen pontban leírt folyamat alapján.

5.5.4 Az archívum mentési folyamatai

A naplófájl mentési eljárásai fejezetben írtak szerint kell eljárni.

5.5.5 Az adatok időbélyegzésére vonatkozó követelmények

Az archivált elektronikus adatokat legalább fokozott biztonságú elektronikus aláírással vagy bélyegzővel és minősített időbélyeggel kell ellátni.

5.5.6 Az archívum gyűjtési rendszere

Nincs előírás.

5.5.7 Archív információk hozzáférését és ellenőrzését végző eljárások

Nincs előírás.

5.6 Kulcscsere

Minősített bizalmi szolgáltatónak le kell cserélnie a hitelesítő kulcsát amennyiben az alkalmazott kulcsai elavulnak.
Az új kulccsal kiállított új tanúsítvány esetében annak profilját és adatait az aktuális előírásokhoz és legjobb gyakorlathoz kell igazítani.

Minősített bizalmi szolgáltatónak le kell cserélnie hitelesítő tanúsítványát amennyiben az lejár.

Továbbá a Szolgáltató saját belátása szerint egyéb esetben is dönthet tanúsítvány és/vagy kulcscsere mellett.

5.7 Katasztrófa helyzet kezelése

A Minősített bizalmi szolgáltatónak megfelelő intézkedéseket kell végrehajtani az archiválási szolgáltatás biztonságát fenyegető kockázatok kezelése érdekében. Figyelembe véve a legújabb technológiai fejleményeket továbbá biztosítania kell, hogy a kockázatok arányosak legyenek a biztonsági szinttel. A biztonsági események megelőzése és azok hatásának minimálárasára intézkedéseket kell tennie, valamint az érdekelteket tájékozgatással kell ellátnia, ha bármely káros esemény éri a Minősített bizalmi szolgáltatót.

A Minősített bizalmi szolgáltatónak késedelem nélkül minden esetben az értesüléstől számított 24 órán belül értesíteni kell a felügyeleti szervet (NMHH-t) és egyes indokolt esetekben más érintett szerveket, például az adatvédelmi hatóságot.

© NOTARchiv Kft.
Minden jog fenntartva. A NOTARchiv Kft. előzetes írásos engedélye nélkül a jelen dokumentum egyetlen része sem reprodukálható, nem továbbítható semmilyen formában és semmilyen esetben, nem tárolható és nem helyezhető el adatbázisokban.

Amennyiben a biztonság megsértése vagy az adatok integritásának sérülése vélelmezhetően hátrányosan érintheti a szerződött ügyfelelét úgy a Minősített bizalmi szolgáltató indokolatlan késedelem nélkül értesítenie kell az Ügyfeleket és egyéb érintetteket.

5.7.1 Váratlan esemény kezelési eljárások

A Minősített bizalmi szolgáltatónak rendelkeznie kell üzletmenet folytonossági tervvel. Ki kell alakítania és fenn kell tartania egy teljes értékű tartalékrendszert, amely az elsődleges helyszíntől biztonságos távolságra, eltérő fizikai helyszínen található és egyenként is alkalmasak az archiválási szolgáltatás egyes funkcióinak kiszolgálására. Rendszeresen tesztelnie kell a Minősített bizalmi szolgáltatónak a redundáns alrendszer működését és évente felül kell vizsgálnia az üzletmenet folytonossági terveit. Katasztrofális esemény bekövetkezte után a lehető leghamarabb helyre kell állítani a szolgáltatások elérhetőségét.

5.7.2 Meghibásodott IT erőforrások és/vagy adatok

A Minősített bizalmi szolgáltató informatikai rendszereit megbízható hardver és szoftver összetevőkből kell kiépíteni. A kritikus funkciókat redundáns rendszerelemek alkalmazásával kell megvalósítani úgy, hogy azok egyes elemei esetleges meghibásodása esetén is képesek legyenek az archív működés kiszolgálására. A Minősített bizalmi szolgáltató naponta készítsen teljes mentést az adatbázisairól és a keletkezett naplózási eseményekről. A Minősített bizalmi szolgáltató olyan gyakorisággal készítsen teljes rendszermentést, amely lehetővé teszi, hogy abból katasztrofális esemény bekövetkezte esetén az archív szolgáltatás teljes egészében helyreállítható legyen. A kritikus rendszerkomponensek meghibásodásának esetén végrehajtandó pontos előírásokat és feladatokat üzletmenet folytonossági terv kell, hogy tartalmazzon. A Minősített bizalmi szolgáltató a hiba elhárítása és a rendszer integritásának helyreállítása után a lehető leggyorsabb időn belül bocsátsa rendelkezésre az archiválási szolgáltatást.

5.7.3 Magánkulcs kompromittálódása esetén követendő eljárás

A Minősített bizalmi szolgáltatói kulcsának kompromittálódása esetén a Minősített bizalmi szolgáltatónak legalább:

- Tájékoztatnia kell az ügyfeleit, az Érintett feleket és a bizalmi felügyeletet.
- Jeleznie kell, hogy az érintett Minősített bizalmi szolgáltatói kulccsal kibocsátott igazolások már nem érvényesek; és
- vissza kell vonni az érintett Minősített bizalmi szolgáltatói tanúsítványt.

Amennyiben bármelyik algoritmus (vagy a kapcsolódó paraméterek) - amiket a Minősített bizalmi szolgáltató vagy a Végfelhasználók alkalmaznak - nem felel meg az elvárásoknak a fennmaradó tervezett felhasználási időtartamra, akkor a Minősített bizalmi szolgáltató köteles:

- Tájékoztatni az Ügyfeleit, az Érintett feleket és a bizalmi felügyeletet; és
- vissza kell vonnia mindegyik érintett tanúsítványt.

5.7.4 Működés folyamatosságának biztosítása

A Minősített bizalmi szolgáltatónak meg kell határozni az üzletmenet folytonossági tervben, hogy a természeti vagy egyéb katasztrófa bekövetkeztében az esetleges szolgáltatás leállás esetén végrehajtandó feladatokat. A katasztrofális esemény bekövetkezése esetén haladéktalanul életbe kell léptetni a rendelkezéseket a szolgáltatások minél előbbi helyreállítása vonatkozásában.

© NOTARchiv Kft.
Minden jog fenntartva. A NOTARchiv Kft. előzetes írásos engedélye nélkül a jelen dokumentum egyetlen része sem reprodukálható, nem továbbítható semmilyen formában és semmilyen esetben, nem tárolható és nem helyezhető el adatbázisokban.

