



**Bizalmi Szolgáltatási Rend  
a Digitális Állampolgárság Program keretében kibocsátott  
minősített tanúsítványokhoz  
(BR-DÁP-TAN)**

**Verziószám:** v.1.7  
**OID:** 0.2.216.1.200.1100.100.42.3.1.36  
**Hatályba lépés dátuma:** 2025.05.28.  
**Dokumentum besorolása:** NYILVÁNOS

Jóváhagyó	Adorján István

## Változáskövetés

verzió	dátum	a változás leírása	készítette	ellenőrizte	jóváhagyta
0.1	2024.07.29	első változat	NISZ Zrt. Polysys Kft. ACPM Zrt.		
0.2	2024.07.30	visszajelzéseket beépítő, hatóságnak benyújtott változat	ACPM Zrt.	Kővári-Szabó Zoltán	-
0.3	2024.11.06	Továbbfejlesztett változat	Kővári-Szabó Zoltán	Nagy Benjámin ACPM Zrt.	-
1.0	2024.11.29	Első jóváhagyott verzió	Kővári-Szabó Zoltán	Nagy Benjámin ACPM Zrt.	Adorján István
1.1	2024.12.11	A megfelelőségértékelési eljáráson tett észrevételek alkalmazása.	Kővári-Szabó Zoltán	Nagy Benjámin	Adorján István
1.2	2024.12.17	Hatálybalépés dátumának módosítása.	Kővári-Szabó Zoltán	Nagy Benjámin	Adorján István
1.3	2025.01.28	<ul style="list-style-type: none"> <li>A visszavonáskezelésre vonatkozó rendelkezésreállási követelménnyel történő kiegészítés.</li> <li>A 2024. évi LXIX. törvény 116. § által hatályon kívül helyezett, az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényre (Ibtv.) hivatkozó szövegrészek törlése.</li> <li>Elütések javítása.</li> </ul>	Kővári-Szabó Zoltán	Nagy Benjámin	Adorján István
1.4	2025.02.03	A Bizalmi felügyelet észrevételei alapján tovább pontosítások	Nagy Benjámin Gál Ferenc	Kővári-Szabó Zoltán	Adorján István
1.5	2025.03.14	OCSP szolgáltatásra vonatkozó pontosítás.	Kővári-Szabó Zoltán	Nagy Benjámin	Adorján István
1.6	2025.07.11	Általános felülvizsgálat	Polysys Kft.	Buczynszkiné dr. Szabó Zsuzsanna Nagy Benjámin Kővári-Szabó Zoltán	Adorján István
1.7	2026.04.28.	<ul style="list-style-type: none"> <li>kiberbiztonsági felügyelet változása;</li> <li>akadálymentes sablon használata</li> </ul>	Buczynskine dr. Szabó Zsuzsanna	Kővári-Szabó Zoltán Gál Ferenc	Adorján István

## Tartalom

1.	BEVEZETÉS.....	6
1.1.	Áttekintés.....	6
1.2.	Dokumentum neve és azonosítása.....	7
1.3.	PKI közösség.....	7
1.4.	A tanúsítvány alkalmazhatósága.....	9
1.5.	Szabályzat adminisztráció.....	10
1.6.	Fogalmak, rövidítések és hivatkozások.....	12
2.	KÖZZÉTÉTEL ÉS ADATTÁRAK.....	21
2.1.	Tanúsítványtár.....	21
2.2.	Szolgáltatói információ közzététele.....	21
2.3.	A közzététel gyakorisága.....	21
2.4.	Hozzáférés-ellenőrzések.....	22
3.	AZONOSÍTÁS ÉS HITELESÍTÉS.....	22
3.1.	Elnevezések.....	22
3.2.	Kezdeti azonosítás.....	23
3.3.	Azonosítás és hitelesítés kulcscsere esetén.....	24
3.4.	Azonosítás és hitelesítés visszavonási kérelem esetén.....	24
4.	A TANÚSÍTVÁNYOK ÉLETCIKLUSA.....	24
4.1.	Tanúsítványigénylés.....	24
4.2.	Tanúsítványigénylés feldolgozása.....	25
4.3.	Tanúsítvány kibocsátás.....	25
4.4.	Tanúsítványelfogadás.....	25
4.5.	A kulcspár és a tanúsítvány használata.....	26
4.6.	Tanúsítványok megújítása.....	26
4.7.	Kulcscsere.....	27
4.8.	Tanúsítványmódosítás.....	27
4.9.	Tanúsítvány visszavonás és felfüggesztés.....	28
4.10.	Visszavonási állapot szolgáltatások.....	30
4.11.	Az előfizetés vége.....	31
4.12.	Kulcsletét és visszaállítás.....	32
5.	FIZIKAI, ELJÁRÁSBELI ÉS SZEMÉLYZETI BIZTONSÁGI ÓVINTÉZKEDÉSEK.....	32
5.1.	Fizikai óvintézkedések.....	32
5.2.	Eljárásbeli előírások.....	34
5.3.	Személyzetre vonatkozó előírások.....	35
5.4.	A biztonsági naplózás folyamatai.....	36

5.5.	Adatok archiválása .....	37
5.6.	Kulcsátállítás .....	38
5.7.	Helyreállítás rendkívüli üzemeltetési helyzetek esetén .....	38
5.8.	A szolgáltatási tevékenység megszüntetése .....	39
6.	MŰSZAKI BIZTONSÁGI ÓVINTÉZKEDÉSEK .....	40
6.1.	Kulcspár előállítás és telepítés .....	40
6.2.	Magánkulcs védelme és kriptográfiai modul műszaki szabályozások .....	41
6.3.	Kulcspár gondozás egyéb szempontjai .....	43
6.4.	Aktivizáló adatok .....	43
6.5.	Informatikai biztonsági óvintézkedések .....	43
6.6.	Életciklusra vonatkozó műszaki óvintézkedések .....	44
6.7.	Hálózatbiztonsági óvintézkedések .....	44
6.8.	Időforrások .....	44
7.	TANÚSÍTVÁNY, CRL ÉS OCSP PROFILOK .....	44
7.1.	Tanúsítvány profil .....	44
7.2.	CRL profil .....	45
7.3.	OCSP profil .....	46
8.	MEGFELELŐSÉGVIZSGÁLAT ÉS EGYÉB ÉRTÉKELÉSEK .....	46
8.1.	Vizsgálatok gyakorisága és körülményei .....	46
8.2.	Auditor azonosítása és képesítése .....	46
8.3.	Auditor függetlensége .....	47
8.4.	Audit során vizsgált területek .....	47
8.5.	Hiányosságok esetén végrehajtandó tevékenységek .....	48
8.6.	Eredmény kommunikációja .....	48
9.	EGYÉB ÜZLETI ÉS JOGI KÉRDÉSEK .....	48
9.1.	Díjak .....	48
9.2.	Anyagi felelősség .....	48
9.3.	Üzleti információk bizalmassága .....	49
9.4.	Személyes adatok védelme .....	49
9.5.	Szellemi tulajdonjogok .....	50
9.6.	Tevékenységért viselt felelősség és helytállás .....	50
9.7.	Helytállás érvénytelenségi köre .....	51
9.8.	Felelősség korlátozása .....	51
9.9.	Kártérítések .....	51
9.10.	Hatályosság és megszűnés .....	51
9.11.	Egyéni hirdetések és kommunikáció a résztvevőkkel .....	52
9.12.	Módosítások .....	52

9.13.	Vitás kérdések rendezése.....	52
9.14.	Irányadó jog .....	52
9.15.	Hatályos jognak megfelelés .....	52
9.16.	Vegyes rendelkezések .....	52
9.17.	Egyéb rendelkezések .....	53

## 1. BEVEZETÉS

- 1) Jelen dokumentum a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. (továbbiakban, mint Kormányzati Hitelesítés Szolgáltató vagy Szolgáltató) Bizalmi Szolgáltatási Rendje, amely a Digitális Állampolgárság Program keretében megvalósított elektronikus aláírás funkcióhoz szükséges minősített tanúsítványszolgáltatás nyújtására és igénybevételére vonatkozik.
- 2) A Szolgáltató a fenti tárgykörben a {J1} eIDAS 3. cikk 16.pont a) alpontjának megfelelő, alábbi bizalmi szolgáltatást nyújtja:
- 3) a Digitális Állampolgárság Program (DÁP) keretében az állampolgárok, mint természetes személyek számára a {J2} DÁP tv. 52. § (1) bekezdés b) pontja szerinti eAláíráshoz kapcsolódó, elektronikus aláírás célú EU minősített tanúsítvány kibocsátása,
- 4) Jelen bizalmi szolgáltatási rend a kibocsátott tanúsítványok kezelésére (előállítás, kibocsátás, közzététel, megújítás, felfüggesztés, újra-érvényesítés, visszavonás, továbbiakban együttesen: Szolgáltatások) vonatkozó követelményeket és a Szolgáltatások működtetésének követelményeit tartalmazza.
- 5) A DÁP eAláírás digitális keretszolgáltatásban történő elektronikus aláírás létrehozás és távoli elektronikus aláírást létrehozó eszköz kezelés nem része a Szolgáltatásoknak, azokra a {D10} „Bizalmi Szolgáltatási Rend a Digitális Állampolgárság Program keretében nyújtott elektronikus aláírások létrehozása és távoli elektronikus aláírást létrehozó eszköz kezelése minősített bizalmi szolgáltatáshoz” (BR-DÁP-TK) és {D11} „Bizalmi Szolgáltatási Szabályzat a Digitális Állampolgárság Program keretében nyújtott elektronikus aláírások létrehozása és távoli elektronikus aláírás létrehozó eszköz kezelése minősített bizalmi szolgáltatáshoz” (BSZ-DÁP-TK) vonatkozik.
- 6) A Szolgáltató a Szolgáltatásokat a vele szerződéses viszonyban álló állampolgárok (továbbiakban Aláírók) részére nyújtja, de egyes szolgáltatási elemeket hozzáférhetővé tesz az elektronikus aláírások hitelességét ellenőrző Érintett Felek részére is.

### 1.1. Áttekintés

- 7) Jelen bizalmi szolgáltatási rend egy olyan szabálygyűjtemény, amely egy tanúsítvány felhasználhatóságát határozza meg egy közös biztonsági követelményekkel rendelkező közösség és/vagy alkalmazások egy osztálya számára, valamint rögzíti azokat a követelményeket, melyeket a Szolgáltatónak a Szolgáltatások nyújtása során teljesítenie kell.
- 8) Jelen bizalmi szolgáltatási rend az {Sz13} RFC 3647 nemzetközi ajánlás alapján készült, felépítésében és tartalmában – a szükséges, Szolgáltatóra specifikus eltérésektől eltekintve – szigorúan követi annak előírásait.
- 9) Jelen bizalmi szolgáltatási rend előírja az állampolgárok, mint természetes személyek számára kibocsátott minősített tanúsítványokkal kapcsolatos, a Szolgáltatások nyújtása során teljesíteni szükséges összes követelményt, melyeket az alábbi nemzetközi szabványok határoznak meg:
  - a) EN 319 401: General policy requirements for Trust Service Providers {Sz1}
  - b) EN 319 411-1: Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements {Sz2}
  - c) EN 319 411-2: Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates {Sz3}
  - d) EN 319 412-1: Certificate Profiles; Part 1: Overview and common data structures {Sz4}
  - e) EN 319 412-2: Certificate Profiles; Part 2: Certificate profiles for certificates issued to natural persons {Sz5}
  - f) EN 319 412-5: Certificate Profiles; Part 5: QCStatements {Sz6}

- 10) Ezen követelmények teljesítésének módját, illetve az itt megnevezett eljárások részletes leírását a {D5} "Bizalmi Szolgáltatási Szabályzat a Digitális Állampolgárság Program keretében kibocsátott minősített tanúsítványokhoz" (BSZ-DÁP-TAN) dokumentum tartalmazza.
- 11) Jelen bizalmi szolgáltatási rendnek megfelelően kibocsátott tanúsítványok az {Sz4} EN 319 412-1 szabvány 3.1 fejezetében meghatározott "EU minősített tanúsítványok", és tartalmazzák jelen dokumentum objektum azonosítóját, mely alapján az érintett felek képesek meghatározni az adott tanúsítvány alkalmazhatóságát és megbízhatóságát.
- 12) Jelen bizalmi szolgáltatási rend megfelel a {J1} eIDAS rendeletben megállapított - minősített bizalmi szolgáltatásra vonatkozó - követelményeknek, és a hatálya alatt nyújtott szolgáltatás EU minősített bizalmi szolgáltatásnak minősül.

## 1.2. Dokumentum neve és azonosítása

### 1.2.1. A dokumentum neve

- 13) Jelen bizalmi szolgáltatási rend teljes neve: NISZ Zrt. "Bizalmi Szolgáltatási Rend a Digitális Állampolgárság Program keretében kibocsátott minősített tanúsítványokhoz".
- 14) A bizalmi szolgáltatási rend rövid neve: BR-DÁP-TAN.
- 15) A bizalmi szolgáltatási rend objektum azonosítója és verziószáma a címlapon található.
- 16) A jelen BR-DÁP hatálya alatt kiadott tanúsítványok kibocsátására és felhasználására vonatkozó részletes szabályokat a {D5} BSZ-DÁP-TAN szolgáltatási szabályzat tartalmazza.
- 17) Jelen BR-DÁP-TAN hatályba lépését és hatályának megszűnését a 9.10 fejezet tartalmazza.
- 18) Jelen BR-DÁP-TAN-nak csak a Szolgáltató elektronikus bélyegzőjével vagy a Szolgáltatásokért felelős vezető elektronikus aláírásával ellátott változata tekinthető hitelesnek.

### 1.2.2. A dokumentum azonosítása

- 19) A BR-DÁP-TAN a {J2} DÁP tv. 8. § 5. pontja szerinti *bizalmi szolgáltatási rend*, mely a Szolgáltatásokra vonatkozó feltételeket és biztonsági követelményeket tartalmazó szabálygyűjtemény.

### 1.2.3. Hitelesítési rendek

- 20) A BR-DÁP-TAN bizalmi szolgáltatási rend megfelel az {Sz3} EN 319 411-2 szabvány 5.5.1 fejezetében definiált QCP-n-qscd (OID: 0.4.0.194112.1.2) hitelesítési rendnek.

## 1.3. PKI közösség

- 21) Jelen bizalmi szolgáltatási rendben szereplő PKI közösség az alábbi felekből áll:
  - a) **Szolgáltató:** a jelen bizalmi szolgáltatási rendnek megfelelő tanúsítványokat kibocsátó minősített bizalmi szolgáltató, amely a tanúsítványok kibocsátásával és menedzmentjével kapcsolatos műszaki tevékenységeket végzi;
  - b) **Közreműködő Felek:** a Szolgáltatóval szerződéses kapcsolatban álló és/vagy jogszabályban meghatározott, a Szolgáltatások nyújtásában közreműködő felek;
  - c) **Végfelhasználók:** a tanúsítványt igénylő állampolgárok (Aláírók);
  - d) **Érintett Felek:** a tanúsítvány felhasználásával létrehozott elektronikus aláírásokat fogadó harmadik felek.

- 22) Azon tevékenységek vonatkozásában, melyeket a Szolgáltató nem maga lát el, Szolgáltató teljes körű felelősséget vállal azért, hogy a Közreműködő Fél tevékenysége során jelen dokumentumban foglalt követelmények teljesülnek.

### **1.3.1. Hitelesítő szervezet**

- 23) A hitelesítő szervezet a Szolgáltató központi szervezete, amely a hitelesítőközpontokból, a szolgáltatás-támogató informatikai rendszerek erőforrásaiból, az ezt körül vevő biztonságos fizikai környezetből, valamint az üzemeltető és szolgáltatást ellátó személyzetből áll. Jelen szolgáltatási rend szempontjából feladatai közé tartozik a tanúsítvány igénylések feldolgozása, tanúsítványok kibocsátása, tanúsítványok visszavonása, valamint a kibocsátott tanúsítványokra vonatkozóan visszavonási információk szolgáltatása.
- 24) Jelen bizalmi szolgáltatási rend hatálya alatt Szolgáltató kizárólag az állampolgárok részére, a Digitális Állampolgárság Program keretében bocsát ki tanúsítványokat.

#### **1.3.1.1. Gyökér-hitelesítőközpont**

- 25) A Szolgáltató elsőnek létrehozott, fizikailag is működő hitelesítőközpontja, amely az alárendelt másodlagos (produktív) hitelesítőközpontokat hitelesíti.

#### **1.3.1.2. Produktív hitelesítőközpont**

- 26) A gyökér hitelesítőközpont által létrehozott logikailag vagy fizikailag létező hitelesítőközpont, amely egy adott alkalmazási, szervezeti, földrajzi stb. területre ad ki tanúsítványokat.

#### **1.3.1.3. Szabályozási Csoport**

- 27) A Szabályozási Csoport a Szolgáltató által létrehozott szervezeti egység, amely a hitelesítés szolgáltatással kapcsolatos bizalmi szolgáltatási rendek, szolgáltatási szabályzatok és egyéb szabályzatok elkészítéséért, elfogadásáért, karbantartásáért és adminisztrációjáért felelős.

#### **1.3.1.4. Telefonos Ügyfélszolgálat**

- 28) Szolgáltató Telefonos Ügyfélszolgálatot (Kormányzati Ügyfélvonal - 1818) tart fenn, melynek révén heti hét napban, napi 24 órában biztosítja az Aláírók számára a tanúsítvány telefonos visszavonásának kezelését, továbbá ellátja a Szolgáltatásokkal kapcsolatos ügyfélszolgálatot.
- 29) Szolgáltató - a Telefonos Ügyfélszolgálat (Kormányzati Ügyfélvonal – 1818) kivételével - az állampolgárokkal közvetlen kapcsolatot nem tart, Aláírók a DÁP Keretalkalmazáson keresztül vehetik igénybe a tanúsítvány kibocsátásra és visszavonás kezelésre irányuló szolgáltatásokat.

### **1.3.2. Közreműködő Felek**

#### **1.3.2.1. DÁP szolgáltató**

- 30) A DÁP szolgáltató olyan külső közreműködő fél, mely elvégzi a 3.2.3 fejezet szerinti személyazonosítást és a Szolgáltató számára igazolja az Aláírók személyazonosságát.

### **1.3.3. Előfizetők**

- 31) Előfizetők Magyarország azon állampolgárai, akik a DÁP Keretalkalmazásban elvégzett regisztráció során aktiválják a digitális állampolgársághoz kapcsolódó felhasználói profiljukat, amellyel digitális állampolgárrá válnak és szerepelnek a Digitális Állampolgárság nyilvántartásban, amely tartalmazza az Aláírók kizárólagosan

azonosító DÁP Azonosítót, valamint ahhoz hozzárendelten a DÁP Keretalkalmazás működéséhez szükséges technikai adatokat.

