Elektronikusan aláírta:
Péchy Gábor
2026-10-07 09:41:42 +0200

NOTARchiv

Minősített archiválási szolgáltatási szabályzat
OID: 1.3.6.1.4.1.54136.1.1.1.2.1.11

A dokumentum azonosítása angolul	Preservation Practice Statement
A dokumentum rövid azonosítása	Minősített archiválási szolgáltatási szabályzat
Közzététel dátuma	Időbélyeg szerint
Hatályba lépés dátuma	2026.11.15.

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.

NOTARchiv		
	Cím	Minősített archiválási szolgáltatási szabályzat
	Kiadás dátuma	lásd: borító
	Biztonsági besorolás	PUBLIKUS
	OID	1.3.6.1.4.1.54136. 1.1.1.2.1.11

A DOKUMENTUM ADATAI

Cím	Minősített archiválási szolgáltatási szabályzat
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.

1 Tartalom

1 Bevezetés 9

1.1 Áttekintés 9

1.2 A dokumentum azonosítása 9

1.2.1 Hatály 9

1.2.2 Archiválási rend 10

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 szolgáltatási szabályzat 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 12

1.5.4 A szolgáltatási szabályzat elfogadási eljárása 12

1.6 Fogalmak és rövidítések 12

1.6.1 Fogalmak 12

1.6.2 Rövidítések 14

2 Közzététel 15

2.1 Minősített bizalmi szolgáltatói információ közzététele 15

2.2 A közzététel időpontja és gyakorisága 15

2.3 Információk hozzáférésének biztosítása 15

2.4 Bizalmi jegy közzététele 15

3 Azonosítás és hitelesítés 15

4 Elektronikus archiválás szolgáltatás 16

4.1 A szolgáltatás igénylése – Szolgáltatási szerződés kötése 17

4.2 Szolgáltatás nyújtása 17

4.2.1 Dokumentum feltöltése és a visszaigazolás 17

4.2.2 Archivált objektum és érvényességi lánc elérhetőségének biztosítása (Dokumentum letöltése) 18

4.2.3 Igazolás kibocsátása 18

4.2.4 Dokumentum megjelenítése 18

4.3 Szolgáltatás elérhetősége 19

© 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 szolgáltatási szerződés megszűnése 19
4.4.1 Dokumentum és érvényességi lánc törlése 19
4.5 Általános biztonsági garanciák 19
4.6 Az informatikai rendszer biztonsága 20
4.7 Életciklus tervezés 20
4.8 Felülhitelesítés 20
4.9 Az archivált adatok titkosítása 21
4.10 A technológia folyamatos figyelése 21
4.11 Olvashatóság és értelmezhetőség fenntartása 21
4.12 Export-import 21
5 Fizikai, eljárásrendi és üzemeltetési előírások 22
5.1 Fizikai követelmények 22
5.1.1 Telephelyek és szerkezeti felépítésük 22
5.1.2 A fizikai hozzáférés szabályozása 22
5.1.3 Áramellátás és légkondicionálás 23
5.1.4 Beázás és vízbetörés elleni védelem 23
5.1.5 Tűz megelőzés és tűzvédelem 23
5.1.6 Adathordozók tárolása 23
5.1.7 Hulladék megsemmisítése 23
5.1.8 A mentési példányok fizikai elkülönítése 23
5.2 Eljárásrendi előírások 24
5.2.1 Bizalmi szerepkörök 24
5.2.2 Az egyes feladatokhoz szükséges személyzeti létszámok 24
5.2.3 Az egyes szerepkörökhöz elvárt azonosítás és hitelesítés 25
5.2.4 Egymást kizáró szerepkörök 25
5.3 Személyzetre vonatkozó előírások 25
5.3.1 Képzettségre, gyakorlatra és megbízhatóságra vonatkozó követelmények 25
5.3.2 Biztonsági ellenőrzésre vonatkozó követelmények 26
5.3.3 Képzési terv 26
5.3.4 Továbbképzés gyakorisága 26
5.3.5 Munkabeosztás körforgása 26
5.3.6 Felhatalmazás nélküli tevékenységek szankciói 26
5.3.7 Szerződéses jogviszonyra vonatkozó követelmények 27
5.3.8 Működést támogató dokumentációk 27

© 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 A biztonsági naplózás folyamatai 27
5.4.1 Tárolt események típusai 28
5.4.2 A naplófájl feldolgozásának gyakorisága 29
5.4.3 A naplófájl megőrzési időtartama 29
5.4.4 A naplófájl védelme 29
5.4.5 A naplófájl mentési eljárásai 29
5.4.6 A naplózás adatgyűjtési rendszere 29
5.4.7 Az eseményeket kiváltó Ügyfelek értesítése 30
5.4.8 Sebezhetőség felmérése 30
5.5 Adatok archiválása 30
5.5.1 Az archiválandó adatok típusa 30
5.5.2 Adatok megőrzésének időpontartama 30
5.5.3 Az archívum védelme 30
5.5.4 Archív információk hozzáférését és ellenőrzését végző eljárások 31
5.5.5 Az archívum mentési folyamatai 31
5.5.6 Az adatok időbélyegzésére vonatkozó követelmények 31
5.5.7 Az archívum gyűjtési rendszere 31
5.5.8 Archív információk hozzáférését és ellenőrzését végző eljárások 31
5.6 Kulcscsere 31
5.7 Katasztrófa helyzet kezelés 31
5.7.1 Váratlan esemény kezelési eljárások 32
5.7.2 Meghibásodott IT erőforrások és/vagy adatok 32
5.7.3 Magánkulcs kompromittálódása esetén követendő eljárás 32
5.7.4 Működés folyamatosságának biztosítása 32
5.8 A szolgáltatás leállítása 33
6 Műszaki biztonsági óvintézkedések 34
6.1 Kulcspár generálás és telepítés 34
6.1.1 Kulcspár előállítása 34
6.1.2 Magánkulcs eljuttatása Végfelhasználóhoz 34
6.1.3 A nyilvános kulcs eljuttatása a tanúsítványkibocsátóhoz 34
6.1.4 Kulcsméretek 34
6.1.5 A nyilvános kulcs paraméterek előállítása, a minőség ellenőrzése 34
6.2 A magánkulcsok védelme 35
6.2.1 Kriptográfiai modulra vonatkozó szabványok és előírások 35

© 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.

6.2.2 Magánkulcs használata ... 36
6.2.3 Magánkulcs letétbe helyezése ... 36
6.2.4 Magánkulcs mentése ... 36
6.2.5 Magánkulcs archiválása ... 36
6.2.6 Magánkulcs import és export ... 36
6.2.7 Magánkulcs tárolása hardware kriptográfiai eszközben ... 36
6.2.8 Magánkulcs aktiválása ... 36
6.2.9 Magánkulcs deaktiválása ... 36
6.2.10 Magánkulcs megsemmisítése ... 36
6.2.11 Kriptográfiai modulok értékelése ... 36
6.3 Kulcspárkezelés szempontjai ... 36
6.4 Aktivizáló adatok ... 37
6.4.1 Aktivizáló adatok előállítása és alkalmazása ... 37
6.4.2 Az aktivizáló adatok védelme ... 37
6.5 Informatikai biztonsági előírások ... 37
6.5.1 Speciális informatikai biztonsági műszaki követelmények ... 37
6.5.2 Az informatikai biztonság ellenőrzése ... 37
6.6 Életciklusra vonatkozó műszaki előírások ... 37
6.6.1 Rendszerfejlesztési előírások ... 37
6.6.2 Biztonságkezelési eljárások ... 38
6.7 Életciklusra vonatkozó biztonsági előírások ... 38
6.8 Hálózati biztonsági előírások ... 38
7 Tanúsítványprofil, megőrzési profil ... 39
7.1 Megőrzési profil – Megőrzés aláírással és kiterjesztéssel, tárolással ... 39
7.1.1 A profil hatálya ... 39
7.1.2 Séma Azonosító ... 39
7.1.3 Megőrzési célok ... 39
7.1.4 Megőrzési tárolási modell ... 40
7.1.5 Megőrzési profil változtatási eljárása ... 40
7.1.6 Támogatott műveletek ... 40
7.1.7 A megőrzési bizonyítékok generálása és ellenőrzése ... 40
7.1.8 A megőrzési bizonyítékok kiterjesztése ... 41
7.1.9 Megőrzési bizonyíték szabályok ... 41
7.1.10 Aláírás ellenőrzési szabályok ... 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.

7.1.11 Archiválási bizonyítékok létrehozása 41
7.1.12 Archiválási bizonyítékok érvényességének ellenőrzése 42
7.1.13 Elektronikus aláírás és bélyegző megőrzése 42
7.1.14 Archiválási bizonyítékok frissítése 42
8 A megfelelőség vizsgálata 43
8.1 Az ellenőrzések gyakorisága 43
8.2 Az auditor és az auditált függetlensége 43
8.3 A vizsgálat által érintett területek 44
8.4 A hiányosságok kezelése 44
8.5 Az eredmények közzététele 44
9 Egyéb üzleti és jogi kérdések 45
9.1 Díjak 45
9.1.1 Archiválás szolgáltatás díjai 45
9.1.2 Visszatérítési politika 45
9.2 Pénzügyi felelősség 45
9.2.1 Biztosítási fedezet 45
9.2.2 Egyéb eszközök 45
9.3 Bizalmasság, adatvédelem 46
9.3.1 Bizalmas információk köre 46
9.3.2 Bizalmas információk körén kívül eső adatok 46
9.3.3 Bizalmas információk védelme 46
9.4 Személyes adatok védelme 46
9.4.1 Adatkezelési tájékoztató 47
9.4.2 Személyes adatok 47
9.4.3 Személyes adatnak nem minősülő adatok 47
9.4.4 Személyes adatok védelme 47
9.4.5 Személyes adatok felhasználása 47
9.4.6 Adatkezelés 47
9.4.7 Egyéb adatvédelmi követelmények 47
9.5 Szellemi tulajdonjogok 48
9.6 Felelősség és helytállás 48
9.6.1 A Minősített bizalmi szolgáltató felelőssége és helytállása 48
9.6.2 Az ügyfél felelőssége és helytállása 48
9.6.3 Egyéb szereplők tevékenységéért viselt felelősség és helytállás 48

© 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.

9.7 A helytállás érvénytelenségi köre 48
9.8 A felelősség korlátozása 49
9.9 Kártérítési kötelezettség 49
9.10 Érvényesség és megszűnés 49
9.10.1 Érvényesség 49
9.10.2 Megszűnés 49
9.10.3 A megszűnés következményei 49
9.11 A felek közötti kommunikáció 49
9.12 Módosítások 49
9.12.1 Módosítási eljárás 49
9.12.2 Értesítések módja és határideje 50
9.12.3 A szolgáltatási szabályzat azonosítójának megváltoztatása 50
9.13 Vitás kérdések rendezése 50
9.14 Irányadó jog 51
9.15 Az érvényben lévő jogszabályoknak való megfelelés 51
9.16 Vegyes rendelkezések 51
9.16.1 Teljességi záradék 51
9.16.2 Átruházás 51
9.16.3 Részleges érvénytelenség 51
9.16.4 Igényérvényesítés 51
9.16.5 Vis major 52
9.17 Egyéb rendelkezések 52
10 Alkalmazott szabványok 53
11. Bizalmi lista 53

© 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 archiválási szolgáltatására vonatkozó szolgáltatási szabályzatot (továbbiakban „Szabályzat") tartalmazza. A dokumentum az RFC 3647 előírásai szerinti szerkezet követi, az eIDAS, a DÁP. és releváns magyar jogszabályok és EN 319 401 és TS 119 511 szabványoknak felel meg.

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

1.1 Áttekintés

Jelen Szabályzat egyike azon dokumentumoknak melyek a Minősített bizalmi szolgáltató által kiadott publikus biztonsági besorolással rendelkező dokumentumoknak, és a Minősített bizalmi szolgáltató által nyújtott archiválási szolgáltatást együtt hivatottak szabályozni.

Jelen Szabályzat „Fogalmak és rövidítések" pontja különböző fogalmat magyaráz meg, amelyeket más területeken nem, vagy nem teljes értelmezésben használnak.

Jelen Szabályzat célja, hogy leírja mindazokat az információkat, amelyeket a Minősített bizalmi szolgáltatóval kapcsolatba kerülő Ügyfeleknek tudniuk kell. Ezzel szándékozik segíteni abban, hogy:

- Jelenlegi és leendő Ügyfelei minél könnyebben megismerhessék Minősített bizalmi szolgáltató által kínált szolgáltatások feltételeit és részleteit;
- Jelenlegi és leendő Ügyfelei átláthassák a Minősített bizalmi szolgáltató működési mechanizmusát, és ennek következtében könnyebb tudják eldönteni, hogy az igénybe vett vagy igénybe venni szándékolt szolgáltatások megfelelnek-e az elvárásaiknak.

1.2 A dokumentum azonosítása

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

1.2.1 Hatály

Jelen Szabályzat fenti hatálybalépési időpontjától annak visszavonásáig vagy az újabb verzió hatálybalépéséig van érvényben.

Jelen dokumentumban foglaltak tartalmát évente a Minősített bizalmi szolgáltató felülvizsgálja. A dokumentum hatálya kiterjed az „A közösség" pontban definiált közösség típusok minden tagjára. Jelen dokumentum a magyar jog alapján, elsősorban magyar Ügyfelek számára, magyar nyelven nyújtott szolgáltatásokra konkrét követelményeket fogalmaz meg.

A Minősített bizalmi szolgáltató a szolgáltatás területi hatályát kiterjesztheti, ez esetben a szolgáltatásra vonatkozó magyar jogszabályoknál nem alkalmazhat enyhébb követelményeket.

A jelen Szabályzat alapján igénybe vehető szolgáltatás kizárólag ebben a dokumentumban, valamint az Archiválási rendben leírtak szerint használható fel.

