Szolgáltatási Szabályzat Minősített Archiválásszolgáltatásra

A NETLOCK Kft. nyilatkozata a minősített archiválásszolgáltatás nyújtásának és igénybevételének részletes eljárási és működési szabályairól

NETLOCK Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaság

A dokumentum magyar neve:	Szolgáltatási Szabályzat Minősített Archiválás szolgáltatásra
A dokumentum angol neve:	Service Practice Statement for Qualified Preservation Service
A dokumentum rövid neve:	SPS-QP-HU
Verzió	20210331
Azonosító szám (OID):	1.3.6.1.4.1.3555.1.47.20210331
Jóváhagyás időpontja:	2021.03.31.
Közzététel időpontja:	2021.04.01.
Hatály kezdőnapja:	2021.04.30.
Oldalak száma:	a fedlappal együtt összesen 72 oldal
Szakmai felelős:	**Kővári-Szabó Zoltán** Senior Compliance Manager
Jóváhagyó:	**dr. Fehér Zsófia,** Jogtanácsos

1 Tartalom

1 Tartalom 2
1. Bevezetés 8
1.1 Áttekintés 8
1.1.1 A Szabványok és előírások 8
1.1.2 A Szolgáltató 8
1.2 A dokumentum neve és azonosítása 10
1.2.1 Dokumentum revíziók 11
1.3 A PKI szereplők 12
1.3.1 Szolgáltató 12
1.3.2 Előfizető, Végfelhasználó és Igénylő 12
1.3.3 Érintett Fél 12
1.3.4 Egyéb szereplők 12
1.4 Tanúsítványok alkalmazhatósága 13
1.5 Szabályzatadminisztráció 13
1.5 A Bizalmi Szolgáltatási Szabályzat adminisztrációja 13
1.5.1 A dokumentum adminisztrációját végző szervezet 13
1.5.2 A dokumentum kapcsolattartó személye 13
1.5.3 A szolgáltatási szabályzat szolgáltatási rendnek megfelelésért felelős szervezet 14
1.5.4 A Szolgáltatási szabályzat elfogadása 14
1.6 Fogalmak és rövidítések 14
1.6.1 Fogalmak 14
1.6.2 Rövidítések 24
2 Közzététel 27
2.1 Adattárak 27
2.2 A tanúsítványokra vonatkozó információk közzététele 27
2.3 A közzététel időpontja és gyakorisága 27
2.4 Tanúsítványtár elérésének szabályai 27
3 Azonosítás és hitelesítés 27
4 Életciklus követelmények 28
4.1 Szolgáltatás igénylése 28
4.2 Dokumentum befogadása 28
4.2.2 Megőrzés 29
4.2.3 Archivált állomány és érvényességi lánc átvételének biztosítása 29
4.2.3.1 Harmadik személy hozzáférése 29

4.2.4 Igazolások kibocsátása 30
4.2.5 Dokumentum megjelenítése 30
4.2.6 Felülhitelesítés 30
4.3 Szolgáltatás elérhetősége és rendelkezésre állása 30
4.4 A szolgáltatási szerződés megszűnése 30
4.5 Export-import 31
4.6 Dokumentum és érvényességi lánc törlése 31
5 Fizikai, eljárásbeli és személyzeti biztonsági óvintézkedések 31
5.1 Fizikai óvintézkedések 32
5.1.1 Telephely felépítése 32
5.1.2 Fizikai hozzáférés 32
5.1.3 Áramellátás, légkondicionálás 33
5.1.4 Beázás és elárasztódás veszélyeztetettsége 33
5.1.5 Tűzmegelőzés és tűzvédelem 34
5.1.6 Adathordozók kezelése 34
5.1.7 Hulladékelhelyezés 34
5.1.8 Mentés külső helyszínen 34
5.2 Eljárásrendi biztonsági intézkedések 34
5.2.1 Bizalmi munkakörök 35
5.2.2 Az egyes feladatokhoz szükséges személyzeti létszám 35
5.2.3 Az egyes szerepkörökhöz tartozó azonosítás és hitelesítés 35
5.2.4 Egyes szerepkörök összeférhetetlensége 36
5.3 Személyzeti biztonsági intézkedések 36
5.3.1 Képzettségre, gyakorlatra és megbízhatóságra vonatkozó követelmények 36
5.3.2 Ellenőrzési eljárások 37
5.3.3 Képzési követelmények 38
5.3.4 Továbbképzési gyakoriságok és követelmények 38
5.3.5 Munkabeosztás körforgásának sorrendje és gyakorisága 38
5.3.6 Jogosultatlan tevékenységek büntető következményei 38
5.3.7 Szerződéses közreműködőkre vonatkozó követelmények 38
5.3.8 A személyzet számára biztosított dokumentumok 38
5.4 Naplózási eljárások 39
5.4.1 A tárolt események típusai 39
5.4.2 A naplófájl feldolgozásának gyakorisága 39
5.4.3 A naplófájl megőrzési időtartama 40
5.4.4 A naplófájl védelme 40

5.4.5 A naplófájl mentési eljárásai 40
5.4.6 A naplózás adatgyűjtési rendszere 40
5.4.7 Az eseményeket kiváltó Ügyfelek értesítése 40
5.4.8 Sebezhetőség felmérése 40
5.5 Adatok archiválása 41
5.5.1 Az archiválandó adatok típusai 41
5.5.2 Archiválási időtartam 41
5.5.3 Az archívum védelme 41
5.5.4 Az archívum mentési folyamatai 42
5.5.5 Az adatok időbélyegzésére vonatkozó követelmények 42
5.5.6 Az archívum gyűjtési rendszere 42
5.5.7 Archív információk hozzáférését és ellenőrzését végző eljárások 42
5.5.8 Egyéb archiválási rendelkezések 42
5.6 Kulcscsere 42
5.7 Katasztrófaelhárítás és helyreállítás 42
5.7.1 Incidens- és kompromittálódás-kezelési eljárások 42
5.7.2 IT erőforrások, szoftverek és/vagy adatok meghibásodása 43
5.7.3 Magánkulcs kompromittálódása esetén követendő eljárás 44
5.7.4 A működés folytonosságának fenntartása katasztrófaesemény után 44
5.8 A szolgáltatás megszűnése 45
6 Műszaki biztonsági óvintézkedések 45
6.1 Kulcspár generálás és telepítés 46
6.1.1 Kulcspár előállítása 46
6.1.2 Magánkulcs eljuttatása a Végfelhasználóhoz 46
6.1.3 Nyilvános kulcs eljuttatás a tanúsítvány kibocsátóhoz 46
6.1.4 A szolgáltatói nyilvános kulcs közzététele 46
6.1.5 Kulcsméretek 46
6.1.6 A nyilvános kulcs paraméterek előállítása, a minőség ellenőrzése 47
6.1.7 A kulcshasználat célja (az X.509 v3 kulcs használati mező tartalmának megfelelően 47
6.2 Magánkulcs védelem és kriptográfiai modul előírások 47
6.2.1 Kriptográfiai modulra vonatkozó szabványok és előírások 47
6.2.2 Magánkulcs többszereplős (n-ből m) használata 49
6.2.3 Magánkulcs letétbe helyezése 49
6.2.4 Magánkulcs mentése 49
6.2.5 Magánkulcs archiválása 49

6.2.6 Magánkulcs bejuttatása a kriptográfiai modulba, vagy onnan történő exportja 50
6.2.7 Magánkulcs tárolása kriptográfiai modulban 50
6.2.8 A magánkulcs aktiválásának módja 50
6.2.9 A magánkulcs deaktiválásának módja 50
6.2.10 A magánkulcs megsemmisítésének módja 50
6.2.11 A kriptográfiai modulok értékelése 50
6.3 A kulcspárkezelés további szempontjai 50
6.4 Aktiváló adat 51
6.4.1 Aktiváló adat generálás és telepítés 51
6.4.2 Aktiváló adat védelme 51
6.5 Informatikai biztonsági előírások 51
6.5.1 Speciális informatikai biztonsági műszaki követelmények 51
6.5.2 Informatikai biztonság értékelése 51
6.6 Életciklusra vonatkozó biztonsági előírások 51
6.6.1 Rendszerfejlesztési óvintézkedések 51
6.6.2 Biztonságkezelési előírások 52
6.6.3 Az életciklusra vonatkozó biztonsági előírások 52
6.7 Hálózati biztonság 53
6.8 Időbélyegzés 53
7 Tanúsítványprofil, megőrzési profil 53
7.1 Megőrzési profil – Megőrzés aláírással és kiterjesztéssel, tárolással 54
7.1.1 A profil hatálya 54
7.1.2 Séma Azonosító 54
7.1.3 Megőrzési célok 54
7.1.4 Megőrzési tárolási modell 54
7.1.5 Támogatott műveletek 54
7.1.5.1 Kötelező műveletek 55
7.1.5.2 Opcionális műveletek 55
7.1.6 A megőrzési bizonyítékok generálása és ellenőrzése 55
7.1.7 A megőrzési bizonyítékok kiterjesztése 55
7.1.8 Megőrzési bizonyíték szabályok 56
7.1.9 Aláírás ellenőrzési szabályok 56
8 A megfelelőség vizsgálata 56
8.1 Az ellenőrzések körülményei és gyakorisága 56
8.2 Az értékelő és szükséges képesítése 57
8.3 Az auditor és az auditált entitás kapcsolata 57

8.4 Az értékelés/audit által lefedett területek 58
8.5 A hiányosságok kezelése 58
8.6 Az eredmények közzététele 58
9 Egyéb üzleti és jogi tudnivalók 58
9.1 Díjak 58
9.1.1 Archiválás szolgáltatás díjai 59
9.1.2 Visszatérítési politika 59
9.2 Pénzügyi felelősség 59
9.2.1 Biztosítási fedezet 60
9.2.2 Egyéb eszközök 60
9.2.3 Az Érintett felek számára elérhető biztosítások és garanciák 60
9.3 Bizalmas üzleti információk kezelése 60
9.3.1 A bizalmas információk köre 60
9.3.2 A bizalmas információk körén kívül eső adatok 61
9.3.3 A bizalmas információk védelme 61
9.4 Személyes adatok kezelése 62
9.4.1 Adatkezelési szabályok 62
9.4.2 Személyes adatok 62
9.4.3 Személyes adatnak nem minősülő információk 62
9.4.4 Személyes adatok védelme 63
9.4.5 Személyes adatok felhasználása 63
9.4.6 Adatkezelés 63
9.4.7 Egyéb adatvédelmi követelmények 63
9.5 Szellemi tulajdonhoz fűződő jogok 63
9.6 Felelősség és garanciák 64
9.6.1 A Hitelesítő Egység felelőssége 64
9.6.2 A Regisztrációs Egység felelőssége 64
9.6.3 Ügyfelek felelőssége és kötelezettségei 64
9.6.4 Érintett felek felelőssége 65
9.6.5 Egyéb résztvevők felelőssége 65
9.7 Szavatosság kizárása 65
9.8 Felelősség korlátozása 65
9.9 Kártérítés, kártalanítás 66
9.10 A szabályzat hatálya 66
9.10.1 Érvényesség 66
9.10.2 Megszűnés 66

9.10.3 A megszűnés következményei 66
9.11 Egyedi értesítések és a résztvevők közti kommunikáció 66
9.12 Módosítások 67
9.12.1 A módosítási eljárás 68
9.12.2 Az értesítések módja és határideje 68
9.12.3 A dokumentumazonosító változása 68
9.13 Vitás kérdések rendezése 69
9.13.1 Panaszok kezelésének eljárása 69
9.13.2 Vitás kérdések rendezése békés, tárgyalásos úton 69
9.13.3 Vitás kérdések rendezése peres úton 70
9.14 Irányadó jog 70
9.15 A hatályos jogszabályoknak és szabványoknak való megfelelés 70
9.16 Vegyes rendelkezések 72
9.16.1 Teljességi záradék 72
9.16.2 Átruházás 72
9.16.3 Részleges érvénytelenség 72
9.16.4 Igényérvényesítés 72
9.16.5 Vis maior 72
9.17 Egyéb rendelkezések 72

1. Bevezetés

Jelen dokumentum a NETLOCK Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaság (továbbiakban: Szolgáltató) nyilatkozata a minősített bizalmi archiválásszolgáltatás nyújtásával kapcsolatosan alkalmazott részletes eljárási és működési követelményekről (a továbbiakban: Szolgáltatási Szabályzat vagy Szabályzat).

A dokumentumban alkalmazott fogalmak és rövidítések tekintetében az 1.6 fejezetet.

1.1 Áttekintés

Szolgáltató jelen dokumentum által szabályozott szolgáltatás a minősített archiválás szolgáltatás.

1.1.1 A Szabványok és előírások

Jelen Szolgáltatási Szabályzat a *NETLOCK Bizalmi Szolgáltatási Rend Minősített Archiválás szolgáltatásra* dokumentum szerkezetét követve készült, az abban foglalt elvárásoknak való megfelelés módját ismerteti. Az egyes fejezetcímek csak a tartalom adott logikai rend szerinti rendezésére szolgálnak, a rendelkezések értelmezése tekintetében nem irányadók.

A Szabályzat tartalmi vonatkozásokban eleget tesz az eIDAS, az Eüt. és a BM rendelet előírásainak és ajánlásainak.

A Szolgáltató által használt és alkalmazott jogszabályok, szabványok és előírások a 9.15 pontban kerültek részletezésre.

1.1.2 A Szolgáltató

Név:	**NETLOCK Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaság**
Rövidített név:	NETLOCK Kft.
Székhely:	1101 Budapest, Expo tér 5-7.
Telephely (Ügyfélszolgálat):	1143 Budapest, Hungária körút 17.
Postázási cím:	1439 Budapest, Pf. 663
Cégjegyzékszám:	01-09-563961
Adószám:	12201521-2-42
Telefonszám:	(1) 437-6655 (Tanúsítvány állapotváltozás igénylése: 3. menüpont)
Fax:	(1) 700-2828
Weboldal:	netlock.hu
Kikötések és feltételek közzététele:	netlock.hu/aktualis-szabalyzatok
Ügyfélkapcsolati e-mail:	info@netlock.hu
Megrendelések, dokumentummásolatok, szerződések küldése:	igenylesek@netlock.hu
NETLOCK Szabályzatelfogadó Egység email címe:	szee@netlock.hu
Ügyfélfogadás / Nyitva tartás	A Szolgáltató weboldalán feltüntetett helyen és időintervallumban.

Az Eat.[1] rendelkezéseinek megfelelő minősített archiválás szolgáltatóként a Bizalmi Felügyelet 2010. szeptember 15-én vette nyilvántartásba Szolgáltatót. Regisztrációs szám: HL/18188-4/2010.

A Bizalmi Felügyelet Eat szerinti szolgáltatásokat tartalmazó nyilvántartásának elérhetősége: http://webpub-ext.nmhh.hu/esign/

Jelen Szolgáltatási Szabályzat az eIDAS és az Eüt. rendelkezéseinek megfelelő minősített bizalmi archiválásszolgáltatás nyújtásával kapcsolatos eljárási és működési követelményeket tartalmaz, melyek nyújtását Szolgáltató jelen szabályzat első verziójának (lásd 1.2.1) hatálybalépésével egyidejűleg kezdte meg az alábbi feltételekkel:

- Szolgáltató a jelen szabályzat szerinti minősített bizalmi szolgáltatások elindítása előtt külső megfelelőségértékelést végeztetett (lásd 8. fejezet) valamint az Eüt. 80. § értelmében a Bizalmi Felügyelet által rendszeresített elektronikus űrlapon bejelentette a Felügyeletnek a minősített bizalmi szolgáltatás nyújtásának megkezdésére vonatkozó szándékát, megadva az űrlap által kért adatokat, egyebek mellett a Szolgáltató nevét és székhelyét.
- A megfelelőségértékelési eljárás eredményét tartalmazó megfelelőségértékelési jelentést (Conformity Assessment Report), Szolgáltató megküldte a Bizalmi Felügyeletnek.
- a Szolgáltatási Rend, a Szolgáltatási Szabályzat és az Általános Szerződési Feltételek jóváhagyott nyilvános tervezeteit valamint a 470/2017 (XII. 28.) Korm. rendelet 2. § (2) bekezdésében meghatározott további dokumentumokat, iratokat és nyilatkozatokat Szolgáltató megküldte a Bizalmi Felügyeletnek a minősített bizalmi szolgáltatás bejelentésekor.
- Szolgáltató minősített bizalmi szolgáltatóként azt követően indíthatja el a jelen szabályzatban meghatározott eIDAS szerinti minősített bizalmi szolgáltatásokat, hogy
  - a Bizalmi Felügyelet felvette a Szolgáltatót és a bizalmi szolgáltatását a minősített bizalmi szolgáltatókat és minősített bizalmi szolgáltatásokat tartalmazó, az Eüt 94. §-ban meghatározott nyilvántartásába, valamint
  - az eIDAS 22. cikk (1) bekezdésében meghatározott bizalmi listákon (EUTSL) a bizalmi szolgáltatás eIDAS szerinti „minősített” státusza feltüntetésre került (a listák elérhetőségét lásd lentebb).

A jelen Szabályzat szerinti minősített bizalmi szolgáltatások Bizalmi Felügyelethez történő bejelentése jelen nyilvános szabályzattervezet első nyilvános tervezetként közreadott verziójának (lásd 1.2.1.) közzétételével egyidejűleg megtörtént. A Bizalmi Felügyelet a helyszíni szemléjét a Szolgáltatónál megtartotta.

A Bizalmi Felügyelet nyilvántartásba vételről szóló határozatát Szolgáltató 2017. június 16-án vette kézhez, mely szerint a Bizalmi Felügyelet az EF/15066/3/2017 nyilvántartási számon a Szolgáltatót mint minősített elektronikus időbélyegző szolgáltatást nyújtó eIDAS szerinti minősített bizalmi szolgáltatót nyilvántartásba vette és ezzel egyidejűleg az EU bizalmi listára (EU TL) felvette.

A Bizalmi Felügyelet eIDAS szerinti minősített szolgáltatókat és szolgáltatásokat tartalmazó közhiteles nyilvántartásának elérhetősége:

http://webpub-ext.nmhh.hu/esign2016/szolgParams/init.do?tipus=mi

Szolgáltató jogosult az EU Trust Mark[2] [SZ1] használatára a minősített szolgáltatásai tekintetében.

A bizalmi felügyelet által gondozott és közzétett magyar bizalmi lista elérhetőségei:

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

Az Európai Bizottság által gondozott és közzétett bizalmi listák listája (EU TL) elérhetőségei:

- géppel feldolgozható (xml) formában: https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml
- böngészhető, kereshető formában: https://webgate.ec.europa.eu/tl-browser

A listákon feltüntetett szolgáltatások eIDAS szerinti „minősített" státuszát a „ServiceTypeIdentifier" „PSE/Q" és a „ServiceStatus" „granted" értékei jelzik.

Szolgáltató jogosult az EU Trust Mark[2] használatára a minősített szolgáltatásai tekintetében.

Évente elvégzett önkéntes akkreditációk és egyéb minősítések:

- A szolgáltató Tanúsítása az ETSI EN 319 401, az ETSI EN 319 411-1 és ETSI EN 319 411-2 szabványok szerint.
- ISO 9001 szabvány
- ISO 27001 szabvány

Lásd még a 8. fejezetet.

Szolgáltató – az erre vonatkozó jogszabályi kötelezettségeinek betartásán túl – kiemelt figyelmet fordít a diszkriminációmentes kiszolgálásra és az egyenlő bánásmódra illetve Ügyfelei, az Érintett felek és a szolgáltatásai iránt érdeklődők kiszolgálása és informálása kapcsán biztosítja a szolgáltatásokhoz és az információkhoz való egyenlő hozzáférést. Ennek értelmében a Szolgáltatóhoz forduló Ügyfelek, Érintett felek és más érdeklődők kiszolgálását és informálását semmilyen körülmények között nem befolyásolhatja bármilyen előítélet, hátrányos megkülönböztetés akár üzleti akár személyes viszonyok mentén. Így például (de nem kizárólagosan) Szolgáltató és munkatársai sem nemi, faji, vallási vagy politikai hovatartozásból, sem gazdasági méretből adódó különbözőségek alapján nem tesznek különbséget az Ügyfelek, az Érintett felek és a szolgáltatások iránt érdeklődők között. A diszkrimináció mentes működést és szolgáltatások biztosítását Szolgáltató feltétel nélkül elvárja minden munkatársától és partnerétől is.

1.2 A dokumentum neve és azonosítása

A dokumentum nevét és OID azonosítóját lásd a fedlapon (első számozás nélküli oldal a Szolgáltató logójával) - "A dokumentum magyar neve" és "A dokumentum angol neve" valamint az "Azonosító szám (OID)" sorokban.

A dokumentum többi oldalain a dokumentum magyar neve a láblécben, OID azonosítója pedig a fejécben kerül feltünetésre.

[2] Lásd https://ec.europa.eu/digital-single-market/en/eu-trust-mark

Jelen dokumentum egyike a Szolgáltató által kiadott azon dokumentumoknak, amelyek az általa nyújtott szolgáltatások feltételeit együttesen szabályozzák. Ilyen dokumentumok továbbá például az Általános szerződési feltételek, a Szolgáltatási szerződés, a szolgáltatási szabályzatok, az Ügyfelekkel és a Partnerekkel kötött egyéb szerződések.

A jelen dokumentumban Szolgáltatónak nevezett entitás a NETLOCK Kft. - adatait lásd az 1.1.2 pontban.

1.2.1 Dokumentum revíziók

OID	Hatálya	Változás leírása	Készítő
1.3.6.1.4.1.3555.1.47.20170301	nem hatályosított verzió	Egységes – minősített és nem-minősített szolgáltatásokat egyaránt tartalmazó – szolgáltatási szabályzat első nem nyilvános draft verziója	Almási János dr. Barabás Anett Varga Viktor Szabó Zoltán
1.3.6.1.4.1.3555.1.47.20170426	nem hatályosított verzió	A draft verzióból a nem archiválásszolgáltatásokra vonatkozó előírások törlése; pontosítások, javítások az archiválás szolgáltatás kapcsán.	Szabó Zoltán
1.3.6.1.4.1.3555.1.47.20170515	nem hatályosított verzió	A MATRIX Vizsgáló, Ellenőrző és Tanúsító Kft. által végzett megfelelőségértékelési eljárás során tett észrevételek alapján pontosított és kiegészített verzió.	Szabó Zoltán Varga Viktor
1.3.6.1.4.1.3555.1.47.20170615	2017.06.19-2017.10.31.	NL SIGN fogalmának pontosítása	dr. Barabás Anett
1.3.6.1.4.1.3555.1.47.20170904	nem hatályosított verzió	Szolgáltató által használt eszközök módosítása	dr. Barabás Anett
1.3.6.1.4.1.3555.1.47.20171012	2017.11.01-2018.05.23	Az előző verzió kiegészítése és pontosítása a bizalmi felügyelet észrevételei alapján: - az SSCD és QSCD minősítésű eszközök EU-s listája elérési helyének megadása (1.1.2.) - az alkalmazott eszközök megfelelőségi tanúsítványának elérési helyének megadása (6.2.1.) - NAIH nyilvántartási száma feltüntetése (9.4.1.)	Szabó Zoltán
1.3.6.1.4.1.3555.1.47.20180416	2018.05.24-2018.09.02.	*A dokumentum következő verziójának nyilvános tervezete az alábbi módosításokat tartalmazza:* • Dokumentum címének rövidítése • Fedlap kiegészítése • A megőrzésre átadott állományok megőrzési idejére vonatkozó szabályok pontosítása (4.2.2). • Egyes – a közelmúltban változott – jogszabályok hivatkozásának frissítése.	Szabó Zoltán
1.3.6.1.4.1.3555.1.47.20180727	nem hatályosított verzió	• A megfelelőségértékelő szervezet (MÁTRIX Kft.) által az éves felülvizsgálat keretében jelzett észrevételek alapján történő pontosítások a 1.1.2., 9.4 és 9.12 fejezetekben. • Egyes fogalommeghatározások pontosítása (1.6) • Egyéb kisebb pontosítások, javítások.	Szabó Zoltán
1.3.6.1.4.1.3555.1.47.20180817	2018.09.03-2020.08.13.	Az előző tervezet állapotú verzió pontosítása a bizalmi felügyelet észrevételei alapján (Érintett pont: 4.1).	Szabó Zoltán

1.3.6.1.4.1.3555.1.47.20200714	2020.08.14-2021.04.29.	• A módosítás oka az ETSI TS 119 511 V1.1.1 szabvánnyal összefüggésben tett változtatások. (4,5, 7, 8) • Kisebb pontosítások dokumentumszerte	Varga Viktor
1.3.6.1.4.1.3555.1.47.20210331	2021.04.30-tól visszavonásig vagy új verzió hatálybalépéséig	• A Szolgáltató telephelyének feltüntetése a szabályzat 1.1.2 fejezetében	Varga-Szabó Éva

1.3 A PKI szereplők

Jelen Szolgáltatási Szabályzat keretében a PKI szereplők alatt az archiválás szolgáltatás Ügyfeleit (Igénylőit és Előfizetőit), Végfelhasználóit, a Szolgáltatót és szervezeti egységeit, valamint az Érintett feleket kell érteni.

Lásd még az 1.6.1 Fogalmak fejezet releváns fogalom meghatározásait.

1.3.1 Szolgáltató

Szolgáltató a bizalmi minősített archiválás szolgáltatás keretében elektronikus aláírások, elektronikus bélyegzők, időbélyegzők és ezek tanúsítványai érvényességének megőrzését biztosítja, beleértve az aláírt vagy bélyegzett és időbélyegzett elektronikus dokumentum megőrzését is.