- 32) Előfizető a DÁP Keretalkalmazásban végzett regisztráció során, a regisztrációs folyamattól elválaszthatatlanul jelen bizalmi szolgáltatási rend szerinti aláíró tanúsítvány is igényel, így a Szolgáltatások vonatkozásában bizalmi szolgáltatás ügyfélle válik a digitális állampolgárrá válással egyidejűleg.
- 33) Mivel az Előfizető a Digitális Állampolgárság Program keretében csak a saját nevére szóló tanúsítványt igényelhet, így jelen dokumentum fogalomrendszerében az Előfizető és az Aláíró személye azonos.
- 34) Az Aláíró felelősségét és kötelezettségeit a 9.6.3 fejezet írja le.

#### **1.3.4. Érintett Felek**

- 35) Az Érintett Fél a tanúsítványon alapuló elektronikus aláírással ellátott elektronikus dokumentumot fogadó természetes vagy jogi személy, aki vagy amely az elektronikus aláírásra hagyatkozva jár el a dokumentum hitelességének ellenőrzésekor. Az Érintett Fél nem áll szerződéses viszonyban a Szolgáltatóval.
- 36) Az Érintett Felek felelősségét a 9.6.4 fejezet írja le.

#### **1.3.5. Egyéb felek**

##### **1.3.5.1. Bizalmi Felügyelet**

- 37) A Bizalmi Felügyelet ellátja a Szolgáltató és az általa nyújtott bizalmi szolgáltatások felügyeletét, ellenőrzi a Szolgáltatások jogszabályi megfelelését, ellátja az ezzel kapcsolatos felügyeleti feladatokat. Többek között, figyelemmel kíséri az elektronikus aláírásokkal kapcsolatos technológiai és kriptográfiai algoritmusok fejlődését és határozatba foglalja Szolgáltató szolgáltatásainak nyújtása során használható biztonságos kriptográfiai algoritmusokat, és az azok meghatározott paraméterekkel történő alkalmazására vonatkozó követelményeket; határozatában elrendelheti Szolgáltató számára az aláírói tanúsítvány(ok) visszavonását.

##### **1.3.5.2. Kiberbiztonsági Felügyelet**

- 38) . A NISZ Zrt. a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény 1. § (1) bekezdés b) pontja alá tartozó szervezet. A társaság által végzett egyes tevékenységek a törvény 2. és 3. mellékletében is szerepelnek, a 2024. évi LXIX. törvény 16. § (1) bekezdése, a hatásköröket kijelölő 23. § (1) bekezdés a) pontja, valamint a végrehajtására kiadott 418/2024. (XII. 23.) Korm. rendelet 17. § (1) bekezdés e) pontja értelmében a szervezet auditálásának és felügyeletének kizárólagos jogköre a nemzeti kiberbiztonsági hatósághoz (Nemzeti Kiberbiztonsági Intézet) tartozik.

#### **1.4. A tanúsítvány alkalmazhatósága**

- 39) A BR-DÁP-TAN hatálya alatt kibocsátott tanúsítvány a {J1} eIDAS szerinti minősített tanúsítvány.
- 40) A BR-DÁP-TAN hatálya alatt kibocsátott tanúsítványok minősített elektronikus aláírást létrehozó eszköz alkalmazását megkövetelő, minősített tanúsítványok, így a kapcsolódó magánkulccsal együtt minősített elektronikus aláírás létrehozására, illetve ellenőrzésére használhatók.
- 41) A minősített elektronikus aláírás joghatását a {J3} Pp. 325. § (f) pontja határozza meg. E szerint a BR-DÁP-TAN hatálya alatt kibocsátott tanúsítvány felhasználásával létrehozott minősített elektronikus aláírással hitelesített dokumentum teljes bizonyító erejű magánokirat.

#### 1.4.1. Teszt tanúsítványok

- 42) A Szolgáltató az éles szolgáltatást nyújtó gyökér hitelesítő központ hierarchiájában - kizárólag csak a saját rendszerének tesztelése céljából - bocsát ki teszttanúsítványokat a {D5} BSZ-DÁP-TAN-ban foglaltak szerint.
- 43) A Szolgáltató az Aláírók vagy más, harmadik felek részére a Szolgáltatások keretében nem bocsát ki teszttanúsítványokat.
- 44) A teszt tanúsítványokhoz és azon alapuló elektronikus aláírásokhoz semmilyen joghatás nem kapcsolódik.

#### 1.4.2. Engedélyezett tanúsítvány használat

- 45) A kibocsátott tanúsítványokhoz kapcsolódó magánkulcsok kizárólag csak a {J2} DÁP tv. 52. § (1) bekezdés b) pontja szerinti eAláírás digitális keretszolgáltatás igénybevételével, elektronikus aláírás létrehozására használhatók.
- 46) A kibocsátott tanúsítványok, illetve a hozzájuk kapcsolódó nyilvános kulcsok kizárólag elektronikus aláírás érvényesítésére használhatók.

#### 1.4.3. Tiltott tanúsítvány használat

- 47) A Digitális Állampolgárság Program keretében kiadott tanúsítványt, illetve a kapcsolódó magánkulcsot az Aláíró kizárólag magánszemélyként használhatja fel; ezek használata bármilyen üzleti, munkahelyi vagy egyéb szakmai tevékenység céljából nem megengedett.
- 48) Tilos a tanúsítványt (illetve a hozzá kapcsolódó kulcspárt) felhasználni titkosításra vagy visszafejtésre, azonosításra, más tanúsítványok aláírására vagy bármilyen bizalmi szolgáltatás nyújtásához.

### 1.5. Szabályzat adminisztráció

#### 1.5.1. Szabályzatot karbantartó szerv

- 49) A Szolgáltatónak szervezetén belül Szabályozási Csoportot kell működtetnie, amely többek között jelen bizalmi szolgáltatási rend karbantartásáért is felelős.

#### 1.5.2. Kapcsolat

- 50) Szolgáltató adatai:

**NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.**

Cégjegyzék szám:	01-10-041633
Székhely:	1149 Budapest, Róna utca 52-80.
Levelezési cím:	1389 Budapest, Pf.: 133.
Telefon:	+36 1 459 4200
Fax:	+36 1 303 1000
URL:	<a href="http://hiteles.gov.hu">http://hiteles.gov.hu</a>
email:	<a href="mailto:ekozig@1818.hu">ekozig@1818.hu</a>
telefonos ügyfélszolgálat:	1818

### **1.5.3. A szolgáltatási rend alkalmasságának meghatározása**

- 51) A Szolgáltató legalább évente egyszer meg kell vizsgálja a bizalmi szolgáltatási rend, illetve a bizalmi szolgáltatási szabályzat tartalmi és formai megfelelőségét a vonatkozó jogszabályok, előírások és műszaki szabványok tekintetében, és ennek eredményeit változtatási igényként figyelembe kell vegye.
- 52) Amennyiben a változtatási igények befolyásolhatják a Szolgáltatásnak az Alanyok, Előfizetők vagy Érintett Felek általi elfogadását, a Szolgáltató erről előzetes értesítést kell közzé tegyen a Szolgáltatások internetes honlapján.
- 53) A változtatási igényeket a Szabályozási Csoport gyűjti, a módosításokat legalább évente egyszer elvégzi, majd ellenőrzésre és jóváhagyásra előterjeszti.

### **1.5.4. Szabályzat jóváhagyásának eljárása**

- 54) Szolgáltatónak rendelkeznie kell a szabályzatainak jóváhagyására és kiadására vonatkozó eljárásrenddel, melyet a szolgáltatási szabályzatában ismertetnie kell. Az eljárásrendben meg kell jelölni az eljárásért felelős személyt, valamint az egyéb fontos részleteket (pl. hatályba lépés napja).
- 55) A jóváhagyott szabályzatot Szolgáltató azonnal közzé kell tegye a Szolgáltatások internetes honlapján.

## 1.6. Fogalmak, rövidítések és hivatkozások

### 1.6.1. Fogalmak

1. **alany:** A Szolgáltató által kiadott tanúsítványban azonosított entitás, aki a tanúsítványban szereplő nyilvános kulcsnak (elektronikus aláírást érvényesítő adat) megfelelő magánkulcsot (elektronikus aláírás létrehozásához használt adat) birtokolja. Jelen bizalmi szolgáltatási rend szerint az Alany az állampolgár.
2. **aláíró:** elektronikus aláírást létrehozó természetes személy. Jelen bizalmi szolgáltatási rend szerint az Aláíró az állampolgár.
3. **aláírás érvényesítési adat:** olyan egyedi adat, amelyet az elektronikus aláírt dokumentumot megismerő személy (vagy eszköz) az elektronikus aláírás érvényesítésére használ. Jellemzően kriptográfiai nyilvános kulcs.
4. **aláírás létrehozásához használt adat:** olyan egyedi adat, amelyet az aláíró elektronikus aláírás létrehozásához használ. Jellemzően kriptográfiai magánkulcs.
5. **bizalmi felügyelet:** az adott tagállamban kijelölt felügyeleti szerv (Magyarországon a Nemzeti Média- és Hírközlési Hatóság), amely a bizalmi szolgáltatók felügyeletét végzi, melynek keretében előzetes és utólagos felügyeleti tevékenységek révén ellenőrzi, hogy a szolgáltatók és az általuk nyújtott szolgáltatások eleget tesznek a jogszabályban megállapított követelményeknek.
6. **bizalmi lista:** a tagállam által összeállított, fenntartott és közzétett elektronikus lista, amelyben kötelezően szerepelnek a tagállam felelőssége alá tartozó minősített bizalmi szolgáltatókra (opcionálisan a nem minősített bizalmi szolgáltatók is) valamint e szolgáltatók által nyújtott bizalmi szolgáltatásokra vonatkozó információk. A bizalmi lista automatizált feldolgozásra alkalmas, hitelességét elektronikus aláírás vagy elektronikus bélyegző biztosítja.
7. **bizalmi szolgáltatás:** rendszerint díjazás ellenében nyújtott, az alábbiakból álló szolgáltatások:
  - a) elektronikus aláírások tanúsítványainak, elektronikus bélyegzők tanúsítványainak, weboldal-hitelesítő tanúsítványoknak vagy egyéb bizalmi szolgáltatások nyújtására vonatkozó tanúsítványoknak a kibocsátása;
  - b) elektronikus aláírások tanúsítványainak, elektronikus bélyegzők tanúsítványainak, weboldal-hitelesítő tanúsítványoknak vagy egyéb bizalmi szolgáltatások nyújtására vonatkozó tanúsítványoknak az érvényesítése;
  - c) elektronikus aláírások vagy elektronikus bélyegzők létrehozása;
  - d) elektronikus aláírások vagy elektronikus bélyegzők érvényesítése;
  - e) elektronikus aláírásoknak, elektronikus bélyegzőknek, elektronikus aláírások tanúsítványainak vagy elektronikus bélyegzők tanúsítványainak a megőrzése;
  - f) távoli elektronikus aláírást létrehozó eszközök vagy távoli elektronikus bélyegzőt létrehozó eszközök kezelése;
  - g) elektronikus attribútumtanúsítványok kibocsátása;
  - h) elektronikus attribútumtanúsítványok érvényesítése;
  - i) elektronikus időbélyegzők létrehozása;
  - j) elektronikus időbélyegzők érvényesítése;
  - k) ajánlott elektronikus kézbesítési szolgáltatások nyújtása;
  - l) az ajánlott elektronikus kézbesítési szolgáltatásokon keresztül továbbított adatok és a kapcsolódó bizonyítékok érvényesítése;
  - m) elektronikus adatok és elektronikus dokumentumok elektronikus archiválása;
  - n) elektronikus adatok rögzítése elektronikus főkönyvbe.

A jelen bizalmi szolgáltatási rend szerinti bizalmi szolgáltatás az a) pont alatti szolgáltatás, azzal, hogy a Szolgáltató a Szolgáltatások keretében kizárólag elektronikus aláírások tanúsítványainak kibocsátását végzi.

8. **bizalmi szolgáltató:** egy vagy több bizalmi szolgáltatást nyújtó természetes vagy jogi személy; a bizalmi szolgáltató lehet minősített vagy nem minősített bizalmi szolgáltató.
9. **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.
10. **bizalmi szolgáltatási szabályzat:** a bizalmi szolgáltató nyilatkozata az egyes bizalmi szolgáltatások nyújtásával kapcsolatosan alkalmazott részletes eljárási és egyéb működési szabályokról, a szolgáltatási rendben meghatározott követelmények teljesítésének módjáról.
11. **biztonsági tisztviselő:** a bizalmi szolgáltatás biztonságáért, a biztonsági irányelvek és szabályzatok érvényre juttatásáért felelős személy.
12. **biztonságos környezet:** olyan fizikai környezet, mely védett illetéktelen hozzáféréstől, és bizonyos mértékig tűz, víz és egyéb katasztrófaeseményektől, egyéb erőszakos behatásoktól.
13. **DÁP Keretalkalmazás:** a digitális állampolgárság szolgáltatások igénybevétele céljából a nyilvánosság számára mobil eszközökre tervezett és kifejlesztett mobilalkalmazás. A {J2} DÁP tv. ezt keretalkalmazásnak nevezi.
14. **DÁP portál:** a DÁP szolgáltató és a DÁP szolgáltatások központi weboldala, mely a dap.gov.hu címen érhető el.
15. **DÁP szolgáltató:** olyan külső fél, mely a Szolgáltató számára különböző szolgáltatásokat biztosít (pl. nyilvántartás vezetés, keretalkalmazás nyújtása, adatkezelés), ezen belül elvégzi az Aláírók azonosítását és hitelesítését.
16. **digitális állampolgárság:** az állampolgárok azon joga, amellyel digitálisan ügyet intézhetnek, szolgáltatást vehetnek igénybe.
17. **digitális állampolgár azonosító (DÁP azonosító):** matematikai módszerrel képzett, különleges adatra nem utaló számjegysor, amely egyedi és tartós azonosítóként a polgárt a digitális térben egyértelműen azonosítja. A DÁP azonosító az Alaptörvény XXVI. cikk (2) bekezdésében meghatározott, a digitális ügyintézéshez mindenki számára biztosít egyedi digitális azonosítót.
18. **digitális állampolgárság nyilvántartás:** a {J2} DÁP tv. által létrehozott, a digitális állampolgár azonosítót tartalmazó ügyfélregisztrációs nyilvántartás.
19. **elektronikus aláírás:** olyan elektronikus adat, amelyet más elektronikus adatokhoz csatolnak, illetve logikailag hozzárendelnek, és amelyet az aláíró aláírásra használ.
20. **elektronikus aláírás érvényesítési adat:** lásd „Aláírás érvényesítési adat”.
21. **elektronikus aláírás létrehozásához használt adat:** lásd „Aláírás létrehozásához használt adat”.
22. **elektronikus aláírás célú tanúsítvány:** olyan elektronikus igazolás, amely az elektronikus aláírást érvényesítő adatokat egy természetes személyhez kapcsolja és igazolja legalább az érintett személy nevét vagy álnévét.
23. **elektronikus aláírás célú minősített tanúsítvány:** olyan elektronikus aláírás céljára használt tanúsítvány, amelyet minősített bizalmi szolgáltató bocsát ki; és amely megfelel a {J1} eIDAS I. mellékletében megállapított követelményeknek.
24. **elektronikus aláírás érvényesítés:** az elektronikusan aláírt elektronikus dokumentum aláírás kori, illetve ellenőrzés kori tartalmának összevetése, továbbá az aláíró személyének azonosítása a dokumentumon szereplő, illetve a bizalmi szolgáltató által közzétett elektronikus aláírás érvényesítési adat, tanúsítvány visszavonási információk, valamint a tanúsítvány felhasználásával.

25. **elektronikus aláírás létrehozó eszköz:** elektronikus aláírás létrehozására használt, konfigurált hardver- vagy szoftvereszköz.
26. **elektronikus azonosítás:** a természetes vagy jogi személyt, illetve egy másik természetes személyt vagy egy jogi személyt képviselő természetes személyt egyedileg azonosító elektronikus személyazonosító adatok felhasználásának folyamata.
27. **elektronikus azonosító eszköz:** olyan fizikai és/vagy nem fizikai egység, amely a személyazonosító adatokat tartalmaz, és amelyet online szolgáltatások, vagy adott esetben offline szolgáltatások céljából történő hitelesítésre használnak.
28. **elektronikus bélyegző:** olyan elektronikus adatok, amelyeket más elektronikus adatokhoz csatolnak, illetve logikailag hozzárendelnek, hogy biztosítsák a kapcsolt adatok eredetét és sértetlenségét.
29. **elektronikus bélyegzés célú tanúsítvány:** olyan elektronikus tanúsítvány, amely az elektronikus bélyegzőt érvényesítő adatokat egy jogi személyhez kapcsolja, és igazolja az érintett jogi személy nevét.
30. **elektronikus bélyegzés célú minősített tanúsítvány:** elektronikus bélyegző olyan tanúsítványa, amelyet minősített bizalmi szolgáltató bocsát ki; és amely megfelel a {J1} eIDAS III. mellékletében megállapított követelményeknek.
31. **elektronikus bélyegző létrehozásához használt adatok:** olyan egyedi adatok, amelyeket az elektronikus bélyegző létrehozója elektronikus bélyegző létrehozásához használ (jellemzően kriptográfiai magánkulcs)
32. **elektronikus bélyegzőt létrehozó eszköz:** elektronikus bélyegző létrehozására használt, konfigurált hardver- vagy szoftvereszköz.
33. **elektronikus dokumentum: elektronikus formában, különösen szöveg, hang-, képi vagy audiovizuális felvétel formájában tárolt bármilyen tartalom.**
34. **elektronikus időbélyegző:** olyan elektronikus adatok, amelyek más elektronikus adatokat egy adott időponthoz kötnék, amivel igazolják, hogy utóbbi adatok léteztek az adott időpontban.
35. **előfizető (aláíró):** a természetes személy, aki a érvényes Szolgáltatási Szerződéssel rendelkezik a Szolgáltatások igénybe vételére. Jelen bizalmi szolgáltatási rend szerint az Előfizető az Aláíró állampolgár.
36. **entitás:** a nyilvános kulcsú infrastruktúra (PKI) eleme, pl. egy tanúsítványkiadó, regisztrációs szervezet, végfelhasználó vagy eszköz.
37. **EU minősített tanúsítvány:** a {J1} eIDAS rendelettel összhangban kibocsátott minősített tanúsítvány.
38. **érintett fél:** az a természetes személy vagy jogi személy, aki/amely az elektronikusan aláírt, és/vagy elektronikusan időbélyegzett dokumentum fogadója, és az adott tanúsítványon alapuló elektronikus aláírásra hagyatkozva jár el az elektronikus aláírás és/vagy az elektronikus időbélyegző hitelességének ellenőrzésekor.
39. **érvényesítés:** az a folyamat, amelynek keretében ellenőrzik és igazolják, hogy az elektronikus adatok a {J1} eIDAS rendelettel összhangban érvényesek.
40. **érvényesítési adatok:** elektronikus aláírás vagy elektronikus bélyegző érvényesítéséhez használt adatok, jellemzően kriptográfiai nyilvános kulcs.
41. **felhasználó:**
  - a) (DÁP tv): a digitális szolgáltatást biztosító szervezet feladat- és hatáskörébe tartozó ügyben ügyfélként, félként vagy az eljárás alanyaként, az eljárás egyéb résztvevőjeként, a szolgáltatás igénybe vevőjeként vagy ezek képviselőjeként részt vevő olyan természetes személy vagy egyéb jogalany, ide nem értve a digitális szolgáltatást biztosító szervezetet és az ügyben eljáró digitális szolgáltatást biztosító szervezet tagját vagy alkalmazottját.

