

3/2005. (III. 18.) IHM rendelet

az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről

Az elektronikus aláírásról szóló 2001. évi XXXV. törvény (a továbbiakban: Eat.) 27. §-a (2) bekezdésének *a*) pontjában foglalt felhatalmazás alapján az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről a következőket rendelem el:

1. § A rendelet hatálya kiterjed a belföldi lakóhelyű vagy belföldön tartózkodási hellyel rendelkező természetes személyekre, illetve belföldi székhelyű (telephelyű) jogi személyekre vagy jogi személyiség nélküli szervezetekre (a továbbiakban: szolgáltató), amelyek az Eat. 6. §-ának (1) bekezdése szerinti, elektronikus aláírással kapcsolatos szolgáltatást (a továbbiakban: szolgáltatás) nyújtanak vagy a Nemzeti Hírközlési Hatósághoz (a továbbiakban: Hatóság) ilyen szolgáltatás nyújtására irányuló bejelentést tesznek.

2. § E rendelet alkalmazásában

a) bizalmi munkakör az alábbiakban felsorolt valamennyi munkakör:

aa) a szolgáltató informatikai rendszeréért általánosan felelős vezető,

ab) biztonsági tisztviselő: a szolgáltatás biztonságáért általánosan felelős személy,

ac) rendszeradminisztrátor: az informatikai rendszer telepítését, konfigurálását, karbantartását végző személy,

ad) rendszerüzemeltető: az informatikai rendszer folyamatos üzemeltetését, mentését és helyreállítását végző személy,

ae) független rendszervizsgáló: a szolgáltató naplózott, illetve archivált adatállományát vizsgáló, a szolgáltató által a szabályszerű működés érdekében megvalósított kontroll intézkedések betartásának ellenőrzéséért, a meglévő eljárások folyamatos vizsgálatáért és monitorozásáért felelős személy,

af) regisztrációs felelős: a végtanúsítványok előállításának, kibocsátásának, visszavonásának és felfüggesztésének jóváhagyásáért felelős személy;

b) igénylő: a tanúsítvány iránti igényt benyújtó személy;

c) információbiztonsági irányítási rendszer: irányítási rendszer egy szervezet vezetésére és szabályozására, az információ bizalmosságának, sértetlenségének és rendelkezésre állásának megőrzése szempontjából;

d) informatikai rendszer: a szolgáltató által a szolgáltatói kulcspár kezeléséhez, az aláírás-létrehozó adat előállításához, a tanúsítványok kibocsátásához, a kibocsátott tanúsítványt tartalmazó nyilvántartáshoz, a visszavonási nyilvántartásokhoz és a visszavonás kezelési szolgáltatáshoz, az időbélyegzés-szolgáltatáshoz, az elektronikus archiválás szolgáltatás, valamint e tevékenységek informatikai védelméhez használt, az Eat. 3. számú mellékletének *f*) pontja szerinti megbízható rendszerek és termékek;

e) kriptográfiai kulcs: olyan kriptográfiai transzformációt vezérlő egyedi jelsorozat, amelynek ismerete a kriptográfiai transzformáció elvégzéséhez, különösen az elektronikus aláírás előállításához vagy ellenőrzéséhez szükséges;

f) minőségirányítási rendszer: irányítási rendszer egy szervezet vezetésére és szabályozására, a minőség szempontjából;

g) rendkívüli üzemeltetési helyzet: olyan, a szolgáltató üzemmenetében zavart okozó rendkívüli helyzet, amelyben a szolgáltató rendes üzemmenetének folytatására ideiglenesen vagy véglegesen nincsen lehetőség. Rendkívüli üzemeltetési helyzetnek minősül az is, ha a szolgáltató szolgáltatói magánkulcsa olyan személy birtokába kerül, aki a szolgáltatói magánkulcs birtoklására nincsen feljogosítva, illetve, ha a fenti esemény megtörténte alappal feltételezhető, vagy annak közvetlen veszélye fennáll;

h) szolgáltatói kulcspár: a szolgáltatói magánkulcs és a szolgáltatói nyilvános kulcs;

i) szolgáltatói magánkulcs: olyan kriptográfiai kulcs, amelyet a hitelesítés-szolgáltató vagy az időbélyegzést nyújtó szolgáltató saját elektronikus aláírási szolgáltatásának igazolására, így különösen a tanúsítvány kibocsátására, a visszavonási nyilvántartásokra, az időbélyegzésre, a naplózáshoz, az archiváláshoz használ;

j) szolgáltatói nyilvános kulcs: olyan kriptográfiai kulcs, amelyet a szolgáltatói magánkulcs használatával létrehozott elektronikus aláírás ellenőrzésére használnak;

k) tanúsítvány kibocsátása: a tanúsítvány átadása az aláírónak, valamint a szolgáltató nyilvántartásában a tanúsítvány elérhetővé tétele az aláíró hozzájárulása esetén;

l) változáskezelés: azon szabályok összessége, amelyek meghatározzák a szolgáltatási folyamatokban és az azt

kiszolgáltató informatikai szolgáltatásokban bekövetkező módosítások, változások biztonságos végrehajtását;

m) *visszavonás kezelése*: az Eat. 14. §-ban meghatározott esetekben a kibocsátott tanúsítványok visszavonására és felfüggesztésére vonatkozó eljárások lefolytatása;

n) *visszavonási nyilvántartások*: nyilvántartások a felfüggesztett, illetőleg a visszavont tanúsítványokról, amelyek tartalmazzák legalább a felfüggesztés vagy visszavonás tényét, és a felfüggesztés vagy visszavonás időpontját.

I. Fejezet

A szolgáltatókra vonatkozó közös követelmények

3. § (1) A szolgáltatónak tevékenységének bejelentése előtt szolgáltatási szabályzatot kell készítenie.

(2) A szolgáltatónak a szolgáltatási szabályzatot a szolgáltatási tevékenység megkezdésével egyidejűleg nyilvánosságra kell hoznia, és azt az ügyfélforgalom számára nyitva álló helyiségben, valamint interneten elérhetővé kell tennie.

(3) A szolgáltatás igénybe vevőjét a szolgáltatási szerződés megkötését megelőzően tájékoztatni kell a szolgáltatási szabályzat tartalmáról és a szolgáltatási szabályzat elérhetőségéről.

4. § A szolgáltatási szabályzatnak legalább az *1. számú mellékletben* meghatározottakat kell tartalmaznia.

5. § A szolgáltatási szabályzat módosítása esetén a külön jogszabályban e tekintetben előírt eljárást kell alkalmazni.

6. § (1) A szolgáltató az elektronikus aláírás felhasználásával elkövetett bűncselekmények felderítése céljából, illetőleg nemzetbiztonsági érdekből az Eat. 11. §-ának (2) bekezdésében meghatározott esetekben és adatokra vonatkozóan a nyomozó hatóságnak és a nemzetbiztonsági szolgálatoknak díjmentesen adatokat továbbít.