Amennyiben a rendkívüli üzemeltetési helyzet meghaladja a szolgáltatáskiesésre a bizalmi felügyelet ajánlásában[1] megállapított legfeljebb 3 naptári napot, Minősített bizalmi szolgáltatónak értesítenie kell a bizalmi felügyeletet a rendkívüli üzemeltetési helyzettel kapcsolatos alábbi információkról:

- a helyzet kezdete, ha eltér, észlelése időpontja és a helyzet leírása,
- a helyzet hatása (biztonsági esemény esetén az érintett szolgáltatások, informatikai vagyonelemek és az érintett személyes adatok körének leírása, az érintett bizalmi szolgáltatási ügyfelek száma is része kell legyen),
- a helyzet várható időtartama,
- a helyzet elhárítása és jövőbeli elkerülése érdekében tett és tervezett intézkedések, és
- a helyzet megszűnése.

5.8 A szolgáltatás megszűnése

A szolgáltatás megszüntetésekor a Minősített bizalmi szolgáltatónak teljesítenie kell a jogszabályokban megfogalmazott követelményeket:

- A tervezett megszüntetésről a szolgáltatási szabályzatban meghatározott idő előtt értesíti az Ügyfeleket és Hatóságot.
- mindent meg kell tennie annak érdekében, hogy egy erre alkalmas Minősített bizalmi szolgáltató a nyilvántartásait és szolgáltatási kötelezettségeit legkésőbb a szolgáltatás leállításáig átvegye tőle.
- visszavonni a szolgáltatói tanúsítványokat, a hozzájuk tartozó magánkulcsokat meg kell semmisítenie.
- a szolgáltatás leállítása utáni pillanatban egy teljes rendszermentést és archiválást kell végeznie;
- a rendszermentést és az archivált adatokat pedig át kell adnia a szolgáltatást átvevő Szolgáltatónak vagy ha nincs ilyen, a Hatóságnak.

1 Ajánlás elektronikus archiválási szolgáltatások nyújtásához felhasznált megbízható rendszerekre vonatkozó biztonsági követelményekre - http://nmhh.hu/dokumentum/4066/m_kovetelmenyek_v20_080707.pdf

© NOTARchiv Kft.
Minden jog fenntartva. A NOTARchiv Kft. előzetes írásos engedélye nélkül a jelen dokumentum egyetlen része sem reprodukálható, nem továbbítható semmilyen formában és semmilyen esetben, nem tárolható és nem helyezhető el adatbázisokban.

6 Műszaki biztonsági óvintézkedések

A Minősített bizalmi szolgáltató köteles intézkedéseket eszközölni az adathamisítás és az adatlopás ellen; ezért arról kell megbizonyosodnia, hogy az archiválási szolgáltatás nyújtáshoz - a kriptográfiai kulcsok az alkalmazott rendszerekben és termékekben a teljes életciklus alatt megbízhatóak és a módosítás ellen védettek.

6.1 Kulcspár generálás és telepítés

6.1.1 Kulcspár előállítása

Minősített bizalmi szolgáltatónak a Minősített bizalmi szolgáltatói kulcsokat védett módon kell generálni és a magánkulcsok bizalmasságáról gondoskodnia kell.
A Minősített bizalmi szolgáltatói kulcsok generálására vonatkozóan az alábbiakat kell követni:

- A kulcsok generálását fizikailag védett környezetben kell megvalósítania legalább két bizalmi munkakört betöltő személy együttes részvételével. A feljogosított munkatársak számát a minimumon kell tartani és a tevékenységnek a szabályzatokkal összhangban kell zajlani.
- Csak olyan algoritmus és kulcshosszúság használható, amely megfelel a célra vonatkozó szabványoknak, a Hatóság engedélyezett algoritmusokra és minimális kulcsméretekre vonatkozó határozatának.
- Csak olyan kriptográfiai modulok alkalmazhatók, amelyek megfelelnek a Szolgáltató szabályzataiban nyilvánosságra hozott műszaki és egyéb követelményeknek. A kulcsok nem importálhatók olyan eszközökbe, amelyek az alkalmazásra vonatkozó elvárásokat nem teljesítik.
- Az alkalmazott algoritmusokat a Szolgáltatási szabályzatban fel kell tüntetni.
- Minősített bizalmi szolgáltatónak forgatókönyvvel kell rendelkeznie a Minősített bizalmi szolgáltatói kulcsok generálására, aminek legalább a következőket kell tartalmaznia:
    - Részt vevő szerepkörök, akik részt kulcsgenerálásban;
    - Az általuk végrehajtandó feladatok;
    - Felelősségek (eljárás alatt és utána)
    - Szükséges adminisztráció (bizonyítékok előállítása)
- A Szolgáltatónak az eljárás során jegyzőkönyvet kell előállítani, melynek tartalma a forgatókönyvhöz kell igazodjon.

6.1.2 Magánkulcs eljuttatása Végfelhasználóhoz

Nem értelmezett.

6.1.3 A nyilvános kulcs eljuttatása a tanúsítványkibocsátóhoz

Az archiváló rendszer részére előállított kulcspár előállítását követően tanúsítványkérelem jön létre. Ezen kérelem tartalmazza a nyilvános kulcsot és ez alapján zajlik le a tanúsítvány kibocsátása.

6.1.4 A Minősített bizalmi szolgáltatói nyilvános kulcs közzététele

A Minősített bizalmi szolgáltatónak a Minősített bizalmi szolgáltatói nyilvános kulcsot - beleértve az archiválás kulcsot - a Minősített bizalmi szolgáltatói tanúsítványai részeként Interneten elérhetővé kell tennie az érintett felek számára.

6.1.5 Kulcsméretek

A 6.1.1 fejezetben megfogalmazott előírások az irányadók.

6.1.6 A nyilvános kulcs paraméterek előállítása, a minőség ellenőrzése

Nincs előírás.

© NOTARchiv Kft.
Minden jog fenntartva. A NOTARchiv Kft. előzetes írásos engedélye nélkül a jelen dokumentum egyetlen része sem reprodukálható, nem továbbítható semmilyen formában és semmilyen esetben, nem tárolható és nem helyezhető el adatbázisokban.

6.2 A magánkulcsok védelme

6.2.1 Kriptográfiai modulra vonatkozó szabványok és előírások

A Minősített bizalmi szolgáltató rendszerei a magánkulcsokat biztonságos hardver eszközökben kell tárolják, amelyek megfelelnek a következő előírási és szabvány követelményeknek:

- az ISO/IEC 19790 (12),
- vagy FIPS 140-2 (13) level 3-as, illetve magasabb szintű követelmények,
- vagy az MSZ/ISO/IEC 15408 (11) szerint 4-es vagy magasabb biztonsági garancia szinten vannak értékelve.

