NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.

Szolgáltatási kivonat
a DÁP eAláírás szolgáltatáshoz
(PDS-DÁP)

A NISZ Zrt. Digitális Állampolgárság Program keretében nyújtott minősített tanúsítványszolgáltatásának és a hozzá kapcsolódó távoli elektronikus aláírást létrehozó eszköz kezelése és elektronikus aláírások létrehozása minősített bizalmi szolgáltatás szolgáltatási kivonata

Verziószám	**1.1**
Objektum azonosító (OID)	**0.2.216.1.200.1100.100.42.3.1.40**
Hatályba lépés dátuma	**2024.12.20.**
Dokumentum besorolása	**nyilvános**
Jóváhagyó	**Adorján István**

Adorján István

Digitálisan aláírta: Adorján István
Dátum: 2024.12.17 17:05:03 +01'00'

Változáskezelés

Verzió	Dátum	A változás leírása	Készítette/Módosította	Ellenőrizte	Jóváhagyta
0.1	2024.12.01	Új PDS dokumentum (PDS-DÁP) első kezdeti (v0.1) verziója	ACPM	Kővári-Szabó Zoltán Nagy Benjámin	-
1.0	2024.12.07.	Első jóváhagyott verzió	Kővári-Szabó Zoltán	Nagy Benjámin	Adorján István
1.1	2024.12.17	Aláírásformátum pontosítása és hatálybalépés dátumának módosítása.	Kővári-Szabó Zoltán	Nagy Benjámin	Adorján István

Tartalom

1. Bevezetés

Jelen dokumentum a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. (továbbiakban **Szolgáltató**) által nyújtott alábbi minősített bizalmi szolgáltatásokra vonatkozó szolgáltatási kivonata (a továbbiakban: Szolgáltatási Kivonat):

- A Digitális Állampolgárság Program (a továbbiakban: **DÁP**) keretében az állampolgárok, mint természetes személyek számára elektronikus aláírás célú EU minősített tanúsítvány kibocsátása, ezen tanúsítványokhoz kapcsolódóan visszavonási és tanúsítvány állapot információk biztosítása (a továbbiakban **DÁP-TAN szolgáltatás**) A DÁP-TAN szolgáltatás a {J1} eIDAS 3. cikk 16. pont a) alpontjának megfelelő alábbi bizalmi szolgáltatásnak felel meg:

  elektronikus aláírások tanúsítványainak kibocsátása

- A Digitális Állampolgárság Program (DÁP) keretében távoli elektronikus aláírás létrehozó eszköz kezelése és elektronikus aláírások létrehozása (a továbbiakban**: DÁP-TK szolgáltatás)** A DÁP-TK szolgáltatás a {D11} 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:
  - elektronikus aláírások létrehozása;
  - távoli elektronikus aláírás létrehozó eszköz kezelése.

A DÁP-TAN szolgáltatás és a DÁP-TK szolgáltatás jelen Szolgáltatási Kivonatban együttesen Szolgáltatásként (a továbbiakban: **Szolgáltatás**) kerül feltüntetésre.

A Szolgáltatás megfelel az eIDAS Rendelet által támasztott követelményeknek, a minősített bizalmi szolgáltatások megfelelősségét a Hunguard Kft. mint független megfelelőségértékelő szervezet ellenőrizte.

1.1. Áttekintés

Tekintettel arra, hogy a Szolgáltató a bizalmi szolgáltatás keretében az Aláírók számára tanúsítványt bocsát ki, az Aláírók részére jelen Szolgáltatási Kivonatot is elérhetővé teszi.

A jelen Szolgáltatási Kivonat egy adott verziójának időbeli hatálya a címlapon feltüntetett hatályba lépés dátumával kezdődik, és határozatlan időre szól. Az időbeli hatály megszűnik a Szabályzat újabb verziójának hatályba lépésével vagy amennyiben a Szolgáltató jövőre nézve beszünteti a jelen Szolgáltatási Kivonat szerinti bizalmi szolgáltatás nyújtását.

A Szolgáltatási Kivonat módosulását a verziószám megfelelő változása jelzi. A Szabályzat módosítása esetén a Szolgáltató a módosulás hatályba lépésének napja előtt 30 nappal közzéteszi internetes honlapján a módosult Szabályzatot.

