

# Minősített Elektronikus Archiválás- Szolgáltatás Szolgáltatási Szabályzat



NetLock Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaság

Nyilvántartási szám (OID): ----- 1.3.6.1.4.1.3555.1.47.20110308

A Szabályzat hatályának kezdőnapja: ----- **2011. március 15.**

OLDALAK SZÁMA: ----- **38, HARMINCNYOLC**

**© COPYRIGHT NETLOCK KFT. ----- MINDEN JOG FENNTARTVA**

Jóváhagyta: ----- **Rózsahegyi Zsolt**, Ügyvezető

Jóváhagyás dátuma: ----- **2011. március 8.**

Jóváhagyom: .....

PH.

OID	Változás leírása	Hatálybalépés	Készítő	Ellenőrző
1.3.6.1.4.1.3555.1.46.20100723	Dokumentum létrehozása	2010.07.23.	NetLock Szabályzat Elfogadó Egység (SzEE)	NetLock Szabályzat Elfogadó Egység (SzEE)
1.3.6.1.4.1.3555.1.46.20100819	NHH észrevételek alapján történő pontosítások	Nem lépett hatályba	NetLock Szabályzat Elfogadó Egység (SzEE)	NetLock Szabályzat Elfogadó Egység (SzEE)
1.3.6.1.4.1.3555.1.46.20100827	NMHH észrevételek alapján történő pontosítások	2010.09.01.	NetLock Szabályzat Elfogadó Egység (SzEE)	NetLock Szabályzat Elfogadó Egység (SzEE)
1.3.6.1.4.1.3555.1.47.20101213	NMHH észrevételek alapján történő pontosítások	2011.01.01.	NetLock Szabályzat Elfogadó Egység (SzEE)	NetLock Szabályzat Elfogadó Egység (SzEE)
1.3.6.1.4.1.3555.1.47.20110301	NMHH észrevételek alapján történő pontosítások	2011.03.01.	NetLock Szabályzat Elfogadó Egység (SzEE)	NetLock Szabályzat Elfogadó Egység (SzEE)
1.3.6.1.4.1.3555.1.47.20110308	Hatálybalépés időpontjának módosítása	2011.03.08.	NetLock Szabályzat Elfogadó Egység (SzEE)	NetLock Szabályzat Elfogadó Egység (SzEE)

# Tartalomjegyzék

<b>1</b>	<b>Bevezetés</b>	<b>6</b>
<b>1.1</b>	<b>Áttekintés</b>	<b>6</b>
1.1.1	A Szabályzat	6
1.1.2	A Szabályzat hatálya	6
1.1.3	A Szolgáltató	7
1.1.4	Szolgáltatások	7
1.1.5	Szabványok és előírások	9
<b>1.2</b>	<b>Dokumentum neve és azonosítása</b>	<b>10</b>
<b>1.3</b>	<b>Közösség</b>	<b>10</b>
1.3.1	Szolgáltató	11
1.3.2	Előfizető	11
1.3.3	Érintett fél	11
<b>1.4</b>	<b>Alkalmazhatóság</b>	<b>11</b>
<b>1.5</b>	<b>Kapcsolattartás</b>	<b>11</b>
1.5.1	A Szolgáltató adatai	11
1.5.2	Ügyfélszolgálat	11
1.5.3	Szabályzattal kapcsolatos kérdések	11
1.5.4	Szabályzat-jóváhagyási eljárás	12
<b>1.6</b>	<b>Fogalmak és rövidítések</b>	<b>12</b>
	Fogalmak	12
<b>2</b>	<b>Közzététel</b>	<b>14</b>
<b>2.1</b>	<b>A Szolgáltatói információ közzététele</b>	<b>14</b>
2.1.1	Közzétételi és tájékoztatási elvek	14
2.1.2	Kikötések és feltételek közzététele	14
2.1.3	Rendkívüli információk közzététele	14
<b>2.2</b>	<b>A közzététel gyakorisága</b>	<b>15</b>
2.2.1	Kikötések és feltételek közzétételi gyakorisága	15
2.2.2	Rendkívüli információk közzétételi gyakorisága	15
<b>2.3</b>	<b>Hozzáférés ellenőrzések</b>	<b>15</b>
<b>3</b>	<b>Az elektronikus archiválás szolgáltatás nyújtása</b>	<b>16</b>
<b>3.1</b>	<b>Szolgáltatási szerződés kötése</b>	<b>16</b>
<b>3.2</b>	<b>Dokumentum feltöltése</b>	<b>16</b>
3.2.1	A visszaigazolás	18
<b>3.3</b>	<b>Érvényességi lánc elérhetőségének biztosítása</b>	<b>18</b>
<b>3.4</b>	<b>Az igazolás</b>	<b>19</b>
<b>3.5</b>	<b>Dokumentum megjelenítése</b>	<b>20</b>
<b>3.6</b>	<b>Dokumentum és érvényességi lánc törlése</b>	<b>20</b>
<b>3.7</b>	<b>A szolgáltatási szerződés megszűnése</b>	<b>21</b>
<b>4</b>	<b>Fizikai, eljárásbeli és személyzeti biztonsági óvintézkedések</b>	<b>22</b>
<b>4.1</b>	<b>Fizikai óvintézkedések</b>	<b>22</b>
4.1.1	A telephely elhelyezése és szerkezeti felépítése	22
4.1.2	Fizikai hozzáférés	22
4.1.3	Fizikailag elkülönítetten őrzött mentési példányok	23

<b>4.2</b>	<b>Eljárásbeli óvintézkedések .....</b>	<b>23</b>
4.2.1	Bizalmi munkakörök .....	23
4.2.2	Az egyes feladatokhoz szükséges személyzeti létszámok .....	24
4.2.3	Az egyes munkakörökben elvárt azonosítás és hitelesítés .....	24
4.2.4	Változáskezelés .....	24
<b>4.3</b>	<b>Személyzetre vonatkozó óvintézkedések .....</b>	<b>24</b>
<b>4.4</b>	<b>A biztonsági naplózás folyamatai .....</b>	<b>24</b>
<b>4.5</b>	<b>Egyéb rendelkezések .....</b>	<b>25</b>
<b>4.6</b>	<b>Helyreállítás kompromittálódás és katasztrófa esetén .....</b>	<b>25</b>
4.6.1	Incidens- és kompromittálódás-kezelési eljárások .....	25
4.6.2	Sérült számítási erőforrások, szoftverek és/vagy adatok .....	25
4.6.3	Biztonsági képesség egy természeti vagy más egyéb katasztrófát követően .....	25
<b>4.7</b>	<b>A Szolgáltató leállítása .....</b>	<b>26</b>
4.7.1	Szolgáltatás megszüntetése .....	26
<b>5</b>	<b>Műszaki óvintézkedések .....</b>	<b>27</b>
<b>5.1</b>	<b>Rendszeres felülhitelesítés .....</b>	<b>27</b>
<b>5.2</b>	<b>A technológia folyamatos figyelése .....</b>	<b>27</b>
<b>5.3</b>	<b>Hitelesítés- és időbélyegző szolgáltató elfogadása .....</b>	<b>27</b>
<b>5.4</b>	<b>Az elektronikus dokumentumok értelmezhetőségének (olvashatóságának) fenntartása .....</b>	<b>27</b>
<b>5.5</b>	<b>Az elektronikus archiválási szolgáltatás egyes elemeinek rendelkezésre állása .....</b>	<b>27</b>
<b>5.6</b>	<b>Biztonsági garanciák .....</b>	<b>28</b>
<b>5.7</b>	<b>Számítógép-biztonsági óvintézkedések .....</b>	<b>28</b>
5.7.1	Speciális számítógép-biztonsági műszaki követelmények .....	28
5.7.2	Informatikai biztonsági osztályozás .....	29
<b>5.8</b>	<b>Életciklusra vonatkozó műszaki óvintézkedések .....</b>	<b>29</b>
<b>5.9</b>	<b>Hálózatbiztonsági óvintézkedések .....</b>	<b>29</b>
<b>6</b>	<b>Megfelelőség vizsgálata .....</b>	<b>30</b>
<b>6.1</b>	<b>A megfelelés vizsgálatának gyakorisága .....</b>	<b>30</b>
<b>6.2</b>	<b>Az átvizsgáló egységek megnevezése .....</b>	<b>30</b>
<b>6.3</b>	<b>Az átvizsgáló egységek és a vizsgált fél kapcsolata .....</b>	<b>30</b>
<b>6.4</b>	<b>A vizsgálat által érintett területek .....</b>	<b>31</b>
<b>6.5</b>	<b>Hiányosságok esetén végrehajtandó tevékenységek .....</b>	<b>31</b>
<b>7</b>	<b>Üzleti és jogi tudnivalók .....</b>	<b>32</b>
<b>7.1</b>	<b>Díjak .....</b>	<b>32</b>
<b>7.2</b>	<b>Bizalmasság, adatkezelés .....</b>	<b>32</b>
7.2.1	Személyes adatok .....	32
7.2.2	Archivált adatok .....	32
7.2.3	Törvény által elrendelt adatszolgáltatás .....	33
<b>7.3</b>	<b>Szellemi alkotásokhoz fűződő jogok .....</b>	<b>33</b>
<b>7.4</b>	<b>Jogok és kötelezettségek .....</b>	<b>33</b>
7.4.1	Az Előfizető jogai és kötelezettségei .....	33
7.4.2	Ajánlások az Érintett Fél részére .....	33
7.4.3	Szolgáltató egyéb kötelezettségei .....	34

<b>7.5</b>	<b>Felelősség .....</b>	<b>35</b>
7.5.1	A Szolgáltató általános felelőssége .....	35
7.5.2	Az Előfizető felelőssége .....	36
<b>7.6</b>	<b>Változtatási eljárás.....</b>	<b>36</b>
<b>7.7</b>	<b>Panaszkezelés.....</b>	<b>36</b>
7.7.1	Panaszok benyújtásának helye.....	36
7.7.2	Panaszok benyújtásának módja .....	36
7.7.3	Panaszok kezelésének eljárása.....	36
7.7.4	Illetékes fogyasztóvédelmi felügyelőség .....	36
<b>7.8</b>	<b>Hivatkozott jogszabályok, szabványok és egyéb dokumentumok .....</b>	<b>37</b>
<b>7.9</b>	<b>Értelmezés és érvényesítés.....</b>	<b>38</b>
7.9.1	Irányadó jog.....	38
7.9.2	A rendelkezések különválaszthatósága.....	38
7.9.3	A rendelkezések kiterjesztése .....	38
7.9.4	Értesítések .....	38
7.9.5	Vitás kérdések megoldására vonatkozó eljárások.....	38

# 1 Bevezetés

## 1.1 Áttekintés

A jelen Szabályzat a NetLock Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaság (a továbbiakban: Szolgáltató) Minősített Elektronikus Archiválás Szolgáltatásra vonatkozó Szolgáltatási Szabályzata (a továbbiakban: Szabályzat).

A Szolgáltató – az elektronikus archiválás szolgáltatáson túlmenően - az elektronikus kommunikáció hitelességét és bizalmasságát biztosító elektronikus tanúsítványok kiadását, az ehhez kapcsolódó nyilvános adatbázisok, illetve infrastruktúra karbantartását és üzemeltetését végzi. A hitelesítés-szolgáltatói tevékenység mellett kiemelt terület a PKI tanácsadás- és integráció: vállalati és országos szintű elektronikus hitelesítési rendszerek tervezése és megvalósítása, valamint a hiteles és bizalmas kommunikációhoz elengedhetetlen eszközök, az elektronikus kulcsok biztonságos készítését, tárolását biztosító hardvereszközök (intelligens kártyák és USB kompatibilis egységek) telepítése és folyamatos támogatása.

Az archiválás szolgáltatás, tanúsítványhitelesítés, PKI tanácsadás és rendszerintegráció mellett a Szolgáltató időbélyeg-szolgáltatást is végez, illetve elektronikus aláírást létrehozó adat elektronikus aláírást létrehozó eszközön való elhelyezése szolgáltatást is nyújt.

A Szolgáltató szolgáltatásait a vele szerződéses viszonyban álló Felek részére biztosítja. Jelen szabályzat vonatkozik az elektronikus archiválás szolgáltatás keretében kiállított igazolások ellenőrzésében Érintett Félre is.

**Jelen Szabályzat kizárólag a minősített elektronikus archiválás szolgáltatásra vonatkozó szabályokat tartalmazza.**

### 1.1.1 A Szabályzat

Jelen Szolgáltatási Szabályzat a Szolgáltató minősített elektronikus archiválás szolgáltatásként nyújtott szolgáltatásaival kapcsolatos részletes eljárási és egyéb működési szabályokat tartalmazza.

A Szabályzat összefoglalóan tartalmazza mindazon szabályokat, információkat, melyek a Szolgáltató tevékenységével kapcsolatosak, és amelyeket a Szolgáltatóval valamilyen módon kapcsolatba kerülőknek (elsősorban a Előfizető és Érintett Feleknek) érdemes tudni. Mint ilyen, a Szolgáltató működésének átláthatóságát biztosítja, és lehetővé teszi a felhasználók számára, hogy megállapítsák, hogy a Szolgáltató gyakorlata mennyiben felel meg elvárásaiknak.

A jelen Szabályzat tartalmára és felépítésére az RFC 3647 [9] dokumentum adott útmutatót, amely struktúráját a Szabályzat követi.

### 1.1.2 A Szabályzat hatálya

#### 1.1.2.1 Tárgyi hatály

A Szabályzat tárgyi hatálya az 1.1.4 pontban ismertetett szolgáltatások nyújtását és igénybevételét foglalja magában.

#### 1.1.2.2 Időbeli hatály

A Szabályzat időbeli hatálya a jelen verzió hatálybalépésének dátumától kezdődik, és a szolgáltatási tevékenység beszüntetéséig, illetve egy újabb szabályzat verzió hatályba lépéséig tart.

### 1.1.2.3 Személyi hatály

A Szabályzat személyi hatálya az Előfizetőre és a Szolgáltatóra terjed ki.