Minősített bizalmi szolgáltatónak elkülönítve kell kezelni és működtetni a szolgáltatás nyújtásához használt bizalmi szolgáltatást megvalósító termékeit az egyéb tevékenységeihez használt termékektől;

6.2.2 Magánkulcs használata

A Minősített bizalmi szolgáltatónak biztosítania kell, hogy a szolgáltatáshoz használt magánkulcsaival végzett akciók végrehajtásához legalább két bizalmi szerepkört betöltő személy jelenlétére van szükség.

6.2.3 Magánkulcs letétbe helyezése

A Minősített bizalmi szolgáltató az aláíró magánkulcsait nem helyezheti letétbe.

6.2.4 Magánkulcs mentése

A Minősített bizalmi szolgáltatónak másolatokat kell készítenie szolgáltatói magánkulcsokról, ebből minimum egyet a szolgáltatás nyújtás telephelyétől eltérő földrajzi helyszínen kell letárolni. A biztonsági másolatok készítése csak védett környezetben, a bizalmi szerepkört betöltő személyek közül legalább két egyén jelenléte szükséges.

A Minősített bizalmi szolgáltatói magánkulcsok a kriptográfiai eszközön kívül is az eszköz védelmi szintjén kell védeni. A kulcs titkosítása során olyan algoritmust és kulcsméretet kell használni, ami alkalmas arra, hogy annak teljes hátralévő idejében biztosítsa a védelmet.

A Minősített bizalmi szolgáltatónak a nem használt magánkulcs másolatait/részleteit legalább a használt kulccsal azonos szintű biztonsági eljárásokkal kell védenie.

6.2.5 Magánkulcs archiválása

A Minősített bizalmi szolgáltató magánkulcsait nem archiválhatja.

6.2.6 Magánkulcs import és export

A Minősített bizalmi szolgáltató valamennyi magánkulcsát a fenti követelményeknek megfelelő kriptográfiai eszközben kell előállítani. Nyílt formában a magánkulcsok nem létezhetnek a kriptográfiai hardveren kívül. A magánkulcsot a Minősített bizalmi szolgáltató biztonsági másolat készítése céljából exportálhatja a kriptográfiai eszközből.

6.2.7 Magánkulcs tárolása hardware kriptográfiai eszközben

A Minősített bizalmi szolgáltatónak a jelen dokumentum szerinti archiválási szolgáltatás magánkulcsait kriptográfiai modulban kell tárolnia. A magánkulcs tárolására használt cél hardveren belüli nincs előírás a tárolási formára.

© NOTARchiv Kft.
Minden jog fenntartva. A NOTARchiv Kft. előzetes írásos engedélye nélkül a jelen dokumentum egyetlen része sem reprodukálható, nem továbbítható semmilyen formában és semmilyen esetben, nem tárolható és nem helyezhető el adatbázisokban.

6.2.8 Magánkulcs aktiválása

A Minősített bizalmi szolgáltató a magánkulcsait a felhasznált kriptográfiai eszközön a tanúsítási dokumentumokban megfogalmazott eljárásoknak és a felhasználói útmutatójában leírtak alapján kell aktiválni, legalább két bizalmi munkakört betöltő személy részvételével.

6.2.9 Magánkulcs deaktiválása

Nincs előírás

6.2.10 Magánkulcs megsemmisítése

A használatból lejárt érvényességű, funkcióját vesztett és kivezetett magánkulcsait meg kell semmisíteni, hogy lehetetlenné tegye a magánkulcs további használatát. A megsemmisítést a kriptográfiai hardver felhasználói útmutatójában leírt eljárásoknak megfelelően kell elvégezni. A magánkulcsról készült minden mentett példányt dokumentált módon visszaállíthatatlanná kell tenni vagy meg kell semmisíteni.

6.2.11 Kriptográfiai modulok értékelése

Lásd a Kriptográfiai modulra vonatkozó szabványok és előírások fejezetet.

6.3 Kulcspárkezelés szempontjai

A Minősített bizalmi szolgáltató köteles a törvényi előírásoknak megfelelően használni és kezelni Minősített bizalmi szolgáltatói kulcsait, különös tekintettel az alábbiakra:

- Minősített bizalmi szolgáltató saját Minősített bizalmi szolgáltatói kulcsait nem használhatja a Minősített bizalmi szolgáltatói tanúsítványok érvénytelensége esetén vagy a kulcspár használati idején túl.
- az Ügyfelek részére kibocsátott igazolások és értesítések hitelesítésére, valamint az archiválásra befogadott állományok felülhitelesítéséhez használtkulcsok nem használhatók semmilyen más célra.

6.4 Aktivizáló adatok

6.4.1 Aktivizáló adatok előállítása és alkalmazása

A Minősített bizalmi szolgáltató az általa használt kriptográfiai eszközök felhasználói útmutatójában megadott módon kell az aktiváló módszereket alkalmaznia a magánkulcsainak megvédésére. Amennyiben az aktivizáló adat jelszó, annak kellően hosszúnak kell lennie.

6.4.2 Az aktivizáló adatok védelme

A Minősített bizalmi szolgáltató által foglalkoztatott munkavállaóknak a kulcsok aktiválásához szükséges eszközöket, adatokat biztonságosan kell tárolniuk. Jelszavak csak kódolt formában tárolhatók.

6.5 Informatikai biztonsági előírások

6.5.1 Speciális informatikai biztonsági műszaki követelmények

A Minősített bizalmi szolgáltató informatikai rendszereinek az következő követelmények teljesülését kell biztosítani konfigurálás és üzemeltetés során:

© NOTARchiv Kft.
Minden jog fenntartva. A NOTARchiv Kft. előzetes írásos engedélye nélkül a jelen dokumentum egyetlen része sem reprodukálható, nem továbbítható semmilyen formában és semmilyen esetben, nem tárolható és nem helyezhető el adatbázisokban.

• a rendszerhez való hozzáférés engedélyezése előtt a felhasználó azonosságát ellenőrizni kell;
• különböző felhasználókhoz különböző szerepköröket kell párosítani.
• minden felhasználó csak a szerepkörének megfelelő jogosultságokkal rendelkezzen;
• minden tranzakcióról naplóbejegyzést kell előállítani és azokat archiválni kell;
• biztosítani kell, hogy kellően védettek legyenek a jogosulatlan hozzáféréstől a Minősített bizalmi szolgáltató belső hálózata;
• olyan eljárásokat kell alkalmazni, amely megfelelően tud reagálni a kulcsvesztés vagy rendszerhiba után a szolgáltatás visszaállítása érdekében.