1.2.1.1 Dokumentum verziók

Azonosító	Kiadás	Leírás	Készítette
1.3.6.1.4.1.54136. 1.1.1.2.1.0	2020. 12. 07.	első kiadás (v1.0)	Bajusz Balázs
1.3.6.1.4.1.54136. 1.1.1.2.1.1	2021. 02. 15.	A tanúsító szervezet által javasolt módosítások és helyesbítések rögzítése	Bajusz Balázs
1.3.6.1.4.1.54136. 1.1.1.2.1.2	2022.01.10.	Módosítások az NMHH és a Tanúsító szervezet észrevételei alapján. Kisebb javítások, pontosítások elvégzése.	Bajusz Balázs

© 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. 1.1.1.2.1.3	2022.07.08.	Éves felülvizsgálat elvégzése. Érvényes minősített aláírással ellátott .pdf és .acis kiterjesztésű fájlok is befogadása is biztosított. Tanúsított HSM firmware.	Bajusz Balázs
1.3.6.1.4.1.54136. 1.1.1.2.1.4	2022.11.30	Éves felülvizsgálat elvégzése. Tanúsító szervezet által javasolt módosítások figyelembevételével	Bajusz Balázs
1.3.6.1.4.1.54136. 1.1.1.2.1.5	2023.11.27	Éves felülvizsgálat elvégzése a tanúsító szervezet által javasolt módosítások figyelembevételével	Bajusz Balázs
1.3.6.1.4.1.54136. 1.1.1.2.1.6	2024.02.26	HSM firmware tanúsítványra mutató link módosítása	Bajusz Balázs
1.3.6.1.4.1.54136. 1.1.1.2.1.7	2024.02.29	HSM firmware tanúsítványra mutató link módosítása	Bajusz Balázs
1.3.6.1.4.1.54136. 1.1.1.2.1.8	2024.08.23	5.8 Szolgáltatás leállítási követelmények módosítása. Módosítások elvégzése a 2024.09.01-én hatályba lépő DÁP jogszabály vonatkozásában.	Bajusz Balázs
1.3.6.1.4.1.54136. 1.1.1.2.1.9	Időbélyeg szerint	Éves felülvizsgálat elvégzése. Kisebb javítások, pontosítások	Bajusz Balázs
1.3.6.1.4.1.54136. 1.1.1.2.1.10	Időbélyeg szerint	Éves felülvizsgálat elvégzése. Kisebb javítások, pontosítások	Bajusz Balázs
1.3.6.1.4.1.54136. 1.1.1.2.1.11	Időbélyeg szerint	Éves felülvizsgálat elvégzése. Kisebb javítások, pontosítások	Bajusz Balázs

1.2.2 Archiválási rend

A jelen Szabályzat szerint nyújtott szolgáltatás megfelel az „Archiválási rend” követelményeinek.

A részletes követelményeket a Minősített bizalmi szolgáltató az „Archiválási rend” nevű dokumentum tartalmazza.

A Minősített bizalmi szolgáltató megfelel az ETSI TS 119 511-nek, és Annex A fejezeteinek, így annak azonosítása során jogosult a minősített archiválási szolgáltatás a szabályzat azonosítóját is feltünteti amely:
0.4.0.19511.1.2
itu-t(0) identified-organization(4) etsi(0) pres-service-policies(19511) policy-identifiers(1) qualified (2).

1.3 Szereplők

A Minősített bizalmi szolgáltató az alábbiakat különbözteti meg közösségi csoportok vonatkozásában:

1.3.1 A Minősített bizalmi szolgáltató

A szolgáltatást nyújtó Minősített bizalmi 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 Minősített bizalmi szolgáltató telephelye	1087 Budapest, Stróbl Alajos utca 3/b 1041 Budapest Mády Lajos utca 4
Postázási cím:	1087 Stróbl Alajos utca 3/b
Cégjegyzékszám:	01-09328760

© 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.

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

Az archiválási rendben találhatók a követelmények a minősített archiválás szolgáltatás nyújtásához.

A Minősített bizalmi szolgáltató minősített szolgáltatást csak felügyeleti nyilvántartásba felvételt és a bizalmi listán feltüntetést követően végezhet (lásd: jelen szabályzat 11. pontja).

A felügyelet nyilvántartásának elérhetősége:
https://esign.nmhh.hu/bszny/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

1.3.2 Az ügyfelek

Az elektronikus archiválási szolgáltatást igénybe vevő fél (Ügyfél), aki Szolgáltatási szerződést köt a Minősített bizalmi szolgáltatóval és az igénybe vett szolgáltatással kapcsolatos költségek ellenértékét a Minősített bizalmi szolgáltató felé 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

Az 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 kiállítás) használhatók.

1.5 A szolgáltatási szabályzat 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	NOTARchiv 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

© 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.

1.5.3 A szolgáltatási szabályzat megfelelőségéért felelős személy és/vagy szervezet

A szolgáltatási szabályzatnak és az archiválási rendnek való megfeleléséért és az abban leírtak szerinti szolgáltatás nyújtásáért a szabályzatot kibocsátó Minősített bizalmi szolgáltató a felelős. Jóváhagyást csak a Minősített bizalmi szolgáltató vezető pozícióját betöltő személy teheti meg (lásd: 2. oldal „Jóváhagyók").

1.5.4 A szolgáltatási szabályzat elfogadási eljárása

Amennyiben a szabályzat módosításra szorul, a módosított új verzió megírása, elfogadása és kibocsátása 9.12.1 fejezete szerint zajlik. Az új verzió jóváhagyásáért felelős munkatárs, ha meggyőződött róla, hogy a Szabályzat megfelel a Szolgáltatási Rend előírásainak, jóváhagyja a szabályzatot és legkésőbb az új verzió hatálybalépése előtt 30 nappal gondoskodik annak közzétételéről, ettől eltérni csak a Hatóság külön igénye estén lehetséges.

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. cikkében meghatározott követelményeknek.
Fokozott biztonságú elektronikus	olyan elektronikus bélyegző, amely megfelel az eIDAS rendelet

© 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.

bélyegző	36. cikkében 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.
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.

© 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.

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.

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

© 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.

2 Közzététel

2.1 Minősített bizalmi szolgáltatói információ közzététele

A Minősített bizalmi szolgáltató a feltételeit és szabályzatait Minősített bizalmi szolgáltató honlapján nyilvános elektronikus formában teszi elérhetővé. Publikálás előtt legalább 30 nappal a hatálybalépés előtt kerülnek a kommunikálásra váró új vagy módosított dokumentumok. Az érvényben levő dokumentumokon felül a Minősített bizalmi szolgáltató honlapján elérhető a dokumentum valamennyi korábbi verziója is.

2.2 A közzététel időpontja és gyakorisága

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

2.3 Információk hozzáférésének biztosítása

Az információk elérése bárki számára biztosított.

A szolgáltatási szabályzatok és a szerződési feltételek aktuális verziója olvasható formában a Minősített bizalmi szolgáltató irodájában van jelen.

2.4 Bizalmi jegy közzététele

A Minősített bizalmi szolgáltató a BIZOTTSÁG (EU) 2015/806 végrehajtási rendeletében megfogalmazott előírásainak megfelelően teszi közzé a minősített bizalmi szolgáltatások bizalmi jegyét.

3 Azonosítás és hitelesítés

A Minősített bizalmi szolgáltató az Ügyfél szerződésbe kerülő adatait ellenőrzi a célra megfelelő módon és adatforrás segítségével.

A személyes adatok ellenőrzése személyiazonosításra alkalmas igazolvány alapján történhet, míg a szervezeti adatok ellenőrzésére rendszeresen frissített cégnyilvántartás alapján történhet.

© 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 Elektronikus archiválás szolgáltatás

A Szolgáltatási szerződés (a továbbiakban: Szerződés) aláírásával és keretei közt a Minősített bizalmi szolgáltató minősített bizalmi elektronikus archiválás szolgáltatást nyújt az Ügyfél számára. A Minősített bizalmi szolgáltató a Szerződés keretében a minősített bizalmi elektronikus archiválás Minősített bizalmi szolgáltatóként nyújtja a szolgáltatást az Ügyfelek számára.

Az elektronikus archiválási szolgáltatást a 2023. évi CIII. törvény és a 910/2014/EU (eIDAS) rendelet szabályozza és a szolgáltatás a következőket foglalja magában (a továbbiakban együttesen röviden Szolgáltatások):

- Az ügyfél elektronikusan aláírt és/vagy elektronikus bélyegzővel ellátott fájlokat tölthet fel befogadásra a Minősített bizalmi szolgáltató által üzemeltetett archiválási rendszerbe. A Minősített bizalmi szolgáltató ellenőrzi az elektronikus aláírás és/vagy elektronikus bélyegző hitelességét és érvényességét, majd biztosítja az elektronikus aláírással és vagy elektronikus bélyegzővel ellátott e-aktákban mentett dokumentumok hosszú távú és sértetlen megőrzését.
- A Minősített bizalmi szolgáltató biztonságosan tárolja az e-aktákat (fájlokat és érvényességi láncokat) és biztosítja, hogy a bizalmas dokumentumokhoz még saját munkatársai sem rendelkezzenek közvetlen hozzáféréssel. A megőrzés során biztosítja a Minősített bizalmi szolgáltató, hogy utólag ne lehessen módosítani az e-aktákat, és csak is az arra jogosult Ügyfél hozzáférhessen hozzá az e-aktákhoz. A megőrzés során a Minősített bizalmi szolgáltató a jogosulatlan hozzáférést, módosítást és törlést, kizárja és a megőrzési idő alatt biztosítja az e-akták a Minősített bizalmi szolgáltató által támogatatott fájl típusainak hosszú távú olvashatóságát. A megőrzés a Szolgáltatási szerződésben foglalt megőrzési időtartalomra szól. Ezek részleteit a „Fizikai, eljárásrendi és üzemeltetési előírások” fejezet írja le.
- Az Ügyfél a Szerződés időtartama alatt folyamatosan 99%-os rendelkezésre állással elérheti a Minősített bizalmi szolgáltató archiválási rendszerébe befogadott dokumentumait.
- Az Ügyfél kifejezett írásos kérésére a Minősített bizalmi szolgáltató igazolást bocsát ki arról, hogy az egyes dokumentumokat eltárolja, és azon dokumentumokon az archiválás pillanatában érvényes elektronikus aláírás szerepel.

Az Ügyfél kifejezett írásos törlési kérésére a Minősített bizalmi szolgáltató visszaállíthatatlanul törli a dokumentumokat az archívumából.

A működés műszaki jellemzői

- A Minősített bizalmi szolgáltató két különböző földrajzi helyen tárolja az archivált elektronikus dokumentumokat egy elsődleges (Primer) és a másodlagos (Seconder) adatközpontban redundáns működéssel. A másodlagos rendszer képes kritikus esetben az elsődleges rendszer kiszolgálási funkcióját átvenni, a Primer rendszer kiesése esetén. Kiszolgálási funkció vonatkozásában a befogadott elektronikus dokumentumok elérhetőek lesznek. A befogadási funkció viszont csak abban az esetben működhet, amennyiben mindkét helyszínen lévő adatközpont eltudja látni általános üzemi funkcióját.
- Az üzlet folytonosság növelése érdekében a Minősített bizalmi szolgáltató általa biztosított szolgáltatásokhoz szükséges hardver, szoftver, illetve egyéb eszközeit két, fizikailag egymástól elkülönült helyszínen is tárolódnak a befogadott elektronikus dokumentumok. A biztonsági szabályokra vonatkozó rendelkezéseket a Minősített bizalmi szolgáltató Informatikai Biztonsági Szabályzat című „Belső felhasználásra” biztonsági minősítésű dokumentum tartalmazza.
- A folyamatos rendelkezésre állást és a biztonságos informatikai szolgáltatást a Minősített bizalmi szolgáltató tanúsított ISO/IEC 27001:2023 szabványnak megfelelő információbiztonsági irányítási keretrendszert alkalmaz, amelyet rendszeresen külső és belső auditorok közreműködésével szavatol.

© 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.

- Minőségirányítási rendszere a tanúsított ISO 9001:2015 szabványnak felel meg.

4.1 A szolgáltatás igénylése – Szolgáltatási szerződés kötése

Az Ügyfél az alábbiak alapján veheti igénybe a Minősített bizalmi szolgáltató által nyújtott archiválási szolgáltatást:

1. A leendő Ügyfél kapcsolatba lép a Minősített bizalmi szolgáltatóval.
2. A Minősített bizalmi szolgáltató tájékoztatja a leendő Ügyfelet a Szolgáltatási szabályzatban foglaltakról, ezen tájékoztatást a kapcsolatfelvétel során az Ügyfél tudomására kerül. A Minősített bizalmi szolgáltató honlapján egy a tájékoztatás céljából közzétett dokumentum is elérhető.
3. Az Ügyfél a Minősített bizalmi szolgáltató honlapján keresztül juthat információkhoz az elektronikus archiválás szolgáltatás felhasználásának módjáról, biztonsági fokáról, szolgáltatási szabályzatáról, a szerződés feltételeiről, valamint az alkalmazandó adatvédelmi szabályokról.

A Minősített bizalmi szolgáltató internetes honlapján megtalálható nyilvános biztosági osztályú dokumentumok úgymint:

- Általános szerződési feltételek,
- Archiválási rend,
- Archiválási szolgáltatási szabályzat,
- Archiválási szolgáltatási kivonat
- Adatkezelési tájékoztató.

Az Ügyfél és a Minősített bizalmi szolgáltató közti Szerződés kötés a következő esetekben tekinthető hitelesnek:

-kézzel alulírott,

-elektronikus aláírással vagy bélyegzővel ellátott.

A Szolgáltatási szerződés határozatlan időre szól.

4.2 Szolgáltatás nyújtása

4.2.1 Dokumentum feltöltése és a visszaigazolás

A Minősített bizalmi szolgáltató kizárólag az Ügyfél azonosítása (archiválási rendszerbe történő belépés) után, fogad el dokumentumokat befogadásra a Minősített bizalmi szolgáltató az Ügyfél irányából. Az eljárás biztosítja, hogy a dokumentumok integritásának, bizalmasságának, megőrzését és az Ügyfél számára történő rendelkezésre állását a szerződésben foglal időpontig.

A dokumentum a Minősített bizalmi szolgáltató irányába való kommunikálása titkosított SSL/TLS csatornán történik meg. A feltöltés az alábbi módon történhet:

- Az Ügyfél a Minősített bizalmi szolgáltató rendszerébe történő belépése után titkosított SSL/TLS kapcsolat jön létre a Minősített bizalmi szolgáltató és az Ügyfél között.
- A sikeres rendszerbe történő belépést követően az Ügyfél a titkosított SSL/TLS kapcsolaton keresztül töltheti fel a dokumentumokat befogadásra a Minősített bizalmi szolgáltató által üzemeltetett archiválási rendszerbe.

Feltölthető dokumentumok a következők lehetnek:

- bitfolyam (a formátuma nincs megkötve, értelmezhetőséget Minősített bizalmi szolgáltató nem biztosítja)
- dokumentum (.pdf és .txt) (az értelmezhetőséget biztosítja amennyiben az Ügyfél nyilatkozza, hogy a Minősített bizalmi szolgáltató által biztosított szoftverrel a beküldött dokumentum megjeleníthetőségét ellenőrizte.)

A feltöltést után a Minősített bizalmi szolgáltató ellenőrzi, hogy a dokumentum formátumára vonatkozó feltételek megfelel-e a Minősített bizalmi szolgáltató honlapján közzétett és a rendszer által támogatott formátumok valamelyikével. A minősített bizalmi szolgáltató az alábbi formátumokat fogadja be: .pdf, .es3, .asic.

© 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.

- Az aláírások és bélyegzők hitelességének az ellenőrzését követően a befogadási folyamat csak abban az esetben folytatódik, ha a dokumentumon szereplő elektronikus aláírás és/vagy bélyegző és időbélyeg aláírás/bélyegzés időpontjában történő érvényessége megbízható.

