Digitoll Informatikai és Szolgáltató Kft.
1124 Budapest, Stromfeld Aurél út 9.
Tel.: +361 487 9900
E-mail: digitoll@digitoll.co.hu
Web: www.digitoll.co.hu

Szolgáltatási Szabályzat

Fokozott biztonságú elektronikus aláíráshoz és bélyegzőhöz kapcsolódó bizalmi szolgáltatásokhoz, nem minősített időbélyegzés szolgáltatáshoz és nem minősített weboldal-hitelesítés szolgáltatáshoz

Egyedi objektum-azonosító (OID): 1.3.6.1.4.1.46800.1.1.1.6
Verziószám: 1.6
Jóváhagyta: Németh Viktor Péter
Jóváhagyás dátuma: 2016.08.12.
Hatályba lépés dátuma: 2016.08.24.

1124 Budapest, Stromfeld Aurél út 9.
Tel.: +361 487 9900
E-mail: digitoll@digitoll.co.hu
Web: www.digitoll.co.hu

Változáskövetés

Verzió	A változás leírása	Hatálybalépés	Készítette
1.0	Első változat	2011.05.10.	Németh Ágnes Krisztina Németh Viktor Péter
1.1	Módosítás a NMHH észrevételeinek megfelelően	2011.07.10.	Németh Ágnes Krisztina Németh Viktor Péter
1.2	Technikai paraméter változások az NMHH észrevételeinek megfelelően	2011.07.10.	Németh Ágnes Krisztina Németh Viktor Péter
1.3	Módosítások a 2013. évi NMHH felügyeleti eljárás határozata alapján. Felfüggesztési ügyelet (korábban: Visszavonási ügyelet) megnevezése és telefonszáma módosult. A tanúsítvány profilok kiegészítésre kerültek.	2013.10.10.	Németh Ágnes Krisztina Németh Viktor Péter
1.4	Aktualizálás	2015.03.01.	Németh Ágnes Krisztina Németh Viktor Péter
1.5	eIDAS és változó törvényi hátterek szerinti módosítás, aktualizálás. Ügyfélszolgálati elérhetőségek módosultak. Változik a dokumentum neve és OID-ja is.	2016.07.01.	Németh Ágnes Krisztina Németh Viktor Péter
1.6	Módosítás Hatósági észrevételek alapján	2016.08.12.	Németh Ágnes Krisztina Németh Viktor Péter

1124 Budapest, Stromfeld Aurél út 9.
Tel.: +361 487 9900
E-mail: digitoll@digitoll.co.hu
Web: www.digitoll.co.hu

Tartalomjegyzék

1. Általános információ

Jelen dokumentum a Digitoll Informatikai és Szolgáltató Kft (továbbiakban: Szolgáltató) nem minősített bizalmi és időbélyegzés szolgáltatására vonatkozó Szolgáltatási Szabályzata (továbbiakban: Szabályzat). E dokumentum a Szolgáltató szolgáltatásaira vonatkozó eljárási és működési szabályokat tartalmazza, és ajánlásokat fogalmaz meg a szolgáltatások segítségével létrehozott elektronikus aláírások és időbélyegzők ellenőrzésében Érintett felek számára.

A Szolgáltató szolgáltatásait a vele szerződéses viszonyban álló ügyfelek részére (továbbiakban: Ügyfél) biztosítja, a szolgáltatások felhasználója a tanúsítvány alanya (továbbiakban: Alany) és/vagy az elektronikus bélyegző létrehozója.

A Szolgáltató felügyeleti szerve a Nemzeti Média- és Hírközlési Hatóság (továbbiakban: Bizalmi felügyelet).

Szolgáltató bizalmi szolgáltatásait 2016.07.06.-án jelentette be a Bizalmi felügyeletnek, mint nem minősített bizalmi szolgáltató.

A Bizalmi felügyelet nyilvántartásainak elérhetősége:
http://nmhh.hu/

Jelen Szabályzat tartalmi vonatkozásokban eleget tesz a 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól (továbbiakban: E-ügyintézési tv.), a 2014. július 23-i 910/2014/EU európai parlamenti és tanácsi rendeletben (továbbiakban: eIDAS) foglaltaknak, és egyéb jogszabályok előírásainak és ajánlásainak.

1.1. Szolgáltató adatai

Név:	Digitoll Informatikai és Szolgáltató Kft.
Cégjegyzék szám:	01-09-861809
Székhely:	1124 Budapest, Stromfeld Aurél út 9.
Ügyfélszolgálati iroda:	1113 Budapest, Bartók Béla út 152/H
Nyitva tartás:	Munkanapokon 8:30 – 15:30 óra között
Telefonszám:	(+36-1) 487 9900
Felfüggesztési ügyelet (0-24):	(+36-1) 487 9978
Email cím:	ugyfelszolgalat@digitoll.co.hu digitoll@digitoll.co.hu
Internet cím:	http://www.digitoll.co.hu http://ds.digitoll.co.hu

1124 Budapest, Stromfeld Aurél út 9.
Tel.: +361 487 9900
E-mail: digitoll@digitoll.co.hu
Web: www.digitoll.co.hu

1.2. Bizalmi szolgáltatások

A Szolgáltató az alábbi bizalmi szolgáltatásokat (továbbiakban: Szolgáltatás) illetve tevékenységeket nyújthatja, illetve végezheti a bizalmi szolgáltatási ügyfelei (továbbiakban: Ügyfél) részére, jelen Szabályzat keretein belül:

- Nem minősített elektronikus aláírás szolgáltatás;
- Nem minősített elektronikus bélyegző szolgáltatás;
- Nem minősített weboldal - hitelesítés szolgáltatás;
- Nem minősített időbélyegzés szolgáltatás.

1.2.1. *Nem minősített elektronikus aláírás szolgáltatás*

A fokozott biztonságú elektronikus aláírásnak az alábbi követelményeknek kell megfelelnie:

- kizárólag az aláíróhoz köthető;
- alkalmas az aláíró azonosítására;
- olyan, elektronikus aláírás létrehozásához használt adatok felhasználásával hozzák létre, amelyeket az aláíró nagy megbízhatósággal kizárólag saját maga használhat;
- olyan módon kapcsolódik azokhoz az adatokhoz, amelyeket aláírtak vele, hogy az adatok minden későbbi változása nyomon követhető.

Az elektronikus aláírás joghatása és bírósági eljárásokban bizonyítékként való elfogadhatósága nem tagadható meg kizárólag amiatt, hogy az elektronikus formátumú, illetve nem felel meg a minősített elektronikus aláírásra vonatkozó követelményeknek.

Az elektronikus aláírás szolgáltatás keretében az alábbi szolgáltatásokat tartalmazza (a megnevezett szolgáltatások együtt értelmezendőek):

- Regisztráció, személyazonosság megállapítása,
- Tanúsítvány igénylés feldolgozása,
- Tanúsítvány-menedzselés:
    - Tanúsítvány kibocsátás,
    - Tanúsítvány felfüggesztés és visszavonás kezelés,
    - Tanúsítvány megújítás,
    - Tanúsítvány közzététel.

1.2.1.1. Tanúsítványfajták

A Szolgáltató a nem minősített bizalmi szolgáltatás keretében többféle tanúsítványfajtát bocsát ki, mely különbözhet felhasználási körben, alkalmazásban és felelősségvállalásban is.

A tanúsítvány fajtája jelölve van a kibocsájtott tanúsítványon és a Szolgáltatási szerződésben.

A tanúsítvány profilok megtalálhatóak a jelen szabályzat és a kapcsolódó Bizalmi Rendjének idevonatkozó pontjában.

A nem minősített tanúsítványok igen erős biztosítékokkal szolgálnak a bennük megnevezett személyek kilétét illetően, mivel ez esetben az igénylő személyes megjelenése a regisztrációs egységnél követelmény. A Szolgáltató a nem minősített tanúsítványokat fokozott biztonságú elektronikus aláíráshoz és bélyegzőhöz valamint ezen alapuló aláíró azonosításhoz bocsátja ki, magasabb értékű, illetve hosszú időre biztonságot követelő szerződések, kereskedelmi tranzakciók, alkalmazások (elektronikus levelezés, intranet, extranet, on-line vásárlás stb.) esetében.

A pénzügyi felelősségvállalás mértékét a Szolgáltatási szerződés tartalmazza.

1.2.2. *Nem minősített elektronikus bélyegző szolgáltatás*

A fokozott biztonságú elektronikus bélyegzőnek az alábbi követelményeknek kell megfelelnie:

- kizárólag a bélyegző létrehozójához kötött;
- alkalmas a bélyegző létrehozójának azonosítására;
- olyan, elektronikus bélyegző létrehozásához használt adatok felhasználásával hozzák létre, amelyeket a bélyegző létrehozója nagy megbízhatósággal kizárólag saját maga elektronikus bélyegző létrehozására használhat;
- olyan módon kapcsolódik azokhoz az adatokhoz, amelyekre vonatkozik, hogy az adatok minden későbbi változása nyomon követhető;

Az elektronikus bélyegző joghatása és bírósági eljárásokban bizonyítékként való elfogadhatósága nem tagadható meg kizárólag amiatt, hogy az elektronikus formában létezik, illetve nem felel meg a minősített elektronikus bélyegzőkre vonatkozó követelményeknek.

Az elektronikus bélyegző igazolja, hogy az elektronikus dokumentumot jogi személy bocsátotta ki, biztosítva a dokumentum eredetének és sértetlenségének bizonyosságát.

Az elektronikus bélyegző, jogi személy elektronikus aláírása. Bizalmi szolgáltatás keretében az alábbi szolgáltatásokat tartalmazza (a megnevezett szolgáltatások együtt értelmezendőek):

- Regisztráció, személyazonosság megállapítása,
- Tanúsítvány igénylés feldolgozása,
- Tanúsítvány-menedzselés:
  - Tanúsítvány kibocsátás,
  - Tanúsítvány felfüggesztés és visszavonás kezelés,
  - Tanúsítvány megújítás,
  - Tanúsítvány közzététel.

Mivel az elektronikus bélyegző jogi személy aláírása, így a bélyegzővel elkövetett esetleges visszaélések miatt okozott károkért az előfizető szervezet (jogi személy) felelős vezetője a felelős.

1.2.1. *Nem minősített weboldal - hitelesítő szolgáltatás*

Szerver tanúsítvány szolgáltatás keretében Szolgáltató egy domain névvel (egy címmel) rendelkező web szerver vagy oldal részére bocsát ki hitelesítő (autentikációs) tanúsítványt, mely a titkosított, biztonságos és hitelesített kapcsolatok létrehozását segíti elő. A tanúsítványban egy cím szerepelhet.

Wildcard szerver tanúsítvány szolgáltatás keretén belül Szolgáltató web szerverek fő- és aldomainjára (fő- és alcímére) bocsát ki autentikációs tanúsítványt, mely a titkosított, biztonságos és hitelesített kapcsolatok létrehozását segíti elő. A tanúsítványban a fődomain szerepel joker karakterrel (Pl.: *.digitoll.co.hu).

Jelen szolgáltatás alkalmazható egyéb eszközök valamint kapcsolatok azonosítására is.

1.2.2. *Nem minősített időbélyegzés szolgáltatás*

Jelen Szabályzat 5.10. pontja szerint.

2. Bevezetés

2.1. Áttekintés

2.1.1. *A Szabályzat célja, használhatósága, leírása*

Jelen Szabályzat célja, hogy a Szolgáltatóval kapcsolatba kerülő felek, a Szolgáltató által nyújtott Szolgáltatásokról, azok működéséről, feltételeiről teljes áttekintést kapjanak, mely

elősegíti a Szolgáltató működésének és az általa nyújtott Szolgáltatások gyakorlati hátterének megismerését.

A Szabályzat összefoglalóan tartalmazza mindazon szabályokat, információkat, melyek a Szolgáltató bizalmim szolgáltatás keretein belül kibocsátott tanúsítványokkal és egyéb kapcsolódó szolgáltatásokkal kapcsolatosak, és melyeket a Szolgáltatóval kapcsolatba kerülő felhasználóknak és érintett feleknek érdemes tudni. Biztosítja a Szolgáltató működésének átláthatóságát, és lehetővé teszi a felhasználók számára, hogy megállapítsák, hogy a Szolgáltató működése, illetve adott Szolgáltatás mennyiben felel meg elvárásaiknak, igényeiknek. A Szabályzat megismerésével és értelmezésével, a tanúsítvány felhasználói egyértelműen meg kell, tudják állapítani a tanúsítvány kezelésének módját, az általa garantált biztonság és garancia mértékét és az erre vonatkozó technikai, üzleti és pénzügyi garanciákat, jogi felelősségvállalásokat.

Az igénybe vehető Szolgáltatásokkal kapcsolatos előírásokat tartalmazhat jelen Szabályzaton kívül, a mindenkori Általános Szerződési Feltételek (továbbiakban: ÁSzF), a Bizalmi Rend, az Időbélyegzési rend, a Szolgáltatási szerződés (továbbiakban: Szerződés), vagy bármilyen írásos szabályzat illetve megállapodás a Szolgáltató és az igénybevevő között, illetve egyéb, a Szolgáltatótól független dokumentum vagy szabályzat is.

2.1.2. *A Szabályzat hatálya*

2.1.2.1. Tárgyi hatálya

A Szabályzat tárgyi hatálya az 1.2. fejezetben ismertetett Szolgáltatások nyújtására és igénybevételére, illetve e Szolgáltatásokkal kapcsolatos tárgyi eszközökre terjed ki.

2.1.2.2. Időbeli hatálya

A Szabályzat időbeli hatálya jelen dokumentum hatályba lépésének dátumától kezdődik és annak módosításáig, vagy visszavonásáig, illetve a Szolgáltatások beszüntetéséig érvényes. Jelen szabályzatot verziószám és egyedi objektum-azonosító (Object Identifier - OID) alapján lehet azonosítani. A verziószám, az OID és a hatálybalépés dátuma jelen dokumentum címlapján olvasható. Változtatás esetén új verziószámos dokumentum jön létre.

2.1.2.3. Személyi hatálya

A Szolgáltató a Szolgáltatásokat a vele előfizetői szerződéses viszonyban álló Ügyfelek részére szolgáltatja. A Szabályzat személyi hatálya a Szolgáltató PKI közösségének minden tagjára (jogi

vagy nem jogi személyiségekre is), a felhasználó közösségre (Aláíró, Ellenőrző fél) és az Ügyfélre egyaránt kiterjed.

2.2. Dokumentum név és azonosító

Jelen Szabályzat hivatalos elnevezése: Digitoll Informatikai és Szolgáltató Kft. Fokozott biztonságú elektronikus aláíráshoz és bélyegzőhöz kapcsolódó bizalmi szolgáltatás és nem minősített időbélyegzés szolgáltatás Szolgáltatási Szabályzata.

Jelen a Szabályzatot az OID azonosítja, ami megfelel a vonatkozó szabványoknak és ajánlásoknak. Az OID és a Szabályzat egyéb paraméterei jelen Szabályzat fedőlapján olvashatóak.

Jelen dokumentum korábbi verziói Szolgáltatási Szabályzat néven érhetőek el elektronikusan a Szolgáltató dokumentum tárában a http:/ds.digitoll.co.hu/ internetes címen.

A Szolgáltatásokat a Szolgáltató jelen Szolgáltatási Szabályzatban, a hozzá elválaszthatatlanul kapcsolódó Általános Szerződési Feltételekben (ÁSZF), a Bizalmi Szolgáltatási Rendben (Bizalmi Rend), és az Időbélyegzési Rendben leírtak szerint nyújtja. A nem minősített időbélyegzés szolgáltatásra vonatkozó, a Bizalmi Rendben nem taglalt szabályozásait, feltételeit az Időbélyegzési Rend tartalmazza.
Szolgáltató szabályzatai elérhetőek a Szolgáltató ügyfélszolgálati irodájában, vagy elektronikusan a http:/ds.digitoll.co.hu/ internetes címen.

2.3. PKI résztvevők

A Szolgáltató Szolgáltatásaihoz tartozó közösség, a Szolgáltatóból, a végfelhasználókból (Ügyfelek, Aláírók) és az Érintett felekből áll.

2.4. Hitelesítő egység - CA (Certification Authority)

A Szolgáltató, saját egységén belül Hitelesítő egységet működtet, melynek fő feladata a Regisztrációs egységhez benyújtott kérelmek, a Szolgáltató saját szabályozásának, a magyar és az Európai Unió jogszabályainak megfelelően a tanúsítványok - előre definiált profilok alapján - előállítása, kibocsátása, menedzselése (visszavonás, felfüggesztés), azok közzététele. Szintén ez az egység végzi és felügyeli az időbélyegzés szolgáltatást, a kulcsgenerálást, a kulcstároló eszközök menedzselését, és a Szolgáltató szabályzatainak kialakítását, publikálását, valamint a visszavonási listák (CRL) kiadását és publikálását.

A rendszer a gyökérelemből (Root CA), illetve az alátartozó időbélyegzőből (TSA) áll. A gyökérelem bocsátja ki a felhasználói végtanúsítványokat (user), illetve visszavonási adatokat (CRL). A gyökérelem és az időbélyegző a bizalmi szolgáltatói oldal, a végfelhasználói tanúsítványok felhasználói oldal részét képezik.

A gyökérelem lenyomata:

- SHA-1:
  E3 : E5 : AE : F8 : 59 : 9A : 07 : AB : 55 : 0A : 19 : 85 :
  31 : CF : BB : 3A : 36 : EA : 95 : FD
- SHA-256:
  76 : 5B : 27 : 1C : 5E : 01 : 9C : 01 : 5B : 7A : D3 : E8 :
  F6 : 10 : 30 : E8 : E5 : 11 : 25 : FF : 28 : 6E : 3D : 68 :
  C1 : 54 : F0 : CF : 81 : AF : AC : 7D

Az időbélyegző lenyomata:

- SHA-1:
  56 : 0A : 17 : E7 : D4 : 69 : 4A : 80 : 8B : 32 : C8 : DC :
  C3 : 6B : E5 : 66 : AA : 9F : C8 : 3F
- SHA-256:
  07 : 8E : BB : EF : 9C : 18 : 69 : 89 : 33 : 89 : 37 : D6 :
  71 : F2 : B1 : 99 : 98 : 59 : C4 : E3 : D0 : 91 : DC : BC :
  21 : 0D : 59 : 46 : 02 : AF : 51 : 26

2.5. Regisztrációs egységek- RA (Registration Authority)

A Szolgáltató, saját szervezetén belül Regisztrációs egységet működtet, melynek feladata az ügyfélkezelés, mely a kezdeti regisztrációból és tanúsítványokkal kapcsolatos egyéb feladatok elvégzéséből és az ügyfelekkel való kommunikációból áll.

Ezek a feladatok részletezve:

- Regisztrációs tevékenységek, kezdeti regisztráció:
  - Tanúsítványigénylések fogadása, feldolgozása és elbírálása,
  - Az Ügyfél és az Alany azonosítása (okmányok alapján),
  - Az Ügyfél és az Alany író adatainak ellenőrzése,
  - Szerződéskötés,
  - Adatok átadása a Hitelesítő egységnek.

- Tanúsítványokkal kapcsolatos feladatok:

- Az aláírás létrehozó adat és az aláírás ellenőrző adat generálásának felügyelete
- A CA-tól lekért tanúsítvány elhelyezése az aláírást-létrehozó eszközön (továbbiakban: ALE), vagy letöltési helyen
- A kész tanúsítvány, aláíró-eszközök átadása az Ügyfélnek és/vagy Alanynak,
- Az aláírás létrehozó adat aktiválása,
- Az előfizetői kérelmek, módosítások fogadása, feldolgozása és elbírálása,
- Tanúsítványokkal kapcsolatos műveletek (felfüggesztés, visszavonás, visszaállítás csere) elvégzése, dokumentálása,
- Tanúsítvány-állapotszolgáltatáshoz és Időbélyeg szolgáltatáshoz kapcsolódó adminisztrációs tevékenység,
- Egyéb adminisztráció, dokumentálás,
- Kapcsolattartás, panaszkezelés.

A Regisztrációs egység regisztrációs tevékenységet végezhet:

- A Szolgáltató ügyfélszolgálati irodájában,
- Külön díjazás ellenében és előre egyeztetett időpontban az ügyfél által megjelölt helyszínen.

A Szolgáltató egyéb szervezetekkel szerződést köthet külső Regisztrációs helyek kialakítására, melyeknek önálló működési szabályzata van, melyet a Szolgáltató elfogad. A külső Regisztrációs egység szabályzatának tartalmilag és felelősségvállalás szempontjából is összhangban kell lennie a Szolgáltató szabályzataival, valamint meg kell felelnie a vonatkozó magyar jogszabályi feltételeknek.

2.6. Végfelhasználók

A Szolgáltató által nyújtott Szolgáltatások végfelhasználói a következőek lehetnek:

- Az Előfizető, aki Szerződést köt a Szolgáltatóval, az általa nyújtott szolgáltatásokra. Az Ügyfél határozza meg a Szolgáltatásokat igénybe vevő Aláírók körét, és megfizeti az igénybe vett Szolgáltatások díjait. A kibocsátott tanúsítvány és az ahhoz tartozó kulcspár tulajdonosa, web tanúsítvány esetén a tanúsítványban megjelölt domain név tulajdonosa. Az Ügyfél lehet természetes illetve jogi személy, vagy jogi személyiség nélküli szervezet, vagy képviselője (meghatalmazottja).
- A tanúsítvány alanya (Alany), aki a kibocsátott aláíró tanúsítványhoz tartozó kulcspár teljes jogú, kizárólagos használója. Az aláíró elektronikus aláírás esetén csak természetes személy lehet.

- Elektronikus bélyegző létrehozója, aki a kibocsátott tanúsítvánnyal elektronikus bélyegzőt hoz létre. Az elektronikus bélyegző alanya csak jogi személyiség lehet, ezért a bélyegző létrehozója a jogi személy képviseletében alkalmazhatja a bélyegzőt.

- Az Érintett fél, aki lehet természetes illetve jogi személy, vagy jogi személyiség nélküli szervezet. Nem áll szerződéses viszonyban a Szolgáltatóval, csak befogadja a hitelesített adatokat. A Szolgáltatónál ellenőrizheti a kapott aláírás, tanúsítvány és időbélyeg érvényességét. A Szolgáltatóval elsősorban a Szolgáltató által karbantartott nyilvántartásokon keresztül érintkezik.

2.7. Egyéb egységek

Olyan harmadik felek, melyek nem előfizetők, de van hozzáférésük a bizalmi szolgáltatással kapcsolatos adatokhoz.

A harmadik feleknek hozzáférésüknek van a visszavonási információkhoz (CRL), szabályzatokhoz, hogy ellenőrizni tudják az aláírást vagy bélyegzőt.

2.8. Tanúsítvány használat, alkalmazási lehetőségek

A tanúsítványt csak az arra jogosultak, és csak a hatályos hazai és Uniós törvényekben és rendeletekben, a Szolgáltató szabályzataiban és a megkötött Szerződésben meghatározott célra használhatják. A tanúsítvány minden más célú használata tiltott.