- b) (eIDAS): az e rendelettel összhangban nyújtott bizalmi szolgáltatásokat vagy elektronikus azonosító eszközöket igénybe vevő természetes vagy jogi személy, vagy egy másik természetes személyt vagy egy jogi személyt képviselő természetes személy.
  - c) (Jelen bizalmi szolgáltatási rendben): olyan entitás, aki/amely a Szolgáltatások keretében előállított kulcsokat és tanúsítványokat rendeltetésüknek megfelelően használja.
42. **fokozott biztonságú elektronikus aláírás:** olyan elektronikus aláírás, amely megfelel a {J1} eIDAS 26. cikkben meghatározott követelményeknek, azaz:
- a) kizárólag az aláíróhoz köthető;
  - b) alkalmas az aláíró azonosítására;
  - c) olyan, elektronikus aláírás létrehozásához használt adatok felhasználásával hozták létre, amelyeket az aláíró nagy megbízhatósággal kizárólag saját maga használhat;
  - d) olyan módon kapcsolódik azokhoz az adatokhoz, amelyeket aláírtak vele, hogy az adatok minden későbbi változása nyomon követhető.
43. **fokozott biztonságú elektronikus bélyegző:** olyan elektronikus bélyegző, amely megfelel a {J1} eIDAS 36. cikkben meghatározott követelményeknek, azaz:
- a) kizárólag a bélyegző létrehozójához kötött;
  - b) alkalmas a bélyegző létrehozójának azonosítására;
  - c) olyan, elektronikus bélyegző létrehozásához használt adatok felhasználásával hozták létre, amelyeket a bélyegző létrehozója nagy megbízhatósággal kizárólag saját maga elektronikus bélyegző létrehozására használhat;
  - d) olyan módon kapcsolódik azokhoz az adatokhoz, amelyekre vonatkozik, hogy az adatok minden későbbi változása nyomon követhető.
44. **gyökér-hitelesítőközpont (ROOT CA, vagy Főtanúsítvány kiadó):** az elsőnek létrehozott, fizikailag is működő hitelesítőközpont, amely az alárendelt másodlagos (produktív) hitelesítőközpontokat hitelesíti.
45. **hitelesítés:** olyan elektronikus folyamat, amely lehetővé teszi a természetes vagy jogi személy elektronikus azonosításának vagy az elektronikus adatok eredetének és sértetlenségének az igazolását.
46. **hitelesítési rend (Certificate Policy - CP):** olyan bizalmi szolgáltatási rend, amely bizalmi szolgáltatás keretében kibocsátott tanúsítványra vonatkozik.
47. **hitelesítési szabályzat (Certificate Policy Statement - CPS):** olyan bizalmi szolgáltatási szabályzat, amely bizalmi szolgáltatás keretében kibocsátott tanúsítványra vonatkozik.
48. **hitelesítőközpont (CA):** a Szolgáltató azon egysége, amely a hitelesítés-szolgáltatás magánkulccsal folytatott tevékenységét végzi. Egy hitelesítőközpontoz mindig egy magánkulcs tartozik. A hitelesítőközpont fizikailag egy telephelyre koncentráltan, védett, biztonságos körülmények között működik.
49. **időbélyegző:** lásd „elektronikus időbélyegző”.
50. **időbélyegzés:** az a folyamat, melynek során az elektronikus dokumentumhoz elektronikus időbélyegző hozzárendelése történik.
51. **informatikai rendszer:** a Szolgáltató által a bizalmi szolgáltatásokhoz, illetve annak elemeihez, így különösen a szolgáltatói kulcspár kezeléséhez, az elektronikus aláírás vagy bélyegző létrehozásához használt adatok előállításához, a tanúsítványok kibocsátásához, a kibocsátott tanúsítványt tartalmazó nyilvántartáshoz, a visszavonási nyilvántartásokhoz és a visszavonás kezeléséhez, az időbélyegzés szolgáltatáshoz, az elektronikus archiválás szolgáltatáshoz, valamint e tevékenységek informatikai védelméhez használt, a {J1} eIDAS 24. cikk (2) bekezdés e) és f) pontja szerinti megbízható rendszerek és termékek.

52. **Kiberbiztonsági Felügyelet:** az adott tagállamban kijelölt felügyeleti szerv, amely azon vállalatok, szervezetek – köztük a bizalmi szolgáltatók – kiberbiztonsági felügyeletét végzi, amelyek a társadalom és a gazdaság működése szempontjából alapvető szolgáltatásokat, illetve a digitalizáció fejlődése miatt nélkülözhetetlen infrastrukturális szolgáltatásokat nyújtanak. A NISZ Nemzeti Infokommunikációs Zrt. esetében a Nemzeti Kibervédelmi Intézet (NKI).
53. **kompromittálódás:** az az eset, amikor a magánkulcs (elektronikus aláírás létrehozásához használt adat vagy elektronikus bélyegző létrehozásához használt adat) használatára arra nem jogosított személy képessé válik vagy azokat megismeri.
54. **kriptográfiai kulcs:** olyan kriptográfiai transzformációt vezérlő egyedi jelsorozat, amelynek ismerete a kriptográfiai transzformáció elvégzéséhez, különösen az elektronikus aláírás vagy bélyegző előállításához, vagy ellenőrzéséhez szükséges.
55. **kriptográfiai modul (Hardware Security Module - HSM):** olyan hardver alapú biztonságos eszköz, amely előállítja, tárolja és védi a kriptográfiai kulcsokat, valamint biztonságos környezetet biztosít a kriptográfiai funkciók végrehajtására.
56. **lenyomat:** olyan meghatározott hosszúságú, az elektronikus dokumentumhoz rendelt bitsorozat, amelynek képzése során a használt eljárás (lenyomatképző eljárás) a képzés időpontjában teljesíti a következő feltételeket:
- a) a képzett lenyomat egyértelműen származtatható az elektronikus dokumentumból;
  - b) a képzett lenyomattól az elvárható biztonsági szinten belül nem lehetséges az elektronikus dokumentum tartalmának meghatározása vagy a tartalomra történő következtetés;
  - c) a képzett lenyomat alapján az elvárható biztonsági szinten belül nem lehetséges olyan elektronikus dokumentum utólagos létrehozatala, melyre alkalmazva a lenyomatképző eljárást, annak eredményeképp az adott lenyomat keletkezik.
57. **megfelelőségértékelő szervezet:** a 765/2008/EU rendelet 2. cikkének 13. pontjában meghatározott (megfelelőségértékelési tevékenységeket – beleértve a kalibrálást, vizsgálatot, tanúsítást és ellenőrzést – végző) szervezet, amelyet az említett rendelettel összhangban illetékesnek ismernek el a minősített bizalmi szolgáltató és az általa nyújtott minősített bizalmi szolgáltatások megfelelőségének értékelésére, vagy az európai digitális személyiadat-tárcák vagy az elektronikus azonosító eszközök tanúsításának elvégzésére.
58. **minősített bizalmi szolgáltatás:** olyan bizalmi szolgáltatás, amely megfelel a {J1} eIDAS rendeletben foglalt alkalmazandó követelményeknek, azaz a Bizalmi Listán szerepel.
59. **minősített bizalmi szolgáltató:** olyan bizalmi szolgáltató, amely egy vagy több bizalmi szolgáltatást nyújt és amelynek minősített státuszát a Bizalmi Felügyelet jóváhagyta, azaz a Bizalmi Listán szerepel.
60. **minősített elektronikus aláírás:** olyan, fokozott biztonságú elektronikus aláírás, amelyet minősített elektronikus aláírást létrehozó eszközzel állítottak elő, és amely elektronikus aláírás célú minősített tanúsítványon alapul.
61. **minősített elektronikus aláírás létrehozó eszköz:** olyan elektronikus aláírást létrehozó eszköz, amely megfelel a {J1} eIDAS II. mellékletben megállapított követelményeknek, rövidítése: QSCD (Qualified Signature Creation Device).
62. **minősített elektronikus bélyegző:** olyan, fokozott biztonságú elektronikus bélyegző, amelyet minősített elektronikus bélyegzőt létrehozó eszközzel állítottak elő, és amely elektronikus bélyegzés célú minősített tanúsítványon alapul.
63. **minősített elektronikus bélyegzőt létrehozó eszköz:** olyan elektronikus bélyegzőt létrehozó eszköz, amely értelemszerűen megfelel a {J1} eIDAS II. mellékletben megállapított követelményeknek.

64. **nyilvános (publikus) kulcsú infrastruktúra (PKI):** az elektronikus aláírás vagy elektronikus bélyegző, valamint titkosítás létrehozására, érvényesítésére, kezelésére szolgáló, aszimmetrikus kulcspárt alkalmazó infrastruktúra, beleértve a mögöttes intézményrendszert, a különböző bizalmi szolgáltatókat és eszközöket is.
65. **OCSP (Online Certificate Status Protocol):** Valós idejű tanúsítvány-állapotellenőrzési protokoll, amely lehetővé teszi a tanúsítványt felhasználó felek számára, hogy lekérdezzék egy adott tanúsítvány érvényességi állapotát (érvényes, visszavont vagy ismeretlen) egy megbízható válaszkiszolgálótól (OCSP responder). Az OCSP a hagyományos CRL (Certificate Revocation List) alternatívája vagy kiegészítője, gyorsabb és célzottabb ellenőrzést biztosítva.
66. **produktív hitelesítőközpont:** a gyökér-hitelesítőközpont által létrehozott logikailag vagy fizikailag létező hitelesítőközpont, amely egy adott alkalmazási, szervezeti, földrajzi stb. területre ad ki tanúsítványokat.
67. **rendkívüli üzemeltetési helyzet:** olyan, a Szolgáltató üzemmenetében zavart okozó rendkívüli helyzet, amikor a Szolgáltató rendes üzemmenetének folytatására ideiglenesen vagy véglegesen nincs lehetőség, beleértve a szolgáltatói magánkulcsok kompromittálódását is, vagy annak közvetlen veszélyét.
68. **rendszeradminisztrátor:** az informatikai rendszer telepítését, konfigurálását, karbantartását végző személy.
69. **rendszerüzemeltető:** az informatikai rendszer folyamatos üzemeltetését, mentését és helyreállítását végző személy.
70. **rendszervizsgáló:** a bizalmi szolgáltató naplózott, illetve archivált adatállományait vizsgáló, a szolgáltató által a szabályszerű működés érdekében megvalósított kontroll intézkedések betartásának ellenőrzéséért, a meglévő eljárások folyamatos vizsgálatáért és monitorozásáért felelős személy.
71. **személyazonosító adat:** egy természetes vagy jogi személy, vagy egy másik természetes személyt vagy egy jogi személyt képviselő természetes személy személyazonosságának megállapítását lehetővé tevő, az uniós vagy a nemzeti joggal összhangban kibocsátott adatok.
72. **szolgáltatási szabályzat (Certificate Practice Statement - CPS):** a bizalmi szolgáltató nyilatkozata az egyes bizalmi szolgáltatások nyújtásával kapcsolatosan alkalmazott részletes eljárási vagy más működési követelményekről.
73. **szolgáltatási szerződés:** a bizalmi szolgáltató és a bizalmi szolgáltatási ügyfél között – általános szerződési feltételek elfogadásával létrejött szerződés, amely a bizalmi szolgáltatás nyújtására és a szolgáltatás igénybevételére vonatkozó feltételeket tartalmazza;
74. **szolgáltatói kulcspár:** a szolgáltatói magánkulcsból és a szolgáltatói nyilvános kulcsból álló, kriptográfiai kulcspár.
75. **szolgáltatói magánkulcs:** olyan kriptográfiai magánkulcs, melyet a szolgáltató a saját bizalmi szolgáltatásának igazolására, így különösen a tanúsítványok kibocsátására, visszavonási nyilvántartásokra, az időbélyegzésre, az archiváláshoz használ.
76. **szolgáltatói nyilvános kulcs:** olyan kriptográfiai nyilvános kulcs, melyet a szolgáltató magánkulcsának használatával létrehozott elektronikus aláírás, elektronikus bélyegző vagy elektronikus időbélyegző érvényesítésére használnak.
77. **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.
78. **tanúsítvány visszavonási lista (Certificate Revocation List - CRL):** valamely okból visszavont vagy felfüggesztett, azaz érvénytelenített tanúsítványok azonosítóit tartalmazó elektronikus lista, melyet a bizalmi szolgáltató bocsát ki és hitelesít.

79. **tanúsítványokkal kapcsolatos szabályzatok:** a bizalmi szolgáltatási rend, a szolgáltatási szabályzat, a szolgáltatási kivonat, valamint az általános szerződéses feltételek.
80. **távoli minősített elektronikus aláírás létrehozó eszköz:** az aláíró nevében valamely minősített bizalmi szolgáltató által a {J1} eIDAS 29a. cikkével összhangban kezelt, minősített elektronikus aláírást létrehozó eszköz.
81. **üzenethitelesítő kulcspár:** Az üzenethitelesítő kulcspár a DÁP Keretalkalmazás által generált hitelesítő kulcspár, melynek magánkulcsa az alkalmazás által generált és a Szolgáltató informatikai rendszere felé küldött adatok („üzenetek”) hitelességét hivatott biztosítani, oly’ módon, hogy ezen üzeneteket műszaki értelemben (és nem jogi értelemben) digitálisan aláírja.
82. **visszavonási jelszó:** az elektronikus aláíró tanúsítvány ügyfél kérelmére történő visszavonásához szükséges kód.

### 1.6.2. Rövidítések

57) A dokumentumban az alábbi rövidítések fordulnak elő:

Rövidítés	Angol megfelelő	Megnevezés
ÁSZF-DÁP	-	Általános Szerződési Feltételek a DÁP eAláírás szolgáltatáshoz
BR-DÁP-TAN	-	Bizalmi Szolgáltatási Rend a Digitális Állampolgárság Program keretében kibocsátott minősített tanúsítványokhoz
BSZ-DÁP-TAN	-	Bizalmi Szolgáltatási Szabályzat a Digitális Állampolgárság Program keretében kibocsátott minősített tanúsítványokhoz
BR-DÁP-TK	-	Bizalmi Szolgáltatási Rend a Digitális Állampolgárság Program keretében nyújtott elektronikus aláírások létrehozása és távoli elektronikus aláírás létrehozó eszköz kezelése minősített bizalmi szolgáltatáshoz
CA	Certification Authority	hitelesítő szervezet
CP	Certificate Policy	hitelesítési rend
CPS	Certificate Practice Statement	hitelesítési szolgáltatási szabályzat
CRL	Certification Revocation List	tanúsítvány visszavonási lista
DÁP	-	Digitális Állampolgárság Program
DÁP-TK	-	Szolgáltató {D10} BR-DÁP-TK szerinti szolgáltatása
HSM	Hardware Security Module	hardver kriptográfiai eszköz
NTP	Network Time Protocol	időforrás protokoll
OCSP	Online Certificate Status Protocol	valós idejű tanúsítvány-állapot protokoll
PDS-DÁP	Public Disclosure Statement	Szolgáltatási Kivonat a Digitális Állampolgárság Program keretében biztosított bizalmi szolgáltatásokhoz
PKI	Public Key Infrastructure	nyilvános kulcsú infrastruktúra
QSCD	Qualified Signature Creation Device	minősített elektronikus aláírást létrehozó eszköz
RA	Registration Authority	regisztrációs szervezet
UTC	Coordinated Universal Time	koordinált univerzális idő

### 1.6.3. Hivatkozások

#### 1.6.3.1. Jogszabályi hivatkozások

{J1}	910/2014/EU Európai Parlament és a Tanács rendelete a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről (eIDAS)
{J2}	2023. évi CIII. törvény a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól (a továbbiakban: DÁP tv.)
{J3}	2013. évi V. törvény a Polgári Törvénykönyvről (a továbbiakban: Pp.)
{J4}	2016. évi CXXX. törvény a polgári perrendtartásról (a továbbiakban Ptk.)
{J5}	24/2016. (VI.30.) BM rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről
{J6}	679/2016/EU Európai Parlament és a Tanács rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (a továbbiakban: GDPR)
{J7}	2024. évi LXIX. törvény Magyarország kiberbiztonságáról (Kiberbiztonsági tv.)
{J8}	7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről
{J9}	Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS2 irányelv)
{J10}	A Bizottság (EU) 2024/2690 végrehajtási rendelete a 2022/2555 irányelvnek (NIS2 irányelv) a kiberbiztonsági kockázatkezelési intézkedések technikai és módszertani követelményei, valamint a DNS-szolgáltatók, a legfelső szintű doménnév-nyilvántartók, a felhőszolgáltatók, az adatközpont-szolgáltatók, a tartalomszolgáltató hálózati szolgáltatók, az irányított szolgáltatók, az irányított biztonsági szolgáltatók, az online piacterek, online keresőprogramok vagy közösségimédia-szolgáltatási platformok szolgáltatói és a bizalmi szolgáltatók tekintetében jelentősnek minősülő biztonsági események eseteinek további pontosítása tekintetében történő alkalmazására vonatkozó szabályok megállapításáról

#### 1.6.3.2. Szabványok és műszaki-technikai hivatkozások

{Sz1}	EN 319 401	General policy requirements for Trust Service Providers
{Sz2}	EN 319 411-1	Policy and security requirements for Trust Service Providers issuing certificates
{Sz3}	EN 319 411-2	Policy and security requirements for Trust Service Providers issuing EU qualified certificates
{Sz4}	EN 319 412-1	Certificate Profiles; Part 1: Overview and common data structures
{Sz5}	EN 319 412-2	Certificate Profiles; Part 2: Certificate profiles for certificates issued to natural persons
{Sz6}	EN 319 412-5	Certificate Profiles; Part 5: QCStatements

{Sz7}	ETSI TS 119 312	Electronic Signatures and Infrastructures (ESI);Cryptographic Suites
{Sz8}	ITU-T X.520	Information technology - Open Systems Interconnection - The Directory: Selected attribute types
{Sz9}	ITU-T X.509	Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate framework
{Sz10}	MSZ/ISO/IEC 15408	ISO/IEC 15408 (parts 1 to 5): Information security, cybersecurity and privacy protection – Evaluation criteria for IT security
{Sz11}	ISO/IEC 19790	ISO/IEC 19790: Information technology – Security techniques – Security requirements for cryptographic modules
{Sz12}	TS 119 615	Trusted Lists; Procedures for using and interpreting European Union Member States national trusted lists
{Sz13}	RFC 3647	Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework
{Sz14}	RFC 4514	Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names
{Sz15}	RFC 5280	Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile
{Sz16}	RFC 6960	X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol - OCSP
{Sz17}	TS 119 172-4	Signature policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists

### 1.6.3.3. Hivatkozott dokumentumok

{D1}	Általános Szerződési Feltételek a NISZ Zrt. Digitális Állampolgárság Programhoz kapcsolódó hitelesítés szolgáltatásaihoz (ÁSZF-DÁP)
{D2}	Általános Szerződési Feltételek Digitális Állampolgárság Keretalkalmazás szolgáltatás (DÁP Keretalkalmazás ÁSZF); Elérhetősége: <a href="https://dap.gov.hu/mobilapp-aszf">https://dap.gov.hu/mobilapp-aszf</a>
{D3}	Adatkezelési tájékoztató a DÁP eAláírás szolgáltatáshoz
{D5}	Bizalmi Szolgáltatási Szabályzat a Digitális Állampolgárság Program keretében nyújtott minősített tanúsítvány szolgáltatásokhoz (BSZ-DÁP-TAN)
{D10}	Jelen bizalmi szolgáltatási rend
{D11}	Bizalmi Szolgáltatási Szabályzat a Digitális Állampolgárság Program keretében nyújtott elektronikus aláírások létrehozása és távoli elektronikus aláírás létrehozó eszközök kezelése minősített bizalmi szolgáltatáshoz (BR-DÁP-TK)

## 2. KÖZZÉTÉTEL ÉS ADATTÁRAK

### 2.1. Tanúsítványtár

- 58) A Szolgáltatónak gondoskodnia kell arról, hogy az általa kibocsátott szolgáltatói tanúsítványok, a tanúsítványok visszavonási állapotára vonatkozó információk, valamint az egyéb közérdekű szolgáltatói információk az Aláírók és az Érintett Felek részére folyamatosan, napi 24 órában, heti hét napban rendelkezésre álljanak. A Szolgáltatónak mindent meg kell tennie annak érdekében, hogy az információk elérhetetlensége ne haladhassa meg a jogszabályokban és a szolgáltatási szabályzatban meghatározott időtartamot.
- 59) A Szolgáltatónak továbbá gondoskodnia kell arról, hogy a kibocsátott tanúsítványokat tartalmazó nyilvántartása (belső tanúsítványtár) a saját, DÁP-TAN és DÁP-TK szolgáltatást megvalósító informatikai rendszere és a DÁP szolgáltató számára folyamatosan, napi 24 órában, heti hét napban rendelkezésre álljon. A Szolgáltatónak mindent meg kell tennie annak érdekében, hogy a nyilvántartás elérhetetlensége ne haladhassa meg a jogszabályokban és a szolgáltatási szabályzatban meghatározott időtartamot.