### 1.1.2.4 Területi hatály

A jelen Szabályzat szerint elektronikusan nyújtott szolgáltatások az egész világon elérhetőek. A jelen szabályzat szerint archivált dokumentumok, érvényességi láncok, illetve a velük kapcsolatban kiállított igazolások érvényessége független attól, hogy mely földrajzi helyről kerültek az archívumba beküldésre. A Szolgáltató működését ugyanakkor a mindenkor hatályos magyar jogszabályok alapján végzi. Az elektronikus archiválás szolgáltatás jogszabályi alapját a Törvény [1] tette lehetővé.

## 1.1.3 A Szolgáltató

A jelen Szabályzatban Szolgáltatónak nevezett entitás a NetLock Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaság. Cégjegyzékszám: 01-09-563961.

Nem minősített szolgáltatóként a Felügyelet 2001. október 27-én vette nyilvántartásba a Szolgáltatót. Felügyelet regisztrációs szám: FA 6133-5/2001.

Minősített szolgáltatóként a Felügyelet 2003. március 19-én vette nyilvántartásba a Szolgáltatót. Felügyelet regisztrációs szám: MH-1372-12/2003.

Minősített archiválás szolgáltatóként a Felügyelet 2010. szeptember 15-én vette nyilvántartásba a Szolgáltatót. Felügyelet regisztrációs szám: HL/18188-4/2010

Önkéntes akkreditáció, egyéb minősítések:

- Ernst and Young AICPA/CICA WebTrust for Certification Authorities audit (2000)
- ISO 9001:2000 (2001. óta folyamatosan)
- BS 7799-2:2002 (2005)
- ISO/IEC 27001:2005 (2005. óta folyamatosan)

Tekintettel arra, hogy Magyarországon a [1] Törvény 8/B § szerinti önkéntes akkreditációs rendszer még nem működik, a Szolgáltató ilyen tanúsítással nem rendelkezik.

## 1.1.4 Szolgáltatások

A Szolgáltató Szolgáltatási Szerződés (a továbbiakban: Szerződés) keretében minősített elektronikus archiválás szolgáltatást nyújt az Előfizető részére. Az elektronikus archiválás szolgáltatást a Törvény [1] határozza meg, mely a következő 3 funkciócsoportot foglalja magában:

- Befogadással kapcsolatos funkciók:
  - az Előfizető azonosítása és jogosultságának ellenőrzése;
  - az archiválásra benyújtott információk fogadása;
  - az archiválásra benyújtott információk ellenőrzése;
  - a megőrzési időtartam kezelése, befejezése;
  - az archiválással kapcsolatosan benyújtott információk visszaigazolása;
  - a hozzáférési jogosultságok kezelése.
- Megőrzési funkciócsoport
  - az archivált elektronikus adatok rendelkezésre állásának megőrzése, mely során a Szolgáltató garانتálja, hogy az archivált adatokat az archiválás időtartamának végéig megőrzi, és az erre jogosult hozzáférők számára folyamatosan elérhetővé teszi;

- az archivált elektronikus adatok elektronikus sérthetlenségének megőrzése, mely során a Szolgáltató garantálja, hogy az archivált adatokat oly módon őrzi meg, amely megakadályozza azok módosítását és jogosulatlan megsemmisítését;
  - az archivált elektronikus adatok bizalmasságának megőrzése, mely során a Szolgáltató garantálja, hogy az archivált adatokat oly módon őrzi meg, amely megakadályozza azok jogosulatlan megismerését;
  - amennyiben értelmezett - figyelemmel, 1.1.4.1 pontban foglaltakra - az archivált elektronikus adatok titkosított formában történő megőrzése, mely során a Szolgáltató biztosítja, hogy a hozzá részben vagy egészben titkosítatlanul benyújtott archivált adatokat a befogadás után titkosítja és ily módon tárolja a bizalmasság fokozott biztosítása érdekében;
  - az archivált elektronikus adatok hitelességének és letagadhatatlanságának megőrzése, mely során a Szolgáltató garantálja, hogy az - archivált adatot a benyújtás előtt elektronikus aláírással ellátó – utólag nem vitathatja, hogy az adat tőle származik;
  - amennyiben értelmezett - figyelemmel, 1.1.4.1 pontban foglaltakra - az archivált elektronikus adatok értelmezhetőségének fenntartása, mely során a Szolgáltató az archivált adat eredeti céljának folyamatos megvalósíthatóságát garantálja (pl. szöveg esetén a megjeleníthetőséget, program esetén a futtathatóságot);
  - az archivált információk törlése az archiválásra vonatkozó Szolgáltatási Szerződés szerinti esetekben, mely során a Szolgáltató garantálja, hogy az archivált adatokkal kapcsolatos különböző tényekről a hozzáférők számára hiteles igazolásokat képes kibocsátani.
- Kibocsátás funkciócsoport
    - a hozzáférő azonosítása és jogosultságának ellenőrzése;
    - az archivált adat kiadása a jogosult hozzáférőnek (Adatkérés teljesítése);
    - igazolások kiadása az archivált adatokra (Igazolás kérésének teljesítése);
    - az archivált adat és igazolás átadása más archiválási szolgáltatónak (A szolgáltatás befejezés előkészítése).

Az archiválás-szolgáltatás igénybe vétele során az Előfizető elektronikus aláírással vagy elektronikus aláírással és időbélyeggel hitelesített dokumentumokat tölthet fel a Szolgáltató által üzemeltetett archívumba. A dokumentumok feltöltését a Szolgáltató előzetes entitásazonosításhoz kötheti. A Szolgáltató ellenőrzi a feltöltésre került dokumentum elektronikus aláírását és – amennyiben értelmezett - időbélyegét, majd beszerzi elektronikus aláírás hosszú távú érvényességéhez szükséges információkat, így különösen a tanúsítvánnyal kapcsolatos információkat, az aláírás ellenőrző adatot, a tanúsítvány aktuális állapotára, visszavonására vonatkozó információkat, valamint a tanúsítvány kibocsátójának szolgáltatói aláírás-ellenőrző adataira és annak visszavonására vonatkozó információkat. Az információk beszerzése után a Szolgáltató minősített időbélyegzőt és – választása alapján – minősített elektronikus aláírást (kivéve: 5.1 pont) helyez vagy helyezett el az érvényességi láncon.

A Szolgáltató a Felügyelet határozata szerinti, elfogadott kriptográfiai algoritmuson alapuló minősített elektronikus aláírást és minősített időbélyegyet helyez vagy helyezett el az érvényességi láncon az 5.1 pontban meghatározott esetekben.

A Szolgáltató – a bizalmasság megőrzésének biztosításával tárolja az elektronikus dokumentumokat, mely során biztosítja, hogy ahhoz a munkakörüknel fogva a rendszerek üzemeltetését biztosító munkatársakon kívül más ne férhessen hozzá, ezen munkatársak is csak szigorúan indokolt esetben.. Ezen túlmenően a Szolgáltató a megőrzés során minden esetben biztosítja az elektronikus dokumentumok utólagos módosítása lehetőségének kizárását, valamint azt, hogy ahhoz az a jogosultak folyamatosan hozzáférjenek. A Szolgáltató a megőrzés során minden esetben védi az elektronikus dokumentumokat a törlés, a megsemmisítés, a véletlen megsemmisülés és sérülés, illetve a jogosulatlan hozzáférés ellen. A megőrzés a Szerződés időtartamára szól.

A Szolgáltató a Szerződés időtartama alatt folyamatosan biztosítja az Előfizető (Hozzáférő) részére a Szolgáltató által megőrzött dokumentumok, elektronikus aláírások, illetve a hozzájuk tartozó

érvényességi láncok folyamatos elérhetőségét, azzal, hogy a dokumentumok tartalmát a Szolgáltató, vagy a vele megbízási vagy munkaviszonyban, illetve munkavégzésre irányuló egyéb jogviszonyban álló személyek kizárólag az Előfizető írásbeli engedélye alapján ismerhetik meg.

A Szolgáltató kizárólag azon változatát nyújtja [1] Törvény szerint definiált elektronikus archiválás szolgáltatásnak, amely szerint az Előfizető az elektronikus aláírással vagy elektronikus aláírással és időbélyeggel hitelesített dokumentumokat tölti fel a Szolgáltató Archivumába, és nem nyújtja azon szolgáltatást, amely szerint a Szolgáltató kizárólag az elektronikus aláírással hitelesített állomány lenyomatát kapja meg.

A Szolgáltató kizárólag elektronikus aláírások megőrzésével és hosszú távú érvényességnek biztosításával foglalkozik. Ebből következően csak olyan állományokat fogad el, amelyen elektronikus aláírás vagy elektronikus aláírás és időbélyeg szerepel, nem fogad el viszont olyan állományokat, amelyeken kizárólag időbélyegző szerepel.

A Szolgáltató – külön megállapodás esetét kivéve – kizárólag olyan elektronikus aláírások és időbélyegyek hosszú távú érvényességét biztosítja, amelyek megfelelnek az XAdES szabványnak (ETSI TS 101 903) [25].

A Szolgáltató az alábbi Archiválási rend szerint nyújtja szolgáltatását:

- Minősített Elektronikus Archiválás-Szolgáltatásra vonatkozó Archiválási Rend (OID: 1.3.6.1.4.1.3555.1.48.20110215 )

#### 1.1.4.1 Korlátozások

Előzetes megállapodás esetét kivéve a Szolgáltató a tárolt elektronikus dokumentumok értelmezhetőségét (olvashatóságát), valamint az archivált állományok titkosított formában történő tárolását nem biztosítja, illetve a szolgáltatásban nem lehet megőrzésre elhelyezni kizárólag az érvényességi láncot úgy, hogy az nem tartalmazza az elektronikus dokumentumot.

### 1.1.5 Szabványok és előírások

#### 1.1.5.1 Szolgáltatási Szabályzat

A Szabályzat az RFC 3647 [19] szabványa alapján készült. A Szabályzat tartalmi vonatkozásokban eleget tesz az elektronikus aláírásról szóló 2001. évi XXXV. törvény [1] (továbbiakban: Törvény), a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről szóló 2/2002. (IV. 26.) MeHVM irányelv [4], és az elektronikus aláírásokkal kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről szóló 3/2005. (III. 18.) IHM rendelet [5] (továbbiakban: Rendelet) előírásainak és ajánlásainak, és felhasználja az **Hiba! A hivatkozási forrás nem található.** ETSI 102 042 [13], illetve az x.509 [10] szabvány ajánlásait.

#### 1.1.5.2 A Szolgáltató által elfogadott tanúsítványok

A Szolgáltató az x509v3 [10], illetve az RFC 5280 [8] szabványban foglaltaknak megfelelő tanúsítványokat fogad el **Hiba! A hivatkozási forrás nem található.**

#### 1.1.5.3 A szolgáltatás nyújtása során használt időbélyeg

A Szolgáltatások nyújtása során használt időbélyeg megfelel az RFC3161 Time-Stamp Protocol ajánlásban [12] meghatározottaknak. A Szolgáltató kizárólag ezen ajánlásnak megfelelő időbélyeget fogad el, melynek jelenleg a Szolgáltatón kívül a Microsec Számítástechnikai Fejlesztő Kft., valamint a MÁV Informatika Kft. által kibocsátott időbélyegek felelnek meg.

#### **1.1.5.4 A Szolgáltató által elfogadott elektronikus aláírás formátumok**

A Szolgáltató alapesetben az ETSI TS 101 903 (XAdES) [25] specifikációnak megfelelő elektronikus aláírásokat bocsát ki és fogad el, egyéb esetben a Szolgáltató ettől egyedileg eltérhet.

#### **1.1.5.5 A Szolgáltató által elfogadott dokumentum formátumok**

A Szolgáltató a weboldalán közzétett, aláírásformátumban szereplő, az érvényességi lánc részét képező elektronikus adat formájára, illetve struktúrájára nézve semmilyen előírással vagy megkötéssel nem él,

#### **1.1.5.6 A Szolgáltató által végzett ellenőrzések**

A Szolgáltató a CWA 14171 [26] specifikációban foglaltak szerint ellenőrzi az elektronikus aláírásokat és időbélyegeket.

#### **1.1.5.7 Kriptográfiai algoritmusok**

A Szolgáltatás során a Szolgáltató a Felügyelet Algoritmus Határozatában [8] foglaltak szerinti algoritmusokat alkalmazza.

#### **1.1.5.8 Az Archiválás szolgáltatást nyújtó rendszer**

A Szolgáltatást nyújtó rendszer megfelel az RFC 4810 (Long-Term Archive Service Requirements) specifikációban [23], valamint a Felügyelet által kibocsátott követelményekre vonatkozó ajánlásoknak [10],[11].

#### **1.1.5.9 Alkalmazott eszközök**

A Szolgáltató archiválás szolgáltatás nyújtása során az alábbi kriptográfiai modult használja:

- ProtectServer Gold (hardver verzió: B2, firmware verzió: 2.03.00)
- ProtectServer Orange (korábbi nevén CSA 8000 Adapter), hardver verzió: G verzió, Cprov főmver verzió: 1.10

## **1.2 Dokumentum neve és azonosítása**

Jelen dokumentum:

- Teljes neve: NetLock Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaság Minősített Elektronikus Archiválás Szolgáltatás Szolgáltatási Szabályzata
- Rövid neve: Minősített Archiválás Szolgáltatási Szabályzat
- Verziószáma: a fedőlapon található egyedi azonosító (OID)

A Szabályzat hivatalos és aktuális verziója megtalálható és letölthető:

- Szolgáltató Internetes oldalairól: [www.netlock.hu](http://www.netlock.hu) (ld. még 2.1.2 pont).
- A Felügyelet internetes oldaláról: <http://www.nmhh.hu>

## **1.3 Közösség**

Az archiválási szolgáltatást igénybe vevők közössége, a Szolgáltató, illetve a Szolgáltatóval szerződéses kapcsolatban álló egyéb közreműködő szervezetek és az Érintett Felek.