1.1.1. A Szolgáltató adatai

Szolgáltató neve:	**NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.**
Cégjegyzék szám:	Cg. 01-10-041633
Székhely:	1149 Budapest, Róna utca 52-80.
Levelezési cím:	1389 Budapest, Pf.: 133.
Telefonszám:	(36-1) 459-4200
Internetes honlap címe:	http://www.nisz.hu/
Szolgáltatás internetes honlapjának címe:	*http://*hiteles.gov.hu és dap.gov.hu

1.1.2. Felügyeleti szerv

A Szolgáltató felügyeleti szerve a Nemzeti Média- és Hírközlési Hatóság (továbbiakban: „**Bizalmi Felügyelet**”).

A Bizalmi Felügyelet ellátja a Szolgáltató és az általa nyújtott Szolgáltatás felügyeletét, ellenőrzi a Szolgáltatás jogszabályi megfelelőségét. Többek között, figyelemmel kíséri a bizalmi szolgáltatásokkal kapcsolatos technológia és kriptográfiai algoritmusok fejlődését, továbbá jogerős és végrehajtható határozatában elrendelheti a bizalmi szolgáltatások keretében kibocsátott tanúsítványok felfüggesztését vagy visszavonását.

Szolgáltató a Szolgáltatást 2024. július 31. napján jelentette be a Bizalmi Felügyeletnek, mint minősített bizalmi szolgáltató.

A Bizalmi Felügyelet elérhetősége: *https://nmhh.hu/cikk/205215/A_szerv_hivatalos_neve_szekhelye_postai_cime_telefon_es_telefaxszama_elektronikus_levelcime_honlapja_ugyfelszolgalatanak_elerhetosegei*

A Bizalmi Felügyelet által közzétett magyar bizalmi szolgáltatók listájának elérhetősége:

http://www.nmhh.hu/tl/pub/HU_TL.xml (géppel feldolgozható formátum)
http://www.nmhh.hu/tl/pub/HU_TL.pdf (olvasható formátum)

1.1.3. Megfelelőségértékelés

A Szolgáltatás megfelel az eIDAS Rendelet által támasztott követelményeknek, a minősített bizalmi szolgáltatások megfelelősségét a Hunguard Kft. mint független megfelelőségértékelő szervezet ellenőrizte.

A megfelelőségértékelési jelentés tanúsítványának azonosítója: [kiadása folyamatban]

A Szolgáltató jogosult a 910/2014 EU rendelet 23. cikke szerinti „uniós bizalmi jegy” használatára:

1.1.4. Fogyatékkal élők

A Szolgáltató az erre vonatkozó jogszabályi kötelezettségeinek betartásán túl törekszik arra, hogy az általa nyújtott szolgáltatásokhoz biztosítsa az egyenlő esélyű hozzáférést.

Szolgáltató minden rendelkezésre álló megoldással törekszik a diszkriminációmentes kiszolgálásra és egyenlő bánásmódra.

1.1.5. Egyenlő bánásmód

A szolgáltatás elérését biztosító nyilvános felületek biztosítják, hogy azokat a fizikai, látási, hallási, értelmi és kognitív fogyatékossággal küzdő emberek is képesek legyenek használni. Az ügyfélszolgálati munkatársak felkészítése révén a fogyatékkal élők támogatást kapnak a szolgáltatás használatával kapcsolatban. A webes felületek, alkalmazások támogatják a szövegfelolvasó szoftverek használatát, a gyengénlátók számára kontrasztos megjelenítési mód áll rendelkezésre.

1.2. A Dokumentum neve és azonosítása

1.2.1. A dokumentum neve

A Szolgáltatási kivonat teljes neve, azonosítója és verziószáma a címlapon található.

1.2.2. A dokumentum azonosítása

A Szolgáltatási kivonat a {J5} 24/2016 BM rendelet 3. § (3) bekezdése szerinti szolgáltatási kivonat, mely a DÁP-TAN és a DÁP-TK szolgáltatásokra vonatkozó, a Szolgáltató weboldaláról letölthető alábbi szabályozási dokumentumok rendelkezéseivel összhangban, tömören, jól áttekinthető módon, összefoglaló jelleggel tartalmazza a Szolgáltatás főbb ismertetőit.

Szolgáltatási rendek

(Előírják azokat a követelményeket, amelyeknek a Szolgáltató meg kell, hogy feleljen.)