(2) A szolgáltató az (1) bekezdésben meghatározott kötelezettségeknek haladéktalanul köteles eleget tenni, és az adatok továbbítását nem kötheti egyéb feltételekhez, így különösen az adatszolgáltatás költségeiben való megállapodáshoz vagy a költségek előlegezéséhez.

7. § A szolgáltató köteles biztosítani, hogy a 2. § a) pontja szerinti bizalmi munkakörök közül:

a) a biztonsági tisztviselő nem töltheti be a független rendszervizsgáló munkakört;

b) az informatikai rendszerért általánosan felelős vezető nem láthatja el a biztonsági tisztviselő, illetve a független rendszervizsgáló feladatait.

8. § A szolgáltató a tevékenységével kapcsolatos panaszokat köteles a panasz bejelentésétől számított 30 napon belül kivizsgálni, és annak eredményéről a bejelentőt értesíteni.

9. § A hitelesítés- és időbélyeg-szolgáltatónak biztosítania kell a szolgáltatói nyilvános kulcsának sértetlenségét, hitelességét és elérhetőségét. Ennek érdekében a szolgáltatói nyilvános kulcsot interneten is elérhetővé kell tennie.

A szolgáltató tevékenységének befejezése

10. § (1) A hitelesítés-szolgáltatónak tevékenysége befejezésekor az informatikai rendszerében foglalt adatairól teljes körű, időbélyegzővel ellátott mentést kell készítenie. A mentett adatállományokat védeni kell a jogosulatlan módosítástól, illetve biztosítani kell azt, hogy az adatállomány tartalmához jogosulatlan személyek ne férhessenek hozzá. Biztosítani kell továbbá, hogy az adatok a megőrzési időn belül az arra jogosult személyek számára hozzáférhetőek és értelmezhetőek legyenek.

(2) Az archiválási szolgáltatás tevékenység befejezésére vonatkozó, az Eat.-ben meghatározott bejelentési kötelezettséget követően az archiválási szolgáltató a Hatóság határozata szerinti, elfogadott kriptográfiai algoritmuson alapuló minősített elektronikus aláírást és minősített szolgáltató által kibocsátott időbélyegzőt köteles elhelyezni vagy elhelyeztetni az érvényességi láncon, és azt az igénybe vevőnek köteles átadni. Az érvényességi láncot ezt követően visszaállíthatatlan módon törölni kell az archiválási szolgáltató informatikai rendszeréből.

Felelősségbiztosítás

11. § (1) A szolgáltatónak a megbízhatóság biztosítása érdekében felelősségbiztosítással kell rendelkeznie.

(2) A felelősségbiztosítási szerződésnek ki kell terjednie az alábbi, a szolgáltató által a szolgáltatások nyújtásával összefüggésben okozott károokra:

a) az elektronikus aláírással vagy időbélyegzővel, illetve az ezzel ellátott elektronikus dokumentummal, illetőleg

az archiválási szolgáltató által őrzött érvényességi lánc vagy az elektronikus dokumentumok sérülésével vagy megsemmisülésével szerződésen kívül okozott károkra;

b) az elektronikus aláírással vagy időbélyegzővel, illetve az ezzel ellátott elektronikus dokumentummal, illetőleg az archiválási szolgáltató által őrzött érvényességi lánc vagy az elektronikus dokumentumok sérülésével vagy megsemmisülésével szerződésszegéssel okozott károkra;

c) az Eat. 16. §-ának (4) bekezdésében foglaltak megszegésével a Hatóságnak okozott károkra.

(3) A felelősségbiztosítási szerződésnek egy biztosítási esemény vonatkozásában káreseményenként nem minősített szolgáltató esetében a tanúsítványban, illetve a szolgáltatási szabályzatban vállalt felelősségvállalási érték legalább háromszorosáig, minősített szolgáltató esetében ötszöröséig kell fedezetet biztosítani az összes károsultnak okozott károkra. Több azonos okból bekövetkezett, időben összefüggő káresemény egy biztosítási eseménynek minősül.

(4) A felelősségbiztosításnak a (3) bekezdésben meghatározott összeg erejéig fedezetet kell nyújtania a károsultnak a szolgáltató károkozó magatartásával összefüggésben keletkező teljes kárára, függetlenül attól, hogy a kárt szerződésszegéssel vagy szerződésen kívül okozták.

(5) Ha egy biztosítási eseménnyel kapcsolatban több jogosult megalapozott kártérítési igénye meghaladja a károkra biztosítási eseményenként a felelősségbiztosítási szerződésben meghatározott összeget, akkor a kártérítési igények megtérítése az összes kártérítési igénynek a felelősségbiztosítási szerződésben meghatározott összeghez viszonyított arányában történik.

II. Fejezet

A minősített szolgáltatókra vonatkozó különös követelmények

1. Pénzügyi követelmények

12. § A szolgáltató a szolgáltatási tevékenységének megszűnésével kapcsolatos költségek biztosítása és a megbízhatóság érdekében köteles a 13-14. §-ban meghatározott követelmények legalább egyikének megfelelni.

13. § (1) A hitelesítés-szolgáltató legalább huszonötmillió forint összegű, feltétel nélküli és visszavonhatatlan bankgaranciával rendelkezik.

(2) Az (1) bekezdésben meghatározott bankgaranciának legalább az alábbiakat kell tartalmaznia:

a) a garanciavállaló megnevezését, bankszámlaszámát;

b) a szolgáltató (megbízó) nevét, székhelyét, bankszámlaszámát;

c) annak a tevékenységnek (célnak) a megnevezését, amellyel kapcsolatban a garancianyilatkozatot kiadták;

d) a bankgarancia összegét számmal és betűvel;

e) a bankgarancia kezdő és végső időpontját, a garancia lejártát, mely a végső időpontot követő harminc nap. A garanciavállaló arra vonatkozó nyilatkozatát, hogy a lejáraton belül benyújtott és a bankgarancia kezdő és végső időpontja között keletkezett fizetési kötelezettségről szóló igénybejelentéseket fogadja el;

f) a kedvezményezettként a Hatóság megnevezését;

g) a garanciavállaló feltétel nélküli kötelezettségvállalását arra vonatkozóan, hogy amennyiben a szolgáltató a Hatóságnak az Eat. 16. §-ának (4) bekezdése szerinti feladatai ellátása miatt felmerült költségeit nem fizeti ki a Hatóság erre irányuló felszólításától számított 15 napon belül, a garanciavállaló a Hatóság első írásbeli felszólítására, az alapjogviszony vizsgálata nélkül, a felszólítás kézhezvételétől számított három banki munkanapon belül a felszólításban megjelölt kincstári számlára megfizeti a szolgáltató lejárt fizetési kötelezettségét. A felszólításnak tartalmaznia kell a szolgáltató nevét és címét, a fizetési kötelezettség alapján fizetendő összeget, az előírt és a nem teljesített fizetési határidőt.