1.3.2 Előfizető, Végfelhasználó és Igénylő

Előfizető és Igénylő a Szolgáltató Ügyfelei, akikkel Szolgáltató szerződéses kapcsolatba kerül.

Végfelhasználó személyét az Előfizető határozza meg.

Lásd még a 1.6 Fogalmak és rövidítések fejezet vonatkozó fogalom magyarázatait.

1.3.3 Érintett Fél

Az Érintett fél jellemzően nem áll szerződéses kapcsolatban a Szolgáltatóval, de részére a minősített archiválás szolgáltatási szabályzat ajánlásokat fogalmazhat meg. Az Érintett felek bizonyos köre az archiválás szolgáltatás bizonyos, Kikötésekben megadott funkcióit egy a Szolgáltatóval szerződéses kapcsolatban álló Előfizető kezdeményezésére, az általa megjelölt dokumentumok és egyéb állományok vonatkozásban díjmentesen használhatja (lásd 1.3.5)

1.3.4 Egyéb szereplők

Hozzáférő

Szolgáltatónak biztosítania kell, hogy a szolgáltatás egyes funkcióit szolgáltatási szerződést Szolgáltatóval nem kötő Érintett felek (lásd 1.3.4) is igénybe vehessék ún. Hozzáférő jogosultságú felhasználóként. Hozzáférő jogosultságot Előfizető adhat az általa megőrzésre átadott állományok vonatkozásában.

Lásd még az 1.6.1 fejezet Hozzáférő fogalmát.

1.4 Tanúsítványok alkalmazhatósága

Archiválás szolgáltatásra az RFC 3647 ezen pontja nem értelmezett, ilyen követelmény megfogalmazása nem szükséges.

1.5 Szabályzatadminisztráció

Jelen Bizalmi Szolgáltatási Szabályzat kibocsátását és karbantartását a Szolgáltató szabályzatért felelős egysége végzi.

1.5 A Bizalmi Szolgáltatási Szabályzat adminisztrációja

Jelen Bizalmi Szolgáltatási Szabályzat kibocsátását és karbantartását a Szolgáltató szabályzatért felelős egysége végzi. A Szolgáltató a szabályzatért felelős egységet saját egységén belül működteti s ennek pontos felépítését, feladatát, hatáskörét és felelősségét külön szabályzat tartalmazza.

1.5.1 A dokumentum adminisztrációját végző szervezet

A Szolgáltató szabályzatokért (kikötésekért) felelős egységének neve NETLOCK Szabályzatelfogadó Egység. A Szabályzatelfogadó Egység állandó tagjai a Szolgáltató munkatársai, akiket a Szolgáltató Ügyvezetése írásban jelöl ki. Az Egység működését a Szabályzatelfogadó Egység belső, nem nyilvános működési szabályzata írja le.

A Szolgáltató szabályzatainak módosításával kapcsolatban lásd a 9.12 fejezetet.

1.5.2 A dokumentum kapcsolattartó személye

Jelen dokumentummal kapcsolatban a Szabályzatelfogadó Egység kapcsolattartásért felelős személye a jelen dokumentum jóváhagyója (lásd a dokumentum fedlapját).

Jelen dokumentummal kapcsolatos kérdésekkel és észrevételekkel az Ügyfelek, a Végfelhasználók és az Érintett felek elektronikus levélben az szee@netlock.hu címen kereshetik meg a NETLOCK Szabályzatelfogadó Egységét.

Szolgáltató munkatársai észrevételeiket egyéb csatornán keresztül is, de szintén csak írásban juttathatják el a Szabályzatelfogadó Egységhez.

A Szabályzatelfogadó Egységnek elektronikus levélben küldött megkeresések (lásd 1.5.1) megválaszolásáért illetve - amennyiben szükséges az észrevétel nyomán megtenni szükséges egyéb intézkedések megtételéért a kapcsolattartó személy felelős.

A Szabályzatelfogadó Egység részére jelen dokumentummal kapcsolatban eljutatott kérdés vagy észrevétel esetén a kapcsolattartónak kell kijelölnie az Egység azon munkatársát, aki a megkeresést feldolgozza. Összetettebb tárgyú megkeresés esetén összehívja a Szabályzatelfogadó Egység ülését - az Egység szabályzatában foglaltaknak megfelelően.

A megkeresés feldolgozása során, az Egység vagy munkatársa azonosítja a dokumentum észrevétellel, kérdéssel érintett pontját/pontjait, majd az Egység többi munkatársával egyeztetve - és szükség esetén a Szolgáltató más munkatársak véleményét is kikérve - küld választ elektronikus levélben az értesítést küldőnek.

Amennyiben a megkeresés nyomán jelen Szolgáltatási Szabályzat vagy más dokumentum

módosítása szükségessé válik, a módosítással kapcsolatban a 9.12 fejezet szerint kell Szolgáltatónak eljárnia.

1.5.3 A szolgáltatási szabályzat szolgáltatási rendnek megfelelésért felelős szervezet

A Szolgáltatási Szabályzat alapján nyújtott minősített archiválás nyújtásának és igénybevételének részletes gyakorlati előírásait tartalmazó Szolgáltatási Szabályzat Szolgáltatási Rendnek való megfelelését a NETLOCK Szabályzatelfogadó Egysége ellenőrzi. A jelen szolgáltatási szabályzatot a Szabályzatelfogadó Egység a Szolgáltatási Rendnek való maradéktalan megfelelés esetén hagyhatja jóvá.

A Szabályzat vagy nyilvános tervezete közzétételének feltétele, annak jóváhagyása.

1.5.4 A Szolgáltatási szabályzat elfogadása

Amennyiben a szabályzat módosításra szorul, a módosított új verzió megírása, elfogadása és kibocsátása 9.12.1 fejezetnek megfelelő egységes eljárás szerint és az Egység működési szabályzatában foglaltak szerint történik. Amennyiben az új verzió jóváhagyásáért felelős munkatárs meggyőződött róla, hogy a Szabályzat a módosítást követően is maradéktalanul megfelel a Szolgáltatási Rend előírásainak, jóváhagyja a szabályzatot és haladéktalanul, de legkésőbb az új verzió hatálybalépése előtt 30 nappal gondoskodik annak közzétételéről.

1.6 Fogalmak és rövidítések

1.6.1 Fogalmak

AIA	CAI (Authority Information Access:Certificate Authority Issuers): Az adott tanúsítvány kiadói tanúsítványára vonatkozó elérhetőséget (URL) tartalmazó tanúsítványmező.
Alárendelt szolgáltatás	Szolgáltató szabályzatai alapján működő nem minősített bizalmi szolgáltatás, mely számára Szolgáltató biztosít tanúsítványt.
Aktiváló adat	Olyan a szolgáltató által előállított vagy végfelhasználó által megadott, kizárólag a végfelhasználó által ismert kódsorozat (jelszó, PIN kód), ami a magánkulcsot alkalmazásra képes állapotba helyezi. Tanúsítványaktiváláshoz nincs köze.
Aláírás	Lásd elektronikus aláírás
Aláírás / Bélyegző Létrehozó eszköz	Olyan kriptográfiai eszköz, amely minősített aláírás / bélyegző létrehozására nem alkalmas (lásd még 1.6.2. Rövidítések, SCD).
Aláírási szolgáltatás	Az eIDAS szerinti alábbi szolgáltatások: ● elektronikus aláírások és elektronikus bélyegzők létrehozása, ellenőrzése és érvényesítése, ● valamint ezekhez kapcsolódó tanúsítványok ellenőrzése és érvényesítése. Jelen szabályzat keretében e szolgáltatások “felhőalapú” nyújtását értjük, a

	végfelhasználói aláíró és bélyegző kulcsok szolgáltató által tárolásával és az ügyfelek által webes felületen/protokollon keresztül feltöltött dokumentumok aláírásával/bélyegzésével (beleértve opcionálisan az időbélyeg elhelyezését is), illetve ezek ellenőrzésével.
Aláírói partner	Szolgáltatói partner, aki az aláírási szolgáltatást saját ügyfelei számára biztosítja, amelynek részeként részt vehet a Végfelhasználók azonosításában (akik tekintetében korlátozott információs és adminisztrációs jogokkal bír), s aki az aláírási szolgáltatást saját szolgáltatásával integráltan szolgáltatás nyújtására használja, s aki Előfizetőként vállalja a díjfizetést a végfelhasználók után.
Alany	Lásd az Eüt. 1. § 43. pontjának meghatározását. Jelen szabályzat keretében a tanúsítvány Subject és SAN mezőit, illetve az ezekben feltüntetésre kerülő adatokat értjük alatta, amelyek utalhatnak egy természetes személyre és/vagy egy szervezetre és/vagy egy védjegyre/terméknévre vagy egy eszköz/rendszer azonosítójára/más elnevezésére vagy egy álnévre. Lásd az Igénylő, Előfizető, Ügyfél és Végfelhasználó entitásokat.
Állapotváltoztatás	Az az eljárás, aminek eredményeként a tanúsítvány állapota (érvényes, felfüggesztett) megváltozik és új értéket vesz fel (érvényes, felfüggesztett, visszavont).
Archiválási szolgáltatás	Az Eüt. 1. § 2 szerint: “Az elektronikus dokumentumok hosszú távú megőrzésére vonatkozó szolgáltatás, amely magában foglalja az eIDAS Rendelet 3. cikk 16. pont c) alpontja szerinti bizalmi szolgáltatást is”. Jelen szabályzat keretén belül olyan minősített bizalmi szolgáltatás, mely során a Bizalmi Szolgáltató a hozzá archiválás céljából eljuttatott elektronikusan hitelesített (aláírt vagy bélyegzett) dokumentumok aláírása vagy bélyegzője teljes érvényességi láncát létrehozza vagy kiegészíti, az érvényességi láncot archív időbélyeggel ellátja, majd az így kiegészített dokumentumot vagy fájlt biztonságosan eltárolja.
Átvevő	A végfelhasználó valamely kulcsát vagy eszközét (pl. Ügyféleszköz) és aktiváló adatát Szolgáltatótól (személyesen, hagyományos vagy elektronikus kézbesítés útján) átvevő személy, aki az lehet, aki az adott tanúsítvány esetében Igénylő lehet.
Bélyegző	Lásd elektronikus bélyegző
Bizalmi lista	Hatóság vagy szoftvergyártó által kezelt lista, amely a megbízhatónak tartott bizalmi szolgáltatások azonosítóit (jellemzően tanúsítványait) tartalmazza. Egy adott bizalmi listát kezelő szoftver a benne lévő szolgáltatásokra visszavezethető aláírásokat, bélyegzőket és időbélyegzőket elfogadja. Jelemzően az EU bizalmi listát értjük alatta, ahol az eIDAS szerinti nem minősített és minősített szolgáltatások kerülnek feltüntetésre az egyes tagországok felügyeleti szervei által. Lásd: https://ec.europa.eu/digital-single-market/en/eu-trusted-lists-certification-service-providers
Bizalmi Szolgáltatási Rend	NETLOCK Bizalmi Szolgáltatási Rend Minősített Tanúsítványszolgáltatásra

Bizalmi Felügyelet	Az Eüt. által a bizalmi szolgáltatások felügyeletére kijelölt szerv. Konkrétan a Nemzeti Média- és Hírközlési Hatóság.
Bizalmi munkakör	A szolgáltató informatikai rendszeréért általánosan felelős vezetői munkakör,.Lásd az 5.2.1 Bizalmi munkakörök fejezetet.
Bizalmi munkatárs	A Szolgáltatónál vagy Szolgáltatói partnerénél bizalmi munkakört betöltő személy.
Bizalmi szolgáltatás	Az eIDAS 3. cikk 16. Pontja szerint: “Rendszerint díjazás ellenében nyújtott, jelen Szabályzat keretében az alábbiakból álló elektronikus szolgáltatások: - elektronikus aláírások, elektronikus bélyegzők vagy elektronikus időbélyegzők, ajánlott elektronikus kézbesítési szolgáltatások, valamint az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok létrehozása, ellenőrzése és érvényesítése; vagy - weboldal-hitelesítő tanúsítványok létrehozása, ellenőrzése és érvényesítése; vagy elektronikus aláírások, bélyegzők vagy az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok megőrzése.” Jelen szabályzat keretén belül a Szolgáltató elektronikus aláírásokhoz, elektronikus bélyegzőkhöz és weboldal hitelesítéshez kapcsolódó, a tanúsítványok kibocsátását és életciklusmenedzsmentjét biztosító, valamint az Időbélyegző szolgáltatását értjük alatta.
Biztonságos zóna:	Olyan (logikailag vagy fizikailag) védett terület, amely védi a titkosságát, integritását és elérhetőségét a Szolgáltató által használt rendszereknek.
CAA ellenőrzés	Olyan ellenőrzés, amikor a DNS bejegyzésben RFC 6844 szerinti CAA rekordokat keres a Szolgáltató. Ha itt arra utaló bejegyzés van, hogy más Szolgáltatóval tart kapcsolatot a domaintulajdonos, akkor nem adható ki tanúsítvány.
Eakta (formátum)	Elektronikus aláírás konténerformátum, amely dokumentumokat, illetve hozzájuk kapcsolódó profilokat (metaadatokat), aláírásokat, ellenjegyzéseket és időbélyegzőket tartalmazhat, szabványos, az ETSI TS 101 903 (XAdES) specifikációnak megfelelően. Lásd bővebben: https://e-szigno.hu/tudasbazis/e-akta-formatum-specifikacioja.html
EV tanúsítvány Extended Validation Certificate (EVC)	Olyan weboldal-hitelesítő tanúsítvány, ami megfelel az EVCG követelményeinek.
Elektronikus aláírás	Olyan elektronikus adat, amelyet más elektronikus adatokhoz csatolnak, illetve logikailag hozzárendelnek, és amelyet az aláíró aláírásra használ (eIDAS 3 cikk 10. pont). Jelen szabályzat keretén belül: A Szolgáltató által kibocsátott aláíró tanúsítvány magánkulcs párjával természetes személy által létrehozott elektronikus adat, amelyet az aláírandó elektronikus dokumentumhoz (vagy más elektronikus adatokhoz) csatolnak, s ami a tanúsítvánnyal és a benne foglalt nyilvános kulccsal ellenőrizhető.
Elektronikus bélyegző	Olyan elektronikus adatok, amelyeket más elektronikus adatokhoz csatolnak, illetve logikailag hozzárendelnek, hogy biztosítsák a kapcsolt

	adatok eredetét és sértetlenségét. (eIDAS 3 cikk 25. pont) Jelen szabályzat keretén belül: A Szolgáltató által kibocsátott bélyegző tanúsítvány magánkulcs párjával jogi személy által létrehozott elektronikus adat, amelyet az bélyegzendő elektronikus dokumentumhoz (vagy más elektronikus adatokhoz) csatolnak, s ami a tanúsítvánnyal és a benne foglalt nyilvános kulccsal ellenőrizhető. Az elektronikus aláírás jogi személy által létrehozott megfelelője.
Előfizető	Szolgáltató azon szerződéses partnere, aki a szolgáltatási díjak fizetését vállalja. Jogai és kötelezettségei az ÁSZF-ben és a Szolgáltatási szerződésben elkülönülten megjelennek. Tanúsítványszolgáltatás esetén amennyiben a tanúsítvány Alanyként szervezet is megnevezésre került vagy csak egy természetes személy van benne megnevezve, akkor jellemzően azzal megegyezik. NL Sign szolgáltatás esetén megegyezik az Aláírói Partnerrel vagy a Végfelhasználóval. Lásd még az Ügyfél, Igénylő és Végfelhasználó entitásokat, valamint az 1.3.3 Előfizető, Végfelhasználó és Igénylő fejezetet.
Érintett fél	Természetes vagy jogi személy, aki Szolgáltatóval nem kerül szerződéses kapcsolatba, de annak valamely - jellemzően ingyenes - tanúsítvány állapot szolgáltatását igénybe veszi (pl. elektronikus aláírást, bélyegzőt vagy időbélyegzőt ellenőriz és ennek kapcsán az egyes tanúsítványok érvényességi információit vagy szolgáltató szabályzatait ellenőrzi). Lásd az 1.3.4 Érintett felek fejezetet.
Érvényes tanúsítvány	Olyan tanúsítvány, amelynek az érvényességi idejébe esik a mindenkori jelen időpont, és amelynek állapota nem felfüggesztett vagy visszavont (lásd Tanúsítványállapot).
Érvényességi idő(tartam)	Egy kezdeti és végső időpont közötti időtartam, amelyre a tanúsítvány kiadásra került.
Eszközös tanúsítvány	Olyan tanúsítvány, aminek magánkulcsa Kriptográfiai eszközre kerül kiadásra.
Érvényességi lánc	Az elektronikus dokumentum vagy annak lenyomata és azon egymáshoz rendelhető információk (így különösen azon tanúsítványok, a tanúsítványokkal kapcsolatos információk, az aláírás vagy bélyegző létrehozásához használt adatok, a tanúsítvány aktuális állapotára, visszavonására vonatkozó információk, valamint a tanúsítványt kibocsátó szolgáltató érvényességi adatára és annak visszavonására vonatkozó információk) sorozata, amelyek segítségével megállapítható, hogy az elektronikus dokumentumon elhelyezett fokozott biztonságú vagy minősített elektronikus aláírás, bélyegző vagy időbélyegző, az aláírás, bélyegző vagy időbélyegző elhelyezésének időpontjában érvényes volt. Általánosabb értelemben egymást hitelesítő tanúsítványok hierarchiája, egészen a gyökér tanúsítványig.
Fokozott biztonságú elektronikus aláírás	Olyan elektronikus aláírás, amely megfelel az eIDAS 26. cikkben meghatározott követelményeknek.

Fokozott biztonságú elektronikus bélyegző	Olyan elektronikus bélyegző, amely megfelel az eIDAS 36. cikkben meghatá-rozott követelményeknek.
Hitelesítési rend	Az Eüt. 1. § 24 szerint: olyan bizalmi szolgáltatási rend, amely bizalmi szolgáltatás keretében kibocsátott tanúsítványra vonatkozik. Szolgáltató szabályzati keretében egy szabványos eljárásrend, ami alapján Szolgáltató tanúsítványt bocsát ki és kezel. Szolgáltató szabályzatai több hitelesítési rendet is magukban foglalnak, megkülönböztetve a nekik megfelelő követelményeket és eljárásokat.
Hitelesítő egység	Szolgáltató szervezeti egysége, amely a Regisztrációs egység kérelme alapján a tanúsítványok kiadását, publikálását, visszavonását, felfüggesztését, valamint a Tanúsítványvisszavonási lista publikálását végzi. Lásd az 1.3.1 fejezetet.
Hitelesítési Ügyintéző	A Hitelesítő Egységen belül e munkakörben dolgozó munkatársak a tanúsítványok kibocsátásának jóváhagyását végzik.
Hozzáférő	Az archiválásszolgáltatás Előfizetőjének kezdeményezésére a szolgáltatás bizonyos funkcióit a kezdeményező Előfizető által meghatározott dokumetumok tekintetében díjmentesen elérő Érintett fél. Lásd az 1.3.5 Érintett felek fejezetet.
Igénylő	Tanúsítványszolgáltatás esetén a tanúsítványkibocsátási tanúsítványkezelési és állapotváltoztatási eljárásban eljáró, a szolgáltatói szerződést Ügyfél részéről elfogadó természetes személy, aki lehet: ● a tanúsítvány Alanyaként megjelölt természetes személy (Álnév esetén az álnév kérelmezője); ● ennek hiányában a tanúsítvány Alanyaként megjelölt szervezet képviselője vagy meghatalmazottja; ● ezek hiányában a tanúsítvány Alanyaként megjelölt domain név, trademark vagy terméknév tulajdonosa, ill. szervezet tulajdonos esetén annak képviselője vagy meghatalmazottja, illetve a domain név fölött kontrollal rendelkező személy. Előfizetővel megegyezik, amennyiben a tanúsítvány Alanyaként egy természetes személy kerül feltüntetésre (és szervezetnem). NL Sign szolgáltatás esetén megegyezik Végfelhasználóval. Archiválás- és Időbélyegszolgáltatás esetén megegyezik Előfizetővel.
Időbélyegző	Olyan elektronikus adat, amely más elektronikus adatokat egy adott időponthoz köt, amivel igazolja, hogy utóbbi adatok léteztek az adott időpontban.
Időbélyegző Kiszolgáló	A Szolgáltató időbéyegzőket kibocsátó műszaki rendszere.
Időbélyegző szolgáltatás	Szolgáltató azon szolgáltatása, amely a számára küldött elektronikus adatok lenyomata alapján egy időbélyegzőt állít elő, az adott adatokhoz.
Időbélyeg-URL	Az időbélyeg-szolgáltatás elérését biztosító, az Előfizető egyedi azonosítóját tartalmazó virtuális token, melyen keresztül Végfelhasználó időbélyeg kéréseket továbbíthat Szolgáltató felé, Szolgáltató pedig a kérés alapján időbélyeg választ továbbít Végfelhasználó felé.

Kézbesítési Megbízott	Olyan Szolgáltatói partner, aki Szolgáltató megbízásából - Igénylő ilyen irányú igénye esetén - az Igénylővel egyeztetett helyen és időben végzi el a Tanúsítványkibocsátáshoz kapcsolódóan az ügyféleszköz átadását. Adott esetben megegyezhet a Regisztrációs Megbízottal.
KGyHSz	Közigazgatási Gyökér Hitelesítés-Szolgáltató Lásd 1.3.5 és http://www.kgyhsz.gov.hu/
Központi Regisztrációs Egység	A Szolgáltató azon saját szervezetén belül működtetett szervezeti egysége, mely feldolgozza a szolgáltatások igényléseit, azonosítja azok Igénylőjét és Előfizetőjét, ellenőrzi az eljárási jogukat és adataikat.
Kezdeti felfüggesztés	A Tanúsítványfelfüggesztés egy speciális esete, amikor a Szolgáltató a tanúsítványt kibocsátása után azonnal felfüggeszti, így megóvva azt a visszaélésektől arra az időszakra, míg a Tanúsítvány és a magánkulcs biztonságosan eljut az Ügyfélhez.
Képviseleti jog	Teljes vagy részleges képviseleti jog vagy ekként is értelmezhető jogviszony (lásd eüt. 82. § (9)).
Kiadó	Szolgáltató tanúsítványokat kibocsátó műszaki rendszere. Szolgáltatónál létezik végfelhasználói és egyes szolgáltatói tanúsítványokat kibocsátó Köztes Kiadó, valamint az ezen egységeket hitelesítő legfelső szintű Gyökér Kiadó, amelyek hierarchiába szervezetten működnek.
Kihelyezett Hitelesítő Egység	A Szolgáltatótól független, önálló szervezet vagy személy (mint Szolgáltatói partner) által, a Szolgáltató előírásai alapján működtetett Hitelesítő Egység.
Kihelyezett Regisztrációs Egység	A Szolgáltatótól független, önálló szervezet vagy személy (mint Szolgáltatói partner) által, a Szolgáltató előírásai alapján működtetett Regisztrációs Egység.
Kikötések (és feltételek)	Szolgáltató azon dokumentumai, amelyek ismertetik, hogy a szolgáltatások nyújtásával kapcsolatosan, milyen elvárásoknak, milyen módon felel meg, s ismertetik a többi szereplő kötelezettségeit és jogait. Ide tartozik a Szolgáltató Szolgáltatási kivonata, Hitelesítési rendje, Szolgáltatási szabályzata, ÁSZF-e, szolgáltatási szerződése, valamint a közöttük létrejött egyéb megállapodások együttesen.
Kriptográfiai eszköz	Olyan biztonságos hardver eszköz, amely a Végfelhasználó magánkulcsát tartalmazza, azt védi a kompromittálódás ellen, s a kulccsal kriptográfiai műveleteket (pl. aláírás, titkosítás) végez a Végfelhasználó számára. Lehet SCD és QSCD, HSM vagy más nem aláírás célú eszköz is. Lehet a Szolgáltató vagy az Ügyfél kezelésében. Utóbbi esetben “Ügyféleszközként” hivatkozunk rá.
Kritikus szolgáltatások	A Szolgáltató tanúsítvány- és kulcselőállítással, az Ügyfelek eszközzel való ellátásával és az állapotváltoztatással kapcsolatos szolgáltatásai.
Kulcscsere	Az a folyamat, amikor a Szolgáltató egy már regisztrált Ügyfél (vagy saját maga) részére bocsát ki új Tanúsítványt és magánkulcsot, annak egy már létező tanúsítványát alapul véve. Az új tanúsítványban a végfelhasználó

	nyilvános kulcsa megváltozik. Lásd a 4.7 fejezet.
Kulcsletét szolgáltatás	Olyan szolgáltatás, amely a végfelhasználó magánkulcsának megőrzését és annak végfelhasználó számára történő átadását biztosítja (arra az esetre, ha a végfelhasználó kulcs elveszne, megsemmisülne vagy más okból használhatatlanná válna).
Magánkulcs	A szolgáltató vagy ügyfél által generált kulcspár egyik kulcsa, amit végfelhasználó kezel. Lásd nyilvános kulcs. Amennyiben a nyilvános kulcs aláíró vagy bélyegző tanúsítványba kerül, akkor megfelel az eIDAS elektronikus aláírás létrehozásához használt adat és elektronikus bélyegző létrehozásához használt adatok definíciójának.
Minősített Aláírás / Bélyegző Létrehozó eszköz	Olyan kriptográfiai eszköz, amely minősített aláírás / bélyegző létrehozására alkalmas (lásd még 1.6.2. Rövidítések, QSCD).
Minősített tanúsítvány	Olyan tanúsítvány, amelyet minősített bizalmi szolgáltató bocsát ki, és amely megfelel az eIDAS Annex I, III vagy IV részének vagy a 1999/93/EC direktívának, attól függően, hogy a tanúsítvány kiadásakor melyik volt hatályban.
Minősített weboldal hitelesítő tanúsítvány	Az eIDAS 3. cikk 39. Pontja szerint: “Olyan weboldal-hitelesítő tanúsítvány, amelyet minősített bizalmi szolgáltató bocsát ki, és amely megfelel az eIDAS IV. mellékletben megállapított követelményeknek.” Olyan minősített tanúsítvány, amely a benne megjelölt weboldalak hitelesítésével biztosítja az oldal látogatóit, hogy a mögött egy valódi és legitim szervezet áll.
Mobil Regisztrációs Munkatárs	Olyan regisztrációs ügyintéző, aki - amennyiben személyes találkozó szükséges - az Igénylő azonosítását - ilyen irányú igénye esetén - az Igénylővel egyeztetett helyen és időben végzi el.
NL Sign szolgáltatás	Biztonságos központi kulcstárolási (menedzselt SCD) és kulcsmenedzsment-szolgáltatás, mely webes felületen keresztül feltöltött dokumentumok elektronikus aláírását/bélyegzését (és időbélyegzését). Az NL Sign szolgáltatás keretében használható tanúsítványok igénylése és az ehhez szükséges regisztrációs adatok bekérése valamint a tanúsítvány kibocsátását követően annak használatba vétele az NL Sign szolgáltatás webes felületein történik.
Nyilvános kulcs	A szolgáltató vagy ügyfél által generált kulcspár egyik kulcsa, amit szolgáltató az általa létrehozott tanúsítványban helyez el. Lásd magánkulcs.
Permanens azonosító	Olyan azonosító, mely a tanúsítvány birtokosát egyedileg azonosítja. A tanúsítványban történő megvalósítása az RFC 4043 alapján történik. Lehet szolgáltató által képzett, vagy hivatalos nyilvántartásban szereplő egyedi azonosító adat. A szolgáltató által képzett azonosító egy OID, ami két részből áll: a Szolgáltató (1.3.6.1.4.1.3555) és az Ügyfél egyedi azonosítójából, ami ezt követi. Az Ügyfél egyedi azonosítója 5-tel kezdődik, amelyet egy szám követ, ami a következő értékeket veheti fel:

	● 1,6,8,10: személyes vagy üzleti tanúsítványok esetén, amikor az azonosító a természetes személy adataiból képzett. ● 2,7,9,11: szervezeti tanúsítványok esetén, amikor az azonosító a szervezet adataiból képzett. Alkalmazása esetén a tanúsítvány Subject/SerialNumber mezőjébe kerül.
Regisztráció	Kezdeti azonosítási eljárás, amelyet Szolgáltató Igénylő és Előfizető személyazonosságának megállapítására, eljárási joguk ellenőrzésére, valamint adatainak felvételére végez.
Regisztrációs egység	A Szolgáltató azon egysége, amely a szolgáltatások igénylésének feldolgozását, az Igénylő és Előfizető regisztrációját, valamint tanúsítványszolgáltatás esetén a tanúsítványba kerülő adatok ellenőrzését végzi. Létezhet a Szolgáltatón belül (mint belső szervezeti egység) vagy kívül (Kihelyezett Regisztrációs Egység) egyaránt.
Regisztrációs felelős	Bizalmi munkakör. Lásd az 5.2.1 Bizalmi munkakörök fejezetet.
Regisztrációs megbízott	Olyan Szolgáltatói partner (illetve annak munkatársa), aki Szolgáltató megbízásából Igénylő helyszínén végzi el a tanúsítványkibocsátáshoz kapcsolódó személyazonosítási feladatokat.
Regisztrációs (és visszavonási) ügyintéző	Szolgáltató Regisztrációs egységén belül e munkakörben dolgozó munkatársak feladata a tanúsítványigénylések kezelése és a tanúsítványigénylésben megadott adatok valódiságának ellenőrzése (lásd 4.2.1 fejezet) valamint a visszavonási igények feldolgozása és végrehajtása (4.9).
SSL tanúsítvány	Weboldal-hitelesítő tanúsítvány
Szabályzatok	Jelen Szolgáltatási Rend és a Szolgáltatási Szabályzat együttes említése.
Szervezet	Tanúsítvány alanya vagy előfizetője tekintetében: jogi személy vagy egyéni vállalkozó vagy egyéni ügyvéd.
Szoftveres tanúsítvány	Olyan tanúsítvány, aminek magánkulcsa nem Kriptográfiai eszközre kerül kiadásra.
Szolgáltatás	Jelen szabályzat keretén belül Szolgáltató bizalmi szolgáltatásai (lásd 1.1 fejezet).
Szolgáltatási Szabályzat, Szabályzat	A bizalmi szolgáltató nyilatkozata az egyes bizalmi szolgáltatások nyújtásával kapcsolatosan alkalmazott részletes eljárási vagy más működési követelményekről (lásd Eüt. 1. § 41.), mely Szolgáltató tevékenységével kapcsolatos részletes eljárási és egyéb működési szabályokat tartalmaz.
Szolgáltatási szerződés	Szolgáltató és Ügyfél között létrejött szerződés, amely a szolgáltatás nyújtására és igénybevételére vonatkozó feltételeket tartalmazza. Megkötése a szolgáltatás igénybevételének előfeltétele.
Szolgáltató	Jelen Szolgáltatási szabályzat szerinti bizalmi szolgáltatásokat nyújtó NETLOCK.
Szolgáltató	Jelen Bizalmi Szolgáltatási Rend, a Bizalmi Szolgáltatási Szabályzat, az

szabályzatai	ÁSZF, a szolgáltatási szerződés, a Szolgáltatási kivonat. Valamint egyéb nem nyilvános szabályzatok.
Szolgáltatói partner	Olyan a szolgáltatótól független, önálló természetes vagy jogi személyek, amelyek a Szolgáltatóval való megállapodás alapján a Szolgáltatás nyújtásában részt vesznek.
Szolgáltatói rendszer	Szolgáltató szolgáltatásnyújtást végző rendszereinek együttese.
Szolgáltatói tanúsítvány	Szolgáltató azon tanúsítványai, amelyeket a szolgáltatásnyújtás érdekében használ (pl. Kiadók és Időbélyegző Kiszolgálók tanúsítványai).
Tanúsítvány	Szolgáltató által kibocsátott hiteles igazolás, amely a nyilvános kulcsot az Alanyhoz kapcsolja, és igazolja e Tanúsítványban közzétett adatok valódiságát.
Tanúsítványaktiválás	Az az állapotváltoztatási eljárás, amely felfüggesztett tanúsítvány érvényességét visszaállítja. Aktiválása után a tanúsítvány visszamenőlegesen, azaz a felfüggesztés időtartamára is újra érvényessé válik, mintha a felfüggesztés meg sem történt volna..
Tanúsítványállapot	A szolgáltató által a tanúsítványok érvényességi ideje alatt nyilvántartott érvényes / visszavont / felfüggesztett státusza, amelyről a tanúsítványvisszavonási listán és a Tanúsítványállapot szolgáltatáson keresztül ad tájékoztatást Ügyfelei és az Érintett felek részére.
Tanúsítványállapot-szolgáltatás (OCSP)	Olyan szolgáltatás, ami egy adott tanúsítvány állapotáról ad valós idejű információt az érintett felek számára. Lásd még: tanúsítványvisszavonási lista.
Tanúsítványfelfüggesztés	Az az állapotváltoztatási eljárás, amelyben a Szolgáltató egy még érvényes Tanúsítvány érvényességét átmenetileg megszünteti az eredetileg tervezett érvényességi idő vége előtt. A tanúsítványfelfüggesztés egy átmeneti állapot, a felfüggesztett Tanúsítvány visszavonható, vagy a Tanúsítvány eredeti érvényességi idejében újra érvényessé tehető. A felfüggesztés visszavonása esetén a Tanúsítvány visszamenőleges hatállyal érvényessé válik, mintha a felfüggesztés meg sem történt volna.
Tanúsítványigénylés	Az a folyamat, amikor Igénylő tanúsítványt igényel, azaz a tanúsítvány elkészítéséhez szükséges adatokat megadja és igazolja a Szolgáltatónak, végül pedig Szolgáltatási szerződés Igénylő és - amennyiben nem egyezik Igénylővel - Előfizető általi aláírásával hitelesíti kérelmét az igényelt tanúsítványra vonatkozóan és ezzel felhatalmazza Szolgáltatót az igényelt tanúsítvány kibocsátására.
Tanúsítványkezelési eljárás	Olyan eljárás, ami új tanúsítvány kibocsátását eredményezi egy meglévő tanúsítvány illetve korábbi ügyfél-regisztráció adatai alapján (lásd 3.3 Azonosítás és hitelesítés tanúsítványkezelési eljárás során és 4. Életciklus követelmények fejezeteket).
Tanúsítványszolgáltatás	Szolgáltató azon szolgáltatása, amelynek keretén belül új tanúsítványt állít elő. Ez történhet egy már létező tanúsítvány alapján (követő kibocsátás tanúsítványkezelési eljárással) vagy ilyen előzmények nélkül (eredeti kibocsátás).

Tanúsítványmegújítás	Az a folyamat, amikor a Szolgáltató ugyanarra a nyilvános kulcsra, változatlan Alannyal egy új Tanúsítványt állít ki, új érvényességi időszakra. Lásd a 4.6 fejezet.
Tanúsítványmódosítás	Az a folyamat, amikor a Szolgáltató egy már regisztrált Igénylő részére bocsát ki új Tanúsítványt egy korábban kibocsátott Tanúsítványa alapján, az abban szereplő nyilvános kulccsal, de megváltozott Alany vagy Szolgáltató adatokkal. Lásd a 4.8 fejezet.
Tanúsítványtár	Szolgáltató kibocsátott tanúsítványokat tartalmazó nyilvántartása, amelyen keresztül lekérdezhetők a szolgáltató által kiadott nyilvános tanúsítványok és a Tanúsítványvisszavonási lista.
Tanúsítványtípus	Szolgáltató által kibocsátott különböző tanúsítványok megkülönböztetése valamilyen jellemző szerint, legfőképpen a felhasználási cél alapján. Lásd a Szolgáltatási szabályzat 1.2.1 pontját.
Tanúsítvány-visszavonás	Az az állapotváltoztatási eljárás, amelyben a Szolgáltató a tanúsítvány érvényességét megszünteti az eredetileg tervezett érvényességi idő lejárta előtt. A tanúsítvány-visszavonás visszafordíthatatlan és végleges állapotváltozást jelent, a visszavont tanúsítvány a visszavonás időpontjában érvényességét veszti, s már soha többé nem lehet újra érvényes.
Tanúsítványvisszavonási lista (CRL)	Szolgáltató által rendszeres időközönként, valamint állapotváltozások hatására a Tanúsítványtárban közzétett hiteles lista azon tanúsítványokról, amelyek ideiglenesen vagy véglegesen nem érvényesek. A listán szereplő tanúsítványok elfogadása, illetve alkalmazása nem ajánlott. A 24/2016. BM rendelet 17. szerinti visszavonási nyilvántartás egy fajtája.
Teszttanúsítvány	A Szolgáltató által tesztelési célra kibocsátott tanúsítvány, ami tartalmában valamely valódi tanúsítvánnyal egyezik meg, de hitelesítési rend mezője és az Alany elnevezése jelzi a felhasználás teszt voltát. Az ilyen tanúsítványok köztelezettségvállalásra nem használhatók, joghatás nem kapcsolódik hozzájuk, elfogadásuk csak tesztelési céllal lehetséges. Szolgáltató nem vállal felelősséget az ilyen tanúsítványok adattartalma, felhasználása, és a hozzájuk kapcsolódó szolgáltatások rendelkezésre állása tekintetében.
UCC weboldal-hitelesítő tanúsítvány	Olyan weboldal-hitelesítő tanúsítvány, melyben több különböző domain név kerül feltüntetésre (a SubjectAltName/DNSname mezőben).
Ügyfélmenü	A Szolgáltató ügyfelei számára a tanúsítványokkal és hozzájuk kapcsolódó szolgáltatásokkal kapcsolatos különböző igénylések elvégzésére illetve a folyamatban lévő igénylések állapotának megtekintésére biztosított, a Szolgáltató weboldalán keresztül elérhető felület, melybe egyedi felhasználónév és jelszó megadásával lehet belépni (ügyfélmenü regisztrációt követően). A minősített tanúsítványok kezeléséhez a minősített ügyfélmenübe, a nem-minősített tanúsítványok kezeléséhez a fokozott biztonságú ügyfélmenübe kell regisztrálni és bejelentkezni.
Ügyfélmenü regisztráció	Az a folyamat, amikor egy természetes vagy jogi személy adatai megadásával létrehozza saját Ügyfélmenüjét, illetve az Ügyfélmenübe való bejelentkezéshez szükséges bejelentkező nevét és jelszavát.

Ügyfél	A Szolgáltatatóval szerződést kötő fél. Tanúsítványszolgáltatás esetén a tanúsítvány Igénylője és Előfizetője (adott esetben ezek a szereplők meg is egyeznek). NL Sign szolgáltatás esetén az Aláírói Partner és a Végfelhasználó. Lásd még az 1.3.3 Előfizető, Végfelhasználó és Igénylő fejezetet
Ügyféleszköz	Lásd Kriptográfiai eszköz.
Ügyfél-regisztráció	Természetes és nem természetes személyek azonosítása, adataik ellenőrzése és rögzítése az első szolgáltatási szerződés és az első tanúsítványkibocsátás megelőzően. Lásd a 3.2 Kezdeti azonosítás fejezetet.
Végfelhasználó	Az a természetes személy, aki a tanúsítványban szereplő nyilvános kulcs magánkulcs párja felett rendelkezik (kizárólagosan használja vagy a használatáért felelős). NL Sign szolgáltatás esetén az a személy, aki az aláírási szolgáltatás keretén belül a magánkulcsa aktiválásával elektronikus aláírási/bélyegző műveletet hajt végre. Lásd még az Ügyfél és Előfizető entitásokat, valamint az 1.3.3 Előfizető, Végfelhasználó és Igénylő fejezetet
Végfelhasználói tanúsítvány, Végfelhasználói kulcs	Az Előfizetők tanúsítványát és kulcsát jelöli, megkülönböztetve a Szolgáltató saját tanúsítványaitól és kulcsaitól.
Weboldal-hitelesítő tanúsítvány	Az eIDAS 3. cikk 38. pontja szerinti tanúsítvány.
Wildcard weboldal-hitelesítő tanúsítvány	Olyan weboldal-hitelesítő tanúsítvány, melyet több aldomain hitelesítésére bocsátott ki szolgáltató (a domain név *.domain.hu formában kerül feltüntetésre, így magában foglalja a domain.hu cím alá tartozó valamennyi aldomaint).

1.6.2 Rövidítések

Hivatkozott jogszabályok rövidítései

eIDAS	Az Európai Parlament és Tanács 910/2014/EU rendelete a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről.
Eüt.	Az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. Évi CCXXII. törvény.
Nytv.	A polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény.

Szmtv.	2007. évi I. törvény a szabad mozgás és tartózkodás jogával rendelkező személyek beutazásáról és tartózkodásáról.
Harmtv.	2007. évi II. törvény a harmadik országbeli állampolgárok beutazásáról és tartózkodásáról szóló törvény
Infotv.	2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
24/2016 BM rendelet	A bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről szóló 24/2016. (VI. 30.) BM rendelet.

Műszaki szakkifejezések rövidítései

ASN.1	Abstract Syntax Notation 1
CA	Certification Authority Kiadó
CAA	Certification Authority Authorization Bizalmi szolgáltató Felhatalmazás
IP	Internet Protocol
IT	Information Technology
BRG	Baseline Requirements Guidelines
CAB Forum	CA/Browser Forum
CP	Certificate Policy Hitelesítési Rend
CPS	Certification Practice Statement
CRL	Certificate Revocation List Tanúsítványvisszavonási lista
CSP	Certification Service Provider
EAL	Evaluation Assurance Level
EV	Extended Validation

EVC	Extended Validation Certificate
EVCG	Extended Validation Certificate Guidelines
FQDN	Fully qualified domain name
gTLD	Generic top-level domain
HSM	Hardware Security Module
ICANN	Internet Corporation for Assigned Names and Numbers
OCSP	Online Certificate Status Protocol Tanúsítványállapot-szolgáltatás
OID	Object Identifier Azonosító
OVC	Organizational Validation Certificate
PIN	Personal Identification Number
PKI	Public Key Infrastructure
SAN SubjectAltName	Subject Alternative Name
SCD	Signature / Seal Creation Device Aláírás / Bélyegző Létrehozó eszköz (Nem minősített)
SSL	Secure Socket Layer
TLS	Transport Layer Security
TSP	Trust Service Provider Bizalmi Szolgáltató
QSCD Korábbi nevén SSCD	Qualified Signature / Seal Creation Device Minősített Aláírás / Bélyegző Létrehozó eszköz
UN	United Nations
IETF	Internet Engineering Task Force
QC	Qualified Certificate

URL	Uniform Resource Locator

Lásd még jelen dokumentum 9.15 pontjában foglaltakat.

2 Közzététel

2.1 Adattárak

Szolgáltató szerződéses feltételeit és szabályzatait PDF formátumban hozza nyilvánosságra weboldalán keresztül. Itt a dokumentumok hatályos verziója mellett megtalálhatóak azok korábban érvényes változatai és a jövőbeli változatok nyilvános tervezetei is.

2.2 A tanúsítványokra vonatkozó információk közzététele

A szolgáltató köteles az archiválás szolgáltatás nyújtásához használt szolgáltatói tanúsítványokat a Kikötésekben előírt módon közzétenni, tanúsítványtárat létrehozni és naprakészen tartani.

A kikötéseket és feltételeket az RFC 3647 szerinti tartalommal és struktúrában kell közzétenni.

2.3 A közzététel időpontja és gyakorisága

Jelen Szabályzattal kapcsolatos új verziók közzététele a 9.12 fejezetben ismertetett eljárásoknak megfelelően történik. A Bizalmi Szolgáltatási Rend új verzióinak közzététele tekintetében lásd a 9.12 fejezetet.

Szolgáltató egyéb szabályzatai és szerződéses feltételei, illetve ezek újabb változatai szükség esetén kerülnek kibocsátására.

Szolgáltató a rendkívüli információkat – amikor arra szükség van – a jogszabályi előírásoknak megfelelően, ennek hiányában késlekedés nélkül közzéteszi.

Az archiválásszolgáltatásban alkalmazott szolgáltatói tanúsítványokat Szolgáltató a használatukat megelőzően teszi közzé.

2.4 Tanúsítványtár elérésének szabályai

Nem értelmezett.

3 Azonosítás és hitelesítés

Archiválás szolgáltatás esetén Szolgáltató az Ügyfél regisztrációját igényli, valamint az előfizetői és szerződéses adatok ellenőrzésre különböző nyilvántartásokat vesz igénybe.

A regisztrált Ügyfelek azonosítása felhasználónév és jelszó alapon történik.

4 Életciklus követelmények

Jelen (4.) fejezet a Szolgáltató archiválás szolgáltatásának igénybevételét és a szolgáltatás életciklusát kezelő műveleteket írja le.

Szolgáltató lenyomatok archiválását (dokumentum nélkül) nem végzi. Az archiválási szolgáltatásából csak a dokumentumok megőrzésre való átvételét szüneteltetheti.
Az archiválási szolgáltatás előzetes regisztrációt követően vehető igénybe, melynek része a szolgáltatásigénylés és a szolgáltatási szerződés megkötése.

4.1 Szolgáltatás igénylése

Archiválás szolgáltatás az alábbiak szerint igényelhető:

- A Szolgáltató weboldaláról letölthető megrendelő űrlap kitöltésével és Szolgáltató email címére való elküldésével.
- Szolgáltatáscsomag keretében a szolgáltatáscsomag webes megrendelő űrlapjának kitöltésével és Szolgáltatóhoz való elküldésével.

Szolgáltató a szolgáltatási szerződés megkötését megelőzően teljes körűen tájékoztatja Igénylőt a szolgáltatás minősített voltáról, a szolgáltatás igénybevételére vonatkozó pontos szerződési feltételekről, beleértve az igénybevételre vonatkozó bármely korlátozást is, az szolgáltatás használatával kapcsolatos kikötésekről és feltételekről, valamint a kapcsolódó jogszabályokról.
Szolgáltató a szabályzatait és egyéb tájékoztató dokumentumait weboldalán nem szerkeszthető, PDF formában teszi közzé, illetve közvetlen a weboldalon megjelenített tartalmak útján is közöl információkat.
Legkésőbb a szerződéskötést követően Szolgáltató elektronikus levélbe illesztett link(ek)en keresztül elérhetővé teszi az Ügyfél számára a szolgáltatási szerződést, a szolgáltatási rendet és a szabályzatot.

4.2 Dokumentum befogadása

Szolgáltató az archiválási szolgáltatás keretében elektronikusan aláírt és időbélyegzett (PAdES és XAdES-T és magasabb) PDF és e-akta formátumú állományokat fogad be, a korábban regisztrált Ügyfeleitől. Egy e-akta állomány egyszerre több hitelesített dokumentumot is tartalmazhat.
Az állományokat Ügyfél titkosított és hiteles (Szolgáltatót azonosító) kapcsolaton keresztül tudja Szolgáltatónak megküldeni, saját azonosítását követően. Tömeges befogadás esetén lehetőség van az állományok tartós dokumentumhordozón való eljuttatására is Szolgáltató részére. A befogadás során Ügyfél metaadatokat is megadhat az egyes állományokkal kapcsolatban.
Szolgáltató az állományokon elhelyezett hitelesítési adatok (aláírások, bélyegzők, tanúsítványok, érvényesítési adatok és időbélyegzők) kapcsán elvárja az általa is követett előírásoknak és szabványoknak való megfelelést. Szolgáltató csak olyan fokozott biztonságú és minősített aláírásokat és bélyegzőket fogad el, melyek tanúsítványait nyilvántartásba vett európai bizalmi szolgáltató bocsátotta ki, s amely gyökértanúsítványa szerepel a szolgáltatás tanúsítványtárában. Ugyanez ez elvárás az időbélyegzők tekintetében. Szolgáltató saját hatáskörben dönthet ettől eltérő aláírások befogadása mellett.

Amennyiben az aláírás / bélyegző érvényesítésére vonatkozó kivárási idő még nem telt el, akkor Szolgáltató a befogadást visszautasíthatja.

Szolgáltató az állomány átvételekor ellenőrzi a rajta található - közvetlenül elérhető (külső) - elektronikus aláírás(okat)t vagy bélyegző(ke)t, valamint az azokon Szolgáltató által kötelezően elvárt időbélyegzőket, majd - amennyiben nem tartalmazzák - beszerezi ezek hosszú távú érvényesítéséhez szükséges információkat (lásd Szolgáltatási Rend 6.9.1 fejezete). Amennyiben az állomány nem aláírt / bélyegzett és időbélyegzett, vagy ha ezen érvényesítési információk nem állnak rendelkezésre és nem is szerezhetők be, illetve ha ezek nem felelnek meg az elvárt formátumoknak, előírásoknak és szabványoknak, vagy ha az ellenőrzés sikertelen, akkor szolgáltató a dokumentumot nem fogadja be, s erről a tényről ügyfelet haladéktalanul értesíti.
Az érvényesítési információ beszerzésére a szolgáltatónak maximum 3 nap áll rendelkezésre.

Az információk beszerzése és a sikeres ellenőrzéseket követően szolgáltató az érvényességi láncon minősített időbélyegzőt helyez el, majd az állomány több helyszínen és eszközön is letárolja, a befogadást pedig e-mailben visszaigazolja az Ügyfél részére, az alábbi tartalommal:

- egy véletlenszerűen generált, egyedi állományazonosító, amellyel a benyújtó a jövőben hivatkozhat a befogadott állományra;
- a benyújtó azonosítója;
- az archiválás időtartama;

A Szolgáltató a visszaigazolásokat legalább fokozott biztonságú elektronikus bélyegzővel és minősített időbélyegzővel látja el. Ügyfélnek meg kell győződnie arról, hogy a visszaigazolás valóban az általa feltöltött dokumentumra vonatkozik és a visszaigazoláson szereplő elektronikus aláírás érvényes. A Szolgáltató kizárólag a végleges visszaigazolás elküldése esetén felel a dokumentum megőrzéséért és a benne szereplő elektronikus aláírások hitelességének hosszú távú biztosításáért.

4.2.2 Megőrzés

Szolgáltató a befogadott elektronikus állományokat az Ügyfél által igényelt időtartamra őrzi meg, majd ezt követően törli a rendszeréből (lásd 6.9.7). A megőrzésre átadott elektronikus állományok megőrzési ideje legalább egy hónap, de legfeljebb 50 év.
Szolgáltató állományokat védi a jogosulatlan hozzáférés, módosítás, törlés vagy megsemmisítés ellen, s biztosítja a jogosultak hozzáférését.
Szolgáltató a befogadott állományok érvényességének megállapítását a teljes megőrzési időre biztosítja.

4.2.3 Archivált állomány és érvényességi lánc átvételének biztosítása

Ügyfél kizárólag biztonságos csatornán, azonosítást és jogosultságellenőrzést követően férhet hozzá a Szolgáltató archívumában lévő (törlési kérést nem kapott) állományaihoz. Az állományok között azok metaadatai alapján tud keresni.

4.2.3.1 Harmadik személy hozzáférése

Ügyfél az általa feltöltött állományokhoz harmadik személy számára hozzáférést engedményezhet (megosztás). Ehhez az adott személyek számára meghívót kell küldenie, s a személynek regisztrálva kell lenni a rendszerben (korábbi vagy ezt követő regisztráció útján). A

megosztott hozzáférés lehet korlátozott (olvasási jog) vagy teljes körű (beleértve a lejárati dátum módosítását, az állomány törlését). A hozzáférés engedményezése megvonható.

