



**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)**

Verziószám: 1.8
OID: 0.2.216.1.200.1100.100.42.3.1.39
Hatályba lépés dátuma: 2026.08.13.
Dokumentum besorolása: NYILVÁNOS

Jóváhagyó	Adorján István

Változáskövetés

verzió	dátum	a változás leírása	készítette	ellenőrizte	jóváhagyta
0.1	2024.07.17	első változat	NISZ Zrt. Polysys Kft. ACPM Zrt.	Kővári-Szabó Zoltán Németvári Tibor Nagy Benjámin	-
0.2	2024.07.24	elsődleges észrevételeket beépítő, a DÁP-TAN szolgáltatásba tartozó részeket elhagyó változat	ACPM Zrt.	Kővári-Szabó Zoltán Németvári Tibor Nagy Benjámin	-
0.3	2024.07.30	Felügyeleti szervnek benyújtott előzetes változat	ACPM Zrt.	Kővári-Szabó Zoltán Nagy Benjámin	-
0.4	2024.11.05.	Továbbfejlesztett változat	ACPM Zrt. Kővári-Szabó Zoltán	Nagy Benjámin Polysys Kft.	-
0.5	2024.11.28.	További pontosítások, javítások	Kővári-Szabó Zoltán	Nagy Benjámin ACPM Zrt.	-
1.0	2024.11.29	Első jóváhagyott verzió	Kővári-Szabó Zoltán	Nagy Benjámin ACPM Zrt. DÁP szolgáltató	Adorján István
1.1	2024.12.13	Megfelelőségértékelés észrevételeinek alkalmazása	Kővári-Szabó Zoltán	Nagy Benjámin	Adorján István
1.2	2024.12.17	Aláírási formátum pontosítása, hatálybalépés dátumának módosítása.	Kővári-Szabó Zoltán	Nagy Benjámin	Adorján István
1.3	2025.01.24	- Aktivizáló adat rontott bevitelére vonatkozó korlátozás követelményével való kiegészítés - 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. - Elütések javítása.	Kővári-Szabó Zoltán	Nagy Benjámin	Adorján István
1.4	2025.02.03	A Bizalmi felügyelet észrevételei alapján további pontosítások	Gál Ferenc Nagy Benjámin	Kővári-Szabó Zoltán	Adorján István
1.5	2025.11.11	Integrált eAláírás szolgáltatás bevezetésével kapcsolatos módosítások Kapcsolódó pontosítások és egyéb javítások	Kővári-Szabó Zoltán	Buczynskiné dr. Szabó Zsuzsanna Nagy Benjámin DÁP Szolgáltató	Adorján István
1.6	2026.04.24	- kiberbiztonsági felügyelet változása - akadálymentes sablon használata	Buczynskiné dr. Szabó Zsuzsanna	Kővári-Szabó Zoltán Gál Ferenc	Adorján István
1.7	2026.05.15.	kapcsolati adatok módosítása	Buczynskiné dr. Szabó Zsuzsanna	Kővári-Szabó Zoltán	Adorján István
1.8	2026.07.10	Felülvizsgálat	Polysys Kft.	Buczynskiné dr. Szabó Zsuzsanna; Kővári-Szabó Zoltán	Adorján István

Tartalomjegyzék

1.	BEVEZETÉS.....	9
1.1.	Áttekintés.....	9
1.2.	Dokumentum neve és azonosítása.....	10
1.2.1.	A dokumentum neve.....	10
1.2.2.	A dokumentum azonosítása.....	10
1.2.3.	Hitelesítési rendek.....	10
1.3.	PKI közösség.....	10
1.3.1.	Hitelesítő szervezet.....	10
1.3.2.	Közreműködő felek.....	11
1.3.3.	Előfizetők.....	11
1.3.4.	Érintett Felek.....	12
1.3.5.	Egyéb felek.....	12
1.4.	A szolgáltatás alkalmazhatósága.....	12
1.4.1.	Engedélyezett használat.....	13
1.4.2.	Tiltott használat.....	13
1.5.	Szabályzat adminisztráció.....	13
1.5.1.	Szabályzatot karbantartó szerv.....	13
1.5.2.	Kapcsolat.....	13
1.5.3.	A szabályzat alkalmasságának meghatározása.....	13
1.5.4.	A szabályzat jóváhagyásának eljárása.....	13
1.6.	Fogalmak, rövidítések és hivatkozások.....	14
1.6.1.	Fogalmak.....	14
1.6.2.	Rövidítések.....	18
	Rövidítés.....	18
	Angol megfelelő.....	18
	Megnevezés.....	18
1.6.3.	Hivatkozások.....	20
2.	KÖZZÉTÉTEL ÉS ADATTÁRAK.....	22
2.1.	Adattárak.....	22
2.2.	Szolgáltatói információ közzététele.....	22
2.3.	A közzététel gyakorisága.....	22
2.4.	Hozzáférés-ellenőrzések.....	22
3.	AZONOSÍTÁS ÉS HITELESÍTÉS.....	22
3.1.	Az azonosítás és hitelesítés biztonsági szintje.....	23
3.2.	Az Aláírók felhasználóazonosítása.....	23

4.	A SZOLGÁLTATÁS ÉLETCIKLUSA.....	23
4.1.	A Szolgáltatás igénylése	23
4.2.	A Szolgáltatás használatba vétele	23
4.3.	A Szolgáltatás elérhetősége és rendelkezésre állása	23
4.4.	A Szolgáltatás használata	24
4.5.	Előfizetés vége	25
5.	FIZIKAI, ELJÁRÁSBELI ÉS SZEMÉLYZETI BIZTONSÁGI ÓVINTÉZKEDÉSEK	25
5.1.	Fizikai óvintézkedések	26
5.1.1.	Telephelyek elhelyezése és szerkezeti felépítése	26
5.1.2.	Fizikai hozzáférés	26
5.1.3.	Áramellátás és légkondicionálás	26
5.1.4.	Beázás és elárasztás veszélyeztetettség.....	27
5.1.5.	Tűz megelőzés és tűzvédelem	27
5.1.6.	Adathordozók tárolása	27
5.1.7.	Selejt kezelése és megsemmisítése	27
5.1.8.	Fizikailag elkülönítetten őrzött mentési példányok	27
5.2.	Eljárásbeli előírások	27
5.2.1.	Bizalmi munkakörök	27
5.2.2.	Az egyes feladatokhoz szükséges személyzeti létszámok	28
5.2.3.	Bizalmi munkakörökben elvárt azonosítás és hitelesítés	28
5.2.4.	Egymást kizáró munkakörök	29
5.3.	Személyzetre vonatkozó előírások	29
5.3.1.	Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények	29
5.3.2.	Biztonsági háttér ellenőrzés eljárásai	29
5.3.3.	Képzési követelmények	30
5.3.4.	Továbbképzési gyakoriságok és követelmények	30
5.3.5.	Munkabeosztás körforgásának gyakorisága és sorrendje	31
5.3.6.	Felhatalmazás nélküli tevékenységek büntető következményei	31
5.3.7.	Szerződéses munkavállalókra vonatkozó követelmények	31
5.3.8.	A személyzet számára biztosított dokumentációk	31
5.4.	A biztonsági naplózás folyamatai	31
5.4.1.	Naplózott esemény típusok	31
5.4.2.	Naplóállomány feldolgozásának gyakorisága	32
5.4.3.	Naplóállomány megőrzési időtartama	32
5.4.4.	Naplóállomány védelme	32
5.4.5.	Naplóállomány mentési folyamatai	32
5.4.6.	Naplózás gyűjtési rendszere	32

5.4.7.	Rendellenes eseményeket kiváltó alanyok értesítése	32
5.4.8.	Sebezhetőség értékelések.....	33
5.5.	Adatok archiválása.....	33
5.5.1.	A tárolt adatok típusai	33
5.5.2.	Archívum megőrzési időtartama.....	33
5.5.3.	Archívum védelme	34
5.5.4.	Archívum mentési eljárásai	34
5.5.5.	Az adatok időbélyegzésére vonatkozó követelmények	34
5.5.6.	Archívum gyűjtési rendszere	34
5.5.7.	Archívum hozzáférés és ellenőrzés eljárásai	34
5.6.	Kulcsátállítás.....	34
5.7.	Helyreállítás rendkívüli üzemeltetési helyzetek esetén	35
5.7.1.	Rendkívüli események és kompromittálódás kezelésének eljárásai.....	35
5.7.2.	Sérült számítási erőforrások, szoftverek és/vagy adatok	35
5.7.3.	Magánkulcs kompromittálódása esetén követendő eljárás.....	35
5.7.4.	Üzletmenet folytonosság helyreállítás katasztrófát követően	36
5.8.	A szolgáltatási tevékenység megszüntetése	36
6.	MŰSZAKI BIZTONSÁGI ÓVINTÉZKEDÉSEK	37
6.1.	Kulcspár előállítás és telepítés	37
6.1.1.	Kulcspár előállítás	37
6.1.2.	Magánkulcs eljuttatása a tulajdonoshoz	37
6.1.3.	Nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz	37
6.1.4.	A szolgáltatói nyilvános kulcs közzététele	37
6.1.5.	Kulcsméretek	37
6.1.6.	A nyilvános kulcs paraméterek előállítása és megfelelőségének ellenőrzése	38
6.1.7.	A kulcshasználat célja (X.509 v3 kulcs használati mezőnek megfelelően).....	38
6.2.	Magánkulcs védelme és kriptográfiai modul műszaki szabályozások.....	38
6.2.1.	Kriptográfiai modul szabványok és szabályozások.....	38
6.2.2.	Több szereplős ("n-ből m") ellenőrzés	39
6.2.3.	Magánkulcs letét.....	39
6.2.4.	Magánkulcs visszaállítása	39
6.2.5.	Magánkulcs mentése.....	39
6.2.6.	Magánkulcs bejuttatása a kriptográfiai modulba	39
6.2.7.	Magánkulcs kriptográfiai modulban történő tárolásának módja.....	39
6.2.8.	Magánkulcs aktiválásának módja.....	39
6.2.9.	Magánkulcs aktív állapotának megszüntetési módja	40
6.2.10.	Magánkulcs megsemmisítésének módja	40

6.2.11.	Kriptográfiai modul értékelése	40
6.3.	Kulcspár gondozás egyéb szempontjai	40
6.3.1.	Nyilvános kulcs archiválása	40
6.3.2.	Tanúsítvány érvényességi időszaka és kulcspár felhasználás időtartama	40
6.4.	Aktivizáló adatok	40
6.4.1.	Aktivizáló adatok előállítása	40
6.4.2.	Aktivizáló adatok védelme	41
6.4.3.	Aktivizáló adatok egyéb szempontjai	41
6.5.	Informatikai biztonsági óvintézkedések	41
6.5.1.	Informatikai biztonsági műszaki követelmények meghatározása	41
6.5.2.	Informatikai biztonsági értékelés	41
6.6.	Életciklusra vonatkozó műszaki óvintézkedések	41
6.6.1.	Rendszerfejlesztési óvintézkedések	41
6.6.2.	Biztonságkezelési óvintézkedések	42
6.6.3.	Életciklus biztonsági óvintézkedések	42
6.7.	Hálózatbiztonsági óvintézkedések	42
6.8.	Időforrások	42
7.	TANÚSÍTVÁNY, CRL ÉS OCSP PROFILOK	42
7.1.	Tanúsítvány profil	42
7.2.	CRL profil	42
7.3.	OCSP profil	42
8.	MEGFELELŐSÉG VIZSGÁLAT ÉS EGYÉB ÉRTÉKELÉSEK	43
8.1.	Vizsgálatok gyakorisága és körülményei	43
8.2.	Auditor azonosítása és képesítése	43
8.3.	Auditor függetlensége	43
8.4.	Audit során vizsgált területek	43
8.5.	Hiányosságok esetén végrehajtandó tevékenységek	44
8.6.	Eredmény kommunikációja	44
9.	EGYÉB ÜZLETI ÉS JOGI KÉRDÉSEK	45
9.1.	Díjak	45
9.2.	Anyagi felelősség	45
9.2.1.	Biztosítási fedezet	45
9.2.2.	További követelmények	45
9.2.3.	Felelősségbiztosítás vagy garancia végfelhasználók számára	45
9.3.	Üzleti információk bizalmassága	45
9.3.1.	Bizalmasan kezelendő információk köre	45
9.3.2.	Bizalmasnak nem tekintett információk köre	46

9.3.3.	Bizalmas információk védelmének felelőssége	46
9.4.	Személyes adatok védelme	46
9.4.1.	Adatvédelem	46
9.4.2.	Bizalmasként kezelendő személyes adatok.....	46
9.4.3.	Bizalmasként nem kezelendő személyes adatok	46
9.4.4.	Személyes adatok védelmének felelőssége	46
9.4.5.	Személyes adatok felhasználásának elfogadása	46
9.4.6.	Felfedés hatósági vagy polgári peres eljárás keretében.....	46
9.4.7.	Egyéb, felfedést eredményező körülmények.....	47
9.5.	Szellemi tulajdonjogok	47
9.6.	Tevékenységet viselt felelősség és helytállás	47
9.6.1.	Szolgáltató felelőssége és helytállása	47
9.6.2.	A regisztrációs szervezet felelőssége.....	48
9.6.3.	Aláíró felelőssége és helytállása.....	48
9.6.4.	Érintett Felek felelőssége és helytállása	48
9.6.5.	Egyéb felek felelőssége és helytállása	48
9.7.	Helytállás érvénytelenségi köre	49
9.8.	Felelősség korlátozása	49
9.9.	Kártérítések	49
9.10.	Hatályosság és megszűnés	49
9.10.1.	Hatályosság.....	49
9.10.2.	Megszűnés.....	50
9.10.3.	Megszűnés után is hatályban maradó rendelkezések	50
9.11.	Egyéni hirdetmények és kommunikáció a résztvevőkkel.....	50
9.12.	Módosítások.....	50
9.12.1.	Módosítás eljárása	50
9.12.2.	Értesítés módszere és időtartama.....	50
9.12.3.	OID megváltozását előidéző körülmények	50
9.13.	Vitás kérdések rendezése.....	50
9.14.	Irányadó jog	51
9.15.	Hatályos jognak megfelelés	51
9.16.	Vegyes rendelkezések	51
9.16.1.	Teljességi záradék	51
9.16.2.	Átruházás	51
9.16.3.	Részleges érvénytelenség.....	51
9.16.4.	Igényérvényesítés	51
9.16.5.	Force Majeure (Vis maior)	51

9.17.	Egyéb rendelkezések	52
9.17.1.	Hozzáférhetőség a fogyatékossgal élő személyek számára	52

1. BEVEZETÉS

- (1.) Jelen dokumentum a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. (a továbbiakban, mint Kormányzati Hitelesítés Szolgáltató vagy Szolgáltató) Bizalmi Szolgáltatási Szabályzata, amely a Digitális Állampolgárság Program keretében megvalósított, a {J2} DÁP tv. 52. § (1) bekezdés b) pontja szerinti eAláírás keretszolgáltatáshoz szükséges minősített bizalmi szolgáltatás nyújtására és igénybevételére vonatkozik, melyet Szolgáltató a {J3} 320/2024. Korm. rend. 2. § (2) bekezdés alapján nyújt.
- (2.) A Szolgáltató a fenti tárgykörben a {D9} BSZ-DÁP-TAN szolgáltatási szabályzatban meghatározott szolgáltatás keretében kibocsátott minősített tanúsítványokhoz kapcsolódóan, jelen szabályzat keretében az alábbi szolgáltatást nyújtja:

A Digitális Állampolgárság Program (DÁP) keretében távoli elektronikus aláírás létrehozó eszköz kezelése és elektronikus aláírások létrehozása (a továbbiakban: DÁP-TK szolgáltatás vagy Szolgáltatás).
- (3.) A DÁP-TK szolgáltatás a {D9} BSZ-DÁP-TAN szolgáltatási szabályzatban meghatározott DÁP-TAN szolgáltatás kiegészítő szolgáltatása, mely a {J1} eIDAS 3. cikk 16. pont c) és f) alpontjában megfogalmazott, alábbi minősített bizalmi szolgáltatásoknak felel meg:
 - a) elektronikus aláírások létrehozása;
 - b) távoli elektronikus aláírás létrehozó eszköz kezelése.
- (4.) Jelen dokumentum a DÁP-TK szolgáltatás eljárásrendi és működési szabályait tartalmazza.
- (5.) A Szolgáltató a Szolgáltatásait a vele szerződéses viszonyban álló állampolgárok (a továbbiakban: Aláírók) részére nyújtja.

1.1. Áttekintés

- (6.) A szolgáltatási szabályzat célja, hogy összefoglalja mindazokat az információkat, melyeket a Szolgáltató DÁP-TK szolgáltatással kapcsolatba kerülő feleknek ismerni szükséges vagy érdemes. Biztosítja a Szolgáltató működésének átláthatóságát és annak megítélését a Szolgáltatásokat igénybe vevők számára, hogy az ismertetett szolgáltatási gyakorlat és tárolt magánkulcsok mennyiben felelnek meg az elvárásaiknak.
- (7.) Jelen bizalmi szolgáltatási szabályzat az alábbi bizalmi szolgáltatási rend hatálya alá tartozó Szolgáltatásra vonatkozik:

"Bizalmi Szolgáltatási Rend a Digitális Állampolgárság Program keretében nyújtott távoli elektronikus aláírás létrehozó eszköz kezelése és elektronikus aláírások létrehozása - minősített bizalmi szolgáltatáshoz"; OID: 0.2.216.1.200.1100.100.42.3.1.37 (BR-DÁP-TK).
- (8.) Jelen bizalmi szolgáltatási szabályzat az {Sz8} RFC 3647 nemzetközi ajánlás alapján készült, felépítésében és tartalmában – a szükséges, Szolgáltatóra és DÁP-TK szolgáltatásra specifikus eltérésektől eltekintve – szigorúan követi annak előírásait. Az ott meghatározott felépítés szigorú megtartása érdekében azok az ajánlás által meghatározott fejezetek is szerepelnek a dokumentumban, melyeknél jelen BSZ-DÁP-TK kereteiben nincs követelmény előírva; ezekben a fejezetekben a "Nincs kikötés" szöveg szerepel.
- (9.) Szolgáltató a jelen bizalmi szolgáltatási szabályzathoz kapcsolódó szolgáltatásait a Bizalmi Felügyeletnek 2024.07.31-én jelentette be. A Bizalmi Felügyelet erre vonatkozó nyilvántartásának elérhetősége: <https://esign.nmhh.hu/>

1.2. Dokumentum neve és azonosítása

1.2.1. A dokumentum neve

- (10.) Jelen szolgáltatási szabályzat teljes neve: „Bizalmi Szolgáltatási Szabályzat a Digitális Állampolgárság Program keretében nyújtott elektronikus aláírások létrehozása és távoli elektronikus aláírás létrehozó eszköz kezelése minősített bizalmi szolgáltatásokhoz”.
- (11.) A bizalmi szolgáltatási szabályzat rövid neve: BSZ-DÁP-TK.
- (12.) A BSZ-DÁP-TK objektum azonosítója és verziószáma a címlapon található.
- (13.) Jelen BSZ-DÁP-TK tartalmazza a {D10} BR-DÁP-TK bizalmi szolgáltatási rend hatálya alatt tárolt magán kulcsok generálására, tárolására és felhasználására vonatkozó részletes szabályokat.
- (14.) Jelen BSZ-DÁP-TK hatályba lépését és hatályának megszűnését a 9.10 fejezet tartalmazza.
- (15.) Jelen BSZ-DÁP-TK-nak csak a Szolgáltató elektronikus bélyegzőjével vagy a Szolgáltatásokért felelős vezető elektronikus aláírásával ellátott változata tekinthető hitelesnek.