A dokumentumon elhelyezett elektronikus aláírásnak/bélyegzőnek megbízható közegből származó minősített elektronikus aláírásnak/bélyegzőnek kell lennie.

Az Ügyfél olyan magánkulccsal rendelkezik, amely a szolgáltatás igénybevételére szolgáló titkosító tanúsítványához tartozik. Ezzel a kulccsal dekódolja a fájlt, így hozzájut a tartalmához.

A hozzáférés az Ügyfél által archivált dokumentumhoz a fent említett módon (vagy írásban meghatalmazott képviselője) nem tanúsítvány, hanem valamely személyazonosításra alkalmas okmány alapján azonosítja magát. A befogadott fájlok az Ügyfél tulajdonában vannak (lásd: 1.4. fejezet), így az adat tulajdonos szerepét az Ügyfél vagy általa meghatalmazott személy tölti be.

4.2.2 Archivált objektum és érvényességi lánc elérhetőségének biztosítása (Dokumentum letöltése)

Az archiválási szolgáltatásba történő sikeres authentikáció esetén a megőrzött dokumentum és a hozzá kapcsolódó befogadási igazolás, és a Minősített bizalmi szolgáltató által aláírt érvényességet és sértetlenséget igazoló file letöltési link jelenik meg.

4.2.3 Igazolás kibocsátása

A Minősített bizalmi szolgáltató az Ügyfél számára igazolást ad ki az alábbi tényekről:

a) a megőrzésében lévő elektronikus dokumentumon elhelyezett fokozott biztonságú vagy minősített elektronikus aláírás, bélyegző vagy időbélyegző, illetve az azokhoz kapcsolódó tanúsítvány az időbélyegzés időpontjában érvényes volt,

b) a megőrzésében lévő lenyomathoz kapcsolódó fokozott biztonságú vagy minősített elektronikus aláírás, bélyegző vagy időbélyegző, illetve az azokhoz kapcsolódó tanúsítvány az aláírás, bélyegzés vagy időbélyegzés időpontjában érvényes volt,

c) a megőrzésében lévő, az érvényességi lánc részét képező elektronikus dokumentum tartalma megegyezik a bizalmi szolgáltatási ügyfél által bemutatott elektronikus dokumentummal,

d) a megőrzésében lévő, az érvényességi lánc részét képező lenyomat megegyezik az Ügyfél által bemutatott elektronikus dokumentum lenyomatával,

e) a megőrzésében lévő, az érvényességi lánc részét képező elektronikus dokumentumon, amelynek tartalma megegyezik az Ügyfél által bemutatott elektronikus dokumentummal, meghatározott személy érvényes elektronikus aláírást vagy bélyegzőt helyezett el,

f) a megőrzésében lévő, az érvényességi lánc részét képező elektronikus dokumentumon, amelynek tartalma megegyezik az Ügyfél által bemutatott elektronikus dokumentummal, meghatározott időpontban érvényes elektronikus aláírást, bélyegzőt vagy időbélyegzőt helyeztek el.

A fenti 4.2.3 pontban felsorolt tények együttes tejlesülésekor a Minősített bizalmi szolgáltató igazolást ad ki elektronikusan.

Az igazolás harmadik személy számára is kiadható, ha a kérelméhez csatolja az Ügyfél teljes bizonyító erejű magánokiratba vagy közokiratba foglalt meghatalmazását.

A befogadási igazolást a Minősített bizalmi szolgáltató elektronikusan bocsátja ki melyet minősített elektronikus bélyegzővel és minősített időbélyegzővel lát el.

4.2.4 Dokumentum megjelenítése

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

© 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.

4.3 Szolgáltatás elérhetősége

A Minősített bizalmi szolgáltató a tevékenységét 7/24 kell biztosítja, a befogadást kivéve, melyet szüneteltethet.
A szolgáltatás esetében a következő kerülnek biztosításra:

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

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

A szolgáltatás a biztonságos használatra előírt feltételek mellett használható.

4.4 A szolgáltatási szerződés megszűnése

A Minősített bizalmi szolgáltató a Szerződés megszűnése esetén inaktíválja az Előfizető felhasználói fiókját majd a biztosítja az Ügyfél adatállományainak visszaállíthatatlan törlését.

4.4.1 Dokumentum és érvényességi lánc törlése

Törlésre csak kivételesen, szerződésben meghatározott esetekben kerül sor.

A Minősített bizalmi szolgáltató az Ügyféltől érkező írásos törlési igény vonatkozásában a törlési műveletet visszaállíthatatlanul végre hajtja, a törlés keretében a dokumentum minden mentett példányát megsemmisíti.

Az Ügyfél a Minősített bizalmi szolgáltatótól írásos törlési kérelmét személyesen vagy minősített elektronikus aláírással/bélyegzővel ellátott kérelem formájában kérelmezheti. A törlést a Minősített bizalmi szolgáltató 15 munkanapon belül bírálja el és hajtja végre.

A törlésről a Minősített bizalmi szolgáltató az Ügyfél számára elektronikus bélyegzővel és minősített időbélyegzővel ellátott igazolást (tértivevényt) küld.

A visszaigazolás tartalmazza
- törölt dokumentum egyedi azonosítóját,
- a törlés időpontját,
- a törlési kérelmet benyújtó azonosítóját is.

4.5 Általános biztonsági garanciák

A Minősített bizalmi szolgáltató megbízható rendszereket és termékeket használ, melyek a jogosulatlan módosítások ellen védettek. Biztonságtechnikai szempontból megbízható termékekből álló, a konzisztens informatikai rendszert használó szolgáltatás nyújtásához.

A Minősített bizalmi szolgáltató és a rendszert szállító és üzemeltető szerződött alvállalkozók az archiválási-szolgáltatás kiépítésében és üzemeltetésében jelentős tapasztalatokkal rendelkeznek és világszinten elismert technológiát alkalmaznak.

Abban az esetben, ha a Minősített bizalmi szolgáltató harmadik féltől bizalmi szolgáltatást vesz igénybe, ellenőrzi, hogy ezen harmadik fél eleget tesz-e a jogszabályban rögzített kötelezettségének. A Minősített bizalmi szolgáltató fizikailag biztonságos környezetben tárolja el az archivált fájlokat.

Az archivált adatok biztonságát, sérthetetlenségét és rendelkezésre állását a Minősített bizalmi szolgáltató belső biztonsági szabályzatai és a rendszeres belső és külső biztonsági felülvizsgálat garantálják. A belső felülvizsgálat fél évente történik, a biztonsági szabályzat felülvizsgálata legalább évente. A Minősített bizalmi szolgáltató a változásokat kommunikálja a bizalmi munkakörösök felé.

[1] https://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.

A Minősített bizalmi szolgáltató biztosítja, hogy az archívumban lévő dokumentumokat saját munkatársai sem olvashatják el. A Minősített bizalmi szolgáltató a dokumentumokat kizárólag akkor bocsátja harmadik fél (pl. NMHH vagy más Hatósági jogkörrel rendelkező szervezet) rendelkezésére, amennyiben ezt jogszabály írja elő, illetve, ha erre az Ügyfél irányából a Minősített bizalmi szolgáltató aláírt felhatalmazást kap.

A tárolt elektronikus dokumentumok integritását a rendszer fizikai védelme, valamint az elektronikus aláírással kapcsolatos technológiák biztosítják. Az archivált és titkosított fájlok rendelkezésre állását a Minősített bizalmi szolgáltató magas színvonalú informatikai rendszer redundanciája, valamint a rendszer működését szabályzó

-belső szabályzatai,

- üzletmenet-folytonossági és katasztrófakezelési eljárásai

-és egyéb rendkívüli üzemeltetési helyzetek kezelésére szolgáló folyamatai biztosítják.

A Minősített bizalmi szolgáltató az üzemeltetés és a karbantartás során felmerülő hibákat az eljárások és szabályzatok, valamint ezek folyamatos külső és belső ellenőrzése és tesztelése segítségével kerüli el.

A Minősített bizalmi szolgáltató két, egymástól távoli fizikai helyszínen tárolja az archivált fájlokat. A Minősített bizalmi szolgáltató az archivált fájlokat az Ügyfél kérése vagy a Szolgáltatási szerződés megszűnése esetén – jelen dokumentum „Dokumentum és érvényességi lánc törlése” pontjában leírt eljárás mellett semmisíti meg.

A Minősített bizalmi szolgáltató az aláírására használt kulcsokat, az archivált dokumentumok titkosításához és dekódolásához használt kulcsokat, és az infrastrukturális és rendszervezérlési kriptográfiai kulcsokat kriptográfiai célhardverben (HSM modulban) állítja elő.

A kulcsokat a Minősített bizalmi szolgáltató lecseréli amennyiben azt észleli,

-hogy kriptográfiai technológiai elvárásainak valamely kulcs már nem használható biztonságosan,

- illetve, ha a NMHH határozata szerint az adott algoritmus már nem használható, akkor haladéktalanul lecseréli az érintett kulcsot vagy kulcsokat.

4.6 Az informatikai rendszer biztonsága

A Minősített bizalmi szolgáltató rendszerét redundánsan alakította ki annak érdekében, hogy az informatikai biztonság és rendelkezésre állás magas szinten funkcionáljon. Minden kritikus archiválási szolgáltatást biztosító rendszerelemből egyenként két példány üzemel, bármelyik elem kiesése esetén a másik egyazon funkcionalitású elem és átveszi a kiesett elem funkciójának betöltését. Hardveres kriptográfiai eszközben (HSM modulban) állítja elő és tárolja az aláíró kulcsokat, az archivált adatok titkosításához/dekódoláshoz szükséges kulcsokat. Az informatikai rendszerét a Minősített bizalmi szolgáltató több hardveres tűzfallal védi. Minden tűzfalból két példány működik, bármelyik kiesése esetén a másik ugyanolyan egység átveszi a funkcióját.

4.7 Életciklus tervezés

A szolgáltatások nyújtásához használt termékek életciklusukra vonatkozó biztonsági szempontok figyelembevételével kerültek a Minősített bizalmi szolgáltató által alkalmazásra.

Annak érdekében, hogy a Minősített bizalmi szolgáltató valamennyi rendszerfejlesztési keretében a biztonsági követelmények magas színvonalon biztosítottak legyenek, a teljes fejlesztés során (már a tervezési és követelmény-definiálás fázisban is) figyelembe vette a fokozott követelményeket.

4.8 Felülhitelesítés

A Minősített bizalmi szolgáltató köteles minősített időbélyegzőt elhelyezni vagy elhelyeztetni az alábbi esetekben:

- a befogadott adatállományokon lévő utolsó archív aláírás érvényességének lejárata előtt legkésőbb 3 hónappal,
- amennyiben az NMHH ilyen határozatot hoz.

© 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.

4.9 Az archivált adatok titkosítása

Az archivált elektronikus dokumentumok titkosítva tárolódnak az archívumban. A Minősített bizalmi szolgáltató biztosítja, hogy az archivált dokumentumok mindenkor biztonságos algoritmussal kerülnek titkosításra. Újra titkosítás szükséges a következő esetekben:

- a használt titkosító algoritmusban a bizalom meginog – ebben az esetben a titkosítás időpontjában biztonságos algoritmussal kell újra titkosítani;
- a Minősített bizalmi szolgáltató dekódoló kulcsának bizalmassága megsérül;
- a Szolgáltatási szabályzat vagy az Ügyféllel kötött Szolgáltatási szerződés így rendelkezik.

A fájlok újra titkosítása után a korábbi, már nem kellően biztonságosnak ítélt módon titkosított példányokat a Minősített bizalmi szolgáltató megsemmisíteni.

4.10 A technológia folyamatos figyelése

A Minősített bizalmi szolgáltató figyelemmel kíséri a mindenkori hitelesítéssel és kriptográfiával kapcsolatos technológia fejlődését. Amennyiben a Minősített bizalmi szolgáltató értesülései szerint vagy az NMHH határozata szerinti, a használatban levő kriptográfiai algoritmusok már nem felelnek meg a követelményeknek, erről informálja az NMHH-t és beszünteti a használatát illetve a mindenkor hatályos NMHH határozatban szereplő másik algoritmust használni a szolgáltatás nyújtásához.

A Minősített bizalmi szolgáltató bármikor szabadon dönthet a használt kriptográfiai algoritmuskészletek és paramétereik megváltoztatásáról amennyiben a használandó megoldások szerepelnek az NMHH mindenkori hatályos határozatában.

4.11 Olvashatóság és értelmezhetőség fenntartása

A Minősített bizalmi szolgáltató gondoskodik arról, hogy az archiválási időtartam alatt bizonyos formátumú fájlok megjelenítéséhez szükséges lehetőségek folyamatosan rendelkezésére álljanak. A Minősített bizalmi szolgáltató a műszaki értelemben vett olvashatóságát biztosítja, így nem vállal felelősséget a fájlok tartalmának értelmezhetőségéért (pl. hibás szkennelés következtében feltöltött üres, de szabályos formátumú .pdf fájl.) A Minősített bizalmi szolgáltató csak „.pdf” és „.txt” kiterjesztésű fájlok olvashatóságát biztosítja.

A Minősített bizalmi szolgáltató az elektronikus dokumentumok megőrzését és olvashatóságának fenntartását is a szolgáltatási szerződés érvényességi idejéig vállalja, illetve amíg írásos törlési kérelem nem érkezik az Ügyfél irányából.

4.12 Export-import

A Minősített bizalmi szolgáltató a felülhitelesítési információkat a dokumentumokba ágyazza, ezért a letöltött dokumentum tartalmazza az evidenciát is, külön exportálásra (evidenciákkal) nincs szükség, a letöltött állomány másik Minősített bizalmi szolgáltató által is befogadható; más Minősített bizalmi szolgáltatótól a kiterjesztett állomány standard feltöltéssel teljesíthető, így export-importot a Minősített bizalmi szolgáltató a standard eléréseken biztosít.

Egyedi eljárás igénylése írásban az ügyfélszolgálati eléréseken lehetséges, a dátum és a kritérium naplózásra kerül.

Az elektronikus dokumentumok átadása minden esetben az átvevő személyének és jogosultságának ellenőrzése után történik. Minden Előfizető alapesetben csak az általa betöltött fájlokhoz férhet hozzá. Az Interneten történő lekérdezés esetében a jogosultság ellenőrzése authentikációs soft-token és felhasználónév/jelszó alapján történik.

A személyesen történő fájl átadás során az átvevő személyazonosságát a Minősített bizalmi szolgáltató személyazonosításra alkalmas hatósági igazolvány alapján ellenőrzi.

A Minősített bizalmi szolgáltatóval előzetesen egyeztetve az Előfizető akár adathordozón, például pendrive (flashdrive-on) is átveheti a Minősített bizalmi szolgáltatónál tárolt elekronikus dokumentumait és archiválási bizonyítékait. Az elektronikus dokumentumok átadása minden esetben az átvevő személy azonosságának és jogosultságának ellenőrzése után kerül kiadásra.