4.2.4 Igazolások kibocsátása

Szolgáltató az archívumában őrzött (törlési kérést nem kapott) elektronikus állományokkal kapcsolatban Ügyfél igénylésére igazolást állít ki. Az igazolás kibocsátása az archiváló rendszerbe bejelentkezve igényelhető. Az igazolás az alábbiakat igazolhatja a megőrzésben lévő állományt illetően:

- a rajta elhelyezett elektronikus aláírás vagy bélyegző a létrehozás időpontjában érvényes volt (a letagadhatatlanság igazolása);
- a tartalma megegyezik a bemutatott elektronikus adattal (a sértetlenség igazolása);
- azon meghatározott személy érvényes elektronikus aláírást / bélyegzőt helyezett el (eredet igazolása).

A Szolgáltató által kibocsátott igazolás az alábbiakat tartalmazza:

- az igazolás típusa
- az archivált elektronikus állomány egyedi azonosítója,
- az archivált elektronikus állomány lenyomata,
- az igazolás által érintett aláíró azonosítója (letagadhatatlanság és hitelesség igazolása esetén),
- az igazolás eredménye (érvényes / érvénytelen),
- az igazolás kiállításának időpontja.

A Szolgáltató az igazolást minősített elektronikus bélyegzővel és időbélyegzővel hitelesített elektronikus dokumentum formájában bocsátja ki. Az igazolás egyszerre több állományra is vonatkozhat.

4.2.5 Dokumentum megjelenítése

A Szolgáltató szabványos hosszú távú megjelenítésre alkalmas dokumentum formátumokat fogad be (PDF, XML) amelyek hosszú távú megjelenése is biztosított. Amennyiben az Ügyfélnek értelmezhetőségi (olvashatósági) és megjeleníthetőségi problémái akadnak, a szolgáltató saját telephelyén biztosítja ezek elhárítását.

4.2.6 Felülhitelesítés

A Szolgáltató kriptográfiai gyengüléskor, vagy az erre vonatkozó határozat kézhezvételét követően a határozatban előírt időpontban felülhitelesíti a tárolt állományokat. Az ügyfél erről az értesítésekre vonatkozó csatornákon értesítésre kerül.

4.3 Szolgáltatás elérhetősége és rendelkezésre állása

Szolgáltató az állományok befogadását kivéve biztosítja a szolgáltatás éves szinten 99%-os rendelkezésre állását, valamint garantálja, hogy az eseti szolgáltatás kiesések maximális időtartama legfeljebb 72 óra.

4.4 A szolgáltatási szerződés megszűnése

A szolgáltatási szerződés megszűnését megelőzően Szolgáltató figyelmezteti Előfizetőt a

megszűnés következményeire, s - amennyiben díjhátralékkal nem rendelkezik - lehetővé teszi az a tárolt dokumentumok letöltését.
Egyes rendkívüli esetekben (pl. Előfizető halála vagy jogutód nélküli megszűnése, illetve a rendkívüli felmondás esetei) Szolgáltató saját döntése alapján dönthet a tárolt dokumentumok további 60 napig való megőrzéséről.
A Szolgáltatási szerződés megszűnése után Szolgáltató inaktiválja az Előfizető felhasználói fiókját, majd törli az Előfizetőhöz tartozóan a szolgáltatás keretében tárolt dokumentumokat és érvényességi láncokat.

4.5 Export-import

A szolgáltató a dokumentumokba ágyazza a felülhitelesítési információkat, így a letöltött dokumentum tartalmazza az evidenciát is, külön exportálásra (evidenciákkal) nincs szükség, a letöltött állomány másik szolgáltató által befogadható.; más szolgáltatótól a kiterjesztett állomány standard feltöltéssel teljesíthető, így export-importot a szolgáltató a standard eléréseken biztosít. Egyedi eljárás igénylése írásban az ügyfélszolgálati eléréseken lehetséges, a dátum és a kritérium naplózásra kerül.

4.6 Dokumentum és érvényességi lánc törlése

A Szolgáltató a megőrzési idő lejáratakor vagy Ügyfél külön igénylése alapján visszaállíthatatlan módon törli az archivált elektronikus állomány minden példányát. Törlés után az állományt nem lehet visszaállítani.
A törlési igény az Ügyfélmenün keresztül adható le.
A törlést a Szolgáltató az igénylést követő 30 napon belül hajtja végre. Törlési igénylés oly módon is benyújtható, hogy azt a Szolgáltató ne azonnal, hanem egy meghatározott időpontban hajtsa végre.
A törlésről Szolgáltató egy elektronikus bélyegzővel és időbélyegzővel hitelesített igazolást juttat el a törlést kérőnek. A visszaigazolás tartalmazza a törölni kívánt (törölt) elektronikus állomány egyedi azonosítóját, a törlést igénylő azonosítóját, a törlés tényét valamint a törlés időpontját.

5 Fizikai, eljárásbeli és személyzeti biztonsági óvintézkedések

A kockázatok csökkentése érdekében Szolgáltató az általa biztosított szolgáltatásokhoz szükséges hardver, szoftver, illetve egyéb eszközeit két, fizikailag egymástól elkülönült helyszínen, egy elsődleges és egy másodlagos helyszínen tárolja. A két helyszínre vonatkozó előírások megegyezőek, az esetleges eltérések a megfelelő pontoknál feltüntetésre kerültek.

A szolgáltatói rendszerek konfigurációját a Szolgáltató rendszeresen ellenőrzi a biztonsági előírásokat sértő változások kiszűrése érdekében.

A hitelesítő és regisztrációs egységek eszközeit kizárólag az erre felhatalmazott, megfelelően kioktatott és ellenőrzött tudású személyzet kezeli.

Az egységek adatállományairól biztonsági mentések készülnek (ld. 6.5 alfejezet). A mentéseket a Szolgáltató az 5.5.2 pontban meghatározott ideig megőrzi.

A Szolgáltató a fizikai, eljárásbeli és személyzeti előírásokat rendszeresen elvégzett kockázatelemzéssel vizsgálja. A Szolgáltató az általa használt eszközök (beleértve az információs vagyont is) tekintetében vagyonnyilvántartást vezet.

Szolgáltató nem nyilvános Biztonsági Szabályzata tartalmazza az információbiztonsági szabályozással kapcsolatos előírásokat.

A Biztonsági szabályzatot és a vagyonnyilvántartást a Szolgáltató rendszeres időközönként, vagy jelentős változás esetén haladéktalanul felülvizsgálja azok folyamatos alkalmazhatósága, megfelelősége és eredményessége tekintetében.

5.1 Fizikai óvintézkedések

A fizikai óvintézkedések célja a Szolgáltató bizalmas információira és fizikai körleteire (szerverterem, illetve szerverszoba) irányuló jogosulatlan hozzáférés, károkozás és illetéktelen behatolás megakadályozása. A fizikai hozzáférés tekintetében Szolgáltató megfelelő jogosultságrendszert alkalmaz az ellenőrzött hozzáférés érdekében és azokat rendszeres időközönként felülvizsgálja.

Az értékek elvesztésének, sérülésének, kompromittálódásának, valamint a működési tevékenység megzavarásának elkerülésére a Szolgáltató a Biztonsági Szabályzatban meghatározott intézkedéseket követi.

A kritikus és érzékeny információt feldolgozó szolgáltatások megvalósítására és a kriptográfiai modulok alkalmazására és tárolására biztonságos helyszíneken került sor. A biztosított védelem arányban áll a Szolgáltató által végzett kockázatelemzésben megállapított kockázatokkal.

5.1.1 Telephely felépítése

Szolgáltató a telephelyén, egy védett számítógépteremben valósítja meg a leginkább veszélyeztetett szolgáltatásokat. A számítógépteremben a fizikai hozzáférés, beléptetés ellenőrzése és felügyelete, áramellátás, légkondicionálás, beázás és elárasztódás elleni védekezés, tűzmegelőzés és tűzvédelem, adathordozók tárolása, telekommunikációs hálózat elérhetősége, elektromágneses kisugárzás stb. védelmi szempontok egységes érvényesítésére került sor. Illetéktelen személyek a számítógépterembe nehezen juthatnak be, a biztonsági őrség viszont rövid idő alatt meg tudja közelíteni riasztás esetén. A biztonsági körletnek nincs ablaka, a bejárati ajtókon kívül csak a különösen erős fal bontásával lehetne behatolni ide. A helyiség redundáns klíma-, automata tűzoltó, továbbá illetéktelen behatolást jelző (riasztó) berendezéssel van ellátva. Az eszközök többszörösen túlbiztosított elektromos energiaellátással rendelkeznek.

A Szolgáltató másodlagos helyszíne egy védett számítógépterem szerverszéfjében található, melynek biztonsági szintje megegyezik a telephely biztonságával.

5.1.2 Fizikai hozzáférés

A biztonsági körletek pontos paramétereit, illetve a belépni jogosultak listáját a mindenkori belső operációs dokumentumok tartalmazzák. A biztonsági körletekbe bizalmi munkakört betöltő munkatársakon kívül más személyek csak külön felhatalmazással és kísérettel léphetnek be. A számítógépterembe a belépés személyhez kötött elektronikus kártyával történik a belépések fizikai és elektronikus naplózása mellett. A számítógéptermen belül a szolgáltatói rendszerek egy olyan elkülönült részen kerültek kialakításra, ahova biometrikus azonosítást követően lehet belépni. A biztonsági körlet beléptető előhelységét, illetve magát a számítógéptermet 24 órás

videó kamerás megfigyelő rendszer is védi.

A másodlagos helyszín beléptetési rendszere biometrikus azonosítással nem rendelkezik, de az egyenszilárdság megőrzésére, a másodlagos helyszínt biztonságát állandó élőerős védelem is biztosítja. A szerverszobába az arra jogosult munkatársak kártyás azonosítást követően léphetnek be; a be-, illetve kilépések folyamatos naplózásra kerülnek. A szerverszoba 24 órás videós kamerás megfigyelő rendszer is védi.

A Szolgáltató kockázatelemzése a kritikus szolgáltatások keretében foglalkozik a fizikai hozzáférés szabályozásával, a természeti katasztrófa elleni védelemmel, a villámvédelemmel, a tűzbiztonsági tényezőkkel, a támogató eszközök (különösen áram és klíma) meghibásodásával, az építmény összeomlásával, vízvezeték szivárgással, talajvíz elleni védelemmel, lopás, betörés és behatolás elleni védelemmel, valamint a katasztrófa utáni helyreállítással.

5.1.3 Áramellátás, légkondicionálás

A Szolgáltató védett számítógép termének zavartalan áramellátása kiemelten fontos a folyamatos üzemeltetés biztosítása érdekében, melynek érdekében a Szolgáltató az alábbi intézkedéseket alkalmazza/alkalmaztatja:

- szünetmentes energiaellátás,
- zárlati leoldásra szelektív áramkörök,
- villamos zavar, villám és túlfeszültség védelem.

A szünetmentes energiaellátást biztosító rendszer felépítése a következő:

- dízel gépes áramfejlesztő,
- lokális akkumulátoros szünetmentes tápegység,
- redundáns tápválasztó.

Az alkalmazott üzemmód pedig az alábbi:

- az üzemi táp kimaradása vagy csökkenése esetén a rendszer átkapcsol a tartalék tápra,
- ezalatt a rendszer elindítja az áramfejlesztőt,
- amikor az üzemi táp ismét használható (5 percen keresztül folyamatosan), akkor a rendszer visszatér rá.

Zárlati leoldásra szelektív áramkörök segítségével a gépteremben több egymástól független működésű rendszer lett kialakítva a folyamatos üzemeltetés támogatására. Az elosztó hálózat úgy lett megtervezve, hogy egy eszközcsoport zárlata esetén csak a zárlatot okozó eszközcsoport legyen áramtalanítva, a többi hibátlan eszközcsoport üzemben maradjon.

A szerverteremben biztosított a géptermek épülettől független légkondicionálása. A védett számítógépterem a bejutó levegő tisztaságát megfelelő szűrőrendszerrel biztosítja, gondoskodik a levegőből a különféle szennyeződések kiszűréséről, tovább biztosítja a kezelőszemélyzet részére szükséges levegőt. A levegő nedvességtartalma és hőmérséklete folyamatosan ellenőrzött. A légkondicionáló berendezések biztosítják az informatikai rendszerek megfelelő hűtését. A folyamatos üzemvitelt egy második (tartalék) klímaberendezés is támogatja, mely szükség esetén működésbe lép. A klímaberendezések elhelyezésének módja biztosítja, hogy azok karbantartása ne okozzon zavart a gépterem működésében.

5.1.4 Beázás és elárasztódás veszélyeztetettsége

A Szolgáltató szolgáltatási helyszínei védettek a beázástól és az elárasztódástól. A védett számítógépteremben a biztonságot növeli az álpadló alkalmazása.

5.1.5 Tűzmegelőzés és tűzvédelem

A Szolgáltató szolgáltatási helyszínei a tűzvédelmi előírásoknak megfelelően működnek. A helyszínek tűz és füstérzékelőkkel, kézi és automata oltó berendezésekkel rendelkeznek. A kézi oltó berendezések helye és a menekülési útvonal jól látható helyen jelzésre került.

5.1.6 Adathordozók kezelése

Szolgáltató adathordozóinak biztonságos tárolására biztonsági körlet, illetve egy bérelt banki széf szolgál. A kritikus adatokról Szolgáltató több mentési példánnyal rendelkezik. A Szolgáltató folyamatosan gondoskodik, és megfelelő intézkedéseket tesz az adathordozó avulás megakadályozására.

Szolgáltató az érzékeny adatokat tartalmazó adathordozókat a Biztonsági Szabályzatban előírt módon semmisíti meg, amennyiben azokra már nincs szükség. A selejtezett eszközök tartalmát Szolgáltató véglegesen törli, vagy az eszközt helyreállíthatatlanul tönkreteszi.

5.1.7 Hulladékelhelyezés

A fizikailag megsemmisítés kapcsán a Szolgáltató az alábbiak szerint jár el:

- a papíralapú dokumentumok zúzógéppel felaprításra kerülnek,
- a hajlékony lemezek (házából való kibontás után) zúzógéppel felaprításra kerülnek,
- egyéb más mágneses adathordozók demagnetizálás után összetörésre kerülnek;
- egyéb más adathordozók összetörésre kerülnek.

5.1.8 Mentés külső helyszínen

Szolgáltató az üzemmenet folytonossága és az adatvesztés elkerülése érdekében mentéseket végez és biztosítja az informatikai rendszer egészének szükség esetén való helyreállíthatóságát. A mentéseket védi a jogosulatlan hozzáféréstől, módosítástól és törléstől, és a megsemmisüléstől. A rendkívüli helyzetekre való felkészülés magában foglalja a kidolgozott tervek adott esetekre történő alkalmazását és tesztelését is.

A megőrzendő adatok biztonságos tárolását Szolgáltató csak írható médiával, távoli helyen tárolt mentéssel vagy több tárolási helyen történő távoli párhuzamos tárolással végzi.

5.2 Eljárásrendi biztonsági intézkedések

Szolgáltató gondoskodik rendszerei biztonságos, szabályszerű, a meghibásodás minimális kockázata melletti üzemeltetéséről. Ennek érdekében elegendő számú és megfelelő képzettséggel, műszaki tudással, tapasztalattal rendelkező személyzetet alkalmaz.

A minősített szolgáltatások esetében Szolgáltató a jogszabályoknak és szabályzatainak megfelelő naprakész belső irányítási és ellenőrzési eljárásrendet és kapcsolódó felelősségi rendszert működtet. A rendszer megfelelő működését a független rendszervizsgáló ellenőrzési tevékenység is biztosítja.

Szolgáltató külső, független rendszervizsgáló által folyamatosan ellenőrzött minőségirányítási és információbiztonsági irányítási rendszerrel rendelkezik.

Szolgáltató a minősített szolgáltatás nyújtása során létrejövő és kezelt adatot a jogszabályok és a szolgáltatási szabályzatban meghatározott kockázatelemzés alapján biztonsági osztályba sorolja, és gondoskodik azok megfelelő nyilvántartásáról, ellenőrzéséről, védelméről, valamint az

ehhez szükséges felelősségi rendszer működtetéséről.

5.2.1 Bizalmi munkakörök

Szolgáltatónál bizalmi munkakört (lásd Bizalmi Szolgáltatási Rend 5.2.1 fejezet) olyan személy tölt be, akinek a bizalmi munkakör betöltéséhez szükséges befolyásmentességét, szakértelmét szakmai gyakorlat, végzettség és szakképesítés igazolja.

Az informatikai rendszerért általánosan felelős munkakört olyan személy tölti be, aki szakirányú felsőfokú végzettséggel[3] és legalább három év, az informatikai biztonsággal összefüggésben szerzett szakmai gyakorlattal rendelkezik.

Szolgáltató a bizalmi munkakört betöltő személyt munkaviszonyban foglalkoztatja, és a bizalmi munkakört betöltő személy független minden olyan érdektől, amely hátrányosan érintheti a szolgáltatás megbízhatóságát és biztonságát. Szolgáltató gondoskodik arról, hogy a szolgáltatások nyújtásával kapcsolatban álló személy a szükséges és megfelelően naprakész tudással és tapasztalattal rendelkezzen. Szolgáltató valamennyi bizalmi munkakör betöltését biztosítja.

A Szolgáltató a bizalmi munkakörökről naprakész nyilvántartást vezet, változás esetén a változás tényét haladéktalanul bejelenti a Bizalmi Felügyeletnek.

5.2.2 Az egyes feladatokhoz szükséges személyzeti létszám

Nincs előírás.

5.2.3 Az egyes szerepkörökhöz tartozó azonosítás és hitelesítés

A Szolgáltató valamennyi, bizalmi munkakört betöltő munkatársa a zárt körletbe csak megfelelő azonosítást és hitelesítést követően léphet be, amely az informatikai rendszerekhez való hozzáférésnél további azonosítással egészül ki. Sikeres azonosítás és hitelesítés nélkül a zárt körletbe való bejutás, illetve rendszerhozzáférés nem lehetséges, így egyetlen biztonság szempontjából kritikus tevékenység sem végezhető el.

Szolgáltató informatikai rendszerének minden felhasználóját és az adminisztratív folyamatok minden szereplőjét személy szerint azonosítja, kivéve a nyilvános adatszolgáltatásához kizárólag olvasási jogosultsággal rendelkező felhasználókat. Informatikai rendszereihez csak az arra felhatalmazott személyek férhetnek hozzá. A szolgáltató adminisztrálja a Rendszeradminisztrátorok, Rendszerüzemeltetők és Független rendszervizsgálók rendszerhozzáférését, beleértve a felhasználói fiók kezelését, alkalmi módosítását és adott esetben a hozzáférés megszüntetését.

Az egyes alkalmazásokhoz való hozzáférések korlátozásra kerülnek. A rendszer el tudja különíteni az egyes bizalmi munkaköröket, így különösen a Rendszeradminisztrátori és Rendszerüzemeltetői hozzáféréseket.

A személyzetet azonosításra és hitelesítésre kerül a szolgáltatások szempontjából kritikus alkalmazások használata előtt, s tevékenységükkel kapcsolatban elszámoltathatók.

A bizalmi munkakörhöz tartozó jogosultsági szinteket a Szolgáltató a Személyzeti Politikájában rögzíti.

[3] szakirányú felsőfokú végzettség a matematikusi, fizikusi egyetemi végzettség vagy műszaki tudományterületre tartozó mérnöki szakon szerzett főiskolai vagy egyetemi végzettség

5.2.4 Egyes szerepkörök összeférhetetlensége

Szolgáltató a rendszereiben olyan biztonsági előírásokat alkalmaz, illetve jogosultsági szinteket határoz meg, amely minimalizálja az azonosítatlan vagy nem szándékolt módosításokat, illetve csökkenti a visszaélési lehetőségeket.

A feladatkörök elhatárolása végett

- a biztonsági tisztviselő nem látja el a független rendszervizsgáló és az informatikai rendszerért általánosan felelős vezető feladatait;
- a független rendszervizsgáló nem látja el az informatikai rendszerért általánosan felelős vezető feladatait;
- a biztonsági tisztviselő nem látja el a rendszeradminisztrátor feladatait; és
- a független rendszervizsgáló nem látja el a regisztrációs felelős és a rendszeradminisztrátor feladatait.

Az összeférhetetlenségre vonatkozó részletszabályokat Szolgáltató Biztonsági Szabályzata tartalmazza.

5.3 Személyzeti biztonsági intézkedések

A személyzetre vonatkozó óvintézkedések célja az emberi hibák, lopás, csalás és a lehetőségekkel való visszaélés kockázatának csökkentése.

Ennek érdekében Szolgáltató a személyi biztonsággal már a felvételi szakaszban foglalkozik, majd az alkalmazás során történő ellenőrzésekkel biztosítja.

Szolgáltató a Biztonsági Szabályzatának részeként pontosan és részletesen kidolgozott, folyamatosan karbantartott Személyzeti Politikával rendelkezik. A Személyzeti Politikájában meghatározott ideiglenes és állandó szerepköröket és felelősségeket munkaleírásokban dokumentálja, amelyek tartalmazzák:

- a szerepkörök információkezelési lehetőségei és a különböző hitelesítési folyamatokra való hatásai alapján felmérhető kockázati besorolását,
- a szükséges szakismereti és tapasztalati követelményeket,
- a munkakörrel és a munkatárs feladataival összefüggő tevékenységek leírását, a felelősségek körét és mértékét, továbbá a kapcsolódó munkakörök megnevezését.

A Szolgáltató munkavállalói mindaddig nem tölthetnek be bizalmi munkakört, amíg a személyükkel kapcsolatos ellenőrzések végrehajtása és a szükséges nyilatkozatok megtétele meg nem történt, és a megfelelő képzésben és tapasztalatszerzésben részt nem vettek.

A Szolgáltató vezető tisztségviselői, vezető beosztású munkatársai és bizalmi munkaköröket betöltő munkatársai nem állnak a bizalmi szolgáltatási tevékenység gyakorlását kizáró foglalkozástól eltiltás hatálya alatt valamint függetlenek minden olyan kereskedelmi, pénzügyi és egyéb hatástól, ami hátrányosan befolyásolhatja a Szolgáltató által nyújtott szolgáltatások iránti bizalmat.

5.3.1 Képzettségre, gyakorlatra és megbízhatóságra vonatkozó követelmények

Szolgáltató olyan munkatársakat és adott esetben olyan alvállalkozókat alkalmaz, akik megbízhatóak, rendelkeznek a szükséges szakértelemmel, tapasztalattal és képesítésekkel, valamint megfelelő képzésben részesültek a biztonságra és a személyes adatok védelmére

vonatkozó szabályokkal kapcsolatban, továbbá olyan igazgatási és ügyvezetési eljárásokat alkalmaz, amelyek megfelelnek az európai és nemzetközi szabványoknak.

Minden bizalmi munkakörre jelölt személy (emberi megbízhatósága és szakmai alkalmassága ellenőrzése céljából) kezdeti ellenőrzésen megy keresztül. E biztonsági alapellenőrzés során az ellenőrzést végző szakemberek: az életrajzban megadott adatokat (életrajzi elemek, referenciák, szakmai előmenetel stb.) ellenőrzik. Ennek során:

- a képzettségre vonatkozó adatokat egybevetik a jelölt által benyújtandó bizonyítványokkal, diplomákkal,
- a gyakorlati tapasztalatra vonatkozó állításokat személyes referenciákon keresztül, publikációkra alapozva, illetve egyéb úton igazolják.

Az ügyfélregisztráció területén dolgozó munkatársak ismerik a forgalomban lévő hatósági, illetve azonos funkciójú dokumentumokat, azok fajtáit, ismertetőjegyeit, képesek az átadott iratok érvényességének megállapítására.

A minősített szolgáltatónál bizalmi munkakört csak olyan személy tölthet be, akinek a bizalmi munkakör betöltéséhez szükséges befolyásmentességét, szakértelmét a minősített szolgáltató szakmai gyakorlattal, végzettséggel és szakképesítéssel igazolni tudja.

Az informatikai rendszerért általánosan felelős munkakört olyan személynek kell betöltenie, aki a 24/2016 BM rendelet által elfogadott szakirányú felsőfokú végzettséggel és legalább három év, az informatikai biztonsággal összefüggésben szerzett szakmai gyakorlattal rendelkezik.

Szolgáltató a bizalmi munkatársakat munkaviszonyban köteles foglalkoztatni. Szolgáltatónak a bizalmi munkakörre jelölt személy foglalkoztatásának megkezdése előtt meg kell győződnie arról jelölt független minden olyan érdektől, amely hátrányosan érintheti a minősített szolgáltatás megbízhatóságát és biztonságát.

Valamennyi bizalmi munkakört betöltő munkatársnak a biztonsági alapellenőrzésen túl időszakos biztonsági ellenőrzéseken is át kell átesniük.

Nem tölthet be bizalmi munkakört az a személy, aki akár az alap, akár egy időszakos biztonsági ellenőrzésen a „magas biztonsági kockázat” minősítést kapja. Bizalmi munkakört csak büntetlen előélettel rendelkező személy tölthet be, amit a felvételi eljárás során 3 hónapnál nem régebbi erkölcsi bizonyítvánnyal kell igazolni.

Az időszakos biztonsági ellenőrzésre évente kerül sor valamennyi bizalmi munkakört betöltő (lásd 5.2.1 pont) munkatárs esetén.

A Regisztrációs felelősök kijelölésüket követően a munkakörük betöltéséhez szükséges elméleti és gyakorlati alapkiképzésben vesz részt, aminek a végén vizsgázniuk kell. Ennek a képzési formának a fő célja a szolgáltatásra vonatkozó egységes biztonságpolitika megismerése, megértése, az ezen alapuló aktuális eljárások későbbi helyes alkalmazása érdekében. További részletek a Személyzeti Politikában találhatók.