1.2.2. A dokumentum azonosítása

- (16.) A BSZ-DÁP-TK a DÁP tv. 8. § 43. pontja szerinti *szolgáltatási szabályzat*, mely a DÁP-TK szolgáltatás eljárásrendi és működési szabályait tartalmazza és amely egyúttal az {Sz1} EN 319 401 szerinti ún. „*trust service practice statement*”-nek és az {Sz3} TS 119 431-1 4.3.1 pontja szerinti ún. „*SSAS practice statement*”-nek tekintendő.

1.2.3. Hitelesítési rendek

- (17.) A {D10} BR-DÁP-TK bizalmi szolgáltatási rend megfelel az {Sz3} TS 119 431-1 szabvány 4.3.2 fejezetében és A.2 mellékletében definiált EUSPv2 (OID: 0.4.0.19431.1.1.4) hitelesítési rendnek (EUSPv2: EU SSAS Policy).

1.3. PKI közösség

- (18.) Jelen bizalmi szolgáltatási szabályzatban szereplő PKI közösség az alábbi felekből áll:
- a) **Szolgáltató:** a jelen BSZ-DÁP-TK-nak megfelelő minősített bizalmi szolgáltató, amely a magánkulcsok tárolásával és aktiválásával kapcsolatos műszaki tevékenységeket végzi;
 - b) **Közreműködő Felek:** a Szolgáltatóval közvetlenül vagy a DÁP szolgáltatón keresztül (DÁP Integrált eAláírás keretében) szerződéses kapcsolatban álló vagy jogszabályban meghatározott, a Szolgáltatások nyújtásában közreműködő felek;
 - c) **Előfizetők (Aláírók):** a Szolgáltató által tárolt magánkulcsok távoli aktiválásával elektronikus aláírást létrehozó állampolgárok;
 - d) **Érintett Felek:** a távoli aktiválással létrehozott elektronikus aláírásokat fogadó harmadik felek.
- (19.) Azon tevékenységek vonatkozásában, melyeket a Szolgáltató nem maga lát el, Szolgáltató teljes körű felelősséget vállal azért, hogy a Közreműködő Fél tevékenysége során jelen szabályzatban foglalt követelmények teljesülnek.

1.3.1. Hitelesítő szervezet

- (20.) A hitelesítő szervezet a Szolgáltató központi szervezete, amely a hitelesítő központokból, a szolgáltatás-támogató informatikai rendszerek erőforrásaiból, az ezt körül vevő biztonságos fizikai környezetből, valamint az üzemeltető és szolgáltatást ellátó személyzetből áll. Jelen szolgáltatási szabályzat szempontjából feladatai közé tartozik az Aláírók magánkulcsának tárolása, a távoli elektronikus aláírás létrehozó eszköz kezelése és elektronikus aláírások létrehozása.

1.3.1.1. Szerver oldali aláíró alkalmazás szolgáltató

(21.) A szerver oldali aláíró alkalmazás szolgáltató (SSASP) a Szolgáltató által megvalósított bizalmi szolgáltatások azon szolgáltatói komponense, mely a más szolgáltatás komponensek által generált magánkulcsok aktiválásával az Aláírók nevében történő elektronikus aláírások létrehozása során elvégzi az Aláírás Értéket kiszámító Kriptográfiai Műveletet.

1.3.1.2. Szabályozási Csoport

(22.) 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.

1.3.1.3. Telefonos Ügyfélszolgálat

(23.) Szolgáltató Telefonos Ügyfélszolgálatot (Kormányzati Ügyfélvonal - 1818) tart fenn, melynek révén heti hét napban, napi 24 órában biztosítja az Aláírók számára a Szolgáltatással kapcsolatos ügyfélszolgálatot.

(24.) Szolgáltató – a Telefonos Ügyfélszolgálat (Kormányzati Ügyfélvonal – 1818) kivételével – az állampolgárokkal közvetlen kapcsolatot nem tart, Aláírók a DÁP keretalkalmazáson keresztül vehetik igénybe a Szolgáltatást.

1.3.2. Közreműködő felek

1.3.2.1. DÁP szolgáltató

(25.) A DÁP szolgáltató olyan külső közreműködő fél, mely a Szolgáltató számára elvégzi a Delegált Autentikációt, vagyis az Aláírók felhasználóazonosítását, igazolja az Aláíró aláírási szándékát és az általa aláírni kívánt adatokat, majd közvetlenül vagy az Aláíró partneren keresztül a Szolgáltatásban kiszámított Aláírás Értéket szabványos formátumú elektronikus aláírásba foglalja és visszaadja az Aláírónak.

1.3.2.2. Aláíró partnerek

(26.) A DÁP eAláírás keretszolgáltatáshoz a DÁP szolgáltató {D12} csatlakozási szabályzata szerint csatlakozott, a DÁP szolgáltatóval jogviszonyban álló szervezetek, melyek a DÁP Integrált eAláírás szolgáltatás keretében aláíró alkalmazást (Signature Creation Application – SCA) üzemeltetnek a DÁP eAláírás szolgáltatáshoz integrált módon. Az Aláíró partnerek dokumentumok aláírására kérhetik fel az Aláírókat, mely esetben az aláírandó dokumentum előkészítését és lenyomatának DÁP szolgáltatóhoz való eljuttatását, majd a Szolgáltatásban kiszámított Aláírás Érték szabványos formátumú elektronikus aláírásba foglalását az Aláíró partner Aláíró alkalmazása végzi. Az Aláíró partnerek a Szolgáltató felé – a DÁP szolgáltatón keresztül – független auditjelentéssel igazolják a {D12} csatlakozási szabályzat biztonsági követelményeinek való megfelelést.

1.3.3. Előfizetők

(27.) A DÁP-TK szolgáltatás előfizetői Magyarország azon állampolgárai, akik a Szolgáltató által tárolt magánkulcsuk távoli aktiválásával a DÁP keretalkalmazás elektronikus aláírás funkcióját használni kívánják és ezt megelőzően az {D1} ÁSZF-DÁP elfogadásával Szolgáltatási Szerződést kötnek a Szolgáltatóval a DÁP-TAN és DÁP-TK szolgáltatások igénybe vételére. Mivel az Aláíró a {D9} BSZ-DÁP-TAN-ban foglaltaknak megfelelően csak a saját nevére szóló tanúsítványt igényelhet, így jelen dokumentum fogalomrendszerében az Előfizető és az Aláíró személye azonos.

- (28.) Jelen bizalmi szolgáltatási szabályzat hatálya alatt a Szolgáltató kizárólag a Digitális Állampolgárság Program keretében, Magyarország azon állampolgárai, mint Aláírók részére biztosít szolgáltatást, akik megfelelnek a {D9} BSZ-DÁP-TAN 4.1.1 pontjában foglaltaknak.
- (29.) Kizárólag az Aláíró aktivizálhatja saját magánkulcsát a Szolgáltató által felügyelt minősített elektronikus aláírás létrehozó eszközön.
- (30.) Az Aláíró felelősségét és kötelezettségeit a 9.6.3 fejezet írja le.

1.3.4. Érintett Felek

- (31.) Érintett Fél: a Szolgáltatásban tárolt magánkulcs távoli aktiválásával létrehozott elektronikus aláírással ellátott elektronikus dokumentumot fogadó természetes vagy jogi személy, aki/amely az elektronikus aláírásra hagyatkozva jár el a dokumentum hitelességének ellenőrzésekor. Az Érintett Fél nem áll szerződéses viszonyban a Szolgáltatóval.
- (32.) Az Érintett Félnek az elektronikus aláírás ellenőrzéséhez, a tanúsítvány érvényességének megállapításához minden esetben javasolt a Szolgáltató DÁP-TAN szolgáltatása keretében nyújtott visszavonási információ (OCSP) használata.
- (33.) Az Érintett Felek felelősségét a 9.6.4 fejezet írja le.

1.3.5. Egyéb felek

1.3.5.1. Bizalmi Felügyelet

- (34.) A jogszabályokban megjelölt Bizalmi Felügyelet biztosítja a bizalmi szolgáltatásokra vonatkozó jogszabályok felügyeletét, ellenőrzi a Szolgáltatások jogszabályi megfelelőségét, ellátja az ezzel kapcsolatos felügyeleti feladatokat; figyelemmel kíséri az elektronikus aláírásokkal kapcsolatos technológiai és kriptográfiai algoritmusok fejlődését; határozatában elrendelheti a Szolgáltatás felfüggesztését.

1.3.5.2. Kiberbiztonsági Felügyelet

- (35.) A {J8} Kiberbiztonsági törvény hatálya alá tartozó információs rendszerek felügyeletét ellátó hatóság, amely a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. Esetében a Nemzeti Kibervédelmi Intézet (NKI). 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 szolgáltatás alkalmazhatósága

- (36.) A Szolgáltatás önállóan nem vehető igénybe, csak a BSZ-DÁP-TAN bizalmi szolgáltatási szabályzatban leírt tanúsítvány kibocsátási szolgáltatáshoz integrált módon, a DÁP keretalkalmazáson keresztül.
- (37.) Az elektronikus aláírás létrehozásának folyamata során az Aláíró a Szolgáltatást távoli minősített elektronikus aláírás létrehozó eszközként használja a hitelesítendő dokumentum(ok) lenyomatának a magánkulccsal történő titkosításával előállított Aláírás Érték kiszámítására, majd ezen érték szabványos formátumú elektronikus aláírásba foglalására.
- (38.) A Szolgáltatás PAdES formátumú minősített elektronikus aláírások létrehozását támogatja. Az aláírás szintje:
- a) DÁP integrált eAláírás szolgáltatás esetén: az aláírási kérést indító Aláíró partner által meghatározva, de

minimum PAdES-B-T szint

- b) Aláíró partner közreműködése nélkül: PAdES-B-LT

1.4.1. Engedélyezett használat

- (39.) A Szolgáltatás keretében tárolt magánkulcsok kizárólag a Digitális Állampolgárság Keretében kibocsátott tanúsítványon alapuló elektronikus aláírás létrehozására használhatók.
- (40.) A Szolgáltatás keretében az Aláírók kizárólag saját nevükben és magánszemélyként hozhatnak létre elektronikus aláírást. A Digitális Állampolgárság Program keretében kibocsátott tanúsítványban az Aláírók névtelensége és álnév használata nem megengedett.

1.4.2. Tiltott használat

- (41.) Tilos a tárolt magánkulcsot felhasználni titkosítás visszafejtésére, azonosításra, más tanúsítványok aláírására vagy bármilyen bizalmi szolgáltatás nyújtásához.
- (42.) A Digitális Állampolgárság Program keretében kiadott tanúsítványhoz kapcsolódó magánkulcsot Aláíró egyedül magánszemélyként használhatja fel; ezek használata bármilyen üzleti, munkahelyi vagy egyéb szakmai tevékenység céljából nem megengedett.

1.5. Szabályzat adminisztráció

1.5.1. Szabályzatot karbantartó szerv

- (43.) A Szolgáltató szervezetén belül Szabályozási Csoportot működtet, amely többek között jelen bizalmi szolgáltatási szabályzat karbantartásáért is felelős.

1.5.2. Kapcsolat

- (44.) A Szolgáltató hatályos adatai (cégjegyzékszám, székhely, levelezési cím stb.), az illetékes fogyasztóvédelmi felügyelőség, valamint az illetékes békéltető testület elérhetősége a hiteles.gov.hu/kapcsolat menüpont alatt elérhető.

1.5.3. A szabályzat alkalmasságának meghatározása

- (45.) A Szolgáltató legalább évente egyszer felülvizsgálja a bizalmi szolgáltatási rend, illetve a bizalmi szolgáltatási szabályzat, illetve egyéb szabályzatai tartalmi és formai megfelelőségét a vonatkozó jogszabályok, előírások és műszaki szabványok tekintetében, és ennek eredményeit, megfelelő módosításokkal, alkalmazza az érintett dokumentumokban.
- (46.) Amennyiben a változtatási igények befolyásolhatják a Szolgáltatásnak az Előfizetők vagy Érintett Felek általi elfogadását, a Szolgáltató erről előzetes értesítést tesz közzé a Szolgáltatások internetes honlapján.

1.5.4. A szabályzat jóváhagyásának eljárása

- (47.) Az ellenőrzésre, illetve jóváhagyásra a Szolgáltató belső szervezete, illetve a Szolgáltatásokért felelős vezetője rendelkezik hatáskörrel és felelősséggel.
- (48.) A jóváhagyás előtt a Szolgáltató megvizsgálja a szolgáltatási szabályzat bizalmi szolgáltatási rendnek való megfelelését.

- (49.) A szolgáltatási szabályzat új verzióját a Szolgáltató a hatályba lépést megelőzően legalább 30 nappal előzetesen bejelenti a Bizalmi Felügyelet részére. A szolgáltatási szabályzat jogszabályoknak való megfelelését a Bizalmi Felügyelet is ellenőrzi.
- (50.) A jóváhagyott szolgáltatási szabályzat a Szolgáltató elektronikus bélyegzőjével vagy a Szolgáltatásokért felelős vezető elektronikus aláírásával kerül hitelesítésre.
- (51.) A jóváhagyott szolgáltatási szabályzatot a Szolgáltató vezetése lépteti hatályba. A hatályba lépés napját a dokumentum címlapja tartalmazza.
- (52.) A szolgáltatási szabályzat új verziója mindig új verziószámmal kerül nyilvánosságra és egy munkanapon belül közzétételre a Szolgáltatás internetes honlapján.
- (53.) Az új verzió kötelező érvényű az összes Aláíróra, valamint az összes, az új verzió hatálybalépése utáni kulcshasználatra, illetve az így kibocsátott tanúsítványokra.

1.6. Fogalmak, rövidítések és hivatkozások

1.6.1. Fogalmak

- alany:** A Szolgáltató DÁP-TAN szolgáltatásában kiadott tanúsítványban azonosított entitás, aki a tanúsítványban szereplő nyilvános kulcsnak (elektronikus aláírás érvényesítési adat) megfelelő magánkulcsot (elektronikus aláírás létrehozásához használt adat) birtokolja. Jelen bizalmi szolgáltatási szabályzat szerint az Alany az Aláíró (állampolgár).
- Aláírás Érték:** Az Aláíró által a DÁP-HSM modulban tárolt magánkulcsának felhasználásával, távolról aktivált és végrehajtott Kriptográfiai Művelet eredménye, azaz az aláírandó dokumentum(ok) lenyomatának a magánkulccsal történő titkosításával előállított digitális jelsorozat. Jelen dokumentum fogalomrendszerében az Aláírás Érték az elektronikus aláírásban elhelyezett aláírás értéket (SignatureValue) jelenti.
- aláírás érvényesítési adat:** olyan egyedi adat, amelyet az elektronikus aláírt dokumentumot megismerő személy (vagy eszköz) az elektronikus aláírás érvényesítésére használ. Jellemzően kriptográfiai nyilvános kulcs, korábbi elnevezése: aláírás-ellenőrző adat.
- aláírás létrehozásához használt adat:** olyan egyedi adat, amelyet az aláíró elektronikus aláírás létrehozásához használ. Jellemzően kriptográfiai magánkulcs (magánkulcs), korábbi elnevezése: aláírás-létrehozó adat.
- aláíró:** elektronikus aláírást létrehozó természetes személy. Jelen bizalmi szolgáltatási szabályzat szerint az Aláíró az állampolgár.
- aláíró alkalmazás:** olyan, Közreműködő által üzemeltetett, a DÁP-TK szolgáltatást közvetlenül megvalósító informatikai rendszer részét nem képező, de azzal együttműködő alkalmazás, mely a DÁP-TK szolgáltatás keretében az Aláíró magánkulcsával létrehozott aláírási érték felhasználásával létrehozza az aláírt dokumentumot.
- 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.
- 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 az e szolgáltatók által nyújtott bizalmi szolgáltatásokra vonatkozó információk. A Bizalmi Lista automatizált feldolgozásra alkalmas, hitelességét elektronikus aláírás vagy elektronikus bélyegző biztosítja.
- bizalmi szolgáltatás:** rendszerint díjazás ellenében nyújtott, az alábbiakból álló szolgáltatások:
 - elektronikus aláírások tanúsítványainak, elektronikus bélyegzők tanúsítványainak, weboldal-hitelesítő tanúsítványoknak vagy egyéb bizalmi szolgáltatások nyújtására vonatkozó tanúsítványoknak a kibocsátása;
 - 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 aláírás 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 szolgáltatási szabályzat szerinti bizalmi szolgáltatás a c) és az f) pont alatti szolgáltatások, azzal, hogy a Szolgáltató jelen BSZ-DÁP-TK keretében kizárólag elektronikus aláírások létrehozását végzi az állampolgárok, mint Aláírók kezdeményezésére.