(3) A bejelentéshez mellékelt bankgarancia kezdő időpontja a szolgáltató nyilvántartásba vételének napja, illetve amennyiben a nyilvántartásba vétel iránti bejelentéstől számított 30 napon belül a szolgáltatót a Hatóság sem nyilvántartásába nem vette, sem a nyilvántartásba vételt meg nem tagadta, a nyilvántartásba vétel iránti bejelentéstől számított 30. nap. A bankgaranciának legalább a kezdő időponttól számított két évig érvényesnek kell lennie. A bankgaranciában a garanciavállalónak vállalnia kell, hogy a bankgarancia érvényességének lejártá előtt három hónappal értesítést küld a Hatóságnak, amely értesítés tartalmazza a szolgáltató nevét és székhelyét, valamint a bankgarancia lejártának idejét.

(4) A szolgáltató köteles a bankgarancia lejártát megelőző második hónap végéig igazolni a Hatóságnak, hogy a

bankgaranciát meghosszabbította vagy más pénzügyi intézménnyel az itt meghatározott követelményeknek megfelelő új szerződést kötött.

(5) A garanciavállaló jogosult a garancia összegének módosítására, illetve a lejárat meghosszabbítására. Ilyen esetben a garanciavállalás folyamatossága érdekében, a módosításnak tartalmaznia kell a garanciavállaló kötelezettségvállalását arra, hogy az előző garancia érvényességi ideje alatt keletkező fizetési kötelezettségekről szóló igénybejelentéseket 30 napon belül elfogadja.

(6) A bankgaranciában a garanciavállalónak vállalnia kell, hogy garanciavállalási kötelezettségének határidő előtti visszavonásáról hitelt érdemlő módon értesíti a kedvezményezett hatóságot. A visszavonás az értesítés kedvezményezett által, tértivevényes levélpostai küldeményként visszaigazolt tudomásra jutásától számított 30. napon léphet csak hatályba. A garanciavállaló a garanciavállalási kötelezettség alól a visszavonás hatálybalépésétől számított 30. napon mentesülhet.

14. § (1) A hitelesítés-szolgáltató a Hatóság mint jogosult javára, az Eat. 16. §-ának (4) bekezdése szerinti költségek megfizetésének biztosítására pénzügyi intézménynél óvadékot tesz le. Az óvadék összege legalább huszonötmillió forint.

(2) A Hatóság az (1) bekezdésben meghatározott óvadékból akkor kereshet kielégítést, ha a szolgáltató a Hatóságnak az Eat. 16. §-ának (4) bekezdése szerinti feladatai ellátása miatt felmerült költségeit a Hatóság erre irányuló felszólításától számított 15 napon belül nem fizette ki.

(3) Az óvadék vagy annak egy része a szolgáltatónak akkor jár vissza, ha a szolgáltató a Hatóságnak az Eat. 16. §-ának (4) bekezdése szerinti feladatai ellátása miatt felmerült költségeit kifizette, vagy ilyen költségek nem merültek fel, vagy a Hatóság az említett költségeit az óvadékból kielégítette. A költségek kifizetéséről, a költségek felmerülésének hiányáról, illetve a kielégítés megtörténtéről a Hatóság értesíti a pénzügyi intézményt.

15. § Az Eat. 16. §-ának (4) bekezdése szerinti költségek megfizetéséért hitelesítés-szolgáltató esetén legalább százmillió forint jegyzett tőkéjű európai uniós vállalkozás készfizető kezességét vállal. A kezességvállalás mértéke legalább huszonötmillió forintig terjed.

2. A szolgáltató tevékenységével kapcsolatos általános követelmények

16. § A szolgáltató szolgáltatási szabályzatának a *2. számú mellékletben* meghatározottakat is tartalmaznia kell.

Szolgáltatások rendelkezésre állásának biztosítása

17. § (1) A szolgáltatónak minősített hitelesítés-szolgáltatás esetén biztosítania kell a visszavonási nyilvántartások, a kibocsátott tanúsítványokat tartalmazó nyilvántartás és a visszavonás kezelési szolgáltatás legalább 99,9%-os rendelkezésre állását, az eseti szolgáltatás-kiesések nem haladhatják meg a három órát. Minősített időbélyegzés-szolgáltatás esetén az időbélyegzés folyamatos rendelkezésre állását biztosítani kell, az eseti szolgáltatáskiesés időtartama nem haladhatja meg a három órát.

(2) Az archiválás-szolgáltatónak biztosítania kell az őrzésében lévő érvényességi lánc, illetve a 44. § szerinti igazolások jogosultak kérésére történő folyamatos szolgáltatását. Ezen szolgáltatások eseti kiesésének időtartama nem haladhatja meg a három napot.

3. Biztonsági célú követelmények

Irányítási és ellenőrzési követelmények

18. § (1) A szolgáltatónak biztosítania kell a jogszabályoknak és szabályzatoknak megfelelő és naprakész belső irányítási és ellenőrzési eljárásrend és a kapcsolódó felelősségi rendszer folyamatos működtetését. A rendszer megfelelő működését a független rendszervizsgáló ellenőrzési tevékenysége biztosítja.

(2) A szolgáltatónak rendelkeznie kell külső, független rendszervizsgáló által folyamatosan ellenőrzött minőségirányítási és információbiztonsági irányítási rendszerrel.

(3) A szolgáltatások nyújtása során létrejövő, illetve kezelt adatokat a jogszabályok és a szolgáltatási szabályzatban meghatározott kockázatelemzés alapján biztonsági osztályokba kell sorolni, és azok megfelelő nyilvántartásáról, ellenőrzéséről és védelméről, valamint az ehhez szükséges felelősségi rendszer működtetéséről gondoskodni kell.

Személyzeti biztonsági követelmények

19. § (1) A szolgáltatónál bizalmi munkakört csak olyan személyek tölthetnek be, akiknek a bizalmi munkakör betöltéséhez szükséges befolyásmentességét és szakértelmét a minősített szolgáltató erkölcsi bizonyítvánnyal, szakmai gyakorlattal, végzettséggel és szakképesítéssel igazolni tudja.

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

(3) E rendelet alkalmazásában szakirányú felsőfokú végzettség a matematikusi, fizikusi egyetemi végzettség vagy a műszaki tudományterületre tartozó mérnöki szakon szerzett főiskolai vagy egyetemi végzettség.