### 2.2. Szolgáltatói információ közzététele

- 60) A Szolgáltatónak a szolgáltatói tanúsítványokat, valamint a végfelhasználói és szolgáltatói tanúsítványokkal kapcsolatos szabályzatokat (BR-DÁP-TAN, BSZ-DÁP-TAN, ÁSZF-DÁP, PDS-DÁP) internetes honlapján közzé kell tennie.
- 61) A Szolgáltatónak a végfelhasználói tanúsítványokat belső tanúsítványtárában kell tárolnia, a kiadott tanúsítványt az Aláíró számára rendelkezésre kell bocsátania a szolgáltatási szabályzatban meghatározottak szerint. Szolgáltató nem teheti közzé a végfelhasználói tanúsítványokat nyilvánosan elérhető tanúsítványtárban.
- 62) A Szolgáltatónak a szolgáltatói tanúsítványokkal kapcsolatos visszavonási állapot információkat CRL és OCSP formájában is biztosítania kell.
- 63) A Szolgáltatónak a végfelhasználói tanúsítványokkal kapcsolatos visszavonási állapot információkat OCSP formájában kell biztosítania.
- 64) A visszavonási állapot információk közzétételével kapcsolatos információkat a 4.10 fejezet tartalmazza.

### 2.3. A közzététel gyakorisága

- 65) A Szolgáltatónak a szolgáltatói tanúsítványokat legkésőbb azok éles üzembe helyezését megelőző 24 órán belül közzé kell tennie.
- 66) A Szolgáltatónak a tanúsítványokkal kapcsolatos szabályzatokat (BR-DÁP-TAN, BSZ-DÁP-TAN, ÁSZF-DÁP, PDS-DÁP) azok változása esetén legalább 30 nappal a változás hatályba lépését megelőzően közzé kell tennie.
- 67) A Szolgáltatónak a szolgáltatói tanúsítványokra vonatkozó CRL-t legalább 24 óránként frissítenie kell, azaz két egymást követő CRL kibocsátási között idő nem haladja meg a 24 órát. Amennyiben egy szolgáltatói tanúsítvány állapota megváltozik, a Szolgáltatónak a változást követően haladéktalanul, de legfeljebb egy órán belül új CRL-t kell előállítania és közzé tennie.
- 68) A Szolgáltatónak az OCSP szolgáltatása keretében minden OCSP kérésre friss választ kell előállítania és visszaadnia.

## 2.4. Hozzáférés-ellenőrzések

- 69) A Szolgáltatónak olvasás céljára korlátozás nélküli hozzáférést kell biztosítania a szolgáltatói tanúsítványokhoz, a végfelhasználói és szolgáltatói tanúsítványokkal kapcsolatos nyilvános szabályzatokhoz (BR-DÁP-TAN, BSZ-DÁP-TAN, ÁSZF-DÁP, PDS-DÁP), a tanúsítványokkal kapcsolatos visszavonási információkhoz.
- 70) A Szolgáltatónak biztonsági intézkedésekkel és eljárási szabályokkal gondoskodnia kell az információk jogosulatlan megváltoztatása, törlése, sérülése és megsemmisülése elleni védelemről.

## 3. AZONOSÍTÁS ÉS HITELESÍTÉS

### 3.1. Elnevezések

#### 3.1.1. Név típusok

- 71) A tanúsítványokban szereplő nevek megadása meg kell, hogy feleljen az {Sz8} ITU-T X.520 ajánlásnak.
- 72) A tanúsítvány kibocsátója (Issuer) mezőben szereplő név meg kell feleljen az {Sz5} EN 319 412-2 szabvány 4.2.3.1 fejezetében foglalt előírásoknak, így legalább az alábbi, {Sz8} ITU-T X.520 szerinti attribútumokat kell, hogy tartalmazza:
- countryName;
  - organizationName;
  - organizationIdentifier;
  - commonName.
- 73) Az Issuer mező fentiekén túl további attribútumokat is tartalmazhat.
- 74) A tanúsítvány alanya (Subject) mezőben szereplő név meg kell feleljen az {Sz5} EN 319 412-2 szabvány 4.2.4 fejezetében foglalt előírásoknak, így tartalmaznia kell az alábbi, {Sz8} ITU-T X.520 szerinti attribútumokat:
- countryName;
  - givenName;
  - surName;
  - serialNumber;
  - commonName.
- 75) A Subject mező fentiekén túl további név elemeket is tartalmazhat, azonban nem tartalmazhat álnevet (pseudonym).

#### 3.1.2. Nevek jelentése

- 76) A tanúsítvány Issuer mezőjében szereplő attribútumok jelentése megegyezik az {Sz8} ITU-T X.520 szerintivel. Ezen túl, az organizationIdentifier attribútum a Szolgáltató adószámát tartalmazza, tartalma és jelentése megfelel az {Sz4} EN 319 412-1 5.1.4 fejezetében megadottaknak.
- 77) A tanúsítvány Subject mezőjében szereplő attribútumok jelentése megegyezik az {Sz8} ITU-T X.520 szerintivel. Az ezen túl alkalmazandó további szabályokat a szolgáltatási szabályzatban kell ismertetni.

#### 3.1.3. Előfizetők névtelensége és álnév használata

- 78) Az Aláírók névtelensége és álnév használata nem megengedett.

#### 3.1.4. Különbéle név formák megjelenítési szabályai

- 79) A tanúsítványba foglalt megkülönböztető nevek (Distinguished Name) ASN.1 szintaxisa az {Sz15} RFC 5280 szerinti, megjelenítési szabályait az {Sz14} RFC 4514 adja meg.

#### 3.1.5. A nevek egyedisége

- 80) A Szolgáltatónak biztosítania kell a tanúsítvány Subject mezőjébe foglalt megkülönböztető név (Distinguished Name) egyediségét, azaz gondoskodnia kell arról, hogy egy adott megkülönböztető nevet soha nem fog egy másik Aláíróhoz rendelni.

#### 3.1.6. Márkanevek elismerése, hitelesítése és szerepe

- 81) Szolgáltató nem foglalja be a tanúsítványba azokat a védjegyeket vagy márkanéveket, melyekkel Aláíró esetleg rendelkezik.

### 3.2. Kezdeti azonosítás

- 82) Szolgáltatónak az Aláíró kezdeti azonosítását, hitelesítését és jogosultságának ellenőrzését a DÁP szolgáltató, mint közreműködő fél által végzett, a {J2} DÁP tv. 63. § szerinti személyazonosításra alapozva kell végeznie, ennek részleteit a szolgáltatási szabályzatban kell ismertetnie.
- 83) A Szolgáltatónak a közte és DÁP szolgáltató, mint közreműködő fél között lévő jogviszonyt külön megállapodásban kell rendeznie, amelynek része a személyazonosság fentiek szerinti hitelesítésében történő közreműködése is.

#### 3.2.1. A magánkulcs birtoklásának bizonyítása

- 84) Az Aláíró számára a tanúsítványhoz tartozó magánkulcsot a Szolgáltató saját szervezetén belül maga generálja QSCD minősítésű kriptográfiai eszközben (DÁP-HSM modul) és azt hozzárendeli Aláíróhoz a 3.2.3 fejezetben leírt személyazonosság hitelesítését követően. A DÁP HSM modul állítja össze a produktív hitelesítőközpont felé a tanúsítványkérelmet, saját infrastrukturális magánkulcsával, elektronikus aláírással hitelesítve annak tartalmát, egyúttal bizonyítva, hogy a kapcsolódó magánkulcsot az Aláíró birtokolja.
- 85) A kérelmek, illetve kérések az eszközben valósulnak meg, azt el nem hagyják és a szükséges rendszerelemek egyazon zárt rendszert képezik.

#### 3.2.2. A szervezeti azonosság hitelesítése

- 86) A tanúsítvány az állampolgárok, mint természetes személyek számára kerül kibocsátásra és magánszemélyi minőségben kerül felhasználásra.
- 87) Következésképpen a Szolgáltatónak nem kell szervezeti azonosságot vizsgálnia, hitelesítenie.

#### 3.2.3. A személyazonosság hitelesítése

- 88) Az Aláíró személyazonosságának hitelesítését a DÁP szolgáltatónak kell végeznie a {J2} DÁP tv. 63. § szerint, ami meg kell feleljen a {J1} eIDAS rendelet 24.cikk (1a) bekezdés (c) pontja szerinti olyan egyéb azonosítási módszernek, amely biztosítja a természetes személy magas megbízhatósági szintű azonosítását.
- 89) A DÁP szolgáltatónak az általa végzett személyazonosítás magas megbízhatósági szintjét megfelelőségértékelő szervezet által kibocsátott megfelelőségértékelési jelentéssel kell igazolnia Szolgáltató felé.

#### **3.2.4. Előfizető nem ellenőrzött adatai**

90) Nincs kikötés.

#### **3.2.5. Jogosultság ellenőrzése**

91) A 3.2.3 fejezet szerinti személyazonosítás sikeressége esetén az Aláíró Szolgáltatás igénybevételére való jogosultságát a Szolgáltatónak igazoltnak kell tekintenie.

#### **3.2.6. Együttműködési kritériumok**

92) Szolgáltató a Szolgáltatások nyújtása során nem működhet együtt más bizalmi szolgáltatókkal.

### **3.3. Azonosítás és hitelesítés kulcscsere esetén**

93) A Szolgáltató nem nyújt kulcscsere szolgáltatást.

#### **3.3.1. Azonosítás és hitelesítés érvényes tanúsítvány esetén**

94) Nincs kikötés.

#### **3.3.2. Azonosítás és hitelesítés érvénytelen tanúsítvány esetén**

95) Nincs kikötés.

### **3.4. Azonosítás és hitelesítés visszavonási kérelem esetén**

96) Az Aláíró visszavonási kérelmének azonosításához szükséges felhasználóazonosítását a DÁP szolgáltató, mint külső fél kell végezze.

97) Szolgáltatónak a szolgáltatási szabályzatban foglaltak szerint meg kell győződnie a DÁP szolgáltató által továbbított visszavonási kérés hitelességéről és sértetlenségéről.

## **4. A TANÚSÍTVÁNYOK ÉLETCIKLUSA**

98) A tanúsítványok teljes életciklus folyamatát a Szolgáltatónak kell működtetnie.

### **4.1. Tanúsítványigénylés**

#### **4.1.1. Ki nyújthat be tanúsítványigénylést**

99) A Szolgáltatónak a szolgáltatási szabályzatban meg kell adnia azon személyek körét, akik jogosultak a tanúsítvány igénylésére.

#### **4.1.2. Igénylési folyamat és felelőségek**

100) Tanúsítvány a DÁP Keretalkalmazás megfelelő funkciójával igényelhető a szolgáltatási szabályzatban foglaltak szerint.

101) A tanúsítványigénylés folyamatát és az ezzel kapcsolatos felelőségeket a Szolgáltatónak a szolgáltatási szabályzatban kell részleteznie.

## 4.2. Tanúsítványigénylés feldolgozása

### 4.2.1. Azonosítási és hitelesítési műveletek

102) A Szolgáltató kizárólag a DÁP szolgáltatótól érkezett tanúsítványkérelmet fogadhat el, melyek hitelességét és sértetlenségét a szolgáltatási szabályzatban foglaltak szerint kell ellenőriznie. Ennek során:

- a) a DÁP szolgáltatót az üzeneten elhelyezett elektronikus bélyegző érvényesítésével azonosítani és hitelesíteni kell;
- b) a DÁP szolgáltató üzenetében szereplő, Aláíróra vonatkozó adatokat hitelesnek kell elfogadnia.

### 4.2.2. Tanúsítványigénylés elfogadása vagy visszautasítása

103) A Szolgáltatónak el kell fogadnia a sikeresen azonosított és hitelesített tanúsítványkérelmet.

104) A Szolgáltatónak vissza kell utasítania a tanúsítványkérelmet, ha annak azonosítása vagy hitelesítése sikertelen.

### 4.2.3. Tanúsítványigénylés feldolgozás időtartama

105) A Szolgáltatónak a szolgáltatási szabályzatban kell megadnia a tanúsítványkérelem feldolgozására vállalt időtartamot.

## 4.3. Tanúsítvány kibocsátás

### 4.3.1. Tanúsítványkibocsátás során a Szolgáltató által végzett műveletek

106) A Szolgáltatónak a tanúsítványkibocsátás során az alábbi műveleteket kell elvégeznie:

- a) A Szolgáltató ellenőrzi és hosszú távú érvényesítésre alkalmas formára egészíti ki a kulcsgenerálási kérelmet is jelentő tanúsítványkérelem DÁP szolgáltatót igazoló elektronikus bélyegzőjét, majd tárolja azt belső nyilvántartásaiban.
- b) A Szolgáltató saját informatikai rendszerében a szolgáltatási szabályzatban leírtak szerint megvalósítja az igényelt kulcspár generálását a DÁP-HSM modulban. A generált magánkulcs nem hagyja el a DÁP-HSM modult.
- c) A Szolgáltató a DÁP-HSM modultól kapott nyilvános kulcs és a tanúsítványkérelemből származó adatok alapján kiállítja a tanúsítványt.
- d) A kiállított tanúsítványt – a DÁP szolgáltató közvetítésével – visszaküldi a DÁP Keretalkalmazásnak, egyúttal gondoskodik a kibocsátott tanúsítvány saját adatbázisában történő tárolásáról is.

### 4.3.2. Előfizető értesítése a tanúsítvány kibocsátásáról

107) Szolgáltatónak a DÁP szolgáltató közvetítésével értesítenie kell az Aláírót a tanúsítvány kibocsátásáról.

## 4.4. Tanúsítványelfogadás

### 4.4.1. Tanúsítvány Előfizető általi elfogadása

108) A tanúsítványelfogadás módját Szolgáltatónak a szolgáltatási szabályzatban kell ismertetnie.

#### **4.4.2. Tanúsítvány közzététele**

109) Szolgáltató nem teheti közzé a végfelhasználói tanúsítványokat nyilvánosan elérhető tanúsítványtárban.

#### **4.4.3. További felek értesítése a tanúsítvány kibocsátásáról**

110) Szolgáltatónak a tanúsítvány kibocsátásáról automatizált elektronikus úton értesítenie kell a DÁP szolgáltatót.

### **4.5. A kulcspár és a tanúsítvány használata**

#### **4.5.1. Az Előfizető magánkulcs- és tanúsítvány használata**

111) Az Aláíró csak azt követően használhatja a magánkulcsot és a tanúsítványt, hogy a tanúsítványban foglalt adatok helyességéről meggyőződött.

112) Az Aláíró csak az 1.4.2 fejezetben ismertetett célokra és módon használhatja a magánkulcsot és a tanúsítványt.

113) Az Aláírónak a magánkulcs és a tanúsítvány használata során be kell tartania a 9.6.3 fejezetben ismertetett kötelezettségeit, különösen gondoskodnia kell a Szolgáltató által tárolt magánkulcsának távoli aktiválását lehetővé tevő aktiváló adat illetéktelen hozzáférés elleni védelméről.

#### **4.5.2. Az Érintett Felek nyilvános kulcs- és tanúsítvány használata**

114) A jelen bizalmi szolgáltatási rend hatálya alatt kibocsátott tanúsítványon alapuló elektronikus aláírás elfogadása során szükséges, hogy az Érintett Fél megfelelő körültekintéssel járjon el.

115) Az Érintett Félnak az elektronikus aláírás ellenőrzéséhez, a tanúsítvány érvényességének megállapításához minden esetben javasolt igénybe vennie a Szolgáltató visszavonási információt szolgáltató Szolgáltatásait (OCSP).

116) Az erre vonatkozó követelményeket a szolgáltatási szabályzat részletezi.

### **4.6. Tanúsítványok megújítása**

117) A Szolgáltató nem nyújt tanúsítvány megújítási szolgáltatást.

118) Az Aláírónak lejárt vagy lejárfélben lévő tanúsítvány esetén új tanúsítványt kell igényelnie, a 4.1 fejezetben leírt módon.

#### **4.6.1. Tanúsítvány megújítás körülményei**

119) Nincs kikötés.

#### **4.6.2. Ki kérelmezhet tanúsítvány megújítást**

120) Nincs kikötés.

#### **4.6.3. Tanúsítvány megújítási kérelmek feldolgozása**

121) Nincs kikötés.

#### **4.6.4. Az Előfizető értesítése a megújított tanúsítvány kibocsátásáról**

122) Nincs kikötés.

#### **4.6.5. Tanúsítvány Előfizető általi elfogadása**

123) Nincs kikötés.

#### **4.6.6. Megújított tanúsítvány közzététele**

124) Nincs kikötés.

#### **4.6.7. További felek értesítése tanúsítvány megújításról**

125) Nincs kikötés.