10. **bizalmi szolgáltató:** egy vagy több bizalmi szolgáltatást nyújtó természetes vagy jogi személy. A bizalmi szolgáltató lehet minősített vagy nem minősített bizalmi szolgáltató.
11. **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.
12. **biztonsági tisztviselő:** a bizalmi szolgáltatás biztonságáért, a biztonsági irányelvek és szabályzatok érvényre juttatásáért általánosan felelős személy.
13. **biztonságos környezet:** olyan fizikai környezet, mely védett illetéktelen hozzáféréstől, és bizonyos mértékig tűz, víz és egyéb katasztrófaeseményektől, egyéb erőszakos behatásoktól.
14. **DÁP-HSM:** a Szolgáltatásban működtetett SCDev, melyet az Aláírók távoli elektronikus aláírás létrehozó eszközként, távolról használnak az Aláírás Érték kiszámítására irányuló Kriptográfiai Művelet elvégzésére.
15. **DÁP Integrált eAláírás szolgáltatás:** Aláíró partnerek üzleti folyamataiba integrált eAláírás keretszolgáltatás, mely esetben a DÁP Szolgáltató {D12} csatlakozási szabályzata szerint csatlakozott Aláíró partnerek aláíró alkalmazásának közreműködésével történik a dokumentumok elektronikus aláírása.
16. **DÁP keretalkalmazás:** a digitális állampolgárság szolgáltatások igénybevétele céljából a nyilvánosság számára mobil eszközökre tervezett és kifejlesztett mobilalkalmazás. A {J2} DÁP tv. ezt keretalkalmazásnak nevezi.
17. **DÁP szolgáltató (eID szolgáltató):** olyan külső közreműködő fél, mely a Szolgáltató számára elvégzi a delegált autentikációt, vagyis az Aláírók felhasználóazonosítását.
18. **delegált autentikáció:** az {Sz5} EN 419 241-1 szabvány lehetővé teszi, hogy a felhasználóazonosítást külső fél végezze és meghatározza az erre vonatkozó műszaki és biztonsági követelményeket. A delegált autentikáció folyamatábráját az {Sz3} TS 119 431-1 szabvány 4.4 fejezete tartalmazza. Szolgáltató a Szolgáltatás biztosítása előtt ellenőrizte, hogy a külső fél maradéktalanul teljesíti a számára meghatározott követelményrendszerben szereplő, a delegált autentikációra vonatkozó valamennyi műszaki és biztonsági követelményt.
19. **digitális állampolgárság:** az állampolgárok azon joga, amellyel digitálisan ügyet intézhetnek, szolgáltatást vehetnek igénybe.
20. **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.
21. **digitális állampolgárság nyilvántartás:** a {J2} DÁP tv. által létrehozott ügyfélregisztrációs nyilvántartás.
22. **elektronikus aláírás:** olyan elektronikus adat, amelyet más elektronikus adatokhoz csatolnak, illetve logikailag hozzárendelnek, és amelyet az aláíró aláírásra használ.
23. **elektronikus aláírás érvényesítési adat:** lásd „aláírás érvényesítési adat”.
24. **elektronikus aláírás létrehozásához használt adat:** lásd „aláírás létrehozásához használt adat”.

25. **elektronikus aláírás tanúsítványa:** olyan elektronikus igazolás, amely az elektronikus aláírás érvényesítési adatokat egy természetes személyhez kapcsolja és igazolja legalább az érintett személy nevét vagy álnévét.
26. **elektronikus aláírás minősített tanúsítványa:** olyan elektronikus aláírás céljára használt tanúsítvány, amelyet minősített bizalmi szolgáltató bocsát ki; és amely megfelel a {J1} eIDAS I. mellékletében megállapított követelményeknek.
27. **elektronikus aláírás érvényesítése:** az elektronikusan aláírt elektronikus dokumentum aláíráskori, illetve ellenőrzéskori 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.
28. **elektronikus aláírás létrehozó eszköz:** elektronikus aláírás létrehozására használt, konfigurált hardver- vagy szoftvereszköz.
29. **elektronikus azonosítás:** a természetes vagy jogi személyt, illetve jogi személyt képviselő természetes személyt egyedileg azonosító, elektronikus személyazonosító adatok felhasználásának folyamata.
30. **elektronikus azonosító eszköz:** olyan fizikai és/vagy nem fizikai egység, amely személyazonosító adatokat tartalmaz, és amelyet online szolgáltatások, vagy adott esetben offline szolgáltatások céljából történő hitelesítésre használnak.
31. **elektronikus azonosítási rendszer:** elektronikus azonosításra alkalmas rendszer, amelynek keretében természetes vagy jogi személy, illetve egy jogi személyt képviselő természetes személy számára elektronikus azonosító eszközöket bocsátanak ki.
32. **elektronikus dokumentum:** elektronikus formában, különösen szöveg, hang-, képi vagy audiovizuális felvétel formájában tárolt bármilyen tartalom.
33. **előfizető:** a természetes személy, aki a Szolgáltatóval érvényes Szolgáltatási Szerződéssel rendelkezik a Szolgáltatások igénybevételére. Jelen bizalmi szolgáltatási szabályzat szerint az Előfizető az Aláíró állampolgár.
34. **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.
35. **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 szolgáltatási szabályzatban: olyan entitás, aki/amely a Szolgáltatások keretében előállított kulcsokat és tanúsítványokat és/vagy időbélyegeket rendeltetésüknek megfelelően használja.
36. **felhasználóazonosítás:** az Aláírók azonosítását elvégző folyamat, amely meg kell feleljen az ezen dokumentumban szereplő biztonsági és műszaki követelményeknek. A felhasználóazonosítás sikeressége előfeltétele az Aláíró DÁP-HSM modulban tárolt magánkulcsa távolról történő aktiválásának, és így az elektronikus aláírás Aláíró által távolról történő létrehozásának.
37. **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)
38. **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.
39. **kriptográfiai kulcs:** olyan kriptográfiai transzformációt vezérlő egyedi jelsorozat, amelynek ismerete a kriptográfiai transzformáció elvégzéséhez, különösen az elektronikus aláírás vagy előállításához, vagy ellenőrzéséhez szükséges.

40. **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.
41. **Kriptográfiai Művelet:** az elektronikus aláírás létrehozásához szükséges, az {Sz9} RFC 6979 szabvány által meghatározott kriptográfiai műveletek összessége, amely kiszámítja az Aláírás Értéket (a hitelesítendő dokumentum(ok) lenyomatának az Aláíró DÁP-HSM-ben tárolt magánkulcsával történő titkosításával előállított digitális jelsorozatot). A Kriptográfiai Műveletet a Felhasználó távolról hajtja végre, azt követően, hogy a Szolgáltatásban tárolt magánkulcsát aktiválta.
42. **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 lenyomathoz 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.
43. **magánkulcs aktiválása:** az a folyamat, melynek során a jogosult- különféle azonosító elemek (pl. jelszó, PIN kód megadásával)- engedélyezi, hogy az elektronikus aláírás létrehozó eszközön tárolt magánkulcs megkezdje üzemszerű működését. Az aktiválás a DÁP keretalkalmazással, mobil eszközön történik és egyszeri használatra érvényes.
44. **magánkulcs deaktiválása:** az a folyamat, melynek során az elektronikus aláírás létrehozó eszközön tárolt magánkulcs üzemszerű működésre megszüntetésre kerül. A Szolgáltatásban működtetett SCDev a magánkulcsot a használat után automatikusan deaktiválja.
45. **megfelelőségértékelő szervezet:** a {J6} 765/2008/EK rendelet 2. cikkének 13. pontjában meghatározott 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.
46. **minősített bizalmi szolgáltatás:** olyan bizalmi szolgáltatás, amely megfelel a {J1} eIDAS rendeletben foglalt alkalmazandó követelményeknek, azaz a Bizalmi Listán szerepel.
47. **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.
48. **minősített elektronikus aláírás:** olyan, fokozott biztonságú elektronikus aláírás, amelyet minősített elektronikus aláírás létrehozó eszközzel állítottak elő, és amely elektronikus aláírás célú minősített tanúsítványon alapul.
49. **minősített elektronikus aláírás létrehozó eszköz:** olyan elektronikus aláírás létrehozó eszköz, amely megfelel a {J1} eIDAS II. mellékletben megállapított követelményeknek, rövidítése: QSCD (Qualified Signature Creation Device).
50. **minősített elektronikus bélyegző:** olyan, fokozott biztonságú elektronikus bélyegző, amelyet minősített elektronikus bélyegzőt létrehozó eszközzel állítottak elő, és amely elektronikus bélyegzés célú minősített tanúsítványon alapul.
51. **minősített elektronikus bélyegzőt létrehozó eszköz:** olyan elektronikus bélyegzőt létrehozó eszköz, amely értelemszerűen megfelel a {J1} eIDAS II. mellékletben megállapított követelményeknek.
52. **PADES-B-B szint:** Alap szintű aláírás. Addig érvényes, amíg az aláíráshoz használt tanúsítvány érvényes. Csak a legalapvetőbb elemeket tartalmazza, amelyeket egy elektronikus aláírásnak tartalmaznia kell (a használt algoritmusok azonosítója, az aláíró tanúsítványa).
53. **PADES-B-T szint:** A PADES-B-B aláírás kiterjesztése. Az aláíráson elhelyezésre kerül egy időbélyeg is, amely bizonyítja, hogy az adott állomány az adott időpontban, vagyis az időbélyegzés pillanatában már létezett.
54. **PADES-B-LT szint:** A PADES-B-T aláírás kiterjesztése. Az aláíráson az aláírás érvényesítéséhez szükséges adatok is elhelyezésre kerülnek, így tipikusan az aláíró tanúsítványa, az időbélyeg tanúsítványa, CRL és/vagy OCSP visszavonási adatok. Lehetővé teszi az aláírt dokumentum érvényesség ellenőrzését, kizárólag a tárolt aláírt adat alapján.
55. **privilegizált felhasználó:** a Szolgáltató informatikai rendszerben olyan, a hivatkozott szabványok szerinti megbízható felhasználó, aki jogosult biztonsági funkciók beállítására vagy módosítására.
56. **rendkívüli üzemeltetési helyzet:** a Szolgáltató üzemmenetében zavart okozó olyan rendkívüli helyzet, amikor a Szolgáltató rendes üzemmenetének folytatására ideiglenesen vagy véglegesen nincs lehetőség,

beleértve a szolgáltatói magánkulcsok kompromittálódása is, vagy annak közvetlen veszélyét.

57. **rendszeradminisztrátor:** az informatikai rendszer telepítését, konfigurálását, karbantartását végző személy.
58. **rendszerüzemeltető:** az informatikai rendszer folyamatos üzemeltetését, mentését és helyreállítását végző személy.
59. **rendszervizsgáló:** a bizalmi szolgáltató naplózott, illetve archivált adatállományait vizsgáló, a szolgáltató által a szabályszerű működés érdekében megvalósított kontroll intézkedések betartásának ellenőrzéséért, a meglevő eljárások folyamatos vizsgálatáért és monitorozásáért felelős személy.
60. **SCDev:** az {Sz3} TS 119 431-1 szabvány 3.1 fejezetében definiált fogalom, azaz olyan konfigurált szoftver és hardver elemek összessége, melynek működési célja a tárolt magánkulcs felhasználásával az Aláírás Érték kiszámítása (a Kriptográfiai Művelet végrehajtásával)
61. **személyazonosító adatok:** 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.
62. **szolgáltatási szabályzat (Certificate Practice Statement- CPS):** a bizalmi szolgáltató nyilatkozata az egyes bizalmi szolgáltatások nyújtásával kapcsolatosan alkalmazott részletes eljárási vagy más működési követelményekről.
63. **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.
64. **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.
65. **tanúsítványokkal kapcsolatos szabályzatok:** a bizalmi szolgáltatási rend, a szolgáltatási szabályzat, a szolgáltatási kivonat, valamint az általános szerződéses feltételek.
66. **távoli minősített elektronikus aláírás létrehozó eszköz:** az aláíró nevében valamely minősített bizalmi szolgáltató által a {J1} eIDAS 29a. cikkével összhangban kezelt, minősített elektronikus aláírás létrehozó eszköz.
67. **üzeneithitelesítő kulcspár:** Az üzeneithitelesítő kulcspár a DÁP keretalkalmazás által a DÁP-TAN szolgáltatás keretében történő tanúsítványigénylésekor 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. Az üzeneithitelesítő kulcspár nyilvános kulcsát, annak generálását követően a DÁP keretalkalmazás továbbítja a Szolgáltató informatikai rendszere felé, mely tárolja azt az adott Aláíróhoz kapcsolva.

1.6.2. Rövidítések

(54.) 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
BSZ-DÁP-TK	-	Bizalmi Szolgáltatási Szabályzat 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-TAN	-	Szolgáltató BR-DÁP-TAN szerinti szolgáltatása
EC	Elliptic Curve	elliptikus görbe
eID	electronic Identification	elektronikus azonosítás
HSM	Hardware Security Module	hardver kriptográfiai eszköz
NTP	Network Time Protocol	időforrás protokoll
OCSP	Online Certificate Status Protocol	valós idejű tanúsítvány-állapot protokoll
PADES	PDF Advanced Electronic Signatures	PDF aláírási formátum
PADES-B-B	PADES-basic	-
PADES-B-T	PADES-basic + Timestamp token	-
PADES-B-LT	PADES-basic + Long term	-
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
SCA	Signature Creation Application	aláíró alkalmazás
SCAL	Sole Control Assurance Level	kizárólagos irányítás biztosítási szintje
SCDev	Signature Creation Device	aláírás létrehozó eszköz
SSAS	Server Signing Application Service	szerver oldali aláírási szolgáltatást megvalósító bizalmi szolgáltatás, amellyel az Aláíró a DÁP-HSM-ben tárolt magánkulcs távoli aktiválásával kiszámíttatja az Aláírás Értéket
SSASP	Server Signing Application Service Provider	a szerver oldali aláírási szolgáltatást működtető bizalmi szolgáltató
UTC	Coordinated Universal Time	koordinált univerzális idő

1.6.3. Hivatkozások

1.6.3.1. Jogszabályi hivatkozások

- {J1} A 1183/2024/EU rendelettel módosított európai és parlamenti (EU) 910/2014 rendelet a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről (továbbiakban: eIDAS)
- {J2} 2023. évi CIII. törvény a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól (továbbiakban: DÁP tv.)
- {J3} 320/2024 (XI. 6.) Korm. rendelet a digitális állam megvalósításához kapcsolódó egyes szervezetek kijelöléséről
- {J4} 2013. évi V. törvény a Polgári Törvénykönyvről (továbbiakban: Ptk.)
- {J5} 24/2016 (VI. 30.) BM rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről
- {J6} 765/2008/EU Európai Parlament és Tanács rendelete a termékek forgalmazása tekintetében az akkreditálás és piacfelügyelet előírásainak megállapításáról és a 339/93/EGK rendelet hatályon kívül helyezéséről
- {J7} 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 (továbbiakban: GDPR)
- {J8} 2024. évi LXIX. törvény Magyarország kiberbiztonságáról (Kiberbiztonsági tv.)
- {J9} 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről
- {J10} 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)
- {J11} 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
- {J12} A Bizottság (EU) 2025/1567 végrehajtási rendelete a 910/2014/EU európai parlamenti és tanácsi rendeletnek a távoli minősített elektronikus aláírást létrehozó eszközök és a távoli minősített elektronikus bélyegzőt létrehozó eszközök minősített bizalmi szolgáltatásként történő kezelése tekintetében történő alkalmazására vonatkozó szabályok megállapításáról

1.6.3.2. Szabványok és műszaki-technikai hivatkozások

- {Sz1} EN 319 401 V3.1.1 (2024-06) General policy requirements for Trust Service Providers

{Sz2}	ENISA ACM	European Cybersecurity Certification Group, Sub-group on Cryptography: 'Agreed Cryptographic Mechanism'
{Sz3}	TS 119 431-1 V1.3.1 (2024-12)	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev
{Sz4}	TS 119 461	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects
{Sz5}	EN 419 241-1:2018	Trustworthy Systems Supporting Server Signing; Part 1: General System Security Requirements
{Sz6}	ISO/IEC 15408-1-5:2022	ISO/IEC 15408 (parts 1 to 5): Information Information security, cybersecurity and privacy protection – Evaluation criteria for IT security
{Sz7}	ISO/IEC 19790:2012	ISO/IEC 19790: Information technology – Security techniques – Security requirements for cryptographic modules
{Sz8}	RFC 3647 (November 2003)	Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework
{Sz9}	RFC 6979 (August 2013)	Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA)

1.6.3.3. Hivatkozott dokumentumok

{D1}	Általános Szerződési Feltételek a NISZ Zrt. Digitális Állampolgárság Programhoz kapcsolódó hitelesítés szolgáltatásaihoz (ÁSZF-DÁP)
{D3}	NISZ Zrt. Szervezeti és Működési Szabályzata
{D4}	Adatkezelési tájékoztató a DÁP eAláírás szolgáltatáshoz
{D5}	NISZ Zrt. PKI szolgáltatások informatikai biztonságpolitikája
{D6}	NISZ Zrt. PKI szolgáltatások biztonsági szabályzata
{D7}	NISZ Zrt. PKI szolgáltatások üzletmenet-folytonossági terve
{D8}	Bizalmi Szolgáltatási Rend a Digitális Állampolgárság Program keretében kibocsátott minősített tanúsítványokhoz (BR-DÁP-TAN)
{D9}	Bizalmi Szolgáltatási Szabályzat a Digitális Állampolgárság Program keretében nyújtott minősített tanúsítvány szolgáltatásokhoz (BSZ-DÁP-TAN)
{D10}	Bizalmi Szolgáltatási Rend a Digitális Állampolgárság Program keretében nyújtott elektronikus aláírások létrehozása és távoli elektronikus aláírást létrehozó eszközök kezelése minősített bizalmi szolgáltatáshoz (BR-DÁP-TK)
{D11}	Bizalmi Szolgáltatási Szabályzat a Digitális Állampolgárság Program keretében nyújtott elektronikus aláírások létrehozása és távoli elektronikus aláírás létrehozó eszközök kezelése minősített bizalmi szolgáltatáshoz (BSZ-DÁP-TK)

{D12} A DÁP Szolgáltató „DÁP – Integrált eAlírás: Csatlakozási szabályzat” c. dokumentuma (csatlakozási szabályzat)

2. KÖZZÉTÉTEL ÉS ADATTÁRAK

2.1. Adattárak

(55.) Szolgáltató a DÁP-TK szolgáltatás keretében nem tart fenn adattárakat. Az Aláírók magánkulcsához kiadott végfelhasználói tanúsítványok, valamint az ún. szolgáltatói tanúsítványok közzétételéről lásd a BSZ-DÁP-TAN 2. fejezetét.