20. § (1) A szolgáltató köteles biztosítani, hogy

a) a biztonsági tisztviselő és a regisztrációs felelős nem töltheti be a független rendszervizsgálói munkakört;

b) a rendszeradminisztrátor nem töltheti be a biztonsági tisztviselő és a független rendszervizsgálói munkakört;

c) az informatikai rendszerért általánosan felelős vezető nem láthatja el a biztonsági tisztviselő és a független rendszervizsgáló feladatkörét.

(2) A szolgáltatónál törekedni kell a bizalmi munkakörök teljes személyi elválasztására.

21. § (1) A bizalmi munkakört betöltő személynek munkaviszonyban kell állnia a szolgáltatóval.

(2) A bizalmi munkakört betöltő személynek minden olyan érdektől függetlennek kell lennie, amely hátrányosan érintheti a szolgáltatás megbízhatóságát és biztonságát.

(3) A hitelesítés-, illetve időbélyeg-szolgáltatónak a 2. § *aa)-af)* pontjában meghatározott bizalmi munkakörökkel kell rendelkeznie. Archiválási szolgáltatónak a 2. § *ab)-ad)* pontjában meghatározott bizalmi munkakörökkel kell rendelkeznie. A szolgáltatási szabályzatban meg kell nevezni a bizalmi munkaköröket.

(4) A szolgáltatónak gondoskodnia kell arról, hogy a szolgáltatások nyújtásával kapcsolatban álló személyek a szükséges és megfelelően naprakész tudással és tapasztalattal rendelkezzenek.

A szolgáltatói kulcspár kezelése

22. § (1) A szolgáltatói magánkulcs létrehozását, mentését és helyreállítását fizikailag védett környezetben, két bizalmi munkakört betöltő személy együttes részvételével, más személyek jelenlétét kizárva kell végezni.

(2) A szolgáltatói magánkulcsot biztonságos módon kell tárolni, és meg kell akadályozni, hogy a szolgáltatói magánkulcshoz jogosulatlan személyek hozzáférhessenek, vagy a kulcsot arra jogosulatlan személyek használhassák.

(3) Amennyiben a szolgáltató a szolgáltatói magánkulcsot többé nem kívánja használni, az lejárt vagy kompromittálódott, azt olyan módon kell megsemmisítenie, hogy a kulcs további használata lehetetlenné váljon.

(4) A tanúsítványok előállításához, a kibocsátott tanúsítványt tartalmazó nyilvántartásokhoz, a visszavonási nyilvántartáshoz, valamint időbélyegzés-szolgáltatás esetén az időbélyegzéshez használt szolgáltatói magánkulcsokat csak fizikailag védett környezetben lehet felhasználni. Az ilyen rendeltetési célú szolgáltatói magánkulcsokat csak az adott kulcsra meghatározott rendeltetési célból lehet felhasználni.

Üzemeltetési és hozzáférési biztonság

23. § (1) A szolgáltatások nyújtásához biztosítani kell a szabályozott változáskezelést és a megbízható üzemeltetést.

(2) Az üzemeltetést el kell választani a fejlesztéstől.

(3) Az informatikai rendszer minden felhasználójának és az adminisztratív folyamatok minden szereplőjének személy szerint azonosítottak kell lennie, kivéve azt a felhasználót, aki kizárólag a szolgáltatót terhelő nyilvánosságra hozatali kötelezettségek körébe eső nyilvántartásokhoz csak olvasási jogosultsággal fér hozzá.

Fizikai és környezeti biztonság

24. § (1) A szolgáltatás nyújtásával összefüggésben használt elektronikus aláírási termékeket, illetve azokat a helyiségeket, amelyekben a szolgáltató ilyen termékeket helyez el, vagy az archiválási-szolgáltató az archiválásra átvett adatokat őrzi, a jogosulatlan hozzáféréstől fizikailag is védeni kell, a jogosulatlan személyek bejutását kizárva.

(2) Meg kell akadályozni, hogy az (1) bekezdésben említett helyiségekbe olyan személyek jussanak be, akik erre nem jogosultak. A belépésre jogosultak belépésének időpontját, tartózkodásának célját, időtartamát, kilépésének

időpontját naplóban kell rögzíteni.

(3) A fizikai és környezeti biztonság komplex kezelése magába foglalja élet- és vagyonvédelem alábbi területeit is: tűz, árvíz, elárasztás, fizikai behatolás, sugárzás, áramellátás-kimaradás elleni megfelelő szintű védelem.

Elektronikus aláírási termékekre vonatkozó biztonság

25. § (1) A szolgáltatónak a szolgáltatások nyújtásához használt elektronikus aláírási termékeit elkülönítetten kell kezelnie és működtetnie az egyéb tevékenységeihez használt termékektől. Elkülönítve kell kezelnie továbbá a minősített szolgáltatások nyújtásához használt elektronikus aláírási termékeit a nem minősített szolgáltatásokhoz használt elektronikus aláírási termékektől. Az egyéb tevékenységeihez használt termékek nem befolyásolhatják az elektronikus aláírási termékek megbízható üzemeltetését.

(2) A szolgáltatások nyújtásához használt valamennyi elektronikus aláírási terméket a szabályzatban meghatározott kockázatelemzések alapján biztonsági osztályokba kell sorolni, és ezekről nyilvántartást kell vezetni.

(3) Mielőtt a szolgáltató a szolgáltatás nyújtásához használt elektronikus aláírási termékeket a saját maga által végzett szolgáltatásnyújtáson kívüli célokra kívánja felhasználni, meg kell bizonyosodnia arról, hogy a termékek nem tartalmaznak olyan adatokat, amelyek az elektronikus aláírással kapcsolatos szolgáltatásokhoz fűződnek, valamint arról, hogy az ilyen adatok visszaállítására nincsen lehetősége. E vizsgálatokat, illetve a vizsgálatok eredménye alapján végrehajtott intézkedéseket naplózni kell.

A folyamatos szolgáltatás biztosítása

26. § (1) A szolgáltatónak a rendkívüli üzemeltetési helyzetek esetére olyan eljárást kell kidolgoznia, amely lehetővé teszi a megbízható szolgáltatás mielőbbi helyreállítását.

(2) A rendkívüli üzemeltetési helyzet bekövetkezése esetén a visszavonási nyilvántartások megbízható üzemeltetésének helyreállítása minden más szolgáltatás vagy tevékenység helyreállítását meg kell, hogy előzze.

(3) Rendkívüli üzemeltetési helyzet 17. §-ban foglalt határidőn túli fennállása esetén a szolgáltató köteles haladéktalanul értesíteni a Hatóságot a rendkívüli üzemeltetési helyzet bekövetkezéséről, annak hatásáról, várható időtartamáról, a rendkívüli üzemeltetési helyzet elhárítása érdekében tett és tervezett intézkedésekről, valamint a rendkívüli üzemeltetési helyzet megszűnéséről. A szolgáltató köteles a rendkívüli üzemeltetési helyzetről és annak hatásáról közvetlenül, illetve elektronikus levél formájában értesíteni a szolgáltatást igénybe vevő mindazon személyeket, akiket a rendkívüli üzemeltetési helyzet érint, valamint az erről szóló tájékoztatást az interneten elérhetővé tenni.