### 1.3.1 Szolgáltató

Az elektronikus archiválás szolgáltatást nyújtó fél. (lásd: 1.1.3. fejezet)

### 1.3.2 Előfizető

Az elektronikus archiválás szolgáltatást igénybe vevő fél.

### 1.3.3 Érintett fél

Az elektronikus archiválás szolgáltatás során kibocsátott igazolásokat befogadó, illetve felhasználó fél.

## 1.4 Alkalmazhatóság

Jelen Szabályzat szerint nyújtott elektronikus archiválás szolgáltatás kizárólag az itt, valamint a szolgáltatási szerződésben leírtak alapján használható fel.

## 1.5 Kapcsolattartás

### 1.5.1 A Szolgáltató adatai

Név:	<b>NetLock Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaság</b>
Egység:	NetLock Kft.
Székhely:	1023 Budapest, Zsigmond tér 10.
Telefon:	(40) 22-55-22;
Fax:	(1) 345-2250
Internet cím:	www.netlock.hu
E-mail:	info@netlock.hu
Ügyfélfogadás/Nyitvatartás	Munkanapokon 9:00-17:00

### 1.5.2 Ügyfélszolgálat

Az archiválás szolgáltatással kapcsolatos kérdésekkel, problémákkal az Előfizetők a Szolgáltató Ügyfélszolgálatához fordulhatnak szóban vagy írásban. A Szolgáltató az Interneten információs szolgáltatást működtet.

A Szolgáltató Internetes információs rendszere és e-mail fiókjai minden nap 0–24 óráig fogadják a bejelentéseket. A Szolgáltató a bejelentésre legkésőbb a bejelentést követő 3. munkanapon felveszi a kapcsolatot a bejelentővel (válasz e-mail cím vagy telefonszám birtokában) és a bejelentőt a tartalmi válasz megérkezésének várható idejéről is tájékoztatja.

A Szolgáltató Ügyfélszolgálati munkatársai a 1.5.1 pontban meghatározott időpontban személyesen is fogadják az Előfizetőket, Érintett Feleket, valamint az egyéb érdekelteket.

### 1.5.3 Szabályzattal kapcsolatos kérdések

A Szolgáltató szabályzatainak karbantartását a Szabályzat Elfogadó Egység végzi. A szabályzatokkal és szerződésekkel kapcsolatos kérdésekkel és észrevételekkel a Szolgáltató ügyfélszolgálatára vagy közvetlenül a Szabályzat Elfogadó Egység kereshető meg az info@netlock.hu e-mail címen (ld. még 7.4.3.2 pont).

## 1.5.4 Szabályzat-jóváhagyási eljárás

Lásd 7.4.3.2 pont.

## 1.6 Fogalmak és rövidítések

### Fogalmak

- **Archiválás:** Elektronikusan aláírt dokumentumok hosszú távú megőrzése oly módon, mely
  - biztosítja az elektronikus dokumentum későbbi megjeleníthetőségét és ellenőrizhetőségét;
  - kizárja az utólagos módosítás, illetve a jogosulatlan hozzáférés lehetőségét;
  - védi az elektronikus dokumentumot a törléssel, megsemmisítéssel, a véletlen megsemmisüléssel és sérüléssel szemben;
  - valamint lehetővé teszi az elektronikus aláírás érvényességének ellenőrzését.
- **Archiválási szolgáltató:** a Törvényben [1] meghatározott, az elektronikus aláírással ellátott dokumentumok elektronikus archiválására vonatkozó szolgáltatást nyújtó szolgáltató.
- **Archivált elektronikus adat/dokumentum:** lásd: Elektronikus dokumentum
- **Benyújtó (adatgazda):** Az Előfizető (lásd lentebb) által meghatározott szerepkört betöltő természetes személy, aki
  - a Szolgáltatónak adatot archiválásra benyújt;
  - az általa benyújtott adat tekintetében archiválási időt változtat, teljes jogú hozzáférő, illetve további hozzáférő számára jogosultságot ad.
- **Dokumentum:** lásd: Elektronikus dokumentum
- **Elektronikus aláírás:** Elektronikusan aláírt elektronikus dokumentumhoz azonosítás céljából logikailag hozzárendelt vagy azzal elválaszthatatlanul összekapcsolt elektronikus adat.
- **Elektronikus dokumentum:** Elektronikus archiválás szolgáltatás keretében a Szolgáltató rendszere elektronikus aláírást tartalmazó dokumentumokat fogad be. Az elektronikus dokumentumok egy vagy több fájl, és rajtuk egy vagy több ETSI TS 101 903 [25] szabványnak megfelelő formátumú elektronikus aláírást tartalmazhatnak. A dokumentum tartalmazhatja továbbá a benne foglalt elektronikus aláírásokhoz tartozó érvényességi láncok egy részét, illetve a teljes érvényességi láncokat is.
- **Ellenőrzési lépések:** Az elektronikus aláírás ellenőrzésekor kötelezően végrehajtandó lépések, melyeket a Szabályzat tartalmaz.
- **Előfizető:** Az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki/amely archiválási szerződést köt a Szolgáltatóval és az archiválásra átadott adatok birtokosa.
- **Eredeti példány:** Magán- vagy jogi személy azonosító okmány eredeti aláírásokat és pecsétet, vagy elektronikus aláírást tartalmazó példánya, vagy ezek hitelesített másolata.
- **Érintett Fél:** Az elektronikus archiválás szolgáltatás során kibocsátott igazolásokat befogadó, illetve felhasználó fél.
- **Érvényességi lánc:** az elektronikus dokumentum vagy annak lenyomata, és azon egymáshoz rendelhető információk sorozata, amelyek segítségével megállapítható, hogy az elektronikus dokumentumon elhelyezett fokozott biztonságú vagy minősített elektronikus aláírás, illetve időbélyegző, valamint az azokhoz kapcsolódó tanúsítvány az aláírás és időbélyegző elhelyezésének időpontjában érvényes volt.

- **Fájl:** Olyan bitsorozat, amelyen elektronikus aláírás helyezhető el. A fájlok az elektronikus archiválás szolgáltatás során az elektronikus dokumentumban találhatóak meg. Ettől eltekintve a Szolgáltató nem foglalkozik a fájl tartalmával.
- **Felügyelet:** Nemzeti Média- és Hírközlési Hatóság és jogelődjei (a továbbiakban Felügyelet), a [1] Törvény szerinti elektronikus aláírással kapcsolatos szolgáltatásokat nyújtó szolgáltatók felügyeleti szerve.
- **Fizikailag biztosított terület:** Olyan helyiség, amely ésszerű határok mellett képes megvédeni a benne elhelyezett eszközöket az elemi károktól, illetve a szándékos illetéktelen hozzáféréstől.
- **Folyamatosan elérhető szolgáltatás:** Az év 365 napján a nap 24 órájában elérhető szolgáltatást jelent a Szolgáltató szabályzataiban meghatározott rendelkezésre állási idővel.
- **Fokozott biztonságú elektronikus aláírás:** Elektronikus aláírás, amely megfelel a következő követelményeknek:
  - alkalmas az Aláíró azonosítására és egyedülállóan hozzá köthető,
  - olyan eszközökkel hozták létre, amelyek kizárólag az aláíró befolyása alatt állnak,
  - a dokumentum tartalmához olyan módon kapcsolódik, hogy minden - az aláírás elhelyezését követően a dokumentumon tett - módosítás érzékelhető.
- **Hozzáférő:** A benyújtó (adatgazda) rendelkezése szerint archivált adatot kikér, igazolást kér, vagy egyéb meghatározott tevékenységet végez.
- **Információbiztonsági irányítási rendszer:** irányítási rendszer egy szervezet vezetésére és szabályozására, az információ bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzése szempontjából.
- **Késedelem nélküli cselekedet:** A mindenkori technikai feltételek által megengedett lehető leggyorsabb intézkedést jelenti.
- **Másolati példány:** Eredeti okmányról készült másolat.
- **Minősített elektronikus aláírás:** olyan - fokozott biztonságú - elektronikus aláírás, amelyet az aláíró biztonságos aláírás-létrehozó eszközzel hozott létre, és amelynek hitelesítése céljából minősített tanúsítványt bocsátottak ki.
- **Nyílt elektronikus dokumentum:** Olyan elektronikus dokumentum, amely közvetlenül fájlokat és azon elhelyezett aláírásokat nyíltan tartalmaz. (Az aláírt fájl titkosított is lehet.)
- **Szabályzat Elfogadó Egység:** A jelen és kapcsolódó szabályzatok kialakításáért, elfogadásáért és adminisztrációjáért felelős szolgáltatói egység.
- **Szolgáltatási Szabályzat:** A [1] Törvény 2. § (20) alapján a Szolgáltató elektronikus aláírással kapcsolatos – jelen esetben elektronikus archiválás szolgáltatási – tevékenységére vonatkozó részletes eljárási és egyéb működési szabályokat tartalmazó nyilvános dokumentum (ld. 1.1.1).
- **Szolgáltatási Szerződés:** A Szolgáltató által nyújtott szolgáltatások igénybevételéhez szükséges dokumentum, melynek elfogadása és aláírása a szolgáltatás igénybevételének előfeltétele. A Szolgáltató által nyújtott szolgáltatások igénybe vétele Szolgáltatási Szerződés megkötése helyett Belépési Nyilatkozat (lásd fentebb) elfogadásával is történhet, továbbá Szolgáltató a Belépési Nyilatkozat elfogadását kötelezővé teheti.
- **Szolgáltató:** A NetLock Kft., amely az archiválás szolgáltatást végzi.
- **Tanúsítvány:** A Szolgáltató által kibocsátott elektronikus igazolás, amely az aláírás-ellenőrző adatot a tanúsítvány alanyához kapcsolja.

## 2 Közzététel

### 2.1 A Szolgáltatói információ közzététele

#### 2.1.1 Közzétételi és tájékoztatási elvek

##### 2.1.1.1 A szabályzatban nem tárgyalt elemek

Szolgáltató nyilvános szabályzataiban csak azon eljárásait hozza nyilvánosságra, melyek ismerete a szolgáltatás biztonságát nem veszélyezteti. Szolgáltató több belső biztonsági és egyéb szabállyzattal, operatív szintű előírással rendelkezik, melyeket bizalmasan kezel (jelen Szabályzat több ilyen is megemlíti).

##### 2.1.1.2 A Szabályzat közzététele

Szolgáltató szabályzatainak a változásokkal egybeszerkesztett új verzióját, annak tervezett hatályba lépését megelőzően megküldi a Felügyelet részére. A Szolgáltató alkalmanként ezt megelőzően is tájékoztathatja a Közösséget a tervezett változtatásairól. A jelen szabállyzattal kapcsolatos közölteendőket a 7.4.3.2 pont határozza meg.

A Szolgáltató a honlapján teszi közzé, hogy mely megbízható gyökératanúsítványokra milyen feltételek szerint vállalja az érvényességi lánc felépítését. A Szolgáltató az Előfizetővel egyedi szolgáltatási szerződést köthet, a kapcsolódó árakat és díjakat ezen szerződés melléklete tartalmazhatja.

A Szolgáltató az Előfizető írásbeli értesítését az Előfizető által megadott e-mail címre küldött egyszerű, elektronikus aláírás nélküli értesítéssel is megteheti. Kivételt jelent ez alól a Szolgáltatási Szerződés felmondása, melyet – elektronikus út esetén – a Felek kizárólag elektronikusan aláírt értesítés formájában tehetnek meg.

##### 2.1.1.3 Észrevételek kezelése

A közzétett szabályzatokkal kapcsolatos észrevételeket a Szolgáltató az info@netlock.hu címen fogadja. A Szabályzat észrevételekkel módosított változatát Szolgáltató az előző pont alapján teszi ismételt közzé.

#### 2.1.2 Kikötések és feltételek közzététele

A Szolgáltató szerződéses feltételeit és szabályzatait elektronikus formában (Microsoft Word és PDF formátumokban) hozza nyilvánosságra Internetes oldalain keresztül. A dokumentumok aktuális verziója mellett megtalálhatóak azok korábban érvényben lévő változatai is.

#### 2.1.3 Rendkívüli információk közzététele

A Szolgáltató a következő eseményekről honlapján hirdetést jelentet meg:

- új szolgáltatás beindítása,
- valamely szolgáltatás tervezett beszüntetése vagy tartós (7 naptári napot meghaladó) szüneteltetése,
- tevékenységének befejezése (ld. bővebben 4.7 alfejezet),
- rendkívüli üzemeltetési helyzetről tájékoztatás.

## **2.2 A közzététel gyakorisága**

### **2.2.1 Kikötések és feltételek közzétételi gyakorisága**

Jelen Szabályzattal kapcsolatos új verziók közzététele a 2.1 és 7.4.3.2 alfejezetben ismertetett eljárásoknak megfelelően történik.

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

### **2.2.2 Rendkívüli információk közzétételi gyakorisága**

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

## **2.3 Hozzáférés ellenőrzések**

A Szolgáltató által közzétett kikötések és feltételek, rendkívüli információk, nyilvános információk. Olvasás céljából bárki elérheti ezeket az információkat, a közlő közegek sajátosságainak megfelelően.

Szolgáltató által közölt információkat kizárólag csak a Szolgáltató egészítheti ki, törölheti vagy módosíthatja. A Szolgáltató különböző védelmi mechanizmusokkal akadályozza meg az információkhoz való jogosulatlan hozzáféréseket.

## 3 Az elektronikus archiválás szolgáltatás nyújtása

### 3.1 Szolgáltatási szerződés kötése

A Szolgáltató az elektronikus archiválás szolgáltatással kapcsolatos minden szükséges és vonatkozó információt elhelyez honlapján, illetve azok a Szolgáltató Ügyfélszolgálati irodájában is megtalálhatóak.