2.2. Szolgáltatói információ közzététele

(56.) A Szolgáltató gondoskodik arról, hogy a Szolgáltatással kapcsolatos szabályzatok (BR-DÁP-TK, BSZ-DÁP-TK, ÁSZF-DÁP, PDS-DÁP), valamint az egyéb közérdekű szolgáltatói információk az Aláírók és Érintett Felek részére folyamatosan rendelkezésre álljanak. A Szolgáltató az információk elérhetőségét az év minden napján, napi 24 órában, éves szinten 97%-os rendelkezésre állással biztosítja, úgy, hogy a kiesés nem lépheti túl esetenként a 24 órás időtartamot.

(57.) A Szolgáltató nem hozza nyilvánosságra azokat az érzékeny és/vagy bizalmas információkat tartalmazó dokumentációkat, melyek biztonsági intézkedéseket, eljárási szabályokat és belső biztonsági szabályzatokat tartalmaznak.

2.3. A közzététel gyakorisága

(58.) A Szolgáltató a Szolgáltatással kapcsolatos szabályzatokat azok változása esetén legalább 30 nappal a változás hatályba lépését megelőzően közzé teszi.

2.4. Hozzáférés-ellenőrzések

(59.) A Szolgáltató olvasás céljára korlátozás nélküli hozzáférést biztosít a Szolgáltatással kapcsolatos nyilvános szabályzatokhoz (BR-DÁP-TK, BSZ-DÁP-TK, ÁSZF-DÁP, PDS-DÁP).

(60.) A Szolgáltató biztonsági intézkedésekkel és eljárási szabályokkal gondoskodik az információk jogosulatlan megváltoztatása, törlése, sérülése és megsemmisülése elleni védelemről.

(61.) A Szolgáltatással kapcsolatos szabályzatoknak csak az elektronikus, aláírással vagy bélyegzővel ellátott formája tekinthető hitelesnek, a dokumentumok nyomtatott változatai semmilyen formában nem tekinthetők hivatalos példánynak vagy hiteles másolatnak.

3. AZONOSÍTÁS ÉS HITELESÍTÉS

(62.) A Szolgáltató a DÁP-TK szolgáltatást a DÁP-TAN-hoz kapcsolódó, minősített bizalmi szolgáltatásként nyújtja. Az Aláírók kezdeti azonosítását (személyazonosságának és jogosultságának ellenőrzését) valamint az alkalmazott névtípusokat és jelentésüket lásd a {D9} BSZ-DÁP-TAN 3.1. és 3.2. fejezeteiben.

(63.) A kriptográfiai műveletek aktiválásához szükséges felhasználóazonosítás az alábbiak szerint történik.

3.1. Az azonosítás és hitelesítés biztonsági szintje

(64.) A Szolgáltató a Szolgáltatás nyújtása során teljesíti az {Sz5} EN 419 241-1 szabvány 5.4 fejezete szerinti - a minősített elektronikus aláírásra vonatkozó – SCAL2 (Sole Control Assurance Level 2) biztonsági szinthez előírt valamennyi követelményt az Aláírók azonosítása, jogosultságuk ellenőrzése, valamint a kriptográfiai műveletek aktiválása során.

3.2. Az Aláírók felhasználóazonosítása

(65.) Az Aláíró szempontjából a DÁP-TK szolgáltatás igénybevételéhez szükséges felhasználóazonosítás az alábbi lépésekből áll:

- a) a DÁP keretalkalmazás elindítása saját mobileszközén;
- b) az azonosításhoz szükséges adat megadása a DÁP keretalkalmazásban.

(66.) A Szolgáltató szempontjából az Aláíró felhasználóazonosítását a DÁP szolgáltató, mint Delegált Autentikációt végző külső fél végzi, a {D9} BSZ-DÁP-TAN 3.2 fejezete szerinti személyazonosításra építve.

4. A SZOLGÁLTATÁS ÉLETCIKLUSA

4.1. A Szolgáltatás igénylése

(67.) A DÁP-TK szolgáltatást közvetlenül nem kell igényelni.

(68.) A DÁP-TAN szolgáltatás alábbi elemeinek igénylése automatikusan a tanúsítványhoz kapcsolódó magánkulcs generálásának, tárolásának és kezelésének igénylését is jelenti:

- a) tanúsítványigénylés (lásd {D9} BSZ-DÁP-TAN 4.1 fejezete).

(69.) A DÁP-TAN szolgáltatás alábbi elemeinek igénylése automatikusan a tanúsítványhoz kapcsolódó magánkulcs megsemmisítésének igénylését is jelenti:

- a) tanúsítvány visszavonás (lásd {D9} BSZ-DÁP-TAN 4.9 fejezete).

4.2. A Szolgáltatás használatba vétele

(70.) Az Aláírók a Szolgáltatást csak azt követően használhatják, hogy a DÁP-HSM modulban tárolt kulcspárjukhoz kapcsolódó, minősített tanúsítvány kibocsátása és nyilvántartásba vétele rendben megtörtént, a {D9} BSZ-DÁP-TAN szerint.

(71.) A Szolgáltató a Szolgáltatás teljes életciklusában biztosítja a tárolt kulcs és az ahhoz tartozó minősített tanúsítvány közötti összerendelés sértetlenségét.

4.3. A Szolgáltatás elérhetősége és rendelkezésre állása

(72.) A Szolgáltatás a DÁP keretalkalmazáson keresztül érhető el.

(73.) A Szolgáltató a Szolgáltatás elérhetőségét az év minden napján, napi 24 órában, éves szinten 97 %-os rendelkezésre állással biztosítja úgy, hogy a kiesés nem lépheti túl esetenként a 24 órás időtartamot.

4.4. A Szolgáltatás használata

- (74.) A Szolgáltatás használatának előfeltétele az Aláíró sikeres felhasználóazonosítása, a 3.2 fejezetben leírt módon.
- (75.) Az Aláírók a DÁP-TK szolgáltatást a DÁP szolgáltató közvetítésével, a DÁP keretalkalmazásban használhatják, kétféle módon:
- a) Az Aláíró által kezdeményezett aláírás esetén: az Aláíró a saját mobil eszközén tárolt, a DÁP szolgáltató által szabott technikai feltételeknek megfelelő PDF formátumú dokumentumok minősített elektronikus aláírással és minősített időbélyegzővel¹ történő ellátását kérheti a Szolgáltatótól.
 - b) Aláíró partner által kezdeményezett aláírás esetén: az Aláíró az Aláíró partner által számára megadott és a saját mobil eszközén megtekintett, a DÁP szolgáltató által szabott technikai feltételeknek megfelelő PDF formátumú dokumentumok minősített elektronikus aláírással és – amennyiben az aláírást kérő Aláíró partner időbélyeggel ellátott aláírást kér – minősített időbélyegzővel² történő ellátását kérheti a Szolgáltatótól.
- (76.) Aláíró által kezdeményezett aláírás esetén a DÁP keretalkalmazás először megmutatja az Aláírónak a tanúsítványa adatait és az aláírni kívánt dokumentum tartalmát, majd a kiválasztott dokumentumról – a fent említett technikai feltételek ellenőrzését és az Aláíró jóváhagyását követően – az Aláíró mobil eszközén SHA-384 algoritmussal egyedi hash lenyomat készül, melyet az eszköz – a DÁP szolgáltatón keresztül – szabványos aláírási kérekként küld el a Szolgáltató informatikai rendszere felé.
- (77.) Aláíró partner által kezdeményezett aláírás esetén az aláírandó dokumentumról az Aláíró partner Aláíró alkalmazásában SHA-384 algoritmussal egyedi hash lenyomat készül, majd az Aláíró partner a DÁP szolgáltatón keresztül értesíti az Aláírókat az aláírási kérekről. Az értesítés alapján, az Aláíró azonosítását követően, a DÁP keretalkalmazás először megmutatja az Aláírónak a tanúsítványa adatait és az aláírandó dokumentum tartalmát, majd az Aláíró jóváhagyását követően a DÁP szolgáltató az Aláíró partner által készített egyedi hash lenyomatot szabványos aláírási kérekként küldi el a Szolgáltató informatikai rendszere felé.
- (78.) Az aláírási kérés az Aláíró mobil eszközén tárolt egyedi üzenethitelesítő kulccsal kerül hitelesítésre a hozzá tartozó egyedi jelszó Aláíró általi megadását követően, hogy a Szolgáltató egyértelműen azonosíthassa az Aláíró által használt keretalkalmazást. Ezt az üzenethitelesítő kulcspárt a DÁP keretalkalmazás a DÁP-TAN szolgáltatás keretében történő tanúsítványigénylés során generálja, majd annak nyilvános kulcsát továbbítja mind a Szolgáltatónak, mind pedig a DÁP szolgáltatónak. Szolgáltató az üzenethitelesítő nyilvános kulcsot a megfelelő aláíróhoz rendelve rögzíti a szolgáltatást megvalósító saját informatikai rendszerében. A későbbiekben a DÁP keretalkalmazás az üzenethitelesítő kulcspár magánkulcsával hitelesíti üzenetét mind a Szolgáltató, mind a DÁP szolgáltató felé – a jelen DÁP-TK szolgáltatás és a DÁP-TAN szolgáltatás keretén belül egyaránt (lásd BSZ-DÁP-TAN 4.1.2.4).
- (79.) A Szolgáltató ellenőrzi a DÁP szolgáltatótól kapott kérés formai és tartalmi megfelelőségét.
- (80.) A Szolgáltató visszautasítja a kérést, ha:
- a) az Aláíró (illetve az általa használt DÁP keretalkalmazás) azonosítása és/vagy jogosultságának ellenőrzése sikertelen;

¹ A minősített időbélyegzőt a DÁP-TK szolgáltatás Szolgáltató minősített időbélyegszolgáltatásának igénybevételével biztosítja. Szolgáltató minősített időbélyegszolgáltatásáról bővebben lásd az „*Időbélyegzés Bizalmi Szolgáltatási Szabályzat*” c. dokumentumot (OID: 0.2.216.1.200.1100.100.42.3.3.15), mely letölthető Szolgáltató internetes weboldaláról.

² A minősített időbélyegzőt a DÁP-TK szolgáltatás Szolgáltató minősített időbélyegszolgáltatásának igénybevételével biztosítja, amennyiben azt az Aláíró partner kéri. Szolgáltató minősített időbélyegszolgáltatásáról bővebben lásd az „*Időbélyegzés Bizalmi Szolgáltatási Szabályzat*” c. dokumentumot (OID: 0.2.216.1.200.1100.100.42.3.3.15), mely letölthető Szolgáltató internetes weboldaláról.

- b) a kérés nem felel meg a vonatkozó rendszerkövetelményeknek;
- c) a tárolt kulcshoz kapcsolódó tanúsítvány lejárt vagy visszavont;
- d) a kérésben a kriptográfiai művelet végrehajtásához megadott aláírási algoritmus a nemzetközi mértékadó szakmai dokumentumok szerint nem kellően erős a tárolt kulcshoz kapcsolódó tanúsítvány teljes érvényességi időszakában.

- (81.) A Szolgáltató elfogadja és kiszolgálja a kérést, ha a fenti ellenőrzések mindegyike sikeresen megtörtént.
- (82.) A Szolgáltató, elfogadott aláírási kérés esetén, a kapott lenyomat Aláíró magánkulcsával történő titkosításával, előállítja az Aláírás Értéket, majd ezen értéket továbbítja a DÁP szolgáltató felé, aki közvetlenül vagy Aláíró partner közreműködésével PAdES formátumú minősített elektronikus aláírásba foglalja azt és összekapcsolja a dokumentummal.
- (83.) Aláíró által kezdeményezett aláírás esetén az aláírás szintje minden esetben PAdES-B-LT, Aláíró partner által kezdeményezett aláírás esetén az aláírás szintjét az Aláíró partner határozza meg.

4.5. Előfizetés vége

- (84.) Az előfizetés az {D1} ÁSZF-DÁP-ban meghatározott esetekben és módon szűnik meg.
- (85.) A Szolgáltatás a tárolt kulcshoz tartozó tanúsítvány érvényességének {D9} BSZ-DÁP-TAN szerinti lejáratával szűnik meg. A Szolgáltatás igénybevételét a tárolt kulcshoz tartozó tanúsítvány {D9} BSZ-DÁP-TAN szerinti visszavonásával lehet megszüntetni.

5. FIZIKAI, ELJÁRÁSBELI ÉS SZEMÉLYZETI BIZTONSÁGI ÓVINTÉZKEDÉSEK

- (86.) A Szolgáltató a Szolgáltatások nyújtása során a kellő, az irányadó szabványoknak megfelelő fizikai, eljárásbeli és személyzeti biztonsági óvintézkedéseket és az ezeket érvényre juttató adminisztratív és irányítási eljárásokat alkalmazza.
- (87.) A Szolgáltató a rendszer kialakításakor kockázat-elemzést végzett üzleti kockázatainak felmérésére, valamint a szükséges biztonsági követelmények és működési eljárások meghatározására; a kockázatok felülvizsgálatáról legalább negyedévente rendszeresen, valamint szükség esetén eseti jelleggel gondoskodik. Szolgáltató a szervezetén belüli biztonságkezeléshez szükséges informatikai biztonsági infrastruktúrát folyamatosan fenntartja. A biztonság szintjére hatást gyakorló bármilyen változtatást a Szolgáltató vezetősége hagy jóvá.
- (88.) A biztonságkezelési szabályokat a Szolgáltató {D5} PKI szolgáltatások biztonságpolitikája tartalmazza. A Szolgáltató informatikai rendszerei vonatkozásában a Szolgáltató {D6} biztonsági szabályzat érvényesül. Ez a szabályzat szervezeti egység szinten és munkakörökre lebontva rögzíti a biztonságkezeléssel összefüggő feladatokat, felelősségeket és szabályokat, így többek között a bizalmi munkakörök felsorolását, a kinevezési feltételeket és az összeférhetetlenségi kritériumokat.
- (89.) A Szolgáltató megvalósította és folyamatosan fenntartja a Szolgáltatásokat nyújtó eszközök, rendszerek biztonsági ellenőrzéseit és üzemeltetési eljárásait. A Szolgáltató rendszeres belső ellenőrzései és külső auditjai ezen eljárásokat, a vonatkozó dokumentumokat és a Szolgáltatásokra vonatkozó előírások teljesülését rendszeres időközönként vizsgálja.
- (90.) A fenti eljárásokat a Szolgáltatóval munkaviszonyban álló, megbízható és szakértő üzemeltető személyzet biztosítja.
- (91.) A Szolgáltató gondoskodik arról, hogy eszközei és információi a megfelelő szintű védelemben részesüljenek. A Szolgáltató valamennyi informatikai értékéről leltárt vezet, ezek védelmi követelményeit az elvégzett kockázatelemzéssel összhangban osztályokba sorolja és minősíti.

(92.) A Szolgáltató a szolgáltatásnyújtásban közreműködő informatikai rendszereit, berendezéseit és eszközeit a legmagasabb védelmi szintet képező központi géptermben helyezi el.

5.1. Fizikai óvintézkedések

5.1.1. Telephelyek elhelyezése és szerkezeti felépítése

(93.) A Szolgáltató a Szolgáltatások nyújtásában közreműködő informatikai rendszereit fizikai és logikai védelemmel ellátott, legmagasabb védelmi szintet képező objektumokban helyezte el és üzemelteti.

(94.) A telephelyek elhelyezése és kialakítása során olyan egymásra épülő és egymást támogató védelmi megoldásokat alkalmaz, melyek képesek megakadályozni az illetéktelen hozzáférést és alkalmasak az informatikai rendszerek és Szolgáltató által tárolt bizalmas adatok megóvására.

5.1.2. Fizikai hozzáférés

(95.) A Szolgáltató megvédi a Szolgáltatások nyújtásában közreműködő eszközeit és berendezéseit a jogosulatlan fizikai hozzáféréstől az eszközök manipulálásának megakadályozása érdekében.

(96.) Ehhez biztosítja az alábbiakat:

- a) a géptermbekbe történő minden be- és kilépés, valamint a belépés célja naplózásra kerül;
- b) a géptermbekbe 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 géptermben megfelelő jogosultságú és létszámú, bizalmi munkakört betöltő kísérő személy állandó felügyelete mellett;
- d) az eszközök aktivizáló adatai (jelszavak, PIN kódok stb.) a géptermben 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

(97.) A Szolgáltató a géptermben olyan szünetmentes áramellátó rendszert alkalmaz, 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.

(98.) A Szolgáltató a géptermben olyan légkondicionáló berendezést alkalmaz, 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 üzemi hőmérséklet biztosítására, az eszközök és berendezések túlhevülésének megakadályozására.

5.1.4. Beázás és elárasztás veszélyeztetettség

(99.) A Szolgáltató megvédi a géptermet a beázástól, víz betöréstől és elárasztástól nedvességérzékelő és riasztó rendszer alkalmazásával.

5.1.5. Tűz megelőzés és tűzvédelem

(100.) A Szolgáltató a géptermet füst- és tűzérzékelőkkel szerelte fel, melyek automatikusan riasztják az illetékes személyzetet. Minden helyiségben jól látható helyen van elhelyezve a vonatkozó előírásoknak megfelelő típusú és mennyiségű kézi tűzoltó készülék. A gépteremben automatikus tűzoltó rendszer került kialakításra, amely emberi egészségre nem veszélyes és nem károsítja az informatikai eszközöket.

5.1.6. Adathordozók tárolása

(101.) A Szolgáltató megvédi valamennyi adathordozóját a jogosulatlan hozzáféréstől, a megsemmisüléstől vagy véletlen rongálódástól, jellemzően páncélszekrénybe történő elzárással.

5.1.7. Selejt kezelése és megsemmisítése

(102.) A Szolgáltató a környezetvédelmi előírások betartásával gondoskodik feleslegessé vált eszközeinek, adathordozóinak megsemmisítéséről. A felesleges eszközök és adathordozók az erre kijelölt munkatárs személyes felügyelete mellett, széleskörűen elfogadott módszerekkel kerülnek használhatatlanná tételre vagy visszaállíthatatlan módon törlésre.

5.1.8. Fizikailag elkülönítetten őrzött mentési példányok

(103.) A Szolgáltató azt az adatmentést, amiből meghibásodás esetén a teljes szolgáltatás helyreállítható, olyan külső helyszínen tárolja, mely megfelelő fizikai és működési védelemmel rendelkezik. Biztosítja a mentett adatok helyszínek közötti biztonságos továbbítását. Az adatmentést, vagy abból a helyreállítást rendszerüzemeltető bizalmi munkakört betöltő személy végzi el.