27. § (1) Az üzemmenet folytonossága és az adatvesztés elkerülése végett a szolgáltatónak mentéseket kell végeznie, és biztosítania kell, hogy szükség esetén az informatikai rendszer egészét helyre tudja állítani.

(2) A mentéseket védeni kell a jogosulatlan módosítások, törlés, megsemmisülés ellen, illetve az ellen, hogy jogosulatlan személyek a mentett adatállományhoz hozzáférhessenek.

(3) A rendkívüli helyzetekre való felkészülés magában foglalja a kidolgozott tervek adott esetekre történő alkalmazását és tesztelését is.

Naplózás

28. § A szolgáltatónak minden, az informatikai rendszerével és a szolgáltatás nyújtásával kapcsolatos eseményt folyamatosan naplózni kell. A naplózott adatállománynak a szolgáltatás nyújtásának teljes folyamatát át kell fognia, és lehetővé kell tennie, hogy a valós helyzetek megítéléséhez a szükséges mértékben minden, a szolgáltatással kapcsolatos eseményt rekonstruálni lehessen.

29. § (1) A naplózott adatállománynak tartalmaznia kell a naplózott esemény bekövetkeztének dátumát és pontos idejét, az esemény követhetőségéhez, rekonstruálásához szükséges adatokat, az esemény kiváltásában közreműködő felhasználó vagy más személy nevét.

(2) A naplózott adatállomány minden bejegyzését védeni kell a módosítástól, illetve biztosítani kell, hogy a napló tartalmához csak arra feljogosított személyek férhessenek hozzá.

(3) A napló kezelését olyan módon kell megoldani, hogy kizárható legyen a napló megsemmisítése, a napló bejegyzéseinek törlése, módosítása, a bejegyzések sorrendjének bármilyen módon történő megváltoztatása. A naplóról rendszeresen mentést kell készíteni.

(4) A szolgáltatónak gondoskodnia kell a naplóadatok folyamatos értékeléséről és ellenőrzéséről.

Adatbiztonság, archiválás

30. § A szolgáltatónak gondoskodnia kell az adatvédelem és az adatbiztonság területén a jogszabálynak megfelelő működésről, a jogok, kötelezettségek és felelősségi körök meghatározásáról.

31. § (1) A szolgáltató az Eat. 9. §-ának (7) bekezdése szerinti adatokat az ott előírt határidőig, az azon kívüli naplózott adatokat a keletkezésüktől, a szolgáltatási szabályzatot és annak módosításait pedig hatályon kívül helyezésétől számított 10 évig köteles megőrizni, illetve megőrzéséről gondoskodni.

(2) Az (1) bekezdés szerint archivált adatállomány minden bejegyzését védeni kell a jogosulatlan módosítástól, törléstől, megsemmisüléstől, illetve biztosítani kell azt, hogy az adatállomány tartalmához jogosulatlan személyek ne férhessenek hozzá. Az elektronikus formában tárolt archivált adatállományt legalább fokozott biztonságú aláírással és időbélyegzővel kell ellátni.

32. § A szolgáltató köteles biztosítani, hogy mindaddig, amíg az adatokat őrzi, az adatok hitelesek, az arra jogosult személyek számára hozzáférhetőek és értelmezhetőek legyenek.

Időszinkronizáció

33. § A hitelesítés, illetve időbélyeg-szolgáltató a kibocsátott tanúsítványt tartalmazó nyilvántartásban, valamint a visszavonási nyilvántartásban, a naplókban és a kibocsátott időbélyegzésben feltüntetett időt előállító megbízható időforrását olyan gyakorisággal szinkronizálja a szolgáltatási szabályzatban megjelölt referencia időforráshoz, hogy a saját idő és a referencia időforrás közti eltérés ne haladjon meg az egy másodpercet.

4. Az egyes szolgáltatási tevékenységekre vonatkozó követelmények

Az igénylő regisztrációja

34. § (1) Az elektronikus aláírással kapcsolatos szolgáltatások iránti igényt az igénylő elektronikus úton, a szolgáltatási szabályzat által meghatározott esetekben minősített aláírással ellátott elektronikus dokumentum formájában is benyújthatja.

(2) A minősített hitelesítés-szolgáltató a minősített tanúsítvány kiállítása előtt megállapítja az előtte személyesen megjelent aláíró, és amennyiben szükséges, az igénylő vagy a nevében eljárni jogosult személyazonosságát, valamint mindazon adatok hitelességét, amelyeket a minősített tanúsítványában feltüntet.

A szerződéskötést megelőző tájékoztatási kötelezettség

35. § (1) A minősített hitelesítés-szolgáltató a szolgáltatás igénybevételére vonatkozó szerződés megkötését megelőzően köteles a tanúsítvány kibocsátását kérő személyt teljeskörűen és közérthetően az alábbiakról tájékoztatni:

- a) az aláírás-létrehozó adat használatával kapcsolatosan szükséges biztonsági intézkedésekről;
- b) az aláírás-létrehozó eszköz használatáról, amennyiben a tanúsítvány kibocsátását kérő ezt a hitelesítés-szolgáltatótól szerzi be;
- c) az aláíró és az aláírást ellenőrizni kívánó felek felelősségéről, kötelezettségeiről;
- d) a tanúsítványok visszavonásának, felfüggesztésének lehetőségéről;
- e) a tanúsítványok kibocsátásának körülményeiről;
- f) a tanúsítvány érvényességéről, érvényességi idejének lejártaáról;
- g) a szolgáltatási szabályzat tartalmáról és elérhetőségéről;
- h) a tanúsítvánnyal kapcsolatos, a tanúsítványban meghatározott tárgybeli, időbeli, földrajzi vagy egyéb korlátozásokról;
- i) a szolgáltatói nyilvános kulcsról, valamint annak elérhetőségéről;
- j) a szolgáltatási díjról;
- k) a panaszok benyújtására, a jogviták rendezésére vonatkozó szabályokról;
- l) amennyiben a szolgáltató rendelkezik önkéntes akkreditációs rendszer keretében szerzett, Eat. 8/B. §-ának (3) bekezdés szerinti tanúsítással, úgy erről a tényről.

(2) Minősített időbélyeg-szolgáltató a szolgáltatás igénybevételére vonatkozó szerződés megkötését megelőzően

köteles az igénybevevőt teljeskörűen és közérthetően tájékoztatni a szolgáltatás igénybevételének feltételeiről és az annak során követendő eljárásról.