2.8.1. *Engedélyezett alkalmazási lehetőségek*

Szolgáltató Bizalmi Rendjének érvényességi körében kibocsátott nem minősített tanúsítványok olyan elektronikus aláírások igazolására használhatók, amelyek az írásbeliség jogi követelményeit elektronikus formájú adatok vonatkozásában kielégítik, továbbá:

- az aláíró valamint bélyegző tanúsítvány létrehozója az elektronikus aláírás vagy bélyegző létrehozásához használt adatot kizárólag elektronikus aláírás, illetve bélyegző létrehozására használhatja.
- a weboldalak hitelesítésére kibocsátott tanúsítványok kizárólag az adott web, szerver vagy kapcsolat azonosítására és titkosítására használhatóak.
- tanúsítványokhoz tartozó aláírás létrehozó adat tanúsítványok aláírására történő felhasználása, vagy bármilyen egyéb bizalmi szolgáltatás nyújtásához történő alkalmazása tilos,

- a Szolgáltató a végfelhasználói tanúsítványok felhasználását a Szerződésben tovább korlátozhatja.

A bizalmi szolgáltatás és jelen Szabályzat keretében a Szolgáltató által kibocsátott nem minősített tanúsítványok, generált kulcspárok, és az időbélyegzés szolgáltatás keretein belül kibocsátott időbélyegekre és a további szolgáltatásokra a következő alpontokban leírt alkalmazhatósági szabályok érvényesek. Az esetleges egyéb alkalmazási lehetőségeket illetve korlátokat a Szerződés is tartalmazhatja.

A Szolgáltató általa kibocsátott tanúsítványokhoz tartozó magánkulcsok elektronikus aláírás vagy bélyegző létrehozására, a hozzá tartozó nyilvános kulcsok, a tanúsítvány, a tanúsítvány visszavonási listák (továbbiakban: CRL), az időbélyegek (vagy időpecsét) a létrehozott elektronikus aláírás vagy bélyegző ellenőrzésére használhatóak fel. Az időbélyegek további feladata, hogy hitelesítsenek egy adott dokumentumot vagy állományt abban a pillanatban, amikor az időpecsételés történt.

Jogi személy által kibocsátott dokumentum hitelesítésén felül az elektronikus bélyegző a jogi személy digitális eszközei, például a szoftverkód vagy a szerverek hitelesítésére is használható.

A Szolgáltató a részére kibocsátott tanúsítvánnyal hitelesíti az általa kibocsátott tanúsítványokat és azzal készíti el az időbélyegeket.

A kibocsátott tanúsítványok minden olyan informatikai alkalmazásban használhatóak, amelyek támogatják a PKI technológián alapuló aláírási és bélyegzési funkciókat.

További engedélyezett alkalmazási lehetőségeket jelen Szabályzat, a Bizalmi Rend, a Szerződés, az ÁSzF és a vonatkozó rendeletek tartalmazhatnak.

2.8.2. *Korlátozott illetve tiltott alkalmazási lehetőségek*

A tanúsítványt csak az arra jogosult használhatja, és olyan céllal, amivel a tanúsítványt létrehozták. Ez a cél rögzítve van a tanúsítványban is és a Szerződésben is.

A Szolgáltató a Szerződésben leírtaknak megfelelően korlátozhatja az általa kibocsátott tanúsítványok felhasználhatóságát területi, pénzügyi és egyéb vonatkozásban. A korlátozások mértékét a Szolgáltató és hatályos hazai és Uniós jogszabályok határozzák meg.

Az Ügyfél az Alanyra, valamint az elektronikus bélyegző létrehozójára vonatkozó egyéb korlátozásokat is megadhat, melyet az előfizetői Szerződésben rögzíteni kell.

A tanúsítványokhoz tartozó aláírás létrehozó adat tanúsítványok aláírására történő felhasználása, vagy bármilyen egyéb bizalmi szolgáltatás nyújtásához történő alkalmazása tilos.

A kibocsátott tanúsítványok használatára vonatkozó bármely korlátozás megszegése tilos. A Szolgáltató nem vállal felelősséget a kibocsátott tanúsítvány illetve a hozzá kapcsolódó magán és nyilvános kulcs kibocsátási céltól eltérő felhasználásért.

További korlátozott, illetve tiltott alkalmazási lehetőségeket jelen Szabályzat, a Bizalmi Rend, a Szerződés, az ÁSzF és a vonatkozó rendeletek tartalmazhatnak.

2.9. Szabályzat adminisztráció

2.9.1. *Szervezeti dokumentum adminisztráció*

Szervezet:

- Név: Digitoll Informatikai és Szolgáltató Kft.
  - Cím: 1124 Budapest, Stromfeld Aurél út 9.
  - Ügyfélszolgálat: 1113 Budapest, Bartók Béla út 152/H
  - Telefon: 06 1 487 9900
  - E-mail: digitoll@digitoll.co.hu
  - Web: www.digitoll.co.hu, ds.digitoll.co.hu

2.9.2. *Kapcsolattartó személyek*

Általános információ:

- Név: Németh Ágnes
  - Telefon: 06 1 487 9923
  - E-mail: info@digitoll.co.hu

Technikai támogatás

- Név: Németh Viktor
  - Telefon: 06 1 487 9912
  - E-mail: support@digitoll.co.hu

2.9.3. *Fogyasztóvédelem*

A Szabályzat szerinti Szolgáltatásokkal kapcsolatban illetékes fogyasztóvédelmi hatóság adatait a következő táblázat tartalmazza:

Név:	Budapest Főváros Kormányhivatal Fogyasztóvédelmi Felügyelőség
Cím:	1052 Budapest, Városház u. 7.
Postai cím:	1364 Budapest, Pf. 144.
Telefonszám:	(+36-1) 450 2598
Email cím:	fogyved_kmf_budapest@nfh.hu
Internet cím:	http://www.nfh.hu

2.9.4. *Bizalmi felügyelet*

Név:	Nemzeti Média- és Hírközlési Hatóság
Cím:	1015 Budapest, Ostrom utca 23-25.
Postacím:	1525 Budapest, Pf.75
Telefonszám:	(+36-1) 457 7100
Internet cím:	http://www.nmhh.hu

2.10. Meghatározások és rövidítések

Az alábbi meghatározásokat és fogalmakat a 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól (továbbiakban: E-ügyintézési tv.) törvény értelmezésében és a 2014. július 23-i 910/2014/EU európai parlamenti és tanácsi rendeletben (továbbiakban: eIDAS) foglaltaknak szerint alkalmazza Szolgáltató szabályzataiban:

Aláíró: elektronikus aláírást létrehozó természetes személy;
Automatikus információátadás: információátadás az információ átadását biztosító együttműködő szerv részéről emberi beavatkozást nem igénylő módon;
Automatikus információátadási felület: az információ átadását biztosító együttműködő szerv által létrehozott és üzemeltetett, automatikus információátadást lehetővé tevő műszaki megoldás;
Azonosításra visszavezetett dokumentumhitelesítés: olyan szolgáltatás, amelynek keretében a jogszabályban meghatározott szolgáltató az ügyfél által rendelkezésre bocsátott nyilatkozatot az általa igazolt személyhez rendeli, majd a személyhez rendelést hitelesen igazolja;
Bélyegző létrehozója: elektronikus bélyegzőt létrehozó jogi személy;

1124 Budapest, Stromfeld Aurél út 9.
Tel.: +361 487 9900
E-mail: digitoll@digitoll.co.hu
Web: www.digitoll.co.hu

Bizalmi szolgáltatás: rendszerint díjazás ellenében nyújtott, az alábbiakból álló elektronikus szolgáltatások:

- elektronikus aláírások, elektronikus bélyegzők vagy elektronikus időbélyegzők, ajánlott elektronikus kézbesítési szolgáltatások, valamint az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok létrehozása, ellenőrzése és érvényesítése; vagy
- weboldal-hitelesítő tanúsítványok létrehozása, ellenőrzése és érvényesítése; vagy
- elektronikus aláírások, bélyegzők vagy az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok megőrzése;

Bizalmi szolgáltatási rend: olyan szabálygyűjtemény, amelyben egy bizalmi szolgáltató, igénybe vevő vagy más személy valamely bizalmi szolgáltatás használatának feltételeit írja elő igénybe vevők valamely közös biztonsági követelményekkel rendelkező csoportja vagy meghatározott alkalmazások számára;

Bizalmi szolgáltatási ügyfél: a bizalmi szolgáltatóval szolgáltatási szerződést kötő természetes vagy jogi személy (továbbiakban: ügyfél);

Bizalmi szolgáltató: egy vagy több bizalmi szolgáltatást nyújtó természetes vagy jogi személy; a bizalmi szolgáltató lehet minősített vagy nem minősített bizalmi szolgáltató;

Elektronikus aláírás: olyan elektronikus adat, amelyet más elektronikus adatokhoz csatolnak, illetve logikailag hozzárendelnek, és amelyet az aláíró aláírásra használ;

Elektronikus aláírás létrehozásához használt adat: olyan egyedi adat, amelyet az aláíró elektronikus aláírás létrehozásához használ;

Elektronikus aláírást létrehozó eszköz: elektronikus aláírás létrehozására használt, konfigurált hardver- vagy szoftvereszköz;

Elektronikus aláírás tanúsítványa: olyan elektronikus igazolás, amely az elektronikus aláírást érvényesítő adatokat egy természetes személyhez kapcsolja, és igazolja legalább az érintett személy nevét vagy álnevét;

Elektronikus azonosítás: a természetes vagy jogi személyt, illetve jogi személyt képviselő természetes személyt egyedileg azonosító, elektronikus személyazonosító adatok felhasználásának folyamata;

Elektronikus azonosító eszköz: olyan hardver- és/vagy szoftvereszköz, amely a személyazonosító adatokat tartalmazza, és amelyet online szolgáltatások céljából történő azonosításra használnak;

Elektronikus bélyegző: olyan elektronikus adatok, amelyeket más elektronikus adatokhoz csatolnak, illetve logikailag hozzárendelnek, hogy biztosítsák a kapcsolt adatok eredetét és sértetlenségét;

Elektronikus bélyegző létrehozásához használt adatok: olyan egyedi adatok, amelyeket az elektronikus bélyegző létrehozója elektronikus bélyegző létrehozásához használ;

Elektronikus bélyegzőt létrehozó eszköz: elektronikus bélyegző létrehozására használt, konfigurált hardver- vagy szoftvereszköz;

1124 Budapest, Stromfeld Aurél út 9.
Tel.: +361 487 9900
E-mail: digitoll@digitoll.co.hu
Web: www.digitoll.co.hu

Elektronikus bélyegző tanúsítványa: olyan elektronikus tanúsítvány, amely az elektronikus bélyegzőt érvényesítő adatokat egy jogi személyhez kapcsolja, és igazolja az érintett jogi személy nevét;
Elektronikus dokumentum: elektronikus formában, különösen szöveg, hang-, képi vagy audiovizuális felvétel formájában tárolt bármilyen tartalom;
Elektronikus időbélyegző: olyan elektronikus adatok, amelyek más elektronikus adatokat egy adott időponthoz kötnek, amivel igazolják, hogy utóbbi adatok léteztek az adott időpontban;
Érvényesítés: olyan folyamat, amelynek keretében ellenőrzik és igazolják, hogy az elektronikus aláírás vagy bélyegző érvényes
Érvényesítési adat: elektronikus aláírás vagy elektronikus bélyegző érvényesítéséhez használt adatok;
Érvényességi lánc: az elektronikus dokumentum vagy annak lenyomata és azon egymáshoz rendelhető információk (így különösen azon tanúsítványok, a tanúsítványokkal kapcsolatos információk, az aláírás vagy bélyegző létrehozásához használt adatok, a tanúsítvány aktuális állapotára, visszavonására vonatkozó információk, valamint a tanúsítványt kibocsátó szolgáltató érvényességi adatára és annak visszavonására vonatkozó információk) sorozata, amelyek segítségével megállapítható, hogy az elektronikus dokumentumon elhelyezett fokozott biztonságú vagy minősített elektronikus aláírás, bélyegző vagy időbélyegző, az aláírás, bélyegző vagy időbélyegző elhelyezésének időpontjában érvényes volt;
Fokozott biztonságú elektronikus aláírás: olyan elektronikus aláírás, amely megfelel az alábbi követelményeknek:

- kizárólag az aláíróhoz köthető;
- alkalmas az aláíró azonosítására;
- olyan, elektronikus aláírás létrehozásához használt adatok felhasználásával hozzák létre, amelyeket az aláíró nagy megbízhatósággal kizárólag saját maga használhat;
- olyan módon kapcsolódik azokhoz az adatokhoz, amelyeket aláírtak vele, hogy az adatok minden későbbi változása nyomon követhető.

Fokozott biztonságú elektronikus bélyegző: olyan elektronikus bélyegző, amely megfelel az alábbi követelményeknek:

- kizárólag a bélyegző létrehozójához kötött;
- alkalmas a bélyegző létrehozójának azonosítására;
- olyan, elektronikus bélyegző létrehozásához használt adatok felhasználásával hozzák létre, amelyeket a bélyegző létrehozója nagy megbízhatósággal kizárólag saját maga elektronikus bélyegző létrehozására használhat;
- olyan módon kapcsolódik azokhoz az adatokhoz, amelyekre vonatkozik, hogy az adatok minden későbbi változása nyomon követhető;

Hitelesítés: olyan elektronikus folyamat, amely lehetővé teszi a természetes vagy jogi személy elektronikus azonosításának vagy az elektronikus adatok eredetének és sértetlenségének az igazolását;

Hitelesítési rend: olyan bizalmi szolgáltatási rend, amely bizalmi szolgáltatás keretében kibocsátott tanúsítványra vonatkozik;
Igénybe vevő fél: olyan természetes vagy jogi személy aki, vagy amely elektronikus azonosítási vagy bizalmi szolgáltatást vesz igénybe;
Irányadó bizalmi szolgáltatási követelmények: az eIDAS Rendeletben, az eIDAS Rendelet uniós végrehajtási aktusaiban, az e törvényben, az e törvény felhatalmazása alapján kiadott jogszabályokban, a bizalmi szolgáltató szolgáltatási szabályzatában, bizalmi szolgáltatási rendjében, valamint a Bizalmi felügyelet bizalmi szolgáltatóra vonatkozó határozatában meghatározott követelményeket;
Lenyomat: olyan meghatározott hosszúságú, az elektronikus dokumentumhoz rendelt bitsorozat, amelynek képzése során a használt eljárás (lenyomatképző eljárás) a képzés időpontjában teljesíti az e törvény végrehajtására kiadott rendeletben megfogalmazott követelményeket;
Személyazonosító adat: egy természetes vagy jogi személy vagy egy jogi személyt képviselő természetes személy személyazonosságának megállapítását lehetővé tevő adat;
Szolgáltatási szabályzat: a bizalmi szolgáltató nyilatkozata az egyes bizalmi szolgáltatások nyújtásával kapcsolatosan alkalmazott részletes eljárási vagy más működési követelményekről;
Szolgáltatási szerződés: a bizalmi szolgáltató és a bizalmi szolgáltatási ügyfél között létrejött szerződés, amely a bizalmi szolgáltatás nyújtására és a szolgáltatás igénybevételére vonatkozó feltételeket tartalmazza;
Tanúsítvány alany: a tanúsítványban a bizalmi szolgáltató által igazolt azonosságú vagy tulajdonságú személy, így különösen elektronikus aláírás tanúsítványa esetén az aláíró(továbbiakban: Alany);
Tanúsítvány: az elektronikus aláírás tanúsítvány, az elektronikus bélyegző tanúsítvány és a weboldal-hitelesítő tanúsítvány, valamint mindazon, a bizalmi szolgáltatás keretében a szolgáltató által kibocsátott elektronikus igazolás, amely tartalmazza a tanúsítványra vonatkozó érvényesítési adatot és a tanúsítvány használatához szükséges kapcsolódó adatokat, és amely elektronikus dokumentum megbízhatóan védve van a kibocsátáskor és az érvényességi ideje alatt rendelkezésre álló technológiákkal elkövetett hamisítás ellen;
Tartós adathordozó: olyan eszköz, amely a címzett számára lehetővé teszi a neki címzett adatoknak az adat céljának megfelelő ideig történő tartós tárolását és a tárolt adatok változatlan formában és tartalommal történő megjelenítését. Ilyen eszköz különösen a papír, az USB kulcs, a CD-ROM, a DVD, a memória kártya, a számítógép merevlemeze;
Termék: olyan hardver- vagy szoftvereszköz vagy ezek megfelelő része, amelyet bizalmi szolgáltatások nyújtásában való felhasználásra szántak;
Természetes személy: nem gazdálkodó szervezetként eljáró, a polgári törvénykönyvről szóló törvény szerinti természetes személy;

Természetes személy tanúsítvány alany: a tanúsítványban szereplő természetes személy, függetlenül attól, hogy a tanúsítványban egyúttal valamely nem természetes személy képviseletére való jogosultságát vagy azzal való kapcsolatát is igazolják;
Weboldal-hitelesítő tanúsítvány: olyan igazolás, amely lehetővé teszi a weboldal hitelesítését és a weboldalt ahhoz a természetes vagy jogi személyhez kapcsolja, akinek vagy amelynek részére a tanúsítványt kiállították;

Egyéb meghatározások, melyeket Szolgáltató alkalmazhat szabályzataiban:
Aláírás-létrehozó eszköz (ALE): olyan hardver, illetve szoftver eszköz, melynek segítségével az aláíró az aláírás-létrehozó adatok felhasználásával az elektronikus aláírást létrehozza.
Álneves tanúsítvány: Akkor nevezünk egy tanúsítványt álneves tanúsítványnak, ha a tanúsítványban nem a tanúsítványhoz tartozó felhasználó (Alany) valódi - személyazonosításra alkalmas igazolványában szereplő - neve szerepel, hanem valamely más szöveg.
Bizalmi felügyelet vagy Hatóság: Az elektronikus aláírással kapcsolatos szolgáltatásokat nyújtó szolgáltatókat felügyelő hatóság, a Nemzeti Média- és Hírközlési Hatóság (NMHH).
Elektronikus dokumentum: elektronikus eszköz útján értelmezhető adat együttes.
Előfizető vagy Ügyfél: A hitelesítés-szolgáltatónál egy vagy több aláíró nevében előfizető természetes, vagy jogi személy, vagy jogi személyiség nélküli szervezet.
Időbélyegzési Rend: olyan szabálygyűjtemény, amelyben egy szolgáltató, igénybe vevő vagy más személy (szervezet) valamely időbélyegző felhasználásának feltételeit írja elő igénybe vevők valamely közös biztonsági követelményekkel rendelkező csoportja, illetőleg meghatározott alkalmazások számára.
Igénybe vevő: elektronikus aláírással kapcsolatos szolgáltatást igénybe vevő természetes személy, jogi személy vagy jogi személyiség nélküli szervezet.
Kompromittálódás: az Alany magánkulcsa kompromittálódik, ha elveszik illetve ha véletlenül vagy szándékosan nyilvánosságra kerül.
Kriptográfiai kulcs: Olyan kriptográfiai transzformációt vezérlő egyedi digitális jelsorozat, amelynek ismerete titkosításhoz és dekódoláshoz, specifikusan az elektronikus aláírás előállításához, illetőleg ellenőrzéséhez szükséges.
Kulcspár: Az elektronikus aláírás létrehozásához és ellenőrzéséhez létrehozott egyedi aszimmetrikus kriptográfiai jelsorozat pár, mely áll egy publikus (nyilvános) és agy privát (magán) kulcsból.
Nyilvános kulcsú infrastruktúra (Public Key Infrastructure, PKI): Olyan szabványrendszer, mely meghatároz különböző biztonsági szolgáltatások körét, amelyek a kétkulcsos aszimmetrikus titkosítást és szabványos tanúsítványok használatát teszi lehetővé. Célja az adatvédelem, hitelesítés, bizalmasság, letagadhatatlanság és rendelkezésre állás megteremtése.
Tanúsítványtár: A végfelhasználói és szolgáltatói tanúsítványok, felfüggesztett, visszavont tanúsítványadatok, Szolgáltatói Szabályzatok publikálásáért, tárolásáért felelős alegység.

Tanúsítvány Visszavonási Lista (CRL – Certificate Revocation List): Valamely okból visszavont, azaz érvénytelenített, illetve felfüggesztett, azaz ideiglenesen érvénytelenített tanúsítványok azonosítóit tartalmazó elektronikus lista, melyet a Szolgáltató bocsát ki.

3. Közzététel, nyilvánosságra hozatal, tanúsítványtár

3.1. A szolgáltatói információ közzététele

3.1.1. *Szabályzatok, kikötések és feltételek közzététele*

A Szolgáltató szerződéses feltételeit és szabályzatait elektronikus formában (PDF) teszi közzé az internetes honlapján (http://ds.digitoll.co.hu/). Ugyanitt elérhetőek a dokumentumok esetleges korábban érvényben lévő változatai is.

A dokumentumok internetes oldalról nyomtatott változatai semmilyen formában sem tekinthetők hivatalos példánynak vagy hiteles másolatnak.

Szolgáltató nyilvános szabályzataiban csak azon eljárásait hozza nyilvánosságra, melyek ismerete a Szolgáltatás biztonságát nem veszélyezteti.

Szolgáltató a szerződéskötést követően tartós adathordozón a bizalmi szolgáltatás ügyfelének rendelkezésére bocsátja a szolgáltatási szerződést, a bizalmi szolgáltatási rendet és a szolgáltatási szabályzatot.

3.1.2. *Rendkívüli információk közzététele*

A Szolgáltató a rendkívüli információkat késlekedés nélkül közzéteszi internetes oldalán, a jogszabályi előírásoknak megfelelően, illetve akkor, amikor arra szükség van.

Rendkívüli információnak számít:

- Tájékoztatás új szolgáltatás vagy szolgáltatás-csoport indításáról.
- Tájékoztatás a Szolgáltatás szüneteléséről (E-ügyintézési tv. 89. §), tervezett beszüntetéséről.
- Tájékoztatás a Szolgáltató magánkulcsának kompromittálódásáról, tanúsítványának felfüggesztéséről, visszavonásáról.
- Tájékoztatás a Szolgáltató tevékenységének befejezéséről.
- Tájékoztatás rendkívüli üzemeltetési helyzetről, körülményről, mely akadályozza a Szolgáltató rendes üzemmenetének folytatását.

Egyes rendkívüli információk esetén, a Szolgáltató írásban (elektronikusan vagy postai úton) is tájékoztathatja a Végfelhasználókat.

A szolgáltatói gyökértanúsítvány állapotváltozásával (visszavonásával), szolgáltatás befejezésével kapcsolatban a Szolgáltató hirdetésként közzéteszi az állapotváltozás tényét, illetve az érintett tanúsítvány adatait (lenyomatát) országos terjesztésű napilapban.

3.2. A tanúsítvány állapot információk közzététele

3.2.1. *A tanúsítványtár*

A Szolgáltató a végfelhasználók számára tanúsítványtárat üzemeltet, mely internetes oldalán elérhető. Szolgáltató itt teszi közzé a visszavonási listákat és a tájékozató jellegű Nyilvános tanúsítványtárat.

A Szolgáltató a Tanúsítványtárat rendszeres időközönként szükség szerint frissíti.

3.2.1.1. Nyilvános tanúsítványtár

A Szolgáltató által kibocsátott tanúsítványok és azok állapota elérhető a Nyilvános tanúsítványtárban is, a Szolgáltató internetes oldalán (ds.digitoll.co.hu). A Szolgáltató csak az Ügyfél és/vagy Alany előzetes hozzájárulásával teszi közzé a tanúsítványt.

A Nyilvános tanúsítványtárban tárolt információk tájékoztató jellegűek, a mindenkori érvényes tanúsítványállapotokat a visszavonási listák tartalmazzák.