5.2. Eljárásbeli előírások

(104.) A Szolgáltató gondoskodik arról, hogy informatikai rendszereit biztonságosan, szabályszerűen, a meghibásodás minimális kockázata mellett üzemeltessék. A Szolgáltató személyzete a feladatokat olyan eljárásbeli előírások alapján végzi, melyek szinkronban vannak a jogszabályi, szabványi és belső biztonsági előírásokkal.

(105.) Az eljárásbeli szabályokat a következő szabályzatok tartalmazzák:

- a) {D3} a Szolgáltató Szervezeti és Működési szabályzata, mely meghatározza a Szolgáltató szervezeti felépítését, azon belül az egyes szervezetekhez kapcsolt feladat-, felelősség- és hatásköröket;
- b) jelen szolgáltatási szabályzat, mely a Szolgáltató és a PKI közösség (Aláírók, Érintett Felek, Egyéb felek) viszonyát szabályozza;
- c) {D6} Szolgáltató biztonsági szabályzata, mely részletesen előírja az adatokhoz és informatikai rendszerekhez, valamint a személyi és fizikai környezethez kapcsolódó biztonsági szabályokat.

5.2.1. Bizalmi munkakörök

(106.) A Szolgáltató – jelen szolgáltatása keretében – az alábbi bizalmi munkaköröket azonosította, melyektől a szolgáltatások biztonsága függ:

- a) a Szolgáltató informatikai rendszeréért általánosan felelős vezető;
- b) biztonsági tisztviselő: a szolgáltatás biztonságáért általánosan felelős személy;

- c) rendszeradminisztrátor: az informatikai rendszer telepítését, konfigurálását, karbantartását végző személy;
- d) rendszerüzemeltető: az informatikai rendszer folyamatos üzemeltetését, mentését és helyreállítását végző személy;
- e) független rendszervizsgáló: a szolgáltató naplózott, illetve archivált adatállományát vizsgáló, a Szolgáltató által a szabályszerű működés érdekében megvalósított kontroll intézkedések betartásának ellenőrzéséért, a meglévő eljárások folyamatos vizsgálatáért és monitorozásáért felelős személy.

(107.) A b)-e) pont szerinti munkaköröket viselő munkatársak a Szolgáltató informatikai rendszerei szempontjából ún. privilegizált felhasználónak tekintendők.

(108.) A bizalmi munkakörökhöz tartozó feladatkörök és felelősségek leírását a Szolgáltató belső, nem nyilvános szabályzata tartalmazza. A bizalmi munkakört betöltő személy munkaviszonyban áll a Szolgáltatóval. Bizalmi munkakörbe Szolgáltató felső vezetősége nevezi ki a munkatársakat. Minden bizalmi munkakört legalább két személy tölt be.

(109.) A bizalmi munkaköröket betöltő személyekről Szolgáltató nyilvántartást vezet. A nyilvántartásban bekövetkező minden változást a változtatás bevezetése előtt a Bizalmi Felügyeletnek bejelenti.

5.2.2. Az egyes feladatokhoz szükséges személyzeti létszámok

(110.) Szolgáltató {D6} biztonsági szabályzata előírja, hogy csak védett környezetben, legalább kettő, bizalmi munkakört betöltő munkatárs egyidejű jelenléte mellett, illetéktelen személy jelenlétét kizárva végezhetők el az alábbi műveletek:

- a) végfelhasználói (aláírói) kulcspár előállítására és kezelésére szolgáló DÁP-HSM modul üzembe helyezése;
- b) a Szolgáltatás nyújtásához használt informatikai rendszer működtetéséhez szükséges infrastrukturális és vezérlő kulcsok előállítása és egyéb kulcsgondozási funkciói.

5.2.3. Bizalmi munkakörökben elvárt azonosítás és hitelesítés

(111.) A bizalmi munkaköröket betöltő személyek azonosítása és hitelesítése multi-faktoros autentikációs mechanizmusokkal történik meg, mielőtt a Szolgáltatások nyújtásában érintett kritikus informatikai rendszerekhez hozzáférhetnének.

(112.) A Szolgáltató a „legkisebb jogosultságok” elvét alkalmazva adminisztrálja a bizalmi munkaköröket betöltő személyek felhasználói hozzáférési képességeit, teljesítve az alábbiakat:

- a) Biztosítani kell a rendszergazdai célokra, például telepítésre, konfigurálásra, kezelésre vagy karbantartásra használt egyedi fiókok beállítását.
- b) A jogosultsággal rendelkező fiókok csak akkor használhatók, ha a jogosultságok az adott tevékenységhez szükségesek.
- c) A privilegizált fiókok esetében erős azonosítási, hitelesítési és engedélyezési eljárásokat kell alkalmazni.
- d) Tervezett időközönként felül kell vizsgálni a privilegizált és rendszergazdai fiókokhoz való hozzáférési jogokat, és ezeket a szervezeti változások alapján módosítani kell. A felülvizsgálat eredményét, beleértve a hozzáférési jogok szükséges módosításait, dokumentálni kell.
- e) Biztosítani kell, hogy a hozzáférési jogosultságok megfelelően módosuljanak a munkaviszony megszűnésekor vagy a funkcióváltáskor.
- f) Az információhoz és az alkalmazói rendszer funkcióihoz való hozzáférést belső szabályzatnak megfelelően korlátozni kell.
- g) A Szolgáltató rendszerében megfelelő számítógépes biztonsági intézkedéseket kell biztosítani a Szolgáltató gyakorlatában azonosított bizalmi szerepkörök szétválasztásához, beleértve a biztonsági adminisztrációs és üzemeltetési funkciók szétválasztását. Különösen a rendszer-segédprogramok használatát kell korlátozni és ellenőrizni.
- h) A Szolgáltató személyzetét azonosítani és hitelesíteni kell a szolgáltatáshoz kapcsolódó kritikus alkalmazások használata előtt.

- i) A Szolgáltató személyzetének elszámoltathatónak kell lennie a végzett tevékenységéért.
- j) Az érzékeny adatokat védeni kell az újra felhasznált tárolóobjektumokon (pl. törölt fájlok) felfedés ellen, illetve az adathordozókhoz való illetéktelen hozzáféréstől.

5.2.4. Egymást kizáró munkakörök

- (113.) Szolgáltató biztosítja, 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, és a rendszeradminisztrátor feladatait;
 - c) törekedni kell a bizalmi munkakörök teljes személyi szétválasztására.

5.3. Személyzetre vonatkozó előírások

- (114.) A Szolgáltató gondoskodik arról, hogy a személyzeti előírásai, a munkatársak alkalmazására vonatkozó gyakorlatai fokozzák és támogatják a Szolgáltató működésének megbízhatóságát.
- (115.) A Szolgáltató kellő számú, a Szolgáltatások nyújtásához szükséges feladatok jellegének, terjedelmének és mennyiségének megfelelő végzettséggel, képzettséggel, szakmai tudással és tapasztalattal rendelkező személyzetet alkalmaz.
- (116.) A Szolgáltató valamennyi bizalmi munkakört betöltő munkatársa mentes minden olyan ütköző érdektől, ami hátrányosan érinthetné a Szolgáltatások megbízhatóságát és biztonságát.
- (117.) A munkatársak a feladatok szétválasztása és a legkisebb meghatalmazás szempontjai alapján meghatározott munkaköri leírásokkal rendelkeznek.

5.3.1. Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

- (118.) A Szolgáltató biztosítja, hogy bizalmi munkakört csak olyan személyek töltsenek be, akiknek a bizalmi munkakör betöltéséhez szükséges befolyásmentességét és szakértelmét erkölcsi bizonyítvánnyal, szakmai gyakorlattal, végzettséggel vagy szakképesítéssel igazolni tudja.
- (119.) A Szolgáltató informatikai rendszeréért általánosan felelős vezető szakirányú felsőfokú végzettséggel és legalább három év, az informatikai biztonsággal összefüggésben szerzett szakmai gyakorlattal rendelkezik. Szakirányú felsőfokú végzettség a matematikusi, fizikusi egyetemi végzettség vagy a műszaki tudományterületre tartozó mérnöki szakon szerzett főiskolai vagy egyetemi végzettség.
- (120.) A biztonsági tisztviselők és rendszervizsgálók esetén közép vagy felsőfokú végzettség, középfokú végzettség esetén legalább három, felsőfokú végzettség esetén legalább egy év informatikai biztonsággal összefüggésben szerzett szakmai gyakorlat szükséges.
- (121.) A rendszerüzemeltető és rendszeradminisztrátor esetén középfokú végzettség és legalább egy év, hasonló munkakörben szerzett szakmai gyakorlat szükséges.
- (122.) Az egyes bizalmi munkakörök betöltéséhez elvárt szakirányú végzettségek meghatározását a Szolgáltató belső, nem nyilvános szabályzata tartalmazza.

5.3.2. Biztonsági háttér ellenőrzés eljárásai

- (123.) A Szolgáltató vezetői munkakörben, illetve bizalmi munkakörben vagy szerepkörben csak olyan alkalmazottakat foglalkoztat, 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.

(124.) Az 5.2.1 fejezetben meghatározott bizalmi munkakör betöltését a legmagasabb szintű biztonsági ellenőrzés (a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvényben meghatározott nemzetbiztonsági ellenőrzés) előzi meg. A többi, a Szolgáltatás nyújtásával kapcsolatos munkakörben, a munkakör betöltését fokozott szintű, a Szolgáltató által végzett biztonsági ellenőrzés előzi meg. Mind a legmagasabb, mind a fokozott biztonsági ellenőrzés lefolytatásához szükséges az érintett személy hozzájárulása. Nem tölthet be bizalmi munkakört az a személy, akinél a biztonsági ellenőrzés kockázatot tár fel.

(125.) A bizalmi munkakörhöz történő hozzárendeléskor az érintett személy:

- a) pontos és írásos munkaköri leírást vesz át a főlérendelt vezetőtől vagy a Szolgáltató humán szervezetétől;
- b) titoktartási nyilatkozatot kell aláírnia,
- c) szükséges mértékű oktatásban részesül, annak érdekében, hogy a feladat-, felelősség és hatáskörét pontosan megismerje és gyakorolni tudja.

(126.) Kilépéskor:

- a) A kilépésről szóló döntés meghozatalakor a kilépő fizikai és logikai belépési és hozzáférési jogosultságai azonnal megszüntetésre kerülnek. Ezt követően, a kilépő személy csak biztonsági tisztviselő kíséretében léphet be a Szolgáltatásokkal kapcsolatos körletekbe.
- b) Azonnal vissza kell venni az azonosításhoz és hitelesítéshez használt eszközét, és dokumentáltan meg kell semmisíteni azt. A kapcsolódó tanúsítványokat vissza kell vonni.

5.3.3. Képzési követelmények

(127.) A bizalmi munkakörökben Szolgáltató olyan személyeket foglalkoztat, akik az adott munkakör vagy szerepkör ellátásához szükséges mértékben elsajátították:

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

(128.) 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

(129.) A Szolgáltató gondoskodik arról, hogy a munkatársak folyamatosan a megfelelő tudással rendelkezzenek, szükség esetén továbbképzést vagy ismétlő jellegű képzést tart vagy biztosít.

(130.) A Szolgáltató minden lényeges változás esetén megismétli az érintett személyek részére a képzést vagy annak elemeit.

(131.) Jelentős változás, azaz a szervezeti biztonságpolitika módosulása, a szoftver vagy hardver változása (upgrade), valamint a kulcs kezelés és biztonság kezelési óvintézkedések változása esetén, valamennyi munkatárs, az őt érintő mélységben továbbképzésben részesül, illetve megkapja a szükséges dokumentációkat.

(132.) Kisebb változások esetén a munkatársak a változás bekövetkezte előtt írásos tájékoztatást kapnak.

(133.) A Szolgáltató legalább évente egyszer továbbképzést biztosít az újonnan ismertté vált sebezhetőségekről, az IT biztonság aktuális gyakorlatáról a munkatársak saját szakterületét illetően.

5.3.5. Munkabeosztás körforgásának gyakorisága és sorrendje

(134.) Nincs kikötés.

5.3.6. Felhatalmazás nélküli tevékenységek büntető következményei

(135.) A Szolgáltató a munkavállalóval kötött munkaszerződésben vagy külső munkatárssal kötött megbízási szerződésben szabályozza a munkavállaló vagy külső munkatárs felelősségre vonásának lehetőségét az elkövetett mulasztások, vétlen vagy szándékos károkozás esetére.

5.3.7. Szerződéses munkavállalókra vonatkozó követelmények

(136.) A Szolgáltató bizalmi munkakörben csak munkaviszonyban álló személyt foglalkoztat.

(137.) Az egyéb feladatok ellátására, vállalkozási vagy megbízási szerződés keretében a beszállítóval Szolgáltató írásos megállapodást köt. A szerződő fél titoktartási nyilatkozatot ír alá, melyben vállalja, hogy a szerződés teljesítésében közreműködő személyek a munkavégzés során birtokukba kerülő üzleti titkokat és bizalmas információkat illetéktelen személynek fel nem fedik, más módon sem hasznosítják, és amely tartalmazza a megszegése esetén alkalmazott szankciókat.

5.3.8. A személyzet számára biztosított dokumentációk

(138.) A Szolgáltató folyamatosan biztosítja a személyzet részére a munkakörük ellátásához szükséges dokumentációk és szabályzatok rendelkezésre állását.

(139.) Minden bizalmi munkakört betöltő munkatárs megkapja írásban:

- a) egyéni munkaköri leírást;
- b) a Szolgáltató szervezeti és biztonsági szabályzatait;
- c) rendszeres és rendkívüli továbbképzések alkalmával az adott oktatási formához tartozó oktatási segédanyagokat.

5.4. A biztonsági naplózás folyamatai

5.4.1. Naplózott esemény típusok

(140.) A Szolgáltató naplóz minden, az informatikai rendszerével és Szolgáltatások nyújtásával kapcsolatos eseményt. A naplózott adatállomány átfogja a szolgáltatás nyújtásának teljes folyamatát, és lehetővé teszi, hogy a valós helyzetek megítéléséhez a szükséges mértékben minden, a Szolgáltatásokkal kapcsolatos eseményt rekonstruálni lehessen.

(141.) Az informatikai rendszerrel kapcsolatos események különösen a rendszer indítás és leállítás, biztonsági profil változása, rendszer összeomlás és hardver hibák, tűzfal aktivitás, hozzáférési kísérletek, szolgáltatói kulcs kezelés eseményei, óraszinkronizációs események, naplózási funkció elindítása és leállítása, naplózási paraméterek megváltoztatása, naplóadatok tárolásával kapcsolatos hibák, napló adatok integritásának sérülése eseményei.

(142.) A Szolgáltatások nyújtásával kapcsolatos események különösen az alábbiak:

- a) a Szolgáltatás nyújtásához használt informatikai rendszer működtetéséhez szükséges infrastrukturális és vezérlő kulcsok életciklusával kapcsolatos minden esemény;
- b) a Szolgáltatásban kapott kérések és válaszok;
- c) tárolt végfelhasználói magánkulcs életciklusával kapcsolatos minden esemény;
- d) tárolt végfelhasználói magánkulcsok használatának eseményei;

- e) adatok továbbítása;
- f) jogosultságok, jelszavak módosítása;
- g) sikeres és sikertelen belépési kísérletek;
- h) adatok módosítása és továbbítása;
- i) hálózati események.

(143.) A naplózott adatállomány tartalmazza a naplózott esemény bekövetkeztének dátumát és pontos időpontját, az esemény követhetőségéhez, rekonstruálásához szükséges adatokat, az esemény kiváltásában közreműködő felhasználó vagy más személy nevét vagy azonosítóját.

5.4.2. Naplóállomány feldolgozásának gyakorisága

(144.) A Szolgáltató biztosítja a naplóállományok rendszeres ellenőrzését és kiértékelését.

(145.) A Szolgáltatások nyújtásával kapcsolatos események naplóállományait naponta feldolgozzák a rendszervizsgálók.

(146.) Az informatikai rendszer eseményeinek naplóállományait a rendszervizsgálók rendszeres időközönként, a biztonsági szabályzatban meghatározott sűrűséggel végzik el.

5.4.3. Naplóállomány megőrzési időtartama

(147.) A Szolgáltató a naplóállományokat archiválja és gondoskodik azok biztonságos megőrzéséről az 5.5.2 fejezetben előírt időtartamig. Ezen időtartamig Szolgáltató biztosítja az archivált állományok olvashatóságát, megőrzi az ehhez szükséges hardver és szoftver eszközöket.

5.4.4. Naplóállomány védelme

(148.) A Szolgáltató a naplóállományokat és azok mentéseit biztonságos, fizikailag is védett környezetben tárolja. A naplóállományokat időbélyegzővel, a naplóállományok archiv mentéseit időbélyegzőt is tartalmazó elektronikus aláírással vagy bélyegzővel látja el.

(149.) A Szolgáltató gondoskodik arról, hogy a naplóállományokhoz és azok mentéseihez csak az arra feljogosított személyek férhessenek hozzá.

5.4.5. Naplóállomány mentési folyamatai

(150.) A naplóállományokról a Szolgáltató rendszeres mentést készít. A mentéssel kapcsolatos eljárásokat és szabályokat a Szolgáltató belső szabályzata tartalmazza.

5.4.6. Naplózás gyűjtési rendszere

(151.) A naplóbejegyzések gyűjtését belső komponens oldja meg. A naplóbejegyzések gyűjtése megkezdődik rendszer indításkor és rendszer leállítáig folyamatosan működik, és közben biztosítja a gyűjtött bejegyzések integritását és rendelkezésre állását, szükség esetén a bizalmasságát is.

(152.) A naplóbejegyzések gyűjtési rendszerének működési rendellenessége esetén Szolgáltató felfüggeszti az érintett területek működését az üzemzavar elhárításáig.

5.4.7. Rendellenes eseményeket kiváltó alanyok értesítése

(153.) A rendellenes eseményeket kiváltó alanyokat (személyeket, szervezeteket) Szolgáltató nem feltétlenül értesíti minden esetben. Szolgáltató szükség esetén bevonhatja az eseményt kiváltó alanyt az esemény

kivizsgálásába. Ilyen esetben az érintett Közreműködő Fél, Aláíró kötelessége a Szolgáltatóval való együttműködés az esemény feltárása érdekében.