6.5.2 Az informatikai biztonság ellenőrzése

Az adat biztonság és a minőségi szolgáltatás biztosítása érdekében a Minősített bizalmi szolgáltató nemzetközileg elfogadott szabványok és módszertanok alapján felépített minőség irányítási rendszert kell alkalmazzon, ezek megfelelőségét független tanúsító szervezet által kiállított tanúsítvánnyal kell igazolnia.

6.6 Életciklusra vonatkozó műszaki előírások

6.6.1 Rendszerfejlesztési előírások

A Minősített bizalmi szolgáltató az éles szolgáltatást nyújtó elsődleges rendszereiben csak olyan eszközöket, alkalmazásokat használhat, amelyek:

- „dobozos szoftverek” melyeket dokumentáltan terveztek és fejlesztettek ki;
- a Minősített bizalmi szolgáltató részére megbízható fél által kifejlesztett egyedi hardver és szoftver megoldások, amelyek létrehozásánál ellenőrzött fejlesztési környezetet használtak;
- olyan nyílt forráskódú szoftverek, amelyek teljesítik a biztonsági követelményeket. A szolgáltatás nyújtásához használt hardver és szoftver komponensek csak Minősített bizalmi szolgáltató által biztosított archiválási szolgáltatásra használhatók.

A Minősített bizalmi szolgáltató különböző védelmi intézkedésekkel megakadályozza, hogy kártékony szoftver juthasson be az archív szolgáltatás körében használt eszközökre. A Minősített bizalmi szolgáltatónak ugyanolyan gondossággal kell eljárnia a programfrissítések vásárlása vagy fejlesztése vonatkozásában, mint az első verzió beszerzésekor.

Megbízható és megfelelő szaktudással rendelkezőknek kell kivitelezni a szoftverek és eszközök telepítését. A Minősített bizalmi szolgáltató csak a szolgáltatás nyújtása vonatkozásában telepítheti a szoftvereket az informatikai berendezéseire. A Minősített bizalmi szolgáltató egy változáskövető rendszerben minden változást dokumentálni kell. A Minősített bizalmi szolgáltató alkalmazzon olyan eljárásokat melyek a jogosulatlan változás észlelésére szakosodott.

6.6.2 Biztonságkezelési eljárások

A Minősített bizalmi szolgáltatónak rendelkezni kell olyan dokumentált információkkal, amelyekben rögzítve vannak a szolgáltatásban használt:

- rendszerek telepítése,
- konfigurációk és specifikációk,
- üzemeltetése,
- ellenőrzése, monitorozása és karbantartása,
- beleértve a módosításokat és továbbfejlesztéseket is.

A változáskövető funkciónak észlelnie kell a szolgáltatást nyújtó rendszerben történt bármilyen jogosulatlan hozzáférést, adatbevitelt, amely érinti a szolgáltatásban használt rendszer szoftveres és hardveres összetevőket. A Minősített bizalmi szolgáltató rendszereiben használt programok integritását Minősített bizalmi szolgáltatónak rendszeresen ellenőrizze kell.

© NOTARchiv Kft.
Minden jog fenntartva. A NOTARchiv Kft. előzetes írásos engedélye nélkül a jelen dokumentum egyetlen része sem reprodukálható, nem továbbítható semmilyen formában és semmilyen esetben, nem tárolható és nem helyezhető el adatbázisokban.

6.7 Életciklusra vonatkozó biztonsági előírások

A Minősített bizalmi szolgáltatónak gondoskodnia kell a felhasznált kriptográfiai eszközök védelméről azok teljes életciklusa alatt.

- Megfelelő tanúsítással rendelkező HSM-et kell használnia.
- A HSM átvételekor meg kell róla győződni, hogy a szállítás során biztosították az eszközök feltörés elleni védelmét.
- A tárolás során biztosítani kell a HSM feltörés elleni védelmét.
- Az üzemeltetés során folyamatosan be kell tartani a HSM, használati útmutatójában és a tanúsítási dokumentációban szereplő követelményeket.
- A Minősített bizalmi szolgáltatónak a használatból kivont HSM eszközökben tárolt magánkulcsokat visszaállíthatatlanul kell törölnie.

6.8 Hálózati biztonsági előírások

Az alkalmazott IT rendszereinek konfigurációját, minden változást, beleértve a legkisebb módosítást, fejlesztést, szoftverfrissítést is dokumentáljon a Minősített bizalmi szolgáltató. Az informatikai rendszereiben a Minősített bizalmi szolgáltató vezessen be megfelelő eljárásokat a bekövetkezett hardver vagy szoftver változás monitorizálás vonatkozásában. Minden szoftverkomponens első integrálásakor a Minősített bizalmi szolgáltató ellenőrizze eredetiségét. A Minősített bizalmi szolgáltató alkalmazzon megfelelő hálózatbiztonsági intézkedéseket, mint például

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

A Minősített bizalmi szolgáltatónak sérülékenységvizsgálatot kell végeznie vagy végeztetnie a használatos nyilvános és privát IP címein és évente penetrációs tesztet kell végeztetnie a rendszerén.

© NOTARchiv Kft.
Minden jog fenntartva. A NOTARchiv Kft. előzetes írásos engedélye nélkül a jelen dokumentum egyetlen része sem reprodukálható, nem továbbítható semmilyen formában és semmilyen esetben, nem tárolható és nem helyezhető el adatbázisokban.

7 Tanúsítvány profil

A szolgáltatási szabályzatnak tartalmaznia kell a Minősített bizalmi szolgáltatói tanúsítvány tanúsítványprofilját.

8 A megfelelőség vizsgálata

A Minősített bizalmi szolgáltató tevékenységét az Európai Uniós szabályozással összhangban a Hatóság felügyeli. A Hatóság évente legalább egyszer átfogó helyszíni ellenőrzést tart a Minősített bizalmi szolgáltató telephelyein. A Minősített bizalmi szolgáltató köteles külső auditori szolgáltatás igénybevételével átvilágíttatnia az üzemeltetését és az auditálásról készült jelentést a Hatóságnak benyújtani kézhez vétel után legfeljebb három nappal.

Az átvizsgálás során megállapításra kell kerülnie, hogy a Minősített bizalmi szolgáltató működése megfelel-e az eIDAS Rendeletben (1) és a vonatkozó magyar jogszabályokban rögzített elvárásoknak, valamint az alkalmazott archiválási rendben és az archiválási szolgáltatási szabályzatban támasztott követelményeknek egyaránt.