A Nyilvános tanúsítványtár helye:
http://ds.digitoll.co.hu/tanusitvanytar.php?m=41

3.2.1.2. Tanúsítvány visszavonási lista (CRL)

Szolgáltató a tanúsítványok érvényességének ellenőrzésére tanúsítvány visszavonási listát (továbbiakban CRL) bocsát ki. A CRL tartalmazza a Szolgáltató által visszavont és felfüggesztett tanúsítványokat.

A visszavonási lista kibocsátása Szolgáltató zárt tanúsítványtárából történik. A CRL-ek kibocsátása között eltelt idő legfeljebb 24 óra. A CRL akkor is kibocsátásra kerül, ha a legutóbbi kibocsátás óta nem történt tanúsítvány visszavonás vagy felfüggesztés. A visszavonási lista mindig tartalmazza a következő lista kibocsátásnak idejét, vagy a kibocsátott CRL érvényességi

idejét, de Szolgáltató ennél korábban is kibocsáthat új listát. Felfüggesztés, visszaállítás és visszavonás esetén a Szolgáltató soron kívül új CRL-t bocsát ki. Új CRL kibocsátásakor a régebbi érvényessége megszűnik.

A tanúsítvány visszavonási listák helye:
http://pki.digitoll.co.hu/pki/crls/rootca_adv.crl

A Szolgáltató Nyilvános tanúsítványtára és a visszavonási listája, legalább 99%-os rendelkezésre állással elérhetők, egyúttal az eseti szolgáltatás kiesések nem haladják meg a 24 órás időtartamot.

3.3. Adattárak

A Szolgáltató web-alapú felületen hozzáférést biztosít a Végfelhasználók számára a visszavonási adatokhoz (CRL), tanúsítvány információkhoz (Nyilvános tanúsítványtár), és a Szolgáltató publikus dokumentumaihoz (többek között: ÁSzF, Bizalmi Rend, Időbélyegzési Rend, jelen Szabályzat).

A Szolgáltató dokumentumainak elérhetősége:
http://ds.digitoll.co.hu/dok.php?m=5

Bizalmi Rend a tanúsítványban:
http://ds.digitoll.co.hu/doc/cp_1_3_6_1_4_1_46800_1_2_1_6.pdf

Visszavonási lista publikus helye:
http://pki.digitoll.co.hu/pki/crls/rootca_adv.crl

3.4. A közzététel gyakorisága

3.4.1. *Szabályzatok, kikötések és feltételek közzétételi gyakorisága*

A Szabályzattal kapcsolatos új verziók közzététele jelen Szabályzat 3. pontjában van ismertetve. A Szolgáltató szükség szerint bocsátja ki szerződéses feltételeit és szabályzatait, illetve azok újabb változatait.

3.4.2. *Rendkívüli információk közzétételi gyakorisága*

A Szolgáltató a rendkívüli információkat közzéteszi a jogszabályi előírásoknak megfelelően, illetve ennek hiányában akkor, amikor arra szükség van.

3.4.3. *Tanúsítványokkal kapcsolatos információk közzétételének gyakorisága*

A Szolgáltató az egyes tanúsítványok nyilvános közzététele kapcsán a következő gyakorlatot követi:

- a végfelhasználói tanúsítványokat a Nyilvános tanúsítványtárában az előállítást követően tíz munkanapon belül teszi közzé, amennyiben a tanúsítványt tulajdonló Ügyfél és Alany ehhez előzetesen írásban hozzájárult.
- A visszavont, felfüggesztett tanúsítványokat a Szolgáltató a CRL-ben teszi közzé a visszavonást követően, rendszeres gyakorisággal, amikor erre szükség van.

A lehetséges esetek a következőek:

- lejárt a tanúsítvány,
- jogos felfüggesztési kérelem esetén,
- a tanúsítvány visszavonása esetén,
- felfüggesztés esetén.

3.5. Adattárak hozzáférési szabályzása

A Szolgáltató által közzétett kikötések és feltételek, rendkívüli információk, tanúsítványok és állapot információk nyilvános információk, a web alapú felületeken harmadik – külső felek – felé is elérhetőek, így megtekintés céljából letölthetőek külön hitelesítés nélkül.

A tanúsítványok adatainak nyilvános közzététele csak az Ügyfél és az Alany előzetes írásos hozzájárulásával lehetséges.

A Szolgáltató által közölt információkat kizárólag csak a Szolgáltató egészítheti ki, törölheti vagy módosíthatja. A Szolgáltató többféle védelmi mechanizmussal védi az információkat jogosulatlan módosítások ellen.

4. Azonosítás és hitelesítés

4.1. Névtípusok

A tanúsítványban alkalmazható mezők és megnevezéseik:

Subject (alany) mező	
commonName (CN)	Személyi vagy Munkatársi aláíró tanúsítvány esetén a tanúsítvány Alanyának az azonosító okmány szerinti neve. Szervezet tanúsítványában a szervezet bejegyzett neve. Álneves tanúsítvány esetén az álneves tanúsítvány tényének megjelölése. Webhely azonosító tanúsítvány esetén a domain nevet tartalmazza.
Title (T)	Opcionális mező. Személyi vagy Munkatársi aláíró tanúsítvány esetén a tanúsítvány Alanyának titulusa vagy beosztása.
pseudonym	Álnév. Álneves tanúsítványok esetén alkalmazható. Az Alany választott neve szerepel benne. Álneves tanúsítvány esetén, a CN mezőben az álneves tanúsítvány tényét rögzíteni kell-
localityName (L)	Bejegyzett székhely vagy azonosító okmány szerinti lakhely megnevezése (város).
organizationName (O)	Munkatársi tanúsítvány és Szervezet tanúsítványa esetén a szervezet bejegyzett teljes vagy rövidített megnevezése.
organizationalUnitName 1 (OU1)	Opcionális mező. Munkatársi tanúsítvány vagy Szervezet tanúsítványa esetén, a szervezeten belüli egység megnevezése.
organizationalUnitName 2 (OU2)	Opcionális mező. Munkatársi tanúsítvány vagy Szervezet tanúsítványa esetén, a szervezeten belüli egység megnevezése.
countryName (C)	Bejegyzett székhely vagy azonosító okmány szerinti lakhely országának megnevezése, ISO 3166 szerinti országkód.
serialNumber	Opcionális mező. Alany egyedi azonosítója, azonosító okmány szerint i azonosító meghatározott formátumban: ▪ személyi igazolvány vagy jogosítvány száma esetén: IDCXX-a szám (XX az országkód) ▪ útlevél esetén: PASXX- a szám (XX az országkód) ▪ adóazonosító esetén: TINXX- a szám (XX az országkód)

	▪ fent nevezett adatok hiányában egy más egyedi azonosító alkalmazható.
emailAddress (E)	A tanúsítvány alanyának e-mail címe. Megegyezhet SAN mezővel.
subjectAltName (SAN)	A tanúsítvány alanyának e-mail címe. Megfelel az IETF RFC 822 formátumnak.
Issuer (kibocsátó) mező – Szolgáltató tanúsítványa	
commonName (CN)	A Szolgáltató szolgáltatási egységének neve.
countryName (C)	A Szolgáltató bejegyzett székhelyének ISO 3166 szerinti országkódja.
localityName (L)	Bejegyzett székhely megnevezése (város).
organizationName (O)	A Szolgáltató megnevezése.

Természetes személyek tanúsítványa esetén kötelező az alábbi mezők kitöltése:

- commonName (név)
- pseudonym (álneves tanúsítvány esetén)
- countryName (országkód)

Munkatársi tanúsítvány esetén:

- commonName (név)
- pseudonym (álneves tanúsítvány esetén)
- countryName (országkód)

Szervezet tanúsítványa esetén kötelező az alábbi mezők kitöltése:

- commonName (név)
- countryName (országkód)

Ha az adott mezőben a méretbeli korlátok akadályozzák az adatok pontos kiírását, Szolgáltató alkalmazhat rövidítést.

Az azonosítók értelmezése érdekében az Érintett felek a Szolgáltató nyilvános szabályzataiban leírtak alapján kell eljárniuk. Ha az Érintett félnek bármely, a tanúsítványban foglaltak értelmezésével kapcsolatban segítségre van szüksége, akkor a Szolgáltatóval közvetlenül is felveheti a kapcsolatot. A Szolgáltató az Ügyfél vagy Alany adatairól többlettájékoztatást, erre vonatkozó felhatalmazás hiányában nem ad, csak a tanúsítványban feltüntetett adatok értelmezését segítő információt szolgáltatja.

4.1.1. *Márkanevek, védjegyek elismerése, hitelesítése*

A Szolgáltató által kibocsátott tanúsítványok mezőiben előfordulhatnak márkanevek, védjegyek. Ezek jogos használatát a Szolgáltató lehetőségei szerint ellenőrizheti, de nem vállal közvetítő vagy döntnöki szerepet ilyen jellegű viták feloldásában, illetve nem vállalja a felelősséget a név jogtalan használata miatt. A Szolgáltató ezért nem garantálja az Ügyfél számára a márkaneve és/vagy védjegye feltüntetését a tanúsítványban. Az Ügyfél részéről egy védjegy vagy márkanév megszerzése nem tekintendő olyan eseménynek, mely alapján a tanúsítvány megújítását kell kezdeményeznie.

4.1.2. *Álnevek használata*

Az eIDAS, valamint az E-ügyintézési tv. alapján a szolgáltatások igénylője jogosult kérni, hogy a tanúsítványba álnév kerüljön. Így Szolgáltató elérhetővé teszi az álnevek használatát az alábbi feltételek szerint:

- Az álneves tanúsítványok azonosítási, igénylési és kibocsátási folyamata, felfüggesztése és visszavonása megegyezik a nem álneves tanúsítványok felfüggesztési és visszavonási folyamatával.
- Az álneves tanúsítványokra Szolgáltató külön tanúsítvány profillal rendelkezik. Az álneves tanúsítványokban a pseudonym mező az álnevet tartalmazza és a CN mező az álneves tanúsítvány tényét.
- Álnév kizárólag a tanúsítványban használható, Szolgáltató az igénylésben és a Szerződésben az igénylő valódi megnevezését használja és feltünteti az álnevet.
- Mivel az álneves tanúsítványban bármilyen név szerepelhet – akár más természetes vagy jogi személy neve is – így Szolgáltató a név jogos használatáért nem felelős, nem vállal közvetítő vagy döntnöki szerepet ilyen jellegű viták feloldásában, illetve nem vállalja a felelősséget a név jogtalan használata miatt. Ezen okok miatt Szolgáltató megtagadhatja az álnév használatát, ha az sérti a jó ízlést, a szemérmet és az etnikai hovatartozást.
- az álnevek egyediségének garantálása megegyezik Szolgáltató jelen szabályzat idevonatkozó pontjában leírtakkal.

Ha a tanúsítványban az igénybe vevő álnéven szerepel, a Szolgáltató a tanúsítványban szereplő igénybe vevő valódi személyazonosságára vonatkozó adatot csak az érintett igénybe vevő, az Ügyfél vagy a tanúsítványban igazolt igénybe vevő által képviselt más személy beleegyezésével, adhat át. Kivétel ez alól, ha az adatokat hatóságok kérik (jelen szabályzat 9.6. pont), mert ebben az esetben az adatok átadásáról Szolgáltató nem értesítheti az Alanyt.

Elektronikus aláírás tanúsítványa kibocsátható olyan céllal is, hogy az az aláírót más személy (szervezet) képviseletében történő aláírásra jogosítsa fel. Ebben az esetben a bizalmi-szolgáltatás igénybe vevőjére vonatkozó szabályokat a képviselőre kell alkalmazni. Ebben az esetben álnév csak a képviselt hozzájárulása esetén tüntethető fel.

Amennyiben az aláírás időpontjában álnév használatára kerül sor, az álnév használatának tényét egyértelműen fel kell tüntetni a szolgáltatást igénybe vevő fél számára.

4.1.3. *Nevek egyedisége*

A Szolgáltató az általa kibocsátott tanúsítványok esetében a tanúsítványok alanyait egyértelműen megkülönbözteti a tanúsítványban rögzített összes személyes adataik (név, lakóhely ország, lakóhely város, e-mail cím, illetve a Szolgáltató által esetlegesen generált sorszám) segítségével.

4.2. Kezdeti azonosítás

A tanúsítvány igénylése kizárólag írásban történik a Szolgáltató által biztosított online űrlap kitöltésével. Az igényléseket a Szolgáltató elbírálja és ezt követi a regisztrációs folyamat. A regisztrációs folyamat részeként szükséges lehet, hogy az igénylő megjelenjen a Regisztrációs hatóság előtt, melynek helyét és idejét az igénylő a Szolgáltató ügyfélszolgálatával telefonon, vagy írásban egyezteti. A személyes megjelenés történhet az Szolgáltató ügyfélszolgálati irodájában, vagy külön egyeztetés és megállapodás alapján, külső helyszínen.

4.2.1. *Természetes személy személyazonosságának hitelesítése*

Személyi tanúsítvány esetén az Ügyfél és az Alany maga az igénylő természetes személy. Munkatársi tanúsítványban a tanúsítvány alanya szintén természetes személy, aki az igénylő szervezethez tartozik, így az Alany ellenőrzése megegyezik az itt leírtakkal.

A tanúsítványban megnevezésre kerülő személy személyes megjelenését a fokozott biztonságú aláíró tanúsítványok illetve autentikációs tanúsítványok kiadása esetén követelheti meg a Szolgáltató.

Az igénylő személy személyazonosságáról a Szolgáltató Regisztrációs egysége egy bemutatott érvényes, személyazonosításra alkalmas fényképes okmánya (külföldi állampolgárok esetén útlevél) és érvényes lakcímkártyája alapján győződik meg. A bemutatott okmányoknak tartalmaznia kell az igénylő személy:

- nevét,
- állandó lakcímét,
- születésének dátumát és helyét,
- anyja nevét.

Ez alapján a Szolgáltató a következő okmányokat fogadja el:

- személyi igazolvány,
- jogosítvány,
- útlevél,
- lakcímkártya (az előzőekben felsorolt okmányok közül az egyikkel együtt bemutatva).

Személyes megjelenés esetén a bemutatott okmány fényképe alapján az igénylő személynek egyértelműen felismerhetőnek kell lennie, s a benne szereplő aláírásnak meg kell egyezni a Szerződésen az igénylő személy által tett aláírással.

A bemutatott okmányoknak és dokumentumoknak, minden kétséget kizáróan eredetinek, valódinak és érvényesnek kell lenniük. A Szolgáltató az összes nem minősített tanúsítványfajta kiadása esetén az Ügyfél adatait, valamint a bemutatott iratok és okmányok érvényességét és hitelességét E-ügyintézési tv. 82. § szerint közhiteles adatbázisban ellenőrzi.

Külföldi állampolgár esetén a Szolgáltató addig nem állítja ki részére a tanúsítványt, amíg a külföldön kiállított okmányt vagy a külföldi személy személyazonosságát megfelelő biztonsággal nem ellenőrizte.

Az Ügyfél valamint Alany aláírásával igazolja, hogy az általa bemutatott okmányok hitelesek, érvényesek és a megadott adatok a valóságnak megfelelőek.

A Szolgáltató a tanúsítvány kibocsátását visszautasítja, amennyiben:

- az átadott adatok és dokumentumok hiányosak,
- az igénylő személy nem képes a személyazonosságát, hitelt érdemlően bizonyítani,
- a bemutatott okmányok, dokumentumok nem érvényesek,
- az igénylő személy személyazonossága minden kétséget kizáróan nem állapítható meg, a közhiteles adatbázisokkal végzett adategyeztetés során kétely merül fel a fentiekkel kapcsolatban,
- az igénylő személy megtagadja az adatszolgáltatást.

A fenti esetek előfordulásakor a Szolgáltató hiánypótlásra szólíthatja fel az igénylő személyt. Amennyiben a Szolgáltató által megadott határidőn belül, az igénylő Személy a felhívásban

szereplő adatokat, okmányokat és dokumentumokat nem pótolja, illetve nem helyesbíti, a Szolgáltató ebben az esetben is visszautasíthatja a tanúsítvány kiállítását és kibocsátását.

4.2.2. *Jogi személy, Szervezet azonosságának hitelesítése*

Munkatársi tanúsítvány esetén az Ügyfél az igénylő Szervezet, és a tanúsítványokat a Szervezet képviseletében eljáró Alany vagy Alanyok részére állítja ki.

Elektronikus bélyegző esetén az igénylő szervezet (jogi személy) maga az Alany. Így nevében vagy a szervezet felelős vezetője, vagy a felelős vezető által meghatalmazott képviselő járhat el (Ügyfél).

A Munkatársi tanúsítvány vagy elektronikus bélyegző felhasználási körét az igénylő Szervezet határozza meg, de a Szolgáltató csak a szabályzataiban illetve a Szerződésben meghatározott alkalmazási esetekre vállal jogi és pénzügyi felelősséget. Ezekben az esetekben a Szolgáltató a tanúsítványt kizárólag az igénylő szervezet felelős vezetőjének vagy a felelős vezető megbízott képviselőjének meghatalmazásával bocsátja ki, és annak hozzájárulásával menedzseli (felfüggesztés, visszavonás).

A regisztráció során az Ügyfélnek adatokat és bizonyítékokat kell nyújtaniuk a következőkről:

- a szervezet teljes és rövid neve, székhelye,
- a szervezet hivatalos azonosító adatai,
- a szervezeten belüli szervezeti egység neve, ha kérik ennek feltüntetését a tanúsítványban,
- igazolás arra vonatkozóan, hogy a szervezet valóban létező szervezet (cégbírósági bejegyzését igazoló okirat),
- a lehetséges Alanyokról, vagy elektronikus bélyegző esetén a megbízott használók köréről és a szervezetben betöltött szerepükről,
- ha a szervezet nevében meghatalmazott jár el, igazolás arra vonatkozóan, hogy a szervezet nevében a Szerződést aláíró személy jogosult-e az aláírás megtételére,
- ha a szervezet nevében aláírásra jogosult személy jár el, a regisztrációhoz csatolni kell az aláírásra jogosult személy aláírási címpéldányát vagy más azzal egyenértékű hivatalos dokumentumot, mely a szervezet aláírásra jogosult vezetőinek nevét és aláírását tartalmazza.
- amennyiben a szervezet közigazgatási szerv, a közigazgatási szervet képviselő természetes személynek a regisztrációhoz rendelkeznie kell, az adott közigazgatási szerv által kiállított és közokiratba foglalt, a közigazgatási szerv nevét is tartalmazó meghatalmazást arra, hogy a Szervezet képviseletében a Szolgáltatónál előforduló ügyekben eljárjon.

1124 Budapest, Stromfeld Aurél út 9.
Tel.: +361 487 9900
E-mail: digitoll@digitoll.co.hu
Web: www.digitoll.co.hu

A Szolgáltató az Ügyfelek valamint Alanyok adatait, valamint a bemutatott iratok és okmányok érvényességét és hitelességét E-ügyintézési tv. 82. § szerint közhiteles adatbázisban ellenőrzi.

Az Alanyok azonosságának hitelesítési eljárása megegyezik a személy azonosságának hitelesítése pontjában leírtakkal. A Szervezet meghatalmazottjának jelen kell lenni az Alanyok regisztrációjánál és igazolnia kell az Alanyok a Szervezethez főződő kapcsolatát.

A Szolgáltató a tanúsítvány kibocsátását visszautasítja, amennyiben:

- az átadott adatok és dokumentumok hiányosak,
- a meghatalmazott illetve aláíró személyek (alanyok) az igénylő Szervezethez tartozása nem egyértelmű, vagy nem bizonyított,
- nem egyértelmű a Szervezet képviseletében eljáró személy felhatalmazása a tanúsítvány kibocsátásához,
- a bemutatott iratok és okmányok eredetiségével, valódiságával vagy érvényességével kapcsolatban kétség merül fel,
- az igénylő Szervezet azonossága minden kétséget kizáróan nem állapítható meg, a közhiteles adatbázisokkal végzett adategyeztetés során kétely merül fel a fentiekkel kapcsolatban.

A fenti esetek előfordulásakor a Szolgáltató hiánypótlásra szólíthatja fel az igénylő Szervezetet vagy meghatalmazottját. Amennyiben a Szolgáltató által megadott határidőn belül (ÁSzF), a Szervezet a felhívásban szereplő adatokat és dokumentumokat nem pótolja, illetve nem helyesbíti, a Szolgáltató ebben az esetben is visszautasíthatja a tanúsítvány kiállítását és kibocsátását.

Az igénylő Szervezet, mint Ügyfél felelősséget vállal a Szerződésben megnevezett Alanyai, vagy elektronikus bélyeg esetén meghatalmazott használói által tanúsítványokkal végzett műveletekért, vállalja a tanúsítványok kibocsátásával, fenntartásával kapcsolatos és minden egyéb járulékos költséget. Az igénylő Szervezet, mint Ügyfél és a hozzá tartozó Alanyok, elektronikus bélyegző esetén megbízott használók a Szolgáltató szabályzataiban részletesen tárgyalt kötelezettségeket, felelősségeket és jogokat ismerik, és elfogadják azokat.

Ha Szolgáltató által bizalmi szolgáltatás keretében kibocsátott tanúsítvány képviseleti jogosultságot is igazol, akkor Szolgáltató a tanúsítvány kibocsátásáról haladéktalanul értesíti a képviselt személyt, valamint a képviseleti jogosultság megszűnése esetén a képviselt vagy a képviselő személy kérésére köteles a képviseleti jogosultság tényét feltüntető tanúsítványt visszavonni. Szolgáltató kizárólag a képviselt hozzájárulása esetén tüntethet fel álnevet a tanúsítványban.

4.2.3. *Domain név, IP cím vagy eszköz, rendszer azonosítása*

Ha a kibocsátott tanúsítvány Alanya egy eszköz, rendszer vagy termék, az Ügyfélnek megbízható adatforrással igazolnia kell jogosultságát a birtoklásra, névhasználatra.

Ha a kibocsátott tanúsítvány Alanya domain név, IP cím, Ügyfélnek megbízható adatforrással igazolnia kell, hogy a megnevezett domain név, cím használatához joga van.

4.3. Azonosítás és hitelesítés az új kulcs kérésnél

Tanúsítvány kulcscseréjét a Szolgáltató nem támogatja. Amennyiben kulcscsere válna szükségessé, abban az esetben új tanúsítvány-igénylést kell beadni, az ott meghatározott személyazonosítási szabályok szerint eljárva.

4.4. Azonosítás és hitelesítés tanúsítványmegújítás esetén

Tanúsítványmegújítás akkor történik, amikor az Ügyfél illetve az Alany a már meg lévő tanúsítványa helyett újat igényel. Ha a meglévő tanúsítványt a Szolgáltató állította ki, és így az Ügyfél illetve Alany átesett a Szolgáltató kezdeti regisztrációs folyamatán (jelen Szabályzat ide vonatkozó pontja szerint), és semmilyen adat nem változott azóta, akkor az Ügyfélnek illetve az Alanynak az új igénylés mellett, írásban nyilatkoznia kell arról, hogy az új tanúsítványba kerülő adatok helyesek, nem változtak. A nyilatkozatot az Ügyfélnek illetve az Alanynak, aláírásával kell igazolnia és el kell juttatnia a Szolgáltatóhoz. Ezt megteheti elektronikusan (érvényes és hiteles elektronikus aláírással, e-mail), személyesen, illetve postán. Ha a Szolgáltató jóváhagyja az igénylést az Ügyfél egy előre egyeztetett időpontban egy egyszerűsített azonosítási folyamatot követően átveheti az új tanúsítványát. Az egyszerű azonosítási folyamat a kezdeti regisztrációkor megadott azonosító okmány alapján az Ügyfél személyének azonosításából áll.