Ennek keretében a Szolgáltató – minősített szolgáltatóként – honlapján közzétett, jelen Szolgáltatási Szabályzatában az alábbiakról tájékoztatja a szolgáltatás igénylőit:

- a) azon dokumentumformátumokról – amennyiben értelmezett -, amelyek vonatkozásában az archiválási szolgáltató vállalja az olvashatóság folyamatos fenntartását a szolgáltatási szabályzat szerint (lásd 1.1.4.1 pont);
- b) az elektronikus aláírások hosszú távú érvényesítéséhez szükséges információk köréről, valamint annak következményeiről, ha az elektronikus aláírás hosszú távú érvényesítéséhez szükséges információk nem szerezhetők be (lásd 3.2 pont);
- c) az archiválási szolgáltató személyes adatkezeléséről, így különösen a harmadik személyek számára külön törvény által biztosított hozzáférés lehetőségéről, a megkeresésekkel kapcsolatos nyilvántartás vezetéséről és a hozzáférés feltételeiről, a szerződés teljesítéséhez szükséges adatok kezeléséről, valamint - amennyiben az az igénybevevő személyes adatainak kezelésével jár - a naplózás során végzett személyes adatkezelésről (lásd 7.2 pont);
- d) amennyiben az archiválási szolgáltató az Eat. 16/M. §-ának (2) bekezdése alapján felelősségét korlátozza, úgy a felelősségkorlátozásról (lásd 7.5.1.1 pont).

A Szolgáltatás igénybe vétele, valamint a Szolgáltatási Szerződés megkötésének kezdeményezése a Szolgáltató weboldalán, az Előfizető saját Ügyfélmenüjén keresztül vagy a Szolgáltató által egyéb meghatározott módon történik. A szolgáltatás igénybe vétele során az azonosítást a Szolgáltató felhasználónév-jelszó páros használatához vagy tanúsítvány alapú autentikációhoz köti. Továbbá - a Szolgáltatóval kötött előzetes megállapodás alapján - lehetőség van arra, hogy az Előfizető nem bocsátja a Szolgáltató rendelkezésére a személyazonosító adatait és álnév használatával veszi igénybe a szolgáltatást. Szolgáltató az álnév használatához történő hozzájárulását megtagadhatja.

A Szolgáltatási Szerződés papír alapon kézzel aláírva vagy legalább fokozott biztonságú elektronikus aláírással hitelesítve elektronikus formában – a Szolgáltatóhoz történő visszaküldéssel – köthető meg. Amennyiben a Szolgáltató a Szerződést elfogadta, erről az Előfizetőnek elektronikus úton értesítést küld. Ezt követően az Előfizető megkezdheti a dokumentumok feltöltését.

A Szolgáltató a szolgáltatást határozatlan időre nyújtja, mely megszűnhet:

- a) az Előfizető tetszőleges időpontra vagy azonnal történő felmondásával: az archivált dokumentumok a meghatározott időpontban, illetve azonnal törlésre kerülnek. Ebben az esetben az előre kiegyenlített előfizetési díjak - akárcsak arányos - visszatérítésére nincs mód.
- b) az Előfizető díjfizetési kötelezettségének elmulasztásával, melynek felszólításra sem tesz eleget. Az Előfizetőhöz tartozó archivált dokumentumok az eredménytelenül eltelt határidő lejártát követően, a fizetési felszólításban megjelölt időpontban törlésre kerülnek.

### 3.2 Dokumentum feltöltése

A dokumentum Szolgáltatóhoz való eljuttatása titkosított – SSL kapcsolattal biztosított - Interneten, a Szolgáltató honlapján vagy egyéb biztonságos csatornán keresztül lehetséges.

A feltöltés az alábbi módon történhet:

- Az Előfizető titkosított SSL kapcsolatot létesít a Szolgáltatóval. A Szolgáltató az Előfizetőt azonosítja. A sikeres azonosítást követően az Előfizető a titkosított kapcsolaton keresztül töltheti fel a dokumentumokat a Szolgáltató archívumába. Az Előfizető – választása alapján – metaadatokat – pl. Dublin Core [24] szerinti metaadatok - is megadhat az egyes archiválendő elektronikus adatokkal kapcsolatban.
- A feltöltést követően a Szolgáltató ellenőrzi, hogy az aláírást, illetve időbélyeget tartalmazó dokumentum formátuma megfelel-e a Szolgáltató honlapján közzétett formátumok valamelyikének. Ezen ellenőrzés nem terjed ki az érvényességi lánc részét képező elektronikus adat struktúrájára, melynek adat későbbi értelmezhetőségéről az Előfizetőnek kell gondoskodnia.
- Amennyiben a dokumentum formátuma megfelelő, akkor megtörténik az elektronikus aláírás és – amennyiben értelmezett - időbélyeg ellenőrzése, mely során a Szolgáltató ellenőrzi, hogy az egyes aláírások az aláírt archiválendő elektronikus adathoz tartoznak-e. Amennyiben a dokumentumon és a dokumentumban szereplő állományokon is szerepel elektronikus aláírás, akkor a Szolgáltató a dokumentumon szereplő összes elektronikus aláírás hitelességét ellenőrzi. Szolgáltató kérheti, hogy az Előfizető a dokumentumban szereplő egyes aláírt állományokat külön-külön küldje be archiválásra.
- Az aláírások ellenőrzését követően a Szolgáltató megkísérli visszavezetni az aláírást valamely elfogadott gyökér tanúsítványra és vagy CRL alapján ellenőrzi a tanúsítványlánc minden elemének visszavonási állapotát is. A befogadási folyamat csak abban az esetben folytatódik, ha a dokumentumon szereplő elektronikus aláírás és időbélyeg aláírás időpontjában történő érvényessége megállapítható.

A Szolgáltató visszautasítja azon dokumentumok befogadását,

- amelyeken az elektronikus aláírás érvényessége nem állapítható meg, illetve a hosszú távú érvényesítéshez szükséges információk nem szerezhetőek be,
- továbbá azokat, amelyek elektronikus aláírást és időbélyeget, vagy elektronikus aláírást nem tartalmaznak.

A dokumentumon elhelyezett elektronikus aláírásnak megbízható szolgáltatótól származó legalább fokozott biztonságú elektronikus aláírásnak kell lennie. A Szolgáltató úgy győződik meg arról, hogy az aláírás valóban megbízható szolgáltatótól származó aláírás, illetve az időbélyeg valóban időbélyeg, hogy visszavezeti egy elfogadott hitelesítés- vagy időbélyegzés-szolgáltató megbízható gyökértanúsítványára. Előfordulhat, hogy egy hitelesítés-szolgáltató olyan teszt tanúsítványt bocsát ki, amely saját megbízható gyökértanúsítványok alapján ellenőrizhető. Az ilyen tanúsítványokat a Szolgáltató nem tudja elkülöníteni a valódi, fokozott biztonságú elektronikus aláírás ellenőrzésére alkalmas tanúsítványoktól, és az ebből adódó károkért nem vállal felelősséget. A Szolgáltató az elektronikus aláírás érvényességének megállapításához szükséges összes információt (tanúsítványok, a végtanúsítványokra vonatkozó visszavonási információ), illetőleg az elektronikus aláírás adott időbeni létezését megbízható módon jelző adatot (időbélyeg) a befogadástól számított legkésőbb 3 napon belül beszerzi. Amennyiben létezik megbízható információ azon időpontról, amikor az elektronikus aláírás már létezett, akkor a Szolgáltató ezt veszi az ellenőrzés alapjául.

A Szolgáltató az aláírás ellenőrzéséhez elektronikus aláírás termék tanúsító szervezet által tanúsítottolyan eszközt használ, mely minősítése alapján minősített aláírás létrehozó alkalmazás. A Szolgáltató az aláírásokat a CWA 14171:2004 [26] szerint ellenőrzi és az ETSI TS 101 903 [25] szerinti formátumot hoz létre.

- A Szolgáltató felépíti a dokumentumon szereplő elektronikus aláíráshoz tartozó érvényességi láncokat és minősített aláírást, illetve időbélyeget helyez el rajtuk.

- A Szolgáltató a szükséges visszavonási információkat OCSP szolgáltatás vagy CRL segítségével gyűjti össze. Amennyiben a tanúsítványláncban szereplő minden OCSP szolgáltatásra vonatkozó kivárási idő 0, akkor a visszavonási információk rövid időn belül előállnak. Amennyiben valamely kivárási idő nem 0, akkor a Szolgáltató a szükséges ellenőrzéseket a kivárási idő elteltével végzi el.
- Az archiválandó dokumentumokat a Szolgáltató a bizalmasság biztosításával tárolja. A dokumentumokat a Szolgáltató a 3.6 fejezetben leírt biztonságos módon semmisítheti meg, melyet követően a dokumentum visszaállítására semmilyen módon nem jogosult.

### 3.2.1 A visszaigazolás

A Szolgáltató haladéktalanul, de legkésőbb 3 munkanapon belül visszaigazolást küld az Előfizetőnek arról, hogy a dokumentumot sikeresen befogadta. Ha a folyamat valahol megszakad, akkor a Szolgáltató - lehetőség szerint az ok megjelölésével - értesíti az Előfizetőt. A Szolgáltató a visszaigazolásokat és az egyéb értesítéseket elektronikus levélben vagy egyéb, az Előfizetővel egyeztetett módon juttatja el.

A befogadási folyamat során a Szolgáltató által küldött visszaigazolás az alábbiakat tartalmazza:

- a formai ellenőrzés sikeressége/sikertelensége (formai befogadás);
- a formai ellenőrzés által meghatározott formátum (dokumentum/lenyomat/bitfolyam);
- a kezdeti ellenőrzés sikeressége/sikertelensége (siker esetén előzetes befogadás);
- az érvényességi adat begyűjtés és az utólagos ellenőrzés sikeressége/sikertelensége, valamint sikeresség esetén a dokumentumom időbélyegző elhelyezése (végleges befogadás);

A végleges befogadást visszaigazoló üzenet legalább az alábbiakat tartalmazza:

- egy véletlenszerűen generált, egyedi azonosítót, amellyel a benyújtó a jövőben az adott, véglegesen befogadott adatra hivatkozhat;
- a benyújtó azonosítóját;
- az archiválás időtartamát;
- az archiválási rend azonosítóját;
- az adatra vállalt kiegészítő szolgáltatást (ha van);
- annak egyértelmű jelzését, hogy a Szolgáltató a [1] Törvény hatálya alatt álló elektronikus archiválás szolgáltatást nyújt.

A Szolgáltató a visszaigazolásokat legalább fokozott biztonságú elektronikus aláírással és minősített időbélyegzővel látja el. Az Előfizetőnek meg kell győződnie arról, hogy a visszaigazolás valóban az általa feltöltött dokumentumra vonatkozik és a visszaigazoláson szereplő elektronikus aláírás érvényes voltáról. A visszaigazolás, mint elektronikus dokumentum hitelességének megőrzése során az Előfizetőnek a elektronikus archiválásra vonatkozó jogszabályok alapján kell eljárnia.

Ha az Előfizető végleges befogadást tartalmazó értesítést nem kap, akkor azt úgy kell tekinteni, hogy a dokumentum nem került befogadásra. A Szolgáltató kizárólag a végleges befogadást igazoló dokumentum elküldése esetén felel a dokumentum megőrzéséért és a benne szereplő elektronikus aláírások hitelességének hosszú távú biztosításáért.

## 3.3 Érvényességi lánc elérhetőségének biztosítása

Az Előfizető kizárólag biztonságos csatornán keresztül férhet hozzá a Szolgáltató archívumában lévő dokumentumhoz, érvényességi láncokhoz. Az Interneten keresztül történő hozzáférés folyamata:

- A Előfizető titkosított – jellemzően SSL kapcsolatot – létesít a Szolgáltatóval. A Szolgáltató az Előfizetőt azonosítja. Az azonosítás felhasználó név-jelszó páros vagy autentikációs tanúsítvány alapján történik.
- A Szolgáltató megállapítja, hogy az Előfizető mely archivált dokumentumhoz kíván hozzáférni, valamint azt, hogy jogosult-e rá. Ekkor lehetősége van a dokumentumhoz kapcsolódó metaadatok alapján keresni a fájlokra.
- Ha az Előfizető jogosult letölteni a fájlt, akkor a Szolgáltató biztonságos csatornán keresztül elküldi azt (azokat) az Előfizetőnek.

A Szolgáltató megtagadja a dokumentum letöltését, amennyiben azzal kapcsolatban elbírált és hatályosult törlési kérelmet kapott.

A Szolgáltatóval való előzetes egyeztetés esetén lehetőség van arra, hogy az Előfizető ne csak hálózaton keresztül, hanem valamely adathordozón (pl. optikai lemez) is átveheti az archívumban szereplő dokumentumokat, érvényességi láncokat. A Szolgáltató ebben az esetben az archívumban szereplő dokumentumokhoz való hozzáférési jogosultságokat egyéb módon ellenőrizheti.

### 3.4 Az igazolás

A Szolgáltató archívumában őrzött elektronikus dokumentumokkal kapcsolatban a Szolgáltató az Előfizető vagy a Hozzáférő kérésére igazolást állít ki. Az igazolás – a Felügyelet ajánlásának [11] megfelelően – az alábbi tényekre vonatkozóan tartalmazhat információt:

- Igazolja, hogy a megőrzésben lévő elektronikus adaton elhelyezett fokozott biztonságú vagy minősített elektronikus aláírás vagy időbélyegző, illetve az azokhoz kapcsolódó tanúsítvány az időbélyegzés időpontjában érvényes (a letagadhatatlanság igazolása).
- Igazolja, hogy megőrzésben lévő, az érvényességi lánc részét képező elektronikus adat tartalma megegyezik a hozzáférő által bemutatott elektronikus adattal (a sértetlenség igazolása)
- Igazolja, hogy a megőrzésben lévő, az érvényességi lánc részét képező elektronikus adaton, amelynek tartalma megegyezik a Hozzáférő által bemutatott elektronikus adattal, meghatározott személy érvényes elektronikus aláírást vagy meghatározott időpontban időbélyegzőt helyezett el (az eredet hitelességének igazolása).