Az átvilágítás 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;
- ETSI EN 319 401 V2.3.1 (2021-05); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
- ETSI TS 119 511 V1.1.1 (2019-06); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques

A vizsgálati eredmény bizalmas dokumentum, csak az arra jogosultak számára hozzáférhető. A megfelelőségi tanúsítványt közzé kell tenni a Minősített bizalmi szolgáltató honlapján. A Minősített bizalmi szolgáltató fenntartja a jogot, hogy tetszőleges időpontban független szakértő bevonásával átvizsgálja a követelmények betartásának ellenőrzése érdekében a jelen archiválási rend alapján.

8.1 Az ellenőrzések gyakorisága

A megfelelőség vizsgálatot a Minősített bizalmi szolgáltató évente köteles elvégeztetni.

8.2 Az auditorral szembeni elvárások

A Minősített bizalmi szolgáltató a belső auditokat elvégezheti a független rendszervizsgáló biztonsági besorolással felruházott alkalmazott segítségével. Az EU akkreditációs szervezete által felhatalmazott szervezet végezheti el az eIDAS követelményeknek való megfelelőséget.

8.3 Az auditor és az auditált függetlensége

A külső auditot csak olyan egyén végezheti el, amely:

- aki független a Minősített bizalmi szolgáltató tulajdonosi körétől, vezetőségétől és üzemeltetésétől;
- aki független a vizsgált szervezettől, vagyis nincs munkaviszonyban vagy üzleti kapcsolatban a Minősített bizalmi szolgáltatóval;

© NOTARchiv Kft.
Minden jog fenntartva. A NOTARchiv Kft. előzetes írásos engedélye nélkül a jelen dokumentum egyetlen része sem reprodukálható, nem továbbítható semmilyen formában és semmilyen esetben, nem tárolható és nem helyezhető el adatbázisokban.

8.4 A vizsgálat által érintett területek

Az átvizsgálásnak az az alábbi pontokat kell hatálya alá venni:

- hatályos jogszabályoknak való megfelelés;
- műszaki szabványoknak való megfelelés;
- archiválási rendnek és archiválási szolgáltatási szabályzatnak való megfelelés;
- a folyamatok megfelelősége;
- a dokumentálás;
- a fizikai biztonság;
- a személyi állomány megfelelősége;
- az Információ biztonság és adatvédelmi szabályok betartása.

8.5 A hiányosságok kezelése

A külső megfelelőségértékelések eredményét egy értékelésjelentésben kell összefoglalni. A jelentésben – amennyiben vannak – rögzíteni kell a vizsgálat során feltárt eltéréseket és az elhárításukra kitűzött határidőket.

8.6 Az eredmények közzététele

A Minősített bizalmi szolgáltató nem köteles a belső megfelelőségértékelési jelentés publikálására, az abban foglaltakat bizalmas információként kezelheti.
A Minősített bizalmi szolgáltatónak az auditidőszakot követő három 3 hónapon belül nyilvánosságra kell hoznia a külső megfelelőségértékelési jelentést. A Minősített bizalmi szolgáltató nem köteles nyilvánosságra hozni az auditjelentés azon általános megállapításait, melyek nincsenek hatással az audit eredményére.
A Minősített bizalmi szolgáltató a megfelelőségértékelés eredményét 3 munkanapon megküldi a Bizalmi Felügyeletnek.

© NOTARchiv Kft.
Minden jog fenntartva. A NOTARchiv Kft. előzetes írásos engedélye nélkül a jelen dokumentum egyetlen része sem reprodukálható, nem továbbítható semmilyen formában és semmilyen esetben, nem tárolható és nem helyezhető el adatbázisokban.

9 Egyéb üzleti és jogi kérdések

9.1 Díjak

A Minősített bizalmi szolgáltató a díjakat a honlapján nyilvánosan köteles közzé tenni.

9.1.1 Archiválás szolgáltatás díjai

A Minősített bizalmi szolgáltató a nyilvános árlista alapján számíthat fel díjat, illetve attól előzetes egyeztetés alapján eltérhet.

9.1.2 Visszatérítési politika

Nincs megkötés.

9.2 Pénzügyi felelősség

A Minősített bizalmi szolgáltató a mindenkor hatályos polgári törvénykönyvben meghatározott szerződésszegésért való felelősség szabályai szerint, s a mindenkor hatályos bizalmi szolgáltatásokra és ezek Minősített bizalmi szolgáltatóira vonatkozó részletes követelményekről szóló rendeletben meghatározott mértékig; s a szolgáltatási szabályzatában, általános szerződéses feltételeiben foglaltaknak megfelelően felel a szolgáltatásaival okozott károkért.
A Szolgáltató korlátozhatja a felelősségvállalása értékét, az ügyfeleket és érintett feleket a weboldalán keresztül tájékoztatva.

9.2.1 Biztosítási fedezet

A Minősített bizalmi szolgáltató köteles felelősségbiztosítással rendelkezni.
A felelősségbiztosításnak ki kell terjedni a Szolgáltató által nyújtott bizalmi szolgáltatásokkal összefüggésben okozott károkra és költségekre:

- az ügyfélnek a szerződés megszegésével összefüggésben okozott károkra,
- az ügyfélnek és harmadik személynek szerződésen kívüli okozott károkra,
- a DÁP.-ben foglalt kötelezettségek nem teljesítése miatt a bizalmi felügyeletnél felmerült, a DÁP szerinti költségekre, és
- az eIDAS Rendelet vonatkozó rendelkezései alapján a bizalmi felügyelet által felkért megfelelőségértékelő szervek eljárásának költségeire, ha azt a bizalmi felügyelet eljárási költségként érvényesíti.

A biztosítási szerződésben szereplő felelősségvállalási érték káreseményenként nem lehet alacsonyabb, mint 3 000 000 (hárommillió) forint.

A Szolgáltatónak biztosítania kell, hogy az általa kötött biztosítási szerződés kifejezetten nevesítse, hogy a szerződés kiterjed a fentiekre.

9.2.2 Egyéb eszközök

A Minősített bizalmi szolgáltató a szolgáltatás megszűnésével kapcsolatos költségek biztosítása és a megbízhatóság garantálása érdekében kell rendelkezzen.

- legalább 25 000 000 (huszonötmillió) forint összegű, feltétel nélküli és visszavonhatatlan bankgaranciával kell rendelkeznie VAGY
- pénzügyi intézménynél óvadékot kell alapítania legalább 25 000 000 (huszonötmillió) forint értékben VAGY

© NOTARchiv Kft.
Minden jog fenntartva. A NOTARchiv Kft. előzetes írásos engedélye nélkül a jelen dokumentum egyetlen része sem reprodukálható, nem továbbítható semmilyen formában és semmilyen esetben, nem tárolható és nem helyezhető el adatbázisokban.