Ha adatváltozás történik, illetve a tanúsítvány már legalább 2 hónapja lejárt (és ez alatt az idő alatt nem érkezett kérvény a megújításra), az új tanúsítvány kiadásához a kezdeti regisztrációs folyamat megismétlése szükséges.

Munkatársi tanúsítvány esetén az Szervezet képviseletében eljáró meghatalmazottnak új meghatalmazást kell felmutatnia. Minden tanúsítványmegújítás egy új tanúsítvány kibocsátását jelenti, és új Szerződéskötést igényel.

Munkatársi tanúsítvány megújítása esetén, ha a változás az Alanyok személyében történik, úgy az új Alanyoknak részt kell venniük jelen Szabályzat ide vonatkozó pontjában megfogalmazott kezdeti regisztrációs eljáráson.

Elektronikus bélyegző megújítás esetén a munkatársi tanúsítvány igénylésével megegyező az eljárásrend.

A Szolgáltató minden egyes tanúsítványmegújítás esetén igényelheti a jelen Szabályzatban megfogalmazott kezdeti azonosítási folyamatot és ismételt egyeztetést végezhet a közhiteles adatbázisokkal, és ha bármilyen problémát észlel az ide vonatkozó pontban megfogalmazott eljárást követi.

4.5. Azonosítás és hitelesítés a visszavonási és felfüggesztési kérelemhez

Felfüggesztési és/vagy visszavonási kérelmekhez kapcsolódó azonosítási és hitelesítési vonatkozásokat jelen Szabályzat idevonatkozó pontja tárgyalja.

5. A tanúsítvány életciklus működési követelményei

5.1. A tanúsítvány kérelem létrehozása

5.1.1. *Az igénylés feltétele*

A tanúsítványigénylés és szerződéskötés elengedhetetlen feltételei, hogy az igénylőnek hozzáférése legyen az Internethez és rendelkezzen e-mail címmel. A Szolgáltató az esetek többségében elektronikusan kommunikál a meglévő és leendő ügyfeleivel.

5.1.2. *A tanúsítványigénylés és feldolgozás folyamata*

A tanúsítvány igényléséhez szükséges a Szolgáltató internetes oldalán levő tanúsítványigénylési űrlap pontos kitöltése és elküldése a Szolgáltató részére.

A tanúsítványigénylés eljárás részletes folyamata a következő:

- Az Igénylő fél tájékozódik a Szolgáltató által kibocsátásra kerülő tanúsítványfajtákról és az igénylés feltételeiről, majd kiválasztja a neki megfelelőt. A választáshoz igényelhet segítséget a Szolgáltató ügyfélszolgálati irodájától telefonon, vagy írásban.
- Az Igénylő a Szolgáltató internetes oldalán található elektronikus tanúsítványigénylő űrlap kitöltésével kérelmezi a kiválasztott tanúsítvány kibocsátását. Az igénylőlapon

megadott adatok fognak szerepelni a tanúsítványban. Az igénylőlap kitöltése online történik, elküldése a Szolgáltató részére a kitöltés és nyilatkozattétel után történik.

- Az Igénylő az igénylés elküldése után kap egy elektronikus levelet ahol meg kell erősítenie a kérelmét és ezzel együtt a Szolgáltató le tudja ellenőrizni a megadott e-mail cím valódiságát.
- Munkatársi tanúsítvány igénylése esetén, az Alanyok számát, elektronikus bélyegző tanúsítványa esetén a felhasználók körét előre meg kell adni, és az igénylésen azok adatait pontosan fel kell tüntetni.
- Munkatársi tanúsítvány vagy elektronikus bélyegző igénylése esetén, ha a szerződéskötéssel és az igényléssel kapcsolatos műveletek elvégzését az Igénylő (Szervezet) megbízott képviselő látja el, akkor a személyes találkozó alkalmával - a Szolgáltatási Szabályzat idevonatkozó pontjában megfogalmazottakon kívül - a megbízott képviselőnek magával kell hoznia a Szolgáltató internetes oldaláról letölthető Meghatalmazási nyomtatvány - elektronikusan kitöltött és cégszerűen aláírt - kettő darab példányát. A Szolgáltató csak a megfelelően kitöltött és aláírt Meghatalmazási nyomtatványt fogadja el.
- Az igénylési folyamat történhet személyesen, a Szolgáltató ügyfélszolgálati irodájában, vagy előre egyeztetett időpontban külső helyszínen is. A Szolgáltató ebben az esetben is ellenőrzi a megadott e-mail címek helyességét.

Az Igénylő - Munkatársi tanúsítvány és elektronikus bélyegző esetében az igénylő Szervezet -, mint Ügyfél és az általa megnevezett Alany is, aki részére igényelve lett a tanúsítvány - az igénylés elküldésével nyilatkozik a következőkről:

- A Szolgáltató Szolgáltatásaira vonatkozó szabályzatait elolvasta, a benne foglaltakat megismerte és elfogadja.
- Büntetőjogi felelőssége tudatában kijelenti, hogy a megadott adatai helyesek, és a valóságnak megfelelnek.
- A választott Szolgáltatásokkal kapcsolatos díjak megfizetését vállalja.
- Tudomásul veszi, hogy a Szolgáltató, a szerződéskötés keretében a megadott személyes és szervezeti adatait a jogszabályi kötelezettségeknek megfelelően:
    - közhiteles adatbázissal egyeztesse, és nyilvántartsa
    - a tanúsítvány gondozása céljából nyilvántartsa,
    - a tanúsítványt nyilvánosságra hozza,
    - a hatóságoknak, kormányzati, illetve bírósági illetékeseknek, mint harmadik félnek kiadhatja.

A Szolgáltató a hozzá beérkezett tanúsítványigényléseket nyilvántartásba veszi és feldolgozza. A feldolgozás részeként ellenőrzi, hogy a választott tanúsítványhoz minden adat rendelkezésére áll-e, illetve ellenőrzi azokat. Ha megfelelőnek találja, időpontot egyeztet az

Igénylővel. A személyes találkozó alkalmával történik meg a Szerződés létrejötte a Szolgáltató – vagy megbízott alkalmazottja - és az Igénylő - vagy megbízottja - együttes aláírásával. Az Igénylő a továbbiakban már Ügyfélnek minősül. A tanúsítvány elkészítésére a tanúsítványigénylés során, az igénylésben megadott, a Szerződésben megerősített, a tanúsítvány fajtájától függően ellenőrzött, illetve az igénylés során érvényesnek elismert adatok alapján kerül sor. A tanúsítványigénylés feltételeinek teljesülése esetén a Szolgáltató feldolgozza azt.

Ha a beérkező adatokat a Szolgáltató hiányosnak, vagy valótlannak találja, felhívást küldhet az Igénylőnek hiánypótlásra, pontosításra. Az Igénylő köteles a felhívásnak a felhívásban meghatározott időn belül eleget tenni, vagy késedelmét írásban indokolni. Amennyiben ezt nem teszi meg, a Szolgáltató semmisnek veheti az igénylést. A Szolgáltató, megfelelő indoklással visszautasíthatja az igénylést.

Egyes Szolgáltatásokhoz szükséges az Igénylőnek a személyes megjelenése azonosítás céljából. Az eljárás részletei jelen Szabályzat idevonatkozó pontjában vannak rögzítve.

Ha a Szolgáltató az igénylést visszautasítja, vagy ha a Szerződés megkötésének megtagadása történik, illetve bármely más ok miatt a felek között a Szerződés nem jön létre, az Igénylő személyes adatait a Szolgáltató 5 napon belül megsemmisíti.

A Szolgáltató a tanúsítványigénylések feldolgozását beérkezési sorrendben kezdi meg. A feldolgozás ideje függ az Ügyfél által igényelt Szolgáltatásoktól.

Jelen folyamatoktól külön írásos megállapodás keretében, a jogszabályi és törvényi előírásokat betartva el lehet térni, amennyiben az eltérő tanúsítványigénylési folyamat nem befolyásolja a tanúsítvány kibocsátási folyamat biztonságosságát.

Jelen folyamatokat a Szolgáltató Regisztrációs egysége végzi.

5.2. A tanúsítványkérelem feldolgozása

A tanúsítványkérelem feldolgozási folyamata:

- Az ügyfélszolgálat (RA) ellenőrzi a regisztrációs információkat. Ezután dönt az regisztráció elfogadásáról vagy visszautasításáról.
- Elfogadás esetén az ügyfélszolgálat kitölti a kiadási űrlapot elektronikus formában.

A tanúsítványkérelem létrehozásának folyamata:

- Az ügyfélszolgálat és az RA operátorok hagyhatják jóvá a tanúsítvány kérelmeket.
- Az ügyfélszolgálat (RA) terjeszti elő a tanúsítványkérelmet, amelyhez szükség van a felhasználói adatokra.
- Az elfogadási folyamat egy web alapú interfészen keresztül történik (HTTPS protokollon). Az interfész egy RA modulhoz kapcsolódik, ahol az operátornak a titkos kulcsával kell aláírni a kérelmet.

5.3. A tanúsítvány kibocsátása

A tanúsítvány kibocsátás folyamata:

- A Regisztrációs egység, a tanúsítványigénylés feldolgozását követően, ha a személy- és szervezetazonosítás megtörtént, egyezteti a Szerződésben foglalt adatokat a személy- és szervezetazonosítás során ellenőrzött adatokkal. Ha nem történik személyes megjelenés, a Regisztrációs egység akkor is ellenőrzi a megadott adatokat. Ezután dönt a regisztráció elfogadásáról vagy visszautasításáról.
- Elfogadás esetén az Regisztrációs egység kitölti a kiadási űrlapot elektronikus formában és megküldi az adatokat a Hitelesítő egységnek.
- Az adatok kiegészítésre és megerősítésre (pl.: CRL-ek) kerülnek. Csak az érvényes kérelmek kerülnek az adatbázisba.
- A regisztrációs információk mentésre kerülnek az RA regisztrációs adatbázisába. A tanúsítványok státusz információi el vannak tárolva az adatbázis tábláiban.
- A kulcspár szerver oldalon generálódik.
- A CA operátor érvényesíti a tanúsítvány kérelmeket a CA interfészét használva.
- A CA operátor manuálisan indítja el a tanúsítványok kiadását minden kérésre.
- A kibocsátott tanúsítványok az adatbázisba mentődnek.
- A titkos kulcsot (PKCS#12 állományokat és kapcsolódó jelszavakat) egy különválasztott CA hálózaton levő adatbázisba kell archiválni.
- Ezt követően a Hitelesítő egység kiállítja az igényelt tanúsítványt, majd visszaküldi a Regisztrációs egységnek.
- A Regisztrációs egység az eszközre helyezett Tanúsítványt és kulcsot átadja az Ügyfélnek illetve Alanyainak.
- A Szolgáltató a kibocsátást követően közzéteszi a tanúsítványt a Nyilvános tanúsítványtárában, ha az Ügyfél ehhez előzetesen írásban hozzájárult.

Aláíró tanúsítvány kibocsátható olyan céllal is, hogy az Alanyt más személy (szervezet) képviseletében történő aláírásra jogosítsa fel. Ebben az esetben a bizalmi szolgáltatás igénybe

vevőjére vonatkozó szabályokat a képviselőre kell alkalmazni. A tanúsítvány akkor bocsátható ki, ha a képviseleti jogosultságot igazolják. A képviseleti jogosultság meglétét Szolgáltató ellenőrzi és a kibocsátásról a képviselt személyt (szervezetet) haladéktalanul tájékoztatja.

5.4. A tanúsítvány elfogadása

A tanúsítványok és a kulcsok adathordozókon vannak tárolva. A CA tanúsítványok, felfüggesztési és visszavonási információk (nyilvános adatok) elérhetőek még nyilvános, web alapú könyvtárakban.

A tanúsítvány elfogadás az Alany részéről kétféleképpen történhet:

- online letöltéssel (online igazolás),
- személyes megjelenés alkalmával biztonságos (tanúsított) aláírás-létrehozó eszközön (ALE) való átvétel (személyes igazolás).

Az Alany a tanúsítvány használatba vétele előtt köteles igazolni a tanúsítvány átvételét, és a tanúsítvány adatainak helyességét. Ha az Alany rendellenességet talál, a magánkulcsot nem használhatja fel, hanem azonnal intézkednie kell a tanúsítvány visszavonása érdekében. Amennyiben rendellenességről Szolgáltató nem kap bejelentést a kiadástól számított 1 munkanapon belül, a tanúsítvány elfogadottnak tekintendő és az ebből eredő minden kár és kockázat az Alanyt terheli.

A Szolgáltató a tanúsítvány kibocsátásáról és elfogadásáról értesíti az Alanyt és/vagy Ügyfelet az általa megadott e-mail címen.

5.5. Kulcspár és tanúsítvány használat

Az előre megadott tanúsítvány-profilok tartalmaznak előfeltételeket a keyUsage és extKeyUsage kiegészítőkhöz. Bővebb információkat a Bizalmi Rend ide vonatkozó pontja tartalmaz.

5.5.1. *Az Alanyra és az Érintett félre vonatkozó általános szabályok, ajánlások*

A kulcspár és a tanúsítvány használata során a következő pontokat kell betartani:

- az aláíró valamint bélyegző tanúsítvány alanya az elektronikus aláírás vagy bélyegző létrehozásához használt adatot kizárólag elektronikus aláírás, illetve bélyegző létrehozására használhatja.
- Az elektronikus aláírás vagy elektronikus bélyegző használója a tanúsítványt kizárólag a tanúsítványban szereplő kulcshasználatnak megfelelően használhatja. A használat

során be kell tartani az 2.8. fejezetben, valamin a Szerződésben leírt egyéb korlátozásokat.
- Csak érvényes és fel nem függesztett tanúsítvány használható fel.
- Az Alanynak vagy elektronikus bélyegző esetén a bélyegző alanyának gondoskodnia kell arról, hogy az aláírás-létrehozó adata ne kompromittálódjon. Ha esetleg ez mégis megtörténik, akkor arról a lehetőségei szerint azonnal tájékoztassa a Szolgáltatót és ne alkalmazza azt.

Annak érdekében, hogy az Érintett fél megalapozottan hagyatkozhasson a tanúsítvánnyal hitelesített kriptográfiai kulcspár használatával működő alkalmazásra, ajánlott a kulcspár megfelelő használatát és a hozzá tartozó tanúsítványt az adott helyzetben tőle általában elvárható gondossággal ellenőriznie. Az Érintett fél csak abban az esetben fogadjon el nyilvános kulcsokat, ha azokat a tanúsítványban rögzített módon alkalmazták illetve csak abban az esetben fogadja el a kulcsokhoz tartózó tanúsítványokat, ha azok érvényesek és nincsenek felfüggesztett vagy visszavont állapotban. Elektronikus aláírás és elektronikus bélyegző ellenőrzése esetén, ha az ellenőrzendő elektronikus aláírás, bélyegző a hozzá kapcsolódó tanúsítvány vagy a tanúsítványlánc bármely adata a művelet érvénytelenségére utal, illetve ha az adott alkalmazásban nem elfogadható, akkor az elektronikus aláírást, az elektronikus bélyegzőt és a tanúsítvány elfogadását az Érintett félnek célszerű elutasítania.

Nem érvényes elektronikus aláírás elfogadásból eredő minden kár és kockázat az Érintett felet terheli.

5.5.2. *Elektronikus aláírás, bélyegző készítése*

Az elektronikusan aláírt adat, üzenet, levél vagy bármely dokumentum előállításának folyamatáért elsősorban az Alany a felelős. Az Alany birtokolja a magánkulcsot, ismeri az aláírandó adat, üzenet, levél vagy bármely dokumentum tartalmát, dönt az aláírási szándékról és üzemelteti az aláírást elvégző technikai eszközt. Így ha nem tartja be az alkalmazásra vonatkozó előírásokat (jelen Szabályzat, Bizalmi Rend, Szerződés, törvényi és jogszabályi előírások) úgy az ebből származó kárért ő felel.

Elektronikus bélyegző esetén a bélyegző alanya jogi személy, így az elektronikusan aláírt adat, üzenet, levél vagy bármely dokumentum előállításának folyamatáért elsősorban a jogi személy képviselője a felelős. A képviselő birtokolja a magánkulcsot, ismeri az bélyegzendő adat, üzenet, levél vagy bármely dokumentum tartalmát, dönt az bélyegzési szándékról és üzemelteti az bélyegzést elvégző technikai eszközt. Így ha nem tartja be az alkalmazásra vonatkozó előírásokat (jelen Szabályzat, Bizalmi Rend, Szerződés, törvényi és jogszabályi előírások) úgy az ebből származó kárért ő felel.

5.5.3. *Magánkulcs birtoklása*

A magánkulcsot az Alany, elektronikus bélyegző esetén annak megbízott képviselője birtokolja. Az elektronikus aláírás, bélyegzés csak akkor biztonságos, ha a magánkulcs az Alanyon, vagy alanyon kívül más számára nem hozzáférhető. A kulcsot jelszóval kódoltan és hardvervédelemmel kell ellátni. A kulcs elvesztéséből, véletlen vagy szándékos nyilvánosságra hozatalából eredő károkért az Alany vagy alany a felelős. A kulcs kompromittálódását a Szolgáltatónál be kell jelenteni.

5.5.4. *Az elektronikus aláírás ellenőrzése*

Az elektronikus aláírás elfogadása előtt ellenőrizni kell azt, az alábbiak szerint:

- A tanúsítvány és az aláírás összetartozik.
- Munkatársi tanúsítvány esetén az Alany jogosult-e a tanúsítvány használatára.
- Elektronikus bélyegző esetén szintén vizsgálni kell az alkalmazás jogosultságát.
- A tanúsítvány érvényes volt (érvényességi idő nem telt le, nincs felfüggesztve, visszavonva) az aláírás pillanatában, illetve időbélyeg hiányában az elfogadáskor.
- A tanúsítvány alkalmazása megfelel a tanúsítványban rögzített alkalmazási lehetőségeknek.
- A kibocsátó szervezet tanúsítványa illetve kulcsa érvényes

5.6. Tanúsítvány csere

A tanúsítvány cserét (új tanúsítvány kibocsátása régi kulccsal) Szolgáltató nem támogatja.

5.7. Tanúsítvány megújítás

A tanúsítvány megújítás azt a folyamatot jelenti, amikor egy már a regisztrációs folyamaton átesett Ügyfélnek és/vagy Alanynak a már érvényes Szerződése keretében korábbi tanúsítványa helyett másik tanúsítványt kell kibocsátani. A tanúsítvány megújítás illetve csere minden esetben új tanúsítvány kibocsátását jelenti.

Tanúsítvány megújítás a következő esetekben lehet szükséges meglévő érvényes tanúsítvány esetén:

- a tanúsítvány (és magánkulcs) le fog járni,
- a magánkulcs kompromittálódott,
- a regisztrációs folyamat alatt rögzített adatokban változás történt.

A tanúsítvány megújítására a következő szabályok vonatkoznak:

- A tanúsítvány megújítását az Ügyfél kezdeményezheti.
- A Szolgáltató minden esetben megkövetelheti a személyes megjelenést és azonosítást.
- Abban az esetben, ha az Ügyfél és/vagy Alany korábbi tanúsítványa még érvényes, de szükség van a tanúsítvány megújítására, megfelelő egyeztetések után a korábbi tanúsítványt vissza kell vonni.
- Az adatváltozás esetén a régi tanúsítványt vissza kell vonni és újat kell kiállítani. Az Ügyfélnek illetve az Alanynak a kezdeti regisztrációval megegyező módon igazolnia kell magát és a megváltozott adatokat, a Szolgáltató csak a kezdeti regisztrációval megegyező ellenőrzési folyamatokat követően állítja ki az új tanúsítványt. Minden, a Szolgáltatásokat érintő adatváltoztatást haladéktalanul be kell jelenteni a Szolgáltatónak. Ennek elmulasztása esetén a Szolgáltató nem vállal sem jogi, pénzügyi, sem egyéb felelősséget és garanciát.
- Szolgáltató az új tanúsítványt csak új kulcshoz bocsájt ki.
- Az új tanúsítvány kibocsátása előtt a Szolgáltató ellenőrzi, hogy a régi tanúsítvány létezett-e, valamint, hogy az új tanúsítványba kerülő minden új vagy régi adat helyes és érvényes, ismételt egyeztetést végezhet közhiteles adatbázissal.

5.8. Tanúsítvány felfüggesztése és visszavonása

A Szolgáltató tanúsítvány visszavonási és felfüggesztési szolgáltatást nyújt. A tanúsítvány visszavonása a tanúsítvány-állapotát végérvényesen érvénytelenre állítja, a felfüggesztett tanúsítvány mindaddig, míg felfüggesztett állapotban van, ugyanúgy érvénytelenként kezelendő, mint a visszavont. Egy tanúsítvány egy alkalommal legfeljebb 5 napig lehet felfüggesztett állapotban, ezen időtartam után állapotát újra érvényesre kell állítani, vagy vissza kell vonni. A visszavont tanúsítványokhoz tartozó magánkulcs használatát azonnal meg kell szüntetni és felfüggesztett tanúsítványokhoz tartozó magánkulcs használatát pedig felfüggeszteni. Ha a tanúsítvány visszavonásra kerül a hozzátartozó magánkulcsot a visszavonást követően azonnal meg kell semmisíteni, amennyiben ez lehetséges.

Jogos visszavonási, illetve felfüggesztési kérelem esetén a kérelem feldolgozását követően a Szolgáltató értesíti az Alanyt illetve az Ügyfélt, és legfeljebb 8 órán belül közzéteszi a visszavont, vagy felfüggesztett tanúsítványt egy soron kívül kibocsátott visszavonási listában.

A visszavont, visszavonandó és felfüggesztett, felfüggesztendő tanúsítvány elfogadásából eredő károkra a következő felelősségi szabályok vonatkoznak:

- A visszavonási/felfüggesztési kérelem Szolgáltatóhoz történő megérkezéséig az Alany, illetve az Ügyfél a felelős a felmerülő károkért.
- A visszavonási és felfüggesztési kérelem, Szolgáltató általi befogadását követően (megfelelő azonosítás után), a nyilvánosságra hozatalig a Szolgáltató felelős a felmerülő károkért,
- Amennyiben a Szolgáltató már közzétette a tanúsítvány érténytelen visszavonási állapotát, az Érintett Fél felelős a felmerülő károkért.

5.8.1. *A visszavonás körülményei*

A tanúsítvány visszavonását a következő körülmények tehetik szükségessé:

- Ügyfél kezdeményezése alapján:
  - az Ügyfél visszavonási kérelme,
  - a tanúsítvány magánkulcsának kompromittálódása,
  - a tanúsítványban foglalt adatok megváltozása, érvénytelensége,
  - az aláírás-létrehozó eszköz elvesztése, eltulajdonítása, megrongálódása,
  - az aláírás-létrehozó eszköz hozzáférési adatának kompromittálódása.