A Szolgáltató által kibocsátott igazolás az alábbiakat tartalmazza:

- A letagadhatatlanság igazolása esetén
  - az igazolás típusa (letagadhatatlanság),
  - az archivált elektronikus adat egyedi azonosítója,
  - az archivált elektronikus adat lenyomata,
  - amennyiben az eredeti adathoz több elektronikus aláírás is tartozik, az igazolás által érintett aláíró azonosítója,
  - az igazolás eredménye (érvényes / érvénytelen)
  - az igazolás kiállításának időpontja.
- A sértetlenség igazolása esetén
  - az igazolás típusa (sértetlenség),
  - az archivált elektronikus adat egyedi azonosítója,
  - az archivált elektronikus adat lenyomata,
  - az igazolás eredménye (érvényes / érvénytelen)
  - az igazolás kiállításának időpontja.

- Az eredet hitelességének igazolása esetén
  - az igazolás típusa (eredet hitelesség),
  - az archivált elektronikus adat egyedi azonosítója,
  - az archivált elektronikus adat lenyomata,
  - az igazolás által érintett aláíró azonosítója,
  - az igazolás eredménye (érvényes / érvénytelen)
  - az igazolás kiállításának időpontja.

A Szolgáltató az igazolást – előzetes megállapodás esetét kivéve - minősített elektronikus aláírással és időbélyegzővel hitelesített elektronikus dokumentum formájában bocsátja ki. Az igazolás egyszerre több dokumentumra is vonatkozhat. A Szolgáltató az igazolás kiadás kérés teljesítését további entitásazonosításhoz kötheti.

Az igazolás kiállítása során a Szolgáltató az archivált elektronikus dokumentumok tartalmát nem ismeri meg, az igazolás kiállítása során kizárólag az archivált elektronikus adatok lenyomatával dolgozik.

Az Előfizető az igazolás kibocsátását elektronikus úton, alapesetben Ügyfélmenüjén keresztül igényelheti. Az Előfizető meghatalmazottja számára a Szolgáltató kizárólag abban az esetben bocsát ki igazolást, ha a meghatalmazást az Előfizető teljes bizonyítóerejű magánokiratba foglalta vagy az Előfizető saját Ügyfélmenüjében történt meg a hozzárendelés. Az Előfizető által történő további jogosultság hozzárendeléseket a Szolgáltató autentikációhoz, jellemzően felhasználó név-jelszó páros használatához, vagy tanúsítvány alapú autentikációhoz köti.

Az igazolás kiállítása elektronikus dokumentum formájában, az ETSI 101 903 [25]specifikációban meghatározott elektronikus aláírás formában történik (XAdES).

Amennyiben az archivált elektronikus dokumentummal kapcsolatban a Szolgáltató az igazolás kérését megelőzően törlési kérést kapott és a kérés jóváhagyásra került, a Szolgáltató megtagadja az igazolás kibocsátását.

### **3.5 Dokumentum megjelenítése**

Az Előfizető (Hozzáférő) a Szolgáltató archívumában tárolt dokumentumait Ügyfélmenüjén keresztül tekintheti meg, illetve töltheti le.

### **3.6 Dokumentum és érvényességi lánc törlése**

A Szolgáltató az Előfizető kérésére visszaállíthatatlan módon törli az archivált elektronikus adatot és az archivált elektronikus adathoz tartozó érvényességi láncot. Ez a törlés a tárolt elektronikus dokumentum fizikai megsemmisítését, illetve olyan módon történő felülírását jelenti, hogy az elektronikus dokumentumot nem, vagy csak irreálisan magas anyagi ráfordítás esetén lehet visszaállítani. A törlést a Szolgáltató a teljes rendszeren végrehajtja, mely során az archivált elektronikus dokumentum minden mentett állományát megsemmisíti.

A törlési kérelmet az Előfizető vagy a Hozzáférő Ügyfélmenüjén keresztül teheti meg. A Szolgáltató a törlési kérelmek benyújtását megelőzően a Szolgáltató az Előfizetőt (Hozzáférőt) azonosítja. Az azonosítás jellemzően felhasználó név-jelszó vagy tanúsítvány alapú autentikációval történik. Az Előfizetővel való előzetes megállapodás alapján a Szolgáltató egyéb módon is fogadhat törlési kérelmeket.

A törlést a Szolgáltató a kérést követő 30 napon belül bírálja el és hajtja végre. Törlési kérelem oly módon is benyújtható, hogy azt a Szolgáltató ne azonnal, hanem egy meghatározott időpontban hajtsa végre.

A törlésről a Szolgáltató egy elektronikus aláírással és időbélyegzővel hitelesített nyilatkozatot juttat el a törlést kérőnek. A visszaigazolás tartalmazza a törölni kívánt (törölt) elektronikus dokumentum egyedi azonosítóját, a törlést kérő azonosítóját, a törlés tényét valamint a törlés időpontját.

### **3.7 A szolgáltatási szerződés megszűnése**

A Szolgáltatási Szerződés megszűnése esetén a Szolgáltató a 3.6 pontban meghatározott módon törli az Előfizető dokumentumait a rendszerből.

## 4 Fizikai, eljárásbeli és személyzeti biztonsági óvintézkedések

A Szolgáltató fizikai, eljárásbeli, személyzeti óvintézkedéseket, valamint adminisztratív és irányítási eljárásokat alkalmaz a szabványoknak megfelelően.

A Szolgáltató az archivált elektronikus dokumentumokat két, egymástól fizikailag elkülönített helyen, az elsődleges rendszeren és a háttérrendszeren tárolja. A háttérrendszer képes átvenni az elsődleges rendszer kritikus funkcióit, az elsődleges rendszer kiesése esetén.

A kockázatok csökkentése és az üzembiztonság növelése érdekében Szolgáltató az általa biztosított szolgáltatásokhoz szükséges hardver, szoftver, illetve egyéb eszközeit két, fizikailag egymástól elkülönült helyszínen, egy elsődleges és egy másodlagos helyszínen (second site) tárolja. A két helyszín biztonsági előírására vonatkozó szabályok egyenszilárdságúak, az esetleges eltérések a megfelelő pontoknál feltüntetésre kerültek.

A biztonsági szabályokra vonatkozó rendelkezéseket a nem nyilvános Biztonsági Szabályzat tartalmazza.

A folyamatos, magas színvonalú biztonságos szolgáltatás fenntartására a Szolgáltató ISO 27001 (korábban BS 7799-2:2002 elnevezésű) szabványnak megfelelő információbiztonsági irányítási rendszert alkalmaz, amelyet független külső és belső auditorok vizsgálnak folyamatosan. Továbbá ISO 9001 szabvány szerinti minőségirányítási rendszert üzemeltet.

### 4.1 Fizikai óvintézkedések

A fizikai óvintézkedések célja a Szolgáltató bizalmas információira és fizikai körleteire irányuló jogosulatlan hozzáférés, károkozás és illetéktelen behatolás megakadályozása.

A kritikus és érzékeny információt feldolgozó szolgáltatásokat biztonságos helyszíneken valósítják meg a Szolgáltató rendszerében. A biztosított védelem arányban áll a Szolgáltató által végzett kockázatelemzésben megállapított kockázatokkal.

#### 4.1.1 A telephely elhelyezése és szerkezeti felépítése

A Szolgáltató védett számítógép termében valósítja meg az elektronikus archiválás szolgáltatást. A számítógéptermet speciálisan a minősített szolgáltatáshoz kapcsolódó feladatokra és a célra tervezték, valamint alakították ki, és tervezésénél sok különböző védelmi szempont (a telephely elhelyezése és szerkezeti felépítése, a fizikai hozzáférés, beléptetés ellenőrzése és felügyelete, áramellátás, légkondicionálás, beázás és elárasztódás elleni védekezés, tűzmelegelőzés és tűzvédelem, adathordozók tárolása, stb.) egységes érvényesítésére került sor. Illetéktelen személyek 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 Szolgáltató mind az elsődleges, mind a másodlagos telephelyét úgy alakította ki, hogy egy, a rendszerhez esetleg fizikai hozzáférő (támadó) ne okozhasson jelentős kárt, ne sérthesse meg az archivált állományok és az elektronikus dokumentumok hitelességét, sérthetlenségét.

#### 4.1.2 Fizikai hozzáférés

A Szolgáltató védett számítógép terme pontos paramétereit, illetve a belépni jogosultak listáját a mindenkor belső operációs dokumentumok tartalmazzák. Az ott dolgozó bizalmi munkakört betöltő munkatársakon kívül más személyek (pl. karbantartók, takarítók) csak külön felhatalmazással és kísérettel léphetnek be. A belépések biometrikus azonosításra épülő beléptető rendszeren (kivéve másodlagos helyszínen) keresztül történnek a belépések naplózásával. A helyiség kétszerezett

(redundáns) klíma-, automata tűzoltó, továbbá illetéktelen behatolást jelző (riasztó) berendezéssel van ellátva. Az eszközök többszörösen túlbiztosított elektromos energiaellátással rendelkeznek. A biztonsági körletet beléptető zsilipét 24 órás videó kamerás megfigyelő rendszer is védi.

A másodlagos helyszín beléptetési rendszere biometrikus beléptető automatizmussal nem rendelkezik, de az egyenszilárdság megőrzése érdekében, a másodlagos helyszín biztonságát állandó előerős védelem biztosítja.

A biztonsági óvintézkedésekre vonatkozó további részletes rendelkezéseket a Szolgáltató Minősített Szolgáltatási Szabályzata[14] tartalmazza. A Minősített Szolgáltatási Szabályzat aktuális verziója a Szolgáltató honlapján található meg.

### 4.1.3 Fizikailag elkülönítetten őrzött mentési példányok

A szolgáltatásra nagy hatással lévő úgynevezett kritikus adatok, valamint az archivált elektronikus dokumentumok a háttérrendszer biztonsági zónájában kerülnek tárolásra.

## 4.2 Eljárásbeli óvintézkedések

Az eljárásbeli óvintézkedések célja, hogy a bizalmi munkakörök kijelölésével és elkülönítésével, az egyes munkakörök felelősségének dokumentálásával, az egyes feladatokhoz szükséges személyzeti létszámok, valamint az egyes munkakörökben elvárt azonosítás és hitelesítés meghatározásával kiegészítse, egyúttal fokozza a fizikai és személyzetre vonatkozó óvintézkedések hatásosságát.

### 4.2.1 Bizalmi munkakörök

A Szolgáltató biztonság politikája – figyelemmel a Felügyelet tájékoztatójában [12] foglaltakra – a következő bizalmi munkaköröket határozza meg az alábbi felelősségkörökkel:

Megnevezés	Rövid leírás	Archíváló rendszerbeli szerepkör
Biztonsági Tisztviselő	A szolgáltatás biztonságáért általánosan felelős személy.	biztonsági tisztviselő
Rendszeradminisztrátor	Az informatikai rendszer telepítését, konfigurálását, karbantartását végző személy. Felel a rábízott rendszer megfelelő és folyamatos működéséért, valamint a technológia fejlődésének nyomon követéséért, biztonsági rések felderítéséért és megoldási javaslatok kidolgozásáért.	Rendszeradminisztrátor (SYSTEM_ADMIN)
Rendszerüzemeltető	Az informatikai rendszer folyamatos üzemeltetését, mentését és helyreállítását végző személy.	
	USER_ADMIN összes jogosultsága, díjak, előfizetések beállítása	
Független rendszervizsgáló	A Szolgáltató naplózott, illetve archivált adatállományát (ide nem értve a szolgáltatás nyújtása keretében archiválásra átvett adatokat) vizsgáló, a Szolgáltató által a szabályszerű működés érdekében megvalósított kontroll intézkedések betartásának ellenőrzéséért, a meglévő eljárások folyamatos vizsgálatáért és monitorozásáért felelős személy	Független rendszervizsgáló (AUDITOR)
	Díjak, előfizetési csomagok, felhasználói jogosultságok, archivált állományok adatainak lekérdezése, események megtekintése	
-	Hozzáférő és Benyújtó jogosultságok állítása, események megtekintése, keresés az archívumban	Felhasználó adminisztrátor (USER_ADMIN)
-	SYSTEM_ADMIN összes jogosultsága, SYSTEM_ADMIN szerepkör kiosztása, archivált állományok letöltése	Root (ROOT)

A bizalmi munkakörök között a biztonságos feladatvégzést akadályozó, illetve a jogszabályokban tiltott személyi átfedések nincsenek. Valamennyi fent megnevezett bizalmi munkakört részletes munkaköri leírások dokumentálják. A Szolgáltatónál a bizalmi munkakört betöltő személyek szakirányú felsőfokú

végzettséggel és gyakorlattal rendelkeznek. A bizalmi munkakörökbe az ügyvezető nevezi ki a Szolgáltató munkatársait, a biztonsági alapellenőrzés sikeres befejezése után.

A bizalmi munkakörökre vonatkozó részletes szabályokat a Szolgáltató Minősített Szolgáltatási Szabályzata [14] tartalmazza. A Minősített Szolgáltatási Szabályzat aktuális verziója a Szolgáltató honlapján megtalálható.

#### **4.2.2 Az egyes feladatokhoz szükséges személyzeti létszámok**

A Szolgáltató minden munkatársa csak a saját munkakörének megfelelő funkciókat láthatja el. Legalább két bizalmi munkakört betöltő személy együttes jelenléte a titkosított elektronikus dokumentumok dekódolásához szükséges.

#### **4.2.3 Az egyes munkakörökben elvárt azonosítás és hitelesítés**

A Szolgáltató valamennyi, bizalmi munkakört betöltő munkatársának a zárt körletbe való belépéskor az azonosítását és hitelesítését biometrikus azonosító rendszer végzi (kivéve másodlagos helyszínen, ahol biometrikus azonosítás nincs, bővebben lásd. a 4.1.2 pontban foglaltakat), amely a rendszerekhez való hozzáférésnél egyéb, rendszerenként különböző védelemmel egészül ki. Sikeres hitelesítés előtt a zárt körletbe való bejutás, illetve rendszerhozzáférés nem lehetséges, így egyetlen biztonság kritikus tevékenység sem végezhető.