- Egy legalább 100 000 000 (százmillió) forint jegyzett tőkéjű, az Európai Gazdasági Térségben letelepedett vállalkozás készfizető kezességével kell rendelkeznie legalább 25 000 000 (huszonötmillió) forintig terjedően.

9.2.3 Az Érintett felek számára elérhető biztosítások és garanciák

A Minősített bizalmi szolgáltató tegye közzé, hogy az általa nyújtott garanciák és biztosítások mennyiben terjednek ki más felek által okozott károkra.

9.3 Bizalmasság, adatvédelem

A Minősített bizalmi szolgáltatónak az Ügyfél által rendelkezésre bocsájtott adatokat a mindenkori jogszabályoknak megfelelően kell kezelni.

9.3.1 Bizalmas információk köre

A Minősített bizalmi szolgáltatónak az archiválás szolgáltatási szabályzatában pontosan meg kell határoznia, hogy mely adatok minősülnek bizalmas információnak.

9.3.2 Bizalmas információk körén kívül eső adatok

A Minősített bizalmi szolgáltató miden olyan adatot nyilvánosnak tekinthet, melyek nem szerepelnek az archiválási szolgáltatási szabályzat bizalmas adatok felsorolása alatt.

9.3.3 Bizalmas információk védelme

A Minősített bizalmi szolgáltató szerződésbe foglalva vagy titoktartási nyilatkozat aláírásával kell, hogy kötelezze munkavállalóit és szerződött partnereit a bizalmas adatok védelmére. A szolgáltatási szabályzatában meg kell határozni tételesen azon eseteket, amikor a Minősített bizalmi szolgáltató a bizalmas adatokat felfedheti.

9.4 Személyes adatok védelme

A Minősített bizalmi szolgáltatónak az általa kezelt személyes adatok védelméről gondoskodnia kell. Szabályzatainak meg kell felelniük az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (3) és az EU általános adatvédelmi rendelet (GDPR) (2) rendelkezéseinek.
A Minősített bizalmi szolgáltató köteles a nyilvántartott személyes adatokat a jogszabályi előírásoknak megfelelően

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

9.4.1 Adatkezelési tájékoztató

A Minősített bizalmi szolgáltató rendelkeznie kell adatkezelési tájékoztatóval, amelyben részletesen leírja személyes adatok kezeséi folyamatát.

9.4.2 Személyes adatok

A Minősített bizalmi szolgáltató csak közvetlenül az Ügyfelektől, vagy annak előzetes belegyezésével gyűjthet személyes adatokat, ami kimondottan a szolgáltatás nyújtásához szükséges.

Minősített bizalmi szolgáltatónak személyes adatként kell kezelnie minden olyan birtokába kerülő adatot, amely adatok:

- alapján természetes személy beazonosíthatók, vagy

© NOTARchiv Kft.
Minden jog fenntartva. A NOTARchiv Kft. előzetes írásos engedélye nélkül a jelen dokumentum egyetlen része sem reprodukálható, nem továbbítható semmilyen formában és semmilyen esetben, nem tárolható és nem helyezhető el adatbázisokban.

- természetes személlyel kapcsolatba hozhatók, vagy
- adatokból természetes személyre vonatkozó következtetés levonható, és
- nem sorolható egyúttal a személyes adatnak nem minősülő adattá.

9.4.3 Személyes adatnak nem minősülő adatok

A Minősített bizalmi szolgáltató az előző ponton kívül eső adatokat nem tekinti személyes adatnak.

9.4.4 Személyes adatok védelme

Az Minősített bizalmi szolgáltató az adatokat megfelelő intézkedésekkel védenie kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, valamint nyilvánosságra hozatal vonatkozásában. Az Adatkezelési tájékoztatóban leírtak betartásáért a Minősített bizalmi szolgáltató felelőssége, amely egyaránt kiterjed a szállítói által végzett tevékenységekre.

9.4.5 Személyes adatok felhasználása

A Minősített bizalmi szolgáltató csak a szolgáltatás nyújtásához a kapcsolattartás célból használhatja fel az Ügyfél személyes adatait.

9.4.6 Adatkezelés

A Minősített bizalmi szolgáltató értesítése nélkül az Ügyfélről tárolt személyes adatokat csak a vonatkozó jogszabályok által meghatározott esetekben adhat ki (pl: Hatóság irányába).

9.4.7 Egyéb adatvédelmi követelmények

Nincs előírás.

9.5 Szellemi tulajdonjogok

A Minősített bizalmi szolgáltató által befogadott elektronikus állományok tulajdonosa az Ügyfél. A szolgáltatás nyújtásához rendelkezésre bocsátott szoftver és/vagy hardver eszközök tulajdonosa a Minősített bizalmi szolgáltató.

A jelen dokumentum és a kapcsolódó alacsonyabb szintű szabályozás a Minősített bizalmi szolgáltató kizárólagos tulajdonát képezi. Az Ügyfelek és egyéb Érintett felek a dokumentumokat csak a jelen archiválási rend előírásainak megfelelően jogosultak felhasználni, minden egyéb célú felhasználás tilos. Az archiválási rend, mint dokumentum változtatás nélkül szabadon terjeszthető.

A Minősített bizalmi szolgáltató által az igénybevételéhez biztosított szoftverek használatának szabályait az archiválási szolgáltatási szabályzatban kell meghatározni.

9.6 Felelősség és helytállás

9.6.1 A Minősített bizalmi szolgáltató felelőssége és helytállása

A Minősített bizalmi szolgáltató az Ügyféllel kötött Szolgáltatási szerződésben megfogalmazott valamennyi rá vonatkozó kötelezettség betartásáért, a következő esetekben:

- a Minősített bizalmi szolgáltató sajátjaként felel az alvállalkozói által a szolgáltatás nyújtása során okozott károkért;
- a Minősített bizalmi szolgáltató felelősséget vállal az általa támogatott archiválási rendben leírt eljárásoknak való megfelelésért;
- a Minősített bizalmi szolgáltató a vele szerződéses jogviszonyban álló Ügyfelekkel szemben a Ptk. (4) a szerződésszegésért való felelősség szabályai szerint felelős;
- a Minősített bizalmi szolgáltató a vele szerződéses jogviszonyban nem álló harmadik személlyel (ilyen az Érintett fél) szemben a Ptk. (4) általános felelősségi szabálya szerint felelős;

© NOTARchiv Kft.
Minden jog fenntartva. A NOTARchiv Kft. előzetes írásos engedélye nélkül a jelen dokumentum egyetlen része sem reprodukálható, nem továbbítható semmilyen formában és semmilyen esetben, nem tárolható és nem helyezhető el adatbázisokban.