### **4.7. Kulcscsere**

126) A Szolgáltató nem nyújt tanúsítvány kulcscsere szolgáltatást.

#### **4.7.1. Kulcscsere körülményei**

127) Nincs kikötés.

#### **4.7.2. Ki kérelmezhet kulcscserét**

128) Nincs kikötés.

#### **4.7.3. Kulcscsere kérelmek feldolgozása**

129) Nincs kikötés.

#### **4.7.4. Előfizető értesítése az új tanúsítvány kibocsátásáról**

130) Nincs kikötés.

#### **4.7.5. Új tanúsítvány Előfizető általi elfogadása**

131) Nincs kikötés.

#### **4.7.6. Új tanúsítvány közzététele**

132) Nincs kikötés.

#### **4.7.7. További felek értesítése az új tanúsítvány kibocsátásáról**

133) Nincs kikötés.

### **4.8. Tanúsítványmódosítás**

134) A Szolgáltató nem nyújt tanúsítványmódosítás szolgáltatást.

135) Az Aláírónak a meglévő tanúsítványában foglalt adatok módosulása esetén a meglévő tanúsítványát vissza kell vonnia (lásd 4.9 fejezet) és új tanúsítványt kell igényelnie, a 4.1 fejezetben leírt módon.

#### **4.8.1. Tanúsítvány-módosítás körülményei**

136) Nincs kikötés.

#### **4.8.2. Ki kérelmezhet tanúsítvány-módosítást**

137) Nincs kikötés.

#### **4.8.3. Tanúsítvány-módosítási kérelmek feldolgozása**

138) Nincs kikötés.

#### **4.8.4. Előfizető értesítése az új tanúsítvány kibocsátásáról**

139) Nincs kikötés.

#### **4.8.5. Módosított tanúsítvány Előfizető általi elfogadása**

140) Nincs kikötés.

#### **4.8.6. Módosított tanúsítvány közzététele**

141) Nincs kikötés.

#### **4.8.7. További felek értesítése a módosított tanúsítvány kibocsátásáról**

142) Nincs kikötés.

### **4.9. Tanúsítvány visszavonás és felfüggesztés**

143) A Szolgáltató felfüggesztési szolgáltatást nem nyújt.

144) A tanúsítvány visszavonása a tanúsítvány érvényességének a tervezett érvényességi idő lejárta előtti megszűntetését jelenti. A visszavonás végleges és visszafordíthatatlan állapot.

145) A visszavont tanúsítványhoz tartozó magánkulcs használatát azonnal be kell szüntetni. A visszavonási kérelemnek a Szolgáltatóhoz történő benyújtásáig az Aláíró felelős a felmerült károkért. A visszavonási kérelem elfogadásától, a visszavonás tényének közzétételéig a Szolgáltató felelős a felmerülő károkért. Ez alól kivételt képez a bizonyíthatóan csalárd szándékkal történt visszavonás kérés, amely esetben a felmerült károkért a Szolgáltató nem vállal felelősséget. A visszavonás tényének közzététele után az Érintett Fél felelős a felmerülő károkért.

146) Az Érintett Feleknek javasolt ellenőrizniük a tanúsítvány visszavonási állapotát a tanúsítványon alapuló elektronikus aláírás elfogadása előtt.

#### **4.9.1. Visszavonás körülményei**

147) A Szolgáltatónak a szolgáltatási szabályzatban ismertetnie kell a visszavonáshoz vezető körülményeket.

#### **4.9.2. Ki kezdeményezheti a visszavonást**

148) Visszavonást kezdeményezhet:

- a) az Aláíró;

b) a Szolgáltató.

#### **4.9.3. Visszavonási kérelemre vonatkozó eljárás**

- 149) A Szolgáltatónak ellenőriznie kell a visszavonást kérelmező azonosságát és jogosultságát, valamint ellenőriznie kell a visszavonási kérelemben foglalt adatokat. Ha az ellenőrzések sikeresek, a Szolgáltatónak el kell végeznie a tanúsítvány visszavonását és a megváltozott visszavonási állapot információt közzé kell tennie, valamint értesítenie kell az Aláírókat a tanúsítvány visszavonásáról.
- 150) Szolgáltatónak a szolgáltatási szabályzatban meg kell adnia az arra az esetre vonatkozó eljárásrendet, ha a visszavonási kérelem huszonnégy (24) órán belül nem igazolható.
- 151) A tanúsítvány visszamenőleges visszavonása nem megengedett, és az sem, hogy a kérelmező egy jövőbeni visszavonási időpontot jelöljön meg a kérelemben.
- 152) A Szolgáltató az egyszer már visszavont tanúsítvány érvényességét nem állíthatja vissza érvényesre.
- 153) Szolgáltatónak a szolgáltatási szabályzatban tájékoztatást kell adnia arról, hogy az arra jogosultak hogyan kezdeményezhetik tanúsítvány visszavonását.

#### **4.9.4. Kivárási idő visszavonási kérelem esetén**

- 154) A Szolgáltató nem alkalmaz kivárási időt a visszavonási kérelmek teljesítése során.

#### **4.9.5. Visszavonási kérelem feldolgozásának időbelisége**

- 155) A Szolgáltatónak a benyújtott visszavonási kérelmet haladéktalanul, minden más típusú tevékenysége (így különösen tanúsítvány előállítás vagy kibocsátás) előtt fel kell dolgoznia.
- 156) A Szolgáltatónak a visszavonási igények fogadását éves szinten 99,9%-os rendelkezésreállással kell biztosítania.

#### **4.9.6. Visszavonás ellenőrzésének ajánlása az Érintett Felek számára**

- 157) Az Érintett Feleknek a tanúsítvány és az ahhoz felépített tanúsítványlánc minden elemének visszavonási állapotát javasolt ellenőriznie a tanúsítványból megállapított vagy a szolgáltatási szabályzatban megadott elérhetőségekről letöltött CRL vagy megkért OCSP válasz alapján.

#### **4.9.7. CRL kibocsátási gyakoriság**

- 158) A Szolgáltató a végfelhasználói tanúsítványokhoz nem biztosít CRL kibocsátást.
- 159) A Szolgáltatónak a szolgáltatási szabályzatban meg kell határoznia a szolgáltatói tanúsítványokra vonatkozó CRL kibocsátásának gyakoriságát.

#### **4.9.8. CRL előállítása és közzététele között leghosszabb idő**

- 160) A Szolgáltatónak a szolgáltatási szabályzatban meg kell adnia azt a maximális időtartamot, melyen belül a szolgáltatói tanúsítványokra vonatkozó CRL-t az előállítását követően közzéteszi.

#### **4.9.9. OCSP szolgáltatás biztosítása**

- 161) A Szolgáltatónak mind a végfelhasználói, mind a szolgáltatói tanúsítványok visszavonási állapotának megállapításához OCSP szolgáltatást kell nyújtania.

#### 4.9.10. OCSP alapú visszavonás ellenőrzés követelményei

162) A Szolgáltatónak a szolgáltatási szabályzatban meg kell adnia az OCSP alapú visszavonás ellenőrzésével kapcsolatban az Érintett Felek számára fontos figyelmeztetéseket.

#### 4.9.11. Visszavonási állapotközlés más formái

163) Nincs kikötés.

#### 4.9.12. Különleges követelmények a kulcs kompromittálódása esetére

164) A Szolgáltatónak mindent meg kell tennie annak érdekében, hogy a szolgáltatói magánkulcsának kompromittálódása esetén az eseményről az Aláírókat és az Érintett Feleket értesítse.

165) A produktív hitelesítőközpont magánkulcsának kompromittálódása esetén a Szolgáltatónak képesnek kell lennie az összes érintett végfelhasználói tanúsítvány visszavonására és az érintett CRL-nek 24 órán belüli kibocsátására és közzétételére, majd ezt követően, az adott szolgáltatói tanúsítvány visszavonására és az érintett CRL-nek 12 órán belüli kibocsátására és közzétételére.

#### 4.9.13. Felfüggesztés körülményei

166) A Szolgáltató nem nyújt felfüggesztési szolgáltatást.

#### 4.9.14. Ki kérelmezhet felfüggesztést

167) Nincs kikötés.

#### 4.9.15. Felfüggesztésre vonatkozó eljárás

168) Nincs kikötés.

#### 4.9.16. A felfüggesztés megengedett időtartama

169) Nincs kikötés.

### 4.10. Visszavonási állapot szolgáltatások

#### 4.10.1. Működési jellemzők

170) A Szolgáltatónak a végfelhasználói tanúsítványokhoz kapcsolódó visszavonási információkat OCSP formájában kell szolgáltatnia.

171) A Szolgáltatónak a szolgáltatói tanúsítványokhoz kapcsolódó visszavonási információkat mind CRL, mind OCSP formájában szolgáltatnia kell. A Szolgáltatónak biztosítania kell, hogy a visszavonási állapot információ változása mind a CRL, mind az OCSP szolgáltatásban azonosan, konzisztens módon megjelenjen, figyelembe véve az egyes szolgáltatásokban eltérő frissítési időket is.

##### 4.10.1.1. CRL

172) A Szolgáltató által kibocsátott CRL-nek meg kell felelnie a {Sz15} RFC 5280 szabványnak.

173) A CRL-nek tartalmaznia kell minden olyan visszavont tanúsítványt, melyek érvényessége a CRL kibocsátásának időpontjában nem járt még le.

- 174) A CRL-nek tartalmaznia a következő kibocsátás időpontját (nextUpdate). A záró CRL (az adott hitelesítőközpont által kiadott utolsó CRL) esetén a nextUpdate mező tartalma a „99991231235959Z” RFC 5280 {Sz9} szerinti speciális időpont. A Szolgáltatónak biztosítania kell, hogy az új CRL kibocsátása a nextUpdate mezőben jelzett időpont előtt minden esetben megtörténjen.
- 175) A Szolgáltatónak záró CRL-t kell kibocsátania, amikor egy adott hitelesítőközpont működtetését megszünteti:
- a) kulcs átvétel (5.6 fejezet) miatt;
  - b) a szolgáltatói magánkulcs kompromittálódása (5.7.3 fejezet) miatt; vagy
  - c) a szolgáltatási tevékenység megszüntetése (5.8 fejezet) miatt.
- 176) A Szolgáltató csak azt követően bocsáthatja ki a záró CRL-t, miután minden, az adott hitelesítőközpont által kibocsátott tanúsítvány lejárt vagy azok visszavonását elvégezte. Szolgáltatónak (illetve a szolgáltatási tevékenység megszüntetése esetén a szolgáltatást átvevő bizalmi szolgáltatónak, lásd 5.8 fejezet) a záró CRL kibocsátását követő 10 évig biztosítania kell a záró CRL elérhetőségét.
- 177) A Szolgáltatónak a CRL aláírásához ugyanazt a szolgáltatói magánkulcsot kell használnia, melyet a kérdéses tanúsítvány aláírására használt.
- 178) A Szolgáltatónak a szolgáltatási szabályzatban meg kell adnia a szolgáltatói tanúsítványokra vonatkozó CRL elérhetőségét.

#### **4.10.1.2. OCSP**

- 179) A Szolgáltató által biztosított OCSP szolgáltatásnak meg kell felelnie az {Sz16} RFC 6960 szabványnak.
- 180) Az OCSP szolgáltatást a Szolgáltatónak az {Sz16} RFC 6960 2.2 fejezetében meghatározott "Authorized Responder" elvnek megfelelően kell működtetnie.
- 181) Az OCSP szolgáltatás keretében csak olyan tanúsítványra vonatkozóan kerülhet pozitív („good” státuszt tartalmazó) válasz kiadásra, amely tanúsítványt az adott hitelesítőközpont bocsátott ki (azaz szerepel a tanúsítványtárban) és a tanúsítvány nincs visszavont állapotban.
- 182) A Szolgáltatónak a szolgáltatási szabályzatban meg kell adnia az OCSP kérésekre vonatkozó szabályokat.
- 183) Az OCSP szolgáltatás keretében a Szolgáltatónak biztosítania kell a visszavonási információt a tanúsítvány lejáratát követően is, az érintett hitelesítőközpont működtetési időtartamában.
- 184) A Szolgáltatónak a szolgáltatási szabályzatban meg kell adnia a szolgáltatói és a végfelhasználói tanúsítványokra vonatkozó OCSP szolgáltatás elérhetőségét.

#### **4.10.2. Szolgáltatás rendelkezésre állása**

- 185) A szolgáltatói tanúsítványokra vonatkozó CRL-nek, illetve az OCSP szolgáltatásnak az év minden napján, napi 24 órában elérhetőnek kell lennie, 99,9 %-os rendelkezésre állással, úgy, hogy egy eseti szolgáltatáskiesés nem lépheti túl a 3 órás időtartamot.

#### **4.10.3. Opcionális lehetőségek**

- 186) Nincs kikötés.

### **4.11. Az előfizetés vége**

- 187) Szolgáltatónak a szolgáltatási szabályzatban ismertetnie kell az előfizetés végét eredményező körülményeket.

## 4.12. Kulcsletét és visszaállítás

188) Szolgáltató nem nyújt kulcsletét és visszaállítás szolgáltatást.

### 4.12.1. Kulcsletét és visszaállítás szabályai

189) Nincs kikötés.

### 4.12.2. Rejtjelező kulcs tárolásának és visszaállításának rendje és szabályai

190) Nincs kikötés.

## 5. FIZIKAI, ELJÁRÁSBELI ÉS SZEMÉLYZETI BIZTONSÁGI ÓVINTÉZKEDÉSEK

191) A Szolgáltatónak gondoskodnia kell arról, hogy kellő, az irányadó szabványoknak megfelelő fizikai, eljárásbeli és személyzeti biztonsági óvintézkedések, illetve az ezeket érvényre juttató adminisztratív és irányítási eljárások kerüljenek alkalmazásra.

### 5.1. Fizikai óvintézkedések

#### 5.1.1. Telephelyek elhelyezése és szerkezeti felépítése

192) A Szolgáltatónak a Szolgáltatások nyújtásában közreműködő informatikai rendszereit fizikai és logikai védelemmel ellátott, legmagasabb védelmi szintet képező objektumaiban kell elhelyeznie és üzemeltetnie. A telephelyek elhelyezése és kialakítása során olyan egymásra épülő és egymást támogató védelmi megoldásokat kell alkalmazni, melyek képesek megakadályozni az illetéktelen hozzáférést és alkalmasak az informatikai rendszerek és a Szolgáltató által tárolt bizalmas adatok megóvására.

#### 5.1.2. Fizikai hozzáférés

193) A Szolgáltatónak védenie kell a Szolgáltatások nyújtásában közreműködő eszközeit és berendezéseit a jogosulatlan fizikai hozzáféréstől az eszközök manipulálásának megakadályozása érdekében.

194) Ehhez biztosítania kell, az alábbiakat:

- a) a géptermekbe történő minden belépés naplózásra kerül;
- b) a géptermekbe csak a bizalmi szerepkört betöltő, erre feljogosított munkatárs léphet be, azonosítást követően;
- c) önálló jogosultsággal nem rendelkező személy csak indokolt és engedélyezett esetben, a szükséges időtartamig tartózkodhat a géptermekben megfelelő jogosultságú, bizalmi munkakört betöltő kísérő személy állandó felügyelete mellett;
- d) az eszközök aktivizáló adatai (jelszavak, PIN kódok stb.) a géptermen belül sem tárolhatók nyílt formában;
- e) jogosulatlan személy jelenlétében:
  - a bizalmas adatokat tartalmazó adathordozókat fizikailag elzárva tartják;
  - a bejelentkezett terminálok nem maradnak felügyelet nélkül;
  - nem végeznek olyan munkafolyamatot, amely során bizalmas adat felfedésre kerülhet;
- f) a gépterem elhagyásakor ellenőrzésre kerül:
  - minden eszköz és berendezés megfelelően biztonságos üzemállapotban van;
  - minden terminálon megtörtént a kijelentkezés;
  - a fizikai tároló eszközök megfelelően elzárásra kerültek;
  - a fizikai védelmet biztosító rendszerek és berendezések megfelelően működnek.

### 5.1.3. Áramellátás és légkondicionálás

- 195) A Szolgáltatónak a gépteremben olyan szünetmentes áramellátó rendszert kell biztosítania, amely:
- a) megfelelő teljesítménnyel rendelkezik a gépterem informatikai és kiegészítő létesítményi berendezései áramellátásának biztosítására;
  - b) megvédi az informatikai berendezéseket a külső hálózat feszültség ingadozásai, feszültség kimaradásai és egyéb zavarok ellen;
  - c) tartós áramszünet esetére saját áramellátó berendezés biztosítja - üzemanyag utántöltéssel - tetszőlegesen hosszú időtartamig az áramellátást.
- 196) A Szolgáltatónak a gépteremben olyan légkondicionáló berendezést kell alkalmaznia, mely biztosítja az alábbiakat:
- a) az operátorok biztonságos munkavégzéséhez szükséges mennyiségű oxigén biztosított;
  - b) a levegő nedvességtartalma nem haladja meg az informatikai rendszerek által megkívánt szintet;
  - c) hűtés történik a szükséges üzemeltetési hőmérséklet biztosítására, az eszközök és berendezések túlhevülésének megakadályozására.

### 5.1.4. Beázás és elárasztás veszélyeztetettség

- 197) A Szolgáltatónak a géptermet meg kell védenie a beázástól, víz betöréstől és elárasztástól.

### 5.1.5. Tűz megelőzés és tűzvédelem

- 198) A Szolgáltatónak a géptermet füst- és tűzérzékelőkkel kell felszerelnie, melyek automatikusan riasztják az illetékes személyzetet. Minden helyiségben jól látható helyen kell elhelyezni a vonatkozó előírásoknak megfelelő típusú és mennyiségű kézi tűzoltó készüléket. A gépteremben automatikus tűzoltó rendszert kell kialakítani, amely emberi egészségre nem veszélyes és nem károsítja az informatikai eszközöket.

### 5.1.6. Adathordozók tárolása

- 199) A Szolgáltatónak meg kell védenie valamennyi adathordozóját a jogosulatlan hozzáféréstől, a megsemmisüléstől vagy véletlen rongálódástól.

### 5.1.7. Selejt kezelése és megsemmisítése

- 200) A Szolgáltatónak a környezetvédelmi előírások betartásával gondoskodnia kell feleslegessé vált eszközeinek, adathordozóinak megsemmisítéséről. A felesleges eszközöket és adathordozókat az erre kijelölt munkatárs személyes felügyelete mellett, széleskörűen elfogadott módszerekkel használhatatlanná kell tenni vagy visszaállíthatatlan módon törölni kell.

### 5.1.8. Fizikailag elkülönítetten őrzött mentési példányok

- 201) A Szolgáltatónak azt az adatmentést, amiből meghibásodás esetén a teljes szolgáltatás helyreállítható, olyan külső helyszínen kell tárolnia, mely megfelelő fizikai és működési védelemmel rendelkezik. Biztosítani kell a helyszínek között a mentett adatok biztonságos továbbítását.
- 202) A Szolgáltatónak biztosítania kell, hogy az adatmentést vagy abból a helyreállítást csak rendszerüzemeltető bizalmi munkakört betöltő személy végezze el.