- Bizalmi Szolgáltatási Rend a Digitális Állampolgárság Program keretében kibocsátott minősített tanúsítványokhoz (BR-DÁP-TAN); OID: 0.2.216.1.200.1100.100.42.3.1.36
- 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); OID: 0.2.216.1.200.1100.100.42.3.1.37

Szolgáltatási szabályzatok

(Leírják, hogy a Szolgáltató hogyan teljesíti ezeket a követelményeket, és leírja azokat a gyakorlatokat, amelyeket az Szolgáltató alkalmaz.)

- Bizalmi Szolgáltatási Szabályzat a Digitális Állampolgárság Program keretében kibocsátott minősített tanúsítványokhoz (BSZ-DÁP-TAN); OID: 0.2.216.1.200.1100.100.42.3.1.38

- Bizalmi Szolgáltatási Szabályzat a Digitális Állampolgárság Program keretében nyújtott elektronikus aláírások létrehozása és távoli elektronikus aláírást létrehozó eszközök kezelése minősített bizalmi szolgáltatáshoz (BSZ-DÁP-TK); OID: 0.2.216.1.200.1100.100.42.3.1.39

A Szolgáltatási kivonat egyúttal az {Sz2} ETSI EN 319 411-1 szabvány szerinti ún. „*PKI disclosure statement*”-nek (PDS) tekintendő.

1.2.3. A dokumentum hatálya

A dokumentum jelen verziója visszavonásig hatályos.

A hatályosság megszűnik a szolgáltatás megszüntetésekor vagy a dokumentum újabb verziójának hatályba lépésekor.

Jelen dokumentum hatálya kiterjed az 1.3 szerinti pont szerinti szereplőkre.

1.3. Nyilvános Kulcsú Infrastruktúra (PKI) szereplői

Jelen Szolgáltatási Kivonatban szereplő PKI közösség az alábbi felekből áll:

- Szolgáltató: a BSZ-DÁP-TAN-nak és a BSZ-DÁP-TK-nak megfelelő tanúsítványokat kibocsátó minősített bizalmi szolgáltató, amely a tanúsítványok kibocsátásával és menedzsmentjével kapcsolatos műszaki tevékenységeket végzi;
- Közreműködő Felek: a Szolgáltatóval szerződéses kapcsolatban álló és/vagy jogszabályban meghatározott, a Szolgáltatások nyújtásában közreműködő felek;
- Végfelhasználók: a tanúsítványt igénylő állampolgárok (Aláírók);
- Érintett Felek: a tanúsítvány felhasználásával létrehozott elektronikus aláírásokat fogadó harmadik felek.

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

1.4. A tanúsítvány felhasználása

A DÁP-TAN tanúsítvány az {J1} eIDAS - szerinti minősített tanúsítvány, az {Sz4} EN 319 412-1 szabvány 3.1 fejezetében az „EU minősített tanúsítványra” vonatkozó követelményeknek megfelelően.

A DÁP-TAN tanúsítványok minősített elektronikus aláírás létrehozó eszköz (korábbi elnevezése: biztonságos aláírás-létrehozó eszköz) alkalmazását megkövetelő, minősített tanúsítványok, így a kapcsolódó magánkulccsal együtt minősített elektronikus aláírás létrehozására, illetve ellenőrzésére használhatók.

A Szolgáltató DÁP-TAN tanúsítványokhoz kapcsolódó magánkulcsokat minősített elektronikus aláírás létrehozó eszközben generálja és tárolja, azok teljes életciklusában a DÁP-TK szolgáltatás keretében.

A minősített elektronikus aláírás joghatását a {J2} DÁP tv 54. § határozza meg. E szerint DÁP-TAN tanúsítvány felhasználásával létrehozott elektronikus aláírás minősített elektronikus aláírás, mely teljes bizonyító erejű magánokirat és közokirat létrehozására alkalmas.

DÁN-TK szolgáltatás önállóan nem vehető igénybe, csak a BSZ-DÁP-TAN bizalmi szolgáltatási szabályzatban leírt tanúsítvány kibocsátási szolgáltatáshoz integrált módon, a DÁP keretalkalmazáson keresztül.

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.

DÁN-TK szolgáltatás PAdES formátumú, PAdES-B-T szintű minősített elektronikus aláírások létrehozását támogatja.