A bizalmi munkakört a munkatársak a megfelelő gyakorlati tapasztalat megszerzését követően tölthetnek be.

5.3.2 Ellenőrzési eljárások

A felvételi eljárás során a Szolgáltató a személyek személyazonosságáról fizikai jelenlétük során vagy fényképes személyazonosító okmányaik ellenőrzésével győződik meg. Mindezek mellett a Szolgáltató a felvételi eljárás során figyelembe veszi a korábbi munkahelyekre, releváns

végzettséget és szakmai referenciákra vonatkozó információkat is.

A bizalmi munkakör munkatársai az ellenőrzés lefolytatását megelőzően nem kaphatnak hozzáférést a Szolgáltató rendszereihez.

5.3.3 Képzési követelmények

A bizalmi munkakört betöltő munkatársaknak rendelkezniük kell a feladataik ellátásához szükséges tudással. Ennek érdekében a bizalmi munkakört betöltő munkatársaknak kinevezésüket megelőzően tudásuk igazolására vizsgát kell tenniük. Amíg sikeres vizsgát nem tesznek, nem férhetnek hozzá a szolgáltatói rendszerekhez. A vizsga és a képzés a bizalmi munkakör típusától függően a következő ismeretekre terjed ki:

- PKI alapismeretek;
- Hitelesítés és ellenőrzési szabályok és eljárások;
- Biztonsági és adatvédelmi szabályok;
- Általános fenyegetések az információhitelesítési eljárásokra (beleértve az adathalász és egyéb social engineering taktikákat);
- A Szolgáltatási Szabályzat és egyéb szabályzatok előírásai;
- Egyes tevékenységük jogi következményei;
- Szolgáltató informatikai rendszerének sajátosságai és kezelésének módja.

5.3.4 Továbbképzési gyakoriságok és követelmények

A Szolgáltató továbbképzésre és oktatásra vonatkozó gyakorlatát az éves továbbképzési tervben határozza meg.

Abban az esetben, amikor a bizalmi szolgáltatásban jelentős változás következik be, valamennyi munkatárs a szükséges felépítésű és szintű moduláris továbbképzésben részesül, illetve megkapja a szükséges dokumentációkat.

5.3.5 Munkabeosztás körforgásának sorrendje és gyakorisága

A vonatkozó szabályokat a Szolgáltató Személyzeti Politikája tartalmazza.

5.3.6 Jogosultatlan tevékenységek büntető következményei

A szolgáltató rendszerének nem engedélyezett használatára, illetve a szolgáltatás nyújtása közben elkövetett hibákra, mulasztásokra, károkozásokra vonatkozó szankciókat a Szolgáltató a bizalmi munkakört betöltő személyek munkaszerződésében rendezi.

5.3.7 Szerződéses közreműködőkre vonatkozó követelmények

A Szolgáltató nem munkaviszonyban dolgozó szerződéses közreműködőire ugyanazok a biztonsági szabályok vonatkoznak, mint a munkaviszonyban dolgozókra.

5.3.8 A személyzet számára biztosított dokumentumok

A Szolgáltató folyamatosan biztosítja a szolgáltatásnyújtásban közreműködő személyek részére a szerepkörük ellátásához szükséges aktuális szabályzatokat és dokumentációkat.

5.4 Naplózási eljárások

Szolgáltató hitelesítési rendszere a jogszabályi, illetve az egyes szabványokban, előírásokban meghatározott követelményeknek megfelelő, széleskörű naplózási tevékenységet folytat az archiválásra vonatkozó műveletek és az ezek során felhasznált adatok megőrzése érdekében. A napló tartalmazza a bejegyzés pontos idejét, a naplózott esemény bekövetkeztének dátumát és pontos idejét, az esemény típusát, az esemény követhetőségéhez, rekonstruálásához szükséges adatokat, az esemény kiváltásában közreműködő felhasználó vagy más személy nevét, az esemény végrehajtás sikerességét, illetve sikertelenségét. A Szolgáltató a naplókban feltüntetett időt olyan gyakorisággal szinkronizálja, hogy a saját idő és a valódi idő közti eltérés ne haladja meg az 1 másodpercet. Az esetleges ennél nagyobb eltérések szintén naplózásra kerülnek.

A Szolgáltató egyéb rendszerei szintén naplóznak. E naplózások tulajdonságai az adott alkalmazások függvényei. A naplózások elemei elkülönülten keletkeznek a különböző modulokban. A több komponensből álló rendszer miatt a napló állományok nem egy helyen keletkeznek, de feldolgozásuk egy központi helyen történik.

Az archiválási szolgáltatás esetén Szolgáltató naplózza a Bizalmi Szolgáltatási Rendben előírt eseményeket.

Szolgáltató a naplóállomány minden bejegyzését védi a módosítástól és a jogosulatlan hozzáféréstől. A naplót úgy kezeli, hogy kizárható a napló megsemmisítése, a napló bejegyzéseinek törlése, módosítása, a bejegyzések sorrendjének bármilyen módon történő megváltoztatása. Szolgáltató a naplóról rendszeres mentést készít, valamint gondoskodik a naplóadatok folyamatos értékeléséről és ellenőrzéséről.

Operatív szinten az egyes rendszerek üzemeltetési leírásai szabályozzák a napló adatok kezelését.

5.4.1 A tárolt események típusai

Szolgáltató által alkalmazott rendszer minden jogszabályban előírt eseményt és hibát regisztrál, amely a szolgáltatások szempontjából kritikus. A naplóállományok automatikusan vagy manuálisan kerülnek rögzítésre. A naplóállományok mellett a Szolgáltató egyes események rögzítésére jegyzőkönyvet használ.

A Szolgáltató a Biztonsági Szabályzatban részletezi, hogy az egyes események kapcsán pontosan milyen adatokat/eseményeket rögzít.

A naplózott események időponttal ellátott bejegyzésként kerülnek napló állományba. A Szolgáltató a napló minden bejegyzését elektronikus aláírás és biztonsági másolat és mentés alkalmazásával védi a módosítástól, illetéktelen hozzáféréstől, megsemmisítéstől, a napló bejegyzéseinek törlésétől, a bejegyzések sorrendjének bármilyen módon történő megváltoztatásától.

A naplóban lehetséges az esemény típusa és/vagy a felhasználó személye szerinti keresés. A naplóbejegyzések szöveges formátumúak.

5.4.2 A naplófájl feldolgozásának gyakorisága

Szolgáltató naplóbejegyzéseinek átvizsgálása napi rendszerességgel megtörténik az arra megfelelő szakértelemmel és jogosultsággal rendelkező független rendszervizsgálók által. A kiértékelésre manuálisan és szoftvereszközök segítségével kerül sor.

A kiértékelés során az értékelő elemzi a rendszerek által generált hibaüzeneteket, a forgalmi

adatokban bekövetkezett jelentős változásokat, a szokásostól eltérő mintákat, valamint a gyanús aktivitásokat. A kiértékelés tényét és eredményét, valamint az esetleges szükséges intézkedéseket az értékelő, illetve a szoftvereszköz rögzíti.

Szolgáltató hálózati védelmi rendszerei automatikus riasztási funkciókkal is el vannak látva az erőforrásokhoz történő jogosulatlan hozzáférés észlelésének jelzésére. Ilyen riasztási esetekben a naplóbejegyzések soron kívül átvizsgálásra kerülnek. Rendellenességek észleléskor, reklamációkor vagy egyéb megkeresések kapcsán is sor kerülhet a napló adatok rendkívüli átvizsgálására.

5.4.3 A naplófájl megőrzési időtartama

A napló állományok keletkezésük helyén tárolódnak, illetve archiválásra kerülnek (ld. 5.5.2 pont), és a velük kapcsolatba hozható időbélyegeket hitelesítő tanúsítványok érvényességének lejártától számított 10 évig, illetőleg a velük kapcsolatban felmerült és bejelentett jogvita jogerős lezárásáig megőrződnek. A naplófájlok a Független rendszervizsgálók számára hozzáférhetők.

5.4.4 A naplófájl védelme

Szolgáltató hitelesítési rendszerének naplóbejegyzései a Szolgáltató elektronikus aláírásával ellátva, a törlések és beszúrások észrevétlen végrehajtását kizáró módon kerülnek tárolásra.

A napló állományt a véletlen és szándékos rongálások ellen biztonsági mentések védik. A személyes adatokat tartalmazó naplóbejegyzések esetében Szolgáltató gondoskodik az adatok bizalmas tárolásáról. A napló állományokhoz való hozzáférésre csak azok jogosultak, akiknek erre munkakörük folytán szükségük van (jellemzően Független rendszervizsgálók). Szolgáltató a hozzáféréseket biztonságos módon ellenőrzi.

5.4.5 A naplófájl mentési eljárásai

A naplóállományok rendszeresen mentésre kerülnek az 5.1.6 és 5.1.8 pontban meghatározott módon. Amennyiben a naplóbejegyzés egy helyen keletkezik, a Szolgáltató 24 (huszonnégy) órán belül gondoskodik a biztonsági másolat létrehozásáról.

5.4.6 A naplózás adatgyűjtési rendszere

A naplóbejegyzéseket az alkalmazások automatikusan gyűjtik és tárolják a napló állományokban. A mentett médiákat Szolgáltató napi rendszerességgel begyűjti. A médiákat Szolgáltató saját munkatársai szállítják a megőrzési helyre.

5.4.7 Az eseményeket kiváltó Ügyfelek értesítése

A naplóbejegyzéseket kiváltó személyeket, egységeket és alkalmazásokat Szolgáltató nem értesíti, szükség esetén azonban bevonhatja őket az esemény kivizsgálásába. Az esemény kiváltásában közreműködőknek a Szolgáltatóval fennálló szerződéses viszony vagy jogszabály rendelkezése esetén kötelessége a Szolgáltatóval való együttműködés.

5.4.8 Sebezhetőség felmérése

A naplóbejegyzések feldolgozása során Szolgáltató a naplózott események alapján a sebezhetőségre vonatkozó felméréseket végez. A napi rendszerességgel végzett feldolgozáson

túl Szolgáltató szakemberei havonta áttekintik a rendkívüli eseményeket és ezek alapján a sebezhetőségre vonatkozó elemzéseket végeznek. Ezen elemzések alapján a Szolgáltató lépéseket tesz a rendszer biztonságának javítására.

A Szolgáltató negyedévente sebezhetőség felmérést végez, amely segítségével azonosítja, értékeli és kockázati osztályba sorolja az olyan előrelátható külső és belső fenyegetettségeket, amelyek lehetővé tehetik az archiválás szolgáltatás jogosulatlan elérését, a szolgáltatásnyújtással összefüggésben tárolt adatok nyilvánosságra hozatalát, megváltoztatását, megsemmisítését vagy más visszaélést. A kockázatelemzés a bekövetkezés esetén a várható kárra is kiterjed. A kockázatelemzés a fentiek mellett tartalmazza a fenyegetettségek elhárítására a Szolgáltató által alkalmazott folyamatok, védelmi intézkedések leírását is.

5.5 Adatok archiválása

A Szolgáltató a szolgáltatással kapcsolatos adatokat a jelen fejezetben meghatározott módon és ideig őrzi meg.

Szolgáltató az archivált adatállomány minden bejegyzését védi a jogosulatlan módosítástól, törléstől, megsemmisüléstől és jogosulatlan hozzáféréstől. Az elektronikus formában tárolt archivált adatállományt legalább fokozott biztonságú elektronikus aláírással vagy bélyegzővel, és időbélyegzővel látja el. Szolgáltató biztosítja, hogy mindaddig, amíg az adatokat őrzi, azok hitelesek, az arra jogosult személyek számára hozzáférhetők és értelmezhetők legyenek.

5.5.1 Az archiválandó adatok típusai

A Szolgáltató az általa archivált adatokhoz kapcsolódó adatokat – beleértve a személyes adatokat is – meg kell őriznie. Így tárolásra kerül:

- a szolgáltatás igénylése során az Igénylő és Előfizető által megadott adatok (lásd 4.1. fejezet);
- az azonosítási és hitelesítés (lásd 3. fejezet) során a Szolgáltató birtokába jutott elektronikus vagy papír alapú dokumentumok vagy azok másolatai, illetve a nyilvántartásokból lekért adatok;
- a jelen Szabályzat szerinti naplózott információk (5.4 pont).

Az elektronikus adatokat Szolgáltató elektronikus úton őrzi meg. A papír alapon rendelkezésre álló dokumentumokat Szolgáltató elektronikus másolatként vagy eredeti papír alapú formájában őrzi meg.

5.5.2 Archiválási időtartam

A Szolgáltató a naplózott adatokat a keletkezésüktől, a szolgáltatási szabályzatot és annak módosításait pedig hatályon kívül helyezésétől számított 10 évig őrzi.

5.5.3 Az archívum védelme

Az elektronikus dokumentumok és adatok védelmére Szolgáltató az 5.4.4 pontban meghatározott előírásokat alkalmazza - az elektronikusan megkapott dokumentumokra és az általa készített elektronikus másolatokra egyaránt.

A papír alapon rendelkezésre álló dokumentumokat Szolgáltató az 5.1 fejezet szerinti biztonsági körleten belül tárolja, biztosítva, hogy azokba kizárólag a Regisztrációs ügyintézők, Hitelesítési ügyintézők és Regisztrációs felelősök nyerhessenek betekintést.

5.5.4 Az archívum mentési folyamatai

Az archívum mentésére az 5.4.5 pontban meghatározott naplófájl mentésére vonatkozó előírások alkalmazandók.

5.5.5 Az adatok időbélyegzésére vonatkozó követelmények

A Szolgáltató az archiválandó adatokat az 5.4.1 pontban meghatározott módon időbélyeggel vagy időadattal látja el.

5.5.6 Az archívum gyűjtési rendszere

Az archívum gyűjtésére az 5.4.6 pontban meghatározott naplófájl gyűjtésére vonatkozó előírások alkalmazandók.

5.5.7 Archív információk hozzáférését és ellenőrzését végző eljárások

Az archívumhoz Szolgáltató ügyfélszolgálatán keresztül benyújtott kérelem alapján lehet kérni hozzáférést. A hozzáférés az Ügyfélnek a rá vonatkozó adatokhoz lehetséges, más feleknek a 2.4.1 pont szerint. Szolgáltató a jogosultságot minden esetben ellenőrzi, és a hozzáférést naplózza.

5.5.8 Egyéb archiválási rendelkezések

Az archiválásra vonatkozó részletes rendelkezéseket a Biztonsági Szabályzat tartalmazza.

5.6 Kulcscsere

Az archiválás kulcsainak cseréjét a szolgáltató a szükséges időben, lehetőleg üzemen kívül a a megfelelő módon (megújítással, vagy új kulcsra történő tanúsítvány kiadásával) elvégzi.

5.7 Katasztrófaelhárítás és helyreállítás

A Szolgáltató a szolgáltatásokat érintő fenyegetettségek azonosítására és a lehetséges kockázatok kezelésére vonatkozóan kockázatkezelési értékelést alkalmaz, illetve a rendkívüli helyeztek kezelésére, a vészhelyzetek minél gyorsabb elhárítása valamint a folyamatos működés biztosítására vonatkozóan Üzletmenet Folytonossági és Katasztrófa-elhárítási Tervvel (ÜFKT) rendelkezik.

A Szolgáltató a szolgáltatói rendszerek biztonságának megsértéséről, illetve az adatok sértetlenségének megszűnésről, amennyiben az jelentős befolyást gyakorol a szolgáltatásra, vagy a tárolt személyes adatokra (incidens) haladéktalanul, de legkésőbb 24 (huszonnégy) órán belül értesíti a Bizalmi Felügyeletet és adott esetben az egyéb érintett szerveket, valamint a szolgáltatás azon Ügyfeleit, akiket ez hátrányosan érinthet.

5.7.1 Incidens- és kompromittálódás-kezelési eljárások

Az informatikai rendszerekbe való belépésekre, azok felhasználóira és a Szolgáltatási szerződésre vonatkozó rendszertevékenységeket a Szolgáltató folyamatosan ellenőrzi a vonatkozó előírásokban foglaltaknak megfelelően. Az ellenőrzés pontos szempontjait a Biztonsági Szabályzat tartalmazza.

Amennyiben Szolgáltató az informatikai rendszereiben kritikus sérülékenységet észlel, a sérülékenység felfedezésétől számított 48 órán belül az alábbi intézkedések egyikét hajtja végre.

1. Kijavítja a kritikus biztonsági rést.
2. Amennyiben egy kritikus biztonsági rés kijavítása nem lehetséges 48 órán belül, Szolgáltató a sérülékenység enyhítése érdekében egy intézkedési tervet készít és hajt végre, melyben elsődleges intézkedésként határozza meg az alábbiakat:
    a. az ún. CVSS specifikáció[4] szerinti legkritikusabb biztonsági rések javítása (a legmagasabb pontszámúval kezdve);
    b. azon rendszerek biztonsági réseinek javítása, melyek nem rendelkeznek kiegészítő védelmi mechanizmussal és melyek a sérülékenység csökkentése nélkül ki lennének téve az illetéktelen hozzáférés és kompromittálódás veszélyének.
3. Szolgáltató dokumentálja a tényeket, melyek alapján nem szükséges a sérülékenység kijavítása - ennek okai - többek között - az alábbiak lehetnek:
    a. Szolgáltató nem ért egyet a CVSS specifikáció szerinti sérülékenységi besorolással;
    b. a sérülékenység beazonosítása téves;
    c. a sérülékenység kihasználhatóságát a kiegészítő védelmi mechanizmus megakadályozta; *vagy*

A Szolgáltató által alkalmazott ÜFKT tartalmazza a katasztrófa helyreállítási tervet is. Az ÜFKT olyan eljárásokat tartalmaz, amelyek leírják a megbízható üzemmenet mielőbbi helyreállításának leggyorsabb módját. A Szolgáltató ellenőrzések végrehajtásával rendszeresen (minimum évente) teszteli a biztonsági előírások hiánytalan technikai és személyi végrehajtását.

A Szolgáltató mentésekkel biztosítja, hogy szükség esetén az informatikai rendszer egészét helyre tudja állítani. A mentéseket a Szolgáltató védi a módosítások és jogosulatlan személyek hozzáférhesse ellen.

5.7.2 IT erőforrások, szoftverek és/vagy adatok meghibásodása

Szolgáltató megnövelt biztonságú eszközökkel és rendszerekkel rendelkezik a hardver- és szoftver meghibásodások, valamint az adatsérülések minimalizálása érdekében. A szolgáltatások helyreállíthatóságát Szolgáltató háttérszerződései és saját tartalékeszközei garantálják, amelyek az 5.7.4 pontban vállalt időn belül bármely kieső kritikus eszköz pótlására képesek. Szolgáltató rendszeres mentései (lásd 5.5 pont) és tranzakció naplózása (lásd 5.4 pont) biztosítja az adatok visszaállíthatóságát valamely adattároló eszköz kiesésének esetére. Ez a rendszer a legrosszabb esetben az előző napi adatok helyreállítására képes.

Az ÜFKT eseményjelentési előírásokkal rendelkezik valamennyi eszköze meghibásodása, illetve rendellenes működése tekintetében (ezek egy része automatizált, más része a kezelőszemélyzet felelőssége). A jelentéseket szakértő személyzet értékeli ki és válaszadás eljárásokat foganatosítva minimalizálja az esetleges károkat és szolgáltatás kieséseket.

A kritikus rendszerelemek meghibásodására vonatkozó részletes szabályokat az ÜFKT tartalmazza.

[4] Common Vulnerability Scoring System v3.0 (https://www.first.org/cvss/specification-document)

5.7.3 Magánkulcs kompromittálódása esetén követendő eljárás

A szolgáltatói kulcs kompromittálódása esetén a Szolgáltatónak legalább:

- Tájékoztatja az Ügyfeleit, Szolgáltatói partnereit, az Érintett feleket és a bizalmi felügyeletet.
- Jelezi, hogy az érintett szolgáltatói kulccsal végzett műveletek már nem érvényesek; és
- Visszavonja az érintett Szolgáltatói tanúsítványt.

Amennyiben bármelyik algoritmus (vagy a kapcsolódó paraméterek) - amiket a Szolgáltató alkalmaz - nem felel meg az elvárásoknak a fennmaradó tervezett felhasználási időtartamra, akkor a Szolgáltató köteles:

- Tájékoztatja az Ügyfeleit, Szolgáltatói partnereit, az Érintett feleket és a bizalmi felügyeletet, és
- Visszavonja az érintett Szolgáltatói tanúsítványt.

5.7.4 A működés folytonosságának fenntartása katasztrófaesemény után

Szolgáltató rendelkezik üzletfolytonossági tervvel, amit katasztrófa esetén életbe léptet. Katasztrófa bekövetkezte estén - beleértve valamely szolgáltatói magánkulcs vagy más hitelesítő adat kompromittálódását vagy a szolgáltatói rendszer kritikus elemeinek meghibásodását is - szolgáltató normál működése helyreállításra kerül, s egyúttal a hiba újbóli bekövetkeztének megelőzésére is sor kerül.

A Szolgáltató célja, hogy a hiba elhárítása és az integritás helyreállítása után a lehető leghamarabb újraindítsa valamennyi szolgáltatását. A visszavonási nyilvántartások megbízható üzemelésének helyreállítása minden más szolgáltatás vagy tevékenység helyreállítását megelőzi. Amennyiben a rendkívüli üzemeltetési helyzet meghaladja a szolgáltatáskiesésre a bizalmi felügyelet ajánlásában[5] megállapított legfeljebb 3 naptári naptári napot, Szolgáltató értesíti a bizalmi felügyeletet a rendkívüli üzemeltetési helyzettel kapcsolatos alábbi információkról is:

- a rendkívüli üzemeltetési helyzet kezdetének, és ha eltér, észlelésének időpontja és a rendkívüli üzemeltetési helyzet leírása,
- a rendkívüli üzemeltetési helyzet hatása (ennek részeként biztonsági esemény esetén az érintett szolgáltatások, informatikai vagyonelemek és az érintett személyes adatok körének leírása, az érintett bizalmi szolgáltatási ügyfelek száma),
- a rendkívüli üzemeltetési helyzet várható időtartama,
- a rendkívüli üzemeltetési helyzet elhárítása és jövőbeli elkerülése érdekében tett és tervezett intézkedések, és
- a rendkívüli üzemeltetési helyzet megszűnése.

Szolgáltató Katasztrófa-helyreállítási terve foglalkozik az archiválás magánkulcs kompromittálódásának

Az ilyen és egyéb kompromittálódási esetek vagy azok gyanúja esetén Szolgáltató

- az összes Előfizetőt és Érintett felet tájékoztatja;
- az archiválástt felfüggeszti a normál üzemmenet helyreállításáig;

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

- elvégzi a kompromittálódással érintett tanúsítványok azonosítását és az Előfizetők és Érintett felek számára is nyilvánosságra hozza az azonosításukhoz szükséges információkat, az adatvédelmi szempontok figyelembe vételével.

Természeti vagy más katasztrófát követően, illetve a Szolgáltató berendezéseinek meghibásodása esetén a szolgáltatás újbóli elindítását Szolgáltató 5 munkanapon belül vállalja.

5.8 A szolgáltatás megszűnése

Amennyiben a Szolgáltató tevékenységét tervezetten megszűnteti vagy tartósan szünetelteti, a tevékenység leállását megelőzően legalább az alábbi eljárásokat hajtja végre:

- Szolgáltatónak minden ésszerű erőfeszítést meg kell tennie annak érdekében, hogy egy erre alkalmas szolgáltató a nyilvántartásait és szolgáltatási kötelezettségeit legkésőbb a szolgáltatás leállításáig átvegye tőle.
- A szolgáltatás megszűnése előtt legalább 60 nappal értesítést tesz közzé weboldalán, e-mail címmel rendelkező ügyfelei számára a szolgáltatás befejezéséről elektronikus levélben értesítőt küld illetve tájékoztatja erről a Bizalmi felügyelet. Az értesítésekben megjelöli azt a - vele azonos besorolású – szervezetet, amely legkésőbb a tevékenység befejezésekor átveszi a szolgáltatásokat, valamint a regisztrációs információ és az eseménynapló archívumok fenntartására vonatkozó kötelezettségeket a Szolgáltató számára előírt vagy általa vállalt időtartamra.
- Saját magánkulcsait megsemmisíti, illetve a hozzájuk tartozó tanúsítványokat visszavonja, és erről weboldalán tájékoztatást tesz közzé.
- Amennyiben csak bizalmi szolgáltatás kerül megszüntetésre, akkor a szolgáltató lehetőség a visszavonási információkat továbbra is biztosítja.

A Szolgáltató a tanúsítványok visszavonását követően a tevékenysége befejezéséig a nyilvánosságra hozatali kötelezettségének továbbra is eleget tesz.

- A regisztrációs információk és az eseménynapló archívumok megőrzése érdekében, időbélyegzővel ellátott teljes körű mentést hajt végre. A mentés tartalmazza a tanúsítványokkal kapcsolatos korábbi változások adatait, a tanúsítványok helyzetére, esetleges felfüggesztésére, illetve visszavonására vonatkozó adatokat, valamint a tanúsítvány kibocsátásra vonatkozó Szolgáltatói szabályzatokat és az aláírás-ellenőrző adatokat, továbbá a visszavont tanúsítványok nyilvántartását. A mentett adatállományokat Szolgáltató védi a jogosulatlan módosítástól és biztosítja a jogosulatlan hozzáférés kizárását, valamint az adatoknak megőrzési időn belüli, hozzáférhetőségét és értelmezhetőségét a jogosult személyek számára.