(3) Az aláírás-létrehozó adat elhelyezést aláírás-létrehozó eszközön minősített szinten nyújtó szolgáltató a szolgáltatás igénybevételére vonatkozó szerződés megkötését megelőzően köteles az igénybevevőt teljeskörűen és közérthetően tájékoztatni az aláírás-létrehozó eszköz használatáról, valamint az aláírás-létrehozó adat védelméhez szükséges biztonsági intézkedésekről.

(4) Azon szolgáltató, amely a szolgáltatók nyilvántartásában az elektronikus archiválás szolgáltatás tekintetében minősítettként szerepel, köteles a szolgáltatás igénybevétele előtt az igénybevevőt tájékoztatni:

a) azon dokumentumformátumokról, amelyek vonatkozásában az archiválási szolgáltató vállalja az értelmezhetőség (olvashatóság) folyamatos fenntartását a szolgáltatási szabályzat szerint;

b) amennyiben az érvényességi lánc nem tartalmazza az elektronikus dokumentumot, úgy az igénybevevő azon kötelezettségéről, amely szerint a szolgáltatási szerződésben meghatározott időközönként és esetekben köteles az elektronikus dokumentumnak a Hatóság által közzétett elfogadott kriptográfiai algoritmus alkalmazásával képzett lenyomatát a szolgáltató számára átadni, valamint e kötelezettség elmulasztásának következményeiről;

c) az elektronikus aláírások hosszú távú érvényesítéséhez szükséges információk köréről, valamint annak következményeiről, ha az elektronikus aláírás hosszú távú érvényesítéséhez szükséges információk nem szerezhetők be;

d) 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;

e) amennyiben az archiválási szolgáltató az Eat. 16/M. §-ának (2) bekezdése alapján felelősségét korlátozza, úgy a felelősségkorlátozásról.

(5) A szolgáltató köteles az (1) bekezdésben megadott tájékoztatást a szerződéskötéssel egyidejűleg az igénybevevő számára írásban vagy elektronikus formában is teljesíteni, mellékelve a szolgáltatási szabályzatot is.

A tanúsítvány érvényessége és kibocsátása

36. § (1) A minősített tanúsítvány érvényességi ideje nem haladhatja meg azt az időt, amely időpontig a felhasznált kriptográfiai algoritmusok a Hatóság Eat. 18. § szerint kibocsátott határozata értelmében biztonságosan felhasználhatók, de legfeljebb a kibocsátástól számított 2 évet.

(2) A minősített hitelesítés-szolgáltató a kibocsátott minősített tanúsítvány felhasználását korlátozhatja a tanúsítványban meghatározott tárgybeli, időbeli, földrajzi vagy egyéb korlátok szerint, amennyiben a korlátozás a tanúsítványból egyértelműen kitűnik. A korlátozásról és ennek következményeiről a minősített hitelesítés-szolgáltató köteles az aláírot megfelelően tájékoztatni.

(3) A minősített tanúsítványnak tartalmaznia kell azt az időtartamot, ameddig a hitelesítés-szolgáltató az Eat. 9. §-ának (7) bekezdése szerinti feladatot a tanúsítvány vonatkozásában ellátja.

(4) A szolgáltató köteles biztosítani a tanúsítványba foglalt személyazonosító szolgáltatási körén belüli egyediségét.

A tanúsítványok visszavonása és felfüggesztése

37. § A minősített hitelesítés-szolgáltató visszavonási kérelem esetén csak azt követően vonhatja vissza, illetve függesztheti fel a tanúsítványt, hogy a kérelmező visszavonási vagy felfüggesztési jogosultságáról meggyőződött. A visszavont tanúsítvány újbóli használatba vétele nem megengedett.

38. § (1) A minősített hitelesítés-szolgáltató köteles a benyújtott visszavonási vagy felfüggesztési kérelmeket haladéktalanul, minden más típusú tevékenysége (pl. tanúsítvány előállítás, kibocsátás) elé helyezve feldolgozni, és az arra jogosult által benyújtott kérelmeket teljesíteni.

(2) Amennyiben a minősített szolgáltató az Eat. 14. §-a (1), (2) bekezdés *b)*, *c)*, *e)*, illetve *f)* pontjaiban meghatározott valamely körülményről tudomást szerez, így különösen, ha az aláíró a képviselőre nem jogosult, haladéktalanul köteles intézkedni a tanúsítvány felfüggesztéséről vagy visszavonásáról.

A visszavonási nyilvántartások

39. § (1) A tanúsítványok visszavonásának vagy felfüggesztésének a visszavont, illetőleg felfüggesztett

tanúsítványok nyilvántartásában a visszavonási vagy felfüggesztési kérelmek teljesítésével egyidejűleg meg kell jelennie.

(2) A minősített szolgáltatónak biztosítania kell, hogy a visszavont, illetőleg felfüggesztett tanúsítványok nyilvántartásában szereplő adatokat szükség esetén, így különösen a hitelesítés-szolgáltatói tevékenység befejezése esetén az arra jogosult harmadik személyek értelemzessék.

Aláírás-létrehozó adat elhelyezése aláírás-létrehozó eszközön

40. § (1) Az aláírás-létrehozó adat előállítását fizikailag védett környezetben kell végezni, kizárólag bizalmi munkakört betöltő személyek részvételével.

(2) A minősített szolgáltató az aláírás-létrehozó adatot csak a szolgáltatást igénybe vevő személy aláírás-létrehozó eszközében tárolhatja. Amennyiben az aláírás-létrehozó adatot az aláírás-létrehozó eszközön kívül hozzák létre, az aláírás-létrehozó adat aláírás-létrehozó eszközön kívüli minden másolatát azonnal törölni kell, amint az aláírás-létrehozó adat az aláírás-létrehozó eszközbe kerül. Az aláírás-létrehozó adat másolatát olyan módon kell törölni, hogy a törölt másolat további használata lehetetlenné váljon.

(3) A minősített szolgáltatónak biztosítania kell, hogy az aláírás-létrehozó adathoz mások ne férhessenek hozzá.

(4) A minősített szolgáltató az aláírás-létrehozó eszköz használatához szükséges, az aláíró hozzáférési jogosultságát ellenőrző adatot (pl. PIN-kódot) csak abból a célból rögzítheti, hogy azt a szolgáltatást igénybe vevő személy számára - másolat megőrzése nélkül - átadhassa.

(5) A minősített szolgáltató az aláírás-létrehozó eszközt, valamint az aláíró hozzáférési jogosultságát ellenőrző adatot csak közvetlenül az azt igénylő személynek adhatja át. A minősített szolgáltatónak azt is naplózni kell, hogy az aláírás-létrehozó adatot mikor adta át az azt igénylő személynek.

Az elektronikus dokumentumok átvétele elektronikus archiválás szolgáltatás során

41. § (1) Az elektronikus dokumentumok átvételét megelőzően az igénybevevő számára a szolgáltatási szabályzatban meghatározott módon azonosítási lehetőséget kell biztosítani. Az azonosítás az igénybevevő egyedi azonosítását lehetővé tévő bármely módon, álnév, tanúsítvány vagy egyéb azonosító alkalmazásával is történhet.