Teszttanúsítványok

A Szolgáltató az éles szolgáltatást nyújtó gyökér-hitelesítőközpont hierarchiájában – saját rendszerének tesztelése céljából – teszttanúsítványokat is kibocsát.

A teszttanúsítványok megjelölése olyan módon történik, hogy a tanúsítvány Subject\CommonName mezőjében szerepel a „TESZT” szó.

A teszt tanúsítványokhoz és azon alapuló elektronikus aláírásokhoz semmilyen joghatás nem kapcsolódik.

A Szolgáltató az Aláírók vagy más, harmadik felek részére -DÁP-TAN szolgáltatás nyújtás keretében nem bocsát ki teszttanúsítványokat.

1.4.1. Engedélyezett tanúsítvány használat

A kibocsátott tanúsítványokhoz kapcsolódó magánkulcsok kizárólag elektronikus aláírás létrehozására használhatók. A Szolgáltatás keretében az Aláírók kizárólag saját nevükben és magánszemélyként hozhatnak létre elektronikus aláírást. Az Aláírók névtelensége és álnév használata nem megengedett.

A kibocsátott tanúsítványok, illetve a hozzájuk kapcsolódó nyilvános kulcsok kizárólag elektronikus aláírás érvényesítésére használhatók.

1.4.2. Tiltott tanúsítvány használat

Tilos a tanúsítványt (illetve a hozzá kapcsolódó kulcspárt) felhasználni titkosításra vagy visszafejtésre, azonosításra, más tanúsítványok aláírására vagy bármilyen bizalmi szolgáltatás nyújtásához.

A Digitális Állampolgárság Program keretében kiadott tanúsítványt, illetve a kapcsolódó magánkulcsot az Aláíró kizárólag magánszemélyként használhatja fel; ezek használata bármilyen üzleti, munkahelyi vagy egyéb szakmai tevékenység céljából nem megengedett.

1.5. A dokumentum adminisztrációja

A Szolgáltató szervezetén belül Szabályozási Csoportot működtet, amely többek között jelen Szolgáltatási Kivonat karbantartásáért is felelős.

1.5.1. Kapcsolat

Lásd 1.1.1 Szolgáltató.

1.5.2. A szabályzat alkalmasságának meghatározása

A Szolgáltató legalább évente egyszer felülvizsgálja a bizalmi szolgáltatási rend, illetve a bizalmi szolgáltatási szabályzat és egyéb szabályzatai tartalmi és formai megfelelőségét a vonatkozó jogszabályok, előírások és műszaki szabványok tekintetében, és ennek eredményeit megfelelő módosításokkal alkalmazza az érintett dokumentumokban.

A változtatási igényeket a Szabályozási Csoport gyűjti, a módosításokat legalább évente egyszer elvégzi, majd ellenőrzésre és jóváhagyásra előterjeszti.

1.5.3. A szabályzat jóváhagyásának eljárása

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

A jóváhagyott szolgáltatási szabályzat a Szolgáltató elektronikus bélyegzőjével vagy a Szolgáltatásokért felelős vezető elektronikus aláírásával kerül hitelesítésre.

A szolgáltatási szabályzat új verziója mindig új verziószámmal kerül elfogadásra.

A BSZ-DÁP-TAN új verzióját a Szolgáltató vezetése hagyja jóvá és lépteti hatályba.

A BSZ-DÁP-TAN új verzióját a Szolgáltató a hatályba lépést megelőzően legalább 30 nappal előzetesen bejelenti a Bizalmi Felügyelet (Nemzeti Média- és Hírközlési Hatóság) részére. A szolgáltatási szabályzat jogszabályoknak való megfelelőségét a Bizalmi Felügyelet is ellenőrzi.

A Szolgáltató a BSZ-DÁP-TAN új verzióját internetes honlapján közzé teszi. A hatályba lépés napját a dokumentum előlapja tartalmazza.

Az új verzió kötelező érvényű az összes Aláíróra, illetve az így kibocsátott tanúsítványokra, továbbá az abban foglalt változásokat javasolt figyelembe vennie az összes, a BSZ-DÁP-TAN előző verzióinak megfelelően kibocsátott tanúsítványokat használó Érintett Félnek.