9.6.2 Az ügyfél felelőssége és helytállása

Az Ügyfél felelősségét a Szerződés és annak mellékletei (köztük az Általános szerződési feltételek) határozzák meg.

Az Ügyfél köteles a Minősített bizalmi szolgáltató szerződéses feltételeinek és szabályzatainak megfelelően eljárni a szolgáltatás igénybevétele során.

Az Ügyfél kötelezettségeit a jelen archiválási rend, a Szolgáltatási szerződés és annak mellékletei – különösen az Általános szerződési feltételek – és a szolgáltatási szabályzat és kivonata közösen írja le.

9.6.3 Az érintett fél felelőssége

Nincs előírás.

9.6.4 Egyéb szereplők tevékenységéért viselt felelősség és helytállás

Nincs előírás.

9.7 A helytállás érvénytelenségi köre

A Minősített bizalmi szolgáltató kizárja felelősségét, amennyiben:

- az Internet, vagy annak egy részének működési hibájából adódóan a kommunikációs kötelezettségeit nem tudja ellátni;
- a Hatóság algoritmusokkal kapcsolatos határozat által elfogadott kriptográfiai algoritmusok hibájából származtatható.

9.8 A felelősség korlátozása

Nincs megkötés

9.9 Kártérítési kötelezettség

9.9.1 A Minősített bizalmi szolgáltató kártérítési kötelezettsége.

A Minősített bizalmi szolgáltató kártérítési kötelezettségének részleteit a Szolgáltatási szabályzat, az Általános szerződési feltételek és/vagy az Ügyfelekkel kötött szolgáltatási szerződések tartalmazzák.

9.10 Érvényesség és megszűnés

9.10.1 Érvényesség

Az archiválási rend adott verziója hatálybalépésének napja jelen dokumentum fedőlapján kerül eltüntetésre.

9.10.2 Megszűnés

Az archiválási rend hatálya megszűnik egy új verzió hatályba lépésével, vagy a tevékenység megszűnésével.

9.10.3 A megszűnés következményei

Az archiválási rend visszavonása esetén a Minősített bizalmi szolgáltató honlapján közzéteszi a visszavonás részletes szabályait és egyéb kötelezettségeket.

9.11 A felek közötti kommunikáció

A Minősített bizalmi szolgáltató az Ügyfelekkel történő kapcsolattartás érdekében működtessen ügyfélszolgálati irodát.

© NOTARchiv Kft.
Minden jog fenntartva. A NOTARchiv Kft. előzetes írásos engedélye nélkül a jelen dokumentum egyetlen része sem reprodukálható, nem továbbítható semmilyen formában és semmilyen esetben, nem tárolható és nem helyezhető el adatbázisokban.

9.12 Módosítások

A Minősített bizalmi szolgáltató fenntartja magának a jogot, hogy a biztonsági követelmények, irányadó szabályok, piaci környezet vagy egyéb körülmények változása vonatkozásában szabályozott keretek között megváltoztathatja az archiválási rendet.

9.12.1 Módosítási eljárás

A Minősített bizalmi szolgáltató évente, illetve változtatás esetén soron kívül átvizsgálja az archiválási rendet és elvégzi a változtatásokat. A dokumentum változtatás után is új verziószámot kap és az elfogadási procedúra alapján a dokumentum tervezett hatálybalépési időpontja is meghatározásra kerül.

A módosított szabályzat tervezetett legalább 30 nappal a tervezett hatálybalépés előtt meg kell küldeni a Hatóság részére és a Minősített bizalmi szolgáltatónak a honlapján nyilvánosságra kell hoznia azt.

A változások bejelentését felügyelet weboldalán közzétett űrlapon, a 470/2017. Korm. rendeletben foglaltak szerint kell megtennie. Az űrlaphoz csatolni kell

- a módosított és jóváhagyott új Szolgáltatási Rend verziót;
- a módosított és jóváhagyott új Szabályzat verziót;
- a módosított és jóváhagyott új Szabályzatkivonat verziót;

valamint a 470/2017. Korm. rendeletben meghatározott egyéb iratokat és dokumentumokat.

9.12.2 Értesítések módja és határideje

A Minősített bizalmi szolgáltató a „Módosítási eljárás” pontban leírtak szerint értesíti az Érintett feleket az új dokumentum verziók kibocsátásáról.

9.12.3 A hitelesítési rend azonosítójának megváltoztatása

A Minősített bizalmi szolgáltató az archiválási rend legkisebb változtatása esetén is új verziószámot ad ki, ami része a dokumentum azonosítónak.
Minősített bizalmi szolgáltatónak a archiválási Rend és szolgáltatási szabályzat újabb nyilvános változatait, beleértve a tervezeteket is új verziószámmal kell nyilvánosságra hoznia

A dokumentum azonosítója a következő elemekből épül fel – az egyes elemeket pontok választják el egymástól:

- Minősített bizalmi szolgáltatói OID (1.3.6.1.4.1.54136),
- archiválás szolgáltatás,
- dokumentumok,
- nyilvános dokumentum,
- belső dokumentum,
- dokumentumok egyedi azonosító sorszáma,
- dokumentumok verziója,
- dokumentumok alverziója.

Szolgáltatási rend esetén:

1.3.6.1.4.1.54136.1.1.1.1.x.x[2];

Szolgáltatási szabályzat esetén:

[2] Az OID azonosító utolsó két x-el jelölt karaktere az aktuálisan hatályban lévő Minősített archiválási rend és Minősített szolgáltatási szabályzat verzió számait jelzik

© NOTARchiv Kft.
Minden jog fenntartva. A NOTARchiv Kft. előzetes írásos engedélye nélkül a jelen dokumentum egyetlen része sem reprodukálható, nem továbbítható semmilyen formában és semmilyen esetben, nem tárolható és nem helyezhető el adatbázisokban.

1.3.6.1.4.1. 54136.1.1.1.2.x.x[3]

Egy módosított rend vagy szabályzat csak a hatálybalépését követően végzett szolgáltatásokra vonatkozhat.

9.13 Vitás kérdések rendezése

A működése során a Minősített bizalmi szolgáltató felmerülő vitás kérdések békés rendezésére törekszik.

9.14 Irányadó jog

A Minősített bizalmi szolgáltató tevékenységét a mindenkori hatályos jogszabályoknak megfelelően végzi.

A Minősített bizalmi szolgáltató szerződéseire és szabályzataira, azok teljesítésére a magyar jog az irányadó, s azok a magyar jog szerint értelmezendők.