## 5.2. Eljárásbeli előírások

203) A Szolgáltatónak gondoskodnia kell arról, hogy informatikai rendszereit biztonságosan, szabályszerűen, a meghibásodás minimális kockázata mellett üzemeltessék. A Szolgáltató személyzetének a feladatokat olyan eljárásbeli előírások alapján kell végeznie, melyek szinkronban vannak a jogszabályi, szabványi és belső biztonsági előírásokkal.

### 5.2.1. Bizalmi munkakörök

204) A Szolgáltatónak a szolgáltatási szabályzatban egyértelműen azonosítania kell azokat a munkaköröket, amelyekről a Szolgáltatások biztonsága függ. Ezeket a bizalmi munkaköröket és felelőségeket dokumentálni kell. A jogosultságokat és funkciókat olyan módon kell megosztani az egyes bizalmi munkakörök között, hogy egyedül egyetlen felhasználó se legyen képes a biztonsági védelmi intézkedések megkerülésére. A Szolgáltatónak biztosítania kell, hogy minden bizalmi munkakör betöltésre kerüljön.

205) A bizalmi munkakört betöltő személynek munkaviszonyban kell állnia Szolgáltatóval. Bizalmi munkakörbe a Szolgáltató felső vezetésének kell kineveznie a munkatársakat.

### 5.2.2. Az egyes feladatokhoz szükséges személyzeti létszámok

206) A Szolgáltatónak a szolgáltatási szabályzatában meg kell határozni, hogy mely műveletek végezhetőek csak kettős ellenőrzés mellett, egyéb meghatározott feltételek biztosításával.

207) A szolgáltatási szabályzatában az alábbi elvárást mindenképp meg kell fogalmazni:

208) Csak védett környezetben, legalább kettő, bizalmi munkakört betöltő munkatárs egyidejű fizikai jelenlétében végezhető el az alábbi műveletek:

- a) gyökér szolgáltató tanúsítvány kibocsátása;
- b) tanúsítványok aláírására használt szolgáltatói kulcspár létrehozása;
- c) szolgáltatói kulcspár biztonságos kriptográfiai eszközben történő telepítése és helyreállítása;
- d) szolgáltatói aláírás célú magánkulcs mentése, tárolása és visszaállítása.

### 5.2.3. Bizalmi munkakörökben elvárt azonosítás és hitelesítés

209) A bizalmi munkaköröket betöltő személyek azonosítását és hitelesítését multi-faktoros autentikációs mechanizmusokkal kell végezni, mielőtt a Szolgáltatások nyújtásában érintett kritikus informatikai rendszerekhez hozzáférhetnének.

210) A Szolgáltatónak a „legkisebb jogosultságok” elvét alkalmazva kell adminisztrálnia a bizalmi munkaköröket betöltő személyek felhasználói hozzáférési képességeit, különösen a {D5} BSZ-DÁP-TAN-ban meghatározottak biztosításával.

### 5.2.4. Egymást kizáró munkakörök

211) A Szolgáltatónak el kell különítenie az egymásnak ellentmondó feladatokat és felelősségi területeket, hogy csökkentsék eszközeinek jogosulatlan vagy nem szándékos módosításának, vagy azokkal való visszaélések lehetőségét.

212) A Szolgáltatónak biztosítania kell, hogy a bizalmi munkakörök vonatkozásában:

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

- b) a független rendszervizsgáló nem láthatja el az informatikai rendszerért általánosan felelős vezető, a regisztrációs felelős, és a rendszeradminisztrátor feladatait;
- c) törekedni kell a bizalmi munkakörök teljes személyi szétválasztására.

### 5.3. Személyzetre vonatkozó előírások

213) Szolgáltatónak gondoskodnia kell arról, hogy személyzeti előírásai, a munkatársak alkalmazására vonatkozó gyakorlatai fokozzák és támogassák a Szolgáltató működésének megbízhatóságát.

#### 5.3.1. Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

214) Biztosítani kell, hogy bizalmi munkakört csak olyan személyek tölthetnek be, akiknek a bizalmi munkakör betöltéséhez szükséges befolyásmentességét és szakértelmét a Szolgáltató erkölcsi bizonyítvánnyal, szakmai gyakorlattal, végzettséggel és szakképesítéssel igazolni tudja.

#### 5.3.2. Biztonsági háttér ellenőrzés eljárásai

215) A Szolgáltató olyan alkalmazottakat foglalkoztathat, akik:

- a) büntetlen előélettel rendelkeznek és nincs ellenük folyamatban olyan eljárás, ami a büntetlenséget befolyásolhatja (a büntetlen előéletet három hónapnál nem régebbi erkölcsi bizonyítvánnyal kell igazolni);
- b) nem állnak a bizalmi szolgáltatási tevékenység gyakorlását kizáró foglalkoztatástól eltiltás hatálya alatt.

#### 5.3.3. Képzési követelmények

216) A Szolgáltató csak olyan személyeket foglalkoztathat, akik az adott munkakör ellátásához szükséges mértékben elsajátították:

- a) a PKI elméletet;
- b) a kiberbiztonsággal és a személyes adatokkal kapcsolatos szabályokat;
- c) Szolgáltató informatikai rendszerének sajátosságait és kezelésének módját;
- d) a szerepkör ellátáshoz szükséges speciális ismereteket;
- e) Szolgáltató nyilvános és belső szabályzataiban meghatározott folyamatokat és eljárásokat;
- f) az egyes tevékenységek jogi következményeit;
- g) az alkalmazandó biztonsági szabályokat.

217) A Szolgáltató egyes éles informatikai rendszereihez csak az annak megfelelő használatához szükséges ismeretekkel rendelkező alkalmazottak kaphatnak hozzáférési jogosultságot.

#### 5.3.4. Továbbképzési gyakoriságok és követelmények

218) A Szolgáltatónak gondoskodnia kell arról, hogy a munkatársak folyamatosan megfelelő tudással rendelkezzenek, szükség esetén továbbképzést vagy ismétlő jellegű képzést kell tartania.

219) Legalább évente egyszer továbbképzést kell biztosítani az újonnan ismertté vált sebezhetőségekről, az IT biztonság aktuális gyakorlatáról, a munkatársak saját szakterületét érintően.

#### 5.3.5. Munkabeosztás körforgásának gyakorisága és sorrendje

220) Nincs kikötés.

### **5.3.6. Felhatalmazás nélküli tevékenységek büntető következményei**

221) A Szolgáltatónak a dolgozókkal kötendő munkaszerződésben szabályoznia kell a dolgozó felelősségre vonásának lehetőségét az elkövetett mulasztások, vétlen vagy szándékos károkozás esetére.

### **5.3.7. Szerződéses munkavállalókra vonatkozó követelmények**

222) A Szolgáltató bizalmi munkakörben csak munkaviszonyban álló személyt foglalkoztathat.

223) Az egyéb feladatok ellátására, vállalkozási vagy megbízási szerződésben foglalkoztatott személyeket Szolgáltató csak előzetes biztonsági ellenőrzést követően foglalkoztathatja. Az ellenőrzött személyekkel írásos megállapodást kell kötni, melyben rögzíteni kell az esetleges biztonsági szabályokat és a titoktartásra vonatkozó kikötéseket.

### **5.3.8. A személyzet számára biztosított dokumentációk**

224) A Szolgáltatónak folyamatosan biztosítani kell a személyzet részére a munkakörük ellátásához szükséges dokumentációk és szabályzatok rendelkezésre állását.

## **5.4. A biztonsági naplózás folyamatai**

### **5.4.1. Naplózott esemény típusok**

225) A Szolgáltatónak minden, az informatikai rendszerével és a Szolgáltatások nyújtásával kapcsolatos eseményt naplózni kell. A naplózott adatállománynak a szolgáltatás nyújtásának teljes folyamatát át kell fognia, és lehetővé tennie, hogy a valós helyzetek megítéléséhez a szükséges mértékben minden, a Szolgáltatásokkal kapcsolatos eseményt rekonstruálni lehessen.

### **5.4.2. Naplóállomány feldolgozásának gyakorisága**

226) A Szolgáltatónak biztosítani kell a naplóállományok rendszeres ellenőrzését és kiértékelését.

### **5.4.3. Naplóállomány megőrzési időtartama**

227) A naplóállományokat archiválni kell és gondoskodni azok biztonságos megőrzéséről az 5.5.2 fejezetben előírt időtartamig.

### **5.4.4. Naplóállomány védelme**

228) A naplóállomány minden bejegyzését védeni kell a módosítástól, illetve biztosítani kell, hogy a napló tartalmához csak arra feljogosított személyek férhessenek hozzá.

229) A naplóállományok kezelését olyan módon kell megoldani, hogy kizárható legyen a napló megsemmisülése, a napló bejegyzések törlése, módosítása, a bejegyzések sorrendjének bármilyen módon történő megváltoztatása.

### **5.4.5. Naplóállomány mentési folyamatai**

230) A naplóállományokról rendszeres mentést kell készíteni.

#### 5.4.6. Naplózás gyűjtési rendszere

- 231) A naplóbejegyzések gyűjtését belső komponenssel kell megoldani. A naplóbejegyzések gyűjtésének meg kell kezdődnie rendszer indításkor és rendszer leállítáig folyamatosan működni kell, és közben biztosítania kell a gyűjtött bejegyzések integritását és rendelkezésre állását, szükség esetén a bizalmasságát is.
- 232) A naplóbejegyzések gyűjtési rendszerének működési rendellenessége esetén a Szolgáltatónak fel kell függesztenie az érintett területek működését az üzemzavar elhárításáig.

#### 5.4.7. Rendellenes eseményeket kiváltó alanyok értesítése

- 233) Nincs kikötés.

#### 5.4.8. Sebezhetőség értékelések

- 234) A Szolgáltatónak rendszeres időközönként, a naplóállományok és egyéb információk kiértékelésén alapuló sebezhetőség vizsgálatot és behatolás tesztet kell végeznie, mely segítségével feltérképezi a potenciális belső és külső fenyegetéseket, melyek jogosulatlan hozzáférést eredményezhetnek vagy hatással lehetnek a tanúsítvány kibocsátási folyamatra, a tanúsítványban tárolandó adatok megmásítását, módosítását, sérülését vagy megsemmisülését eredményezhetik.
- 235) A Szolgáltatónak folyamatosan figyelemmel kell kísérnie az újonnan ismertté vált, kritikus sebezhetőségeket, és a szükséges ellenintézkedéseket lehetőség szerint 48 órán belül meg kell tennie, illetve – ha az ellenintézkedés költsége nem áll arányban a sebezhetőség lehetséges kihatásaival – cselekvési tervet kell készítenie és végrehajtania annak érdekében, hogy a sebezhetőség ne legyen kihasználható, illetve annak hatása elhanyagolható legyen, vagy dokumentálnia kell annak ténybeli alapját, hogy az adott sebezhetőség nem igényel intézkedést.

### 5.5. Adatok archiválása

#### 5.5.1. A tárolt adatok típusai

- 236) A Szolgáltatónak gondoskodnia kell arról, hogy megőrzésre kerüljön minden olyan információ, amely szükséges ahhoz, hogy egy elektronikus aláírás érvényessége bizonyítható legyen, továbbá amely a Szolgáltató és a rendszereinek megfelelő működését alátámasztja.
- 237) Ehhez legalább a szolgáltatási szabályzatban meghatározott információkat tárolja.

#### 5.5.2. Archívum megőrzési időtartama

- 238) A Szolgáltató az 5.5.1 fejezetben meghatározott archivált adatokat köteles megőrizni:
- az Aláíró tárolt magánkulcsával és a tanúsítványokkal kapcsolatos adatok és naplóállomány esetében a tanúsítvány érvényességnek lejáratáról számított 10 évig, illetve a tanúsítvánnyal előállított elektronikus aláírással kapcsolatos jogvita jogerős lezárásáig;
  - szabályzatok, szerződések esetében a hatályon kívül helyezés vagy megszűnés utáni 10 évig.

#### 5.5.3. Archívum védelme

- 239) A Szolgáltatónak biztosítania kell valamennyi archivált adatra azok sértetlenségét és hitelességét, a rendelkezésre állását és a bizalmasságát.

#### 5.5.4. Archívum mentési eljárásai

240) A Szolgáltatónak biztosítania kell az iratok, dokumentumok, elektronikus állományok biztonságos, hosszú távú megőrzését, illetve tárolását, továbbá az elektronikus formában archivált állományok adathordozóinak elavulás elleni védelmét a megőrzési időn belül.

#### 5.5.5. Az adatok időbélyegzésére vonatkozó követelmények

241) Valamennyi naplóbejegyzést el kell látni olyan időjellel, melyben legalább egy másodperc pontossággal fel van tüntetve a rendszer által szolgáltatott időpont.

242) Az elektronikus formában archivált adatokon legalább fokozott biztonságú elektronikus aláírást vagy bélyegzőt, valamint minősített időbélyegyet kell elhelyezni.

243) Az archivált adatok megőrzése során szükség esetén (pl. algoritmus váltás) gondoskodni kell az elektronikus aláírások, bélyegzők és időbélyegzők hitelességének fenntartásáról.

#### 5.5.6. Archívum gyűjtési rendszere

244) A naplóállományokat és az egyéb elektronikusán keletkezett adatokat a Szolgáltató védett informatikai rendszerén belül kell gyűjteni.

#### 5.5.7. Archívum hozzáférés és ellenőrzés eljárásai

245) A Szolgáltatónak az archivált adatokat meg kell védenie a jogosulatlan hozzáféréstől. A jogosult hozzáféréseket naplózni kell.

### 5.6. Kulcsátállítás

246) A Szolgáltatónak biztosítania kell, hogy a hitelesítő központok folyamatosan rendelkezzenek a működésükhöz szükséges érvényes kulccsal és tanúsítvánnyal.

247) Amennyiben új szolgáltatói kulcspár és tanúsítvány előállítása szükséges, a Szolgáltatónak ezt olyan módon kell kiviteleznie, hogy az átállítás az Aláírók és az Érintett Felek számára a lehető legkisebb kényelmetlenséget jelentse és megfeleljen a vonatkozó jogszabályi és szabványi követelményeknek.

### 5.7. Helyreállítás rendkívüli üzemeltetési helyzetek esetén

248) A Szolgáltató köteles meghozni minden szükséges intézkedést annak érdekében, hogy rendkívüli üzemeltetési helyzet, katasztrófa esetén a szolgáltatás kiesésből származó károkat minimalizálja és a Szolgáltatásokat a lehető legrövidebb időn belül helyreállítsa. A rendkívüli üzemeltetési helyzet bekövetkezése esetén a visszavonási nyilvántartások megbízható üzemeltetésének helyreállítása minden más szolgáltatás vagy tevékenység helyreállítását meg kell, hogy előzze.

249) A visszavonási nyilvántartások, a kibocsátott tanúsítványokat tartalmazó nyilvántartás és a visszavonás kezelési szolgáltatás 3 órát meghaladó kiesése esetén a Szolgáltatónak haladéktalanul értesítenie kell a Bizalmi Felügyeletet.

250) Egyéb incidens esetén - amennyiben az jelentős hatást gyakorol a szolgáltatásra vagy az annak keretében tárolt személyes adatokra -, az esetről való értesüléstől számított 24 órán belül értesíteni kell az Érintett Feleket, valamint jelenteni kell az incidenst a Bizalmi Felügyeletnek.

251) A bekövetkezett incidens kiértékelése alapján a Szolgáltatónak meg kell hoznia a szükséges módosító, javító intézkedéseket, hogy az incidens jövőbeli előfordulását megakadályozza.

### 5.7.1. Rendkívüli események és kompromittálódás kezelésének eljárásai

- 252) A Szolgáltatónak rendelkeznie kell üzletmenet folytonossági tervvel.
- 253) Rendkívüli üzemeltetési helyzetben a Szolgáltatónak dokumentálnia kell az eseményeket, azok körülményeit, az elhárításukra megtett intézkedéseket.
- 254) A Szolgáltatónak ki kell alakítani és fenn kell tartania egy tartalék CA rendszert, mely a rendkívüli üzemeltetési helyzetben képes a nyilvános szabályzatok elérhetőségét, a visszavonás kezelési szolgáltatások teljes értékű működését, a CRL-ek közzétételét biztosítani.
- 255) A rendkívüli üzemeltetési helyzetben a Szolgáltatónak a lehető legrövidebb időn belül tájékoztatást kell közzé tennie internetes honlapján, valamint - lehetőség szerint - elektronikus levélben kell értesítenie azokat a személyeket, akiket az esemény érint.

### 5.7.2. Sérült számítási erőforrások, szoftverek és/vagy adatok

- 256) A Szolgáltatónak olyan megbízható rendszert kell működtetni, mely a rendszerben bekövetkezett hiba esetén is biztosítja a Szolgáltatások működtetését és elérhetőségét.

### 5.7.3. Szolgáltató magánkulcsának kompromittálódása esetén követendő eljárás

- 257) A Szolgáltató magánkulcsának kompromittálódása esetén haladéktalanul meg kell tennie az alábbi lépéseket:
- visszavonja az összes érintett tanúsítványt;
  - záró CRL-t (4.10.1) bocsájt ki;
  - megszünteti az érintett magánkulcs használatát;
  - értesíti a Bizalmi Felügyeletet;
  - értesíti a DÁP szolgáltatót;
  - intézkedik valamennyi érintett fél értesítéséről;
  - új szolgáltatói kulcspárokat és tanúsítványokat hoz létre.

### 5.7.4. Üzletmenet folytonosság helyreállítás katasztrófát követően

- 258) A Szolgáltatónak rendelkeznie kell tartalék helyszínnel és informatikai rendszerrel, továbbá megtervezett eljárásokkal az áttelepülésre.

## 5.8. A szolgáltatási tevékenység megszüntetése

- 259) A Szolgáltatónak rendelkeznie kell a szolgáltatási tevékenység megszüntetésére vonatkozó, aktualizált tervvel.
- 260) A Szolgáltatónak rendelkeznie kell olyan bankgaranciával, mely fedezi a szolgáltatási tevékenység megszüntetésének költségeit abban az esetben, ha a Szolgáltató csődeljárás alá kerül vagy más okból kifolyólag nem képes önmaga fedezni a költségeket.
- 261) A szolgáltatási tevékenység megszüntetésére vonatkozó tervnek tartalmaznia kell legalább az alábbiakat:
- az Aláírók és az Érintett Felek értesítésének módja;
  - a Szolgáltatásokban Közreműködő Felek jogosultságainak megvonása;
  - a Szolgáltatásokkal kapcsolatos azon kötelezettségeknek átadása egy másik minősített bizalmi szolgáltatónak, melyek arra vonatkoznak, hogy bizonyítékot szolgáltatassanak a Szolgáltató működésével kapcsolatban - különösen az 5.5.1 fejezetben meghatározott adatoknak a megőrzése az 5.5.2 fejezetben megjelölt időtartamig;
  - a szolgáltatói magánkulcsok és azok mentései megsemmisítésének módja;
  - a Szolgáltató informatikai rendszerében foglalt adatokról teljes körű mentés készítése.