1.6. Fogalmak, rövidítések és hivatkozások

1.6.1. Fogalmak

alany: A Szolgáltató által kiadott tanúsítványban azonosított entitás, aki a tanúsítványban szereplő nyilvános kulcsnak (elektronikus aláírás érvényesítési adat) megfelelő magánkulcsot (elektronikus aláírás létrehozásához használt adat) birtokolja.

Jelen Szolgáltatási Kivonat szerint az Alany az állampolgár.

aláíró: elektronikus aláírás létrehozó természetes személy.

Jelen Szolgáltatási Kivonat szerint az Aláíró az állampolgár.

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.

bizalmi felügyelet: lásd „felügyeleti szerv”.

bizalmi szolgáltatás: rendszerint díjazás ellenében nyújtott, az alábbiakból álló szolgáltatások:

a) elektronikus aláírások tanúsítványainak, elektronikus bélyegzők tanúsítványainak, weboldal-hitelesítő tanúsítványoknak vagy egyéb bizalmi szolgáltatások nyújtására vonatkozó tanúsítványoknak a kibocsátása;
b) elektronikus aláírások tanúsítványainak, elektronikus bélyegzők tanúsítványainak, weboldal-hitelesítő tanúsítványoknak vagy egyéb bizalmi szolgáltatások nyújtására vonatkozó tanúsítványoknak az érvényesítése;
c) elektronikus aláírások vagy elektronikus bélyegzők létrehozása;
d) elektronikus aláírások vagy elektronikus bélyegzők érvényesítése;
e) elektronikus aláírásoknak, elektronikus bélyegzőknek, elektronikus aláírások tanúsítványainak vagy elektronikus bélyegzők tanúsítványainak a megőrzése;
f) távoli elektronikus 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 Kivonat szerinti bizalmi szolgáltatás az a) pont alatti szolgáltatás, valamint az c) és az f) pont alatti szolgáltatások, azzal, hogy a Szolgáltató BSZ-DÁP-TAN keretében kizárólag elektronikus aláírások tanúsítványainak kibocsátását, BSZ-DÁP-TK keretében kizárólag elektronikus aláírások létrehozását végzi az állampolgárok, mint Aláírók nevében.

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

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.

biztonsági tisztviselő: a bizalmi szolgáltatás biztonságáért, a biztonsági irányelvek és szabályzatok érvényre juttatásáért általánosan felelős személy.

biztonságos környezet: olyan fizikai környezet, mely védett illetéktelen hozzáféréstől, és jogszabályban meghatározott mértékben, a tűz, árvíz, elárasztás, fizikai behatolás, sugárzás, áramellátás kimaradás és egyéb katasztrófaeseményektől, egyéb erőszakos behatásoktól.

DÁP keretalkalmazás: a digitális állampolgárság szolgáltatások igénybevétele céljából a nyilvánosság számára mobileszközökre tervezett és kifejlesztett mobilalkalmazás.
(A {J2} DÁP tv. ezt keretalkalmazásnak nevezi.)

DÁP portál: a DÁP szolgáltató és a DÁP szolgáltatások központi weboldala, mely a dap.gov.hu címen érhető el.

DÁP szolgáltató: olyan külső fél, mely a Szolgáltató számára különböző szolgáltatásokat biztosít (pl. nyilvántartás vezetés, keretalkalmazás nyújtása, adatkezelés), ezen belül elvégzi az Aláírók azonosítását és hitelesítését.

digitális állampolgárság: az állampolgárok azon joga, amellyel digitálisan ügyet intézhetnek, szolgáltatást vehetnek igénybe.

digitális állampolgár azonosító (DÁP azonosító): matematikai módszerrel képzett, különleges adatra nem utaló számjegysor, amely egyedi és tartós azonosítóként a polgárt a digitális térben egyértelműen azonosítja.
(A DÁP azonosító az Alaptörvény XXVI. cikk (2) bekezdésében meghatározott, a digitális ügyintézéshez mindenki számára biztosít egyedi digitális azonosító.)

digitális állampolgárság nyilvántartás: a {J2} DÁP tv. által létrehozott, a digitális állampolgár azonosítót tartalmazó ügyfélregisztrációs nyilvántartás.

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

elektronikus aláírás érvényesítési adat: lásd „aláírás érvényesítési adat”.

elektronikus aláírás létrehozásához használt adat: lásd „aláírás létrehozásához használt adat”.

elektronikus aláírás tanúsítványa: olyan elektronikus igazolás, amely az elektronikus aláírás érvényesítési adatokat egy természetes személyhez kapcsolja és igazolja legalább az érintett személy nevét vagy álnevét.