#### **4.2.4 Változáskezelés**

A Szolgáltató a szolgáltatási folyamatokban és az azt kiszolgáló informatikai szolgáltatásokban bekövetkező módosítások, változások biztonságos végrehajtása érdekében szabályozott és dokumentált változáskezelési eljárást alkalmaz.

### **4.3 Személyzetre vonatkozó óvintézkedések**

A Személyzetre vonatkozó óvintézkedések részletes szabályait a Szolgáltató Minősített Szolgáltatási Szabályzata [14] tartalmazza. A Minősített Szolgáltatási Szabályzat aktuális verziója a Szolgáltató honlapján megtalálható.

### **4.4 A biztonsági naplózás folyamatai**

Szolgáltató archiválási rendszere a jogszabályi követelményeknek, illetve Felügyelet ajánlásának [10] megfelelő, széleskörű naplózási tevékenységet folytat az adatok megőrzése (archiválás) érdekében.

Az erre vonatkozó részletes szabályokat a Szolgáltató Minősített Szolgáltatási Szabályzata [14] tartalmazza, azzal hogy a Minősített Szolgáltatási Szabályzatban taglalt eseménytípus csoportokon túlmenően az alábbi archiválással kapcsolatos események is naplózásra kerülnek:

Befogadással kapcsolatos események naplózása:

- az archiválásra benyújtott információk fogadása;
- az archiválásra benyújtott információk ellenőrzése;
- megőrzési időtartam módosítása;
- archiválásra benyújtott információk visszaigazolása;
- hozzáférők hozzáférési jogosultságának módosítása.

Megőrzéssel kapcsolatos események naplózása:

- archivált elektronikus adatok rendelkezésre állásának megőrzésével kapcsolatos biztonsági események;

- archivált elektronikus adatok sértetlenésének megőrzésével kapcsolatos biztonsági események;
- archivált elektronikus adatok hitelességének és letagadhatatlanságának megőrzésével kapcsolatos biztonsági események;
- archivált információk törlésével kapcsolatos biztonsági események.

Kibocsátással kapcsolatos események naplózása:

- adat kérések teljesítése;
- igazolás kérések teljesítése;
- szolgáltató-váltás előkészítése.

## 4.5 Egyéb rendelkezések

Az adatok archiválására és a biztonsági rendelkezésekre vonatkozó részletes szabályokat a Szolgáltató Minősített Szolgáltatási Szabályzata [14] tartalmazza. A Minősített Szolgáltatási Szabályzat aktuális verziója a Szolgáltató honlapján megtalálható.

## 4.6 Helyreállítás kompromittálódás és katasztrófa esetén

### 4.6.1 Incidens- és kompromittálódás-kezelési eljárások

A Szolgáltató a folyamatos működés biztosítása, illetve a vészhelyzetek minél gyorsabb elhárítása érdekében Üzleti Folytonossági Tervvel (ÜFT) rendelkezik, amely tartalmaz katasztrófa helyreállítási tervet is. Az ÜFT olyan eljárásokat tartalmaz, amelyek leírják a megbízható üzemmenet mielőbbi helyreállításának leggyorsabb módját. A Szolgáltató ellenőrzések végrehajtásával rendszeresen teszteli a biztonsági előírások hiánytalan technikai és személyi végrehajtását.

Az erre vonatkozó további részletes rendelkezéseket a Szolgáltató Minősített Szolgáltatási Szabályzata [14], illetve az ÜFT tartalmazza.

Az incidens körülményeinek és hatásainak felmérését követően a Szolgáltató felveszi a kapcsolatot a katasztrófában érintett állományokat feltöltő Előfizetőkkel, és tájékoztatja őket az eseményről.

### 4.6.2 Sérült számítási erőforrások, szoftverek és/vagy adatok

A Szolgáltató úgy alakította ki az elektronikus dokumentumok és az érvényességi lánc elérhetőségét biztosító archiváló rendszerét, hogy a rendszer bármely eszköz kiesése esetén képes zavartalanul folytatni a működését. Amennyiben a Szolgáltatónak egyszerre több eszköze hibásodik meg, és ezáltal több eszköz egyszerre esik ki, a Szolgáltató 3 órán belül képes háttérrendszerének beindítására, amely képes biztosítani a fenti szolgáltatások folyamatos elérhetőségét.

### 4.6.3 Biztonsági képesség egy természeti vagy más egyéb katasztrófát követően

A Szolgáltató elsődleges működési helyszínén kívül másodlagos működési helyszínnel is rendelkezik. Természeti vagy más katasztrófákat követően, illetve a Szolgáltató rendszereinek olyan mértékű meghibásodása esetén, mely során a Szolgáltató feladatát az elsődleges rendszer nem teljes körűen képes ellátni, a Szolgáltató a másodlagos helyszínen is képes szolgáltatásainak beindítására.

Ilyen esetben a Szolgáltató 3 órán belül vállalja az érvényességi láncok elérhetővé tételével kapcsolatos szolgáltatások ismételt elindítását.

## 4.7 A Szolgáltató leállítása

### 4.7.1 Szolgáltatás megszüntetése

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

- a) A tevékenység befejezését legalább 60 nappal megelőzően értesíti az Ügyfeleket, a Felügyeletet, megjelölve azt a - vele azonos besorolású – szervezetet, amely legkésőbb a tevékenység befejezésekor átveszi a tárolt elektronikus dokumentumokat és a visszafejtésükre szolgáló magánkulcsokat.
- b) A szolgáltatás megszünése előtt 30 nappal értesítést tesz közzé Internetes oldalain e-mail címmel rendelkező ügyfelei számára a szolgáltatás befejezéséről elektronikus levélben értesítőt küld.
- c) A Szolgáltató a szolgáltatás befejezésekor az informatikai rendszerében foglalt adatokról, érvényességi láncokról minősített elektronikus aláírással és minősített szolgáltató által kibocsátott időbélyegzővel ellátott teljes körű mentést hajt végre. A mentett adatállományokat a Szolgáltató védi jogosulatlan módosítástól és biztosítja a jogosulatlan hozzáférés kizárását, valamint az adatoknak megőrzési időn belüli, jogosultak számára való hozzáférhetőségét és – amennyiben értelmezett - értelmezhetőségét.
- d) A szolgáltatás leállítására vonatkozó bejelentést követően a Szolgáltató nem fogad be további elektronikus dokumentumokat. A megszünése időpontjával egyidejűleg a Szolgáltató többi szolgáltatását is leállítja.
- e) A szolgáltatás leállítását követően a Szolgáltató az Előfizetővel egyeztetett módon átadja az archivált fájlokat, aláírásokat, érvényességi láncokat, majd archívumából visszaállíthatatlan módon törli azokat.

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

A Szolgáltató rendelkezik a leállási követelmények teljesítésével kapcsolatos költségek fedezetével. A leálláshoz kapcsolódó kötelezettségek teljesítését 25.000.000 Ft-os bankgarancia szavatolja.

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

## 5 Műszaki óvintézkedések

### 5.1 Rendszeres felülhitelesítés

A Szolgáltató az archivált elektronikus dokumentumokon (beleértve a dokumentumot, aláírást, valamint az időbélyeget) minősített elektronikus aláírást és minősített időbélyeget helyez el.

- a Felügyelet által kiadott határozatban meghatározott időben,
- ha valamely kriptográfiai algoritmusban megrendül a bizalom.

A minősített elektronikus aláírást és minősített időbélyeget a Szolgáltató a Felügyelet határozata [8] szerinti biztonságos kriptográfiai algoritmussal hozza létre.

### 5.2 A technológia folyamatos figyelése

A Szolgáltató folyamatosan figyelemmel kíséri az elektronikus aláírással és titkosítással kapcsolatos technológia fejlődését, és ha a nemzetközi standardok, illetve a Felügyelet határozata alapján egy algoritmus már elavul, akkor elvégzi az 5.1 5.1 pontban meghatározott műveleteket.

### 5.3 Hitelesítés- és időbélyegző szolgáltató elfogadása

A Szolgáltató a honlapján teszi közzé, hogy milyen hitelesítés-szolgáltatók tanúsítványait és mely időbélyegző-szolgáltatók időbélyegeit fogadja el. Szolgáltató szintén a honlapján teszi közzé az elfogadás feltételeit is.

Az elfogadott szolgáltatók listája az alábbi címen érhető el: [www.netlock.hu/archivalas](http://www.netlock.hu/archivalas)

A Szolgáltató az egyes hitelesítés-szolgáltatók tanúsítványainak, valamint az egyes időbélyeg-szolgáltatók által kibocsátott időbélyegek elfogadásáról, illetve annak változásáról belső szabályzatában meghatározott eljárásrend alapján határoz.

### 5.4 Az elektronikus dokumentumok értelmezhetőségének (olvashatóságának) fenntartása

Előzetes megállapodás esetét kivéve a Szolgáltató a tárolt elektronikus dokumentumok értelmezhetőségét (olvashatóságát) alapesetben nem biztosítja. (lásd 1.1.4.1)

### 5.5 Az elektronikus archiválási szolgáltatás egyes elemeinek rendelkezésre állása

Az alábbiakban felsorolt elemekre a Szolgáltató éves szinten 99% rendelkezésre állást biztosít. Ezekben az esetekben az eseti szolgáltatás-kiesés nem haladhatja meg a 3 napot.

- A Szolgáltató által megőrzött (archivált) elektronikus dokumentumok és érvényességi láncok letöltése;
- Keresés az archivált dokumentumokban;
- Törlési kérelmek elektronikus fogadása;
- Időzített törlési kérelmek fogadása, illetve időzített törlési kérelmek módosítása;
- Információkérés

A dokumentumok feltöltésének szüneteltetésére a Szolgáltató a [1] Törvényben meghatározott módon jogosult. A igazolások kibocsátását a Szolgáltató folyamatosan biztosítja. A igazolások kibocsátására vonatkozó szolgáltatás-kiesés nem haladhatja meg a 3 napot.

## 5.6 Biztonsági garanciák

A Szolgáltató szolgáltatásai nyújtása során megbízható termékekből álló rendszert használ szolgáltatásai nyújtásához. Amennyiben a Szolgáltató harmadik féltől bizalmi szolgáltatást vesz igénybe, ellenőrzi, hogy a harmadik fél minden szükséges kötelezettségnek eleget tett-e.

A Szolgáltató a telepítés, illetve az üzemeltetés során esetlegesen felmerülő hibák elkerülése érdekében a rendszer teljeskörű telepítési, illetve üzemeltetési dokumentációval rendelkezik.

A Szolgáltató az archivált elektronikus dokumentumokat fizikailag biztonságos környezetben, 4. fejezetben meghatározott fizikai és eljárásbeli óvintézkedések mellett tárolja, a biztonságot a Szolgáltató belső szabályzataiban foglaltak betartása, valamint a belső és külső szakértői auditok garantálják.

Az archiválás-szolgáltatás biztosítása során a Szolgáltató biztosítja, hogy az archiválásra átvett dokumentumokat a Szolgáltató saját munkatársai se olvashassák el. A Szolgáltató a dokumentumokat harmadik fél rendelkezésére kizárólag akkor bocsátja, ha arra az Előfizető felhatalmazza, vagy annak a Szolgáltató jogszabályi kötelezettség miatt tesz eleget.

A tárolt dokumentumok integritását a fizikai biztonsági intézkedések, valamint a Szolgáltató belső szabályzataiban foglaltak biztosítják. Az archiválásra átvett dokumentumokat a megőrzés és a rendelkezésre állás biztosítása érdekében a Szolgáltató két, fizikailag elkülönült helyen, tükrözött módon tárolja, míg az archiváló rendszer adatbázisa rendszeresen mentésre kerül.

Az archivált dokumentumok megsemmisítésére vonatkozóan a 3.6 pontban foglaltak előírásai az irányadóak.

## 5.7 Számítógép-biztonsági óvintézkedések

A Szolgáltató a következő számítógép-biztonsági óvintézkedéseket alkalmazza:

- megköveteli, hogy az informatikai rendszerek és alkatrészek szállítói olyan dokumentációkat biztosítsanak, melyek érthetővé teszik a megbízható rendszerek helyes és biztonságos működtetését, a rendszerhibák kockázatának minimalizálását biztosító telepítését, a vírusokkal és kártékony szoftverekkel szembeni védelmet a rendszerek és az általuk feldolgozott információk sértetlenségének fenntartása érdekében,
- megköveteli a szolgáltatási rendszerek szállítóitól a következők átadását: telepítési útmutató, rendszeradminisztrációs útmutató, üzemeltetési útmutató,
- az egyes rendszerek kezelése során hozzáférési szinteket, hozzáférési jelszavakat alkalmaz,
- az audit napló állományokat napi, heti és havi, valamint éves gyakorisággal ellenőrzi.

Az ide vonatkozó részletes rendelkezéseket a 4.6, 4.4 és a 4.1 alfejezet, valamint a Biztonsági Szabályzat tartalmazza.

### 5.7.1 Speciális számítógép-biztonsági műszaki követelmények

A Szolgáltató speciális számítógép-biztonsági műszaki követelményekre vonatkozó előírásait a Szolgáltató Minősített Szolgáltatási Szabályzata [14] tartalmazza, melynek mindenkor hatályos verziója a Szolgáltató honlapján elérhető.

## 5.7.2 Informatikai biztonsági osztályozás

Az ide vonatkozó rendelkezéseket a Szolgáltató belső használatú Kockázatkezelési Szabályzata tartalmazza.

## 5.8 Életciklusra vonatkozó műszaki óvintézkedések

A Szolgáltató által alkalmazott, Életciklusra vonatkozó műszaki óvintézkedéseket a Szolgáltató Minősített Szolgáltatási Szabályzata [14] tartalmazza, melynek mindenkor hatályos verziója a Szolgáltató honlapján elérhető.

## 5.9 Hálózatbiztonsági óvintézkedések

A Szolgáltató saját hálózatát a nyílt hálózatokról tűzfal szerverekkel választja le. Az ide vonatkozó részletes rendelkezéseket a Biztonsági Szabályzat és az Üzletmenet Folytonossági- és Katasztrófa Terv tartalmazza.