5.4.8. Sebezhetőség értékelések

- (154.) A Szolgáltató a vonatkozó szabványok által meghatározott rendszeres időközönként, a naplóállományok és egyéb információk kiértékelésén alapuló sebezhetőség vizsgálatot és behatolás tesztet végez. Ennek segítségével feltérképezi a potenciális belső és külső fenyegetéseket, melyek a Szolgáltató által tárolt végfelhasználói magánkulcsok módosítását, sérülését, megsemmisülését vagy jogosulatlan aktiválását eredményezhetik.
- (155.) A sebezhetőség vizsgálathoz kapcsolódóan Szolgáltató kockázatelemzésben értékeli az egyes fenyegetések bekövetkeztének valószínűségét és a bekövetkezés esetén várható kárt. Értékeli az alkalmazott folyamatokat, informatikai rendszereket, védelmi intézkedéseket, hogy azok megfelelően képesek-e ellenállni a fenyegetésnek.
- (156.) A kiértékelést követően a Szolgáltató megteszi a megfelelő intézkedéseket annak érdekében, hogy a feltárt sebezhetőség kihasználhatósága ne következzen be.
- (157.) A Szolgáltató folyamatosan figyelemmel kíséri az újonnan ismertté vált, kritikus sebezhetőségeket, és a szükséges ellenintézkedéseket lehetőség szerint 48 órán belül megteszi. Bármely olyan sebezhetőség esetén, melynek kihatása lehet a Szolgáltatások nyújtására, a Szolgáltató vagy cselekvési tervet készít és hajt végre annak érdekében, hogy a sebezhetőség ne legyen kihasználható, illetve annak hatása elhanyagolható legyen, vagy dokumentálja annak ténybeli alapját, hogy az adott sebezhetőség nem igényel intézkedést.

5.5. Adatok archiválása

5.5.1. A tárolt adatok típusai

- (158.) A Szolgáltató gondoskodik 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.
- (159.) Ehhez legalább az alábbi információkat tárolja papír alapon vagy elektronikusan:
- a) az Aláíró tárolt magánkulcsával kapcsolatos valamennyi információ a teljes életciklusra vonatkozóan;
 - b) a bizalmi szolgáltatási rendek és szolgáltatási szabályzat valamennyi kibocsátott verziója;
 - c) az Általános Szerződési Feltételek valamennyi kibocsátott verziója;
 - d) a Szolgáltató működésével kapcsolatos szerződések, különösen a Közreműködő Felekkel kötött megállapodások;
 - e) valamennyi naplóállomány.

5.5.2. Archivum megőrzési időtartama

- (160.) A Szolgáltató az 5.5.1 fejezetben meghatározott archivált adatokat az alábbi időtartamokig őrzi meg:
- a) 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;
 - b) szabályzatok, szerződések esetében a hatályon kívül helyezés vagy megszűnés utáni 10 évig;

5.5.3. Archívum védelme

- (161.) A Szolgáltató olyan fizikai védelmet biztosít és biztonsági óvintézkedéseket alkalmaz, melyek fenntartják az archivált adatok sértetlenségét, hitelességét, rendelkezésre állását és a bizalmasságát. Az elektronikus formában archivált adatokat a Szolgáltató legalább fokozott biztonságú elektronikus aláírással vagy bélyegzővel, valamint minősített időbélyegzővel látja el.

5.5.4. Archívum mentési eljárásai

- (162.) A Szolgáltató a papír alapú iratokat, dokumentumokat a dokumentumtárban, az elektronikus állományokat pedig több példányban, fizikailag elkülönített helyszíneken őrzi meg, illetve tárolja.
- (163.) A Szolgáltató biztosítja az elektronikus formában archivált állományok adathordozóinak elavulás elleni védelmét a megőrzési időn belül.

5.5.5. Az adatok időbélyegzésére vonatkozó követelmények

- (164.) Valamennyi naplóbejegyzésben olyan időjel szerepel, amely a 6.8 fejezetben ismertetett időforrásokkal szinkronizált rendszeridőt tartalmazza, melynek pontossága egy másodpercen belül.
- (165.) A naplóállományokra óránként legalább fokozott biztonságú elektronikus bélyegző és minősített időbélyeg kerül.
- (166.) Az elektronikus formában archivált adatokon elhelyezett elektronikus aláírás vagy bélyegző minősített időbélyeget tartalmaz.
- (167.) A Szolgáltató az archivált adatok megőrzése során szükség esetén (pl. algoritmus váltás) gondoskodik az elektronikus aláírások vagy bélyegzők, valamint az időbélyegzők hitelességnek fenntartásáról.

5.5.6. Archívum gyűjtési rendszere

- (168.) A naplóállományokat és az egyéb elektronikusan keletkezett adatokat a Szolgáltató védett informatikai rendszerén belül gyűjti.

5.5.7. Archívum hozzáférés és ellenőrzés eljárásai

- (169.) A Szolgáltató az archivált adatokat megvédi a jogosulatlan hozzáféréstől. Szolgáltató a jogosultságot ellenőrzi, és a hozzáféréseket naplózza.
- (170.) A Szolgáltató az Ügyfélszolgálat közreműködésével biztosítja az Aláírók számára a róluk tárolt személyes adatokra vonatkozó tájékoztatást.
- (171.) A Szolgáltató a 9.4.6 fejezetben ismertetett hatósági vagy jogi eljárásokban a szükséges mértékben a biztosítja a hozzáférést az archívumban tárolt adatokhoz.

5.6. Kulcsátállítás

- (172.) A Szolgáltató biztosítja, hogy a hitelesítőközpontok folyamatosan rendelkezzenek a működésükhöz szükséges érvényes kulccsal és tanúsítvánnyal. Részletesen lásd a {D9} BSZ-DÁP-TAN 5.6 fejezetében.

5.7. Helyreállítás rendkívüli üzemeltetési helyzetek esetén

- (173.) A Szolgáltató minden szükséges intézkedést meghoz annak érdekében, hogy rendkívüli üzemeltetési helyzet, katasztrófa esetén a szolgáltatás kiesésből származó károkat minimalizálja és a Szolgáltatásokat a lehető legrövidebb időn belül helyreállítsa.
- (174.) Biztonsági esemény esetén – amennyiben az jelentős hatást gyakorol a szolgáltatásra vagy az annak keretében tárolt személyes adatokra –, Szolgáltató haladéktalanul, de legkésőbb az esetről való értesüléstől számított 24 órán belül értesíti az Érintett Feleket, valamint jelenti az incidenst a Bizalmi Felügyeletnek, valamint személyes adatok érintettsége esetén a {J7} GDPR 51. cikke szerinti illetékes hatóságnak.
- (175.) A bekövetkezett incidens kiértékelése alapján Szolgáltató meghozza a szükséges módosító, javító intézkedéseket, hogy az incidens jövőbeli előfordulását megakadályozza.

5.7.1. Rendkívüli események és kompromittálódás kezelésének eljárásai

- (176.) A Szolgáltató rendelkezik {D7} üzletmenet-folytonossági tervvel. Ez a dokumentum biztonsági okokból kifizetődően nem nyilvános.
- (177.) A rendkívüli üzemeltetési helyzetben a Szolgáltató dokumentálja az eseményeket, azok körülményeit, az elhárításukra megtett intézkedéseket.
- (178.) Rendkívüli üzemeltetési helyzetben a Szolgáltató életbe lépteti az üzletmenet folytonossági tervében megtervezett eljárásait annak érdekében, hogy az üzemeltetés helyreálljon az üzletmenet folytonossági tervben megjelölt időn belül.
- (179.) A helyreállítás időtartamát az esemény súlyossága, azaz az üzletmenet folytonossági terv szerint értelmezett osztályba sorolása határozza meg.
- (180.) Szolgáltató kialakította és fenntartja azt a tartalék rendszert, mely a rendkívüli üzemeltetési helyzetben képes a Szolgáltatás nyújtását és a nyilvános szabályzatok elérhetőségét, illetve közzétételét biztosítani.
- (181.) A rendkívüli üzemeltetési helyzet határidőn túli fennállása esetén a Szolgáltató haladéktalanul értesíti a Bizalmi Felügyeletet, az esemény bekövetkeztéről, annak hatásáról, várható időtartamáról, az elhárítás érdekében tett és tervezett intézkedésekről, továbbá a rendkívüli üzemeltetési helyzet megszűnéséről.
- (182.) A rendkívüli üzemeltetési helyzetben – amennyiben annak hátrányos kihatása van a Szolgáltatást igénybe vevő Előfizetőkre vagy az Érintett felekre – a Szolgáltató a lehető legrövidebb időn belül tájékoztatást tesz közzé internetes honlapján, valamint, lehetőség szerint, a DÁP szolgáltatón keresztül értesíti azokat a személyeket, akiket az esemény érint.

5.7.2. Sérült számítási erőforrások, szoftverek és/vagy adatok

- (183.) A Szolgáltató olyan megbízható rendszert működtet, mely redundáns műszaki megoldásokkal, biztonsági mentésekkel és eljárásokkal a rendszerben bekövetkezett hiba esetén is biztosítja a Szolgáltatások működtetését és elérhetőségét. A pontos és részletes előírásokat és intézkedéseket a Szolgáltató belső szabályzatai tartalmazzák.

5.7.3. Magánkulcs kompromittálódása esetén követendő eljárás

- (184.) A Szolgáltató a Szolgáltatás működéséhez szükséges magánkulcsának kompromittálódása esetére akciótervvel rendelkezik, melyet az üzletmenet folytonossági tervében tervezett meg. E szerint megteszi az alábbi főbb lépéseket:

- a) megszünteti az érintett magánkulcs használatát;
 - b) új szolgáltatói kulcspárt és tanúsítványt hoz létre;
 - c) értesíti a Bizalmi Felügyeletet;
 - d) értesíti a DÁP szolgáltatót.
- (185.) Szolgáltató az általa tárolt végfelhasználói (aláírói) magánkulcsok kompromittálódása esetére akciótervvel rendelkezik, melyet az üzletmenet folytonossági tervében tervezett meg. E szerint megteszi az alábbi főbb lépéseket:
- a) megszünteti az érintett magánkulcsok használatát;
 - b) értesíti az Aláírót és kezdeményezi az érintett tanúsítványok visszavonását;
 - c) intézkedik valamennyi érintett fél értesítéséről;
 - d) értesíti a DÁP szolgáltatót.

5.7.4. Üzletmenet folytonosság helyreállítás katasztrófát követően

- (186.) A Szolgáltató rendelkezik tartalék helyszínnel és informatikai rendszerrel, továbbá megtervezett eljárásokkal az áttelepülésre.
- (187.) A súlyos üzemzavar és a katasztrófa eseteit - többek között - az különbözteti meg egymástól, hogy katasztrófa esetén nagy valószínűséggel nem csak az informatikai rendszer, hanem annak fizikai környezete is megsemmisül részben vagy egészben. Ez utóbbi esetben egy válságstáb az üzletmenet folytonossági tervben meghatározott módon intézkedik a tartalék helyszínre való áttelepülésről és ott az informatikai rendszer szükséges mértékű visszaállításáról a tartalék helyszínen korábban elhelyezett mentések segítségével.

5.8. A szolgáltatási tevékenység megszüntetése

- (188.) A Szolgáltató rendelkezik olyan bankgaranciával, mely fedezi a szolgáltatási tevékenység megszüntetésének költségeit abban az esetben, ha Szolgáltató csődeljárás alá kerül vagy más okból kifolyólag nem képes önmaga fedezni a költségeket. Ha Szolgáltató ellen felszámolási, végelszámolási vagy egyéb kénysztörlési eljárás indult, erről és a felszámolóról vagy végelszámolóról Szolgáltató haladéktalanul tájékoztatja a Bizalmi Felügyeletet.
- (189.) A Szolgáltató az alábbi, a szolgáltatási tevékenység megszüntetésére vonatkozó tervvel rendelkezik:
- a) A tervezett megszűnés előtt kellő időben tárgyalásokat kezdeményez más minősített bizalmi szolgáltatókkal a Szolgáltatásokkal járó kötelezettségek - különösen az 5.5.1 fejezetben meghatározott adatoknak a megőrzése az 5.5.2 fejezetben megjelölt időtartamig- átadás-átvételéről.
 - b) A Szolgáltató gondoskodik a Szolgáltatások megszüntetéséből fakadó, a felhasználói közösséget érintő zavarok minimalizálásáról.
 - c) A megszüntetés előtt legalább 90 nappal korábban:
 - értesíti a Bizalmi Felügyeletet, és internetes honlapján tájékoztatja a felhasználói közösség tagjait;
 - beszünteti az új Szolgáltatás igénylések fogadását;
 - egy másik minősített bizalmi szolgáltatóval megállapodást köt a Szolgáltatásokkal járó kötelezettségek átadás-átvételéről, és ennek másolatát megküldi a Bizalmi Felügyeletnek;
 - d) A megszüntetés előtt legalább 20 nappal korábban:
 - beszünteti a Szolgáltatással kapcsolatos nyilvános szabályzatok közzétételét és gondoskodik arról, hogy ezzel egyidejűleg azok az átvevő szolgáltatónál elérhetővé váljanak;
 - a Szolgáltatás nyújtásához használt informatikai rendszer működtetéséhez szükséges infrastrukturális és vezérlő kulcsokat és azok mentéseit olyan módon semmisíti meg, hogy azok használata a továbbiakban már nem lehetséges;
 - e) A megszüntetés napjával:
 - Szolgáltató az informatikai rendszerében foglalt adatokról teljes körű, időbélyegzővel és elektronikus aláírással vagy bélyegzővel ellátott mentést készít. Szolgáltató a mentett adatállományokat védi a jogosulatlan módosítástól, és biztosítja, hogy az adatállomány tartalmához jogosulatlan személy nem férhet hozzá. Szolgáltató a megkötött szerződés révén biztosítja, hogy az adatok a megőrzési időn

belül az arra jogosult személyek számára hozzáférhetőek és értelmezhetőek maradjanak.

6. MŰSZAKI BIZTONSÁGI ÓVINTÉZKEDÉSEK

6.1. Kulcspár előállítás és telepítés

6.1.1. Kulcspár előállítás

6.1.1.1. Szolgáltatói kulcsok előállítása

(190.) A Szolgáltató a Szolgáltatás működéséhez szükséges kulcspárokat fizikailag védett környezetben, az erre szolgáló HSM modulban, legalább két bizalmi munkakört betöltő személy együttes részvételével generálja. A HSM modul megfelel a 6.2.1 fejezet szerinti követelményeknek, a magánkulcsok teljes életciklusuk alatt a HSM modulban maradnak.

6.1.1.2. Előfizetői kulcspárok előállítása

(191.) A Szolgáltató a végfelhasználói (aláíró) kulcspárok előállítására szolgáló DÁP-HSM modul üzembe helyezését szigorúan védett környezetben, legalább két bizalmi munkakört betöltő személy részvételével, illetéktelen személy jelenlétének kizárásával végzi, az előfizetői kulcspárok generálását megelőzően. A DÁP-HSM modul megfelel a 6.2.1 fejezet szerinti követelményeknek.

(192.) A Szolgáltató a 6.1.5 és 6.1.6 fejezetek szerinti algoritmusú és kulcshosszú végfelhasználói (aláíró) kulcspárt az erre szolgáló DÁP-HSM modulban, szigorúan védett környezetben, közvetlen emberi beavatkozás nélkül állítja elő, a {D9} BSZ-DÁP-TAN 4.3.1 pontja szerinti folyamat részeként. A DÁP-HSM modul megfelel a 6.2.1 fejezet szerinti követelményeknek, a magánkulcsok teljes életciklusuk alatt a DÁP-HSM modulban maradnak.

6.1.2. Magánkulcs eljuttatása a tulajdonoshoz

(193.) Összhangban a {D9} BSZ-DÁP-TAN 6.1.2 pontjával, a Szolgáltató az Aláíró magánkulcsát - annak teljes életciklusa során - abban a DÁP-HSM modulban tárolja, melyben a kulcspár előállítása megtörtént. Következésképpen magánkulcsok tulajdonoshoz történő eljuttatása nem szükséges és nem megengedett.

6.1.3. Nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz

(194.) A nyilvános kulcs eljuttatására a Szolgáltató két elkülönült egysége – a végfelhasználói kulcspárokat generáló és tároló DÁP-HSM és a minősített tanúsítványokat kibocsátó produktív hitelesítő központ - között kerül sor, a {D9} BSZ-DÁP-TAN 6.1.3 pontjában foglaltak szerint.

6.1.4. A szolgáltatói nyilvános kulcs közzététele

(195.) A Szolgáltató nem teszi közzé a DÁP keretében előállított magánkulcsok tárolt elhelyezésével kapcsolatos Szolgáltatás nyújtásához használt informatikai rendszer működtetéséhez szükséges infrastrukturális vagy vezérlő kulcspárokból a nyilvános kulcsot.

6.1.5. Kulcsméretek

(196.) A Szolgáltató Szolgáltatásai nyújtása során az {Sz2} ENISA ACM mindenkor legfrissebb verziója szerint megbízható, szabványos algoritmusokat, paramétereket és kulcshosszakat használ.

- (197.) A DÁP szolgáltatót hitelesítő kulcspár algoritmus és mérete: EC, secp384r1 [NIST P-384], 384 bit.
- (198.) Az előfizető DÁP HSM modulban tárolt aláírói kulcspárjának algoritmus és mérete: EC, secp384r1 [NIST P-384], 384 bit.
- (199.) Az előfizető DÁP keretalkalmazás által generált, az aláíró kulcs aktivizálásához használt üzenethitelesítő kulcspárjának algoritmus és mérete: EC, secp256r1 [NIST P-256], 256 bit.
- (200.) A Szolgáltató folyamatosan figyelemmel kíséri a technikai fejlődést és ennek függvényében szükség esetén, megfelelő időben gondoskodik az algoritmus váltásról vagy a kulcshosszak növeléséről.

6.1.6. A nyilvános kulcs paraméterek előállítása és megfelelőségének ellenőrzése

- (201.) A szolgáltatói kulcspárok előállítása a 6.1.1 fejezet szerint a vonatkozó jogszabályban előírt tanúsítással rendelkező HSM modulban, védett környezetben, legalább két bizalmi munkakört betöltő személy együttes részvételével, illetéktelen személy jelenlétét kizárva történik. A szolgáltatói kulcspárok generálása során a Szolgáltató betartja a HSM modul tanúsítási jelentésében foglalt előírásokat is.