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.

elektronikus aláírás érvényesítés: 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.

elektronikus aláírás létrehozó eszköz: elektronikus aláírás létrehozására használt, konfigurált hardver- vagy szoftvereszköz.

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

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.

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

elektronikus bélyegző tanúsítványa: olyan elektronikus tanúsítvány, amely az elektronikus bélyegzőt érvényesítő adatokat egy jogi személyhez kapcsolja, és igazolja az érintett jogi személy nevét.
Korábbi elnevezése: szervezeti tanúsítvány.

elektronikus bélyegző létrehozásához használt adatok: olyan egyedi adatok, amelyeket az elektronikus bélyegző létrehozója elektronikus bélyegző létrehozásához használt.
(jellemzően kriptográfiai magánkulcs)

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

elektronikus dokumentum: elektronikus formában, különösen szöveg, hang-, képi vagy audiovizuális felvétel formájában tárolt bármilyen tartalom.

elektronikus időbélyegző: olyan elektronikus adatok, amelyek más elektronikus adatokat egy adott időponthoz kötnek, amivel igazolják, hogy utóbbi adatok léteztek az adott időpontban.

entitás: a nyilvános kulcsú infrastruktúra (PKI) eleme, pl. egy tanúsítványkiadó, regisztrációs szervezet, végfelhasználó vagy eszköz.

EU minősített tanúsítvány: a {J1} eIDAS rendelettel összhangban kibocsátott minősített tanúsítvány.

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.

érvényesítés: az a folyamat, amelynek keretében ellenőrzik és igazolják, hogy az elektronikus adatok a {J1} eIDAS rendelettel összhangban érvényesek.

érvényesítési adatok: elektronikus aláírás vagy elektronikus bélyegző érvényesítéséhez használt adatok (jellemzően kriptográfiai nyilvános kulcs).

érvényességi lánc: az elektronikus dokumentum vagy annak lenyomata és azon egymáshoz rendelhető információk (így különösen azon tanúsítványok, a tanúsítványokkal kapcsolatos információk, az aláírás vagy bélyegző létrehozásához használtadatok, a tanúsítvány aktuális állapotára, visszavonására vonatkozó információk, valamint a tanúsítványt kibocsátó szolgáltató érvényességi adatára és annak visszavonására vonatkozó információk) sorozata, amelyek segítségével megállapítható, hogy azelektronikus dokumentumon elhelyezett fokozott biztonságú vagy minősített elektronikus aláírás, bélyegző vagy időbélyegző, azaláírás, bélyegző vagy időbélyegző elhelyezésének időpontjában érvényes volt.

felhasználóazonosítás: az Aláírók visszavonás igényléséhez szükséges azonosítását elvégző folyamat.

felügyeleti szerv: 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.

fokozott biztonságú elektronikus aláírás: olyan elektronikus aláírás, amely megfelel a {J1} eIDAS 26. cikk (1) bekezdésében meghatározott követelményeknek, azaz:

a) kizárólag az aláíróhoz köthető;
b) alkalmas az aláíró azonosítására;
c) olyan, elektronikus aláírás létrehozásához használt adatok felhasználásával hozták létre, amelyeket az aláíró nagy megbízhatósággal kizárólag saját maga használhat;

olyan módon kapcsolódik azokhoz az adatokhoz, amelyeket aláírtak vele, hogy az adatok minden későbbi változása nyomon követhető.

fokozott biztonságú elektronikus bélyegző: olyan elektronikus bélyegző, amely megfelel a {J1} eIDAS 36. cikk (1) bekezdésében meghatározott követelményeknek, azaz:

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

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

hitelesítési rend (Certificate Policy - CP): olyan bizalmi szolgáltatási rend, amely bizalmi szolgáltatás keretében kibocsátott tanúsítványra vonatkozik.

hitelesítőközpont (CA): a Szolgáltató azon egysége, amely a hitelesítés-szolgáltatás magánkulccsal folytatott tevékenységét végzi. Egy hitelesítőközponthoz mindig egy magánkulcs tartozik. A hitelesítőközpont fizikailag egy telephelyre koncentráltan, védett, biztonságos körülmények között működik.