A **tűzfal** és a **behatolás detektáló** által megvalósított biztonsági funkciók az alábbiak:

- biztonsági naplózás (a hálózati kommunikáció naplózása, a biztonsági napló védelme, az ahhoz való hozzáférés rendszervizsgáló szerepkörre korlátozása, a napló folyamatos elemzése: biztonsági riasztások és automatikus válaszok megvalósítása),
- a felhasználói adatok védelme (az információ áramlás ellenőrzési szabályok érvényre juttatása /szűrés, a tiltott információ áramlás megakadályozása, megfigyelése),
- azonosítás és hitelesítés (a saját felhasználók /hálózati adminisztrátorok/ azonosítása, hitelesítése, a saját funkciók elérésének sikeres hitelesítéshez kötése),
- a biztonsági funkciók megbízható védelme (az információ áramlás ellenőrzés megkerülhetlenségének biztosítása).

## 6 Megfelelőség vizsgálata

Szolgáltató szolgáltatásának következő elemeinek megfelelőségét vizsgálja, vizsgálhatja:

- a saját magánkulcsainak tárolására használt kriptográfiai hardver modult;
- minősített elektronikus aláírás létrehozására alkalmas biztonságos aláírás létrehozó eszközöket (pl. intelligens kártyákat);
- az ISO 9001 minőségbiztosítási rendszer előírásai szerinti működést;
- az ISO 27001 információbiztonsági irányítási rendszer előírásainak megfelelő működést,
- Elektronikus Aláírás Szakértő által félévente végzett audit a Szolgáltató minősített szolgáltatói tevékenységének jogszabályi megfelelősége tekintetében.

### 6.1 A megfelelőség vizsgálatának gyakorisága

A különböző vizsgálatokra a jogszabályoknak megfelelően az alábbi gyakorisággal kerül sor:

- az eszközök vizsgálatára a használatba vételt megelőzően egyszer, majd a folyamatos megfelelés ellenőrzéseképpen legalább évente;
- a magas színvonalú szolgáltatást biztosító ISO 9001 minőségbiztosítási rendszer ellenőrzésére évente legalább 1 alkalommal, a teljes rendszerre vonatkozóan;
- az információbiztonsági irányítási rendszer ISO 27001 szabványnak való megfelelés ellenőrzése évente legalább 1 alkalommal a teljes rendszerre vonatkozóan;

### 6.2 Az átvizsgáló egységek megnevezése

A megfelelőségi vizsgálatokat külső szervezetek végzik/végezték:

- a biztonságos aláírás létrehozó eszközök tanúsítását a jogszabályi előírásoknak megfelelő tanúsító szervezet (ld. [1] Törvény 24. §), amelynek kijelölésére a [7] Rendelet előírásainak megfelelően kerül sor;
- a szolgáltatási rendszer jogszabályi követelményeknek való megfelelését, illetve biztonságát legalább évente független szakértő felülvizsgálja. A vizsgálat kiterjed a kontroll rendszerre, a szabályozásra, a szabályok implementációjára és azok monitorozására;
- az ISO 9001 minőségbiztosítási rendszer működtetését legalább évente akkreditált ISO tanúsító szervezet;
- az ISO 27001 információbiztonsági irányítási rendszer működtetését legalább évente akkreditált, külső, független tanúsító szervezet.

A Szolgáltató e külső vizsgálatokon túl saját belső ellenőrzési rendszerrel is rendelkezik, mely rendszeresen vizsgálja a korábbi tanúsításoknak való megfelelőséget, és eltérés esetén megteszi a szükséges lépéseket. Az egyes szolgáltatói tevékenységek a jogszabályoknak és kapcsolódó szabályzatoknak való megfelelését a Szabályzat Elfogadó Egység vizsgálja saját munkarendje szerint.

### 6.3 Az átvizsgáló egységek és a vizsgált fél kapcsolata

Az Átvizsgáló egységek és a vizsgált fél kapcsolatára vonatkozó rendelkezéseket a Szolgáltató Minősített Szolgáltatási Szabályzata [14] tartalmazza, melynek mindenkor aktuális verziója megtalálható a Szolgáltató honlapján.

## **6.4 A vizsgálat által érintett területek**

A vizsgálat által érintett területekre vonatkozó rendelkezéseket a Szolgáltató Minősített Szolgáltatási Szabályzata [14] tartalmazza, melynek mindenkor aktuális verziója megtalálható a Szolgáltató honlapján.

## **6.5 Hiányosságok esetén végrehajtandó tevékenységek**

A hiányosságok esetén végrehajtandó tevékenységekre vonatkozó rendelkezéseket a Szolgáltató Minősített Szolgáltatási Szabályzata [14] tartalmazza, melynek mindenkor aktuális verziója megtalálható a Szolgáltató honlapján.

## 7 Üzleti és jogi tudnivalók

### 7.1 Díjak

A mindenkor érvényes szolgáltatások díjait a Szolgáltató saját Internetes oldalán teszi közzé, illetve azokat a Szolgáltatási szerződés tartalmazhatja.

A Szolgáltató díjaira vonatkozó egyéb szabályokat az ÁSZF [15] tartalmazza.

### 7.2 Bizalmasság, adatkezelés

A Szolgáltató a belső szabályzataiban meghatározott módon, illetve műszaki és egyéb intézkedésekkel biztosítja az Előfizető által feltöltött adatok bizalmasságát.

#### 7.2.1 Személyes adatok

A Szolgáltató az Avtv. [2] mindenkor hatályos rendelkezéseinek megfelelően, az érintett hozzájárulása alapján kezeli az Előfizetők személyes adatait. Ennek során személyes adatnak minősül bármely meghatározott természetes személlyel kapcsolatba hozható, vagy az adatból levonható, az érintettre vonatkozó következtetés.

A Szolgáltató a szolgáltatás igénybevétele kapcsán, az Előfizető azonosítása érdekében alábbi személyes adatait kezeli:

- a) Név
- b) telefonszám
- c) állandó lakcím
- d) személyazonosító okmány azonosítószáma

A kezelt személyes adatokhoz csak az erre jogosult munkatársak férnek hozzá, munkakörük ellátása érdekében.

A Szolgáltató az általa kezelt személyes adatokat harmadik fél részére – a törvény által elrendelt adattovábbítás esetein túl - csak az Előfizető előzetes, egyértelmű, kifejezett és utólagosan visszakereshető formájú hozzájárulása esetén továbbítja.

Az adatokat a Szolgáltató a Polgári Törvénykönyv [3] általános elévülési ideje figyelemmel a szerződés megszűnésétől számított 5 évig, illetve az időközben esetlegesen indult bírósági eljárás jogerős befejezéséig kezeli, ezt követően helyreállíthatatlanul törli.

#### 7.2.2 Archivált adatok

A Szolgáltató az átadott dokumentumokat az Előfizető üzleti titkaként kezeli, annak tartalmát nem ismeri meg, a dokumentumokhoz – annak tartalmának megismerése nélkül - csak az arra jogosult munkatársak férhetnek hozzá kizárólag abban az esetben, ha a hozzáférés az archiváló rendszer működőképességének biztosításához szükséges.

A megőrzésre átadott dokumentumokban foglalt adatok – ideértve a személyes adatokat is – kezelésének jogszerűségéért az Előfizető felel, a Szolgáltató felelőssége a dokumentumok bizalmas kezelésére terjed csak ki.

A Szolgáltató a megőrzésre átadott állományokat harmadik fél részére – a törvény által elrendelt adattovábbítás eseteit kivéve – csak az Előfizető előzetes, írásbeli nyilatkozata alapján adja át, mely hozzáférésekről a Szolgáltató nyilvántartást vezet, és azokat kizárólag elektronikus formában teljesíti. Ezen túlmenően az Előfizető közvetlenül, a Szolgáltató külön, kifejezett értesítése nélkül, saját

felelősségére hozzáférést biztosíthat harmadik fél részére a Szolgáltatónál megőrzött adataihoz, mely hozzáférések a rendszer naplóállományaiból visszakereshetők, azonban ezekről külön nyilvántartás nem készül.

A Szolgáltató a megőrzésre átadott adatokat a szerződéses viszony megszűnésével – figyelemmel a 3.1 pontban foglaltakra - egyidőben helyreállíthatatlanul törli.

### **7.2.3 Törvény által elrendelt adatszolgáltatás**

A Szolgáltató a bizalmasság biztosításának követelménye alól mentesül, ha az adattovábbítást jogszabály írja elő. Ebben az esetben az adattovábbítás jogszerűségéért a Szolgáltatót jogszabály alapján megkereső szervezet felel.

A Szolgáltató az alábbi esetekben teljesíthet adattovábbítást az Előfizető személyes adataiból, valamint a megőrzésre átadott dokumentumaiból:

- a) a büntetőeljárásról szóló 1998. évi XIX: törvény 71. § (1) bekezdése
- b) az adózás rendjéről szóló 2003. évi XCII. törvény 48. § (1) bekezdése

## **7.3 Szellemi alkotásokhoz fűződő jogok**

A szolgáltatási tevékenység során alkalmazott összes név, termék, szabályzat a Szolgáltató tulajdonát képezi, a szoftver és hardver komponensek a Szolgáltató tulajdonát képezik vagy azokat jogszerűen használja.

## **7.4 Jogok és kötelezettségek**

### **7.4.1 Az Előfizető jogai és kötelezettségei**

Az Előfizető jogosult az archiválás szolgáltatás igénybevételére a jelen Szolgáltatási Szabályzatban, a vonatkozó jogszabályokban, valamint a Szolgáltató egyéb nyilvános szabályzataiban foglalt feltételeknek megfelelően.

Az Előfizető kötelessége a jelen szabályzatban a Szolgáltató egyéb szabályzataiban, valamint a jogszabályban foglaltaknak megfelelően eljárni. Amennyiben a szolgáltatást az Előfizető nevében harmadik fél veszi igénybe, az Előfizető köteles biztosítani, hogy a harmadik fél az Előfizetőre vonatkozó szabályokat betartassa.

### **7.4.2 Ajánlások az Érintett Fél részére**

Jelen Szabályzatban az Érintett Fél számára meghatározott tevékenységek ajánlást jelentenek a Szolgáltató részéről, amelyek szükségesek az elektronikus archiválás biztonságos végrehajtásához.

A Szolgáltató kizárja a felelősségét, ha az érintett fél az archiválás szolgáltatás kapcsán kibocsátott igazolások ellenőrzése és felhasználása során - a Szolgáltató archiválási rendjében, szolgáltatási szabályzatában lévő ajánlások ellenére - a tőle az adott helyzetben általában elvárható magatartást nem tanúsítja, illetve ha nem a hatályos jogszabályok szerint jár el.

Az Érintett Fél számára az alábbi előírások betartása ajánlott:

- e) Az Érintett félnek célszerű meggyőződnie arról, hogy a Szolgáltató által kibocsátott igazolás valóban egy adott dokumentumhoz tartozik-e. Mindez elvégezhető – többek között – az igazolásban szereplő lenyomat, valamint a dokumentumról készített lenyomat összehasonlításával.
- f) Olyan eljárásokat, alkalmazásokat használ, amelyek támogatják a Szolgáltató által kibocsátott igazolások hitelességének ellenőrzését. Ehhez az igazoláson elhelyezett minősített elektronikus

aláírást kell ellenőrizni. A minősített elektronikus aláírás ellenőrzése az aláírás, valamint az aláíráshoz tartozó tanúsítvány aláírás időpontjában való érvényességének ellenőrzését jelenti a tanúsítványra vonatkozó szolgáltatási szabályzat szerint.

Az elektronikus igazolás (üzenet), az elektronikus aláírás és a tanúsítvány összetartozására, az igazolás sértetlenségére, a tanúsítvány jogos és a szabályzatokkal összhangban történő használatának ellenőrzése, valamint a nyilvános kulcsot tartalmazó tanúsítvány érvényességének vizsgálatára vonatkozó egyéb ajánlásokat a Szolgáltató Minősített hitelesítés-szolgáltatás szolgáltatási szabályzata tartalmaz.

- g) A Szolgáltató által vállalt felelősségbiztosítás mértéke alapján meggyőződik arról, hogy az igazoláshoz kapcsolódó felelősségvállalás mértéke megfelel-e a kívánt célra.

### 7.4.3 Szolgáltató egyéb kötelezettségei

A Szolgáltató általános kötelessége:

- a) a szolgáltatásainak a hatályos jogi szabályozással, jelen szabályzattal és egyéb nyilvánosságra hozott szabályzataival, szerződéses feltételeivel összhangban való nyújtása;
- b) a magas színvonalú és biztonságos szolgáltatások folyamatos biztosítása;
- c) a Szolgáltatások biztosítása minden olyan igénylő számára, aki elfogadja a Szolgáltató szolgáltatási szabályzataiban és egyéb jogszabályokban meghatározott feltételeket;
- d) az alvállalkozók feladatainak egyértelműen meghatározása, működésük rendszeres ellenőrzése, a Szolgáltató által előírt eljárások betartásának biztosítása, és az esetlegesen szabályzattól eltérő működés esetén a helytelen működés megszüntetésének előírása és ellenőrzése;

#### 7.4.3.1 A Szolgáltatói egységek közös kötelezettségei

A Szolgáltatóhoz tartozó szervezetek, egységek kötelessége:

- a) a Közösség elektronikus hitelesítéssel kapcsolatos tevékenységeinek, alapelveinek meghatározása, ezek alapján a működést részletesen tárgyaló szabályzatok készítése és rendszeres felülvizsgálata,
- b) megfelelő szakmai végzettséggel rendelkező, a folyamatos, szabályzatokban előírt működés biztosításához elégséges számú kezelőszemélyzet biztosítása,
- c) a szabályzatokban előírt, az archiválás és egyéb PKI folyamat elvégzésére alkalmas, megfelelően beállított szoftver és hardver infrastruktúra biztosítása, a szükséges változtatások megtétele,
- d) az infrastruktúra működtetéséért, javításáért és karbantartásáért felelős személyzet munkájának és szakmai felkészültségének folyamatos ellenőrzése, a szükséges változtatások megtétele,
- e) az előző pontokban előírt infrastruktúra folyamatos, biztonságos üzemeltetése, hibajavítása és az infrastruktúrába tartozó eszközökre előírt szabványos karbantartás elvégzése,
- f) Üzleti Folytonossági Terv készítése, alkalmazása,
- g) a szabályzatokban előírt módon folytatott tevékenység során keletkező adatok jelen és kapcsolódó szabályzatokban meghatározott kezelésére, tárolására, archiválására alkalmas szoftver és hardver eszközök biztosítása, működtetése, karbantartása,
- h) az archiválási és egyéb PKI folyamatokat végző és az azok során keletkező adatokat tároló szoftver és hardver rendszer jelen és kapcsolódó szabályzatokban előírt logikai és fizikai védelmét biztosító szoftver és hardver eszközök biztosítása,
- i) a logikai és fizikai védelmet megteremtő eszközök megfelelő üzemeltetése, az informatikai, fizikai, adminisztrációs és üzleti biztonság megteremtése és fenntartása.