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

- (202.) Az Aláírók DÁP-TK szolgáltatás keretében kezelt magánkulcsa kizárólag minősített elektronikus aláírás létrehozására használható. Szolgáltató a kapcsolódó végfelhasználói tanúsítványokban a BSZ-DÁP-TAN 6.1.7 pontja szerint jelzi a kulcshasználat célját.

6.2. Magánkulcs védelme és kriptográfiai modul műszaki szabályozások

6.2.1. Kriptográfiai modul szabványok és szabályozások

- (203.) A Szolgáltató a szolgáltatói magánkulcsok előállítására, tárolására és használatára olyan kriptográfiai modult alkalmaz, amely olyan megbízható rendszer, amelynek értékelése az {Sz6} ISO/IEC 15408 szerint, illetve azzal egyenértékű biztonsági kritériumok szerint 4-es vagy magasabb értékelési garancia szinten történt meg (EAL 4+).
- (204.) A Szolgáltató az Aláíró magánkulcsait olyan DÁP-HSM modulban tárolja és aktiválja, amely rendelkezik kijelölt tanúsító szervezet, vagy az Európai Unió valamely tagállamában nyilvántartásba vett, tanúsításra jogosult szervezet által kiadott igazolással, a minősített elektronikus aláírás létrehozó eszköz (QSCD) követelményeinek való megfelelésről.
- (205.) Az Aláíró magánkulcsokat tároló DÁP-HSM modul megnevezése: Entrust nShield Connect XC 12.60.15. A DÁP-HSM modul rendelkezik a {J1} eIDAS követelményeknek való megfelelésre vonatkozó tanúsítással, Common Criteria EAL4+ szinten, az AVA_VAN.5 és ALC_FLR.2 biztonsági garancia követelményekkel kiegészítve. A tanúsítvány, az értékelési jelentés és a biztonsági előírnyizat elérhetősége: <https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/singapore-common-criteria-scheme/product-list/nshield-solo-xc-hardware-security-module-version-12-60-15/>
- (206.) A DÁP-HSM-hez Entrust Signature Activation Module 1.1.1 kapcsolódik, mely QSCD tanúsítással rendelkezik: https://www.a-sit.at/wp-content/uploads/2025/06/VIG-25-040_QSCD-Certificate_Entrust-Final_sig-HL.pdf
- (207.) Szolgáltató biztosítja valamennyi, a QSCD eszköz tanúsítási jelentésében előírt követelmény teljesülését.

- (208.) A Szolgáltató legalább havonta ellenőrzi a QSCD tanúsított állapotának meglétét, a QSCD tanúsítás lejárati időpontját figyelemmel kíséri. A QSCD tanúsítás lejárata előtt megfelelő időben intézkedik a QSCD tanúsítás meghosszabbításáról vagy megújításáról.

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

- (209.) Szolgáltató alkalmazza a több szereplős "n-ből m" ellenőrzést minden, a Szolgáltatásban használt DÁP-HSM modul esetében, az adminisztrátori- és kulcsgondozási funkcióinak aktiválásánál.

6.2.3. Magánkulcs letét

- (210.) A Szolgáltató nem nyújt az Aláírók számára magánkulcs letét szolgáltatást.

6.2.4. Magánkulcs visszaállítása

- (211.) A Szolgáltató az Aláírók magánkulcsait a 6.2.5 a fejezetben leírt titkosított mentésből visszaállíthatja, hasonlóan szigorú fizikai, biztonsági óvintézkedések és eljárási szabályok betartásával, mint ahogy a kulcspárok előállítása eredetileg történt. A titkosított mentésből történő visszaállítás a DÁP-HSM modul erre szolgáló, tanúsítással rendelkező biztonsági funkciójával történik.

6.2.5. Magánkulcs mentése

- (212.) A Szolgáltató az Aláírók magánkulcsairól infrastrukturális kulcsain alapuló titkosított export állományok formájában biztonsági mentést készít. A titkosításhoz használt szolgáltatói infrastrukturális kulcs algoritmusa és hossza legalább olyan erős, mint az általa védett előfizetői kulcspárok algoritmusa, illetve hossza. A titkosított export állomány előállítása a DÁP-HSM modul erre szolgáló, QSCD tanúsítással rendelkező biztonsági funkciójával történik, védelme pedig megegyezik a DÁP-HSM modulban való tárolás védelmi szintjével.

6.2.6. Magánkulcs bejuttatása a kriptográfiai modulba

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

6.2.7. Magánkulcs kriptográfiai modulban történő tárolásának módja

- (214.) Az Aláírók magánkulcsai teljes életciklusuk alatt a 6.2.1 fejezetben leírt QSCD tanúsított DÁP-HSM modulban kerülnek tárolásra.

6.2.8. Magánkulcs aktiválásának módja

- (215.) A DÁP-TK Szolgáltatás nyújtásához használt informatikai rendszer működtetéséhez szükséges infrastrukturális és vezérlő kulcsok aktiválását Szolgáltató a DÁP-HSM modul gyártói dokumentációjában előírtak szerint végzi el.
- (216.) A Szolgáltató biztosítja, hogy az aktivált HSM modul és DÁP-HSM modul jogosulatlan hozzáférés ellen védett legyen.
- (217.) Az Aláíró magánkulcsának aktiválásához a DÁP keretalkalmazás által előállított üzenethitelesítő kulcspár magánkulcsa szükséges. Szolgáltató akkor aktiválja az Aláíró DÁP-HSM modulban tárolt magánkulcsát, ha az aláírási kérés az Aláíróhoz rendelt üzenethitelesítő nyilvános kulcs magánkulcs párjával

került hitelesítésre. Az üzenethitelesítő magánkulccsal történő hitelesítéshez Aláírónak a kapcsolódó tanúsítvány DÁP-TAN szolgáltatás keretében történt igénylésekor megadott és megerősített jelszó megadása szükséges a DÁP keretalkalmazásban.

(218.) Lásd még 6.4 Aktivizáló adatok.

6.2.9. Magánkulcs aktív állapotának megszüntetési módja

(219.) Minden sikeres elektronikus aláírás létrehozás művelet után a magánkulcs automatikusan inaktív állapotba kerül. Egy következő elektronikus aláírás létrehozás művelethez ismét el kell végezni a távoli aktiválást.

6.2.10. Magánkulcs megsemmisítésének módja

(220.) Új tanúsítvány igénylése esetén az Aláíró magánkulcsa a DÁP-HSM modulban törlésre, illetve felülírásra kerül.

(221.) A Szolgáltató a DÁP-HSM modulban tárolt aláírói (végfelhasználói) magánkulcsokat visszaállíthatatlan módon megsemmisíti az alábbi esetekben:

- a) a kapcsolódó tanúsítvány lejárt;
- b) a kapcsolódó tanúsítvány visszavonásra került.

(222.) A magánkulcs és az aktiválásához szükséges minden adat megsemmisítését olyan módon végzi, hogy annak végrehajtása után a magánkulcs semmilyen része ne legyen kikövetkeztethető vagy levezethető.

6.2.11. Kriptográfiai modul értékelése

(223.) Lásd a 6.2.1 fejezetben.

6.3. Kulcspár gondozás egyéb szempontjai

6.3.1. Nyilvános kulcs archiválása

(224.) A {D9} BSZ-DÁP-TAN 6.3.1 szerint.

6.3.2. Tanúsítvány érvényességi időszaka és kulcspár felhasználás időtartama

(225.) A {D9} BSZ-DÁP-TAN 6.3.2 szerint.

6.4. Aktivizáló adatok

6.4.1. Aktivizáló adatok előállítás

(226.) Az Aláíró magánkulcsának aktiválásához szükséges üzenethitelesítő magánkulcsot a DÁP keretalkalmazás generálja a mobil eszközre, majd a nyilvános kulcs párját továbbítja mind a Szolgáltatónak, mind pedig a DÁP szolgáltatónak. Szolgáltató az üzenethitelesítő nyilvános kulcsot a megfelelő aláíróhoz rendelve rögzíti a szolgáltatást megvalósító saját informatikai rendszerében.

(227.) Az Aláíró magánkulcsának aktiválásához szükséges üzenethitelesítő magánkulcs cseréje a DÁP keretalkalmazás újra telepítésével lehetséges, mely egyúttal a kapcsolódó aláíró tanúsítvány visszavonását és aláírókulcs törlését eredményezi.

6.4.2. Aktivizáló adatok védelme

(228.) Az aláírói magánkulcsokat aktivizáló adatok kizárólagos birtoklását és védelmét az Aláírónak kell biztosítania. Szolgáltató egyrészt azt biztosítja, hogy a DÁP-HSM modulban az előfizetői magánkulcshoz kapcsolódó aktivizáló adat kizárólag csak az Aláíró 3. fejezet szerinti sikeres azonosítását és hitelesítését követően legyen használható. Szolgáltató továbbá biztosítja, hogy amennyiben az Aláíró a kulcsaktiválás során egymást követően 5 alkalommal helytelenül adja meg az aktivizáló adatot, a DÁP szolgáltató az Aláíró számára megfelelő ideig elérhetetlenné tegye a DÁP-TK szolgáltatást.

6.4.3. Aktivizáló adatok egyéb szempontjai

(229.) Nincs kikötés.

6.5. Informatikai biztonsági óvintézkedések

6.5.1. Informatikai biztonsági műszaki követelmények meghatározása

(230.) Az informatikai biztonság műszaki követelményeit a Szolgáltató az {Sz1} EN 319 401, {Sz5} EN 419 241-1 és a {Sz3} TS 119 431-1 szabványok informatikai biztonsági műszaki követelményeiben határozza meg.

(231.) Ezek alapján Szolgáltató olyan megbízható informatikai rendszert (beleértve a redundáns kiépítést) és technikákat alakított ki és üzemeltet, melyek biztosítják a Szolgáltató megbízható működését a Szolgáltatások nyújtásához. Ennek ismertetését a Szolgáltató részben jelen szolgáltatási szabályzatban, részben a belső biztonsági szabályzataiban írja le.

6.5.2. Informatikai biztonsági értékelés

(232.) A Szolgáltató a minősített bizalmi szolgáltatásához kialakított és üzemeltetett informatikai rendszerét a {J9} 7/2024. (VI. 24.) MK rendelet 1. mellékletében felsorolt szempontok szerint biztonsági osztályba sorolta.

(233.) Szolgáltató az informatikai rendszerek biztonsági értékelését a {J8} Kiberbiztonsági. törvény rendelkezései szerint végzi.

(234.) Szolgáltató a Szolgáltatások nyújtásához kialakított és üzemeltetett informatikai rendszerével kapcsolatban teljesíti a {J10} NIS2 irányelv és a kapcsolódó {J11} 2024/2690 végrehajtási rendelet vonatkozó követelményeit.

6.6. Életciklusra vonatkozó műszaki óvintézkedések

6.6.1. Rendszerfejlesztési óvintézkedések

(235.) A Szolgáltató gondoskodik 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.

(236.) Az IT életciklusra vonatkozó rendszerfejlesztési szabályokat a Szolgáltató belső információbiztonsági szabályzata tartalmazza, amely pontosan meghatározza a tervezés és előkészítés, a projekt és kivitelezés, a működtetés és a menedzselés, valamint a visszacsatolás, illetve visszavonás/rekonstrukció ciklus időszakok feladatait és az alkalmazott módszertanokat. A belső információbiztonsági szabályzat figyelembe veszi az {Sz2} EN 319 401 szabvány 7.7 fejezetében előírt követelményeket

6.6.2. Biztonságkezelési óvintézkedések

- (237.) A Szolgáltató olyan eszközöket és eljárásokat alkalmaz, 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.
- (238.) A biztonságkezelési szabályokat a Szolgáltató PKI informatikai biztonságpolitikája {D5}, illetve biztonsági szabályzata {D6} tartalmazza.

6.6.3. Életciklus biztonsági óvintézkedések

- (239.) A Szolgáltató a belső szabályzatai szerinti rendszerességgel elvégzi 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

- (240.) A hálózati védelmi intézkedéseket a Szolgáltató {D6} biztonsági szabályzatában meghatározott követelményeknek megfelelően valósítja meg, melyek figyelembe veszik az {Sz1} EN 319 401 szabvány 7.8 fejezetében leírt követelményeket is..

6.8. Időforrások

- (241.) A Szolgáltatások nyújtásához használt megbízható rendszereket Szolgáltató 24 óránként legalább egyszer, megbízható időforrásokkal (NTP) szinkronizálja az UTC időhöz.
- (242.) A megbízható időforrások Szolgáltató saját rendszerén belüli, redundáns kialakítású, speciális célberendezések (referencia időforrások), melyek pontossága egy másodpercen belüli, és amelyek GPS alapúak, így visszavezethetőek az UTC időforrásra.

7. TANÚSÍTVÁNY, CRL ÉS OCSP PROFILOK

7.1. Tanúsítvány profil

- (243.) Az Aláíró kulcspárokhoz kibocsátott minősített tanúsítvány profilja megfelel a {D9} BSZ-DÁP-TAN bizalmi szolgáltatási szabályzat 7.1 fejezetében leírtaknak.

7.2. CRL profil

- (244.) Az Aláíró kulcspárok minősített tanúsítványaihoz – összhangban a {D9} BSZ-DÁP-TAN bizalmi szolgáltatási szabályzat 7.2 fejezetében leírtakkal – a Szolgáltató nem biztosít CRL-t.

7.3. OCSP profil

- (245.) Az Aláíró kulcspárokhoz kibocsátott minősített tanúsítványok visszavonási állapotának ellenőrzéséhez használható OCSP válaszok profilja megfelel a {D9} BSZ-DÁP-TAN bizalmi szolgáltatási szabályzat 7.3 fejezetében leírtaknak.

8. MEGFELELŐSÉG VIZSGÁLAT ÉS EGYÉB ÉRTÉKELÉSEK

(246.) Jelen bizalmi szolgáltatási szabályzat tartalmazza a DÁP TK bizalmi szolgáltatás nyújtása során teljesítendő valamennyi követelményt, melyeket különösen az alábbi szabványok határoznak meg:

- a) EN 319 401: General policy requirements for Trust Service Providers {Sz1}
- b) TS 119 431-1: Policy and security requirements for Trust Service Providers;
Part 1: TSP service components operating a remote QSCD/SCDev {Sz3}
- c) EN 419 241-1: Trustworthy Systems Supporting Server Signing;
Part 1: General System Security Requirements {Sz5}

8.1. Vizsgálatok gyakorisága és körülményei

(247.) A Szolgáltató vizsgálatának gyakorisága és körülményei megfelelnek a hatályos jogszabályi előírásoknak.

(248.) A Szolgáltató legalább 24 havonta egyszer megfelelőségértékelést és 12 havonta egyszer felülvizsgálatot végeztet a {J1} eIDAS 3. cikk 18. bekezdésben meghatározott megfelelőségértékelő szervezettel, a {J1} eIDAS, illetve a {J2} DÁP tv. követelményeinek való megfelelés tárgykorban. Szolgáltató az elkészült megfelelőségértékelés jelentést annak kézhezvételétől számított három munkanapon belül benyújtja a Bizalmi Felügyeletnek.

(249.) 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

(250.) A megfelelőségértékelés, az NKI által végzett ellenőrzés és a kiberbiztonsági audit előkészítésére, illetve az információbiztonsági rendszer ellenőrzésére Szolgáltató külső rendszervizsgálót alkalmazhat.

(251.) A külső rendszervizsgáló által végzett auditokat Szolgáltató olyan szakértővel vagy szakértői szolgáltatásokat nyújtó szervezettel végezteti el, aki független 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.

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

(253.) A megfelelőségértékelési vizsgálatot a Szolgáltató olyan, a {J6} 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

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

8.4. Audit során vizsgált területek

(255.) 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.

(256.) 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.

(257.) A kiberbiztonsági audit az alábbi – a megfelelőségértékeléssel jelentős átfedésben lévő – kiberbiztonsági követelménycsoportok teljesülését vizsgálja:

- 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

(258.) Az üzemszerű ellenőrzések, belső és külső auditok, szakértői elemzések által feltárt hiányosságok, hibás gyakorlatok kezelésére a Szolgáltató intézkedési tervet készít. A hiányosságokat késlekedés nélkül orvosolja, az intézkedéseket dokumentálja és ellenőrzi.

(259.) A Bizalmi Felügyelet által végzett rendszeres helyszíni ellenőrzések során feltárt esetleges hiányosságokat Szolgáltató a hatóság által megállapított határidőn belül megszünteti a hatályos jogszabályok alapján és a hatóságtól kapott információk és ajánlások figyelembevételével.

8.6. Eredmény kommunikációja

(260.) A belső és külső auditot, szakértői elemzést végző személyek csak a megbízójuknak adhatnak információt a Szolgáltató tevékenységével kapcsolatban.

(261.) A megfelelőségértékelés, az NKI által végzett ellenőrzés, a kiberbiztonsági audit, valamint az információbiztonsági rendszer ellenőrzés eredményei a Szolgáltató bizalmas üzleti információi, ezért azokat a társaság titokvédelmi előírásai szerint kell kezelni. Szolgáltató nem köteles a konkrét hiányosságot nyilvánosságra hozni.

(262.) A hiányosságok felszámolásáról a Felügyeleti Szervet az arra megállapított határidőn belül, de legkésőbb a következő helyszíni ellenőrzés során tájékoztatni kell.

9. EGYÉB ÜZLETI ÉS JOGI KÉRDÉSEK

9.1. Díjak

(263.) Szolgáltató a magánkulcsok tárolásáért, annak távoli aktiválásáért és az Aláírás Érték kiszámításáért Aláíró részére díjat nem számít fel.

9.2. Anyagi felelősség

(264.) A Szolgáltató anyagi felelősségének mértékéről, illetve annak korlátairól a {D1} Általános Szerződési Feltételek rendelkezik.

9.2.1. Biztosítási fedezet

(265.) A Szolgáltató rendelkezik olyan felelősségbiztosítással, mely egyaránt kiterjed az elektronikus aláírással, illetve az ezzel ellátott elektronikus dokumentummal szerződésen kívül okozott károkra és szerződésszegéssel okozott károkra, és amely fedezetet biztosít az összes károsultnak okozott kárra, a szolgáltatói felelősségvállalás maximális értékéig.

(266.) A szolgáltatói felelősségvállalás maximális összege:

- a) tanúsítványonként és káreseményenként 50 millió magyar forint (HUF);
- b) éves szinten 1 milliárd magyar forint (HUF).