(2) Az archiválási szolgáltató az elektronikus aláírás hosszútávú érvényesítéséhez szükséges információkat köteles haladéktalanul, de legfeljebb három naptári napon belül beszerezni.

Az elektronikus dokumentumok megőrzése

42. § (1) A szolgáltatási szabályzatban meghatározott formátumokban átadott elektronikus dokumentumok olvashatóságának és megjeleníthetőségének folyamatos fenntartása érdekében az archiválási szolgáltató a szerződésben, illetve az archiválási szabályzatban meghatározott megőrzési ideig köteles biztosítani az adathordozók olvashatóságát és a dokumentumok megjeleníthetőségét biztosító szoftver- és hardverkönyezetet.

(2) Az (1) bekezdésben meghatározottak érdekében az archiválási szolgáltató köteles a szolgáltatási szabályzat részeként archiválási szabályzatot alkotni.

Az archiválási szolgáltató által kiállított igazolások

43. § (1) Az archiválási szolgáltató az igénybevevő számára igazolást köteles kiadni az alábbi tényekről:

- a) a megőrzésében lévő elektronikus dokumentumon elhelyezett fokozott biztonságú vagy minősített elektronikus aláírás vagy időbélyegző, illetve az azokhoz kapcsolódó tanúsítvány az időbélyegzés időpontjában érvényes volt;
- b) a megőrzésében lévő lenyomathoz kapcsolódó fokozott biztonságú vagy minősített elektronikus aláírás vagy időbélyegző, illetve az azokhoz kapcsolódó tanúsítvány az aláírás és időbélyegzés időpontjában érvényes volt;
- c) a megőrzésében lévő, az érvényességi lánc részét képező elektronikus dokumentum tartalma megegyezik az igénybevevő által bemutatott elektronikus dokumentummal;
- d) a megőrzésében lévő, az érvényességi lánc részét képező lenyomat megegyezik az igénybevevő által bemutatott elektronikus dokumentum lenyomatával;
- e) a megőrzésében lévő, az érvényességi lánc részét képező elektronikus dokumentum, amelynek tartalma megegyezik az igénybevevő által bemutatott elektronikus dokumentummal, meghatározott személy érvényes

elektronikus aláírást helyezett el;

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

(2) Az (1) bekezdésben meghatározott tényekről együttes igazolás is kiadható.

(3) Az igazolás harmadik személy számára is kiadható, amennyiben a kérelméhez csatolja az igénybevevő teljes bizonyító erejű magánokiratba foglalt meghatalmazását.

(4) Ha az igazolást az archiválási szolgáltató elektronikus úton állítja ki, úgy az elektronikus dokumentumon minősített elektronikus aláírást kell elhelyeznie, valamint minősített szolgáltató által kibocsátott időbélyegzőt elhelyeznie vagy elhelyeztetnie.

Az archiválási szolgáltató törlési kötelezettsége

44. § A szolgáltatási szerződés megszűnése vagy az igénybevevő ilyen rendelkezése esetén az archiválási szolgáltató köteles az érvényességi láncot visszaállíthatatlan módon törölni informatikai rendszeréből.

III. Fejezet

Záró rendelkezések

45. § (1) Ez a rendelet 2005. április 1-jén lép hatályba.

(2)

Az Európai Unió jogának való megfelelés

46. § Ez a rendelet az elektronikus aláírásról szóló 2001. évi XXXV. törvénnyel, valamint a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással kapcsolatos feladat- és hatásköréről, valamint eljárásának részletes szabályairól szóló jogszabállyal együtt az Európai Parlament és a Tanács, az elektronikus aláírásra vonatkozó közösségi keretfeltételekről szóló 1999/93/EK irányelvének való megfelelést szolgálja.

1. számú melléklet a 3/2005. (III. 18.) IHM rendelethez

A Hatóságnál bejelentésre kötelezett, elektronikus aláírással kapcsolatos szolgáltatást nyújtó szolgáltató szolgáltatási szabályzatának az alábbiakat kell tartalmaznia:

a) a szolgáltató székhelyének, telephelyének postacímét és telefonszámát, illetve a szolgáltató elérhetőségének egyéb távközlési azonosítóját;

b) a szolgáltató cégjegyzékszámát, illetve a szolgáltató egyéni vállalkozó vállalkozói igazolványának számát;

c) a szolgáltató fokozott biztonságú szolgáltatókénti, illetve minősített szolgáltatókénti nyilvántartásba vételének napját a Hatóság erről szóló határozata szerint, e határozat közzétevése előtt a nyilvántartásba vétel meg nem történtének feltüntetését;

d) a szolgáltatási szabályzat változatának azonosítóját (verziószámát);

e) a szolgáltatási szabályzat hatálybalépését és hatályának a megszűnését;

f) a szolgáltató által a szolgáltatás nyújtásához használt elektronikus aláírási termékek megnevezését, valamint a szolgáltató nyilatkozatát arról, hogy ezek az elektronikus aláírási termékek rendelkeznek az Eat. 7. §-ának (5) bekezdése, illetve az Eat. 7. §-ának (6) bekezdése szerinti igazolással;

g) utalást arra, hogy a szolgáltató az Eat. 8/B. § szerinti önkéntes akkreditációs rendszer keretében tanúsítva lett-e;

h) a szolgáltató tevékenységével kapcsolatos kifogások és panaszok bejelentésének helyét és módját, a szolgáltatói ügyfélszolgálat és az illetékes fogyasztóvédelmi felügyelőség elérhetőségét;

i) a szolgáltató által vállalt egyes nyitvatartási és rendelkezésre állási időket (a továbbiakban: rendelkezésre állási idők): a kibocsátott tanúsítványt tartalmazó nyilvántartás, valamint a visszavonási nyilvántartás, és a visszavonás kezelési szolgáltatások rendelkezésre állási idejét;

j) tájékoztatást a szolgáltató által nyújtott szolgáltatásokról és azok felhasználásának módjáról;

k) tájékoztatást a hitelesítés-, illetve időbélyeg-szolgáltató által kibocsátott hitelesítési, illetve időbélyegzési

rendekről és az azok alapján kiadott tanúsítványok joghatásairól, a tanúsítványok felhasználásának feltételeiről, az aláíró és az ellenőrző feleket terhelő kötelezettségekről;

l) tájékoztatást a tanúsítvány érvényességének lejárt előtti visszavonásának jogkövetkezményeiről;

m) adatkezelési szabályzatot, amely összefoglaló jellegű tájékoztatást ad a szolgáltató által kezelt adatok fajtájáról, az adatkezelés céljáról, a továbbított adatok fajtájáról, címzettjéről, az adattovábbítás jogalapjáról, valamint az egyes adatfajták törlési határidejéről.