## 6. MŰSZAKI BIZTONSÁGI ÓVINTÉZKEDÉSEK

### 6.1. Kulcspár előállítás és telepítés

#### 6.1.1. Kulcspár előállítás

263) A Szolgáltatónak a tanúsítványok és visszavonási listák aláírására használandó kulcspárokat fizikailag védett környezetben, kriptográfiai modulban (HSM) kell előállítania, legalább két bizalmi munkakört betöltő személy együttes részvételével, illetéktelen személy jelenlétének kizárásával. A kriptográfiai modulnak meg kell felelnie a 6.2.1 fejezet szerinti követelményeknek. A tanúsítványok hitelesítésére használt kulcspárok előállítását dokumentált „kulcsceremónia” eljárás szerint kell végezni, melyről a vonatkozó szabvány követelményeinek megfelelő tartalmú jegyzőkönyvet kell felvenni. A Szolgáltató magánkulcsainak teljes életciklusuk alatt a kriptográfiai modulban kell maradniuk.

264) A Szolgáltatónak az Aláíró kulcspárját fizikailag védett környezetben, QSCD tanúsítással rendelkező kriptográfiai modulban (DÁP-HSM) kell előállítania. A kriptográfiai modulnak meg kell felelnie a 6.2.1 fejezet szerinti követelményeknek. Az Aláírók magánkulcsainak teljes életciklusuk alatt a kriptográfiai modulban kell maradniuk.

#### 6.1.2. Magánkulcs eljuttatása a tulajdonoshoz

265) A Szolgáltatónak az Aláíró magánkulcsát - annak teljes életciklusa során - abban a kriptográfiai modulban kell tárolnia, melyben a kulcspár előállítás megtörtént. Következésképpen a magánkulcsok tulajdonoshoz külön történő eljuttatása nem szükséges és nem megengedett.

#### 6.1.3. Nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz

266) A hitelesítőközpont a tanúsítványba foglalandó nyilvános kulcsokat csak az azonosított és feljogosított, kulcspárt előállító kriptográfiai modultól fogadhat el, annak szolgáltatói kulcsával előállított elektronikus bélyegző hitelesítése mellett.

#### 6.1.4. A szolgáltatói nyilvános kulcs közzététele

267) A Szolgáltatónak biztosítania kell, hogy a Szolgáltató nyilvános kulcsa a kicserélésen alapuló támadás (substitution attack) ellen védett módon legyen eljuttatva az Érintett Felekhez.

#### 6.1.5. Kulcs méretek

268) A Szolgáltatónak a Szolgáltatások nyújtása során - mind a szolgáltatói, mind a végfelhasználói kulcsok tekintetében - az {Sz7} ETSI TS 119 312 szabvány mindenkor hatályos verziója szerint megbízható szabványos algoritmusokat, paramétereket és kulcshosszakat kell használnia.

#### 6.1.6. A nyilvános kulcs paraméterek előállítása és megfelelőségének ellenőrzése

269) A szolgáltatói kulcspárokat a 6.1.1 fejezet szerint védett környezetben és tanúsított HSM modulban, legalább két bizalmi munkakört betöltő személy együttes részvételével, illetéktelen személy jelenlétét kizárva kell előállítani. A szolgáltatói kulcspárok generálása során Szolgáltatónak be kell tartania a HSM modul tanúsítási jelentésében foglalt előírásokat is.

270) Az aláírói (végfelhasználói) kulcspárok előállítását a 6.1.1 fejezet szerint védett környezetben és QSCD tanúsított DÁP-HSM modulban kell végrehajtani, olyan eljárások mellett, melyek megfelelnek a QSCD tanúsítási jelentésében foglalt előírásoknak is.

#### **6.1.7. A kulcshasználat célja (X.509 v3 kulcs használati mezőnek megfelelően)**

271) A Szolgáltatónak a tanúsítványokban a KeyUsage és ExtendedKeyUsage kiterjesztésekben az {Sz11} ITU-T X.509 v3 szabványnak megfelelően kell jeleznie a kulcs használat célját.

## **6.2. Magánkulcs védelme és kriptográfiai modul műszaki szabályozások**

### **6.2.1. Kriptográfiai modul szabványok és szabályozások**

272) A Szolgáltató a szolgáltatói magánkulcsok előállítására, tárolására és használatára csak olyan kriptográfiai modult alkalmazhat, amely olyan megbízható rendszer, amelynek értékelése az {Sz10} MSZ/ISO/IEC 15408 szerint, illetve azzal egyenértékű biztonsági kritériumok szerint 4-es vagy magasabb értékelési garancia szinten történt meg (EAL 4+).

273) A Szolgáltató az aláírói (végfelhasználói) magánkulcsok előállítására, tárolására és használatára csak olyan kriptográfiai modult alkalmazhat, amely rendelkezik a Bizalmi Felügyelet által nyilvántartott tanúsító szervezet, vagy az Európai Unió valamely tagállamában nyilvántartásba vett, tanúsításra jogosult szervezet által kiadott igazolással, a minősített elektronikus aláírást létrehozó eszköz (QSCD) követelményeinek való megfelelésről.

274) A Szolgáltatónak rendszeres időközönként ellenőriznie kell a QSCD tanúsított állapotának meglétét, továbbá a QSCD tanúsítás lejáratási időpontját össze kell vetnie a kiadott tanúsítványok lejáratásával, és meg kell tennie a megfelelő intézkedéseket ahhoz, hogy a kriptográfiai modul QSCD tanúsítása folyamatosan – legalább a kiadott tanúsítványok lejáratáig - fennálljon.

275) Amennyiben a QSCD tanúsítása megszűnik (lejár), a Szolgáltatónak vissza kell vonnia az összes olyan végtanúsítványt, amely az adott QSCD-n került kiadásra és érvényessége még nem járt le a tanúsítás megszűnésének időpontjában.

### **6.2.2. Több szereplős ("n-ből m") ellenőrzés**

276) Nincs előírás.

### **6.2.3. Magánkulcs letét**

277) A Szolgáltató a hitelesítőközpontok magánkulcsait nem teszi letétbe semmilyen célból.

278) A Szolgáltató nem nyújt az Aláírók számára magánkulcs letét szolgáltatást.

### **6.2.4. Magánkulcs visszaállítása**

279) A Szolgáltató a hitelesítőközpontok magánkulcsait és az aláírói (végfelhasználói) magánkulcsokat rendkívüli üzemeltetési helyzetek esetén a titkosított mentésből visszaállíthatja, hasonlóan szigorú fizikai, biztonsági óvintézkedések és eljárási szabályok betartásával, mint ahogy a magánkulcs előállítása eredetileg történt.

### **6.2.5. Magánkulcs mentése**

280) A hitelesítőközpontok szolgáltatói és aláírói (végfelhasználói) magánkulcsait biztonsági okokból menteni kell. A mentést titkosított formában, speciális eszközök alkalmazásával kell megvalósítani.

### **6.2.6. Magánkulcs bejuttatása a kriptográfiai modulba**

281) A Szolgáltató a hitelesítőközpontok magánkulcsait a 6.1.1 fejezetben leírtak szerint HSM modulban állítja elő, és azok teljes életciklusuk alatt a HSM modulban maradnak. Amennyiben a magánkulcs visszaállítása rendkívüli üzemeltetési helyzet során szükséges, akkor a Szolgáltató a 6.2.4 fejezet szerint végzi a magánkulcs bejuttatását a kriptográfiai modulba.

282) A Szolgáltató az aláírói (végfelhasználói) magánkulcsokat a 6.1.1 fejezetben leírtak szerint QSCD tanúsított kriptográfiai modulban (DÁP-HSM) állítja elő, és azok teljes életciklusuk alatt a kriptográfiai modulban maradnak. Amennyiben a magánkulcs visszaállítása rendkívüli üzemeltetési helyzet során szükséges, akkor a Szolgáltató a 6.2.4 fejezet szerint végzi a magánkulcs bejuttatását a kriptográfiai modulba.

### **6.2.7. Magánkulcs kriptográfiai modulban történő tárolásának módja**

283) A hitelesítőközpontok magánkulcsai teljes életciklusuk alatt a 6.2.1 fejezetben leírt HSM modulban kerülnek tárolásra.

284) Az Aláírói (végfelhasználói) magánkulcsok teljes életciklusuk alatt a 6.2.1 fejezetben leírt QSCD tanúsított kriptográfiai modulban (DÁP-HSM) kerülnek tárolásra.

### **6.2.8. Magánkulcs aktiválásának módja**

285) A hitelesítőközpontok magánkulcsainak aktiválását a Szolgáltatónak a HSM modul gyártói dokumentációjában előírtak szerint kell végeznie.

286) A Szolgáltatónak biztosítania kell a HSM és DÁP-HSM kriptográfiai modulok jogosulatlan hozzáférés ellen védelmét.

### **6.2.9. Magánkulcs aktív állapotának megszüntetési módja**

287) A szolgáltatói kulcsok deaktiválásának módját a Szolgáltatónak dokumentáltan szabályoznia kell.

288) Az aláírói (végfelhasználói) tanúsítványok magánkulcsát Szolgáltatónak minden egyedi vagy kötegelt aláírási műveletet követően azonnal és automatikusan deaktiválnia kell.

### **6.2.10. Magánkulcs megsemmisítésének módja**

289) A Szolgáltatónak a hitelesítőközpontok magánkulcsát visszaállíthatatlan módon meg kell semmisítenie, amikor használatuk már nem szükséges vagy a kapcsolódó tanúsítvány lejárt vagy visszavonásra került. A magánkulcs és az aktiválásához szükséges minden adat megsemmisítését olyan módon kell végezni, hogy annak végrehajtása után a magánkulcs semmilyen része ne legyen kikövetkezhető vagy levezethető.

290) A Szolgáltatónak a DÁP-HSM modulban tárolt aláírói (végfelhasználói) magánkulcsokat visszaállíthatatlan módon, felülírással meg kell semmisítenie, amikor a kapcsolódó tanúsítvány lejár vagy visszavonásra kerül. A magánkulcs megsemmisítését olyan módon kell végezni, hogy annak végrehajtása után a magánkulcs semmilyen része ne legyen kikövetkezhető vagy levezethető.

### **6.2.11. Kriptográfiai modul értékelése**

291) Lásd a 6.2.1 fejezetben.

### 6.3. Kulcspár gondozás egyéb szempontjai

#### 6.3.1. Nyilvános kulcs archiválása

292) A Szolgáltató köteles minden általa kibocsátott tanúsítvánnyal hitelesített nyilvános kulcsot a tanúsítványba foglalva archiválni és az érvényesség lejártától számított tíz évig megőrizni.

#### 6.3.2. Tanúsítvány érvényességi időszaka és kulcspár felhasználás időtartama

293) A kulcspár felhasználás időtartama azonos a nyilvános kulcs hitelességét igazoló tanúsítvány érvényességi idejével, melyet Szolgáltatónak a szolgáltatási szabályzatban kell megadnia.

294) A Szolgáltatónak biztosítania kell, hogy az előfizetői tanúsítvány érvényességi időszakának lejáratára minden esetben korábbi legyen, mint a hitelesítéséhez használt szolgáltatói tanúsítvány lejáratának időpontja.

### 6.4. Aktivizáló adatok

#### 6.4.1. Aktivizáló adatok előállítása és telepítése

295) A hitelesítőközpontok magánkulcsát aktivizáló adatokat a HSM modul felhasználói gyártói dokumentációjában előírtak szerint kell előállítani és telepíteni.

296) Az aláírói (végfelhasználói) magánkulcsokat aktivizáló adatok előállítását és telepítését a DÁP Keretalkalmazás felhasználói útmutatójában előírtak szerint kell előállítani és telepíteni.

#### 6.4.2. Aktivizáló adatok védelme

297) A hitelesítőközpontok magánkulcsát aktivizáló adatokat a Szolgáltató alkalmazottainak biztonságosan, technikai és szervezési intézkedésekkel védve kell kezelniük, jelszavakat csak titkosított formában tárolhatnak.

298) Az aláírói (végfelhasználói) magánkulcsokat aktivizáló adatok védelmét az Aláírónak kell biztosítania.

#### 6.4.3. Aktivizáló adatok egyéb szempontjai

299) Nincs kikötés.

### 6.5. Informatikai biztonsági óvintézkedések

#### 6.5.1. Informatikai biztonsági műszaki követelmények meghatározása

300) Az informatikai biztonság műszaki követelményeit a Szolgáltató az {Sz1} EN 319 401, {Sz2} EN 319 411-1 és {Sz3} EN 319 411-2 szabványoknak a nyilvános kulcsú tanúsítványokat kibocsátó, minősített bizalmi szolgáltatás nyújtására vonatkozó, informatikai biztonsági műszaki követelményeiben határozza meg.

301) Ennek alapján Szolgáltatónak olyan megbízható informatikai rendszert (beleértve a redundáns kiépítést) és technikákat kell kialakítania és üzemeltetnie, melyek biztosítják a Szolgáltató megbízható működését a Szolgáltatások nyújtásához. Ennek ismertetését a Szolgáltató részben a szolgáltatási szabályzatában (BSZ-DÁP), részben a belső biztonsági szabályzataiban írja le.

#### 6.5.2. Informatikai biztonsági értékelés

302) A Szolgáltatónak a minősített bizalmi szolgáltatásához kialakított és üzemeltetett informatikai rendszerét a {J8} 7/2024. (VI. 24.) MK rendelet 1. mellékletében felsorolt szempontok szerint biztonsági osztályba kell sorolnia.

- 303) Szolgáltatónak az informatikai rendszerek biztonsági értékelését a {J7} Kiberbiztonsági tv. rendelkezései szerint kell elvégeznie.
- 304) A Szolgáltatónak a minősített bizalmi szolgáltatásához kialakított és üzemeltetett informatikai rendszerével kapcsolatban teljesítenie kell a {J9} NIS2 irányelv és a kapcsolódó {J10} 2024/2690 végrehajtási rendelet vonatkozó követelményeit.

## 6.6. Életciklusra vonatkozó műszaki óvintézkedések

### 6.6.1. Rendszerfejlesztési óvintézkedések

- 305) A Szolgáltatónak gondoskodnia kell arról, hogy az általa vagy a nevében végzett valamennyi rendszerfejlesztési projektjében a biztonság követelményeit már a tervezési és követelmény meghatározási fázisban figyelembe vegyék annak érdekében, hogy a biztonság beépüljön az informatikai rendszerekbe.

### 6.6.2. Biztonságkezelési óvintézkedések

- 306) A Szolgáltatónak olyan eszközöket és eljárásokat kell alkalmaznia, melyek garantálják a Szolgáltatásokat megvalósító, megbízható informatikai rendszereinek konfigurációs beállításai, az operációs rendszer beállítások, a hálózati konfigurációs beállítások, továbbá az alkalmazott biztonsági mechanizmusok sértetlenségének és helyes működésének ellenőrzését.
- 307) A biztonságkezelési szabályokat a Szolgáltató belső társasági szintű és rendszer szintű információbiztonsági szabályzata tartalmazza.

### 6.6.3. Életciklus biztonsági óvintézkedések

- 308) A Szolgáltatónak belső szabályzatban meghatározott rendszeres időközönként el kell végeznie a Szolgáltatásokat megvalósító, megbízható informatikai rendszereinek konfigurációs beállításai, az operációs rendszer beállítások, a hálózati konfigurációs beállítások, továbbá az alkalmazott biztonsági mechanizmusok sértetlenségének és helyes működésének ellenőrzését.

## 6.7. Hálózatbiztonsági óvintézkedések

- 309) A hálózati védelmi intézkedéseket a Szolgáltató belső biztonsági szabályzatában meghatározott követelményeknek megfelelően kell megvalósítani, figyelembe véve az {Sz3} EN 319 411-2 szabvány 6.5.7 fejezetében leírt követelményeket is.

## 6.8. Időforrások

- 310) A Szolgáltatások nyújtásához használt megbízható rendszereket 24 óránként legalább egyszer, megbízható időforrásokkal (NTP) szinkronizálni kell az UTC időhöz.

## 7. TANÚSÍTVÁNY, CRL ÉS OCSP PROFILOK

### 7.1. Tanúsítvány profil

- 311) A Szolgáltató által kiadott tanúsítványoknak meg kell felelniük az {Sz8} RFC 5280 és az {Sz4} EN 319 412-1, {Sz5} EN 319 412-2, {Sz6} EN 319 412-5 műszaki szabványoknak, valamint a vonatkozó jogszabályi előírásoknak.
- 312) A tanúsítvány profilokat a Szolgáltatónak a {D5} BSZ-DÁP-TAN-ban meghatározott módon dokumentálnia kell.

#### **7.1.1. Verziószám**

313) A tanúsítványok verziószáma: V3.

#### **7.1.2. Tanúsítvány kiterjesztések**

314) A tanúsítványokban alkalmazott kiterjesztéseknek mindenben követniük kell az {Sz8} RFC 5280 és az {Sz4} EN 319 412-1, {Sz5} EN 319 412-2, {Sz6} EN 319 412-5 műszaki szabványok, valamint a vonatkozó jogszabályok előírásait.

315)

316) A Szolgáltatónak az Aláírók tanúsítványaiiban alkalmaznia kell a minősített tanúsítványokra vonatkozó nyilatkozatokat tartalmazó szabványos kiterjesztéseket, nem kritikusként megjelölve (qcStatements).

#### **7.1.3. Algoritmus azonosítók**

317) A szolgáltatási szabályzatban meghatározva.

#### **7.1.4. Név formák**

318) A név formák leírását és azok értelmezési szabályait a 3.1 fejezet tartalmazza.

#### **7.1.5. Név megszorítások**

319) A Szolgáltató a tanúsítványokban név megszorításokat (NameConstraints) nem tüntethet fel.

#### **7.1.6. Hitelesítési rend objektumazonosító**

320) A Szolgáltatónak a tanúsítványokban fel kell tüntetnie a hitelesítési rend objektumazonosítóját.

#### **7.1.7. Szabályzati megszorítások kiterjesztés használata**

321) Nincs előírás.

#### **7.1.8. Szabályzat minősítő szintaktikája és szemantikája**

322) Nincs előírás.

#### **7.1.9. A kritikus hitelesítési rendek (Certificate Policies) kiterjesztés feldolgozása**

323) Nincs előírás.

### **7.2. CRL profil**

324) A Szolgáltató által kiadott visszavonási listáknak meg kell felelniük az {Sz8} RFC 5280 műszaki szabványnak.

#### **7.2.1. Verziószám**

325) A visszavonási listák verziószáma: V2.

#### **7.2.2. CRL és CRL bejegyzés kiterjesztések**

326) Nincs előírás.

### 7.3. OCSP profil

327) A Szolgáltató által biztosított OCSP szolgáltatásnak meg kell felelnie az {Sz12} RFC 6960 műszaki szabványnak.

328) Az OCSP profilokat a Szolgáltatónak a {D5} BSZ-DÁP-TAN-ban meghatározott módon dokumentálnia kell.

#### 7.3.1. Verziószám

329) Az OCSP válaszok verziószáma: V1.