9.15 Az érvényben lévő jogszabályoknak való megfelelés

A jelen archiválási rend megfelel az alábbi jogszabályoknak:

- AZ EURÓPAI PARLAMENT ÉS A TANÁCS 910/2014/EU RENDELETE (2014. július 23.) valamint az 1999/93/EK irányelv hatályon kívül helyezéséről (1);
- 2011. évi CXII. törvény az információs önrendelkezési jogról (3);
- 2013. évi V. törvény a Polgári Törvénykönyvről (4).
- 2023. évi CIII. törvény a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól (DÁP) (5);
- 24/2016. (VI. 30.) BM rendelet a bizalmi szolgáltatásokra és ezek Minősített bizalmi szolgáltatóira vonatkozó részletes követelményekről (6);
- 25/2016. (VI. 30.) BM rendelet a bizalmi felügyeletnek fizetendő igazgatási szolgáltatási díjak mértékéről (7);
- 470/2017. (XII. 28.) Kormányrendelet a bizalmi felügyelet által vezetett nyilvántartások tartalmáról és a bizalmi szolgáltatás nyújtásával kapcsolatos bejelentésekről (8)

9.16 Vegyes rendelkezések

9.16.1 Teljességi záradék

Nincs megkötés.

9.16.2 Átruházás

Az archiválási rendnek megfelelően működő harmadik felek csak a Minősített bizalmi szolgáltató előzetes írásbeli engedélyével ruházhatják át jogosultságaikat és delegálhatják kötelezettségeiket.

9.16.3 Részleges érvénytelenség

A jelen dokumentum egyes rendelkezései bármilyen okból kifolyólag érvénytelenné válása esetén a többi rendelkezés változatlanul érvényben marad.

[3] Az OID azonosító utolsó két x-el jelölt karaktere az aktuálisan hatályban lévő Minősített archiválási rend és Minősített szolgáltatási szabályzat verzió számait jelzik

© NOTARchiv Kft.
Minden jog fenntartva. A NOTARchiv Kft. előzetes írásos engedélye nélkül a jelen dokumentum egyetlen része sem reprodukálható, nem továbbítható semmilyen formában és semmilyen esetben, nem tárolható és nem helyezhető el adatbázisokban.

9.16.4 Igényérvényesítés

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

9.16.5 Vis major

Az archiválási rendben és az archiválási szolgáltatási szabályzatban megfogalmazott kötelezettség hibás vagy késedelmes, illetve nem teljesítéséért, a Minősített bizalmi szolgáltató nem vonható felelősségre. Amennyiben a hiba vagy késedelem oka előre nem látható és/vagy a Minősített bizalmi szolgáltató ellenőrzési körén kívüli külső ok.

9.17 Egyéb rendelkezések

Nincs megkötés.

10. Megfelelőségi vizsgálat, vizsgált követelmények, vizsgált rendek azonosítói (3.§ (3) f))

A Szolgáltató évente megfelelőségi vizsgálatot hajtat végre.

Az eIDAS szerinti minősített bizalmi archiválás szolgáltatás elkezdéséhez szükséges megfelelőség értékelési eljárást a MATRIX Vizsgáló, Ellenőrző és Tanúsító Kft. végezte, dátuma: 2020.10.05.

Azonosítója: I-NA20T_TAN.QARCHIVE.HU

A vizsgálat tárgyát képző jogszabályok, szabványok:

A jelen archiválási rend megfelel az alábbi jogszabályoknak:

- AZ EURÓPAI PARLAMENT ÉS A TANÁCS 910/2014/EU RENDELETE (2014. július 23.) (1);
- 2011. évi CXII. törvény az információs önrendelkezési jogról (2);
- 2013. évi V. törvény a Polgári Törvénykönyvről (3).
- 2023. évi CIII. törvény a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól (DÁP (4);
- 24/2016. (VI. 30.) BM rendelet a bizalmi szolgáltatásokra és ezek Minősített bizalmi szolgáltatóira vonatkozó részletes követelményekről (5);
- 25/2016. (VI. 30.) BM rendelet a bizalmi felügyeletnek fizetendő igazgatási szolgáltatási díjak mértékéről (6);
- 470/2017. (XII. 28.) Kormányrendelet a bizalmi felügyelet által vezetett nyilvántartások tartalmáról és a bizalmi szolgáltatás nyújtásával kapcsolatos bejelentésekről (7);
- AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2016. április 27-i (EU) 2016/679 RENDELET GDPR (8)
- ISO 9001:2015 Minőségirányítási Rendszer
- ISO/IEC 27001:2013 Információbiztonság irányítási rendszer
- FIPS PUB 140-2: Security Requirements for Cryptographic Modules
- ETSI EN 319 401 V3.3.1 (2024-06)
- ETSI TS 119 511 V1.1.1 (2019-06)
- ETSI TS 119 512 V1.2.1 (2023-05)

© NOTARchiv Kft.
Minden jog fenntartva. A NOTARchiv Kft. előzetes írásos engedélye nélkül a jelen dokumentum egyetlen része sem reprodukálható, nem továbbítható semmilyen formában és semmilyen esetben, nem tárolható és nem helyezhető el adatbázisokban.

- ETSI EN 319 403 V2.2.2 (2015-08)
- ETSI TS 119 312 V1.5.1 (2024-12)
- ETSI EN 301 549 V3.2.1 (2021-03)

A vizsgálat tárgyát képező archiválási rendek és szabályzatok azonosítói:
• Archiválási Rend (OID: 1.3.6.1.4.1.54136.1.1.1.1.x.x[4].),
• Szolgáltatási Szabályzat (OID: 1.3.6.1.4.1.54136.1.1.1.2.x.x.),
• Az ETSI TS 119511 szerinti minősített hitelesítés rend Szabályzat (OID: 0.4.0.19511.1.2)[5]
Az e szerinti megfelelés egyben az minősített archiválási (megőrzési) követelményeknek megfelelés.

[4] Az OID azonosító utolsó két x-el jelölt karaktere az aktuálisan hatályban lévő Archiválási rend és Szolgáltatási szabályzat verzió számait jelzik.

[5] itu-t(0) identified-organization(4) etsi(0) pres-service-policies(19511) policy-identifiers(1) qualified (2).

© NOTARchiv Kft.
Minden jog fenntartva. A NOTARchiv Kft. előzetes írásos engedélye nélkül a jelen dokumentum egyetlen része sem reprodukálható, nem továbbítható semmilyen formában és semmilyen esetben, nem tárolható és nem helyezhető el adatbázisokban.