Ha a Szolgáltató ellen a bíróság jogerős határozata alapján felszámolási vagy végelszámolási eljárás indult, haladéktalanul tájékoztatja a Bizalmi Felügyeletet e tényről, megnevezve az eljárást lefolytató szervezetet.

A Szolgáltató annak érdekében, hogy adatait átadhassa egy másik szolgáltatónak, azokat a szolgáltató által fogadóképes médián és formátumban helyezi el vagy biztosítja a másik szolgáltató számára az adatok eredeti formátumban történő feldolgozásának lehetőségét, melyekhez átadja a megfelelő eszközöket, dokumentációkat és ismereteket.

6 Műszaki biztonsági óvintézkedések

A Szolgáltató megbízható, biztonságtechnikailag értékelt és ellenőrzött termékekből álló informatikai rendszert használ szolgáltatásai nyújtásához.

6.1 Kulcspár generálás és telepítés

6.1.1 Kulcspár előállítása

A szolgáltatói archiválás kulcsok generálását a Szolgáltató fizikailag védett szervertermében két bizalmi munkakört betöltő személy együttes jelenlétében, jegyzőkönyvezetten történik. A szolgáltatói archiválás kulcsok generálása és tárolása során a Szolgáltató a 6.2.1 pont szerint jár el. A Szolgáltató valamennyi szolgáltatói kulcspárt saját maga generálja és ellenőrzi, hogy a nyilvános kulcs korábban nem került-e kiosztásra más entitás számára.

A generált magánkulcsok – a 6.2.4 fejezetben ismertetett mentés esetét leszámítva - teljes életciklusuk alatt a kriptográfiai hardverekben maradnak, megsemmisítésükig sehová nem kerülnek áthelyezésre.

Amennyiben a szolgáltatói magánkulcs bármely okból történő megsemmisítése válik szükségessé, úgy az az eszköz tanúsítványában előírt módon két személyes kontroll mellett történik.

A Szolgáltatói kulcsok lejáratát megelőzően a Szolgáltató az új kiadói kulcsokat úgy generálja és adja ki az új szolgáltatói tanúsítványokat, hogy az átállás az Ügyfél részéről minél zökkenőmentesebb lehessen, és a tanúsítvány cseréje ne okozzon zavart az Ügyfelek és az Érintett Felek számára.

Amennyiben ugyanaz az archiválás kulcs több kriptográfiai modulban is alkalmazásra kerül, akkor Szolgáltató ugyanazt a tanúsítványt kapcsolja hozzá.

A Szolgáltatói kulcsok generálására vonatkozó részletszabályokat a kulcsgenerálási forgatókönyv tartalmazza.

6.1.2 Magánkulcs eljuttatása a Végfelhasználóhoz

A magánkulcs kriptográfiai eszközben jön létre, az RFC 3467 ezen pontja archiválás esetében nem értelmezett.

6.1.3 Nyilvános kulcs eljuttatás a tanúsítvány kibocsátóhoz

Az archiváló rendszer részére előállított kulcspár előállítását követően tanúsítványkérelem jön létre. Ezen kérelem tartalmazza a nyilvános kulcsot, mely kérelem beadásra kerül a minősített tanúsítvány kiadó rendszerbe és ez alapján zajlik le a tanúsítvány kibocsátása.

6.1.4 A szolgáltatói nyilvános kulcs közzététele

Szolgáltató szolgáltatói tanúsítványai 2. fejezet szerint elérhetőek a Szolgáltató weboldalán (1.1.2 pont). Az archiválást hitelesítő szolgáltatói tanúsítványok nyilvános kulcsai a szolgáltatói tanúsítványok részeként elérhetők.

6.1.5 Kulcsméretek

A Szolgáltató által alkalmazott kulcspárok (szolgáltatói és végfelhasználói tanúsítványok esetén egyaránt) megfelelnek a hatályos szabványokban, illetve a Bizalmi Felügyelet határozatban előírtaknak. A Szolgáltató által használt algoritmusok:

Lenyomatképző algoritmusok azonosítói:

- SHA-256 OID ::= { joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) SHA-256 (1) }
- SHA-384 OID ::= {joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) SHA-384(2)}
- SHA-512 OID ::= {joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) SHA-512(3)}

Kriptográfiai algoritmusok azonosítói és kulcsméretei:

- RSA OID ::= { iso(1) member-body (2) USA (840) RSADSI (113549) PKCS (1) PKCS-1 (1) RSA Encryption (1) } – Minimum 2048 bit kulcshossz
- DSA OID ::= { iso(1) member-body(2) us(840) X9-57 (10040) x9algorithm (4) id-dsa (1) }

A Szolgáltató az itt meghatározott algoritmusokat legfeljebb a Bizalmi Felügyelet Algoritmus Határozatában megjelölt időpontig használja.

6.1.6 A nyilvános kulcs paraméterek előállítása, a minőség ellenőrzése

A kulcsgenerálás paramétereinek megfelelőségét a Szolgáltató által használt rendszer két szempontból ellenőrzi:

- a paraméterekhez felhasznált véletlenszám-generálás megfelelőségének ellenőrzése (statisztikailag kellőképpen véletlenszerű-e a generálás),
- a paraméterekre vonatkozó feltételek, összefüggések teljesülésének ellenőrzése.

A véletlenszám-generálás megfelelőség ellenőrzésének alapja, hogy a rendszerben használt valamennyi kriptográfiai hardver modul képes az általa generált bitsorozat egyenletességének és függetlenségének statisztikai tesztelésére. A modulok lehetővé teszik a tesztek meghívását egy szabványos interfészen keresztül.

A külső interfészen meghívható tesztelési utasításon kívül a hardver modulok is folyamatosan tesztelik saját véletlenszám-generálásukat, melyek hibás teszt esetén leállnak.

6.1.7 A kulcshasználat célja (az X.509 v3 kulcs használati mező tartalmának megfelelően

Az archiválás aláíró/bélyegző kulcsa kizárólag az archiválászolgáltatás nyújtása keretében végzett szolgáltatói aláírási műveletek végzésére alkalmazható.

6.2 Magánkulcs védelem és kriptográfiai modul előírások

Szolgáltató olyan fizikai és logikai védelmeket implementált, amelyek megakadályozzák a jogosulatlan hozzáférést.

Szolgáltató az archiválási magánkulcsot biztonságos módon tárolja, ami megakadályozza, hogy jogosulatlan személy hozzáférhessen és használhassa. Szolgáltató a szolgáltatói magánkulcsait csak fizikailag védett környezetben, az adott kulcsra meghatározott rendeltetési célra használja fel.

6.2.1 Kriptográfiai modulra vonatkozó szabványok és előírások

A szolgáltatói kulcsok - beleértve az archiválás kulcsokat is - létrehozása, mentése, tárolása és megsemmisítése kapcsán Szolgáltató az alábbiak szerint jár el:

- a kulcsok létrehozása, tárolása, mentése, helyreállítása, megsemmisítése fizikailag biztonságos környezetben, kettős személyi ellenőrzés mellett (két bizalmi munkakört betöltő munkatárs együttes jelenlétében) valósul meg (lásd 6.1.1.1 pont),
- a Kiadóek kulcsai a vonatkozó szabványoknak megfelelően legalább EAL4 tanúsítással rendelkező, az ISO/IEC 15408 vagy ezzel ekvivalens IT biztonsági elvárás szerint, vagy az ISO/IEC 19790 vagy FIP PUB 140-2 level 3 megfelelő hardver kriptográfiai eszközben kerülnek generálásra, tárolásra, illetve felhasználásra (lásd 6.1.1.2 és a 6.2.7 Magánkulcs tárolása kriptográfiai modulban fejezeteket),
- a kulcsokat kizárólag az arra felhatalmazottak használhatják, a létrehozás céljának megfelelő funkcióra,
- a Szolgáltató rendszerei saját szolgáltatói kulcsaik használata előtt meggyőződnek arról, hogy az e kulcsokhoz kapcsolódó tanúsítványok érvényesek,
- a Szolgáltató tanúsítvány-, CRL és OCSP aláíró kulcsai különböznek minden más funkcióra szolgáló kulcstól,
- a szolgáltatói kulcsfrissítés out-of-band cserével történik,
- biztonságos kriptográfiai modulban tárolt kulcs modulból történő exportálásakor a Szolgáltató gondoskodik a kulcs védelméről,
- azokat a rendszereket, melyek kriptográfiai hardver eszközön kívül dolgoznak fel kriptográfiai szempontból érzékeny információt (magán- vagy titkos kulcsokat) a Szolgáltató védi az elektromágneses kisugárzással történő kompromittálódás ellen (ld. 5.1.3 pont).

Szolgáltató elkülönítve kezeli és működteti a minősített szolgáltatásainak nyújtásához használt kriptográfiai eszközöket a nem minősített szolgáltatásokhoz és egyéb tevékenységeihez használt kriptográfiai eszközöktől, mely utóbbiak így nem befolyásolhatják a minősített szolgáltatást megvalósító termékek megbízható üzemeltetését.

Szolgáltató a minősített bizalmi szolgáltatás nyújtását közvetlenül megvalósító termékeiről biztonsági osztályokba sorolt nyilvántartást vezet.

Mielőtt a minősített szolgáltató a minősített szolgáltatás nyújtásához használt bizalmi szolgáltatást megvalósító termékeit a saját maga által végzett szolgáltatásnyújtáson kívüli célokra használja fel, megbizonyosodik arról, hogy a termék nem tartalmaz olyan adatot, amely bizalmi szolgáltatáshoz fűződik, valamint arról, hogy az ilyen adatot nem lehet visszaállítani. E vizsgálatot és a vizsgálat eredménye alapján végrehajtott intézkedést a minősített szolgáltatónak naplózza.

A Szolgáltató által használt és biztosított kulcstároló, kulcsgeneráló és aláíró eszközök az alábbiak lehetnek:

Eszköz	**Hardware és firmware specifikáció**	**Kulcskezeléshez közvetlenül használt szoftverek specifikációja**
Szolgáltatói kulcsok eszközei	● Luna® PCI-e kriptográfiai modul Hardver verzió: VBD-05-0100, VBD 05-0101 és VBD-05-0103, förmver verzió: 6.2.1 ● Luna® PCI-e kriptográfiai modul Hardver verzió: VBD-05-0100, VBD 05-0102, förmver verzió: 6.10.9 ● ProtectServer Internal Express 2 (PSI-E2) Hardver verzió VBD-05, förmver	● Luna kriptogáfiai modulok driverei

	verzió: 5.00.02)	
	•	•

A fenti eszközök megfelelőségi tanúsítványai letölthetők a Szolgáltató weboldalán (lásd 1.1.2., Kikötések és feltételek közzététele).

Szolgáltató folyamatosan figyelemmel kíséri az általa bejelentett eszközök tanúsításának érvényességét, illetve az alkalmazásukra vonatkozó esetleges újabb korlátozásokat. Ennek érdekében egyrészt belső adminisztrációs lépéseket hozott meg a tanúsítások érvényességének nyilvántartására, illetve az Európai Unión belül elvégzett tanúsítások érvényességei változásainak nyomon követésére, másrészt a tanúsítással érintett eszközök gyártóival, forgalmazóval is kommunikál, hogy minél hamarabb értesülhessen a tanúsítások változásairól.

Szolgáltató saját felhasználásra és ügyféleszközként egyaránt bevezethet további kulcskezelő és aláíró eszközöket, amennyiben azok rendelkeznek a felhasználási célnak megfelelő tanúsítással.

6.2.2 Magánkulcs többszereplős (n-ből m) használata

A Szolgáltató belső Biztonsági Szabályzatának részletes leírást kell tartalmaznia a többszereplős magánkulcskezelés módjáról. Amennyiben jelen Szolgáltatási Szabályzat egy magánkulcs többszereplős kezelését írja elő, az adott művelet végzésére felhatalmazott bizalmi munkatársaknak ezen leírás szerint kell eljárniuk.

6.2.3 Magánkulcs letétbe helyezése

Szolgáltató az archiválás szolgáltatás nyújtása során használt szolgáltatói aláíró magánkulcsokat nem helyezi letétbe.

6.2.4 Magánkulcs mentése

A szolgáltatói magánkulcsok mentését (másolását), tárolását és helyreállítását Szolgáltató jegyzőkönyvezetten, fizikailag védett környezetben végzi legalább két bizalmi munkakört betöltő személy együttes részvételével. E műveletekre feljogosított munkatársak számát a minimumon tartja.

A mentés rejtjeles formában hajtódik végre. A mentés során a magánkulcsot generáló kriptográfiai hardver modulból – a kriptográfiai hardver modul típusának megfelelően - intelligens kártyákra több darabban, védetten másolódik át a magánkulcs vagy ún. backup HSM modulba kerül. A mentett példányok ugyanolyan jellegű és erősségű védelem alatt állnak, mint a kulcsgenerálást végző hardver modul eredeti példánya. A kulcs titkosítása során olyan algoritmus és kulcsméret került alkalmazásra, ami annak teljes hátralévő idejében biztosítja a védelmet. A szolgáltatói magánkulcs nem üzemben lévő másolatait legalább a produktív kulccsal azonos szintű biztonsági eljárások védik.

6.2.5 Magánkulcs archiválása

A Szolgáltató a szolgáltatói magánkulcsokat nem archiválja.

6.2.6 Magánkulcs bejuttatása a kriptográfiai modulba, vagy onnan történő exportja

A szolgáltatói magánkulcsok kriptográfiai modulba juttatását Szolgáltató fizikailag védett környezetben valósítja meg legalább két bizalmi munkakört betöltő személy együttes részvételével.

Lásd a 6.2.4 pontban foglaltakat.

6.2.7 Magánkulcs tárolása kriptográfiai modulban

A kriptográfiai eszközön tárolt magánkulcsok esetében Szolgáltató gondoskodik arról, hogy a kulcsok ne legyenek elérhetők az eszközön kívül (kivéve a 6.2.4 pontban foglalt mentés esetét). A kriptográfiai eszköz esetében Szolgáltató gondoskodik a hamisítás elleni védelemről a szállítás és a tárolás során is.

Lásd a 6.2.1 pontban foglaltakat.

6.2.8 A magánkulcs aktiválásának módja

A szolgáltatói magánkulcsok aktiválását Szolgáltató fizikailag védett környezetben, a többszereplős magánkulcskezelés szabályai szerint valósítja meg legalább két bizalmi munkakört betöltő személy együttes részvételével. A szolgáltatói kulcsok aktiválásának módját a Szolgáltató Biztonsági Szabályzata részletezi.

6.2.9 A magánkulcs deaktiválásának módja

A szolgáltatói kulcsok deaktiválásának módját Szolgáltató Biztonsági Szabályzata részletezi.

6.2.10 A magánkulcs megsemmisítésének módja

A szolgáltatói kulcsokat a Szolgáltató olyan módon semmisíti meg, hogy a szolgáltatói aláíró kulcsok ne legyenek visszanyerhetőek. Ez jelenti a Kriptográfiai eszközről törlést, valamint mentett kulcsrészletek esetben legalább annyi részlet törlését amennyi törlésével a kulcs helyreállíthatatlanná válik.

Szolgáltatói eszköz megsemmisítése esetén Szolgáltató gondoskodik a rajta tárolt magánkulcsok megsemmisítéséről.

6.2.11 A kriptográfiai modulok értékelése

Lásd a 6.2.1 pontban foglaltakat.

6.3 A kulcspárkezelés további szempontjai

A Szolgáltató a Kikötéseknek és a törvényi előírásoknak megfelelően használja és kezeli szolgáltatói kulcsait, különös tekintettel az alábbiakra:

- Szolgáltató saját szolgáltatói kulcsait nem használja a hozzájuk tartozó szolgáltatói tanúsítványok érvénytelensége esetén és a kulcspár használati idején túl (lásd 6.3.2).
- Az archiválás szolgáltatás kapcsán, az Ügyfelek részére kibocsátott igazolások és értesítések hitelesítésére valamint az archiválásra befogadott állományok

felülhitelesítéséhez használt kulcsok kizárólag erre a célra használtak.
- A felülhitelesítésére használt kulcsok csak fizikailag védett helyszínen kerülnek felhasználásra.
- A Szolgáltatói magánkulcsnak kompatibilisnek kell lenni a tanúsítványok aláírására alkalmazott lenyomat és aláíró eljárásokkal és kulcshosszakkal.

6.4 Aktiváló adat

A Szolgáltatói kulcspár telepítése és helyreállítása a kriptográfiai eszközön kizárólag bizalmi munkakörben foglalkoztatott munkatársak legalább kettős kontrollja alatt történik.

6.4.1 Aktiváló adat generálás és telepítés

A Szolgáltatói kulcspár aktiváló adatán előállítása kulcspár generálásakor történik.

6.4.2 Aktiváló adat védelme

A szolgáltató kulcsának aktiválási adatát biztonságosan tárolja.

6.5 Informatikai biztonsági előírások

A Szolgáltató rendszereit csak az arra jogosult személyek érhetik el. A Szolgáltató a belső zónák határait tűzfalakkal védi és megteszi a szükséges intézkedéseket arra vonatkozóan, hogy az érzékeny adatok az adathordozók újrafelhasználása során ne legyenek feltárhatók.

A Szolgáltató által alkalmazott Biztonsági szabályzat biztosítja, hogy a tanúsítványtárhoz az adatok hozzáadása, illetve a tanúsítványállapot változásával kapcsolatos intézkedések (felfüggesztés, visszavonás, aktiválás) csak az arra jogosultak számára legyen elérhetők.

Szolgáltató a jogosulatlan hozzáférések kiszűrésére monitorozó és riasztó eszközöket alkalmaz.

6.5.1 Speciális informatikai biztonsági műszaki követelmények

Nincs szabály.

6.5.2 Informatikai biztonság értékelése

Az ide vonatkozó rendelkezéseket a Szolgáltató belsőhasználatú Kockázatkezelési Szabályzata tartalmazza.

6.6 Életciklusra vonatkozó biztonsági előírások

6.6.1 Rendszerfejlesztési óvintézkedések

A Szolgáltató által fejlesztett rendszerek esetében sor kerül a kockázatok biztonsági felmérésére és elemzésére.

A Szolgáltató a maga által fejlesztett szoftverek esetében változáskezelési eljárást alkalmaz a kibocsátásokra, a módosításokra, és a sürgős szoftverjavításokra. A változáskezelési eljárás

lehetőség szerint az üzembe helyezés előtt lezajlik. Ez alól kivételt képezhetnek a sürgős javítások, melyek esetében a dokumentálás utólagos elvégzésére is van lehetőség, amennyiben a szoftverjavítás késedelmes üzembe helyezése a Szolgáltató működését érdemben veszélyezteti, illetve jelentős anyagi vagy erkölcsi kárt okozna.

Az ide vonatkozó rendelkezéseket részletesen a Szolgáltató belső használatú Szoftverfejlesztési Szabályzata és Informatikai Változáskezelési Szabályzata tartalmazza.

6.6.2 Biztonságkezelési előírások

A Szolgáltató olyan megbízható rendszereket és termékeket használ, amelyek védettek a módosítások ellen és biztosítják az ellátott műveletek műszaki biztonságát és megbízhatóságát. A Szolgáltató különös figyelmet fordít a biztonságra a beszerzések során is: a kulcsfontosságú rendszereinek szállítói a Beszerzési Szabályzat szabályai szerint értékelt beszállítók, illetőleg a beszerzett eszközök értékelt eszközök. Az eszközök gyártói számos referenciával és megbízható háttérrel rendelkező szervezetek. Ezen szabályok biztosítják, hogy Szolgáltató eszközeihez szükség esetén megkapja a szükséges támogatást, illetve meghibásodás esetén a szállítóval szembeni jótállási, szavatossági igények érvényesíthetők legyenek. A felhasznált, beépített eszközök nagyrészt a kereskedelmi forgalomban könnyen beszerezhetők, így azok pótlása több forrásból, viszonylag gyorsan megoldható.

A Szolgáltató védi az informatikai rendszereit és információit a vírusoktól, a rosszindulatú és nem engedélyezett szoftverektől. A Szolgáltató olyan eljárásokat alkalmaz, amely biztosítják, hogy a biztonsági javítások ésszerű időn (6 hónapon) belül alkalmazásra kerüljenek. A Szolgáltató nem alkalmazza a biztonsági javításokat abban az esetben, ha azok további biztonsági réseket tartalmaznak, illetve ha azok instabilitást okoznak.

Szolgáltató adatain kizárólag arra feljogosított személyek végezhetnek bejegyzéseket és változtatásokat. Az adatok hitelessége ellenőrizhető. Az Ügyfelekre vonatkozó adatok kizárólag annak a személynek a hozzájárulásával kereshetők nyilvánosan, akire az adatok vonatkoznak.

6.6.3 Az életciklusra vonatkozó biztonsági előírások

A Szolgáltató folyamatosan monitorozza a kapacitáskihasználtságot és előrejelzéseket készít annak érdekében, hogy elegendő tárhely és feldolgozási kapacitás álljon rendelkezésre a jövőben is.

Szolgáltatónak gondoskodik a szolgáltatásnyújtás során felhasznált kriptográfiai hardvereszközök védelméről azok teljes életciklusa alatt, valamint gondoskodik az alábbiakról:

- Az alkalmazott kriptográfiai hardvereszköznek megfelelő érvényes tanúsítással rendelkezik teljes életciklusa alatt.
- A kriptográfiai hardvereszköz átvételekor Szolgáltatónak meggyőződött arról, hogy a szállítás során biztosított volt a kriptográfiai hardvereszközök feltörés elleni védelme.
- Szolgáltatónak biztosítja a kriptográfiai hardvereszközök feltörés elleni védelmét a tárolás során.
- Szolgáltatónak gondoskodnik a kriptográfiai hardvereszköz üzemeltetése során az eszköz dokumentációjában és a tanúsítási jelentésben szereplő követelmények folyamatos betartásáról.
- A használatból kivont kriptográfiai hardvereszközökben tárolt magánkulcsokat a 6.2.10. A magánkulcs megsemmisítésének módja pont szerint visszaállíthatatlan módon törli az eszközből.

6.7 Hálózati biztonság

A Szolgáltató a szolgáltatások nyújtásához használt rendszereit különböző ún. biztonsági zónákba sorolja. A biztonsági zónákba sorolást követően a Szolgáltató gondoskodik arról, hogy az egyes zónák között a kommunikáció biztonságos módon történjen. A Szolgáltató a szolgáltatásnyújtás során minden olyan kapcsolatot, portot tilt vagy eltávolít, amelyek nem kapcsolódnak a szolgáltatásnyújtáshoz. .

A Szolgáltató a szolgáltatói rendszerek számára külön hálózatot alakított ki. A produktív rendszerek elkülönülnek a fejlesztési, teszt és egyéb felhasználású rendszerektől. A Szolgáltató hálózati kapcsolatát redundáns módon alakította ki azokban az esetekben, ahol a szolgáltatáshoz nagy rendelkezésre állású külső elérés szükséges.

A biztonság folyamatos fenntartása érdekében a Szolgáltató rendszeresen (negyedévenkénti vagy szignifikáns hálózati változás esetén mihamarabbi) sebezhetőségi ellenőrzést végez.

A Szolgáltató a sebezhetőségi ellenőrzések mellett éves periódusban, vagy szignifikáns infrastrukturális változás esetén mihamarabb betörési ellenőrzést is végez.

A hálózati biztonsággal kapcsolatban további rendelkezéseket a Szolgáltató Biztonsági Szabályzata tartalmazza.

6.8 Időbélyegzés

Szolgáltató a minősített archiválás szolgáltatás nyújtása keretében minősített bizalmi szolgáltató által kibocsátott időbélyegzőket használ az érvényességi lánc időbélyegzésére, a felülhitelesítés alkalmával valamint a jelen Szolgáltatási szabályzat által meghatározott naplóbejegyzések és egyéb archiválandó elektronikus állományok hitelesítésére.

A Szolgáltató a rendszerei időforrásait legalább naponta egyszer UTC időforráshoz szinkronizálja.

7 Tanúsítványprofil, megőrzési profil

Az archiválás tanúsítványok profilja eszközön tárolt bélyegző, ahol a tanúsítvány CN mezője a “NETLOCK Minősített Archiválás” vagy NETLOCK Qualified Preservation” tartalommal bír, a többi tanúsítvány mező a bélyegzőnél megszokott szolgáltatói értékeket veszi fel.
A profilokról részleteket lásd a NETLOCK Bizalmi Szolgáltatási Szabályzat Minősített Tanúsítványszolgáltatásokra 7.1 fejezetében.

A szolgáltató kizárólag egy érvényes profilt kezel. Új verzió szabályzat módosítással együtt kerül közzétételre, melyről a módosítási eljárás szerint tájékoztatja ügyfeleit. A már hatályon kívül helyezett profilokat a Függelékbe helyezve teszi közzé, az előírásoknak megfelelően. (Jelenleg nincs hatályon kívüli profil)

A Szolgáltató a minősített megőrzési policy-t (CP-t) támogatja, melynek szabványos azonosítója: 0.4.0.19511.1.2

7.1 Megőrzési profil – Megőrzés aláírással és kiterjesztéssel, tárolással

A megőrzési profil szabványos az ETSI TS 119512 séma minta alapján készült profil leírás, annak minden kötelező tartalmával, és kiegészítő magyarázatokkal az értelmezéshez.