© 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, eljárásrendi és üzemeltetési előírások*

A Minősített bizalmi szolgáltató széles körűen alkalmazott szabványoknak megfelelő fizikai, személyzeti és egyéb biztonsági óvintézkedéseket és irányítási folyamatokat alkalmaz.

A Minősített bizalmi szolgáltató információbiztonsági szabályozást és vagyonnyilvántartást rendszeres időközönként, vagy ha jelentős változás történik, felül vizsgálja.

A Minősített bizalmi szolgáltató nyilvántartást vezet a szolgáltatás nyújtásával kapcsolatos rendszerelemekről és erőforrásokról. Kockázatelemzést végez ezen elemek vonatkozásában.

Az egyes elemekkel kapcsolatban kockázatokkal arányos védelmi megoldásokat alkalmaz. A Minősített bizalmi szolgáltató figyelemmel kísérni a kapacitási igényeket és biztosítja, hogy megfelelő feldolgozási teljesítmény és tárolási kapacitás álljon rendelkezésre a szolgáltatás nyújtásához.

5.1 *Fizikai követelmények*

A Minősített bizalmi szolgáltató gondoskodik arról, hogy a kritikus szolgáltatásokhoz történő fizikai hozzáférés ellenőrzött módon történjen.

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

A Minősített bizalmi szolgáltató valamennyi kritikus szolgáltatását egy külön erre a célra fenntartott biztonsági zónában valósítja meg úgy, hogy ehhez szükséges valamennyi eszközt egy a biztonsági zóna részét képező védett helységben helyezi el.

5.1.1 *Telephelyek és szerkezeti felépítésük*

A két telephelyen az adatközpont kiépítése a környezeti biztonság kezelése során Minősített bizalmi szolgáltató figyelmébe veszi:

- a tűz- és vízvédelemre,
- a folyamatos elektromos áramellátásra,
- a légkondicionálásra,
- a fizikai behatolás megakadályozására,
- a biztonságos zónák kialakítására és a telekommunikációs hálózatok elérhetőségére
- a sugárzás elleni védelemre vonatkozó ajánlásokat és előírásokat.

Az Adatközpont kialakítása során alkalmazott védelmi megoldásokat alkalmaz – mint pl. biztonsági zár, behatolás érzékelők, videó megfigyelő rendszer, beléptető rendszer őrző-védő szolgáltatás, biometrikus azonosítás 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 fenntart egy fizikailag lehatárolt biztonsági területet a biztonságos működés kritikus komponensei számára, amelyet a behatolás ellen fizikailag is megvéd, ahova a bejutást ellenőrzi, érzékeli a jogtalan behatolást és behatolási riasztóval van ellátva. Ugyanezen biztonsági területen belül más tevékenységek kizárólag abban az esetben folytat, ha a területre belépési jogosultsággal rendelkezők azt el tudják végezni.

A Minősített bizalmi szolgáltató biztosítja az alábbiak teljesülését:

- a biztonsági területre történő belépés naplózása;
- az adatközpontban a Minősített bizalmi szolgáltató csak két erre feljogosított munkavállalója tartózkodhat
- indokolt esetben egyéb jogosultsággal rendelkező személyek csak a szükséges ideig tartózkodhatnak a gépteremben megfelelő jogosultságú személyzettel kíséretében;
- a belépési napló fájlokat folyamatosan a Minősített bizalmi szolgáltatónak archiválja, amik heti revízióra kerülnek.

Jogosulatlan személyek jelenlétében a Minősített bizalmi szolgáltató:

© 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.

- az archivált adatokat tartalmazó adattárolókat fizikailag elzárva tartja;
- a bejelentkezett munkaállomásokat nem hagyja felügyelet nélkül;
- ellenőrzi, hogy a munkaállomásokon nincs bejelentkezve maradt felhasználó;
- megfelelően elzárásra kerültek a fizikai adattároló eszközök;
- berendezések és a fizikai védelmet biztosító rendszerek megfelelően működnek.

A Minősített bizalmi szolgáltató felelősöket jelöl ki a fizikai biztonsági vizsgálatok elvégzésére és naplózza a vizsgálatok eredményét.

5.1.3 Áramellátás és légkondicionálás

A Minősített bizalmi szolgáltató az adatközpontokban olyan szünetmentes áramellátási eszközöket alkalmaz:

- 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 helységekben használt légkondicionáló rendszer teljesítménye képes biztosítani a megfelelő üzemelési hőfokot az adatközpont és az üzemeltetett hardverek részére. A levegő páratartalma az informatikai rendszerek által elvárt szintre van csökkentve.

5.1.4 Beázás és vízbetörés elleni védelem

A biztonsági zóna kialakítása során fontos szempont volt a beázás és vízbetörés veszélyének elkerülése. A biztonsági zóna teljes területét vízbetörés érzékelő rendszer felügyeli. Az álpadló alkalmazása az adatközpontban tovább hivatott növelni a vízbetörés elleni védelmet.

5.1.5 Tűz megelőzés és tűzvédelem

A Minősített bizalmi szolgáltató az adatközpont helyszínein működőképes füst- és tűzérzékelőket alkalmaz. Jól látható helyen feltüntetett a menekülési útvonalat és megfelelő típusú és mennyiségű, tűzoltóság által hitelesített kézi tűzoltó eszközöket használ.

Az adatközpontokban automatikusan üzemelő tűzoltó rendszert alkalmaz.

5.1.6 Adathordozók tárolása

A Minősített bizalmi szolgáltató az adathordozóit megvédi valamennyi jogosulatlan hozzáféréstől és esetleges megrongálódástól. A napló és archív fájlokat duplikáltan hozza létre és tárolja és egymástól fizikailag is elkülönítve tárolja, két biztonságos távolságra lévő helyszínen. A káros környezeti körülményektől a tárolt adathordozókat a Minősített bizalmi szolgáltató megvédi, mint pl. alacsony vagy magas hőmérséklet, szennyeződés, nedvesség, napfény, erős mágneses tér, erős sugárzás.

5.1.7 Hulladék megsemmisítése

A mindenkori környezetvédelmi előírások betartásával a Minősített bizalmi szolgáltató gondoskodik arról, hogy a feleslegessé vált eszközeik, adathordozóik selejtezésére és megsemmisítésére kerüljenek. A felesleges és leselejtezett eszközökön, adathordozókon lévő adatokat a Minősített bizalmi szolgáltató munkatársának személyes jelenléte és felügyelete alatt és az elfogadott módszereknek megfelelően véglegesen törli vagy alap funkcióját tekintve használhatatlanná teszi. A Minősített bizalmi szolgáltató az alábbi adat megsemmisítési folyamatokat alkalmazza:

- a papíralapú dokumentumokat iratmegsemmisítő géppel felaprítja;
- a merevlemezeket szétszereli és a kritikus alkatrészeket fizikailag tönkre teszi;
- az optikai lemezeket erre alkalmas megsemmisítő géppel megsemmisíti.

5.1.8 A mentési példányok fizikai elkülönítése

Az üzemmenet folytonosság fenntartása és az adatvesztés elkerülése érdekében a Minősített bizalmi szolgáltató rendszerein folyamatos mentéseket eszközöl, és biztosítja szükség esetén az archiváló rendszer egészének a helyreállíthatóságát.

A Minősített bizalmi szolgáltatónak a mentéseket, amely az utolsó teljes mentést is beleértve egy olyan külső helyszínen tárolja, 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 kockázata melletti üzemeltetéséről a Minősített bizalmi szolgáltató megfelelően gondoskodik. A biztonságos működés érdekében elegendő számú és megfelelő képzettséggel, műszaki tudással, tapasztalattal rendelkező munkavállalókat foglalkoztat.

A Minősített bizalmi szolgáltató naprakész belső szabályzati és ellenőrzési eljárásrendet működtet. A Minősített bizalmi szolgáltató független rendszervizsgáló ellenőrzési tevékenységgel biztosítja az archiválási rendszer biztonságos működését.

A Minősített bizalmi szolgáltató külső, független rendszervizsgáló által folyamatosan ellenőrzött minőségirányítási és információbiztonsági rendszerrel rendelkezik.

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

- megfelelő nyilvántartásáról,
- ellenőrzéséről,
- védelméről.

5.2.1 Bizalmi szerepkörök

A jogszabályban rögzítettek alapján bizalmi munkakört betöltő személyek munkaviszonyban állnak a Minősített bizalmi szolgáltatóval. Bizalmi szerepkör betöltéséről a Minősített bizalmi szolgáltató naprakész nyilván tartást vezet és a változásokat jelenti az NMHH irányába.

Bizalmi pozíciót csak olyan személy tölt be aki:

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

Az általánosan felelős vezetői munkakört olyan személy tölti be, aki szakirányú felsőfokú végzettséggel és legalább három év informatikai szakmai gyakorlattal rendelkezik.

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

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.

Bizalmi munkakört betöltő személyt csak az ügyvezető jogosult kinevezni.

5.2.2 Az egyes feladatokhoz szükséges személyzeti létszámok

A Minősített bizalmi szolgáltató Információ Biztonsági Szabályzata előírja, hogy a Négy Szem Elvét betartva a védett környezetben, két, erre feljogosított személy egyidejű jelenlétében végezhetők el a következő műveletek:

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

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

Szintén két bizalmi szerepkört betöltő munkatárs együttes fizikai jelenléte szükséges az archiválási rendszerben tárolt titkosított dokumentumok visszafejtéséhez. Jelen szabályzat 5.2.2 pontjában felsorolt műveletek végrehajtása során a helyiségben illetéktelen személy tartózkodása tilos.

5.2.3 Az egyes szerepkörökhöz elvárt azonosítás és hitelesítés

A Minősített bizalmi szolgáltató informatikai rendszerét kezelő minden felhasználó egyedi azonosítóval rendelkezik, a biztonságos hitelesítését azonosítás érdekében. A felhasználók a kritikus informatikai rendszerekhez csak sikeres azonosítás és hitelesítés után férhet hozzá.

Azok a felhasználói adatok melyek a kritikus rendszerek hozzáférést és használatot teszik lehetővé a felhasználói jogosultságok megszűnésekor haladéktalanul inaktiválásra kerülnek. Az informatikai rendszer minden szereplője személy szerint kerül azonosításra. A fizikai hozzáférés ellenőrzéséhez a Minősített bizalmi szolgáltató mágneskártyára és ujjlenyomatra épülő beléptető rendszer által történik. Sikeres hitelesítés nélkül egyetlen kritikus feladatot sem lehet végrehajtani. Minden alkalmazott a munkakörének megfelelő hozzáférési jogosultsággal rendelkezik, amely a feladatköre ellátásához elengedhetetlenül szükséges. A személyzetet azonosításra és hitelesítésre kerül a szolgáltatások szempontjából kritikus alkalmazások használata előtt, és tevékenységükkel kapcsolatban elszámoltathatók.

További jogosultságokkal kapcsolatos tevékenységeket a Minősített bizalmi szolgáltató belső jogosultság szabályzó dokumentuma írja le.

5.2.4 Egymást kizáró szerepkörök

A jogszabályi követelmények megfelelően a Minősített bizalmi szolgáltató egyes munkatársai egyidőben akár több bizalmi szerepkört is betölthetnek, kivételt képeznek a következő pontok:

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

5.3 Személyzetre vonatkozó előírások

A Minősített bizalmi szolgáltató gondoskodik arról, hogy archiválási szolgáltatások megbízhatóságát a munkavállalói és szállítói támogassák. A bizalmi munkakörben foglalkoztatott munkavállalók minden olyan összeférhetetlenségtől menteséget a Minősített bizalmi szolgáltató biztosítja.

A személyzetnek az Informatikai Biztonsági Szabályzatban rögzített eljárások összhangban hajtódnak végre a vezetési és adminisztratív eljárásokkal

Az Információ Biztonsági Szabályzatban dokumentálva van a biztonsági munkakörök és felelősségek munkaköri leírásokban vagy más elérhető dokumentációban. A bizalmi munkakörök elvégzéséhez kapcsolódó tevékenységeket a Minősített bizalmi szolgáltató világosan definiált és betölt, amelyet a Minősített bizalmi szolgáltató és munkavállalója kölcsönösen elfogadott.

A munkavállalók (ide tartoznak egyaránt az állandóan és ideiglenesen alkalmazott munkavállalók is) olyan munkaköri leírásokkal rendelkeznek, amelyek a 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 alkalmazottja rendelkezik releváns szakmai végzettséggel, gyakorlattal és tapasztalattal, amelyek a betöltött munkakör ellátásához szükséges. Már a toborzás során a leendő dolgozók kiválasztásánál különös hangsúly fektet arra a Minősített bizalmi szolgáltató, hogy csak megbízható személyek vehetők fel a bizalmi szerepkörbe.

© 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 szolgáltató bizalmi munkakört betöltő munkatársak befolyásmentességét összeférhetetlenségi nyilatkozat aláírattatásával igazolja.

5.3.2 Biztonsági ellenőrzésre vonatkozó követelmények

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 szolgáltatónál bizalmi szerepkört kizárólag olyan személy tölthet be, aki legalább évente igazolni tudja büntetlen előéletét.

5.3.3 Képzési terv

A Minősített bizalmi szolgáltató új belépőit képzés által felkészíti arra, hogy elsajátítják az adott munkakör ellátásához szükséges kompetenciákat:

- a PKI 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 sajátosságai és kezelésének módjait

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

5.3.4 Továbbképzés gyakorisága

A továbbképzést kell tartani abban az esetben, ha a Minősített bizalmi szolgáltatói rendszerekben a használatot jelentősen megváltoztató változás történik.

A Minősített bizalmi szolgáltató legalább 12 havonta tájékoztatja a munkatársait, az elmúlt időszakban megváltozott eljárásokról, szabályokról.

5.3.5 Munkabeosztás körforgása

Munkabeosztásra vonatkozó körforgást a Minősített bizalmi szolgáltató nem alkalmaz.

5.3.6 Felhatalmazás nélküli tevékenységek szankciói

A Minősített bizalmi szolgáltató szankciót alkalmazhat, amelyet az elkövetés módjára és következményeire tekintettel állapít meg. Szankciók lehetnek:

- jutalom megvonása,
- fegyelmi eljárás,
- elbocsátás,
- kinevezés visszavonása,
- büntetőjogi felelősségre vonás kezdeményezése.

A bizalmi szerepkört betöltő személyzet kinevezéskor a foglalkoztatási dokumentumok részeként:

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

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

© 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.

5.3.7 Szerződéses jogviszonyra vonatkozó követelmények

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

A Minősített bizalmi szolgáltató által foglalkoztatott valamennyi szerződő fél a tényleges munkavégzés megkezdése előtt titoktartási nyilatkozatot írattat alá, melyben a Minősített bizalmi szolgáltatóval szerződött fél vállalja, hogy a munkavégzés során későbbiekben megismert üzleti/vállalati titkokat nem fedi fel, nem hasznosítja és egyéb módon nem továbbítja. A titoktartási nyilatkozat tartalmazza a megszegése esetén alkalmazandó szankciókat is. A szerződés alapján foglalkoztatott külső munkavállalókkal szemben elvárás a megfelelő szakismeret megléte.