időbélyegző: lásd „elektronikus időbélyegző”.

időbélyegzés: az a folyamat, melynek során az elektronikus dokumentumhoz elektronikus időbélyegző hozzárendelése történik.

igénylő: az a személy, aki/amely a Szolgáltatóhoz fordul a bizalmi szolgáltatás igénybevétele céljából.

igénybe vevő fél: olyan természetes vagy jogi személy, aki, illetve amely elektronikus azonosítást, európai digitális személyiadat-tárcát vagy más elektronikus azonosító eszközt, vagy bizalmi szolgáltatást vesz igénybe.

informatikai rendszer: a Szolgáltató által a bizalmi szolgáltatásokhoz, illetve annak elemeihez, így különösen a szolgáltatói kulcspár kezeléséhez, az elektronikus aláírás vagy bélyegző létrehozásához használt adatok előállításához, a tanúsítványok kibocsátásához, a kibocsátott tanúsítványt tartalmazó nyilvántartáshoz, a visszavonási nyilvántartásokhoz és a visszavonás kezeléséhez, az időbélyegzés szolgáltatáshoz, az elektronikus archiválás szolgáltatáshoz, valamint e tevékenységek informatikai védelméhez használt, a {J1} eIDAS 24. cikk (2) bekezdés e) és f) pontja szerinti megbízható rendszerek és termékek.

Kiberbiztonsági Felügyelet: az adott tagállamban kijelölt felügyeleti szerv (Magyarországon a Szabályozott

Tevékenységek Felügyeleti Hatósága), 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.

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.

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

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.

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 képzett lenyomat egyértelműen származtatható az elektronikus dokumentumból;
- a képzett lenyomatból az elvárható biztonsági szinten belül nem lehetséges az elektronikus dokumentum tartalmának meghatározása vagy a tartalomra történő következtetés;
- 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.

megfelelőségértékelő szervezet: a 765/2008/EK rendelet 2. cikkének 13. pontjában meghatározott (megfelelőségértékelési tevékenységeket – beleértve a kalibrálást, vizsgálatot, tanúsítást és ellenőrzést – végző) szervezet, amelyet az említett rendelettel összhangban illetékesnek ismernek el a minősített bizalmi szolgáltató és az általa nyújtott minősített bizalmi szolgáltatások megfelelőségének értékelésére, vagy az európai digitális személyiadat-tárcák vagy az elektronikus azonosító eszközök tanúsításának elvégzésére.

minősített bizalmi szolgáltatás: olyan bizalmi szolgáltatás, amely megfelel a {J1} eIDAS rendeletben foglalt alkalmazandó követelményeknek, azaz a Bizalmi Listán szerepel.

minősített bizalmi szolgáltató: olyan bizalmi szolgáltató, amely egy vagy több bizalmi szolgáltatást nyújt és amelynek minősített státuszát a Felügyeleti Szerv jóváhagyta, azaz a Bizalmi Listán szerepel.

minősített elektronikus aláírás: olyan, fokozott biztonságú elektronikus aláírás, amelyet minősített elektronikus aláírás létrehozó eszközzel állítottak elő, és amely elektronikus aláírás célú minősített tanúsítványon alapul.

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). Korábbi elnevezése: biztonságos aláírás-létrehozó eszköz (BALE).

nyilvános kulcsú infrastruktúra (PKI): az elektronikus aláírás vagy elektronikus bélyegző, valamint titkosítás létrehozására, érvényesítésére, kezelésére szolgáló, aszimmetrikus kulcspárt alkalmazó infrastruktúra, beleértve a mögöttes intézményrendszert, a különböző bizalmi szolgáltatókat és eszközöket is.

produktív hitelesítőközpont: a gyökér hitelesítőközpont által létrehozott logikailag vagy fizikailag létező hitelesítőközpont, amely egy adott alkalmazási, szervezeti, földrajzi, stb. területre ad ki tanúsítványokat.