(267.) A felelősségbiztosítás a fentiekén túl kiterjed az alábbiakra is:

- a) a {J2} DÁP tv. 92. §-ban foglalt kötelezettsége nem teljesítése miatt a Bizalmi Felügyeletnél felmerült, a DÁP tv. 93. § (1) bekezdése szerinti költségekre;
- b) a {J1} eIDAS 17. cikk (4) bekezdés e) pontja alapján a Felügyelet Szerv által felkért megfelelőségértékelő szervezet eljárásainak költségeire, ha ezt a Bizalmi Felügyelet eljárási költségként érvényesíti.

9.2.2. További követelmények

(268.) Szolgáltató rendelkezik a {J5} 24/2016 rendelet 20. §-a szerinti, huszonötmillió forint összegű, feltétel nélküli és visszavonhatatlan bankgaranciával.

9.2.3. Felelősségbiztosítás vagy garancia végfelhasználók számára

(269.) Nincs kikötés.

9.3. Üzleti információk bizalmassága

9.3.1. Bizalmasan kezelendő információk köre

(270.) A Szolgáltató minden olyan adatot és információt bizalmasnak tekint, melyek nem kerültek tételes felsorolásra a 9.3.2 fejezetben, különös tekintettel az Aláíró magánkulcsára.

9.3.2. Bizalmasnak nem tekintett információk köre

(271.) Nem bizalmasnak tekintett információk az alábbiak:

- a) a szolgáltatói tanúsítványok és az azokban foglalt adatok;
- b) a tanúsítványokhoz kapcsolódó visszavonási információk;
- c) a Szolgáltató internetes honlapján közzétett nyilvános információk, szabályzatok és egyéb dokumentumok;
- d) az olyan adatok, melyek nyilvános adatforrásból elérhetők.

9.3.3. Bizalmas információk védelmének felelőssége

(272.) A Szolgáltató a bizalmas információkhoz való hozzáférést csak az arra feljogosított személyek és szervezetek számára teszi lehetővé. A bizalmas információk védelmét a személyzet megfelelő képzésével, továbbá a munkavállalókkal, szerződéses partnerekkel megkötött szerződésekkel juttatja érvényre.

9.4. Személyes adatok védelme

9.4.1. Adatvédelem

(273.) A Szolgáltató rendelkezik mind társasági szintű adatvédelmi szabályzattal, mind pedig a Szolgáltatásokra vonatkozó adatvédelmi tájékoztatóval {D4}, melyek összhangban vannak a nemzetközi és hazai vonatkozó jogszabályokkal.

(274.) Szolgáltató adatvédelmi tájékoztatója {D4} elérhető Szolgáltató internetes honlapján.

9.4.2. Bizalmasként kezelendő személyes adatok

(275.) A Szolgáltató a DÁP-TK szolgáltatás keretében tárolt magánkulcsokat, a magánkulcsok aktiválásához szükséges adatokat, valamint az aláírási kéréseket bizalmasan kezeli.

9.4.3. Bizalmasként nem kezelendő személyes adatok

(276.) A Szolgáltató a DÁP-TK szolgáltatás keretében nem kezel bizalmasnak nem tekinthető személyes adatokat.

9.4.4. Személyes adatok védelmének felelőssége

(277.) Szolgáltató gondoskodik a személyes adatok védelméről, működése és szabályzatai megfelelnek a {J7} GDPR rendelkezéseinek.

9.4.5. Személyes adatok felhasználásának elfogadása

(278.) Aláírónak a {D1} ÁSZF-DÁP elfogadásával létrejött Szolgáltatási Szerződés keretében tudomásul kell vennie a szolgáltatások igénybevételéhez szükséges adatok Szolgáltató által történő kezelését és tárolását. Tekintettel arra, hogy a Szolgáltató adatkezelésének jogalapja jogi és szerződési kötelezettség teljesítése, a {J7} GDPR szerinti hozzájárulás nem értelmezhető.

9.4.6. Felfedés hatósági vagy polgári peres eljárás keretében

(279.) A Szolgáltató 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 feltárja a jogszabályban

meghatározott bizalmas információkat. Szolgáltató rögzíti az adatátadás tényét, de arról nem tájékoztatja az érintett Aláíró.

9.4.7. Egyéb, felfedést eredményező körülmények

- (280.) Szolgáltató a szolgáltatási tevékenység, illetve a Szolgáltatások nyújtásának megszüntetése esetén Aláíró adatait a jogszabályi kötelezettségeire tekintettel átadja harmadik félnek.

9.5. Szellemi tulajdonjogok

- (281.) A Szolgáltató által az Aláíró részére generált kulcspár tulajdonosa és teljes jogú használója az Aláíró, tekintet nélkül arra a fizikai közegre, amely tárolja és védi a kulcsokat.
- (282.) A szolgáltatói tanúsítványok a Szolgáltató tulajdonát képezik. A visszavonási információk a Szolgáltató tulajdonát képezik.
- (283.) 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

- (284.) A Szolgáltató felel a bizalmi szolgáltatási rendben és jelen szolgáltatási szabályzatban, valamint az Aláíróval az ÁSZF elfogadásával létrejött Szolgáltatási Szerződésben megfogalmazott valamennyi kötelezettség maradéktalan betartásáért, még akkor is, ha a Szolgáltatások nyújtásához kapcsolódó egyes feladatokat a Közreműködő Felek vagy egyéb alvállalkozók végzik.
- (285.) A Szolgáltató a vele szerződéses jogviszonyban nem álló harmadik személlyel szemben a {J4} Polgári Törvénykönyv 6:519. §-a szerint, a vele szerződéses jogviszonyban álló Aláíróval szemben a szerződésszegésért való felelősség ({J4} Polgári Törvénykönyv 6:142. §) szabályai szerint felelős az elektronikus aláírással hitelesített elektronikus dokumentummal okozott kárért, ha megszegte a bizalmi szolgáltatási rendben és a jelen szolgáltatási szabályzatban, valamint az Aláíróval az ÁSZF elfogadásával létrejött Szolgáltatási Szerződésben előírtakat, vagy a {J1} eIDAS szerinti, rá vonatkozó kötelezettségeket. E kötelezettségek megtartását kétség esetén Szolgáltatónak kell bizonyítania. Szolgáltató sajátjaként felel a Közreműködő Felek vagy egyéb alvállalkozók által a Szolgáltatások nyújtása során okozott kárért.
- (286.) A Szolgáltató a felelősségi körén belül keletkezett, bizonyított károkért, az Aláíróval, a {D1} ÁSZF-DÁP elfogadásával létrejött szerződéses viszonyban és a 9.8 fejezetben foglalt korlátozásokkal kártérítést fizet.
- (287.) A Szolgáltató nem felel:
- a) az Aláírónak a Szolgáltató által tárolt magánkulcsa távoli aktiválásával kapcsolatos tevékenységért;
 - b) az Érintett Felek tanúsítvány ellenőrzési és felhasználási tevékenységeiért;
 - c) az Érintett Felek vagy mások által kibocsátott szabályzatokért.

9.6.1.1. Szolgáltató kötelezettsége

- (288.) Szolgáltató azzal, hogy jelen szolgáltatási szabályzat hatálya alatt tárolja az általa generált, aláírói tanúsítványhoz kapcsoló magánkulcsot, arra vállal kötelezettséget, hogy a Szolgáltatások nyújtása során ő maga és a Szolgáltatások nyújtásában Közreműködő Felek jelen szabályzatban foglaltakat maradéktalanul

betartják. Szolgáltató megteszi a szükséges és tőle telhető intézkedéseket ahhoz, hogy Aláírók is jelen szabályzat előírásainak megfelelően járjanak el.

9.6.2. A regisztrációs szervezet felelőssége

(289.) Jelen bizalmi szolgáltatási szabályzat által tárgyalt Szolgáltatáshoz nem kapcsolódik regisztrációs szervezet.

9.6.3. Aláíró felelőssége és helytállása

(290.) Az Aláíró jogosult:

- a) a számára előállított kulcspárt az 1.4.1 fejezetben leírt célokra és jelen szabályzatban leírt módon használni;
- b) a tárolt kulcshoz kapcsolódó egyéb szolgáltatásokat használni a jelen szabályzatban leírt módon.

(291.) Az Aláíró felelős:

- a) a magánkulcs aktivizáló kódjainak a biztonságos kezeléséért;
- b) azért, hogy a magánkulcs és a kapcsolódó tanúsítvány használatát haladéktalanul és végérvényesen beszüntesse, amennyiben tudomására jut, hogy a Szolgáltató valamely, a tanúsítvány kibocsátásában érintett hitelesítő központja kompromittálódott;
- c) a Szolgáltatót haladéktalanul értesíteni és teljes körűen tájékoztatni vitás ügyekben;
- d) a {D1} Általános Szerződési Feltételekben meghatározott kötelezettségei betartásáért.

(292.) Az Aláíró köteles:

- a) a Szolgáltató által kért, a Szolgáltatás igénybevételéhez szükséges adatokat hiánytalanul és a valóságnak megfelelően megadni;
- b) adat változás esetén haladéktalanul írásban értesíteni erről Szolgáltatót, és beszüntetni a kulcspár használatát;
- c) biztosítani, hogy a Szolgáltatás igénybevételéhez szükséges adatokhoz és eszközökhöz illetéktelen személy ne férhessen hozzá;
- d) jogellenes használat gyanúja esetén a Szolgáltató megkereséseire a Szolgáltató által megadott időtartamon belül reagálni;
- e) haladéktalanul, írásban értesíteni Szolgáltatót, ha a Szolgáltatás felhasználásával létrehozott elektronikus aláírással kapcsolatban jogvita indul.

9.6.4. Érintett Felek felelőssége és helytállása

(293.) Az Érintett Felek a saját belátásuk és/vagy szabályzataik szerint dönthetnek az egyes tanúsítványok elfogadásáról és a felhasználás módjáról. A tanúsítvány érvényességének elbírálása során az Érintett Félnek megfelelő körültekintéssel kell eljárnia, ezért különös tekintettel javasolt:

- a) a szolgáltatási szabályzatban foglalt követelmények és előírások betartása;
- b) megbízható informatikai környezet és alkalmazások használata;
- c) a tőle elvárható magatartás tanúsítása az elektronikus aláírás érvényesítésekor.

(294.) A Szolgáltató kizárja a felelősségét (9.8 fejezet) amennyiben az Érintett Fél az elektronikus aláírás elfogadásakor nem körültekintően, vagy nem a tőle elvárható gondossággal jár el.

9.6.5. Egyéb felek felelőssége és helytállása

(295.) Nincs kikötés.

9.7. Helytállás érvénytelenségi köre

(296.) Szolgáltató kizárja felelősségét, amennyiben:

- a) az Érintett Fél nem körültekintően jár el az elektronikus aláírások ellenőrzése és felhasználás során, azaz nem a mérvadó műszaki szabványoknak vagy a hatályos jogszabályoknak megfelelően jár el;
- b) az Aláíró nem tartja be a magánkulcs aktiválódásának kezelésével kapcsolatos előírásokat;
- c) az Érintett Felek vagy mások által kibocsátott szabályzatok nem felelnek meg a mérvadó műszaki szabványoknak vagy a hatályos jogszabályoknak;
- d) az Internet, vagy annak egy részének működési hibájából fakadóan tájékoztatási vagy egyéb kommunikációs kötelezettségeit nem tudja ellátni;
- e) az Aláíró nem tesz eleget a szolgáltatási szabályzatban előírt kötelezettségeinek.

9.8. Felelősség korlátozása

(297.) A Szolgáltató korlátozza a kártérítési felelősségét a Szolgáltatás keretében történt összes elektronikus aláírással hitelesített dokumentumokat érintően Szolgáltató hibájából bekövetkezett káreseménnyel kapcsolatban fizetendő kártérítési összeg tekintetében.

(298.) Szolgáltató nem felelős az olyan károkért, melyek abból adódnak, hogy az Aláíró nem a jelen BSZ-DÁP-TK-ban foglaltak szerint használja a szolgáltatást.

(299.) A Szolgáltató nem felelős az olyan károkért, melyek abból adódnak, hogy az Érintett Fél a Szolgáltatás keretében létrejött elektronikus aláírások ellenőrzése és felhasználása során nem a hatályos jogszabályok és a mérvadó műszaki szabványok szerint járt el, illetve nem tanúsította a tőle elvárható gondosságot, illetve megatartást.

(300.) A Szolgáltató pénzügyi felelősségének mértékét a {D1} Általános Szerződési Feltételek határozza meg. Ha egy biztosítási eseménnyel kapcsolatban több jogosult megalapozott kártérítési igénye meghaladja ezt az összeget, akkor az egyes kártérítési igények megtérítése az összes kártérítési igénynek a megadott összeghez viszonyított arányában történik.

9.9. Kártérítések

(301.) A kártérítésekről a jelen szabályzat 9.8 fejezetében leírtakon túl a {D1} Általános Szerződési Feltételek rendelkezik.

9.10. Hatályosság és megszűnés

9.10.1. Hatályosság

9.10.1.1. Időbeli hatály

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

9.10.1.2. Tárgyi hatály

(303.) A szolgáltatási szabályzat tárgyi hatálya kiterjed a Szolgáltatások nyújtására és igénybevételére.

9.10.1.3. Személyi hatály

(304.) A szolgáltatási szabályzat személyi hatálya kiterjed Szolgáltatónak, illetve a Közreműködő Feleknek a Szolgáltatások nyújtásában közreműködő munkatársaira és az Aláírókra.

9.10.2. Megszűnés

(305.) A bizalmi szolgáltatási szabályzat a Szolgáltató szolgáltatási tevékenységének befejezésével tekintendő megszűntnek.

9.10.3. Megszűnés után is hatályban maradó rendelkezések

(306.) A megszűnés után is hatályban maradó rendelkezéseket – amennyiben ilyenek vannak - a {D1} Általános Szerződési Feltételek tartalmazza.

9.11. Egyéni hirdetmények és kommunikáció a részvevőkkel

(307.) Azokban az esetekben, melyekre jelen szolgáltatási szabályzat nem rendelkezik a felek közötti értesítésről, illetve annak joghatást kiváltó módjáról, a Szolgáltató értesítése elektronikusan aláírással hitelesítve az ekozig@1818.hu email címre beküldéssel történik. Az elektronikus értesítés csak a Szolgáltató általi visszaigazolást követően tekinthető kézbesítettnek. Szolgáltató a megkeresésekre 30 napon belül válaszol elektronikus aláírással ellátott válasz üzenetben.

9.12. Módosítások

9.12.1. Módosítás eljárása

(308.) A szolgáltatási szabályzat módosítása az 1.5.3 és 1.5.4 fejezetekben leírt szabályok szerint történik. A szolgáltatási szabályzat módosulását a verziószám megfelelő változása jelzi.

9.12.2. Értesítés módszere és időtartama

(309.) A Szolgáltatások jelentős vagy lényeges változása esetén Szolgáltató internetes honlapján közleményt tesz közzé és emailben tájékoztatást küldhet, a hatályba lépést megelőzően kellő időben ahhoz, hogy az érintett a felek a változásokra felkészülhessenek.

9.12.3. OID megváltozását előidéző körülmények

(310.) A szolgáltatási szabályzat OID-ja nem változik.

9.13. Vitás kérdések rendezése

(311.) Bármely vitás kérdés felmerülése esetén Aláírónak kötelessége a Szolgáltató haladéktalan értesítése és teljes körű tájékoztatása a kérdés minden vonatkozását illetően, a vita jogi útra terelése előtt.

(312.) Panaszt a Telefonos Ügyfélszolgálat felé a 1818 hívószámán telefonon, vagy e-mailben az ekozig@1818.hu címre küldve lehet előterjeszteni Szolgáltató részére. Szolgáltató visszaigazolást küld a panasz kézhezvételéről. A panaszt a Szolgáltató az előterjesztéstől számított 30 napon belül kivizsgálja és ennek eredményéről a panaszost elektronikus aláírással ellátott válasz üzenetben tájékoztatja.

- (313.) Bármely vitás kérdés felmerülése esetén Aláíró jogosult az esetleges bírósági eljárást megelőzően békéltető testülethez fordulni. Az illetékes békéltető testület megnevezését és elérhetőségeit jelen szabályzat 1.5.2 fejezete tartalmazza.
- (314.) A jogviták esetén követendő eljárást a {D1} Általános Szerződési Feltételek tartalmazza.

9.14. Irányadó jog

- (315.) 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

- (316.) A Szolgáltató tevékenységét a mindenkor hatályos Európai Unió, illetve magyar jogszabályoknak megfelelően végzi.

9.16. Vegyes rendelkezések

9.16.1. Teljességi záradék

- (317.) Nincs kikötés.

9.16.2. Átruházás

- (318.) A Szolgáltatások nyújtásában érintett Közreműködő Felek vagy alvállalkozók csak a Szolgáltató előzetes írásbeli felhatalmazásával vagy jogszabályi felhatalmazás alapján adhatják tovább jogosultságaikat és delegálhatják kötelezettségeiket harmadik félnek.

9.16.3. Részleges érvénytelenség

- (319.) A jelen szolgáltatási szabályzat egyes rendelkezéseinek tetszőleges okból történő érvénytelenné válása esetén a többi rendelkezés változatlan formában érvényben marad.

9.16.4. Igényérvényesítés

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

9.16.5. Force Majeure (Vis maior)

- (321.) Vis maior: Az olyan – a Szolgáltató és a Közreműködő Felek akaratától, cselekedeteitől és személyétől függetlenül bekövetkező és érdekkörén kívül eső elháríthatatlan – esemény (pl. sztrájk, háború, polgári felkelés, természeti katasztrófa, a Felek bármelyikének partnerénél felmerülő elháríthatatlan fizikai vagy jogi akadály vagy más elháríthatatlan sürgősségi helyzet) minősül vis maiornak, amely megakadályozza vagy lehetetlenné teszi a jelen szolgáltatási szabályzatban foglalt követelmény teljesítését, feltéve, hogy ezen körülmények a jelen szolgáltatási szabályzat hatálybalépését követően keletkeznek, illetőleg azt megelőzően következtek be, ám a jelen szolgáltatási szabályzat teljesítésére kiható következményeik az említett időpontban még nem voltak előre láthatóak.
- (322.) A Szolgáltató nem felelős a vis maior esetekből fakadó károkért.

9.17. Egyéb rendelkezések

9.17.1. Hozzáférhetőség a fogyatékossgal élő személyek számára

(323.) A Szolgáltató a Szolgáltatásokat és a Szolgáltatások során alkalmazott végfelhasználó termékeket hozzáférhetővé teszi a fogyatékossgal élő személyek számára, amennyiben az lehetséges.