5.3.8 Működést támogató dokumentációk

A Minősített bizalmi szolgáltató folyamatosan biztosítja a dolgozók részére a szerepkörük ellátásához szükséges aktuális dokumentációk, szabályzatok elérését. Minden a Minősített bizalmi szolgáltató által foglalkoztatott munkatárs írásban megkapja az alábbi dokumentumokat:

- a Minősített bizalmi szolgáltató Informatikai Biztonsági Szabályzata;
- aláírandó titoktartási nyilatkozat;
- egyéni munkaköri leírás;
- további oktatási segédanyagokat.

Az Informatikai Biztonsági Szabályzatban történő változásokról írásos formájában minden dolgozó kap tájékoztatást.

A Minősített bizalmi szolgáltató az Információ Biztonsági politikájában történő változásokról írásos formában rövid tájékoztatást ad:

- az ügyfelek,
- alvállalkozók,
- hatóság,
- más vele kapcsolatban álló harmadik fél részére.

5.4 A biztonsági naplózás folyamatai

A Minősített bizalmi szolgáltató az informatikai környezet biztonságos üzemeltetés vonatkozásában a teljes informatikai rendszert lefedő eseménynaplózó és ellenőrző rendszert használ.

A Minősített bizalmi szolgáltatónak minden lényeges naplóbejegyzést elérhetővé tesz a független rendszervizsgálók részére revízió céljából.

Minden naplóbejegyzésnél el tárolja az esemény vonatkozásában:

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

A napló fájloknak továbbá eltárolják a felhasználó vagy rendszer azonosítóját, aki/amely az eseményt kiváltotta.

A Minősített bizalmi szolgáltató dokumentálja a naplózott információk elérésének módjait és megőrzési idejét.

Az archiválási szolgáltatás kapcsán a Minősített bizalmi szolgáltató naplózza a következő eseményeket:

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

© 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 rögzíti és folyamatosan hozzáférhetővé teszi egy meghatározott ideig - a tevékenységének megszűnése utáni időszakban is a lényeges információt szolgáltatásfolyamatosság biztosítása céljából és a megfelelőségértékelés számára.

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

5.4.1 Tárolt események típusai

A Minősített bizalmi szolgáltató az általánosan elfogadott informatikai biztonsági gyakorlatnak megfelelően naplóz minden olyan eseményt, amely információt szolgáltathat az informatikai rendszerben történt eseményekről, változásokról.
Minden naplóbejegyzésnél eltárolja a következőket:

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
   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;

© 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.

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;
10. Törlés a rendszerben
   a. törlési igény kezdeményezése
   b. a fájlt egyedi titkosító kulcs lenyomatának törlése adatbázisból
   c. fájl fizikai törlése

Az összes lényeges naplóbejegyzést elérhetővé teszi a független rendszervizsgáló részére, aki a Minősített bizalmi szolgáltató működésének megfelelőségét vizsgálja.

5.4.2 A naplófájl feldolgozásának gyakorisága

A Minősített bizalmi szolgáltató független rendszervizsgálója a keletkezett naplóbejegyzéseket minden munkanapon átvizsgálja és kiértékeli. Ennek során meggyőződik, hogy a vizsgált naplóállományok hitelesek és sértetlenek. A bejegyzésekben talált hibaüzeneteket ellenőrzi, szükség esetén dokumentálja az eltérést és intézkedéseket javasol az ok megszüntetésére.

Az informatikai rendszerek ellenőrzésére a Minősített bizalmi szolgáltató automatizált ellenőrző rendszereket is használ, amelyek előre beállított szempontok szerint folyamatosan figyelik a keletkező naplóbejegyzéseket és szükség esetén riasztást küldenek.

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

5.4.3 A naplófájl megőrzési időtartama

A rendszerből való kitörlés előtt a naplóállományokat a Minősített bizalmi szolgáltató archiválja és gondoskodik azok biztonságos megőrzéséről. 10 évig a Minősített bizalmi szolgáltató biztosítja az archivált adatok olvashatóságát. Folyamatban lévő jogi eljárás esetén a lejáró időpontot követően az eljárás befejezéséig megőrzi.

5.4.4 A naplófájl védelme

A Minősített bizalmi szolgáltató a fent jelzett megőrzési ideig tárolja és védi a keletkezett naplóállományokat. A megőrzési idő teljes időtartama alatt biztosítja a naplóadatok:

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

A Minősített bizalmi szolgáltató a naplóbejegyzéseket időbélyegzővel látja el, a naplóbejegyzések törlés és más fájl módosítások észrevétlen végrehajtását kizáró módon kerülnek tárolásra.

A Minősített bizalmi szolgáltató a hozzáféréseket biztonságos módon ellenőrzi. A naplóállományokat a Minősített bizalmi szolgáltató biztonságos környezetben őrzi. Az állományokról a működés másodlagos helyszínén másolati példányokat is tart.

5.4.5 A naplófájl mentési eljárásai

Az üzemeltetés során az egyes rendszerekben folyamatosan keletkező naplóbejegyzésekből napi naplóállományok generálódnak. A napi naplóállomány SHA 256 függvénnyel generált lenyomatát a Minősített bizalmi szolgáltató két példányban archiválja és a példányokat egymástól fizikailag elkülönülő helyszíneken a fent előírt ideig megőrzi.

5.4.6 A naplózás adatgyűjtési rendszere

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.

5.4.7 Az eseményeket kiváltó Ügyfelek értesítése

Nincs előírás.

5.4.8 Sebezhetőség felmérése

A Minősített bizalmi szolgáltató havonta áttekinti a rendkívüli eseményeket és a sebezhetőségre vonatkozó elemzéseket végez, amely alapján a Minősített bizalmi szolgáltató szükség esetén intézkedéseket hozhat a rendszer biztonságának növelésére. Minden nagyobb jelentőségű feltárt hiányosság vagy külső fenyegetettség esetén az észlelésétől számított 48 órán belül, egyébként évente legalább egyszer a Minősített bizalmi szolgáltató átfogó sebezhetőség vizsgálatot végeztet, amely segítségével feltérképezik a potenciális belső és külső fenyegetettségeket. A vizsgálat eredményei alapján a Minősített bizalmi szolgáltató szükség esetén áttervezi és tovább fejleszti folyamatait és rendszereit a szolgáltatás biztonságának növelése értelmében.
A Minősített bizalmi szolgáltató negyedévente külső sebezhetőség felmérést végeztet, évente pedig penetrációs teszteket hajtat végre.

5.5 Adatok archiválása

A Minősített bizalmi szolgáltatóalábbi jellegű információkat archiválja:
- a szolgáltatás tanúsításával kapcsolatos valamennyi irat;
- az archiválási rend és archiválási szolgáltatási szabályzat valamennyi verziója;
- az általános szerződési feltételek valamennyi kibocsátott verziója;
- a szolgáltatás működésével kapcsolatos szerződések;
- valamennyi elektronikus és papíralapú naplóbejegyzés.

5.5.1 Az archiválandó adatok típusa

A Minősített bizalmi szolgáltatónak a szolgáltatással kapcsolatosan rendelkezésére álló információkat és az ahhoz kapcsolódó személyes adatokat őrzi meg. Melyek:

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

5.5.2 Adatok megőrzésének időpontartama

A Szolgáltatási szabályzatot és egyéb publikus besorolású szabályzó dokumentumait a hatályon kívül helyezéstől számított 10 évig a Minősített bizalmi szolgáltató megőrzi.

5.5.3 Az archívum védelme

A Minősített bizalmi szolgáltató valamennyi archivált adatot két példányban egymástól fizikailag elkülönült helyszínen őriz meg. Az archivált adatok megőrzése során a Minősített bizalmi szolgáltató gondoskodik az archivált adatok

- sértetlenségének megőrzéséről;
- illetéktelen megismerés elleni védelméről;
- 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 rögzíti és tárolja jelen pontban leírt folyamat alapján.

Az archivált elektronikus adatokat fokozott biztonságú elektronikus aláírással vagy bélyegzővel és időbélyegzővel látja el.

© 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 valamelyik minősített időbélyegzés-Minősített bizalmi szolgáltató által szolgáltatott időbélyegzőket használ a naplózott és az archiválandó fájlok hitelesítésére.

5.5.4 Archív információk hozzáférését és ellenőrzését végző eljárások

A Minősített bizalmi szolgáltató az automatikus naplózó rendszer alkalmazása esetén a hitelesített naplóállományokat naponta állít elő. Az Minősített bizalmi szolgáltató megvédi adatait a jogosulatlan hozzáféréstől. Az arra jogosultaknak biztosítja az archivált adatokhoz való ellenőrzött hozzáférését, amely a következő lehet:
- az Ügyfelek jogosultak a róluk tárolt adatok megtekintésére;
- jogi eljárásokban bizonyíték nyújtása céljából biztosítja a szükséges adatokat.

5.5.5 Az archívum mentési folyamatai

A naplófájl mentési eljárásai fejezetben írtak szerint kell eljárni.

5.5.6 Az adatok időbélyegzésére vonatkozó követelmények

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

5.5.7 Az archívum gyűjtési rendszere

Nincs előírás.

5.5.8 Archív információk hozzáférését és ellenőrzését végző eljárások

Nincs előírás.

5.6 Kulcscsere

Minősített bizalmi szolgáltatónak lecseréli hitelesítő kulcsát, amennyiben az általa alkalmazott kulcsai elavulnak.

Az új kulccsal kiállított új tanúsítvány esetében annak profilját és adatait az aktuális előírásokhoz és legjobb gyakorlathoz igazítja.

Minősített bizalmi szolgáltató lecseréli hitelesítő tanúsítványát amennyiben az lejár.

A Minősített bizalmi szolgáltató továbbá saját belátása szerint egyéb esetben is dönthet tanúsítvány és/vagy kulcscsere mellett.

5.7 Katasztrófa helyzet kezelés

A Minősített bizalmi szolgáltatónak megfelelő intézkedéseket hajt végre az archiválási szolgáltatás biztonságát fenyegető kockázatok kezelése érdekében. Figyelembe véve a legújabb technológiai fejleményeket továbbá biztosítja, hogy a kockázatok arányosak legyenek a biztonsági szinttel. A biztonsági események megelőzése és azok hatásának minimálárasára intézkedéseket tesz, valamint az érdekelteket tájékozgatással látja el, ha bármely káros esemény éri a Minősített bizalmi szolgáltatót.

A Minősített bizalmi szolgáltató késedelem nélkül minden esetben a káros esemény észlelésétől számított 24 órán belül értesíti az NMHH-t mint felügyeleti szervet és egyes indokolt esetekben más érintett szerveket, például az információbiztonságért felelős nemzeti szervet vagy az adatvédelmi hatóságot.

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 érintetteket.

© 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.

5.7.1 Váratlan esemény kezelési eljárások

A Minősített bizalmi szolgáltató rendelkezik üzletmenet folytonossági tervvel. Egy teljes értékű tartalékrendszert alakított ki és tart fenn, amely az elsődleges helyszíntől biztonságos távolságra, másik fizikai helyszínen található és az adatközpontok egyenként is alkalmasak az archiválási szolgáltatás egyes funkcióinak a kiszolgálására. Rendszeresen teszteli a redundáns alrendszer működését és évente felül vizsgálja az üzletmenet folytonossági terveit. Katasztrofális esemény bekövetkezte után a lehető leggyorsabb idő alatt helyre állítja a szolgáltatások elérhetőségét.

5.7.2 Meghibásodott IT erőforrások és/vagy adatok

A Minősített bizalmi szolgáltató az archiválási célt szolgáló informatikai rendszerei megbízható hardver és szoftver összetevőkből épül fel. Redundáns rendszerelemek alkalmazásával megvalósítja meg kritikus funkcióit úgy, hogy azok egyes elemei esetleges meghibásodása esetén is képesek a szolgáltatás bizonyos funkcióinak kiszolgálására. A Minősített bizalmi szolgáltató naponta teljes mentést készít az adatbázisairól és a keletkezett naplózási eseményekről. A kritikus rendszerkomponensek meghibásodásának esetén végrehajtandó pontos előírásokat és feladatokat üzletmenet folytonossági terv, hogy tartalmaz. A Minősített bizalmi szolgáltató a hiba elhárítása és a rendszer integritásának helyreállítása után a lehető leggyorsabb időn belül bocsátja rendelkezésre az archiválási szolgáltatást.

5.7.3 Magánkulcs kompromittálódása esetén követendő eljárás

A Minősített bizalmi szolgáltatói kulcsának kompromittálódása esetén a Minősített bizalmi szolgáltató

- tájékoztatja az Ügyfeleit, az Érintett feleket és a Bizalmi felügyeletet.
- jelezi, hogy az érintett Minősített bizalmi szolgáltatói kulccsal kibocsátott igazolások már nem érvényesek; és
- visszavonja 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

- tájékoztatja az Ügyfeleit, az Érintett feleket és a Bizalmi felügyeletet.
- visszavonja az érintett Minősített bizalmi szolgáltatói tanúsítványt.

5.7.4 Működés folyamatosságának biztosítása

A Minősített bizalmi szolgáltató meghatározza 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 lépteti a rendelkezéseket, hogy a szolgáltatások működése minél előbb az Ügyfelek rendelkezésére állhasson.

Amennyiben a rendkívüli üzemeltetési helyzet meghaladja a szolgáltatáskiesésre a bizalmi felügyelet ajánlásában[2] megállapított legfeljebb 3 naptári napot, Minősített bizalmi szolgáltató értesíti 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.

2 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.

5.8 A szolgáltatás leállítása

A Minősített bizalmi szolgáltató a szolgáltatások tervezett megszüntetése esetén legkevesebb 3 hónappal a szolgáltatás leállítás előtt informálja az Ügyfeleket és a Hatóságot. A szolgáltatás leállítására vonatkozó bejelentéssel egyidejűleg leállítja a következő szolgáltatásait:

- Új elektronikus dokumentumok befogadása az elektronikus archiválási rendszerbe.

A Minősített bizalmi szolgáltató a tervezett leállás előtt legalább 30 nappal felmondja a Szolgáltatási szerződéseket és felszólítja az Ügyfeleket a rendszerében archivált elektronikus dokumentumaik lementésére. A Minősített bizalmi szolgáltató a tervezett leállás előtt legalább 20 nappal leállítja a következő szolgáltatásait:

- Igazolások kiadása a dokumentumokról

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

- információ szolgáltatás,
- archívumban tárolt elektronikus dokumentumok letöltése.

A Minősített bizalmi szolgáltató a tervezett szolgálatatás megszűnés előtt tárgyalásokat kezd más vele azonos besorolású Minősített bizalmi szolgáltatókkal szolgáltatásainak átvételéről. Nyilvántartásait a bizalmas felhasználói adatokkal együtt átadja egy ilyen Minősített bizalmi szolgáltatónak, vagy megállapodás hiányában a NMHH-nak, egyéb szolgáltatásait a tárgyalások eredményétől függően átadja vagy átadás nélkül megszünteti. A Minősített bizalmi szolgáltató az Ügyfeleit elektronikus levélben, az más érintett felek tájékoztatását a honlapján történő közzététel útján informálja. A Minősített bizalmi szolgáltató a szolgáltatás befejezésekor az informatikai rendszerében foglalt adatairól teljes körű, időbélyegzővel ellátott mentést készít.