2. számú melléklet a 3/2005. (III. 18.) IHM rendelethez

Azon hitelesítés-, illetve időbélyeg-szolgáltató szolgáltatási szabályzatának, amely valamely szolgáltatását minősítettként nyújtja, az 1. számú mellékletben foglalt előírásokon kívül az alábbiakat is tartalmaznia kell, a hitelesítési, időbélyegzési rendenkénti eltéréseket feltüntetve:

a) annak a leírását, hogy a szolgáltató miként biztosítja a szolgáltatási szabályzatban előírt folyamatos rendelkezésre állást;

b) annak a leírását, hogy ha a szolgáltató a hitelesítés-szolgáltatói tevékenységét befejezi, milyen módon fog megfelelni az Eat. 16. §-ában foglalt előírásoknak;

c) annak a leírását, hogy a szolgáltató

ca) milyen módon felel meg az üzemeltetési és hozzáférési biztonsági követelményeknek,

cb) milyen termékeket használ a szolgáltatás nyújtásához, illetve ahhoz, hogy az üzemeltetési és hozzáférési biztonsági követelményeknek megfeleljen,

cc) miként kívánja az üzemeltetés során előforduló hibákat, így különösen a karbantartási és telepítési hibákat elkerülni,

cd) az üzemeltetés ellenőrzéséhez milyen eljárásokat alkalmaz,

ce) miként teljesíti az e rendelet 31. §-ában foglalt megőrzési kötelezettségét;

d) annak a leírását, hogy az informatikai rendszer felhasználóinak milyen hozzáférési jogosultsággal kell rendelkezniük ahhoz, hogy az informatikai rendszerben bizonyos tevékenységeket elvégezhesenek;

e) a rendkívüli üzemeltetési helyzet esetén követendő eljárás leírását;

f) annak a leírását, hogy az igénylő milyen esetben nyújthatja be igénylését minősített elektronikus aláírással ellátott elektronikus dokumentum formájában;

g) annak a leírását, hogy a szolgáltató az igénylő visszavonási vagy felfüggesztési jogosultságáról milyen módon győződik meg;

h) annak a leírását, hogy milyen feltételei vannak a visszavonási, illetve felfüggesztési kérelem benyújtásának;

i) annak a leírását, hogy a szolgáltató milyen eljárási rend szerint teljesíti a visszavonás kezelési szolgáltatások iránti kérelmeket;

j) a tanúsítványok kibocsátása, valamint a visszavonás kezelési- és aláírás-létrehozási szolgáltatások kapcsán alkalmazott adatformátumokat, azaz a szolgáltatói magán- és nyilvános kulcs és az aláírás-létrehozó adat formátumát, a kibocsátott tanúsítványok formátumát, a visszavonási és felfüggesztési kérelem formátumát;

k) a kibocsátott tanúsítványok leghosszabb érvényességi idejét;

l) a hitelesítés-szolgáltató által kibocsátott egyes hitelesítési rendekhez a Hatóság által kijelölt azonosítót;

m) a szolgáltatói magánkulcsok létrehozásának módját és a kulcsok létrehozásának eljárási rendjét;

n) az aláírás-létrehozó adatok létrehozásának módját, és adatok létrehozásának eljárási rendjét;

o) a szolgáltató által alkalmazott referencia időforrások megnevezését, azok pontosságát és az időszinkronizáció menetének ismertetését;

p) a bizalmi munkakörök megnevezését és leírását.

Azon archiválási szolgáltató szolgáltatási szabályzatának, amely valamely szolgáltatását minősítettként nyújtja, az 1. számú mellékletben foglalt előírásokon kívül az alábbiakat is tartalmaznia kell:

a) a szolgáltató által vállalt egyes nyitvatartási és rendelkezésre állási időket;

b) tájékoztatást a szolgáltató által nyújtott szolgáltatásokról és azok felhasználásának módjáról;

c) az igénybevevővel való együttműködés szabályait abban az esetben, ha a szolgáltató által megőrzött érvényességi láncnak az elektronikus dokumentum nem része, így azon időtartam és események meghatározását, amely eltelte vagy amelyek beállta esetén az igénybevevő köteles az elektronikus dokumentumnak a Nemzeti Hírközlési Hatóság által meghatározott elfogadott kriptográfiai algoritmus alkalmazásával képzett lenyomatát az archiválási szolgáltató számára átadni;

d) archiválási szabályzatot, amely tartalmazza azon dokumentumformátumok felsorolását, amelyek vonatkozásában az archiválási szolgáltató vállalja az értelmezhetőség (olvashatóság) és megjeleníthetőség folyamatos fenntartását, az értelmezhetőség és megjeleníthetőség biztosítását szolgáló eljárásrendet, ideértve a hardver- és

szoftvereszközök rendelkezésre állásának biztosítására (emuláció) vonatkozó szabályokat, illetve az új adathordozóra vagy új formátumba történő átvitel (migráció) kapcsolatos eljárásrendet is, valamint az ezen dokumentumformátumokban őrzött dokumentumokkal kapcsolatban a szolgáltató működésének befejezése esetén követendő eljárást;

e) a kárviselés szabályait és az Eat. 16/M. §-ának (2) bekezdésében meghatározott felelősségkorlátozást;

f) részletes adatkezelési szabályzatot, amely szabályozza a szolgáltató minden személyes adatkezelését, rögzíti azok célját, jogalapját és a törlési határidőket, a megkeresésekről szóló nyilvántartás vezetését, a megkeresések teljesítésekor követendő eljárást;

g) az igazolások kiadása során követett eljárást;

h) annak a leírását, hogy a szolgáltató miként biztosítja a szolgáltatási szabályzatban előírt folyamatos rendelkezésre állást;

i) annak a leírását, hogy a szolgáltató

ia) milyen módon felel meg az üzemeltetési és hozzáférési biztonsági követelményeknek,

ib) milyen termékeket használ a szolgáltatás nyújtásához, illetve ahhoz, hogy az üzemeltetési és hozzáférési biztonsági követelményeknek megfeleljen,

ic) miként kívánja az üzemeltetés során előforduló hibákat, így különösen a karbantartási és telepítési hibákat elkerülni,

id) az üzemeltetés ellenőrzéséhez milyen eljárásokat alkalmaz;

j) annak a leírását, hogy az informatikai rendszer felhasználóinak milyen hozzáférési jogosultsággal kell rendelkezniük ahhoz, hogy az informatikai rendszerben bizonyos tevékenységeket elvégezzenek;

k) a rendkívüli üzemeltetési helyzet esetén követendő eljárás leírását;

l) a bizalmi munkakörök nevesítését és leírását;

m) az igénybevevő azonosítására szolgáló eljárást.