A megőrzési profil azonosítója: http://uri.netlock.hu/19512/profile/pds+wst+aug/1

A működés paramétereinek rövid leírása

- Dokumentum feltöltésekor a rendszer megvizsgálja a visszavonási információk jelenlétét, és ha hiányzik, akkor megpróbálja kiegészíteni az állományt.
- A kiterjesztéssel 1 alkalommal próbálkozik, ezt követően elutasítja az állomány befogadását.
- A rendszer befogadásról visszajelez.
- A szolgáltató a dokumentumokba ágyazza a felülhitelesítési információkat, így a letöltött dokumentum tartalmazza az evidenciát is, külön exportálásra (evidenciákkal) nincs szükség, a letöltött állomány másik szolgáltató által befogadható.; más szolgáltatótól a kiterjesztett állomány standard feltöltéssel teljesíthető, így export-importot a szolgáltató a standard eléréseken biztosít.

7.1.1 A profil hatálya

A profil hatályának kezdő dátuma: Jelen szabályzat hatályba lépésének dátuma.

A profil hatályának vég dátuma: Jelenleg nincs záró dátum.

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 kibővítése 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.

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 szolgáltató tárolt hozzájuk, egyaránt a megőrzési szolgáltató által tárolt. Ez a szolgáltatási modell támogatja a megőrzendő objektumok és bizonyítékok fel és letöltését.

A PreservationStorageModel értéke WithStorage (WST).

7.1.5 Támogatott műveletek

A támogatott műveltek két csoportra oszthatók. A kötelezően megvalósítandó és az opcionális

műveletek. A szolgáltató ezek mindegyikét támogatja.

7.1.5.1 Kötelező műveletek

A 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.

7.1.5.2 Opcionális műveletek

A szolgáltató a következő opcionális művelteket 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.

7.1.6 A megőrzési bizonyítékok generálása és ellenőrzése

A szolgáltatás kibővíti az aláírást a következő megfelelő aláírás formátumokra:

- XADES archív időbélyeg
  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 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.

7.1.7 A megőrzési bizonyítékok kiterjesztése

Az elfogadható kriptográfia algoritmusok monitorozása alapján (mint a például az ETSI TS 119312) a Szolgáltató kiterjesztést hajt végre a megadott bizonyíték formátumban.

7.1.8 Megőrzési bizonyíték szabályok

A bizonyítékok előállításhoz használt minősített időbélyeg szolgáltató: NETLOCK Kft.

A bizalom gyökere: EU Trust list

A szolgáltató által aláírásra/bélyegzésre használt minősített aláíró/bélyegző tanúsítvány kiadója: NETLOCK Kft.

A bizalom gyökere: EU Trust list

7.1.9 Aláírás ellenőrzési szabályok

A befogadásra küldött állományokon található aláírásokat és visszavonási információkat a szolgáltató az állományra releváns PADES, XADES szabványok szerint ellenőrzi, amely alapvetően lánc modell.

Ha a visszavonási információk a megőrzéshez nem elégségesek a szolgáltató megpróbálja beszerezni azokat.

A bizalom gyökere: EU Trust list

8 A megfelelőség vizsgálata

A Szolgáltatónak tevékenységét összhangban végezi

- a vonatkozó és hatályos Európai Uniós és hazai szabályozással,
- a Bizalmi Szolgáltatási rend követelményeivel
- jelen Bizalmi Szolgáltatási szabályzat követelményeivel.

Továbbá a Szolgáltatónak működési helye szerinti Bizalmi felügyelet Bizalmi szolgáltatások nyújtására vonatkozó nyilvántartásában szerepelnie kell.
A szolgáltató tevékenységét a Nemzeti Média és Hírközlési Hatóság felügyeli, évente minimum egyszer átfogó helyszíni ellenőrzést tart.

A Szolgáltatónak tevékenységét külső megfelelőségértékelő szervezettel értékelteti a vonatkozó szabványoknak és jogszabályoknak megfelelően. A Szolgáltató külső megfelelőségértékeléséhez végzett vizsgálat során az alábbiakat kell betartani:

- figyelembe kell venni Szolgáltató összes értékelendő bizalmi szolgáltatás sajátosságát;
- biztosítani kell, hogy a vizsgálat tárgyához tartozó minden szolgáltatói tevékenységet lefedjen a vizsgálat;
- a vizsgálatot vonatkozó szabványok, nyilvánosan hozzáférhető specifikációk és/vagy jogszabályi követelmények alapján kell végezni.
    - 910/2014/EU (eIDAS)
    - Eüt. (2015 évi CCXXII. tv.)
    - 24/2016 Korm rendelet
    - 114/2007 GKM rendelet
    - ETSI TS 119511
    - ETSI 319401

8.1 Az ellenőrzések körülményei és gyakorisága

A Szolgáltató tevékenységének felügyeletét az európai uniós szabályozással összhangban a

Bizalmi Felügyelet látja el. A Bizalmi Felügyelet legalább éves rendszerességgel helyszíni szemlét tart a Szolgáltató székhelyén, telephelyén.

Az ellenőrzések eredményei, valamint az azok alkalmával készült dokumentumok bizalmas jellegűek, hozzáférést csak a megfelelő jogosultsággal rendelkező személyek kapnak.

A 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.

Amíg a Szolgáltató minősített archiválás szolgáltatást nyújt, legalább évente köteles a vonatkozó szabványoknak való megfelelőséget belső auditok és külső megfelelőségértékelés elvégzésével vizsgálni.

A Szolgáltató a jelen Szabályzat 1.1.2 pontjában részletezett ISO 9001, valamint ISO 27001 szabvány megfelelőségét külső auditáló szervezet értékeli és vizsgálja felül folyamatosan, legalább évente egy alkalommal.

8.2 Az értékelő és szükséges képesítése

Szolgáltató a belső auditokat a független rendszervizsgáló szerepkörrel felruházott alkalmazottai segítségével is elvégezheti.

A külső megfelelőségértékeléseket olyan természetes vagy jogi személy végzi, aki rendelkezik egy EU tagállam nemzeti akkreditációs szervezetétől megfelelő felhatalmazással.
A külső értékelések során a Szolgáltató olyan természetes vagy jogi személlyel, vagy természetes személyek csoportjával működik együtt, akik/amelyek

- képesek a 8. fejezetben megadott szabványokra vonatkozó audit elvégzésére;
- megfelelnek a 8.3 pontban foglalt követelménynek;
- megfelelő jártassággal bírnak a PKI, az IT illetve IT biztonsági megoldások, technológiák és auditok terén;
- ETSI szabványok alapján végzett auditok/értékelések esetén rendelkezik vagy rendelkeznek
    - az ETSI EN 319 403 szerinti akkreditációval, *vagy*
    - egy ezzel egyenértékű nemzeti szabvány szerinti akkreditációval, *vagy*
    - a Nemzeti Akkreditációs Hatóság által ISO 17021 szabvány szerinti ISO 27006 módszertannal végrehajtott ISO 27001 vizsgálatra akkreditációval rendelkezik;
- WebTrust audit végzése esetén rendelkezik vagy rendelkeznek WebTrust audit elvégzéséhez szükséges engedéllyel;
- tevékenységét vagy tevékenységüket jogszabályok vagy szakmai etikai kódex szabályozza;
- rendelkezik az értékelő tevékenység végzéséből eredő mulasztások, hibák esetére szóló, legalább egymillió USD fedezetű biztosítással.

8.3 Az auditor és az auditált entitás kapcsolata

A Szolgáltató belső megfelelőségértékeléseit végző Független rendszervizsgáló szerepkörrel felruházott bizalmi munkatársak függetlenek a Szolgáltató szolgáltatásokért felelős szervezeti egységeitől.

A külső megfelelőségértékeléseket végző értékelők függetlenek az alábbiak tekintetében:

- a vizsgált szolgáltató tulajdonosi körétől, vezetőségétől és üzemeltetésétől;
- a vizsgált szervezettől, vagyis sem saját maga, sem közvetlen hozzátartozója nincs munkaviszonyban a Szolgáltatóval;
- díjazása nem függ az értékelés során végzett tevékenységének végkimenetelétől.

8.4 Az értékelés/audit által lefedett területek

Az auditok/értékelések során az alábbi területek kerülnek ellenőrzésre:

- a hatályos, vonatkozó jogszabályoknak való megfelelés;
- műszaki szabványoknak való megfelelés;
- Bizalmi Szolgáltatási Rend(ek)nek és Szolgáltatási szabályzat(ok)nak való megfelelés;
- az alkalmazott folyamatok megfelelősége;
- a fizikai biztonság megfelelősége ;
- a személyi állomány megfelelősége;
- az IT biztonság megfelelősége;
- az adatvédelmi szabályok betartása.

8.5 A hiányosságok kezelése

A külső és belső megfelelőségértékelések eredményét a Szolgáltató egy értékelési jelentésben foglalja össze, amely jelentés kitér a vizsgálat rendszerelemekre, folyamatokra. A dokumentum tartalmazza az ellenőrzés során felhasznált bizonyítékokat és értékelői megállapításokat. A jelentés tartalmazza továbbá az ellenőrzés során feltárt hiányosságokat, eltéréseket és a kijavításukra kitűzött határidőket. A feltárt hiányosságok súlyosságuknak megfelelően az alábbi kategóriába tartoznak:

- “Enyhe” eltérés, mely kapcsán a helyesbítő intézkedéseket igazoló dokumentumokat a következő értékelés alkalmával kell bemutatni.
- “Súlyos” eltérés, mely kapcsán a megvalósított helyesbítő intézkedést igazoló dokumentumokat az aktuális értékelés alkalmával kell bemutatni.

A Szolgáltató köteles a független értékelő által felvett eltérésekre írásában válaszolni, kijavításukra tett intézkedéséről a következő értékelés alkalmával beszámolni.

8.6 Az eredmények közzététele

A Szolgáltató nem hozza nyilvánosságra az ellenőrzésről, értékelésekről készült részletes vizsgálati jelentést, de az értékelést követő három hónapon belül nyilvánosságra hozza az értékelésről kiállított tanúsítványt.

A Szolgáltató a megfelelőségértékelés eredményét 3 munkanapon megküldi a Bizalmi Felügyeletnek.

9 Egyéb üzleti és jogi tudnivalók

9.1 Díjak

Előfizető köteles az időszaki szolgáltatások és az ezek mellett vagy igénylésük során igénybevett egyéb szolgáltatások (pl. opcionális szolgáltatások) ellenértékét, illetve egyéb a Szolgáltató által

megállapított díjakat (pl. adminisztrációs díj) előre, a Szolgáltató weboldalán közzétett mindenkori Árlista vagy egyedi ügyfélajánlatok szerint az ÁSZF-ben foglalt módon megfizetni.

A Szolgáltató a weboldalán közzétett árlistában és ajánlatokban különösen, de nem kizárólagosan teszi közzé a jelen Szabályzat szerinti archiválás szolgáltatáshoz kapcsolódó díjakat.

Szolgáltatásokat a Szolgáltató szolgáltatáscsomagok keretében is értékesítheti, ebben az esetben az archiválás szolgáltatás díját a szolgáltatáscsomag díja tartalmazza.

A feltételeket és a Szolgáltató díjaira vonatkozó egyéb szabályokat az ÁSZF tartalmazza.

9.1.1 Archiválás szolgáltatás díjai

A Szolgáltató az archiválás szolgáltatás igénybevételéért a nyilvános árlista alapján számíthat fel díjat Előfizető részére, illetve attól Előfizetővel való előzetes egyeztetés alapján eltérhet.

9.1.2 Visszatérítési politika

Amennyiben a szolgáltatási szerződés Szolgáltató ÁSZF-ben meghatározott, bizonyított súlyos szerződésszegése vagy ÁSZF módosítása miatt kerül felmondásra vagy a vonatkozó szolgáltatást Szolgáltató megszünteti a szerződés ideje alatt (feltéve, hogy azt más szolgáltató nem veszi át) akkor Szolgáltató az igénybevétellel arányos szolgáltatási díjat térít az Ügyfél részére. A szolgáltatási szerződés megkötésétől számított 14 napon belüli felmondás vagy elállás esetén Szolgáltató a teljes szolgáltatási díjat visszatéríti.

Szolgáltató egyéb esetekben, pl. a szolgáltatási szerződés - adott esetben idő előtti - megszűnése, illetve a szolgáltatás igénybe nem vétele, vagy a szerződési időre vonatkozó díjcsomagok ki nem használása esetén, a kifizetett szolgáltatási díjakat sem egészben sem részben nem téríti vissza Előfizető részére. E szolgáltatások díjai kifejezetten azzal a feltételezéssel lettek megállapítva, hogy az Ügyfelek egy része e kvótákat csak részben veszi majd igénybe.

9.2 Pénzügyi felelősség

Szolgáltató a pénzügyi felelősségét az alábbiak szerint korlátozza:
Az egyes szolgáltatások tekintetében Szolgáltató különböző felelősségvállalási értéket határoz meg az Árlistájában, amely biztosítási eseményenként (egy vagy több azonos okból bekövetkezett, időben összefüggő káresemény) érvényesíthető. Amennyiben egy adott biztosítási eseményben több Ügyfél, illetve több különböző szerződés és azokhoz tartozó archivált állományok is érintettek, akkor a kártérítés mértéke úgy kerül meghatározásra az egyes Ügyfelekkel és szerződésekkel összefüggésben, hogy az összesen kártérítés a legmagasabb felelősségvállalási értéket ne haladja meg és az adott szolgáltatáshoz tartozó felelősségvállalási érték is mindegyik esetben limitálásra kerüljön.
A felelősségvállalási értékekről Szolgáltató weboldalán nyújt tájékoztatást.

Ezen értékek a Szolgáltatások árlista szerinti teljes díjára tekintettel lettek megállapítva. Amennyiben Ügyfél a szolgáltatást kedvezményes díjjal veszi igénybe, akkor a kártérítés mértéke a biztosított kedvezményekhez mérten, azzal arányos módon kerülhet megállapításra.

9.2.1 Biztosítási fedezet

Szolgáltató - az Ügyfelek és Érintett felek esetleges kártalanításhoz és egyéb rendkívüli költségek fedezésére - felelősségbiztosítással rendelkezik. A felelősségbiztosítás kiterjed minden jelen szabályzat szerinti szolgáltatás nyújtása során a Szolgáltató kártérítési kötelezettségeire. Lásd a 9.6 fejezetet.

A felelősségbiztosítás továbbá kiterjed:

- a bizalmi szolgáltatási ügyfélnek a bizalmi szolgáltatási szerződés megszegésével összefüggésben okozott károkra,
- a bizalmi szolgáltatási ügyfélnek és harmadik személynek szerződésen kívüli okozott károkra,
- az Eüt.-ben foglalt kötelezettségek nem teljesítése miatt a bizalmi felügyeletnél felmerült, az Eüt. 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 alacsonyabb, mint 3 000 000 (hárommillió) forint.

9.2.2 Egyéb eszközök

Szolgáltató a szolgáltatás megszűntetési követelmények teljesítésével kapcsolatos költségek fedezetével rendelkezik. A kötelezettségek teljesítését 25.000.000 Ft-os bankgarancia szavatolja.

9.2.3 Az Érintett felek számára elérhető biztosítások és garanciák

Szolgáltató a vele szerződéses jogviszonyban nem álló harmadik személynek okozott kárért a Polgári Törvénykönyv általános szabályai szerint felel.

9.3 Bizalmas üzleti információk kezelése

Szolgáltató a birtokába jutott bizalmas adatokat a hatályos jogszabályi rendelkezésekre figyelemmel és az 5. fejezet rendelkezéseinek és a Szolgáltató nem nyilvános Adatkezelési szabályzatának előírásai szerint tárolja és kezeli.

A megőrzési kötelezettség lejártával - amennyiben az Ügyfél erről másképpen nem rendelkezik - Szolgáltató a bizalmas adatokat visszavonhatatlanul törli adatbázisából.

9.3.1 A bizalmas információk köre

A Szolgáltató bizalmas információnak tekint minden, az egyes Ügyfelekre vonatkozó adatot a 9.3.2 pontban foglaltak kivételével. Különösen és továbbá bizalmas adatok a következők:

- regisztrációs adatok;
- Ügyfél által megküldött dokumentumok;
- az ügyfélszolgálaton rögzített hangfelvételek;
-
- a szolgáltatás igénylése során Ügyfél által megadott adatok;

- szolgáltatási szerződések;
- nem nyilvános szabályzatok;
- a szolgáltatásokkal kapcsolatban keletkezett naplóadatokat;
- minden olyan adat, melynek nyilvánosságra hozatala veszélyeztetné a szolgáltatások biztonságát;
- minden olyan adat, melynek nyilvánosságra hozatala a fenti adatok harmadik felek általi megismeréséhez vezethet.

A bizalmas információkat a Szolgáltató a 9.3.3 fejezet szerint kezeli.

9.3.2 A bizalmas információk körén kívül eső adatok

A Szolgáltató az alábbi adatokat nem tekinti bizalmas információnak a személyes jellegüktől megfosztott adatokat, amennyiben azok semmiképpen nem köthetők az információ birtokosához vagy ahhoz, akire vonatkozóan az információból következtetés vonható le.

A bizalmasnak nem tekintett adatokat a Szolgáltató nyilvánosságra hozhatja, megoszthatja partnereivel, illetve nyilvánosságra kerülésükért nem tartozik felelősséggel.

9.3.3 A bizalmas információk védelme

A Szolgáltató a törvényi előírásokon és jelen Szolgáltatási szabályzat követelményein túlmenően Adatkezelési szabályzatában is rögzített módon mindent megtesz a 9.3.1 fejezet szerinti bizalmas információk biztonságos kezelése érdekében.

Azon adatokat, melyekhez a Szolgáltató elektronikus formában jutott hozzá, elektronikus formában, amelyek pedig papír alapon jutottak a birtokába, azokat papír alapon és/vagy elektronikus formában is megőrizheti és kezelheti.

Szolgáltató a személyes adatok megőrzését azok biztonságát illetve az adatvesztés, -sérülés és az adatok helytelen vagy illetéktelen használata, megismerése elleni védelmét az 5.5. fejezet előírásai szerint végzi, a 6.5. fejezet szerinti informatikai biztonsági előírások figyelembe vételével.

A Szolgáltató a birtokába jutott bizalmas adatokhoz csak azon 5.2.1 pont szerinti munkatársai számára ad hozzáférést, akiknek munkájuk elvégzéséhez ez elengedhetetlen (pl. Regisztrációs ügyintézők).

Szolgáltató az Ügyféladatokat az adott feladat nyújtásához szükséges mértékben és céllal alvállalkozóinak, megbízottainak átadhatja a következő esetekben:

- Szolgáltatás igénybevételéhez szükséges eszközök előállítása;
- Számlázás;
- Ügyfél elleni követelés érvényesítése.

A Szolgáltató az alábbi esetekben fedheti fel a bizalmas adatokat:

- Az Eüt. 93. § (5)-(7) bekezdések szerinti kötelező adatszolgáltatás a bizalmi felügyelet részére; a Szolgáltató az adatszolgáltatás során is biztosítja az adatok bizalmasságát, azok valódiságát és hiánytalanságát.
- Bűncselekmények felderítése vagy megelőzése céljából, illetőleg nemzetbiztonsági érdekből külön törvényben meghatározott feltételek teljesülése esetén a nyomozó hatóság és/vagy a nemzetbiztonsági szolgálatok részére az Eüt. 90. § (1)-(2) bekezdések szerint. Az adatátadás tényét a Szolgáltató rögzíti, az adatátadásról a Szolgáltató a jogszabály értelmében Ügyfelet nem tájékoztathatja.
- Információszolgáltatás polgári vagy büntető peres eljárás keretében, az Eüt. 90. § (3)

bekezdés szerint.
- Bizalmi szolgáltatás megszűnése esetén a megszüntetendő szolgáltatással kapcsolatos törvényben meghatározott adatok átadása az átvevő Szolgáltató részére az Eüt. 88. § bekezdés szerint.

9.4 Személyes adatok kezelése

A Szolgáltató az Ügyfelek személyes adatait a 9.3.1 fejezet szerinti bizalmas információnak tekinti, a 9.3.2 fejezetben foglalt kivételekkel és ennek megfelelő védelem (9.3.3. fejezet) mellett a 9.4.1 fejezet szabályait betartva kezeli őket.

9.4.1 Adatkezelési szabályok

A Szolgáltató az Ügyfelek személyes adatait
- jelen Szabályzat és a Szolgáltatási Rend,
- az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény,
- az Európai Parlament és a Tanács személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló 95/46/EK irányelve, és
- Szolgáltató Adatkezelési Szabályzatának

rendelkezéseit betartva kezeli.

A Szolgáltató biztosítja, hogy bármely adat rendelkezésére bocsátása esetén ezen adatokhoz illetéktelen személyek ne férhessenek hozzá.

Szolgáltató rendelkezik adatkezelési szabályzattal, amely részletes előírásokat tartalmaz a bizalmas és személyes információk kezelésére. Az adatkezelési szabályzat által lefektetett adatkezelési gyakorlatról Szolgáltató a weboldalán (lásd 1.1.2) közzétett Adatvédelmi tájékoztatóban tájékoztatja Ügyfeleit.

Szolgáltatót a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) nyilvántartásába vette, mint adatkezelőt; Szolgáltató adatkezelési nyilvántartási száma: NAIH-50145/2017.

9.4.2 Személyes adatok

A Szolgáltató minden olyan birtokába kerülő adatot személyes adatnak tekint,
- mely alapján természetes személy beazonosítható - különös tekintettel a természetes személy nevére vagy hatóság által nyilvántartott azonosítójára -, vagy
- ami természetes személlyel kapcsolatba hozható, vagy
- melyből a természetes személyre vonatkozó következtetés levonható, és
- amely nem sorolható egyúttal a 9.4.3 fejezet szerinti adatok közé.

A Szolgáltató csak az igényelt szolgáltatás nyújtásához szükséges elengedhetetlenül személyes adatokat kéri el az Ügyfelektől. Ez nem zárja ki, hogy a Szolgáltató a szolgáltatásnyújtáshoz kapcsolódóan olyan adatokat is elkérjen, amely birtokában a Szolgáltató hatékonyabban végezheti tevékenységét. Ezen adatok megadása nem kötelező, kezelésük pedig az érintett hozzájárulásán alapul.

9.4.3 Személyes adatnak nem minősülő információk

A 9.4.2 pontban meghatározott adatok körén kívül eső adatokat Szolgáltató nem tekinti személyes adatnak.

9.4.4 Személyes adatok védelme

Szolgáltató a birtokába jutó személyes adatokat a vonatkozó előírásoknak megfelelően (lásd 9.4.1) biztonságosan tárolja és védi. Az adatokat megfelelő intézkedésekkel védi a jogosulatlan hozzáférés és a megváltoztatás ellen, különösen az Ügyfél és a Szolgáltató egyes egységei között történő továbbítás során. Továbbá védi őket, az adatvesztés, a károsodás és a nem engedélyezett feldolgozás ellen is. Lásd még az 5.3.1, 5.5.1, 5.7.1, 5.7.4 és 9.3.3 fejezeteket.

9.4.5 Személyes adatok felhasználása

A Szolgáltató a személyes adatokat csak az Info tv. előírásaira tekintettel illetve olyan módon és mértékben használhatja fel, amely a szolgáltatással kapcsolatos műveletek elvégzéséhez szükséges.

9.4.6 Adatkezelés

Szolgáltató adatkezelésének jogalapja a Szolgáltató és az érintett jogos érdeke és az érintett előzetes – tájékoztatáson alapuló és konkrét – hozzájárulása.

A Szolgáltató a személyes adatokat a 9.4.1. pontban felsorolt hatályos jogszabályi rendelkezésekre figyelemmel és az 5. fejezet vonatkozó eljárási szabályainak megfelelően tárolja és kezeli; azokat csak a 9.3.3 pontban felsorolt, jogszabályok által meghatározott esetekben adhatja át a jogszabályok szerinti harmadik félnek.

9.4.7 Egyéb adatvédelmi követelmények

Szolgáltató az általa nyújtott bizalmi szolgáltatások felhasználásával elkövetett bűncselekmények felderítése vagy megelőzése céljából vagy nemzetbiztonsági érdekből - az érintett személyazonosságát igazoló, valamint egyeztetett adatok tekintetében - az adatigénylésre külön törvényben meghatározott feltételek teljesülése esetén díjmentesen adatokat továbbít a nyomozó hatóságnak és a nemzetbiztonsági szolgálatoknak. Az adatátadás tényét rögzíti, az adatátadásról az érintett feleket nem tájékoztatja (lásd 9.3.3).

9.5 Szellemi tulajdonhoz fűződő jogok

A szolgáltatási tevékenység során alkalmazott valamennyi

- név,
- termék,
- szoftver és hardver komponensek

a Szolgáltató tulajdonát képezik, vagy azokat jogszerűen használja.

A Szolgáltató tulajdonát képezik továbbá az általa közreadott / kibocsátott / létrehozott:

- szabályzatok,
- szerződési feltételek,
- általa készített egyéb dokumentumok és tájékoztatók.

A Szolgáltató működése során ügyel arra, hogy harmadik személyek szellemi tulajdonjogait ne sértse.

9.6 Felelősség és garanciák

Szolgáltató felelős minden olyan kárért, amelyet szándékosan vagy gondatlanul bármely természetes vagy jogi személynek okozott kötelezettségeinek megszegésével.

Minősített szolgáltatások esetén Szolgáltató szándékossága / gondatlansága vélelmezett mindaddig, amíg Szolgáltató bizonyítja az ellenkezőjét.

Szolgáltató nem felelős a szolgáltatások igénybevételére vonatkozó korlátozásokat meghaladó károkért (a korlátozásokat lásd jelen szabályzatban, a Szolgáltatási Rendben, az ÁSZF-ben, és a Szolgáltatási szerződésben).

Szolgáltató felelős a szabályzatai keretei között végzett szolgáltatói tevékenységekért valamint Regisztrációs és Hitelesítő egységének működéséért akkor is, ha egyes funkciókat Szolgáltatói Partnerek végeznek.

9.6.1 A Hitelesítő Egység felelőssége

Archiválás szolgáltatásban nem értelmezett.