A szolgáltatás leállítását követően a Minősített bizalmi szolgáltató előre egyeztetett módon átadja az archivált fájlokat, aláírásokat, bélyegzőket és érvényességi láncokat az Ügyfeleknek, majd visszaállíthatatlanul törli azokat a rendszeréből.

Ha a Minősített bizalmi szolgáltató ellen jogerős határozat alapján felszámolási vagy végelszámolási eljárás indult, haladéktalanul tájékoztatja a NMHH-t e tényről, megnevezve az eljárást lefolytató szervezetet. A Minősített bizalmi szolgáltató a bizalmi szolgáltatás megszüntetésére belső eljárást rendszeresített: „NOTARchiv_arch_szolg_megszüntetese.pdf ” (OID: 1.3.6.1.4.1.54136.1.1.2.16.x.x[3])

[3] Az OID azonosító utolsó két x-el jelölt karaktere az aktuálisan hatályban lévő eljárás verzió számait jelzi.

© 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 intézkedéseket eszközöl az adathamisítás és az adatlopás ellen; ezért megbizonyosodva arról, hogy az archív szolgáltatásnyújtáshoz - a kriptográfiai kulcsok az alkalmazott rendszerekben a teljes életciklus alatt megbízhatóak és a módosítás ellen védettek.

A Minősített bizalmi szolgáltató a Minősített bizalmi szolgáltatói kriptográfiai kulcsokat a teljes életciklus alatt megfelelő tanúsítással rendelkező kriptográfiai HSM eszközökben kezeli.

6.1 Kulcspár generálás és telepítés

6.1.1 Kulcspár előállítása

Minősített bizalmi szolgáltatónak a Minősített bizalmi szolgáltatói kulcsokat védett generálja és a magánkulcsok bizalmasságáról gondoskodik.
A Minősített bizalmi szolgáltatói kulcsok generálására vonatkozóan az alábbiakat követi:

- A kulcsok generálását fizikailag védett környezetben történik 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 kerülnek használatba, amely megfelel a célra vonatkozó szabványoknak, a Hatóság engedélyezett algoritmusokra és minimális kulcsméretekre vonatkozó határozatának.
- Csak olyan kriptográfiai modulok kerülnek alkalmazásra, amelyek megfelelnek a Minősített bizalmi szolgáltató szabályzataiban nyilvánosságra hozott műszaki és egyéb követelményeknek. A kulcsok nem importálhatók olyan eszközökbe, amelyek az alkalmazásra vonatkozó elvárásokat nem teljesítik.
- Az alkalmazott algoritmusok a Szolgáltatási szabályzatban feltüntetésre kerülnek.
- Minősített bizalmi szolgáltatónak forgatókönyvvel rendelkezik 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 Minősített bizalmi 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. Ezt a Minősített bizalmi szolgáltató megbízható módon juttatja el a tanúsítvány kiadására.

6.1.4. A Minősített bizalmi szolgáltatói nyilvános kulcs közzététele

A Minősített bizalmi szolgáltató a Minősített bizalmi szolgáltatói nyilvános kulcsot a weboldalán közzé teszi,

6.1.4 Kulcsméretek

A 6.1.1 fejezetben megfogalmazott előírások az irányadók.

6.1.5 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

A Minősített bizalmi szolgáltató a birtokában lévő magánkulcsok biztonságos kezeléséről gondoskodik. A magánkulcsok felfedését, lemásolását, törlését, módosítását, jogosulatlan használatát megakadályozza. A Minősített bizalmi szolgáltató a kriptográfiai HSM eszközökben tárolt használatból kivont magánkulcsokat törli az eszköz használati útmutatójában meghatározott módon, ezen akció után gyakorlatilag lehetetlen a kulcsok visszaállítása.

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

Minősített bizalmi szolgáltatónak elkülönítve kezelni és működteti a szolgáltatás nyújtásához használt bizalmi szolgáltatást megvalósító termékeit az egyéb tevékenységeihez használt termékektől.

A Minősített bizalmi szolgáltató által használt kulcstároló, kulcsgeneráló és aláíró eszközök az alábbiak lehetnek:

Eszköz	**Hardware és firmware specifikáció**
Minősített bizalmi szolgáltatói kulcsok eszköze	HSM gyártó: Thales e-Security HSM modell megnevezése: nShield Connect 500+ Éles rendszeren használt HSM firmware verzió: v11.72.02 HSM firmware cert link: https://www.acn.gov.it/portale/documents/20119/915264/ac_rda_eidas_nshield_v1.0.pdf/30bb02fd-bc19-ac70-d15f-49a6c6c915b9?t=1749546048803
Minősített bizalmi szolgáltatói kulcsok eszköze	HSM gyártó: ENTRUST (korábban: Thales e-Security) HSM modell megnevezése: nShield Connect 500+ Éles rendszeren használt HSM firmware verzió: v11.72.03 HSM firmware cert link: https://www.acn.gov.it/portale/documents/20119/914698/ac_rda_eidas_nshield_2019_v1.0.pdf/19586dc4-908e-c5b0-6212-f6f2ce335b95?t=1749546055060
Minősített bizalmi szolgáltatói kulcsok eszköze	HSM gyártó: I4P-informatikai Kft. HSM modell megnevezése: Trident version 3.1.3 Éles rendszeren használt HSM firmware verzió: v3.1.3 HSM firmware cert link: https://www.acn.gov.it/portale/documents/20119/913657/ac_rda_eidas_trident_313_v1.1.pdf/729d6208-9013-5ba1-a709-0e40e0779e97?t=1749546068466

© 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.

6.2.2 Magánkulcs használata

A Minősített bizalmi szolgáltató biztosítja, hogy a szolgáltatáshoz használt magánkulcsaival végzett akciók végrehajtásához legalább két bizalmi szerepkört betöltő személy jelenlétében valósítja meg.

6.2.3 Magánkulcs letétbe helyezése

A Minősített bizalmi szolgáltató az aláíró magánkulcsait nem helyezi letétbe.

6.2.4 Magánkulcs mentése

A Minősített bizalmi szolgáltató másolatokat készít a Minősített bizalmi szolgáltatói magánkulcsokról, ebből minimum egyet a szolgáltatás nyújtás telephelyétől eltérő földrajzi helyszínen tárol el az üzletmenet folytonosság biztosítása vonatkozásában. A biztonsági másolatok készítése csak védett környezetben, a bizalmi szerepkört betöltő személyek közül legalább két fő jogosult jelenlétében történik.

6.2.5 Magánkulcs archiválása

A Minősített bizalmi szolgáltató az aláíró magánkulcsait nem archiválja.

6.2.6 Magánkulcs import és export

A Minősített bizalmi szolgáltató valamennyi magánkulcsát a fenti követelményeknek megfelelő HSM kriptográfiai cél hardver eszközben állítja elő. Nyílt formában a magánkulcsok nem létezhetnek a kriptográfiai hardveren kívül. A magánkulcsot a Minősített bizalmi szolgáltató csak akkor exportálja, ha biztonsági másolat készít a kriptográfiai eszköz vonatkozásában.

6.2.7 Magánkulcs tárolása hardware kriptográfiai eszközben

A Minősített bizalmi szolgáltató az archiválási szolgáltatáshoz használt magánkulcsait kriptográfiai HSM modulban tárolja. A magánkulcs tárolására használt HSM kriptográfiai cél hardveren belül a tárolási formára vonatkozó előírás a mindekori kriptográfiai eszköz kezelési útmutatójában van feltüntetve.

6.2.8 Magánkulcs aktiválása

A Minősített bizalmi szolgáltató a magánkulcsait a felhasznált HSM kriptográfiai eszközön a tanúsítási dokumentumokban megfogalmazott eljárásoknak és a felhasználói útmutatójában leírtak alapján aktiválja.

6.2.9 Magánkulcs deaktiválása

A Minősített bizalmi szolgáltató a magánkulcsait a használt HSM kriptográfiai eszközön a tanúsítási dokumentumokban megfogalmazott eljárásoknak és a felhasználói útmutatójában leírtak alapján deaktiválja.

6.2.10 Magánkulcs megsemmisítése

A Minősített bizalmi szolgáltató a lejárt érvényességű, funkcióját vesztett és kivezetett magánkulcsait a Minősített bizalmi szolgáltató megsemmisíti, hogy lehetetlenné tegye a magánkulcs további használatát. A megsemmisítést a kriptográfiai HSM modul felhasználói útmutatójában leírt eljárásoknak megfelelően végzi el.

A magánkulcsról készült minden mentett példányt dokumentált módon a Minősített bizalmi szolgáltató visszaállíthatatlanul semmisíti meg. A Minősített bizalmi szolgáltató két bizalmi szerepet munkatársának együttes jelenlétében végzi el a műveletet.

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 CERT 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

© 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.

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 használt kulcsok nem használhatók semmilyen más célra.

6.4 Aktivizáló adatok

6.4.1 Aktivizáló adatok előállítása és alkalmazása

A Minősített bizalmi szolgáltató által használt kriptográfiai HSM modul felhasználói útmutatójában megfogalmazott eljárásoknak megfelelő aktiváló módszereket alkalmaz a magánkulcsainak védelmére. Jelszó alapapján aktivizáló adatok használata esetén a jelszavaknak kellően hosszúak és komplexek melynek kritériumai a Minősített bizalmi szolgáltató saját Információ Biztonsági Szabályzatban van rögzítve.

6.4.2 Az aktivizáló adatok védelme

A Minősített bizalmi szolgáltató alkalmazottai a magánkulcsok aktiválásához szükséges eszközöket, aktivizáló adatokat biztonságosan kezelik, a jelszavakat csak kódolt formában tárolják.

6.5 Informatikai biztonsági előírások

6.5.1 Speciális informatikai biztonsági műszaki követelmények

A Minősített bizalmi szolgáltató informatikai rendszereinek az következő követelmények teljesülését biztosítja az üzemeltetés során:

- a rendszerhez való hozzáférés engedélyezése előtt a felhasználói azonosítást ellenőríz;
- különböző felhasználókhoz különböző szerepköröket párosít,
- minden felhasználó csak a szerepkörének megfelelő jogosultságokkal rendelkezik;
- minden tranzakcióról naplóbejegyzést állít elő és azokat archiválja is;
- biztosítja azt, hogy kellően védettek a rendszerek és a Minősített bizalmi szolgáltató belső hálózata a jogosulatlan hozzáféréstől;
- olyan eljárásokat alkalmaz, melyek megfelelően tudnak reagálni a kulcsvesztés vagy rendszerhiba után a szolgáltatás visszaállítása érdekében.

6.5.2 Az informatikai biztonság ellenőrzése

Az adat és információ biztonság minőségi szolgáltatás nyújtása érdekében a Minősített bizalmi szolgáltató nemzetközileg elfogadott szabványok és módszertanok alapján felépített információ biztonsági és minőség irányítási rendszert alkalmaz, ezek megfelelőségét független tanúsító szervezet által kiállított tanúsítvánnyal is igazolja.

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

Megbízható és megfelelő szaktudással rendelkezők alkalmazottakkal kivitelezteti a szoftverek és más eszközök telepítését. A Minősített bizalmi szolgáltató csak a szolgáltatás nyújtás 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.

telepítheti a szoftvereket az informatikai berendezéseire. A Minősített bizalmi szolgáltató olyan eljárásokat alkalmaz, melyek a jogosulatlan változás észlelésére alkalmasak.

6.6.2 Biztonságkezelési eljárások

A Minősített bizalmi szolgáltató rendelkezik olyan dokumentált információkkal, amelyekben rögzítve vannak a szolgáltatásban használt:

- rendszer telepítések,
- konfigurációjának specifikációja,
- üzemeltetése,
- ellenőrzése, monitorozása és karbantartása,
- beleértve a módosításokat és továbbfejlesztéseket is.

A változáskövető funkciók észlelik a szolgáltatást nyújtó rendszerben történt bármilyen jogosulatlan hozzáférést, adatbevitelt, amely érinti a szolgáltatásban használt rendszer szoftveres és hardveres összetevőket. A Minősített bizalmi szolgáltatói rendszereiben használt programok integritását a Minősített bizalmi szolgáltató rendszeresen ellenőrzi.

6.7 Életciklusra vonatkozó biztonsági előírások

A Minősített bizalmi szolgáltatónak gondoskodik a felhasznált kriptográfiai HSM modulok védelméről azok teljes életciklusa alatt.

- Megfelelő tanúsítással rendelkező HSM-et használ.
- A HSM átvételekor meggyőződik arról, hogy a szállítás során biztosították az eszközök feltörés elleni védelmét.
- A tárolás során biztosítja a HSM feltörés elleni védelmét.
- Az üzemeltetés során folyamatosan betartja és betartatja a HSM, használati útmutatójában és a tanúsítási dokumentációban szereplő követelményeket.
- A Minősített bizalmi szolgáltató a használatból kivont kriptográfiai HSM eszközökben tárolt magánkulcsokat visszaállíthatatlanul törli.

6.8 Hálózati biztonsági előírások

Az alkalmazott IT rendszereinek konfigurációját, minden változást, beleértve a legkisebb módosítást, fejlesztést, szoftverfrissítést is dokumentál a Minősített bizalmi szolgáltató. Az IT rendszereiben a Minősített bizalmi szolgáltató megfelelő eljárásokat használ a bekövetkezett hardver vagy szoftver változás monitorizálása vonatkozásában. Minden szoftverkomponens első integrálásakor a Minősített bizalmi szolgáltató ellenőrzi az eredetiségét. A Minősített bizalmi szolgáltató megfelelő hálózatbiztonsági intézkedéseket alkalmaz, mint például:

- letiltja a használaton kívüli hálózati portokat és szolgáltatásokat;
- letiltja a nem használt felhasználókat és hálózati protokollokat,
- csak az informatikai rendszer megfelelő működéséhez feltétlenül szükséges hálózati alkalmazásokat futtat.

A Minősített bizalmi szolgáltatónak sérülékenységvizsgálatot végeztet a használatos nyilvános és privát IP címein:

- minden nagyobb hálózattechnikai változtatás után
- legalább évente.

© 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 Tanúsítványprofil, megőrzési profil

Az arciválás tanúsítványai minősített bélyegző profillal rendelkeznek.

7.1 Megőrzési profil – Megőrzés aláírással és kiterjesztéssel, tárolással

A megőrzési profil szabványos az ETSI TS 119512 séma (szabvány link: https://www.etsi.org/deliver/etsi_ts/119500_119599/119512/01.01.02_60/ts_119512v010102p.pdf) minta alapján készült profil leírás, annak minden kötelező tartalmával, és kiegészítő magyarázatokkal az értelmezéshez.
A Minősített bizalmi szolgáltató a minősített megőrzési policy-t (CP-t) támogatja, melynek szabványos azonosítója: 0.4.0.19511.1.2

A támogatott megőrzési profilokat a szolgáltatási jelen szabályzat tartalmazza.