- j) a Szolgáltató működését szabályozó belső dokumentumok előírásai alapján szabad hozzáférés biztosítása a Szabályzat Adminisztrátor részére a felügyelendő dokumentumokhoz, továbbá a megfelelő körülmények biztosítása számára a belső ügyviteli folyamatok azok helyszínén való ellenőrzéséhez.

#### **7.4.3.2 A Szabályzat Elfogadó Egység kötelezettségei**

A Szabályzat Elfogadó Egység, illetve a Szabályzat Adminisztrátor további kötelezettségeit a Szolgáltató Minősített Szolgáltatási Szabályzata [14] tartalmazza, melynek mindenkor aktuális verziója megtalálható a Szolgáltató honlapján.

## **7.5 Felelősség**

### **7.5.1 A Szolgáltató általános felelőssége**

A Szolgáltató felelős a Szabályzat keretei között végzett szolgáltatói tevékenységeikért.

A Szolgáltató a megbízhatóság biztosítása érdekében felelősségbiztosítással rendelkezik, mely kiterjed a Szolgáltató által őrzött érvényességi lánc vagy az elektronikus dokumentumok sérülésével vagy megsemmisülésével szerződésen kívül, illetve szerződésszegéssel okozott károkra. A Szolgáltató biztosítja azon bizonyított károkért, amelyek a Szolgáltató felelősségi körében annak saját hibájából vagy mulasztásából keletkeztek, kártérítést fizet.

A Szolgáltató a vele szerződéses jogviszonyban nem álló harmadik személynek okozott kárért a Polgári Törvénykönyv [3] általános szabályai szerint felel, az Előfizetővel szemben pedig a szerződésszegésért való felelősség szabályai szerint felelős az archiválási-szolgáltatás biztosítása során okozott kárért, ha az [1] Törvényben vagy egyéb jogszabályokban foglalt kötelezettségeit megszegte.

#### **7.5.1.1 A felelősség korlátai**

Szolgáltató nem felelős az olyan károkért, amelyek abból adódtak, hogy az Előfizető vagy az Érintett Fél a szolgáltatás igénybe vétele, illetve annak felhasználása során nem a hatályos jogszabályoknak, illetve szolgáltatói szabályzatoknak megfelelően járt el, illetve nem tanúsította a tőle elvárható gondosságot.

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 Szolgáltató nem felel az olyan károkért, amely az Internet, vagy annak egy részének működési hibájából adódóan a tájékoztatás és egyéb kommunikációs kötelezettségeit nem tudja ellátni.

A Szolgáltató nem vállal felelősséget továbbá azon károkért sem, melyek az Előfizető által feltöltött dokumentumok tartalmából keletkezhetnek, tekintettel arra, hogy a szolgáltatás nyújtása során – az eljárás sajátosságaiból adódóan – a Szolgáltató a feltöltött dokumentumok tartalmát nem ismeri meg. Ebben az esetben az Előfizető a 7.5.2 pontban foglaltak szerint felel.

A Szolgáltató az érvényességi lánc és az általa őrzött elektronikus dokumentumok sérülése vagy megsemmisülése által – szerződésen kívül vagy szerződésszegéssel – harmadik személynek okozott kár tekintetében káreseményenként legfeljebb 5 millió Ft;

A Szolgáltató által kibocsátott igazolásokkal kapcsolatos felelősségvállalás nem lehet nagyobb, mint az igazolás aláírásakor használt minősített tanúsítványban szereplő tranzakciós limit mértéke. Abban az esetben, ha a tanúsítványban tranzakciós limit nem került feltüntetésre, akkor a felelősségvállalás mértéke káreseményenként legfeljebb 5 M Ft.

Papír alapú igazolás kiadásakor az elektronikus igazolás kibocsátásra vonatkozó korlátozási szabályok az irányadóak.

A Szolgáltató a kárt azt követően téríti meg, miután a kártérítési igény elbírálásához szükséges, valamint a Szolgáltató felelősségét, a kár időpontját és összegét bizonyító valamennyi dokumentum rendelkezésre áll.

## 7.5.2 Az Előfizető felelőssége

Az Előfizető kártérítési felelősséggel tartozik azokért a veszteségekért és károkért, melyeket a kötelezettségeinek és a rá vonatkozó ajánlások be nem tartásával okoz a Szolgáltató számára.

Előfizető köteles biztosítani, hogy kizárólag olyan dokumentumokat töltsön fel a Szolgáltató által üzemeltetett archívumba, amelyeket a személyes adatok védelméről és a közérdekű adatok nyilvánításáról szóló 1992. évi LXIII. törvény [2] értelmében a Szolgáltatónak, mint adatfeldolgozónak átadhat. Az Előfizető ezen kötelezettsége elmulasztásából eredő károkért a polgári jog általános szabályai szerint felel.

Az Előfizető felelősségére vonatkozó további szabályokat a Szolgáltató „Általános Szerződési Feltételek” című dokumentuma [15] tartalmazza

## 7.6 Változtatási eljárás

A Szolgáltató Szabályzat-változtatási eljárásra, a Szabályzat Elfogadó Egységre, illetve annak működésére, a Változtatási eljárásra vonatkozó egyéb szabályokra vonatkozó szabályokat a Szolgáltató Minősített Szolgáltatási Szabályzata [14] tartalmazza.

## 7.7 Panaszkezelés

### 7.7.1 Panaszok benyújtásának helye

A Szolgáltató tevékenységével kapcsolatos kérdések, kifogások és panaszok benyújtásának helye a Szolgáltató ügyfélszolgálati irodája (lásd 1.5 alfejezet).

### 7.7.2 Panaszok benyújtásának módja

A panaszokat a Szolgáltató levélben, e-mailben a info@netlock.hu címen, faxon, telefonon és személyesen fogadja (lásd 1.5 alfejezet).

### 7.7.3 Panaszok kezelésének eljárása

A panasz kézhezvételéről a Szolgáltató az érkeztetést követően 1 munkanapon belül értesíti a beadó felet a megjelölt címen, az ügy kivizsgálásához szükséges idő megjelölésével. A jelzett időn belül, amely lehetőség szerint nem több, mint 10 munkanap, a Szolgáltató a panaszt kivizsgálja, a felmerült hibát a műszakilag indokolt időn belül elhárítja, és mindezen tevékenységekről a bejelentőt írásban tájékoztatja. Ha a választ bejelentő nem fogadja el, egyeztetést kell kezdeményeznie a Szolgáltatóval. Ha a Szolgáltató ezt megtagadja, vagy ha a felek közötti egyeztetés annak megkezdésétől számított 20 munkanapon belül nem vezetne eredményre, akkor a bejelentő jogi útra terelheti az ügyet. A panaszkezelés véghatárideje – a fentiek figyelembevételével – a bejelentéstől számított 30 nap.

### 7.7.4 Illetékes fogyasztóvédelmi felügyelőség

**Budapest Főváros Kormányhivatal Fogyasztóvédelmi Felügyelősége,  
Fogyasztókapcsolati Iroda:**

Cím: 1052 Budapest, V. ker. Városház u. 7.

Levelezési cím: 1364 Budapest, Pf. 144.

Telefon: +36 1 328-0185

Fax: +36 1 411-0116

E-mail: fogyved\_kmf\_budapest@nfh.hu

## 7.8 Hivatkozott jogszabályok, szabványok és egyéb dokumentumok

Jelen dokumentum az alábbi dokumentumokra hivatkozik:

- [1]. 2001. évi XXXV. Törvény az elektronikus aláírásról;
- [2]. 1992 évi LXIII. törvény a személyes adatok védelméről és a közhasznú adatok nyilvánosságáról;
- [3]. 1959. évi IV. Törvény a Polgári Törvénykönyvről;
- [4]. 2/2002. (IV.26) MeHVM irányelve a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről;
- [5]. 3/2005. (III. 18.) IHM rendelet az elektronikus aláírásokkal kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről;
- [6]. 114/2007. (XII. 29.) GKM rendelet a digitális archiválás szabályairól;
- [7]. 45/2005 (III. 11.) Kormányrendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással kapcsolatos feladat- és hatásköréről, valamint eljárásának részletes szabályairól;
- [8]. A Nemzeti Hírközlési Hatóság HL-21917-14/2008. számú határozata a az elektronikus aláírással kapcsolatos szolgáltatások nyújtása során alkalmazható biztonságos kriptográfiai algoritmusok és paramétereik meghatározására;
- [9]. Elektronikus archiválási szolgáltatással kapcsolatos hatósági tájékoztató, Nemzeti Hírközlési Hatóság Hivatala 2008. június;
- [10]. Ajánlás eljárásrendi követelményekre elektronikus aláírás felhasználásával végzett elektronikus archiválási szolgáltatások szolgáltatói számára Nemzeti Hírközlési Hatóság Hivatala 2008. június;
- [11]. Ajánlás elektronikus archiválási szolgáltatások nyújtásához felhasznált megbízható rendszerekre vonatkozó biztonsági követelményekre, Nemzeti Hírközlési Hatóság Hivatala 2008. június;
- [12]. Nemzeti Hírközlési Hatóság Hivatalának tájékoztatója az elektronikus aláírással kapcsolatos szolgáltatások nyújtásához kapcsolódó bizalmi munkakörök vonatkozásában, 2008. május;
- [13]. Minősített elektronikus archiválásra vonatkozó archiválási rend;
- [14]. Minősített Szolgáltatási Szabályzat - NetLock;
- [15]. Általános Szerződési Feltételek (ÁSZF) – NetLock;
- [16]. ISO 3166 English Country Names and Code Elements;
- [17]. FIPS PUB 140-1 (1994. január 11): "Kriptográfiai modulok biztonsági követelményei";
- [18]. RFC 5280 (korábban RFC 3280) Internet X.509 Nyilvános kulcsú infrastruktúra – tanúsítvány- és tanúsítvány visszavonási lista profil;
- [19]. RFC 3647 (korábban RFC 2527) Internet X.509 Nyilvános kulcsú infrastruktúra – tanúsítványtípus és Szolgáltatási Szabályzat keretrendszer;
- [20]. International Telecommunication Union X.509 "Információ technológia – Nyílt rendszerek kapcsolódása - Könyvtár: Nyilvános kulcs és attribútum tanúsítvány-keretrendszer";
- [21]. RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP);

- [22]. ETSI 102 042 v1.1.1 (2002-04) Policy requirements for certification authorities issuing public key certificates;
- [23]. RFC 4810 Long-Term Archive Service Requirements;
- [24]. Dublin Core Metada Element Srt., version 1.1.
- [25]. ETSI 101 903 V1.4.1 (2009-06) V1.4.1 - XML Advanced Electronic Signatures (XAdES)
- [26]. CWA 14171:2004

## **7.9 Értelmezés és érvényesítés**

### **7.9.1 Irányadó jog**

A Szolgáltató tevékenységét a mindenkor hatályos magyar jogszabályoknak megfelelően végzi (ld. [1] Törvény, [4] Irányelv, [5] Rendelet). A Szolgáltató szerződéseire és szabályzataira, azok teljesítésére a magyar jog az irányadó, és azok a magyar jog szerint értelmezendők.

### **7.9.2 A rendelkezések különválaszthatósága**

Bármely rendelkezés hatályon kívül kerülése vagy bíróság általi semmissé nyilvánítása nem befolyásolja a többi rendelkezés hatályát, érvényességét.

### **7.9.3 A rendelkezések kiterjesztése**

A szolgáltatási tevékenységhez kapcsolódó egyéb szerződések figyelemmel vannak jelen Szabályzat rendelkezéseire is.

### **7.9.4 Értesítések**

Az Előfizető jognyilatkozatokat a Szolgáltató felé kizárólag írásban teheti meg. Szervezet képviselőjében való eljárás esetén a jognyilatkozat kizárólag a képviselői jogosultság előzetes igazolását és ellenőrzését követően lehetséges.

A Szolgáltató Előfizetőit, illetve egyéb ügyfeleit honlapján történő közzététel vagy elektronikus levél útján tájékoztatja.

### **7.9.5 Vitás kérdések megoldására vonatkozó eljárások**

A Szolgáltató tevékenységével kapcsolatos kérdéseket, kifogásokat és panaszokat a info@netlock.hu e-mail címen, valamint a Szolgáltató központi fax számán lehet írott formában bejelenteni, illetve telefonon vagy személyesen a Szolgáltató ügyfélszolgálati irodájában.

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

Amennyiben a Felek közötti egyeztetés - mely a Szolgáltató a panasz kivizsgálásának eredményeként adott válaszát követi - valamelyik fél által kezdeményezett egyeztetés napjától számított 30 napon belül nem vezet eredményre, arra az esetre a Felek kölcsönösen alávetik magukat a Kereskedelmi és Iparkamara mellett szervezett Állandó Választottbíróság kizárólagos illetékességének. A Választottbírósági eljárás nyelve a magyar, az eljárásban irányadó jog a mindenkor hatályos magyar anyagi és eljárásjog. Az eljáró bírók száma: 3.