#### 7.3.2. OCSP kiterjesztések

330) Nincs előírás.

## 8. MEGFELELŐSÉGVIZSGÁLAT ÉS EGYÉB ÉRTÉKELÉSEK

331) Jelen bizalmi szolgáltatási rend előírja az összes, állampolgárok, mint természetes személyek számára kibocsátott minősített tanúsítványokkal kapcsolatos szolgáltatások során teljesíteni szükséges követelményt, melyeket a különösen az alábbi nemzetközi szabványok határoznak meg:

- a) EN 319 401: General policy requirements for Trust Service Providers {Sz1}
- b) EN 319 411-1: Policy and security requirements for Trust Service Providers issuing certificates {Sz2}
- c) EN 319 411-2: Policy and security requirements for Trust Service Providers issuing EU qualified certificates {Sz3}
- d) EN 319 412-1: Certificate Profiles; Part 1: Overview and common data structures {Sz4}
- e) EN 319 412-2: Certificate Profiles; Part 2: Certificate profiles for certificates issued to natural persons {Sz5}
- f) EN 319 412-5: Certificate Profiles; Part 5: QCStatements {Sz6}

### 8.1. Vizsgálatok gyakorisága és körülményei

332) A Szolgáltató vizsgálatának gyakoriságának és körülményeinek meg kell felelniük a hatályos jogszabályi előírásoknak.

333) A Szolgáltatónak legalább 24 havonta egyszer megfelelőségértékelést és 12 havonta egyszer felülvizsgálatot kell végeztenie a {J1} eIDAS, illetve a {J2} DÁP tv. követelményeinek való megfelelés tárgyában. A Szolgáltató köteles az elkészült megfelelőségértékelés jelentést annak kézhezvételétől számított három munkanapon belül benyújtani a Bizalmi Felügyeletnek.

334) A Szolgáltató a Szolgáltatások nyújtásához kialakított és üzemeltetett informatikai rendszerére vonatkozó kiberbiztonsági követelmények teljesítését a Nemzeti Kibervédelmi Intézet (NKI) hatósági ellenőrzése és felügyelete alatt állva biztosítja.

### 8.2. Auditor azonosítása és képesítése

335) A megfelelőségértékelés és a kiberbiztonsági audit előkészítésére, illetve az információbiztonsági rendszer ellenőrzésére a Szolgáltató külső rendszervizsgálót alkalmazhat.

336) A külső rendszervizsgáló által végzett auditokra a Szolgáltatónak olyan szakértőt vagy szakértői szolgáltatásokat nyújtó szervezetet kell megbízni, aki független a Szolgáltatótól, illetve az ellenőrzött rendszertől, területtől, és szakértelmét biztosítani tudja a PKI és az informatikai biztonság, valamint az ezen területekre vonatkozó technikai, technológiai, jogi, szabályzati ismeretek és auditálási módszertanok vonatkozásában.

337) A Szolgáltató tevékenységére és az informatikai biztonságra vonatkozó belső ellenőrzéseket a Szolgáltató belső szervezete végzi, az ott dolgozó biztonsági tisztviselők bevonásával.

338) A megfelelőségértékelési vizsgálatot a Szolgáltató olyan, a 765/2008/EU rendelet 2. cikkének 13. pontjában meghatározott megfelelőségértékelő szervezettel végezteti el, melyet az említett rendelettel összhangban illetékesnek ismernek el a minősített bizalmi szolgáltató és az általa nyújtott minősített bizalmi szolgáltatások megfelelőségének értékelésére.

### 8.3. Auditor függetlensége

339) A megfelelőségértékelő szervezet és az auditor, ezek munkatársai, valamint a külső rendszervizsgáló teljes mértékben függetlenek a Szolgáltatótól.

### 8.4. Audit során vizsgált területek

340) A megfelelőségértékelés az alábbi területeket fedi le:

- a) szabályzatok és dokumentációk;
- b) irányítási és ellenőrzési követelmények;
- c) személyzeti biztonsági követelmények;
- d) a szolgáltatói kulcspár kezeléséhez kapcsolódó követelmények;
- e) üzemeltetési és hozzáférési biztonság;
- f) fizikai és környezeti biztonság;
- g) folyamatos szolgáltatás biztosítása;
- h) adatbiztonság és archiválás.

341) A megfelelőségértékelés során megvizsgálásra kerül, hogy Szolgáltató és az általa nyújtott Szolgáltatások megfelelnek:

- a) hatályos jogszabályoknak és szabványoknak;
- b) a szolgáltatási szabályzatnak, illetve a bizalmi szolgáltatási rendnek.

342) Az NKI által végzett ellenőrzés az alábbi – a megfelelőségértékeléssel jelentős átfedésben lévő - kiberbiztonsági követelménycsoportok teljesülését vizsgálhatja:

- a) adathordozók védelme;
- b) azonosítás és hitelesítés;
- c) biztonsági események kezelése;
- d) ellátási lánc kockázatkezelése;
- e) értékelés, engedélyezés és monitorozás;
- f) fizikai és környezeti védelem;
- g) hozzáférés-felügyelet;
- h) karbantartás;
- i) készenléti tervezés;
- j) kockázatkezelés;
- k) konfigurációkezelés;
- l) naplózás és elszámoltathatóság
- m) programmenedzsment;
- n) rendszer- és információ sértetlenség;
- o) rendszer- és kommunikáció védelem;
- p) rendszer- és szolgáltatásbeszerzés;
- q) személyi biztonság;
- r) tervezés;

- s) tudatosság és képzés.

## 8.5. Hiányosságok esetén végrehajtandó tevékenységek

- 343) Az üzemszerű ellenőrzések, belső és külső auditok, szakértői elemzések által feltárt hiányosságok, hibás gyakorlatok kezelésére a Szolgáltatónak intézkedési tervet kell készítenie. A hiányosságokat késlekedés nélkül orvosolnia, az intézkedéseket dokumentálni és ellenőriznie kell.
- 344) A Bizalmi Felügyelet által végzett rendszeres helyszíni ellenőrzések során feltárt esetleges hiányosságokat a Szolgáltatónak a hatósággal megállapodott határidőn belül meg kell szüntetnie a hatályos jogszabályok alapján és a hatóságtól kapott információk és ajánlások figyelembevételével.

## 8.6. Eredmény kommunikációja

- 345) A belső és külső auditokat, szakértői elemzést végző személyek csak a megbízójuknak adhatnak információt a Szolgáltató tevékenységével kapcsolatban. A megfelelésértékelés, az audit és az ellenőrzés eredményei a Szolgáltató bizalmas üzleti információi, ezért azokat a társaság titokvédelmi előírásai szerint kell kezelni, azonban a hiányosságok felszámolásáról a felügyelet szervezet a következő helyszíni ellenőrzés során tájékoztatni kell. A Szolgáltató nem köteles a konkrét hiányosságot nyilvánosságra hozni.

# 9. EGYÉB ÜZLETI ÉS JOGI KÉRDÉSEK

## 9.1. Díjak

- 346) A díjazással kapcsolatos információkat a szolgáltatási szabályzat kell tartalmazza.

## 9.2. Anyagi felelősség

- 347) A Szolgáltatónak az anyagi felelősség mértékéről, illetve annak korlátairól a szolgáltatási szabályzatban rendelkeznie kell.

### 9.2.1. Biztosítási fedezet

- 348) A Szolgáltatónak felelősségbiztosítással kell rendelkeznie, mely egyaránt kiterjed az elektronikus aláírással, illetve az ezzel ellátott elektronikus dokumentummal szerződésen kívül okozott károkra és szerződésszegéssel okozott károkra, valamint a Bizalmi Felügyeletnél felmerült jogszabály szerinti költségekre, és amely fedezetet biztosít az összes károsultnak okozott kárra, a {D5} BSZ-DÁP-TAN-ban foglaltaknak megfelelően.
- 349) A felelősségbiztosítási szerződésnek meg kell felelnie a {J5} 24/2016 BM rendelet előírásainak is.

### 9.2.2. További követelmények

- 350) A Szolgáltatónak teljesítenie kell a {J5} 24/2016 BM rendelet 19. §-a szerinti pénzügyi követelményeket is.

### 9.2.3. Felelősségbiztosítás vagy garancia végfelhasználók számára

- 351) Nincs kikötés.

### 9.3. Üzleti információk bizalmassága

#### 9.3.1. Bizalmasan kezelendő információk köre

352) A Szolgáltatónak a szolgáltatási szabályzatban meg kell határoznia a bizalmasan kezelendő információk körét.

#### 9.3.2. Bizalmasnak nem tekintett információk köre

353) Szolgáltatónak a bizalmasnak nem tekintett információk köréről a szolgáltatási szabályzatban rendelkeznie kell.

#### 9.3.3. Bizalmas információk védelmének felelőssége

354) A Szolgáltatónak meg kell védenie a bizalmas információkat. A bizalmas információk védelmét a személyzet megfelelő képzésével, továbbá a munkavállalókkal, szerződéses partnerekkel megkötött szerződésekkel kell érvényre juttatni.

### 9.4. Személyes adatok védelme

#### 9.4.1. Adatvédelem

355) A Szolgáltatónak rendelkeznie kell adatvédelmi szabályozással, valamint a Szolgáltatásokra vonatkozó adatvédelmi tájékoztatóval {D3}, melyeknek összhangban kell lenniük a nemzetközi és hazai vonatkozó jogszabályokkal. Szolgáltatónak az adatvédelmi tájékoztatót {D4} elérhetővé kell tennie internetes honlapján.

#### 9.4.2. Bizalmasként kezelendő személyes adatok

356) A Szolgáltató csak az Aláíró kifejezett hozzájárulásával gyűjthet személyes adatot és csak olyan mértékben, ami a tanúsítvány kiállításához, valamint Aláíró tájékoztatásához, személyazonosságának megállapításához szükséges.

357) A Szolgáltató bizalmasként kezelendő személyes adatnak tekinti:

- a) az Aláíró minden adatát.

#### 9.4.3. Bizalmasként nem kezelendő személyes adatok

358) Szolgáltató nem bizalmasként kezelendő személyes adatnak tekinti a tanúsítványhoz kapcsolódó státusz információkat, beleértve a tanúsítvány esetleges visszavonásának okát és időpontját is.

#### 9.4.4. Személyes adatok védelmének felelőssége

359) A Szolgáltatónak gondoskodnia kell a személyes adatok védelméről, működésének és szabályzatainak meg kell felelniük a {J6} GDPR rendelkezéseinek.

#### 9.4.5. Személyes adatok felhasználásának elfogadása

360) Az Aláírónak a {D1} ÁSZF-DÁP elfogadásával tudomásul kell vennie a tanúsítvány kiállításához és a szerződés megkötéséhez szükséges adatok Szolgáltató által történő nyilvántartásba vételét, kezelését és tárolását.

#### 9.4.6. Felfedés hatósági vagy polgári peres eljárás keretében

- 361) A Szolgáltatónak bűncselekmények felderítése vagy megelőzése céljából, illetve nemzetbiztonsági érdekből - az adatigénylésre meghatározott jogszabályi feltételek teljesülése esetén - a nyomozó hatóságnak és a nemzetbiztonsági szolgálatoknak haladéktalanul és egyéb feltételek nélkül fel kell tárnia a jogszabályban meghatározott bizalmas információkat. Ilyen esetben a Szolgáltató rögzíti az adatátadás tényét, de arról nem tájékoztathatja az érintett Aláírót.
- 362) A Szolgáltató a tanúsítvány érvényességét érintő polgári peres, illetve nem peres eljárás során - az érintettség igazolása esetén - az ellenérdekű peres félnek vagy képviselőjének, valamint a megkereső bíróságnak feltárhatja a jogszabályban meghatározott bizalmas információkat. Ilyen esetben a Szolgáltató rögzíti az adatátadás tényét, és arról tájékoztatja az érintett Aláírót.

#### 9.4.7. Egyéb, felfedést eredményező körülmények

- 363) A Szolgáltatónak a szolgáltatási tevékenység, illetve a Szolgáltatások nyújtásának megszüntetése esetén az Aláíró adatait a jogszabályi kötelezettségeire tekintettel át kell adnia egy harmadik félnek.

### 9.5. Szellemi tulajdonjogok

- 364) A Szolgáltató által az Aláíró részére kibocsátott tanúsítvány és az ahhoz tartozó kulcspár tulajdonosa az Aláíró. A Szolgáltató a tanúsítványt a kikötéseiben és feltételeiben ismertetett esetekben és módon sokszorosíthatja, visszavonhatja és egyéb módon is kezelheti. A végfelhasználói tanúsítványban szereplő megkülönböztető név használatára az Aláíró jogosult.
- 365) A Szolgáltató tulajdonát képezik a szolgáltatói tanúsítványok, visszavonási információk, a végfelhasználói tanúsítványokban szereplő, Szolgáltató által létrehozott azonosítók.
- 366) Szolgáltató kizárólagos tulajdonát képezik a szabályzatai, szerződéses feltételei és egyéb, a Szolgáltatások internetes honlapján közzétett dokumentumai. Ezen dokumentumok felhasználása csak és kizárólag a Szolgáltatások használatával összefüggésben engedélyezett, minden egyéb kereskedelmi vagy egyéb célú felhasználása szigorúan tilos.

### 9.6. Tevékenységért viselt felelősség és helytállás

#### 9.6.1. Szolgáltató felelőssége és helytállása

- 367) A Szolgáltató felel a jelen bizalmi szolgáltatási rendben és a {D5} BSZ-DÁP-TAN szolgáltatási szabályzatban, valamint a {D1} ÁSZF-DÁP-ban megfogalmazott valamennyi kötelezettség maradéktalan betartásáért, még akkor is, ha a Szolgáltatások nyújtásához kapcsolódó egyes feladatokat a Közreműködő Felek vagy egyéb alvállalkozók végzik.

#### 9.6.2. A regisztrációs szervezet felelőssége

- 368) A Szolgáltató regisztrációs szervezetének felelőssége a tanúsítványkibocsátások megfelelőségének időszakos, {D5} BSZ-DÁP-TAN szerinti ellenőrzése.

#### 9.6.3. Aláíró felelőssége és helytállása

- 369) Az Aláíró jogait, felelősségeit és kötelezettségeit a {D5} BSZ-DÁP-TAN szolgáltatási szabályzatban meg kell határozni.

#### **9.6.4. Érintett Felek felelőssége és helytállása**

370) Az Érintett Felek felelősségeit és helytállását a {D5} BSZ-DÁP-TAN szolgáltatási szabályzatban meg kell határozni.

#### **9.6.5. Egyéb felek felelőssége és helytállása**

371) Nincs kikötés.

### **9.7. Helytállás érvénytelenségi köre**

372) A helytállás érvénytelenségi körét a {D5} BSZ-DÁP-TAN szolgáltatási szabályzatban meg kell határozni.

### **9.8. Felelősség korlátozása**

373) A Szolgáltató a {D5} BSZ-DÁP-TAN-ban foglaltak szerint korlátozhatja a kártérítési felelősségét.

### **9.9. Kártérítések**

374) A kártérítésekről a {D5} BSZ-DÁP-TAN szolgáltatási szabályzatban kell rendelkezni.

## **9.10. Hatályosság és megszűnés**

### **9.10.1. Hatályosság**

#### **9.10.1.1. Időbeli hatály**

375) A bizalmi szolgáltatási rend egy adott verziójának időbeli hatálya a címlapon feltüntetett hatálybalépés dátumával kezdődik és határozatlan időre szól. Az időbeli hatály megszűnik a bizalmi szolgáltatási rend újabb verziójának hatályba lépésével vagy a Szolgáltatások befejezésekor.

#### **9.10.1.2. Tárgyi hatály**

376) A bizalmi szolgáltatási rend tárgyi hatálya kiterjed a Szolgáltatások nyújtására és igénybe vételére.

#### **9.10.1.3. Személyi hatály**

377) A bizalmi szolgáltatási rend személyi hatálya kiterjed a Szolgáltatónak, illetve a Közreműködő Feleknek a Szolgáltatások nyújtásában közreműködő munkatársaira és az Alírókra.

### **9.10.2. Megszűnés**

378) A bizalmi szolgáltatási rend a Szolgáltató szolgáltatási tevékenységének befejezésével tekintendő megszűntnek.

### **9.10.3. Megszűnés után is hatályban maradó rendelkezések**

379) A megszűnés után is hatályban maradó rendelkezéseket a {D5} BSZ-DÁP-TAN szolgáltatási szabályzatban meg kell határozni.

## **9.11. Egyéni hirdetések és kommunikáció a résztvevőkkel**

380) A {D5} BSZ-DÁP-TAN szolgáltatási szabályzatban rendelkezni kell a felek és résztvevők közötti kommunikáció joghatást kiváltó módjairól.

## **9.12. Módosítások**

### **9.12.1. Módosítás eljárása**

381) A bizalmi szolgáltatási rend módosítása az 1.5.3 és 1.5.4 fejezetekben leírt szabályok szerint történik. A bizalmi szolgáltatási rend módosulását a verziószám megfelelő változása jelzi.

### **9.12.2. Értesítés módszere és időtartama**

382) A Szolgáltatások jelentős vagy lényeges változása esetén a Szolgáltatónak internetes honlapján közleményt kell közzé tennie, a hatályba lépést megelőzően kellő időben ahhoz, hogy az érintett felek a változásokra felkészülhessenek.

### **9.12.3. OID megváltozását előidéző körülmények**

383) A bizalmi szolgáltatási rend OID-ja nem változik.

## **9.13. Vitás kérdések rendezése**

384) A {D5} BSZ-DÁP-TAN szolgáltatási szabályzat tartalmazza.

## **9.14. Irányadó jog**

385) A Szolgáltató szerződéseire, szabályzataira és azok teljesítésére a magyar jog az irányadó és azokat a magyar jog szerint kell értelmezni.

## **9.15. Hatályos jognak megfelelés**

386) A Szolgáltató tevékenységét a mindenkor hatályos Európai Unió, illetve magyar jogszabályoknak megfelelően köteles végezni.

## **9.16. Vegyes rendelkezések**

### **9.16.1. Teljességi záradék**

387) Nincs kikötés.

### **9.16.2. Átruházás**

388) Nincs kikötés.

### **9.16.3. Részleges érvénytelenség**

389) A jelen bizalmi szolgáltatási rend egyes rendelkezéseinek tetszőleges okból történő érvénytelenné válása esetén a többi rendelkezés változatlan formában érvényben marad.

#### **9.16.4. Igényérvényesítés**

390) A {D5} BSZ-DÁP-TAN szolgáltatási szabályzat tartalmazza.

#### **9.16.5. Force Majeure (Vis maior)**

391) A {D5} BSZ-DÁP-TAN szolgáltatási szabályzat tartalmazza.

### **9.17. Egyéb rendelkezések**

#### **9.17.1. Hozzáférhetőség a fogyatékossgal élő személyek számára**

392) A Szolgáltatásokat és a Szolgáltatások során alkalmazott végfelhasználó termékeket hozzáférhetővé kell tenni a fogyatékossgal élő személyek számára, amennyiben az lehetséges.