A működés paramétereinek leírása:
Dokumentum feltöltésekor a rendszer megvizsgálja a visszavonási információk jelenlétét, és ha hiányzik, akkor megpróbálja kiegészíteni az állományt.
A kiterjesztéssel maximum az ajánlott 3 napig próbálkozik, ezt követően elutasítja az állomány befogadását.
A rendszer befogadásról visszagazolást küld.
A Minősített bizalmi szolgáltató a dokumentumokba ágyazza a felülhitelesítési információkat, így a letöltött dokumentum tartalmazza az evidenciát is, külön exportálásra (evidenciákkal) nincs szükség, a letöltött állomány másik Minősített bizalmi szolgáltató által befogadható, más Minősített bizalmi szolgáltatótól a kiterjesztett állomány standard feltöltéssel teljesíthető, így export-importot a Minősített bizalmi szolgáltató a standard eléréseken biztosít.

A megőrzési profil azonosítója:

http://uri.notarchiv.hu/19512/profile/pds+wst+aug/1

7.1.1 A profil hatálya

A profil hatályának kezdő dátuma: Jelen szabályzat hatályba lépésének dátuma
A profil hatályának vég dátuma: záró dátum jelenleg nincs

7.1.2 Séma Azonosító

A megőrzési séma azonosítója:

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

7.1.3 Megőrzési célok

A megőrzési séma a következő célokat támogatja:

- digitális aláírások kiterjesztése hosszú távra, amelynek az azonosítója:

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

- a beküldött bizonyítékok kiegészítése, amelynek az azonosítója:
  http://uri.etsi.org/19512/goal/aug

A célok megvalósulását lásd a megőrzési bizonyítékok generálásáról szóló fejezetben.

© 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.

7.1.4 Megőrzési tárolási modell

A tárolási modellje a támogatott sémának: tárolással

A tárolási modell azt jelenti, hogy a beküldött adat objektumok és a megőrzési bizonyítékok, amit a megőrzési Minősített bizalmi szolgáltató tárolt hozzájuk, egyaránt a megőrzési Minősített bizalmi szolgáltató által tárolt.

Ez a szolgáltatási modell támogatja a megőrzendő objektumok és bizonyítékok fel- és letöltését.

A PreservationStorageModel értéke WithStorage (WST).

7.1.5 Megőrzési profil változtatási eljárása

Az érvényben lévő archiválási profil ugyanaz a teljes megőrzési idő alatt. Az archiválási profil időben állandó, minden változó paraméter az archiválási profilon kívül kerül meghatározásra. Adott archiválási profilhoz tartozó valamennyi rend verzió nyilvánosan elérhető.

7.1.6 Támogatott műveletek

A támogatott műveltek két csoportra oszthatók. A kötelezően megvalósítandó és az opcionális műveletek. A Minősített bizalmi szolgáltató ezek mindegyikét támogatja.

7.1.6.1 Kötelező műveletek

A Minősített bizalmi szolgáltató a következő kötelező műveleteket támogatja:

- Feltöltés (PreservePO)
  A kliens azonosítást követően megbízható csatornán keresztül megőrzésre tárolja dokumentumát, mely - ha szükséges kiegészítésre, majd ezt követően – megőrzésre kerül. A sikeres műveletre azonosító érkezik.
- Letöltés (RetrievePO)
  A kliens azonosítást követően megbízható csatornán keresztül letölti tárolt dokumentumát, és ezzel együtt bizonyítékait.
- Törlés (DeletePO)
  A kliens azonosítást követően megbízható csatornán keresztül törlésre jelöli tárolt dokumentumát, és ezzel együtt bizonyítékait, amely végrehajtódik.

7.1.6.2 Opcionális műveletek

A Minősített bizalmi szolgáltató a következő opcionális műveltet támogatja:

- Bizonyíték letöltése (RetrieveTrace)
  Megvalósul a dokumentum Letöltéssel (RetrievePO) , mert digitálisan aláírt dokumentum tartalmazza a bizonyítékot is.
- Validálás (ValidateEvidence)
  Az igazolások kiállításához szükséges a validálás, így támogatott a művelet.
- Keresés (Search)
  A dokumentumok között lehetőség van keresni különféle adataik alapján.

7.1.7 A megőrzési bizonyítékok generálása és ellenőrzése

A szolgáltatás kiterjeszti az aláírást a következő megfelelő aláírás formátumokra:

- XADES archív időbélyeg

© 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.

Azonosítója:
`http://uri.etsi.org/ades/XAdES/ArchiveTimeStamp`

- PADES archív időbélyeg
  Azonosítója:
  `http://uri.etsi.org/ades/PAdES/document-time-stamp`

A megőrzési szolgáltatás ellenőrzi, hogy minden adat a validáláshoz rendelkezésre áll-e, és ha nem, akkor hozzáadja azt, majd védi egy megfelelő időbélyeggel a megfelelő aláírás formátumban. A megőrzési Minősített bizalmi szolgáltató olyan hash algoritmust választ, ami tudomány aktuális szintjén védi a validációs adatot, az aláírást, és az aláírt adatot.

Csak a teljes visszavonási listával rendelkező, vagy azzal kiegészített dokumentumok befogadhatók, mert csak ekkor áll rendelkezésre minden információ, amivel a hosszú távú ellenőrizhetőség megvalósítható.

A bizonyíték a támogatott formátumokban az aláírásba beágyazott.
A vonatkozó szabvány leírja a bizonyítékok ellenőrzésétnek lépéseit.

7.1.8 A megőrzési bizonyítékok kiterjesztése

Az elfogadható kriptográfia algoritmusok monitorozása alapján (ETSI TS 119 312) a Minősített bizalmi szolgáltató kiterjesztést hajt végre a megadott bizonyíték formátumban.

7.1.9 Megőrzési bizonyíték szabályok

A bizonyítékok előállításhoz használt minősített időbélyeg Minősített bizalmi szolgáltató:

- MICROSEC Zrt.

A bizalom gyökere: EU Trust list
A Minősített bizalmi szolgáltató által aláírásra/bélyegzésre használt minősített aláíró/bélyegző tanúsítvány kiadója:

- MICROSEC Zrt.

A bizalom gyökere: EU Trust list

7.1.10 Aláírás ellenőrzési szabályok

A befogadásra küldött állományokon található aláírásokat és visszavonási információkat a Minősített bizalmi szolgáltató az állományra releváns PADES, XADES szabványok szerint ellenőrzi, amely alapvetően lánc modell.
Ha a visszavonási információk a megőrzéshez nem elégségesek a Minősített bizalmi szolgáltató megpróbálja beszerezni azokat.
A bizalom gyökere: EU Trust list.

7.1.11 Archiválási bizonyítékok létrehozása

A Minősített bizalmi szolgáltató az elektronikus aláírások érvényességének hosszú idejű megőrzését a tárolt elektronikus aláírások rendszeres kiterjesztésével valósítja meg. Az érvényesség kiterjesztése során az elektronikus aláíráson egy archív Időbélyegzőt helyez el, amely további évekre biztosítja a megőrzött eredeti elektronikus aláírás érvényességének ellenőrizhetőségét.

Az archiválási bizonyíték létrehozása során a Minősített bizalmi szolgáltató ellenőrzi az adott elektronikus aláírás, bélyegző vagy időbélyegző érvényességét. A Minősített bizalmi szolgáltató az elektronikus aláírás, bélyegző vagy Időbélyegző vizsgálata során az érvényességi láncot visszavezeti egy általa elfogadott hitelesítés- (vagy időbélyegzés-) Minősített bizalmi szolgáltató megbízható gyökér- vagy Minősített bizalmi szolgáltatói köztes tanúsítványára.

© 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.

7.1.12 Archiválási bizonyítékok érvényességének ellenőrzése

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

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

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

7.1.13 Elektronikus aláírás és bélyegző megőrzése

A Minősített bizalmi szolgáltató csak érvényes elektronikus aláírással vagy bélyegzővel rendelkező fájlokat fogad be. A Minősített bizalmi szolgáltató felhasználhatja az Előfizető által feltöltött bizonyítékokat, de ebben az esetben meggyőződik róla, hogy a biztosított bizonyíték megfelel az archiválási profil által támogatott aláírás ellenőrzési rend követelményeinek. Az elektronikus aláírás és bélyegző érvényesíthetőségének és az érvényességének fenntartása érdekében a Minősített bizalmi szolgáltató archív Időbélyegzőt helyez az elektronikus aláírásra vagy bélyegzőre.

7.1.14 Archiválási bizonyítékok frissítése

A Minősített bizalmi szolgáltató folyamatosan nyomonköveti a használt kriptográfiai algoritmusok megfelelőségét a következő dokumentumok alapján: -

- ETSI TS 119 312 ;

A megfigyelési eredmények alapján a Minősített bizalmi szolgáltató az aláírás kiterjesztését hajtja végre új archív Időbélyegző elhelyezésével a fájlokon.

© 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 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.

A minősített bizalmi szolgáltató a megfelelőségértékelő szervezetek által végzett auditok előtt legalább egy hónappal tájékoztatja a Hatóságot a tervezett ellenőrzésekről, és kérésre lehetővé kell tenni a Hatóság megfigyelőként való részvételét az auditon.

Az átvizsgálás során megállapításra kell kerülnie, hogy a Minősített bizalmi szolgáltató működése megfelel-e az eIDAS Rendeletben 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 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers;
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General
- Policy Requirements for Trust Service Providers.
- ETSI TS 119 511 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 honlapján megfelelőségi tanúsítványt közzé teszi a Minősített bizalmi szolgáltató.

A Minősített bizalmi szolgáltató rendelkezik az ISO 9001 szabványnak megfelelő minőségirányítási és az ISO/IEC 27001-nek megfelelő információbiztonsági tanúsítvánnyal, amelyeket külső szervezet auditál és folyamatosan felül vizsgál.

8.1 Az ellenőrzések gyakorisága

A Minősített bizalmi szolgáltató évente egy alkalommal saját belső önellenőrzéseket végez, amely segítségével

rendszeresen felülvizsgálja a Szolgáltatási Rendnek és jelen Szabályzatnak, valamint a korábbi auditoknak és értékeléseknek való megfelelőségét; eltérés esetén pedig megteszi a szükséges lépéseket.

Az auditorral szembeni elvárások

A Minősített bizalmi szolgáltató a belső auditokat elvégezheti a független rendszervizsgáló biztonsági besorolással felruházott alkalmazottjának segítségével.

Az EU akkreditációs szervezete által felhatalmazott szervezet végezheti el az eIDAS követelményeknek való megfelelőség tanúsítását.

8.2 Az auditor és az auditált függetlensége

A külső auditot csak olyan egyén végezhet el:

- 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.

8.3 A vizsgálat által érintett területek

Az átvizsgálásnak az az alábbi pontokat veszi a hatálya alá:

- 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;
- információ biztonsági és adatvédelmi szabályok betartása.

8.4 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.

8.5 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 audit időszakot 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 teszi közzé.

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

A Minősített bizalmi szolgáltató a törvényben előírt garanciális és e-kereskedelemre vonatkozó előírások alapján térít vissza, egyedi kérelem alapján.

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 Minősített bizalmi szolgáltató korlátozhatja a felelősségvállalása értékét, az ügyfeleket és érintett feleket a weboldalán keresztül tájékoztatva.

9.2.1 Biztosítási fedezet

A Minősített bizalmi szolgáltató rendelkezik felelősségbiztosítással.
A felelősségbiztosításnak ki kell terjedni a Minősített bizalmi 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 foglalt kötelezettségek nem teljesítése miatt a bizalmi felügyeletnél felmerült, az 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 Minősített bizalmi 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 rendelkezik:

- 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.

© 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.

Kezességet vállaló társaság adatai:
A cég elnevezése: Közjegyzői Akadémia Nonprofit Korlátolt Felelősségű Társaság (továbbiakban: Közjegyzői Akadémia)
A cég rövidített elnevezése: Közjegyzői Akadémia Nonprofit Kft.
Cégjegyzékszám: 01-09-175411 Fővárosi Törvényszék Cégbírósága
Adószám: 24649472-2-42
Székhely:1087 Budapest, Stróbl Alajos utca 3/b.

A Közjegyzői Akadémia tudomással bír az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2023. évi CIII. törvény (DÁP) 93. § (1) bekezdésében meghatározott, a NOTARchiv Kft.-t terhelő kötelezettségekről, valamint annak lehetséges biztosítékait szabályozó, A bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről szóló 24/2016. (VI. 30.) BM rendelet szabályaival.

A Közjegyzői Akadémia kijelenti, hogy a 24/2016. (VI. 30.) BM rendelet 22. §-ában rögzített feltételeknek maradéktalanul megfelel, kijelenti továbbá, hogy a 24/2016 BM rendelet 20,21. §-aiban foglalt, mint garancia vállaló kész készfizető kezességi kötelességét 25 000 000 (huszonötmillió) forintig terjedően határidőre törleszteni a Nemzeti Média- és Hírközlési Hatóság felé.

9.3 Bizalmasság, adatvédelem

A Minősített bizalmi szolgáltató az Ügyfél által rendelkezésre bocsájtott adatokat a mindenkori jogszabályoknak megfelelően kezeli. A Minősített bizalmi szolgáltató rendelkezik adatkezelési tájékoztatóval (lásd 8.4 fejezet), amely a személyes adatok kezelésével kiemelten foglalkozik.

A Szerződés aláírásával az Ügyfél beleegyezik, hogy a személyes adatait a Minősített bizalmi szolgáltató tárolja, kezelje és kizárólag az archiválási szolgáltatásaival összefüggésben használja fel.

A Minősített bizalmi szolgáltató gondoskodik a nem nyilvános személyes adatok biztonságáról és sértetlenségéről.

9.3.1 Bizalmas információk köre

A Minősített bizalmi szolgáltató bizalmas információként kezeli:
- az Ügyfél adatait kivéve a nyilvános forrásban is meglévő adatokat,
- az Ügyfél archivált dokumentumait,
- nem nyilvános szabályzatokat,
- napló és tranzakciós adatokat.

9.3.2 Bizalmas információk körén kívül eső adatok

A Minősített bizalmi szolgáltató nyilvánosnak tekint miden olyan adatot, amely nyilvánosságra hozatalához az Ügyfél írásban hozzájárult, vagy amely nyilvánosan elérhető forrásból is beszerezhető.

9.3.3 Bizalmas információk védelme

A bizalmas adatok védelmére a Minősített bizalmi szolgáltató szerződésbe foglalva vagy titoktartási nyilatkozat aláírásával kötelezi munkavállalóit és szerződött partnereit. A Minősített bizalmi szolgáltató a birtokába került bizalmas adatokat az szóló 2011. évi CXII. törvény rendelkezéseinek megfelelően kezeli, amely információs önrendelkezési jogról és az információszabadságról szól.