9.6.2 A Regisztrációs Egység felelőssége

A Regisztrációs Egység felelőssége:

- az Igénylők (személy-) azonosságának megállapítása, a szolgáltató rendelkezésére bocsátott adatok ellenőrzése;
- nem természetes személy előfizető esetén az Előfizető szervezeti azonosságának, a szervezet nevében eljáró személy személyazonosságának és képviseleti jogosultságának megállapítása, ellenőrzése;
- a szolgáltatási szerződésbe kerülő adatok valódiságának garantálása;
- a szolgáltatási szerződés megkötését megelőzően Ügyfél tájékoztatása a Bizalmi Szolgáltatási Rend és a Szolgáltatási Szabályzat tartalmáról és elérhetőségéről, a szolgáltatás igénybevételének feltételeiről;
- a szolgáltatási szerződés sikeres megkötését követően a Szolgáltató archiváló rendszerében a Végfelhasználói fiók aktiválása
- szükség esetén a Szolgáltató archiváló rendszerében a Végfelhasználói fiók felfüggesztése, aktiválása vagy törlése
- általános kötelezettségeinek maradéktalan betartása.

9.6.3 Ügyfelek felelőssége és kötelezettségei

Az Ügyfél további kötelezettségeit és felelősségét az Általános szerződési feltételek, valamint a Szolgáltatási Szabályzat s határozzák meg.

Ügyfél köteles:

- a szolgáltatás igénybevétele előtt, a Bizalmi Szolgáltatási Rend és jelen Szolgáltatási Szabályzat, illetve az ÁSZF és a Szolgáltatási szerződés tartalmát megismerni
- a Szolgáltatóval szolgáltatási szerződést kötni, vagy az általános szerződési feltételekkel megegyező megállapodást kötni;
- a szolgáltatási szerződés megkötéséhez valós adatokat megadni, valamint haladéktalanul tájékoztatni a Szolgáltatót ezen adatok változásáról;

- haladéktalanul tájékoztatni a Szolgáltatót a bizalmi szolgáltatással vagy a Szolgáltatónál archivált állományokkal kapcsolatban észlelt, a külön jogszabályban, szolgáltatási szerződésben illetve szolgáltatási szabályzatban meghatározott rendellenességről vagy más, a bizalmi szolgáltatást érintő eseményről, így különösen arról, ha a szolgáltatás használatához szükséges, a Szolgáltató által biztosított időbélyeg-URL-t jogosulatlan személy használhatta;
- haladéktalanul tájékoztatni a Szolgáltatót a bizalmi szolgáltatással kapcsolatos jogvita megindulásáról.

9.6.4 Érintett felek felelőssége

Az Érintett Feleknek a Szolgáltató által garantált biztonsági szint megtartásához szükséges körültekintő eljárás érdekében továbbá javasolt:

- a Szolgáltatás elfogadottságának és minősített voltának bizalmi listán való ellenőrzése;
- a Szolgáltató Bizalmi Szolgáltatási Rendjében és jelen Szabályzatban megfogalmazott követelmények, előírások betartása;
- megbízható informatikai környezet és alkalmazások használata;
- az archivált állományon található aláíráshoz, időbélyeghez vagy felülhitelesítéshez használt tanúsítvány állapotának ellenőrzése az aktuális CRL-lel vagy OCSP válasszal.

Az Érintett Felek saját belátásuk és/vagy szabályzataik alapján jogosultak dönteni az egyes tanúsítványok elfogadásáról, illetve azok felhasználási módjáról.

9.6.5 Egyéb résztvevők felelőssége

Amennyiben a szervezet képviselője nem személyesen jár el az archiválás szolgáltatás igénylése során, úgy a képviselt szervezet felelősséggel tartozik az általa kiadott igazolásokért, különös tekintettel azon igazolásokra, amelyben azt igazolja, hogy az Igénylő jogosult a Szervezet nevében a szolgáltatás igénylésére.

9.7 Szavatosság kizárása

A Szolgáltatóval szemben a szolgáltatásaival kapcsolatban támasztott jótállási, szavatossági vagy kártérítési igényeket Szolgáltató visszautasítja, amennyiben

- annak alapját képező eset Ügyfél mulasztására, kötelezettségeinek és felelősségeinek be nem tartására vagy külső, előre nem látható eseményekre vezethető vissza;
- az Érintett felek által alkalmazott eljárások nem felelnek meg a jelen Szolgáltatási szabályzatnak;
- Szolgáltató az internet, vagy egy részének működési hibájából adódóan nem tudja ellátni a tájékoztatási és egyéb kommunikációs kötelezettségeit;
- a károkozás a Felügyeleti szerv által jóváhagyott kriptográfiai algoritmusok hibájából, illetve gyengeségeiből ered.

9.8 Felelősség korlátozása

Szolgáltató a kártérítési felelősségét a 9.16.5 szerint és az alábbiak szerint korlátozza.

Szolgáltató nem felelős az olyan károkért, amelyeket a Szolgáltató szavatosságának 9.7 pont szerinti kizárásához vezető körülmények okoztak, továbbá abban az esetben, ha Ügyfél vagy az

Érintett fél nem tanúsította a tőle elvárható gondosságot, nem a Szolgáltató Kikötései szerint vagy jogellenesen jártak el.

Szolgáltató a szolgáltatásaival kapcsolatos szerződéses és szerződésen kívüli károkért harmadik személlyel szemben kizárólag a saját hibájából, kötelezettségeinek megszegéséből, valamint a neki felróható okokból bekövetkező, bizonyítható károkért tartozik helyt állni.

A felelősség - és annak korlátozása - tekintetében lásd még a 9.2 és 9.6 pontban foglaltakat.

9.9 Kártérítés, kártalanítás

Szolgáltató kártérítési felelősségének fedezetéül felelősségbiztosítással rendelkezik (lásd. 9.2 pont).

Ügyfél kártérítési felelősséggel tartozik Szolgáltatónak azokért a bizonyított veszteségekért és károkért, amelyeket a rá vonatkozó kötelezettségek és ajánlások szándékos vagy gondatlan megszegésével okoz a Szolgáltató kárára.

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

A felelősség bizonyítása tekintetében lásd a 9.6, a jótállási, szavatossági vagy kártérítési, kártalanítási igényekkel kapcsolatban lásd a 9.7, 9.8 pontban foglaltakat.

9.10 A szabályzat hatálya

9.10.1 Érvényesség

A Szabályzat időbeli hatálya a jelen verzió hatálybalépésének fedlapon jelzett dátumától (hatály kezdőnapja) kezdődik.

A Szabályzat személyi hatálya a Szolgáltató bizalmi munkatársaira, a szolgáltatói partnerekre, az Ügyfelekre és minden Érintett félre kiterjed.

A Szabályzat tárgyi hatálya a jelen Szolgáltatási szabályzat 1.1 pontja szerinti szolgáltatások nyújtását és igénybevételét foglalja magában.

9.10.2 Megszűnés

A Szabályzat érvényessége a szolgáltatási tevékenység beszüntetéséig, a szabályzat visszavonásáig vagy újabb szabályzatverzió hatályba lépéséig tart.

9.10.3 A megszűnés következményei

A Szabályzat visszavonása esetén a Szolgáltató weboldalán teszi közzé a visszavonás részletes szabályait és a visszavonás után is fennálló jogokat és kötelezettségeket.

A Szolgáltató vállalja, hogy a Szolgáltatási Szabályzat visszavonása esetén is érvényben maradnak a mindenkor hatályos vonatkozó jogszabályokban meghatározott bizalmas adatok védelmére vonatkozó előírások.

9.11 Egyedi értesítések és a résztvevők közti kommunikáció

A Szolgáltató az Ügyfelekkel történő kapcsolattartás érdekében ügyfélszolgálati irodát és

telefonos ügyfélszolgálatot működtet az 1.1.2 pontban megadott elérhetőségekkel (lásd még 1.3.2 pont).

Az Ügyfélszolgálat a szolgáltatások igénybevételével és egyéb, az archiválásszolgáltatás igénybevételével kapcsolatos ügyintézések és eljárások során elsősorban e-mailek útján kommunikál Ügyféllel. Emellett az Ügyfélszolgálat telefonon, faxon és személyesen is megkereshető.

Szolgáltató az ügyfelek felé küldött ügyfélszolgálati e-mailjeit egyedi azonosítóval látja el, mely alapján ügyfélmegkeresés esetén könnyen azonosítható az adott ügy vagy téma. Amennyiben Ügyfél egy ilyen levélre válaszol, az adott ügy minél gyorsabb előrehaladása érdekében, ügyelnie kell arra, hogy az üzenet tárgya változatlan maradjon.

Amennyiben Ügyfél nem ügyfélszolgálati levélre válaszol, tegyen meg mindent azért, hogy levele alapján a lehető legkönnyebben beazonosítható legyen, így például az e-mailt elektronikusan aláírva/bélyegezve és/vagy az e-mailt a szolgáltatás igénybevételét megelőző regisztrációkor megadott email címről küldve.

Az e-mailes megkeresések során szükséges továbbá, hogy a levélben egyértelműen beazonosítható legyen a kérdéses szolgáltatás.

Amennyiben Ügyfél keresi fel a Szolgáltatót e-mailben vagy faxon a Regisztrációs ügyintéző felelőssége eldönteni, hogy az email vagy fax alapján milyen lépések tehetők. Amennyiben Szolgáltatónak további információra van szüksége, arról válaszlevélben ad tájékoztatást. Amennyiben az Ügyfél beazonosíthatósága felől merülnek fel kétségek, Szolgáltató megkísérli telefonon felkeresi az Ügyfelet, a személyes adatok egyeztetése céljából.

Az e-mailes kommunikáció mellett az alábbi kommunikációs lehetőségek állnak Ügyfelek rendelkezésére.

Telefon

Az ügyfélszolgálati telefonszámon ügyintéző kizárólag a weboldalon meghirdetett időpontokban érhető el, egyéb időszakokban üzenet hagyható (kivéve a visszavonási igények esetét, lásd 4.9.4).

Ügyfélszolgálati irodában, személyesen

Szolgáltató ügyfélszolgálati irodájában (lásd 1.1.2 pont) személyes egyeztetésre kizárólag előre egyeztetett kérdésekben fogadja az Ügyfeleket.

9.12 Módosítások

A Szolgáltató a normatív szabályok, biztonsági követelmények, piaci környezet vagy egyéb körülmények változása esetén megváltoztathatja Szolgáltatási szabályzatát.

A szabályzatok egymásnak, a vonatkozó jogszabályoknak és szabványoknak való megfelelés vizsgálata legalább évente történik. A szabályzatok rendkívüli felülvizsgálatára és módosítására a jogszabályi és/vagy a műszaki szabványkörnyezet változása esetén kerül sor. Szolgáltató a működése során szerzett gyakorlati tapasztalatok alapján is folyamatosan felülvizsgálja Szolgáltatási szabályzatát.

A módosított szabályzatot Szolgáltató legkorábban a közzétételtől és a bizalmi felügyelet értesítésétől számított 30. napon lépteti hatályba, de rendkívüli esetben a változások azonnali hatállyal is életbe léptethetők.

Szolgáltató a bizalmi felügyelet számára bejelenti, ha a korábbi bejelentések alapján nyilvántartásba vett adatokhoz képest működésében vagy a bizalmi szolgáltatás nyújtásában – így például a szolgáltatási rendben vagy szabályzatban – változás történik.

Lásd még az 1.5 és 2.1 fejezetet.

9.12.1 A módosítási eljárás

Szolgáltató a szabályzatváltoztatási igényeket gyűjti (lásd 1.5), a módosításokat elvégzi, a belső és külső tájékoztatási kötelezettségeknek eleget tesz, s a változtatásokat életbe lépteti.

Szolgáltató a változtatási igényeket előzetesen megvizsgálja a Szolgáltatási Rendben meghatározott tartalmi követelményeknek valamint a jogszabályi és szabvány elvárásoknak való megfelelőség szempontjából. Amennyiben egyikkel kapcsolatban sem merül fel kifogás, a módosítási igényt elfogadja és megkezdi annak kidolgozását.

A változtatásokat gyűjtve a Szabályzatelfogadó Egység belső, nem nyilvános munkaváltozatokat hoz létre a szabályzatokból, melyek a közzététel előtt belső felülvizsgálaton esnek át. Szolgáltató a változásokat – lehetősége szerint – kötegelve szerkeszti új szabályzati változattá, törekedve arra, hogy új szabályzatot csak a lehető legritkábban kelljen kibocsátania.

A kidolgozott módosításokat a Szabályzat jóváhagyója (lásd 1.5) fogadja el, melyet megelőzően szintén megvizsgálja a fenti tartalmi és formai követelményeket. Ezt követően kerül sor a Bizalmi Felügyelet, az Ügyfelek és az Érintett felek értesítésére (lásd 9.12.2). A Szabályzat jóváhagyására a Szolgáltató végső hatáskörrel és felelősséggel rendelkezik, majd bejelentés után a Szabályzatot a Bizalmi Felügyelet nyilvántartásba veszi.

A Szolgáltatási Szabályzat jóváhagyására a Szolgáltató végső hatáskörrel és felelősséggel rendelkezik.

A módosított szabályzatváltozatok – a nyilvános tervezetek is – mindig új verziószámmal kerülnek nyilvánosságra.

A Szolgáltató a közzétett új tervezettel kapcsolatos észrevételeket a hatálybalépést megelőző 14. napig fogadja e-mailben (lásd 1.5). Érdemi változtatást igénylő észrevétel esetén Szolgáltató a tervezeten elvégzi a szükséges módosításokat, az észrevételekkel módosított változatát pedig a hatálybalépést megelőzően közzéteszi.

9.12.2 Az értesítések módja és határideje

Szolgáltató az új szabályzatváltozatok tervezett hatálybaléptetése előtt legalább 30 nappal értesíti a bizalmi felügyeletet az új szabályzatverzióról. Az értesítéssel egyidejűleg Szolgáltató a változásokkal módosított és jóváhagyott új szabályzatverziót is megküldi a Bizalmi felügyeletnek valamint – az Ügyfelek és Érintett felek tájékoztatására – közzéteszi azt a weboldalán (lásd 2.1.2).

Amennyiben a Szolgáltató a változás következtében, azzal egyidejűleg új szolgáltatás indítását is tervezi, az új szolgáltatás tervezett indítása előtt legalább 30 nappal bejelenti azt a Bizalmi felügyeletnek.

A bejelentést Szolgáltató a bizalmi felügyelet weboldalán közzétett űrlapon, a 470/2017 Kormányrendeletben foglaltak szerint teszi meg. Az űrlaphoz a Szolgáltató csatolja

- a módosított és jóváhagyott új Szolgáltatási Rend verziót;
- a módosított és jóváhagyott új Szolgáltatási Szabályzat verziót;
- a módosított és jóváhagyott új Szabályzatkivonat verziót;
- valamint a 470/2017 Kormányrendeletben meghatározott egyéb iratokat és dokumentumokat.

9.12.3 A dokumentumazonosító változása

A Szolgáltatási Szabályzat újabb nyilvános változatai – a tervezetek is – mindig új verziószámmal kerülnek nyilvánosságra, vagyis a két eltérő tartalmú dokumentumnak nem lehet azonos OID azonosítója.

A dokumentum azonosítója a következő elemekből épül fel – az egyes elemeket pontok

választják el egymástól: szolgáltatói OID (1.3.6.1.4.1.3555), nyilvános dokumentumok jelölése (1), dokumentumtípus megjelölése, jóváhagyás dátuma, azaz jelen szolgáltatási szabályzat esetén: 1.3.6.1.4.1.3555.1.47.jóváhagyás dátuma.

A módosított Szabályzat csak a hatálybalépését követően, újonnan kibocsátásra kerülő tanúsítványokra vonatkozik (de a már kibocsátottakra nem).

9.13 Vitás kérdések rendezése

A Szolgáltató (beleértve a szolgáltatói partnereket is) tevékenységével kapcsolatos kérdéseket, kifogásokat és panaszokat e-mailben, telefonon vagy személyesen a Szolgáltató ügyfélszolgálati irodájában fogad (lásd 1.1.2. pont).

Bármely vitás kérdés vagy panasz felmerülése esetén, a vita jogi útra terelése előtt az Ügyfélnek kötelessége, az Érintett Félnek vagy bármely harmadik félnek pedig ajánlott a Szolgáltató haladéktalan értesítése és teljes körű tájékoztatása az ügy minden vonatkozását érintően. A felek vitáikat mindenkor megkísérlik békés, tárgyalásos úton rendezni.

9.13.1 Panaszok kezelésének eljárása

Szolgáltató a panaszokat a bejelentésüktől számított 30 naptári napon belül kivizsgálja, a kivizsgálás eredményéről pedig - felek eltérő megállapodását kivéve - e-mailben tájékoztatja a panasz benyújtóját. Amennyiben a panasz jellege miatt a kivizsgálás előre láthatólag 30 naptári napnál hosszabb időt vesz igénybe, erről a Szolgáltató külön tájékoztatja a panaszbejelentő Ügyfelet.

A személyesen vagy telefonon tett panasz esetén a Szolgáltató jegyzőkönyvet vesz fel a panasz felvételéről.

A Szolgáltató a panasz kivizsgálását követően - amennyiben értelmezett - a felmerült hibát a műszakilag indokolt időn belül elhárítja, és mindezen tevékenységekről a bejelentőt írásban tájékoztatja.

Amennyiben a választ a bejelentő Ügyfél nem fogadja el, akkor egyeztetést kezdeményezhet a Szolgáltatóval. Amennyiben a Szolgáltató ezt megtagadja, vagy ha a felek közötti egyeztetés annak kezdeményezésétől számított 20 munkanapon belül nem vezet eredményre, akkor a vita rendezésére a 9.13.2 pont szerint kerülhet sor.

9.13.2 Vitás kérdések rendezése békés, tárgyalásos úton

Amennyiben Ügyfél és Szolgáltató közötti egyeztetés nem vezet eredményre, akkor az esetleges bírósági eljárást megelőzően javasolt Ügyfél számára a Budapesti Békéltető Testülethez fordulni.

Jelen szabályzat hatálybalépésekor az illetékes szervezetek elérhetőségei a következők:

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
- Weboldal: www.bekeltet.hu

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

9.13.3 Vitás kérdések rendezése peres úton

Amennyiben a vitás kérdés rendezése a 9.13 pont szerinti tárgyalásos megoldások egyikével sem lehetséges, felek bírósági útra terelhetik az ügyet. Ebben az esetben a felek kölcsönösen alávetik magukat a Budapesti II. és III. Kerületi Bíróság kizárólagos illetékességének.

9.14 Irányadó jog

A Szolgáltató tevékenységét a mindenkor hatályos magyar és európai uniós jogszabályoknak megfelelően végzi. A Szolgáltató szerződéseire és szabályzataira, azok teljesítésére a magyar jog az irányadó, és azok a magyar jog szerint értelmezendők (lásd a 9.15 fejezetet).

9.15 A hatályos jogszabályoknak és szabványoknak való megfelelés

A Szolgáltató a hatályos jogszabályoknak és szabványoknak megfelelően végzi tevékenységét. A hatályos jogszabályoknak megfelelő működést a Szolgáltató és a bizalmi szolgáltatások Bizalmi Felügyelet általi nyilvántartásba vétel is igazolja.

A Szolgáltató tevékenységét az alábbi jogszabályok, szabványok és egyéb előírások rá vonatkozó kötelező előírásainak megfelelően végzi:

- **eIDAS:** az Európai Parlament és Tanács 910/2014/EU Rendelet (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről;
- **Eüt.:** 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól;
- **BM rendelet:** a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről szóló 24/2016 (VI. 30.) BM rendelet;
- 470/2017 (XII. 28.) Korm. rendelet a bizalmi felügyelet által vezetett nyilvántartások tartalmáról és a bizalmi szolgáltatás nyújtásával kapcsolatos bejelentésekről
- **Közigazgatási Rendelet:** az elektronikus ügyintézési szolgáltatások nyújtására felhasználható elektronikus aláíráshoz és bélyegzőhöz kapcsolódó követelményekről szóló 137/2016. (VI.13.) Korm. rendelet;
- A Bizottság (EU) 2015/1506 Végrehajtási határozata (2015. szeptember 8.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról szóló 910/2014/EU európai parlamenti és tanácsi rendelet 27. cikkének (5) bekezdése és 37. cikkének (5) bekezdése szerint a közigazgatási szervek által elismert fokozott biztonságú elektronikus aláírások és fokozott biztonságú bélyegzők formátumaira vonatkozó specifikációk meghatározásáról;
- 137/2016. (VI. 13.) Korm. rendelet az elektronikus ügyintézési szolgáltatások nyújtására felhasználható elektronikus aláíráshoz és bélyegzőhöz kapcsolódó követelményekről;
- **Fgytv.:** 1997. évi CLV. törvény a fogyasztóvédelemről;
- **Nytv.:** 1992. évi LXVI. törvény a polgárok személyi adatainak és lakcímének nyilvántartásáról;
- **Szmtv.:** 2007. évi I. törvény a szabad mozgás és tartózkodás jogával rendelkező személyek beutazásáról és tartózkodásáról;

- **Harmtv:** 2007. évi II. törvény a harmadik országbeli állampolgárok beutazásáról és tartózkodásáról;
- **Ket:** 2004. évi CXL. törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól és ennek végrehajtási rendeletei;
- **Ptk.:** 2013. évi V. törvény a Polgári Törvénykönyvről;
- 45/2014 (II. 26.) Kormányrendelet a fogyasztó és a vállalkozás közötti szerződések részletes szabályairól;
- **Info tv.:** az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény;
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról;
- az Európai Parlament és a Tanács személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló 95/46/EK irányelve, és
- Közigazgatási Gyökér Hitelesítés-szolgáltató Hitelesítési Szabályzat;
- ISO 3166 English Country Names and Code Elements;
- FIPS PUB 140-2 (2001. május): "Kriptográfiai modulok biztonsági követelményei";
- RFC 5280 (korábban RFC 3280) és RFC 6818 Internet X.509 Nyilvános kulcsú infrastruktúra – tanúsítvány- és tanúsítvány visszavonási lista profil;
- RFC 3647 (korábban RFC 2527) Internet X.509 Nyilvános kulcsú infrastruktúra – tanúsítványtípus és Szolgáltatási Szabályzat keretrendszer - A szabályzatok szerkezete tekintetében;
- International Telecommunication Union X.509 “Információ technológia – Nyílt rendszerek kapcsolódása - Könyvtár: Nyilvános kulcs és attribútum tanúsítvány-keretrendszer”;
- RFC 6960 Online Certificate Status Protocol (OCSP);
- ETSI EN 319 401 General Policy Requirements for Trust Service Providers;
- ETSI EN 319 411-1 Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements;
- ETSI EN 319 411-2 Policy and security requeriments for Trust Service Providers issuing certificates; Part 2: Requirements for trust services providers issuing EU qualidied certificates;
- ETSI EN 319 412-1 Certificate Profiles; Part 1: Overview and common data structures;
- ETSI EN 319 412-2 Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons;
- ETSI EN 319 412-3 Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons;
- ETSI EN 319 412-4 Certificate Profiles; Part 4: Certificate profile for web site certificates issued to organisations;
- ETSI EN 319 412-5 Certificate Profiles; Part 5: QCStatements;
- ETSI EN 319 421 Policy and Security Requirements for Trust Service Providers issuing Time-Stamps;
- ETSI EN 319 422 Time-stamping protocol and time-stamp token profiles;
- LCP: Lightweight Certificate Policy, Könnyített Hitelesítési Rend, OID: 0.4.0.2042.1.3;
- NCP: Normalized Certificate Policy, Normalizált Hitelesítési Rend, OID: 0.4.0.2042.1.1;
- NCP+: Extended Normalized Certificate Policy, Kiterjesztett (Kriptográfiai eszköz használatát megkövetelő) Hitelesítési Rend, OID: 0.4.2042.1.2;
- EVCP: Extended Validation Certificate Policy: Kibővített ellenőrzésű weboldal-hitelesítő tanúsítványokra vonatkozó Hitelesítési Rend, 0.4.0.2042.1.4;
- IVCP: Individual Validation Certificate Policy Természetes személyek weboldal hitelesítő

tanúsítványára, OID: 2.23.140.1.2.3;
- RFC 6844 DNS Certification Authority Authorization (CAA) Resource Record;
- RFC 2616 Hypertext Transfer Protocol -- HTTP/1.1;
- CA/Browser Forum Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates
- CA/Browser Forum Guidelines For The Issuance And Management Of Extended Validation Certificates

9.16 Vegyes rendelkezések

9.16.1 Teljességi záradék

Teljességi záradékot a Szolgáltató nem köt ki.

9.16.2 Átruházás

A szolgáltatások nyújtásába bevont Szolgáltatói partnerek csak a Szolgáltató előzetes írásbeli engedélyével adhatják tovább jogosultságaikat és/vagy ruházhatják át kötelezettségeiket harmadik félnek.

9.16.3 Részleges érvénytelenség

Jelen Szabályzat egyes rendelkezéseinek bármilyen okból történő érvénytelenné válása esetén a többi rendelkezés változatlan formában érvényben marad.

9.16.4 Igényérvényesítés

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

9.16.5 Vis maior

A Szolgáltató nem felelős a Szabályzatban megfogalmazott követelmények hibás vagy késedelmes teljesítéséért, ha a hiba vagy késedelem oka a Szolgáltató ellenőrzési körén kívül eső, előre nem látható körülmény volt.

9.17 Egyéb rendelkezések

A vezető munkatársaknak függetlennek kell lenni minden olyan üzleti, pénzügyi és más befolyástól, ami hátrányosan hathat a szolgáltatásokba vetett bizalomra.