- Szolgáltató kezdeményezése alapján:
  - A Szerződés és a Szolgáltató egyéb szabályzatai feltételeinek megszegése Alany, illetve Ügyfél által,
  - az Alany és az Ügyfél kötelezettségeinek be nem tartása (különösen azonnali felmondás, fizetési késedelem esetén),
  - a Szolgáltató tudomására jutott tény a regisztráció során megadott, illetve tanúsítványban szereplő adatok valótlanságáról,
  - a tanúsítványban szereplő Szolgáltatói adatok érvénytelensége,
  - a Szolgáltató valamely magánkulcsának kompromittálódása,
  - a Szerződés megszűnése,
  - az Elektronikus aláírás bizalmi szolgáltatás vagy a Szolgáltató megszűnése,
  - Illetve ha a tanúsítvány aláírására használt algoritmus már nem biztonságos, illetve nem alkalmas tanúsítványok aláírására.

Egyéb visszavonáshoz vezető körülmények:

- az Alany illetve az Ügyfél halála vagy megszűnése,
- a Bizalmi felügyelet vagy más hatóság jogerős és végrehajtható határozata,
- jogszabály rendelkezik így,
- különleges esetek (pl.: szolgáltatói névcsere).

Ezek alapján visszavonást kezdeményezhet:

- Ügyfél, vagy szerződéskötéskor azonosított képviseltje
- Szolgáltató,
- Bizalmi felügyelet vagy más hatóság jogerős és végrehajtható határozat ellenében.

5.8.2. *Visszavonás kérelemre vonatkozó eljárás*

Végfelhasználói tanúsítvány visszavonását kezdeményezheti az Ügyfél, a Szolgáltató, vagy egy hatóság. Az Ügyfélnek és Szolgáltatónak kötelessége az 5.8.1 pontban feltűntetett esetekben a visszavonás azonnali kezdeményezése, illetve végrehajtása.

A tanúsítvány visszavonása - az Ügyfél által - történhet személyesen, vagy írásban (papíron, vagy elektronikusan érvényes és hiteles elektronikus aláírással ellátva). A Szolgáltató a visszavonási kérelmeket kizárólag nyitvatartási időben fogadja. Nyitvatartási időn kívül, tanúsítvány felfüggesztési kérelmet lehet benyújtani, jelen Szabályzat 5.8.3.-5.8.4. pontjaiban leírtak szerint.

A visszavonási kérelmeket a Szolgáltató folyamatosan fogadja és haladéktalanul megkezdi azok feldolgozását. A kérelmet kézhezvételtől számítva a Szolgáltató egy munkanapon belül, soron kívül dolgozza fel. A feldolgozás részeként a Szolgáltató Regisztrációs egysége ellenőrzi a visszavonási kérelemben szereplő adatokat, ellenőrzi a kérelmező személyazonosságát. Ha az adatok helytelenek, a kérelmező kiléte vagy a visszavonásra való jogosultság nem állapítható meg, akkor a Szolgáltató a tanúsítvány visszavonást megtagadja. Valóságnak megfelelő és hiteles kérelem esetén a Szolgáltató további mérlegelés nélkül visszavonja a tanúsítványt. Amint a visszavonási kérelem feldolgozásra került, a Szolgáltató értesíti erről az Alanyt illetve az Ügyfelet, és legfeljebb 8 órán belül közzéteszi a visszavont tanúsítványt egy soron kívül kibocsátott visszavonási listában, és megváltoztatja a tanúsítvány státuszát a tanúsítványtárban.

A visszavonási kérelemnek legalább a következő adatokat kell tartalmaznia:

- a visszavonást igénylő megnevezése, elérhetősége (telefon, e-mail),
- a visszavonást igénylő kapcsolata a tanúsítvány birtokosával, vagyis az Alannyal,
- az Alany megnevezése, elérhetősége (telefon, e-mail),
- a tanúsítvány sorszáma vagy egyedi neve,
- a tanúsítvány típusa és kibocsátási dátuma,
- a visszavonás oka.

- Munkatársi tanúsítvány esetén az Ügyfél részéről a meghatalmazással rendelkező képviselő (aki azonosítva lett a Szerződés megkötésekor) kezdeményezheti a

visszavonást. A visszavonási kérelem mellé a következő dokumentumokat kell csatolnia az Ügyfél meghatalmazottjának:

- aláírási címpéldányt,
- a Szervezet cégkivonatát,
- a meghatalmazással rendelkező képviselő személyes adatait tartalmazó okirat,
- a meghatalmazással rendelkező képviselő meghatalmazását.

A tanúsítvány a visszavonási folyamat végéig felfüggesztett állapotban van, a visszaélések ellen. Ezeket a tanúsítványokat már nem lehet visszaállítani.

Amennyiben egy tanúsítvány visszavonásra került, azt nem lehet újra használatba venni. A tanúsítvány visszavonásával a Szolgáltató és az Ügyfél között létrejött Szerződés megszűnik.

A Szolgáltató a tanúsítvány kiállításának díjait nem téríti vissza.

5.8.3. *A felfüggesztés körülményei*

A tanúsítvány érvényességének felfüggesztését a következő körülmények tehetik szükségessé:

- Alany és Ügyfél kezdeményezése alapján:
  - az Alany illetve az Ügyfél felfüggesztési kérelme.

- Szolgáltató kezdeményezése alapján:
  - megalapozottan feltételezhető, hogy a tanúsítványban foglalt adatok nem felelnek meg a valóságnak,
  - megalapozottan feltételezhető, hogy az aláírás-létrehozó adat nem az aláíró vagy Alany kizárólagos birtokában van,
  - fennálló gyanú a regisztráció során megadott, illetve tanúsítványban szereplő adatok érvénytelenségéről,
  - fennálló gyanú a Szolgáltató valamely magánkulcsának kompromittálódása,
  - az Ügyfél nem teljesíti a Szerződésben vállalt kötelességeit (Pl.: díj nem fizetés).

Egyéb felfüggesztéshez vezető körülmények:

- az Bizalmi felügyelet vagy más hatóság jogerős és végrehajtható határozata,
- jogszabály rendelkezik így.

Ezek alapján a felfüggesztést kezdeményezhet:

- Ügyfél, vagy szerződéskötéskor azonosított képviseltje
- Alany,

- Szolgáltató,
- Bizalmi felügyelet vagy más hatóság jogerős és végrehajtható határozat ellenében.

Szolgáltató a visszavonási kérelmeket ideiglenesen kielégítheti felfüggesztéssel is, amennyiben a bejelentett körülmények kivizsgálását szükségesnek tartja.

A Szolgáltató a tanúsítvány kiállításának díját nem téríti vissza.

5.8.4. *Felfüggesztési kérelemre vonatkozó eljárás*

A tanúsítvány felfüggesztése - az Ügyfél és/vagy Alany által - történhet személyesen, írásban (papíron vagy elektronikusan érvényes és hiteles elektronikus aláírással ellátva) vagy telefonon. A Szolgáltató az írásos felfüggesztési kérelmeket (személyesen, vagy levélben érkezett) kizárólag nyitvatartási időben fogadja. Szolgáltató a telefonos felfüggesztési kérelmeket a hét minden napján, a nap 24 órájában, kizárólag az 1.1 pontban megadott Visszavonási ügyeleti számon fogadja.

A felfüggesztési kérelmet a visszavonási kérelemmel megegyező módon dolgozza fel Szolgáltató.

A tanúsítvány felfüggesztett állapotban addig lehet, míg a visszavonáshoz vezető körülmények fennállásának gyanúja bizonyítást vagy cáfolatot nem nyer, de legfeljebb 5 munkanapig. Kivételtét képez ez alól a Szolgáltató általi technikai felfüggesztés időtartalma, mely legfeljebb 30 naptári nap. A felfüggesztett állapot kezdő időpontja a felfüggesztési kérelem elfogadásától számítandó. Ha ez idő alatt a felfüggesztéshez vezető körülmények gyanúja cáfolatot nem nyer, Szolgáltató a tanúsítványt visszavonja. Ha ez idő alatt a felfüggesztéshez vezető körülmények gyanúja cáfolatot nyer, Szolgáltató a tanúsítványt visszaállítja. Amint a felfüggesztési kérelem feldolgozásra került, a Szolgáltató értesíti erről az Alanyt illetve az Ügyfelet, és legfeljebb 8 órán belül közzéteszi a felfüggesztett tanúsítványt egy soron kívül kibocsátott visszavonási listában.

Felfüggesztett tanúsítvánnyal hitelesített elektronikus aláírás érvénytelennek tekintendő. Érvénytelen elektronikus aláírásnak nincs joghatása.

A felfüggesztett állapotról a Szolgáltató mindig értesíti az Alanyt illetve az Ügyfelet. A tanúsítvány felfüggesztés állapota megjelenik a visszavonási listában is.

A Szolgáltató a tanúsítvány kiállításának díjait nem téríti vissza.

5.8.4.1. Felfüggesztés telefonon

A Szolgáltató a sürgős visszavonási - felfüggesztési kérelmekre való tekintettel (kompromittálódás, eltulajdonítás, stb.) 7*24 órás telefonos ügyeletet tart fenn, kizárólag a Szolgáltató adatainál megnevezett telefonszámon. A telefonbeszélgetés naplózásra és rögzítésre kerül.

Telefonos bejelentés esetén a Szolgáltató csak felfüggeszti a tanúsítványt, a visszavonáshoz az Ügyfélnek írásban (papíron vagy elektronikusan aláírva) kell megerősítenie visszavonási kérelmét. Az így felfüggesztett tanúsítvány akkor kerül visszavonásra, amikor Alany illetve az Ügyfél írásos kérelme a Regisztrációs egységhez beérkezett, vagy a felfüggesztéstől számított 5 munkanap letelt. Ha az Ügyfél és/vagy Alany nem erősíti meg a visszavonást, illetve nem kéri a Tanúsítvány visszaállítását, a Szolgáltató az 5 munkanap leteltével visszavonja a Tanúsítványt és erről értesíti az Ügyfelet és/vagy Alanyt. A Szolgáltató a Tanúsítvány díjait nem téríti vissza.

A felfüggesztésről a Szolgáltató mindig küld tájékoztatást az Ügyfélnek és/vagy Alanynak. Így a felfüggesztésből vagy visszavonásból eredő esetleges károkért a Szolgáltató nem vállalja a felelősséget.

Telefonos bejelentés esetén azonosítás céljából a felfüggesztést igénylő Ügyfélnek és/vagy Alanynak a következő adatokat kell megadnia:

- a kérelmező nevét, jogi státuszát
- kezdeti regisztrációkor megadott felfüggesztési jelszót,
- Ügyfél és Alany nevét,
- a Tanúsítvány azonosítóját,
- kezdeti regisztrációkor megadott igazolvány számát,
- felfüggesztés okát.

A Szolgáltató minden esetben a kezdeti regisztrációkor megadott egyéb adatokra is rákérdezhet.

Ha a Szolgáltató nem tudja egyértelműen azonosítani a felfüggesztést kérelmezőt vagy a felfüggeszteni kívánt Tanúsítványt, illetve a kérelmező nem adja meg a fenti listában szereplő, kötelező adatok valamelyikét, vagy nem a helyes jelszót adja meg, a Szolgáltató elutasítja a felfüggesztési kérelmet.
Ebben az esetben a Szolgáltató nem fogadja be a felfüggesztési kérelmet, a felelősség az Ügyfélé és/vagy az Alanyé.

Amint a Szolgáltató a telefonbeszélgetés során sikeresen megállapította a kérelmező felfüggesztési jogosultságát, befogadja a kérelmet és megkezdi annak feldolgozását. Amint a felfüggesztési kérelem feldolgozásra került, a Szolgáltató értesíti erről az Alanyt illetve az Ügyfelet, és legfeljebb 8 órán belül közzéteszi a felfüggesztett tanúsítványt egy soron kívül kibocsátott visszavonási listában.

A felfüggesztés az összes, a kiadott kártyán és/vagy tokenen szereplő tanúsítványra vonatkozik.

5.8.5. *A tanúsítvány visszaállítása*

A tanúsítvány visszaállítása a felfüggesztett tanúsítvány újbóli érvényesítését jelenti.

Ha az Alany illetve az Ügyfél kérvényezte a felfüggesztést, a felfüggesztés időtartalma alatt kérvényezhet a visszaállítást is, de a visszaállítás esetleges következményeiért ő felel (kompromittálódás, jogtalan használat, stb.). A visszaállítás kérelem benyújtása történhet személyesen, vagy elektronikus úton (érvényes és hiteles elektronikus aláírással ellátva). A visszaállítási kérvény befogadása csak a megfelelő azonosítást követően történik meg.

A Szolgáltató díjat számol fel a Tanúsítvány visszaállításáért. A díj a Szolgáltató internetes oldalán a mindenkori árlistájában szerepel. Ha az Ügyfél a díjat a kiküldött számlán jelzett időpontig nem fizeti meg, a Szolgáltató az ÁSzF-ben foglaltak szerint járhat el.

Ha ugyanarra a tanúsítványra több féltől is érkezik felfüggesztési kérelem, akkor a Szolgáltató csak akkor állítja vissza a tanúsítványt, ha mindegyik felfüggesztő fél kéri a visszaállítást is.

5.9. A tanúsítvány előfizetés vége

A Szolgáltató által kibocsátott tanúsítványok érvényességi idejének lejártával megszűnik az adott tanúsítvány előfizetésének ideje is. Tanúsítvány megújításakor a meglévő Szerződés Szolgáltató és Ügyfél közös akaratával meghosszabbítható, Szolgáltató erre a célra használt Szerződés-módosítási űrlapjának kitöltésével.

Az előfizetés lemondható a lejárati idő előtt az Alany illetve az Ügyfél, vagy Munkatársi tanúsítvány és elektronikus bélyegző esetében a megbízott képviselő által. Ebben az esetben a tanúsítvány visszavonására vonatkozó szabályok az irányadóak, és a tanúsítvány kiállításának díjait a Szolgáltató nem téríti vissza. A visszavonással egy időben a Szerződés is megszűnik.

A Szerződést és a tanúsítvány előfizetést indokolt esetben a Szolgáltató is felmondhatja, és a tanúsítványt visszavonhatja. Ezeket az eseteket részletesen az ÁSzF tartalmazza.

Ha az tanúsítvány érvényességének lejártakor az Alany illetve az Ügyfél a Szolgáltató előírásai szerint nem újítja meg a tanúsítványt, a Szerződés automatikusan megszűnik.

5.10. Nem minősített időbélyegzés szolgáltatás

A Szolgáltató Nem minősített biztonságú időbélyegzés szolgáltatást (továbbiakban: időbélyegzés szolgáltatás) jelen szabályzat és a hozzá kapcsolódó Bizalmi Rend és Időbélyegzési Rend alapján nyújt. Jelen pontban nem szabályozott kérdésekre a jelen szabályzatban a tanúsítvány-szolgáltatásnál, az ÁSzF-ben, és az Időbélyegzési Rendben leírtakat értelemszerűen kell alkalmazni.

Az időbélyegzés szolgáltatást természetes személy vagy szervezet egyaránt igényelhet. Az igénylés történhet e-mail-ben, levélben, vagy személyesen a Szolgáltató ügyfélszolgálati irodájában, illetve előre egyeztetett külső helyszínen is.

Az igénybevétel történhet:

- a Szolgáltatóval történő eseti megállapodás, vagy
- a Szolgáltató által nyújtott ajánlatok, csomagok elfogadott megrendelése keretében.

A szolgáltatás használatához szerződéskötés szükséges. A Szolgáltató csak írásos igényléseket fogad el. A szerződéskötés menete megegyezik a Szerződés megkötésének menetével.

Az Szolgáltatás igénybevétele autentikációs tanúsítvány alapján történik. Az autentikációs tanúsítvány kiállításához szükséges a személyes megjelenés és a kezdeti regisztráció. A kezdeti azonosítás, a tanúsítványigénylés és kibocsátás folyamatának leírása jelen Szabályzat 4. és 5. pontjában található.

Az időbélyegzés szolgáltatás igénybevétele során az Ügyfél egy dokumentum lenyomatát adja meg, amelyre a Szolgáltató aláírt időbélyeget ad vissza.

Az időbélyegzés szolgáltatás rendelkezésre állása 98%, míg az eseti szolgáltatás-kiesések nem haladhatják meg a 24 órát.

A Szolgáltató az Interneten keresztül nyújt időbélyegzés szolgáltatást, publikus szervereinek eléréséhez internetkapcsolat szükséges.

A szolgáltatás a https://pki.digitoll.co.hu/tsa címen érhető el.

6. Létesítmény-, menedzsment- és működésellenőrzés

A Szolgáltató rendelkezik belső, nem publikus Informatikai Biztonság Szabályzattal (IBSz). Az itt nem tárgyalt kérdésekben az IBSz-ben leírtak szerint jár el a Szolgáltató.

6.1. Fizikai óvintézkedés

Szolgáltató gondoskodik arról, hogy a kellő fizikai biztonsági óvintézkedéseket telephelyein és bérelt helyiségein belül garantálja. A kialakított infrastruktúra biztonságos fizikai környezetben üzemel, mely biztosítja a jogosulatlan fizikai és informatikai hozzáférések és belépések megakadályozását, valamint a folyamatos üzemmenetet, melyet a Szolgáltató meghatározott időközönként, előre meghatározott folyamatként ellenőriz.

Szolgáltató a fizikai rendszerellenőrzésről jegyzőkönyvet vezet.

6.1.1. *Telephelyek, bérelt helyek elhelyezkedése*

A Szolgáltató védett számítógép teremben, négy egymástól elkülönített, és fizikailag egymástól nagyobb távolságra elhelyezkedő helyen valósítja meg a szolgáltatásokat.

6.1.2. *Fizikai hozzáférés*

A Szolgáltató által igénybevett helyiségekben gondoskodik a megfelelő fizikai védelemről. Ez telephely illetve bérelt helyiség függvényében állhat:

- riasztórendszerből,
- kamerarendszerből,
- 24 órás őrszolgálatból,
- naplózott, mágneskártyás beléptető rendszerből.

A Szolgáltatás nyújtásához szükséges eszközökhöz csak az arra jogosult és kijelölt biztonsági munkakört betöltő személyek férnek hozzá.

A kommunikáció biztonságos, védett bérelt vonalon történik.

6.1.3. *Áramellátás, légkondicionálás*

A Szolgáltató az általa igénybe vett helyiségekben gondoskodik a megfelelő és folyamatos áramellátásról (redundáns, szünetmentes tápegység) és hűtéséről (légkondicionáló berendezés).

6.1.4. *Tűzvédelem*

A Szolgáltató által igénybevett helyiségekben a tűzmegelőzés és tűzvédelem biztosított.

6.1.5. *Vízvédelem (beázás, elázás)*

A Szolgáltató által igénybevett infrastruktúra beázás és elárasztódás ellen védett. A szervertermek kialakítása biztosítja az elárasztódás veszélyének minimalizálását.

6.1.6. *Adathordozók tárolása*

Az adathordozók tárolása a Szolgáltató telephelyén biztonsági, korlátozott hozzáférésű páncélszekrényben történik.

A páncélszekrény tartalma meghatározott időközönként ellenőrzésre kerül az arra kijelölt személy által.

6.1.7. *Bizalmas minősítésű adatok megsemmisítése, selejtkezelés*

A selejtkezelési szempontból a Szolgáltató megkülönböztet papír alapú és elektronikus alapú bizalmas minősítésű adatokat, melyeket különböző módon semmisít meg, ha azok feleslegessé váltak.

A papír alapú bizalmas minősítésű dokumentumok megsemmisítése aprítógéppel történik.

A bizalmas minősítésű adatokat tartalmazó elektronikus adathordozókat először, az arra kijelölt személy törli, majd szétszereli, végül összetöri. Az adathordozókat még tartalmuk törlése után sem használják fel nem bizalmas minősítésű adatok tárolására.

Az egyéb mágneses adathordozókat demagnetizálás után összetörik.

6.1.8. *Mentési példányok fizikai elkülönítése*

A bizalmas minősítést kapott adatok, dokumentumok, adathordozók fizikailag elkülönítve korlátozott hozzáférésű páncélszekrényben vannak őrizve. Ezen kívül minden adatot

biztonsági mentésként a Szolgáltató elektronikusan is archivál elkülönített rendszeren. Az adatokhoz való hozzáférés korlátozott.

6.2. Folyamatellenőrzés

A működési folyamatok Ellenőrző listákban vannak rögzítve.

A rendszer informatikai működésének ellenőrzését, az arra kijelölt személy havi rendszerességgel megteszi a lista vezetésével. A felelős vezető minden hónap elején ellenőrzi a listák vezetését.

A rendszer ellenőrzése havonta egyszer történik Ellenőrzési lista vezetésével, az ellenőrzést az arra kijelölt személy végzi.

Ha a folyamat ellenőrzése közben az ellenőrző személy hibát vagy rendellenességet talál, naplózza és haladéktalanul jelenti a felelős vezetőnek. A felelős vezető elrendeli a hiba javítását. A hibajavítást követően újabb rendszerellenőrzésre kerül sor.

6.3. Személyzet ellenőrzése

Szolgáltató kellő számú, szolgáltatások nyújtásához szükséges feladatok jellegének megfelelő tudással rendelkező személyzetet alkalmaz. Az alkalmazottak a feladatok szétválasztása és a meghatalmazás szempontjai szerint meghatározott munkaköri leírásokkal rendelkeznek. A munkaleírások meghatározzák a munkakört és az ahhoz kapcsolatos feladatokat.

A munkakörökhöz kapcsolódó elvárt azonosítás és hitelesítés a következőek:

- A szolgáltatást ellátó személyek a regisztrációval és tanúsítvány-kezeléssel kapcsolatos alkalmazások használata előtt megfelelő azonosítási és hitelesítési eljáráson esnek át.
- A bizalmas munkakörben dolgozók csak chipkártyás azonosítással végezhetik a munkájukat, mely hatáskörileg, és hozzáférési szint alapján is szabályozva van.

Az személyzet munkáját a felelős vezető ellenőrzi. A szerepkörök elosztását a Bizalmi munkakörök dokumentum tartalmazza.

6.3.1. *A bizalmi munkakörök*

Általános felelős vezető: a szolgáltató informatikai rendszeréért általánosan felelős vezető

Rendszergazda:

- Rendszeradminisztrátor: az informatikai rendszer telepítését, konfigurálását, karbantartását végző személy.

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

Biztonsági tisztviselő: a szolgáltatás biztonságáért általánosan felelős személy.

Regisztrációs felelős: a végtanúsítványok előállításának, kibocsátásának, visszavonásának és felfüggesztésének jóváhagyásáért felelős személy.

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.

A Szolgáltató biztosítja, hogy a bizalmi munkakörök közül:

- a biztonsági tisztviselő nem láthatja el a független rendszervizsgáló és az informatikai rendszerért általánosan felelős vezető feladatait;

- a független rendszervizsgáló nem láthatja el az informatikai rendszerért általánosan felelős vezető feladatait.

A kinevezett személyek munkaköri leírása tartalmazza a feladatukat és titoktartási nyilatkozatot írnak alá.

6.4. Vizsgálati naplózás folyamatai

A Szolgáltató gondoskodik arról, hogy az általa vagy megbízottja által elvégzett műveletek, illetve a Szolgáltatásokkal kapcsolatos rögzített adatok megőrzésre kerüljenek, különösen jogi eljárásokhoz bizonyíték nyújtása érdekében.

A naplóbejegyzések többek között a regisztráció, az aláírás-létrehozó és ellenőrző kulcs-pár generálása, az aláírás-létrehozó eszköz megszemélyesítése, a tanúsítvány létrehozása, kibocsátása és kezelése, valamint egyéb szolgáltatói tevékenységek és az esetleges hibaesemények során készülnek. A naplózott adatállománynak tartalmazzák a naplózott esemény bekövetkeztének dátumát és pontos idejét, az esemény követhetőségéhez, rekonstruálásához szükséges adatokat, az esemény kiváltásában közreműködő felhasználó vagy más személy nevét vagy azonosítóját.