Kizárólag az alábbi esetekben fedi fel azokat:
- A tulajdonos írásos, hivatalos kérésére történő továbbítás vagy felfedés
- NMHH vagy egyéb hatósági szerepet betöltő szervezet részére történő információ szolgáltatás jogszabályban előírt pontok alapján.

9.4 Személyes adatok védelme

A Minősített bizalmi szolgáltató az Ügyfélről nyilvántartott személyes adatokat és információkat a magyar és EU által elfogadott jogszabályi előírásoknak megfelelően megőrzi és törli azokat.

© 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 törlés történhet:
- az Ügyfél kimondottan írásos törlési kérelmére,
- a Szerződés lejárta következtében.

A Minősített bizalmi szolgáltató kifejezetten akkor továbbítja az Ügyfél adatait harmadik fél számára:

- A DÁP 94. § szerinti kötelező adatszolgáltatás a bizalmi felügyelet részére; a Minősített bizalmi szolgáltató az adatszolgáltatás során is biztosítja az adatok bizalmasságát, azok valódiságát és hiánytalanságát.

9.4.1 Adatkezelési tájékoztató

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

9.4.2 Személyes adatok

A Minősített bizalmi szolgáltató megvédi az Ügyfél azon személyes adatait, amelyek nem érhetőek el nyilvános forrásból. A Minősített bizalmi szolgáltató csak annyi adatot igényel az Ügyféltől amennyi a szolgáltatásai nyújtásához szükséges.

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

A Minősített bizalmi szolgáltató az adatokat megfelelő intézkedésekkel védi különösen:
- a jogosulatlan hozzáférés,
- megváltoztatás,
- továbbítás,
- nyilvánosságra hozatal ellen.

9.4.5 Személyes adatok felhasználása

A Minősített bizalmi szolgáltató csak az archiválási szolgáltatás nyújtásához kapcsolattartás céljából használhatja fel az Ügyfél személyes adatait.

9.4.6 Adatkezelés

A Minősített bizalmi szolgáltatói értesítés nélkül az Ügyfélről tárolt személyes adatokat csak a vonatkozó jogszabályok által meghatározott esetekben adhat ki (pl: NMHH vagy egyéb hatósági szerepet betöltő szervezet részére).
A bizalmi Minősített bizalmi szolgáltató az általa nyújtott bizalmi szolgáltatások felhasználásával elkövetett bűncselekményekkel kapcsolatos büntetőeljárás lefolytatása céljából, vagy nemzetbiztonsági érdekből - az érintett személyazonosságát igazoló, valamint a 82. § alapján egyeztetett adatok tekintetében - az adatigénylésre külön törvényben meghatározott feltételek teljesülése esetén díjmentesen adatokat továbbít a nyomozó hatóságnak, az ügyészségnek, a bíróságnak és a nemzetbiztonsági szolgálatoknak. Az adatátadás tényét rögzíteni kell, az adatátadásról a bizalmi Minősített bizalmi szolgáltató az igénybe vevőt nem tájékoztathatja. A bizalmi Minősített bizalmi szolgáltató az ezen kötelezettségeknek haladéktalanul köteles eleget tenni, és az adatok továbbítását nem kötheti egyéb feltételekhez, így különösen az adatszolgáltatás költségeiben való megállapodáshoz vagy a költségek előlegezéséhez.

9.4.7 Egyéb adatvédelmi követelmények

Minősített bizalmi szolgáltató által nyújtott bizalmi szolgáltatás felhasználásával elkövetett bűncselekmények felderítése vagy megelőzése céljából, illetve nemzetbiztonsági érdekből - az érintett személyazonosságát igazoló, valamint egyeztetett adatok tekintetében - az adatigénylésre külön törvényben meghatározott feltételek teljesülése esetén díjmentesen adatokat továbbít a nyomozó hatóságnak, illetve a nemzetbiztonsági szolgálatnak. .

© 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.

9.5 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 szolgáltatás igénybevételéhez biztosított szoftverek Minősített bizalmi szolgáltató általi használatának szabályait a szoftver leírásában vagy felhasználói útmutató tartalmazza.

9.6 Felelősség és helytállás

9.6.1 A Minősített bizalmi szolgáltató felelőssége és helytállása

A Minősített bizalmi szolgáltató felel 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. a szerződésszegésért való felelősség szabályai szerint felelős;
- a Minősített bizalmi szolgáltató a vele szerződéses jogviszonyban nem álló harmadik személlyel szemben a Ptk. általános felelősségi szabálya szerint felelős.

9.6.2 Az ügyfél felelőssége és helytállása

Az Ügyfél felelősségét a Szolgáltatási szerződés mellékletei határozzák meg.

A bizalmi szolgáltatási ügyfél haladéktalanul tájékoztatja a bizalmi Minősített bizalmi szolgáltatót.

- a bizalmi szolgáltatással kapcsolatban észlelt, a külön jogszabályban, szolgáltatási szerződésben, illetve szolgáltatási szabályzatban meghatározott rendellenességről vagy más, a bizalmi szolgáltatást érintő eseményről, így különösen arról, ha a bizalmi szolgáltatás használatához szükséges, a bizalmi Minősített bizalmi szolgáltató által biztosított kriptográfiai vagy más biztonsági eszközt jogosulatlan személy használhatta;
- a bizalmi szolgáltatással kapcsolatos jogvita megindulásáról.

Az érintett fél felelőssége

Az Minősített bizalmi szolgáltató által garantált biztonsági szint megtartásához szükséges, hogy az érintett fél megfelelő körültekintéssel járjon el, ezért különös tekintettel javasolt:

- az archiválási rendben és a szolgáltatási szabályzatban megfogalmazott követelmények, előírások betartása;
- megbízható IT infrastrukturális környezet és alkalmazások használata;
- felhasználására vonatkozó valamennyi korlátozás figyelembevétele, melyek a jelen archiválási rendben és az szolgáltatási szabályzatban szerepel.

9.6.3 Egyéb szereplők tevékenységéért viselt felelősség és helytállás

Nincs megkötés.

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;

© 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 Hatóság algoritmusokkal kapcsolatos határozat által elfogadott kriptográfiai algoritmusok hibájából származtatható.

9.8 A felelősség korlátozása

Nincs megkötés.

9.9 Kártérítési kötelezettség

A Minősített bizalmi szolgáltató kártérítési felelősségének fedezetéül felelősségbiztosítással rendelkezik-

Ügyfél kártérítési felelősséggel tartozik Minősített bizalmi szolgáltatónak azokért a veszteségekért és károkért, amelyeket a rá vonatkozó kötelezettségek és ajánlások szándékos vagy gondatlan megszegésével okoz.

A kártérítési és kártalanítási eljárásokra a Ptk. általános szabályai vonatkoznak, Minősített bizalmi szolgáltató az eljárást részletesen az ÁSZF-ben közli.

A felelősség kapcsán lásd még a 9.6, a jótállási, szavatossági vagy kártérítési igényekkel kapcsolatban lásd a még a 9.7, 9.8 pontban foglaltakat is.

9.10 Érvényesség és megszűnés

9.10.1 Érvényesség

Jelen dokumentum adott verziója hatálybalépésének napja a dokumentum címlapján kerül feltüntetésre.

9.10.2 Megszűnés

Jelen szolgáltatási szabályzat hatálya megszűnik egy új verzió hatályba lépésével, vagy a tevékenység megszűnésével.

9.10.3 A megszűnés következményei

A szolgáltatási szabályzat visszavonása esetén a Minősített bizalmi szolgáltató honlapján közzéteszi a visszavonás részletes szabályait és egyéb kötelezettségeket. A bizalmas információkra vonatkozó szabályzatok a jelen dokumentum visszavonásával is érvényesek a Minősített bizalmi szolgáltató kötelékében.

9.11 A felek közötti kommunikáció

A Minősített bizalmi szolgáltató az Ügyfelekkel történő kapcsolattartás érdekében ügyfélszolgálati irodát működtet. Az értesítéseket elsősorban weboldalán keresztül biztosítja.

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 a jelen szabályzatot.

9.12.1 Módosítási eljárás

A Minősített bizalmi szolgáltató évente, illetve változtatás esetén soron kívül átvizsgálja az archiválási rendet és a szabályzatot és amennyiben indokolt, úgy 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;

© 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 módosított és jóváhagyott új ÁSZF verziót
valamint a 470/2017. Korm. rendeletben meghatározott egyéb iratokat és dokumentumokat.

A Minősített bizalmi szolgáltató változásbejelentési eljárás nélkül jelenti be, a következő iratok módosítását, akkor is, ha az változásbejelentési kötelezettséget érintő adatokat nem érint:

Szolgáltatási Rend,
Szolgáltatási Szabályzat,
Szabályzatkivonat,
ÁSZF.

Továbbá így kerül bejelentésre a felelősségbiztosítást és pénzügyi garancia követelményeket igazoló adat vagy az alátámasztó okiratokban történő változás.

9.12.2 Értesítések módja és határideje

A Minősített bizalmi szolgáltató a jóváhagyott dokumentumot legalább 30 nappal a tervezett hatálybalépés előtt véleményezésre megküldi az NMHH részére és publikálja honlapján.

A Minősített bizalmi szolgáltató a közzétett új szabályzat tervezettel kapcsolatos észrevételeket a hatálybalépést megelőző 14. napig fogadja az alábbi címen: info@notarchiv.hu.

9.12.3 A szolgáltatási szabályzat azonosítójának megváltoztatása

A Minősített bizalmi szolgáltató az szolgáltatási szabályzat legkisebb változtatása esetén is új verziószámmal látja el a dokumentumot.

9.13 Vitás kérdések rendezése

A működése során a Minősített bizalmi szolgáltató felmerülő vitás kérdések békés rendezésére törekszik. A Minősített bizalmi szolgáltató és az Ügyfél kölcsönösen megállapodnak abban, hogy bármilyen vitás kérdés vagy panasz felmerülése esetén, a vita jogi útra való terelése előtt megkísérlik a békés úton, tárgyalással történő egyeztetést. A kezdeményező fél kötelessége, hogy minden érintett többi felet haladéktalanul értesítsen és teljeskörűen tájékoztasson az ügy minden vonatkozását illetően.

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

A Minősített bizalmi szolgáltató által elfogadott békéltető testület és elérhetőségei

Budapesti Békéltető Testület:
Cím: 1016 Budapest, Krisztina krt. 99. III. em. 310.
Levelezési cím: 1253 Budapest, Pf.: 10.
E-mail cím: bekelteto.testulet@bkik.hu

Fogyasztói ügyekben releváns hatóság és elérhetőségei

Budapest Főváros Kormányhivatala Fogyasztóvédelmi Osztály:
Cím: 1056 Budapest, Váci utca 62-64.
Telefon: +36-1 328 5862
Levelezési cím: 1364 Bp., Pf.: 234
E-mail: budapest@bfkh.gov.hu
(A szabályzat érvénybe lépésekor hatályos szervezetek elérhetőségei)

A Minősített bizalmi szolgáltató tevékenységével kapcsolatos kérdéseket, kifogásokat és panaszokat az Minősített bizalmi szolgáltató címére kell eljuttatni írásos formában. A bejelentés kézhezvételétől számított 7 munkanapon belül a Minősített bizalmi szolgáltató értesíti a bejelentő felet az általa megadott címen a bejelentés fogadásáról és a kivizsgáláshoz szükséges időről. A megjelölt határidőig a Minősített bizalmi szolgáltató köteles írásban válaszolni a bejelentőnek. A Minősített bizalmi szolgáltató a válaszadáshoz szükséges információk megadását kérheti a bejelentőtől.

A Minősített bizalmi szolgáltató a panaszt 30 napon belül kivizsgálja, és az eredményekről értesíti a bejelentőt. Amennyiben a választ a bejelentő nem tartja kielégítőnek, vagy az alapján nem sikerül a Minősített bizalmi szolgáltató bevonása nélkül rendezni a felmerült vitát, akkor a bejelentő egyeztetést kezdeményezhet a Minősített bizalmi szolgáltatóval és az Érintett felekkel. Az egyeztetés

© 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.

minden résztvevőjét írásban értesíteni kell az egyeztetés időpontjáról azt megelőzően 15 munkanappal, és írásban meg kell számukra küldeni a bejelentést, a Minősített bizalmi szolgáltató válaszát és egyéb szükséges információkat tartalmazó dokumentumokat.

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

9.14 Irányadó jog

A Minősített 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 értelmezendő.

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.) (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)
- Az Európai Bizottság 2025/2532. számú végrehajtási rendeletére (9)
- Magyarország kiberbiztonságáról szóló 2024. évi LXIX. Törvény (10)

9.16 Vegyes rendelkezések

9.16.1 Teljességi záradék

Nincs megkötés.

9.16.2 Átruházás

A működésbe bevont harmadik fél számára csak a Minősített bizalmi szolgáltató 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.

9.16.4 Igényérvényesítés

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

© 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.

9.16.5 Vis major

Amennyiben az olyan hiba vagy késedelem oka, amely előre nem látható és/vagy a Minősített bizalmi szolgáltató ellenőrzési és hatáskörén körén kívüli külső ok a szolgálatatás teljesítése vonatkozásában, a Minősített bizalmi szolgáltató nem vonható felelősségre.

9.17 Egyéb rendelkezések

Nincs megkötés.

© 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.

10 Alkalmazott szabványok

Szabványok:

- ISO 9001:2015 Minőségirányítási Rendszer
- ISO/IEC 27001:2023 Információbiztonság irányítási rendszer
- FIPS PUB 140-2: Security Requirements for Cryptographic Modules
- ETSI EN 319 401 V3.2.1 (2026-01)
- ETSI TS 119 511 V1.1.1 (2025-10)
- ETSI TS 119 512 V1.2.1 (2023-05)
- ETSI EN 319 403-1 V2.3.1 (2020-06)
- ETSI TS 119 312 V1.5.1 (2024-12)
- ETSI EN 301 549 V3.2.1 (2021-03)

11. Bizalmi lista

A Minősített bizalmi szolgáltató az eIDAS rendelkezéseinek megfelelő minősített archiválás Minősített bizalmi szolgáltató, melyet a Hatóság nyilvántartásba vett és bizalmi listára rakott.

A Nemzeti Média és Hírközlési Hatóság nyilvántartásának elérhetősége a hatóság internetes weboldalán: https://esign.nmhh.hu/bszny/szolgParams/init.do?tipus=mi

A Hatóság által előállított bizalmi lista elérhetősége:

- géppel feldolgozható (xml) formátumban: http://nmhh.hu/tl/pub/HU_TL.xml
- olvasható (pdf) formátumban: http://nmhh.hu/tl/pub/HU_TL.pdf

A Felügyelet 2020. december 07. napján vette nyilvántartásba a Minősített bizalmi szolgáltatót. Határozat száma: EF/24727-5/2020.

© 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.