A naplók vezetését a műveleteket végző, azonosított személy végzi, az ellenőrzési feladatokat a felelős vezető látja el.

6.5. Feljegyzések archiválása

A szolgáltatás nyújtása közben létrejött papír alapú dokumentumokat, papír és elektronikus adat formájában (mint biztonsági mentés) is tárolja a Szolgáltató. A Szolgáltató a napló adatokat fokozott biztonságú fizikai környezetben menti el, a mentett állományokat időbélyeggel ellátott elektronikus aláírással hitelesíti, és védett környezetben tárolja. A naplók olvasása hozzáférési jogosultság szerint korlátozott. A papír alapú adatokat a felelős vezető lezárásként aláírásával látja el és elzárva tárolja. Az intézményi biztonsági dokumentumai szintén ezen eljárás keretében kerülnek mentésre.

Az informatikai rendszerben keletkező napló állományokról (log), adatbázisokról napi egyszeri mentés készül. A lementett fájlokat a szolgáltató külön fizikai eszközön, jelszóval ellátva tárolja. A szerverekről a mentés hetente történik.

A tanúsítvány visszavonási kérelmek pontos naplózásra kerülnek. Ha a kérelem telefonon érkezik, a telefont kezelő személyzet rögzíti a hívás időpontját, a hívó félt, a hívás indokát, függetlenül attól, hogy a hívó félt sikeresen azonosította e vagy sem.

Az E-ügyintézési tv. 84. § (1) szerint Szolgáltató az egyes tanúsítványokkal kapcsolatosan rendelkezésére álló információkat - beleértve az azok előállításával összefüggőket is - és az ahhoz kapcsolódó személyes adatokat legalább a tanúsítvány érvényességének lejártától számított tíz évig megőrzi. Ha a Szolgáltatót valamely igénybevevő, hatóság vagy bíróság a tanúsítványba foglalt adat valódiságával vagy érvényességével kapcsolatosan megindult jogvitáról értesíti, Szolgáltató a megőrzési kötelezettségének a jogvita jogerős lezárásáig akkor is köteles eleget tenni, ha a tanúsítvány lejártától számított tízéves határidő már lejárt. A Szolgáltató a megőrzési határidő lejártáig olyan eszközt is biztosít, amellyel a kibocsátott tanúsítvány tartalma megállapítható.

6.6. Informatikai biztonság

6.6.1. *Jelszókezelés*

A Szolgáltató munkatársai és megbízottjai meghatározott azonosítási eljárást követően saját azonosító tokent kapnak, a rendszerhez való hozzáféréshez – jogosultság függvényében - megfelelően generált jelszót kapnak. A jelszavak tárolása fizikailag biztonságos környezetben, ellenőrzötten történik.

6.6.2. *Vírusirtás*

A Szolgáltató a szolgáltatásban használt számítógépei vírus és kémprogram elleni védelemmel rendelkeznek. Ezek frissítése a „Biztonsági protokollok” pontban foglaltak szerint történik.

6.6.3. *Tűzfal*

A Szolgáltató a szolgáltatás nyújtásához dedikált tűzfallal rendelkezik, melyen több biztonsági zóna is kialakításra került. A tűzfalszabályok kialakítása szerint külön zónába tartoznak a publikus elérésű szerverek, a nem publikus elérésű szerverek, az egyéb, biztonsági funkciókat megvalósító hardverelemek, és a munkaállomások. A zónák közötti átjárás hálózati port, MAC cím és IP cím alapján szűrve van.

6.6.4. *Biztonsági protokollok*

6.6.4.1. Publikus elérés

A szolgáltatást nyújtását biztosító rendszer a Szolgáltató egyéb informatikai infrastruktúrájától elszigetelve működik. A szolgáltató rendszer kívülről, az internet felhasználásával nem elérhető (kivéve a publikus szervereket).

6.6.4.2. Rendszerfrissítések

A szükséges operációs rendszer és vírusadatbázis frissítéseket a megfelelő technikai személyzet minden hónap első napján végzi el a munkaállomásokon. A szervereken előzetesen kitűzött tervezett rendszerkarbantartás keretében történik a telepítés.

6.6.4.3. Adathordozók használata

A szolgáltatás nyújtásához használt munkaállomásokon házirendben (policy) tiltott az USB adattároló eszközök használata, az adatszivárgás megakadályozása érdekében. Ugyancsak tiltott az optikai lemezek írása.

Az adathordozók használata szabály alól kivételt képeznek a rendszer felügyeletét ellátó személyek.

6.7. Helyreállítás betörés vagy katasztrófa után

Katasztrófa illetve betörés, rongálás következtében alkalmazandó eljárásokat a „Helyreállítási terv rendkívüli üzemhelyzetek esetén” című dokumentum tartalmazza.

Rendkívüli üzemeltetési helyzet bekövetkezése esetén Szolgáltató haladéktalanul értesíti a vele szerződéses viszonyban lévő ügyfeleit, valamint erre vonatkozó tájékoztatást tesz közzé internetes oldalán. Szolgáltató értesíti az Bizalmi felügyeletet is a rendkívüli üzemeltetési helyzet bekövetkezéséről, annak várható hatásairól és időtartamáról, a rendkívüli üzemeltetési helyzet elhárítása érdekében tett és tervezett intézkedésekről, az elhárítás közben esetlegesen felmerült további következményekről, valamint a rendkívüli üzemeltetési helyzet megszűnéséről is. A Szolgáltató hivatkozott dokumentumában részletesen szabályozza a különböző sérülések és katasztrófahelyzetek esetén követendő eljárásokat. Jelen Szabályzatban a katasztrófa elhárítási irányelveket foglaljuk össze.

6.7.1. *Sérült számítási erőforrások, szoftverek és/vagy adatok*

Szolgáltató megnövelt biztonságú eszközökkel rendelkezik, a hardver és/vagy szoftver meghibásodások, illetve az adatvesztés elkerülése érdekében. A Szolgáltatások infrastruktúrájának helyreállíthatóságát Szolgáltató szerződései és saját tartalék eszközei biztosítják. Szolgáltató rendszeres biztonsági mentései és naplózási rendszere segítségével teszi lehetővé az adatok visszaállíthatóságát valamely adattároló eszköz meghibásodásának esetére. Szolgáltató ily módon képes a megelőzően elkészített biztonsági mentései közül a megfelelő működőképes állapotot visszaállítani. Az esetleges hibákról, és a visszaállított állapotokról Szolgáltató jegyzőkönyvet készít.

6.7.2. *Szolgáltatói egység kulcsának kompromittálódása*

Szolgáltató hivatkozott dokumentumában rendelkezik a szolgáltatói egység magánkulcsának kompromittálódása esetén követendő eljárásokról. A Szolgáltató saját magánkulcsainak kompromittálódása esetén:

- Beszünteti a kompromittálódott kulcs használatát. Visszavonja a kompromittálódott kulcshoz tartozó tanúsítványt.
- Azonnali hatállyal értesíti a Végfelhasználókat jelen Szabályzat 3.1.2. pontja szerint. Az értesítésben jelzi, hogy az adott szolgáltatói kulcs felhasználásával kiadott tanúsítványok és visszavonási állapot információk már nem érvényesek.
- Szükség esetén új tanúsítvánnyal (és hozzá tartozó kulccsal) látja el az Ügyfeleket és Alanyokat, a szolgáltatói egységet.

- Kivizsgálja a kompromittálódás körülményeit és megteszi a szükséges lépéseket a kompromittálódás megismétlődése ellen.

6.7.3. *Helyreállítás természeti, vagy egyéb katasztrófát követően*

Szolgáltató a Szolgáltatásokkal kapcsolatos tevékenységeit négy, egymástól fizikailag is nagyobb távolságra elhelyezkedő helyszínen végzi. Szolgáltató kialakított struktúrájára jellemző, hogy:

- rendelkezik elsődleges, és másodlagos helyszínnel is,
- elkülönített biztonsági zónával rendelkezik a kiemelt biztonságú eszközök számára (pl.: HSM),
- ügyfélszolgálati irodája az elsődleges és másodlagos helyszíntől elkülönülő, független egységet képez.

Természeti vagy más katasztrófát követően, illetve Szolgáltató rendszereinek olyan szintű meghibásodásakor, amely az elsődleges rendszeren nem, vagy csak hosszabb kieséssel javítható, Szolgáltató a másodlagos helyszínen is képes szolgáltatásai egy részének beindítására. Ilyen esetekben Szolgáltató az alábbi Szolgáltatások legfeljebb 24 órán belüli elindítását vállalja:

- a tanúsítványtár közzététele,
- a felfüggesztés- és visszavonás-kezelés,
- a visszavonási állapot közzététele.

6.8. Szolgáltatások megszűnése

A Szolgáltató a jogszabályokban előírtaknak megfelelően gondoskodik a szolgáltatásainak megszüntetéséből származó, az Alanyokat, Ügyfeleket és az Érintett feleket érintő potenciális zavar minimalizálásáról, továbbá a jogi eljárásokhoz szükséges tanúsítvány nyilvántartások fenntartásáról.

A szolgáltatás megszűnése esetén a Szolgáltató az E-ügyintézési tv. 88. §-a szerint jár el, melyek összefoglalva a következőek:

- A Szolgáltató a szolgáltatásainak befejezéséről legkésőbb a tevékenység megszüntetésekor tájékoztatja a Bizalmi felügyeletet, a szolgáltatás ügyfeleit (Ügyfelek), valamint az általa kibocsátott és még vissza nem vont elektronikus aláírás és bélyegző tanúsítványokban megjelölt (bizalmi szolgáltatási ügyfélnek nem minősülő) igénybe vevőket (Alanyok).

- Ha Szolgáltató más bizalmi szolgáltatás nyújtását továbbra is folytatja, akkor gondosodik a megszüntetni kívánt szolgáltatással összefüggő, a nyilvánosság számára elérhető nyilvántartásainak folyamatos elérhetőségéről (CRL listák).
- Ha a Szolgáltatás megszűnésekor a Bizalmi felügyelet nyilvántartásában nincs megfelelő bizalmi szolgáltató, az átvevő bizalmi szolgáltató feladatait a bizalmi felügyelet látja el.
- A Szolgáltató a bejelentését követően nem bocsát ki új tanúsítványokat.
- A Szolgáltató a tevékenységének befejezésre megjelölt időpontot megelőző 20 nappal visszavonja az általa kibocsátott és érvényes tanúsítványokat.
- A Szolgáltató a tevékenységének befejezésre megjelölt időpontig eleget tesz a nyilvánosságra hozatali kötelességeinek.
- A Szolgáltató megjelöl - egy vele azonos besorolású - szolgáltatót mely átveszi a tanúsítvány visszavonási listákat, a visszavonási állapot nyilvántartásokat (felfüggesztés és visszavonás információkat), a visszavont tanúsítványokkal kapcsolatos minden adatot (naplófájlokat, megőrzési időket), továbbá a visszavont tanúsítványokhoz kapcsolódó személyes adatokat, a nyilvános szabályozási dokumentumokat, valamint az aláírás ellenőrző adatokat. Ezt egy keretszerződés kereteiben teszi meg.
- Ha a bizalmi szolgáltatás megszűnésekor a bizalmi felügyelet nyilvántartásában nincs megfelelő bizalmi szolgáltató, az átvevő bizalmi szolgáltató feladatait a bizalmi felügyelet látja el.

Ha Szolgáltató ellen felszámolási, végelszámolási vagy kényszertörlési eljárás indult, a bizalmi szolgáltató haladéktalanul köteles erről és a felszámolóról vagy végelszámolóról tájékoztatni a bizalmi felügyeletet. A bizalmi felügyelet az eljárás időtartama alatt jogosult a felszámolótól, végelszámolótól vagy a kényszertörlési eljárást lefolytató cégbíróságtól a felszámolás, végelszámolás vagy a kényszertörlési eljárás állásáról tájékoztatást kérni.

7. Műszaki biztonsági ellenőrzés

7.1. Kulcspár-generálás és telepítés

A CA-knak számos kérést kell kezelniük:

- végfelhasználói tanúsítvány kiállítás PKCS#10 kérések feltöltése alapján
- végfelhasználói tanúsítvány kiállítás szerveroldalon generált kulcspárok alapján

A CA kulcsa a biztonságos HSM eszközön belül került létrehozásra, a kulcs aktiválásához egyidejűleg egy darab eszköz (chipkártya) és jelszó megadása szükséges. Összesen négy darab chipkártya került létrehozásra, azaz az „n-ből m” jelen esetben „4-ből 1” a hitelesítésnél.

A Szolgáltató által használt kulcspárok az alábbiak:

- a Szolgáltató gyökér hitelesítő egységének kulcsa 4096 bites,
- a Szolgáltató fokozott időbélyegző egységének kulcsa 2048 bites,
- a Szolgáltató operátori kulcsai 2048 bitesek,
- SSL protokollhoz használt kulcsok 2048 bitesek,
- a végfelhasználói tanúsítványokban lévő kulcsok legalább 2048 bitesek.

A kulcsok a tanúsítványokkal együtt a Szolgáltató által kerülnek feltöltésre az adathordozóra (chipkártya), ez alól a letölthető, valamint a weboldal-hitelesítő tanúsítványok képeznek kivételt, ahol PKCS#12 adatként kerülnek átadásra, külön csatornán eljuttatott jelszó segítségével.

7.2. Magánkulcs megsemmisítése

A hitelesítő egység HSM eszközében tárolt magánkulcsok megsemmisítése a Szolgáltató két munkatársának (a rendszergazda és a biztonsági tisztviselő) együttes jelenlétében lehetséges.

A végfelhasználói tanúsítványokban használt magánkulcsok megsemmisítése az Aláíró felelőssége. A Szolgáltató vállalja ügyfélszolgálati irodájában az intelligens kártyán, vagy tokenen lévő magánkulcsok ügyfél előtt történő megsemmisítését.

7.3. Alkalmazott eszközök

A Szolgáltató a szolgáltatás nyújtásához (kulcskezelés, tárolás, előállítás) nCipher nShield Connect 500 (nShield F3 500e nC4033E-500N) típusú HSM eszközt használ. Az alkalmazott eszköz förmver verziói: 2.38.4-3 és 2.38.7-3.

A végfelhasználói eszközök kulcspár és tanúsítvány tárolására alkalmas aláírás-létrehozó eszközök, melyek típusa Gemalto IDPrime MD, és CCEAL 5+ tanúsítással rendelkeznek. A végfelhasználói eszközök képesek a BALE üzemmódra is, de Szolgáltató jelenleg ALE módban biztosítja az eszközöket

Szolgáltató által használt algoritmusok megfelelnek a mindenkori törvényeknek, jogszabályoknak és ajánlásoknak. Felhasznált algoritmus SHA256 with RSA, 2048-8192 bites kulcshosszal.

1124 Budapest, Stromfeld Aurél út 9.
Tel.: +361 487 9900
E-mail: digitoll@digitoll.co.hu
Web: www.digitoll.co.hu

7.4. Privát kulcsok védelme és a kriptográfiai modul technikai ellenőrzése

A privát kulcsok egy biztonságos hardveres környezetben (aláíró kulcsok) tárolódnak.

A kulcsokat tároló adathordozóknak és kriptográfiai moduloknak független biztonsági ellenőrök által készített igazolások közül legalább egy érvényes tanúsítással rendelkeznie kell.

Szolgáltató HSM modulja FIPS 140-2 level 3 tanúsítással rendelkezik.

A Szolgáltató által az Alanyok részére kiadott végfelhasználói eszközöknek

- Common Criteria EAL5, vagy magasabb tanúsítással kell rendelkezniük.

Amennyiben az Alany saját, már meglévő végfelhasználói eszközét kívánja használni, ugyanezeket a tanúsításokat kell tudnia igazolni az eszközzel kapcsolatban.

7.5. A kulcspár-kezelés egyéb szempontjai

A publikus kulcsok és a tanúsítványok is archiválva tárolódnak. Ez a rendszeres biztonsági mentési folyamat része.

7.6. Aktivációs adatok

Az adathordozókon tárolt, újonnan kiadott tanúsítványokat és kulcsokat jelszó védi. Az adathordozók jelszavát a felhasználó bármikor megváltoztathatja.

7.7. Hálózat és számítógép-biztonsági ellenőrzés

Jelen dokumentum ide vonatkozó pontja, illetve belső biztonsági policy szerint történik.

7.8. Időbélyegzés

A tanúsítványok és a visszavonási információ (CRL) idő- és dátuminformációkat tartalmaznak. Így az idő és a dátum alá van írva.

8. Tanúsítvány-, és CRL-profilok

A profilokban megnevezésre kerülő mezők, névtípusok értelmezése és a rá vonatkozó szabályok, jelen szabályzat 4.1 pontjában találhatóak.

8.1. Tanúsítványprofil

mező/kiterjesztés	tartalom
version	kötelező; tanúsítvány változata (v3)
serialNumber	kötelező; tanúsítvány sorszáma
signature	kötelező; tanúsítvány aláírása (a hatályos törvényi és jogszabályi előírásoknak, illetve a nemzetközi ajánlásoknak megfelelően)
issuer	A tanúsítványt kiadó CA adatai
validity	A tanúsítvány érvényességének kezdete és vége
subject	(ld. táblázatok)
subjectPublicKeyInfo	(ld. táblázatok)
extensions	(ld. táblázatok)

Az alapesettől való eltéréseket az alábbi táblázatok határozzák meg.

8.1.1. *Természetes személyek tanúsítvány profiljai*

8.1.1.1. Személyi fokozott biztonságú aláíró tanúsítvány

mező/kiterjesztés	tartalom
commonName	kötelező; tanúsítvány alanya azonosító okmányban szereplő neve
emailAddress	kötelező; tanúsítvány alanyának e-mail címe (megegyezik az subjectAltName névelemmel)
serialNumber	opcionális mező; tanúsítvány alanyának egyedi azonosítója
countryName	kötelező; tanúsítvány alanyához kapcsolódó ország neve
localityName	opcionális; tanúsítvány alanyához kapcsolódó település neve
title	opcionális; tanúsítvány alanyának titulusa
subjectAltName	kötelező; tanúsítvány alanyának címe (megegyezik az emailAddress névelemmel), vagy Microsoft UPN eleme
subjectPublicKeyInfo	kötelező; tanúsítvány alanyának nyilvános kulcsa (2048 bit)
basicConstraints	kötelező; tanúsítvány típusa (végfelhasználói)

keyUsage	kötelező; tanúsítvány kulcshasználata (digitalSignature, nonRepudiation)
validity	kötelező; tanúsítvány érvényessége (365 nap)
cRLDistributionPoints	tanúsítványhoz kapcsolódó visszavonási adatok elérhetősége http://pki.digitoll.co.hu/pki/crls/rootca_adv.crl
certificatePolicies	tanúsítványhoz kapcsolódó Bizalmi Rend elérhetősége: http://ds.digitoll.co.hu/documents/cp_1_3_6_1_4_1_46800_1_2_1_6.pdf

8.1.1.2. Személyi fokozott biztonságú álneves aláíró tanúsítvány

mező/kiterjesztés	tartalom
commonName	kötelező; tanúsítvány alanyának álnév ténye
pseudonym	kötelező; tanúsítvány alanyának álneve
emailAddress	kötelező; tanúsítvány alanyának e-mail címe (megegyezik az subjectAltName névelemmel)
serialNumber	opcionális mező; tanúsítvány alanyának egyedi azonosítója
countryName	kötelező; tanúsítvány alanyához kapcsolódó ország neve
localityName	opcionális; tanúsítvány alanyához kapcsolódó település neve
title	opcionális
subjectAltName	kötelező; tanúsítvány alanyának e-mail címe (megegyezik az emailAddress névelemmel)
subjectPublicKeyInfo	kötelező; tanúsítvány alanyának nyilvános kulcsa (2048 bit)
basicConstraints	kötelező; tanúsítvány típusa (végfelhasználói)
keyUsage	kötelező; tanúsítvány kulcshasználata (digitalSignature, nonRepudiation)
validity	kötelező; tanúsítvány érvényessége (365 nap)
cRLDistributionPoints	tanúsítványhoz kapcsolódó visszavonási adatok elérhetősége http://pki.digitoll.co.hu/pki/crls/rootca_adv.crl
certificatePolicies	tanúsítványhoz kapcsolódó Bizalmi Rend elérhetősége: http://ds.digitoll.co.hu/documents/cp_1_3_6_1_4_1_46800_1_2_1_6.pdf

8.1.1.3. Munkatársi fokozott biztonságú aláíró tanúsítvány

mező/kiterjesztés	tartalom
commonName	kötelező; tanúsítvány alanya azonosító okmányban szereplő neve
emailAddress	kötelező; tanúsítvány alanyának e-mail címe (megegyezik az subjectAltName névelemmel)
countryName	kötelező; tanúsítvány alanyához kapcsolódó ország neve

localityName	opcionális; tanúsítvány alanyához kapcsolódó település neve
title	opcionális; tanúsítvány alanyának titulusa, beosztása
organizationName	tanúsítvány alanyához kapcsolódó szervezet neve
organizationalUnitName #1	tanúsítvány alanyához kapcsolódó szervezeti egység neve
organizationalUnitName #2	tanúsítvány alanyához kapcsolódó szervezeti egység neve
subjectAltName	kötelező; tanúsítvány alanyának e-mail címe (megegyezik az emailAddress névelemmel)
subjectPublicKeyInfo	kötelező; tanúsítvány alanyának nyilvános kulcsa (2048 bit)
basicConstraints	kötelező; tanúsítvány típusa (végfelhasználói)
keyUsage	kötelező; tanúsítvány kulcshasználata (digitalSignature, nonRepudiation)
validity	kötelező; tanúsítvány érvényessége (365 nap)
cRLDistributionPoints	tanúsítványhoz kapcsolódó visszavonási adatok elérhetősége http://pki.digitoll.co.hu/pki/crls/rootca_adv.crl
certificatePolicies	tanúsítványhoz kapcsolódó Bizalmi Rend elérhetősége: http://ds.digitoll.co.hu/documents/cp_1_3_6_1_4_1_46800_1_2_1_6.pdf

8.1.1.4. Munkatársi fokozott biztonságú álneves aláíró tanúsítvány

mező/kiterjesztés	tartalom
commonName	kötelező; tanúsítvány alanyának álnév ténye
pseudonym	kötelező; tanúsítvány alanyának álneve
emailAddress	kötelező; tanúsítvány alanyának e-mail címe (megegyezik az subjectAltName névelemmel)
countryName	kötelező; tanúsítvány alanyához kapcsolódó ország neve
localityName	opcionális; tanúsítvány alanyához kapcsolódó település neve
title	opcionális
organizationName	tanúsítvány alanyához kapcsolódó szervezet neve
organizationalUnitName #1	tanúsítvány alanyához kapcsolódó szervezeti egység neve
organizationalUnitName #2	tanúsítvány alanyához kapcsolódó szervezeti egység neve
subjectAltName	kötelező; tanúsítvány alanyának e-mail címe (megegyezik az emailAddress névelemmel)
subjectPublicKeyInfo	kötelező; tanúsítvány alanyának nyilvános kulcsa (2048 bit)
basicConstraints	kötelező; tanúsítvány típusa (végfelhasználói)

keyUsage	kötelező; tanúsítvány kulcshasználata (digitalSignature, nonRepudiation)
validity	kötelező; tanúsítvány érvényessége (365 nap)
cRLDistributionPoints	tanúsítványhoz kapcsolódó visszavonási adatok elérhetősége http://pki.digitoll.co.hu/pki/crls/rootca_adv.crl
certificatePolicies	tanúsítványhoz kapcsolódó Bizalmi Rend elérhetősége: http://ds.digitoll.co.hu/documents/cp_1_3_6_1_4_1_46800_1_2_1_6.pdf

8.1.2. *Nem természetes személy fokozott biztonságú tanúsítvány profiljai*

8.1.2.1. Szervezet fokozott biztonságú bélyegző tanúsítványa

mező/kiterjesztés	tartalom
commonName	kötelező; tanúsítvány alanyának bejegyzett neve
emailAddress	kötelező; tanúsítvány alanyának e-mail címe (megegyezik az subjectAltName névelemmel)
countryName	kötelező; tanúsítvány alanyához kapcsolódó ország neve
localityName	opcionális; tanúsítvány alanyához kapcsolódó település neve
organizationName	tanúsítvány tulajdonosához kapcsolódó szervezet neve
organizationalUnitName #1	tanúsítvány alanyához kapcsolódó szervezeti egység neve
organizationalUnitName #2	tanúsítvány alanyához kapcsolódó szervezeti egység neve
subjectAltName	kötelező; tanúsítvány alanyának e-mail címe (megegyezik az emailAddress névelemmel)
subjectPublicKeyInfo	kötelező; tanúsítvány alanyának nyilvános kulcsa (2048 bit)
basicConstraints	kötelező; tanúsítvány típusa (végfelhasználói)
keyUsage	kötelező; tanúsítvány kulcshasználata (digitalSignature, nonRepudiation)
validity	kötelező; tanúsítvány érvényessége (365 nap)
cRLDistributionPoints	tanúsítványhoz kapcsolódó visszavonási adatok elérhetősége http://pki.digitoll.co.hu/pki/crls/rootca_adv.crl
certificatePolicies	tanúsítványhoz kapcsolódó Bizalmi Rend elérhetősége: http://ds.digitoll.co.hu/documents/cp_1_3_6_1_4_1_46800_1_2_1_6.pdf

8.1.2.2. Fokozott biztonságú weboldal-hitelesítő tanúsítvány

mező/kiterjesztés	tartalom
commonName	kötelező; tanúsítvány alanyának neve (domain név, egyéb megnevezés)
countryName	kötelező; tanúsítvány tulajdonosának lakcíme vagy bejelentett székhelye szerinti ország neve
localityName	opcionális; tanúsítvány tulajdonosának lakcíme vagy bejelentett székhelye szerinti település neve
organizationName	tanúsítvány alanyához kapcsolódó szervezet neve, magánszemély igénylése esetén a magánszemély neve
subjectAltName	kötelező; tanúsítvány alanyának e-mail címe (megegyezik az emailAddress névelemmel)
subjectPublicKeyInfo	kötelező; tanúsítvány tulajdonosának nyilvános kulcsa (2048 bit)
basicConstraints	kötelező; tanúsítvány típusa (végfelhasználói)
keyUsage	kötelező; tanúsítvány kulcshasználata (digitalSignature, keyEncipherment, keyAgreement, dataEncipherment)
extKeyUsage	tanúsítvány kibővített kulcshasználata (serverAuth)
validity	kötelező; tanúsítvány érvényessége (365 nap)
cRLDistributionPoints	tanúsítványhoz kapcsolódó visszavonási adatok elérhetősége http://pki.digitoll.co.hu/pki/crls/rootca_adv.crl
certificatePolicies	tanúsítványhoz kapcsolódó Bizalmi Rend elérhetősége: http://ds.digitoll.co.hu/documents/cp_1_3_6_1_4_1_46800_1_2_1_6.pdf

8.1.3. *Szolgáltatók tanúsítvány profiljai*

8.1.3.1. CA tanúsítványa

mező/kiterjesztés	tartalom
commonName	kötelező; tanúsítvány tulajdonosának neve
countryName	kötelező; tanúsítvány tulajdonosához kapcsolódó ország neve
localityName	opcionális; tanúsítvány tulajdonosához kapcsolódó település neve
subjectPublicKeyInfo	kötelező; tanúsítvány tulajdonosának nyilvános kulcsa (4096 bit)
basicConstraints	kötelező; tanúsítvány típusa (CA)
keyUsage	kötelező; tanúsítvány kulcshasználata (cRLSign, keyCertSign)
validity	kötelező; tanúsítvány érvényessége (5479 nap)
cRLDistributionPoints	tanúsítványhoz kapcsolódó visszavonási adatok http://pki.digitoll.co.hu/pki/crls/rootca_adv.crl
certificatePolicies	tanúsítványhoz kapcsolódó Bizalmi Rend elérhetősége: http://ds.digitoll.co.hu/documents/cp_1_3_6_1_4_1_46800_1_2_1_6.pdf

8.1.3.2. TSA fokozott biztonságú végtanúsítványa

mező/kiterjesztés	tartalom
commonName	kötelező; tanúsítvány tulajdonosának neve
countryName	kötelező; tanúsítvány tulajdonosához kapcsolódó ország neve
localityName	opcionális; tanúsítvány tulajdonosához kapcsolódó település neve
subjectPublicKeyInfo	kötelező; tanúsítvány tulajdonosának nyilvános kulcsa (4096 bit)
basicConstraints	kötelező; tanúsítvány típusa (végfelhasználói)
keyUsage	kötelező; tanúsítvány kulcshasználata (nonRepudiation)
extKeyUsage	tanúsítvány kibővített kulcshasználata (timeStamping)
validity	kötelező; tanúsítvány érvényessége (1825 nap)
cRLDistributionPoints	tanúsítványhoz kapcsolódó visszavonási adatok elérhetősége http://pki.digitoll.co.hu/pki/crls/rootca_adv.crl
certificatePolicies	tanúsítványhoz kapcsolódó Bizalmi Rend elérhetősége: http://ds.digitoll.co.hu/documents/cp_1_3_6_1_4_1_46800_1_2_1_6.pdf

8.2. CRL-profil

A CRL visszavonási adatok profilja az IETF RFC 2459 szabványban leírt v2 változatnak felel meg.

mező/kiterjesztés	tartalom
version	kötelező; visszavonási adat változata (v2)
signature	kötelező; visszavonási adat aláírása (a hatályos törvényi és jogszabályi előírásoknak, illetve a nemzetközi ajánlásoknak megfelelően)
issuer	kötelező; visszavonási adat kibocsátója
thisUpdate	kötelező; visszavonási adat kibocsátásának dátuma és időpontja
nextUpdate	visszavonási adat következő kibocsátásának dátuma és időpontja (thisUpdate + 24 óra)
revokedCertificates	kötelező; visszavonási adaton szereplő tanúsítványok sorszáma, a visszavonás dátuma és időpontja, a visszavonás oka

8.3. Időbélyeg profilok

Az időbélyegek profilja az IETF RFC 3161 szabványban leírt v1 változatnak felel meg.

mező/kiterjesztés	tartalom
version	kötelező; időbélyeg változata (v1)

policy	kötelező; időbélyegzéshez kapcsolódó Időbélyegzési Rend azonosítója (1.3.6.1.4.1.46800.1.3.1.4)
messageImprint	kötelező; időbélyeghez kapcsolódó lenyomatképző algoritmus azonosítója és lenyomat
serialNumber	kötelező; időbélyeg sorszáma
genTime	kötelező; időbélyeg kibocsátásának dátuma és időpontja

9. Megfelelőségi vizsgálat és egyéb felmérések (audit)

A Szolgáltató rendszerét, folyamatait megfelelő időközönként felül kell vizsgálni. A vizsgálatok során független auditorok ellenőrzik a Szolgáltatásokhoz kellő eszközök, infrastruktúra megfelelőségét, Szolgáltató szabályzatait, valamint működését.

A Szolgáltató felülvizsgálatát végző szervezetek függetlenek a Szolgáltatótól, és tevékenységét befolyástól mentesen végzik. A felülvizsgálatot végző szervezetek nem rendelkeznek tulajdonrésszel vagy érdekeltséggel a Szolgáltatóban, és a Szolgáltató nem tulajdonosa közvetlenül vagy közvetve a felülvizsgálatot végző szervezeteknek. A felülvizsgálatot végző szervezetek díjazása nem függ a tanúsítás tett megállapításaitól.

A felülvizsgálat kiterjed a rendszerre és a folyamatokra egyaránt. A rendszernek képesnek kell lennie az alapvető bizalmi szolgáltatói folyamatok végrehajtására. A folyamatoknak meg kell felelnie a szabályzatokban leírtaknak, amelyek a Bizalmi felügyelet számára benyújtásra kerültek.

A rendszer ellenőrzése során végre kell hajtani az alábbi feladatokat:

- a rendszerek indítása
- a rendszerek leállítása
- a tanúsítványok kiadása
- a tanúsítványok és kulcsok kimentése
- az adathordozón tárolt kulcsok használata
- a tanúsítványok exportálása
- a tanúsítványok visszavonása
- a CRL soron kívüli kiadása

A folyamatok ellenőrzése során meg kell vizsgálni az alábbi dokumentumokat:

- Általános Szerződési Feltételek fokozott biztonságú elektronikus aláíráshoz és bélyegzőhöz kapcsolódó bizalmi szolgáltatásokhoz, nem minősített időbélyegzés szolgáltatáshoz és nem minősített weboldal- hitelesítő szolgáltatáshoz

- Szolgáltatási Szabályzat fokozott biztonságú elektronikus aláíráshoz és bélyegzőhöz kapcsolódó bizalmi szolgáltatásokhoz, nem minősített időbélyegzés szolgáltatáshoz és nem minősített weboldal- hitelesítő szolgáltatáshoz
- Bizalmi Szolgáltatási Rend fokozott biztonságú elektronikus aláíráshoz és bélyegzőhöz kapcsolódó bizalmi szolgáltatásokhoz, nem minősített időbélyegzés szolgáltatáshoz és nem minősített weboldal- hitelesítő szolgáltatáshoz
- Időbélyegzési Rend fokozott biztonságú időbélyegzés-szolgáltatásokhoz
- Helyreállítási terv rendkívüli üzemhelyzetek esetén fokozott biztonságú bizalmi szolgáltatásokhoz
- Biztonsági mentési és visszaállítási eljárás bizalmi szolgáltatásokhoz
- Informatikai Biztonsági Szabályzat (IBSz)
- Bizalmi munkakörök
- Hálózati beállítások

A felülvizsgálat eredményéről készített jelentést a független auditorok átadják a Szolgáltató felelős vezetőjének, aki kiértékeli azokat, szükség esetén javító intézkedéseket rendel el.

10. Egyéb üzleti és jogi kérdések

10.1. Díjak

A mindenkor érvényes Szolgáltatások díjait a Szolgáltató saját internetes oldalán (http://www.digitoll.co.hu/, és http://ds.digitoll.co.hu/) és ügyfélszolgálati irodájában nyomtatott formában teszi közzé.

A Szolgáltató az árlistát módosíthatja és a módosítást annak a hatályba lépése előtt 30 nappal a honlapján közzéteszi. Az előre kifizetett Szolgáltatások árát a módosítás nem érinti. Az díjak kifizetésével és visszatérítésével kapcsolatos rendelkezéseket a Szerződés és mellékletei – különösen az ÁSzF – tartalmazzák.

A mindenkori árlistától való eltérés kizárólag csak a Szolgáltatóval kötött külön megállapodással, illetve a Szolgáltató által meghirdetett akciókkal lehetséges.

A Szolgáltató Szolgáltatásait csak a vele szerződéses viszonyban levő felek vehetik igénybe.

1124 Budapest, Stromfeld Aurél út 9.
Tel.: +361 487 9900
E-mail: digitoll@digitoll.co.hu
Web: www.digitoll.co.hu

10.2. Jogok, kötelezettségek

10.2.1. *A Szolgáltató kötelezettségei*

A Szolgáltató (és szervezetei) köteles a saját mindenkori szabályzatainak (ÁSzF, jelen Szabályzat, Bizalmi Rend, Időbélyegzési rend, működési szabályzatok, Szerződés) megfelelően a Szolgáltatásait nyújtani, megfelelve a mindenkor magyar jogrendszernek és törvényeknek.

A Szolgáltató kötelezettséget vállal, hogy minden lehetséges és törvényes eszközzel biztosítja a Szolgáltatások problémamentes működését.

A Szolgáltató köteles az Ügyfélt és/vagy az Alanyt, az igénylés előtt pontosan tájékoztatni, az ügymenetekről, és elérhetővé tenni a nyilvános szabályzatait.

A Szolgáltató mindenkor az Ügyfél által az elektronikus tanúsítvány-igénylésben benyújtott, a Regisztrációs szervezet által jelen Szolgáltatási Szabályzatban és Bizalmi Rendben meghatározott módon ellenőrzött adatok alapján bocsátja ki a tanúsítványt, az adatokon változtatást nem alkalmazhat. Az Ügyfél általi – tanúsítványban foglalt adatok változására vonatkozó – bejelentés automatikusan a tanúsítvány visszavonását vonja maga után. A módosított adatokkal kibocsátott tanúsítvány új tanúsítványnak minősül.

Szolgáltató az E-ügyintézési tv. 82. § (1) bekezdése szerint az általa kibocsátott tanúsítványoknak az abban foglalt adatokat a valóságnak megfelelően kell tartalmaznia, kivéve, ha magából a tanúsítványból kitűnik, hogy az adat valódiságát a bizalmi szolgáltató nem ellenőrizte (így különösen álnév esetén). Ennek érdekében Szolgáltató ezen adatokat köteles ellenőrizni. A tanúsítvány tartalmától függően ellenőrzi az tanúsítvány Alany (aláíró) személyazonosságát, a bemutatott személyazonosságot igazoló okmányok érvényességét és azok adatainak valódiságát és - ha van ilyen - közhiteles vagy más központi nyilvántartásban foglalt adatokkal való megegyezőségét. Szintén ellenőriznie kell a tanúsítvány alany nevében a Szolgáltató előtt eljáró képviselő képviseleti jogosultságát, a tanúsítványba foglalandó képviseleti jog meglétét, a tanúsítvány által igazolt címtartomány (domain) fölötti rendelkezési jogot, a tanúsítványban feltüntetendő IP-cím fölötti rendelkezési jogot, a tanúsítványba foglalandó szervezeti egység létezését, a tanúsítványba foglalandó szabályozott szakma megnevezése esetén az annak gyakorlására való jogosultságot.

A Szolgáltató köteles tájékoztatni az Ügyfélt:

- a Szolgáltatásaira irányadó jogszabályváltozásokról,

- bármely szabályzatainak (ÁSzF, jelen Szabályzat, Bizalmi rend, Időbélyegzési rend, Szerződés) megváltoztatásáról,
- bármely döntésről, ami érinti az Ügyfélt, vagy annak igénybevett Szolgáltatásait.

A Szolgáltató nyilvántartást vezet minden eseményről, változásról, és az előfizetői adatokról.

A Szolgáltató jogait, kötelezettségeit és felelősségeit az ÁSzF ide vonatkozó pontja is részletezi.

10.2.2. *A végfelhasználók jogai és kötelezettségei*

Az Ügyfél jogosult a Szolgáltatások igénybevételéhez, a szabályzatok és a Szerződés szerint, ha azok igénybevételéhez a Szerződés rendelkezéseinek megfelelő Szolgáltatásokkal kapcsolatos díjakat határidőre a Szolgáltatónak megfizette.

Az Ügyfél jogosult a Szerződésben meghatározott tanúsítványok visszavonását, felfüggesztését, visszaállítását kérni.

Az Ügyfél jogosult az Alany(ok) adatait megváltoztatni, és törölni, új Alannyal bővíteni az Alany(ok) listáját. Az Ügyfélhez tartozó Alanyok jogait a jelen Szabályzat tartalmazza.

Az Ügyfél jogosult indoklás nélkül betekinteni a róla nyilvántartott adatokba, Szolgáltató ügyfélszolgálati irodájában, nyitvatartási időben.

Az Ügyfél és/vagy Alany tudomásul veszi, hogy a magán kulcsukkal készített elektronikus aláírás a saját elektronikus aláírásának minősül, és viseli ennek jogkövetkezményeit.

Az Ügyfél és/vagy Alany köteles a Szolgáltatásokat kizárólag a hazai és Uniós jogszabályok által megengedett vagy nem tiltott célokra, a jelen Szabályzatban és a hozzá kapcsolódó egyéb szabályzatokban, Szerződésben foglaltaknak megfelelően használni.

A Szolgáltatás igénybevételéhez az Ügyfél és/vagy Alany kötelessége, hogy megismerje, elfogadja és betartsa a Szolgáltató szabályzatait (ÁSzF, jelen Szabályzat, Bizalmi Rend, Időbélyegzési Rend, Szerződés).

Az Ügyfél köteles a Szerződésben meghatározott díjakat megfizetni a Szolgáltatások igénybevételéhez, a meghatározott határidőn belül. Ha ezt nem teszi, köteles vállalni érte a felelősséget, késedelmi díj fizetésére kötelezhető. Ennek értéke és feltételei a Szerződésben van rögzítve.

Továbbá az E-ügyintézési tv. 85. § (1) alapján Ügyfél és Alany haladéktalanul tájékoztatja Szolgáltatót:

- az azonosításához szükséges, a tanúsítványban feltüntetett személyazonosító adatok, más személy képviseletével összefüggésben kiállított tanúsítvány esetén a képviseletre jogosult személy és a képviselt személy adatai, a tanúsítványban feltüntetett egyéb adatokban bekövetkezett változásokról;
- a szolgáltatással vagy a tanúsítvánnyal kapcsolatban észlelt, a külön jogszabályban, Szerződésben illetve jelen Szabályzatban meghatározott rendellenességről vagy más, a szolgáltatást érintő eseményről, így különösen arról, ha a bizalmi szolgáltatás használatához szükséges eszközök, tanúsítványokat jogosulatlan személy használhatta;
- a szolgáltatással kapcsolatos jogvita megindulásáról.

Az Ügyfél és/vagy Alany kérheti a tanúsítvány visszavonását vagy, a tanúsítvány felfüggesztésének lehetőségét, a tanúsítvány felfüggesztését.

Mivel az elektronikus bélyegző jogi személy aláírása, így a bélyegző használatával járó, vagy esetleges visszaélések miatt okozott károkért az előfizető szervezet (jogi személy) felelős vezetője a felelős.

Az Érintett fél kötelessége és felelőssége kiterjed a tanúsítványok elfogadása során tanúsított körültekintő eljárásért és általában a kötelezettségei betartásáért. Az Érintett fél felelőssége fennáll a tanúsítvány elfogadásából fakadó bármely következményért és kárért, ha a tanúsítvány érvényességének és hatályosságának ellenőrzése során nem az irányadó jogszabályok és a tőle elvárható gondosság szerint járt el.

10.3. Anyagi felelősség - Felelősségek

A Szolgáltató a vele szerződéses jogviszonyban álló felekkel szemben az eIDAS 13. cikke szerint felelős minden olyan kárért, amelyet szándékosan vagy gondatlanul bármely természetes vagy jogi személynek okoz az eIDAS rendelet szerinti kötelezettségei megszegéséből eredően. Ennek biztosítása érdekében Szolgáltató felelősségbiztosítással rendelkezik. Amennyiben a Szolgáltató előzetesen megfelelően tájékoztatja az ügyfeleit az általa nyújtott szolgáltatások igénybevételére vonatkozó korlátozásokról, és amennyiben ezek a korlátozások harmadik felek számára felismerhetők, a Szolgáltató nem felelős a szolgáltatások igénybevételéből eredő, a jelzett korlátozásokat meghaladó károkért.

A Szolgáltató kizárja felelősségét, ha az Ügyfél és/vagy Alanyok nem a nyilvános szabályzatokban, Szerződésben meghatározott módon, vagy jogellenesen járnak el.

10.3.1. *A Szolgáltató általános felelőssége és felelősségének korlátai*

A Szolgáltató felelősséget vállal a szabályzataiban leírt eljárásoknak való megfelelőségért.

Szolgáltató az eIDAS 13. cikke szerint felelős minden olyan kárért, amelyet szándékosan vagy gondatlanul bármely természetes vagy jogi személynek okoz eIDAS rendelet szerinti kötelezettségei megszegéséből eredően.

A Szolgáltató szándékosságát vagy gondatlanságát annak a természetes vagy jogi személynek kell bizonyítania, aki/amely állítása szerint az említett kár megtérítését követeli. Amennyiben Szolgáltató előzetesen megfelelően tájékoztatja az ügyfeleket az általa nyújtott szolgáltatások igénybevételére vonatkozó korlátozásokról, és amennyiben ezek a korlátozások harmadik felek (Érintett fél) számára felismerhetők, Szolgáltató nem felelős a szolgáltatások igénybevételéből eredő, a jelzett korlátozásokat meghaladó károkért.

A Szolgáltató a vele szerződéses jogviszonyban álló felekkel (Ügyfél, Alany) szemben a Ptk. szerződésszegésért való felelősség szabályai szerint felelős és a vele szerződéses jogviszonyban nem álló harmadik féllel (Érintett fél) szemben a Ptk. szerződésen kívüli károkozásról szóló szabályai (Ptk. 519 §) szerint felelős.

A Szolgáltató a felelősségi körén belül keletkezett, bizonyított károkért a szabályzataiban és az Ügyféllel és/vagy Alannyal megkötött Szerződésekben rögzített korlátozásokkal kártérítést fizet.

A Szolgáltató felelős a kötelezettségei megszegéséért.

Szolgáltató nem felelős az olyan károkért, amelyek abból adódtak, hogy az Ügyfél, Alany vagy az Érintett Fél a tanúsítványok felhasználása és ellenőrzése során nem a hatályos hazai valamint Uniós jogszabályoknak, illetve a Szolgáltató szabályzatainak megfelelően járt el, illetve nem tanúsította a tőle elvárható gondosságot.

A Szolgáltató nem felelős az abból adódó károkért, amikor valamely külső, elháríthatatlan esemény miatt a tájékoztatás és egyéb kommunikációs kötelezettségeit nem tudja ellátni.

A regisztrációs eljárás részeként a Szolgáltató közhiteles adatbázissal végez adategyeztetést, a tanúsítványok kibocsátását megelőzően. A Szolgáltató nem vállal felelősséget e közhiteles adatbázis által szolgáltatott információk pontatlanságából eredő károkért.

Miután az aláírás-létrehozó adat az Ügyfél és/vagy Alany(ok) birtokába kerül, a Szolgáltató nem vállal semmilyen felelősséget:

- az aláírás-létrehozó eszköz (továbbiakban: ALE), és annak használatához szükséges titkos kódok, jelszavak és maga az aláírás-létrehozó adat védelméért,
- az ALE és az aláírás-létrehozó adat segítségével létrehozott aláírásokért. Kivéve, ha az Ügyfél jelzi - a Szolgáltatási szabályzat szerinti módon - az aláírás-létrehozó adat kompromittálódását, vagy kéri a tanúsítvány felfüggesztését, vagy visszavonását. A Szolgáltató akkor felelős, ha a Szabályzatban meghatározott időintervallumon belül nem hagyja jóvá, vagy viszi véghez a visszavonási, vagy felfüggesztési folyamatot.

A Szolgáltató felelőssége az E-ügyintézési tv., az eIDAS és a kapcsolódó jogszabályok szerint kiadott tanúsítvány hitelességéig terjed, adott pénzügyi és idő intervallumban. Ha az elektronikusan aláírt adaton vagy dokumentumon hitelesített elektronikus aláírás szerepel és az aláírás ellenőrzésének eredményéből más nem következik, vélelmezni kell, hogy a dokumentum tartalma az aláírás óta nem változott.

A Szolgáltatót semmilyen felelősség nem terheli, Szerződésben feltüntetett alkalmazhatósági korlátok be nem tartatása miatt bekövetkezett káreseménnyel kapcsolatban, valamint az Alanyok magánkulcsaival, illetve aláíró eszközeivel kapcsolatos tevékenységeiért, és az Érintett felek tanúsítvány ellenőrzési és felhasználási tevékenységeiért.

A Szolgáltató kötelezettségeit és felelősségeit az ÁSzF ide vonatkozó pontja is részletezi.

10.3.2. *A Szolgáltató pénzügyi felelőssége*

A Szolgáltató a magyar és Uniós jogszabályozás és törvények szerint, az Ügyféllel és/vagy Alannyal szemben a szerződésszegésért való felelősség szabályai szerint felelős az elektronikus aláírással vagy időbélyegzővel, illetve az ezzel ellátott elektronikus dokumentummal okozott kárért, ha megszegte kötelességeit.

A Szolgáltató a kártérítés felső határát az E-ügyintézési tv. 81.§ (6) bekezdése szerint tanúsítványonként és káreseményenként külön és összességében is korlátozhatja. Az egy alkalommal vállalható legmagasabb kötelezettség értéke a Szolgáltató által kibocsátott tanúsítványoknál a tanúsítványban feltüntetett összeg. Ezen korlátokat meghaladó

ügyletekben kibocsátott és aláírt elektronikus dokumentumokból származó követelésekért, illetve az így okozott kárért a Szolgáltató nem felel.

A Szolgáltató pénzügyi felelősségével kapcsolatos további részleteket az ÁSzF ide vonatkozó pontja tartalmazza.

10.3.3. *Felelősségbiztosítás*

A Szolgáltató a megbízhatósága biztosítása érdekében felelősségbiztosítással rendelkezik. Ezen felelősség biztosítás a 24/2016 BM rendelet 5.§ szerint kiterjed a Szolgáltató által a szolgáltatások nyújtásával összefüggésben okozott valamennyi alábbi kárra és költségre:

- a bizalmi szolgáltatási ügyfélnek (Ügyfél/Alany) a Szerződés megszegésével összefüggésben okozott károkra;
- a bizalmi szolgáltatási ügyfélnek (Ügyfél/Alany) és harmadik személynek szerződésen kívüli okozott károkra;
- a E-ügyintézési tv. 88. §-ban foglalt kötelezettségek nem teljesítése miatt a bizalmi felügyeletnél felmerült, az E-ügyintézési tv. 89. § szerinti költségekre;
- a bizalmi felügyelet által felkért megfelelőségértékelő szervek eljárásának költségei, ha azt a bizalmi felügyelet eljárási költségként érvényesíti.

Szolgáltató biztosítja, hogy az itt taglalt eseteket nevesíti a biztosítási szerződésben. A biztosítási szerződésben szereplő felelősségvállalási érték káreseményenként nem lehet alacsonyabb, mint 3000 000 forint.

Több azonos okból bekövetkezett, időben összefüggő káresemény egy biztosítási eseménynek minősül. A vonatkozó jogszabály szerint, ha a 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.

10.3.4. *A Végfelhasználók felelőssége*

Az Ügyfél és Alany felelős a Szolgáltató szabályzatai és a Szerződés betartásáért.

Az Ügyfél és Alany felelős a kezdeti regisztráció keretében megadott adatai valódiságáért, pontosságáért és érvényességéért.

Az Ügyfél és/vagy Alany felelős az adataiban bekövetkezett változások bejelentéséért.

Az Ügyfél felelősséget vállal a Szerződésben megnevezett Alany(ok), adatainak valóságáért és azok megváltozását követi és tájékoztatja erről a Szolgáltatót is.

A magánkulcs védelme és az aláírás készítése kizárólag az Ügyfél és/vagy Alany felelőssége, így annak kompromittálódása, vagy jogszerűtlen használata esetén a Szolgáltatót semmilyen felelősség nem terheli.

Az Ügyfél felelős a Szerződésben rögzített szolgáltatások díjainak kifizetéséért, azaz a számlákon szereplő összegek megjelölt időpontig történő kifizetéséért. Az ettől való eltérés csak írásos megállapodás keretében történhet.

Az Érintett fél kötelessége és felelőssége kiterjed a tanúsítványok elfogadása során tanúsított körültekintő eljárásért és általában a kötelezettségei betartásáért. Az Érintett fél felelőssége fennáll a tanúsítvány elfogadásából fakadó bármely következményért és kárért, ha a tanúsítvány érvényességének és hatályosságának ellenőrzése során nem az irányadó jogszabályok és a tőle elvárható gondosság szerint járt el.

Az Ügyfél és/vagy Alany felelősséget vállal kötelezettségei betartásáért.

Az Ügyfél kötelezettségeit és felelősségeit az ÁSzF ide vonatkozó pontja is részletezi.

10.3.5. *Szolgáltatóval szembeni kártérítés*

Az Ügyfél és/vagy Alany kártérítési felelősséggel tartoznak a Szolgáltatónak azokért a veszteségekért és károkért, amelyeket kötelezettségeik, felelősségeik és a rájuk vonatkozó ajánlások be nem tartásával okoznak számára.

A Szolgáltató a vagyoni felelősségre vonhatóság, a Szolgáltató által okozott károkkal kapcsolatos saját felelősség, illetve a Szolgáltatónak okozott károkért járó kártérítés megállapíthatósága, dokumentálása és bizonyíthatósága érdekében naplózza tevékenységeit, védi a napló állományok sértetlenségét és hitelességét, valamint hosszú távon is megőrzi (archiválja) a naplóadatokat.

1124 Budapest, Stromfeld Aurél út 9.
Tel.: +361 487 9900
E-mail: digitoll@digitoll.co.hu
Web: www.digitoll.co.hu

10.4. Üzleti információ titkossága

A Szolgáltató kötelezettséget vállal arra, hogy a Szolgáltatásai során tudomására jutott üzleti titkokat a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról szóló 1996. évi LVII. törvényben foglaltak szerint megőrzi.

10.5. Adatkezelés, bizalmasság

A Szolgáltató az Ügyfél és Alany adatait a jogszabályoknak megfelelően kezeli. Az Ügyfél és Alany a tanúsítvány igénylésével járul hozzá ahhoz, hogy a személyes adatait a Szolgáltató Adatvédelmi nyilatkozatának megfelelő módon tárolja és kezelje. A Szolgáltató által kibocsátott tanúsítványok és a bennük található személyes adatok nyilvánosságra hozatala csak az Ügyfél és/vagy Alany előzetes írásos hozzájárulásával történhet meg. A hozzájárulásukat a regisztrációs folyamat részeként tehetik meg. A Szolgáltató az Ügyfél és Alany személyes adatait kizárólag csak a szolgáltatásaival összefüggésben használja fel.

A Szolgáltató Adatvédelmi nyilatkozata elérhető az alábbi címen:
http://ds.digitoll.co.hu/dok.php?m=5

10.5.1. *Adatkezelési szabályok, titoktartási kötelezettség*

Az ÁSzF ide vonatkozó pontja és a Szolgáltató Adatvédelmi nyilatkozata és szabályzata szerint.

10.5.2. *Adatok nyilvánosságra hozatala*

A tanúsítványba megjelenő adatok nyilvánosságra hozatala és közzététele, jelen Szabályzat ide vonatkozó pontjában van részletezve.

10.5.3. *Bizalmas jellegű információk*

A Szolgáltató bizalmas információnak tekinti azokat az előfizetői és aláírói adatokat melyek az általa kibocsátott tanúsítványban nem szerepelnek.
A Szolgáltató bizalmasnak nyilvánítja a saját nem nyilvános dokumentumait, vizsgálati és tesztadatait.

10.5.4. *Nem bizalmas jellegű információk*

A Szolgáltató nem bizalmas információnak tekinti azokat az előfizetői és aláírói adatokat, melyek az Ügyfél és Alany engedélye alapján nyilvánosként kezelhet.

A Szolgáltató nem bizalmas információnak tekinti a jogszabályok által meghatározott szabályzatokat (jelen Szabályzat, Bizalmi Rend, Időbélyegzési rend), illetve az általa meghatározott egyéb szabályzatokat, nyilatkozatokat, felhasználói segédleteket és a visszavonási listákat (CRL).

A Szolgáltató nem bizalmas jellegű információként kezeli a tanúsítványtárban elhelyezett azon tanúsítványokat, amelyek nyilvánosságra hozatalát az Ügyfél engedélyezte.

A Szolgáltató az általa kibocsátott tanúsítványok visszavonását és felfüggesztését a tanúsítvány visszavonási listában teszi közzé, a tanúsítvány adatainak jelölésével.

10.6. Személyi adatok bizalmas kezelése

A Szolgáltató kötelezettséget vállal arra, hogy a bizalmi szolgáltatás során tudomására jutott személyes adatokat a jogszabályban foglaltak szerint megőrzi.

A Szolgáltató a Szerződés keretében a Szolgáltatások nyújtása, illetve igénybevétele során tudomására jutott adatokat, információkat – jogszabályi kötelezettséget, hatósági, kormányzati, illetve bírósági kötelezést nem számítva – harmadik személynek kizárólag az érintett személyek írásbeli beleegyezésével adhatják át.

Szolgáltató az E-ügyintézési tv. 90. § szerint (az általa nyújtott bizalmi szolgáltatások felhasználásával elkövetett bűncselekmények felderítése vagy megelőzése céljából, vagy nemzetbiztonsági érdekből az adatigénylésre külön törvényben meghatározott feltételek teljesülése esetén díjmentesen adatokat továbbít a nyomozó hatóságnak és a nemzetbiztonsági szolgálatoknak. Az adatátadás tényét rögzíteni kell, az adatátadásról a bizalmi szolgáltató az igénybe vevőt nem tájékoztathatja. Ha a tanúsítványban az igénybe vevő álnéven szerepel, a Szolgáltató a tanúsítványban szereplő igénybe vevő valódi személyazonosságára vonatkozó adatot is köteles átadni. Ezen kötelezettségeknek haladéktalanul köteles eleget tenni, és az adatok továbbítását nem kötheti egyéb feltételekhez, így különösen az adatszolgáltatás költségeiben való megállapodáshoz vagy a költségek előlegezéséhez.

Szolgáltató az E-ügyintézési tv. 93. § (5) és (6) szerint Bizalmi Felügyelet részére adatokat szolgáltat. Szolgáltató az adatszolgáltatás során biztosítja az adatok bizalmasságát és sértetlenségét.

Szolgáltató a tanúsítvány érvényességét érintő polgári peres, illetve nem peres eljárás során - az érintettség igazolása esetén - az aláíró vagy bélyegzőt elhelyező személyazonosságát igazoló, valamint egyéb, egyeztetett adatokat átadhatja az ellenérdekű félnek vagy képviselőjének, illetve azt közölheti a megkereső bírósággal. Ha a tanúsítványban az igénybe vevő álnéven szerepel, a Szolgáltató a tanúsítványban szereplő igénybe vevő valódi személyazonosságára vonatkozó adatot is köteles átadni.

10.7. Szellemi tulajdonjogok

A Szolgáltató szabályzatai, szerződéses feltételei, dokumentumai, CRL listái a Szolgáltató tulajdonát képezik.

A Szolgáltató által kibocsátott tanúsítványok és az azoknak megfelelő kulcspárok tulajdonosai az Ügyfelek, teljes jogú felhasználója pedig az Alanyok, tekintet nélkül arra a fizikai közegre, amelyek tárolják és védik a kulcsokat. A Szolgáltató a szabályzatokban egyezetett módon kezelheti a tanúsítványokat.

10.8. Garanciák jogi nyilatkozatai

A Szolgáltató kötelezettséget vállal, hogy minden lehetséges és törvényes eszközzel biztosítja a Szolgáltatás problémamentes működését, betartva a saját biztonsági és működési szabályzatait.

A Szolgáltató a vele szerződéses jogviszonyban álló felekkel szemben az általa okozott jelen Szabályzat 10.3.3 pontjában taglalt károkért vállal felelősséget

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 a rendelkezésre áll.

A Szolgáltató kizárja felelősségét, ha az Ügyfelek vagy Alanyok nem a Szerződésben vagy ahhoz tartozó egyéb szabályzatokban meghatározott módon, vagy jogellenesen járnak el.

A Szolgáltató a felelősségi körén belül keletkezett, bizonyított károkért fizetendő kártérítést (a hatályos jogszabályokkal összhangban) korlátozhatja a vele szerződéses jogviszonyban álló ügyfelekkel szemben. A korlátozás mértéke az Ügyfél által választott díjcsomagtól függően eltérő lehet, a korlátozás pontos összegét a Szerződés tartalmazhatja. A kártérítés korlátozása kiterjedhet vagyoni és nem vagyoni kárra, az elmaradt haszonra, költségekre (a veszteségek és károk minden típusára), amely a Szolgáltató hibájából ered. A Szolgáltató kárfelelősségének esetleges korlátozása a Szolgáltatások díjából biztosított kedvezményekre tekintettel, a biztosított kedvezményekhez mérten, azzal arányos módon kerülhet megállapításra. Az élet és testi épségben okozott károkra a felelősség nem terjed ki.

A Szolgáltató kizárja felelősségét, ha az aláírás ellenőrzés lépései a szabályzatokban meghatározott módon bármi okból – beleértve a Szolgáltatónál keletkező előre bejelentett üzemeltetési és menedzselési problémát is – nem hajthatóak végre az aláírás ellenőrzésének időpontjában, és az elektronikus aláírás, illetve az aláírással ellátott dokumentum az aláírás érintett fele által ennek ellenére elfogadásra kerül.

A Szolgáltatót semmilyen felelősség nem terheli, a szerződésben és nyilvános szabályzataiban feltüntetett alkalmazhatósági korlátok be nem tartatása miatt bekövetkezett káresemény miatt.

A Szolgáltató a Szolgáltatás egy részét képező eszközök működéséért és minőségéért nem vállalja a felelősséget, azok garanciája az adott gyártótól függ.

10.9. A felelősség korlátai

Az anyagi felelősség mértéke az adott tanúsítvány típusától függ. Ezt az értéket a Szerződés tartalmazza.

10.10. Érvényesség, módosítás

10.10.1. *A Szabályzat érvényessége*

Jelen Szabályzat visszavonásig, vagy újabb verzió hatályba lépéséig érvényes.

10.10.2. *Érvénytelenség, fennmaradás*

Amennyiben jelen Szabályzat valamely pontja érvénytelen lenne, az a Szabályzat egészének és más pontjainak érvényességét nem érinti.

A Szabályzat 10. fejezete érvényben marad a Szabályzat hatályának megszűnését követően is (a hatályosság megszűnésének módjától függetlenül) mindazon tanúsítványokkal kapcsolatosan, melyet a Szolgáltató a Szabályzat hatálya alatt bocsátott ki.

10.10.3. *A Szabályzat értelmezése*

A Szabályzat a PKI közösség kötelezettségét, felelősségét és jogát tartalmazza. Kivétel ez alól az Érintett Fél, kinek részére kötelezettséget nem, csak ajánlást és felelősséget fogalmaz meg.

A Szabályzat egyetlen pontja sem értelmezhető a jelen dokumentumban foglalt értelmezéstől eltérően, bármely más szerződés vagy szabályzat, írott vagy szóbeli kommunikáció következtében.

Jelen Szabályzat magyarul íródott, és a magyar nyelv szabályai szerint kell értelmezni.

10.11. Egyedi értesítések és kommunikáció a résztvevőkkel - Felek közötti kommunikáció, panaszkezelés

A Szolgáltató az Alanyok illetve az Ügyfelek részére ügyfélszolgálati tevékenységet nyújt.
Az ügyfélszolgálat elérhetőségét a szolgáltató jelen Szabályzat 1.1. pontjában és internetes oldalán közzéteszi: http://ds.digitoll.co.hu/.

Az ügyfélszolgálati iroda minden munkanap 8:30-15:30 óra között érhető el. A Szolgáltató Visszavonási ügyeletet üzemeltet minden nap 0-24 órában a jelen Szabályzat 1.1. pontjában megadott telefonszámon.

Az Ügyfél a reklamáció illetve a hiba bejelentését írásban teheti meg, a Szolgáltató ügyfélszolgálatánál személyesen átadva, postai úton, vagy elektronikus formában elektronikusan aláírva.

A Szolgáltató minden tevékenységével kapcsolatos panaszt, reklamációt és hibabejelentést nyilvántartásba vesz. A nyilvántartásba vett panaszokat a jogi szabályozásnak megfelelően 30 napon belül kivizsgálja és annak eredményéről a bejelentőt tájékoztatja.

A számlareklamációkkal kapcsolatos feltételeket az ÁSzF tartalmazza.

10.12. Módosítások

10.12.1. *A Szabályzat módosítása*

Jelen Szabályzatot a Szolgáltató egyoldalúan módosíthatja. A módosításról a Szabályzat hatályba lépése előtt 30 nappal tájékozatja az Ügyfeleit. Kivétel ez alól azon módosítások, melyek a szolgáltatások biztonsági szintjét, felhasználhatóságát nem módosítják (ilyenek tipikusan a helyesírási hibák, formai változtatások, különböző kapcsolatadatok) együttesen kerülnek módosításra és értesítésre. Azok az Ügyfelek, akik a módosítást nem fogadják el, jogosultak a hatálybalépést követően 15 napon belül, 15 napos felmondási idővel az Szerződést felmondani. A Szerződés felmondása egyben a kiadott tanúsítvány iránti visszavonási kérelemnek is tekintendő, és a Szolgáltató jogosult a tanúsítványt nyilvántartásából törölni. Ebben az esetben a Szolgáltató az Ügyfél által már befizetett díjakat nem köteles visszatéríteni. Az Ügyfél vállalja a visszavonással kapcsolatban felmerülő költségeket.

Minden szabályzat egyedi azonosítóval rendelkezik (OID, verziószám).

A Bizalmi felügyelet megvizsgálja a módosított Szabályzat jogszabályi megfelelősségét majd nyilvántartásba veszi. A Szabályzat csak írott és hitelesített formában módosítható, a Bizalmi felügyelet által vezetett szabályzat-nyilvántartásban való átvezetés mellett.

Az új verziószámmal ellátott Szabályzat hatálybalépésével egyidejűleg, az azt megelőző Szabályzat hatálya visszavonásra kerül, érvényét veszti.

10.13. Rendelkezések a viták rendezéséről

A Szolgáltató és előfizetői (Felek) kölcsönösen megállapodnak abban, hogy a Szerződésből eredő jogvitáikat mindenkor megkísérlik békés úton – peren kívül – tárgyalások útján rendezni.

Felek jogosultak viták rendezése céljából békéltető testülethez fordulni.
Ennek elérhetőségei:

Név:	Budapesti Békéltető Testület
Cím:	1016 Budapest, Krisztina krt. 99. III. em. 310.
Postai cím:	1253 Budapest, Pf.: 10.
Telefonszám:	06 (1) 488 21 31
Email cím:	bekelteto.testulet@bkik.hu
Internet cím:	http://bekeltet.hu/

Amennyiben a Felek közötti egyeztetés valamelyik fél által kezdeményezetett egyeztetés napjától számított 30 napon belül nem vezet eredményre, arra az esetre a Felek értékhatártól függően kölcsönösen alávetik magukat a Fővárosi Bíróság / PKKB kizárólagos illetékességének.

A Szerződésben nem szabályozott kérdésekben a mindenkor hatályos magyar jogszabályok rendelkezései irányadók, különös tekintettel a Polgári Törvénykönyv, E-ügyintézési tv., illetve az adatvédelmi jogszabályok rendelkezései.

A Szolgáltató tevékenységével kapcsolatos kifogásokat és panaszokat Szolgáltató elérhetőségein lehet megtenni.

A Szolgáltatásokkal kapcsolatos bármely vitás kérdés vagy panasz felmerülése esetén a vita jogi útra terelése előtt az Ügyfélnek és/vagy Alanynak kötelessége a Szolgáltató haladéktalan értesítése és teljes körű tájékoztatása az ügy minden vonatkozását érintően.

10.14. Jogi szabályozás

A Szolgáltató tevékenységét a mindenkor hatályos magyar és egyes Uniós jogszabályoknak megfelelően végzi. A Szolgáltató szerződéseire és szabályzataira, azok teljesítésére a magyar jog az irányadó, s azok a magyar jog szerint értelmezendők. A legfontosabb jogszabályok felsorolását az ÁSZF ide vonatkozó pontja tartalmazza.

A legfontosabb jogszabályok:

- 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól
- 24/2016. (VI. 30.) BM rendelet A bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről
- 25/2016. (VI. 30.) BM rendelet A bizalmi felügyeletnek fizetendő igazgatási szolgáltatási díjak mértékéről
- 26/2016. (VI. 30.) BM rendelet A bizalmi felügyelet által vezetett nyilvántartások tartalmáról és a bizalmi szolgáltatás nyújtásával kapcsolatos bejelentésekről
- 2013. évi V. törvény a Polgári Törvénykönyvről
- 1996. évi LVII. törvény a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

- AZ EURÓPAI PARLAMENT ÉS A TANÁCS 910/2014/EU RENDELETE a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről

10.15. Megfelelés az alkalmazandó törvényeknek

A Szolgáltató köteles a saját mindenkori szabályzatainak (ÁSzF, Szolgáltatási szabályzat, Bizalmi Rend, Időbélyegzési Rend, működési szabályzatok, Szolgáltatási szerződés) megfelelően a Szolgáltatásait nyújtani, megfelelve a mindenkori magyar és Uniós törvényeknek és a magyar jogrendszernek.

A Szolgáltató kötelezettséget vállal, hogy minden lehetséges és törvényes eszközzel biztosítja a Szolgáltatás problémamentes működését.

10.16. Vis major

A Szolgáltató és előfizetői (Felek) Szolgáltatásokra kötendő szerződéseire vonatkozóan a "vis major" a Felek érdekkörén kívül álló olyan nem látható eseményt jelenti, amely a Szerződés megkötése után következik be, annak ésszerű teljesítését akadályozza, a Felek ellenőrzésén kívülálló, általuk elháríthatatlan és nem látható előre. Ebben az esetben a Felek mentesülnek szerződésszegésük jogkövetkezményei alól, ha a szerződésszegés "vis major" miatt következett be. "Vis major" esetében Felek legkésőbb 5 napon belül írásban értesítik egymást az ilyen késedelem okairól.

10.17. Felek közötti kommunikáció

10.17.1. *Általános kommunikáció*

A Szolgáltató a Szolgáltatásairól tájékoztatás nyújthat telefonon, írásban illetve az internetes oldalán.

A Szolgáltató az Ügyfeleket és/vagy Alanyokat írásban tájékoztatja az esetleges módosításokról, változásokról és egyéb információkról. Ezt megteheti írásban (elektronikusan vagy postai úton) illetve közzététellel.

Az Ügyfél Szolgáltatóval való kommunikációja történhet írásban aláírva (elektronikusan vagy postai úton) vagy személyesen, kivétel ez alól a tanúsítvány felfüggesztésének kérelme, ami történhet telefonon is.