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.

szolgáltatói kulcspár: a szolgáltatói magánkulcsból és a szolgáltatói nyilvános kulcsból álló, kriptográfiai kulcspár.

szolgáltatói magánkulcs: olyan kriptográfiai magánkulcs, melyet a szolgáltató a saját bizalmi szolgáltatásának igazolására, így különösen a tanúsítványok kibocsátására, visszavonási nyilvántartásokra, az időbélyegzésre, az archiváláshoz használ.

szolgáltatói nyilvános kulcs: olyan kriptográfiai nyilvános kulcs, melyet a szolgáltató magánkulcsának használatával létrehozott elektronikus aláírás, elektronikus bélyegző vagy elektronikus időbélyegző érvényesítésére használnak.

szolgáltatási szabályzat (Certificate Practice Statement - CPS): a bizalmi szolgáltató nyilatkozata az egyes bizalmi szolgáltatások nyújtásával kapcsolatosan alkalmazott részletes eljárási vagy más működési követelményekről.

szolgáltatási szerződés: a bizalmi szolgáltató és a bizalmi szolgáltatási ügyfél között – általános szerződési feltételek elfogadásával létrejött szerződés, amely a bizalmi szolgáltatás nyújtására és a szolgáltatás igénybevételére vonatkozó feltételeket tartalmazza;

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.

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.

tanúsítványokkal kapcsolatos szabályzatok: a bizalmi szolgáltatási rend, a szolgáltatási szabályzat, a szolgáltatási kivonat, valamint az általános szerződéses feltételek.

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.

üzenethitelesítő kulcspár: Az üzenethitelesítő kulcspár a DÁP keretakalmazás által generált hitelesítő kulcspár, melynek magánkulcsa az alkalmazás által generált és a Szolgáltató informatikai rendszere felé küldött adatok („üzenetek") hitelességét hivatott biztosítani, oly' módon, hogy ezen üzeneteket műszaki értelemben (és nem jogi értelemben) digitálisan aláírja. Az üzenethitelesítő kulcspár nyilvános kulcsát, annak generálását követően a DÁP keretalkalmazás továbbítja a Szolgáltató informatikai rendszere felé, mely tárolja azt az adott Aláíróhoz kapcsolva.

visszavonási jelszó: az elektronikus aláíró tanúsítvány ügyfél kérelmére történő visszavonásához szükséges kód, amennyiben a visszavonási igényét az Aláíró a DÁP portálon keresztül jelzi.
Az állampolgár a visszavonási jelszót a sikeres tanúsítvány igénylés után, a DÁP szolgáltatótól e-mail-ben kapja meg.

1.6.2. Rövidítések

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
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
DÁP-TAN		Szolgáltató BSZ-DÁP-TAN szerinti szolgáltatása
DÁP-TK		Szolgáltató BSZ-DÁP-TK szerinti szolgáltatása
HSM	Hardware Security Module	hardver biztonsági modul, kriptográfiai modul
NTP	Network Time Protocol	időforrás protokoll
OCSP	Online Certificate Status Protocol	valós idejű tanúsítvány-állapot protokoll
PDS-DÁP	Public Disclosure Statement	Szolgáltatási Kivonat a Digitális Állampolgárság Program keretében biztosított bizalmi szolgáltatásokhoz

PKI	Public Key Infrastructure	nyilvános kulcsú infrastruktúra
QSCD	Qualified Signature Creation Device	minősített elektronikus aláírás létrehozó eszköz
RA	Registration Authority	regisztrációs szervezet
UTC	Coordinated Universal Time	koordinált univerzális idő

1.6.3. Hivatkozások

1.6.3.1. Jogszabályi hivatkozások

{J1}	Az Európai Parlament és a Tanács (EU) 910/2014 rendelete a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről (eIDAS)
{J2}	2023. évi CIII. törvény a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól (DÁP tv.)
{J3}	2013. évi V. törvény a Polgári Törvénykönyvről
{J4}	2016. évi CXXX. törvény a polgári perrendtartásról
{J5}	24/2016. (VI.30.) BM rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről
{J6}	679/2016/EU Európai Parlament és 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 (GDPR)
{J7}	2013. évi L. törvény az informatikai rendszerek biztonsági értékelését az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.)
{J8}	2023. évi XXIII. törvény a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről (Kibertan törvény)
{J9}	7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetébenalkalmazandó 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

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}	EN 319 411-1 V1.4.1 (2023-10)	Policy and security requirements for Trust Service Providers issuing certificates
{Sz3}	EN 319 411-2 V2.5.1 (2023-10)	Policy and security requirements for Trust Service Providers issuing EU qualified certificates
{Sz4}	EN 319 412-1 V1.5.1 (2023-09)	Certificate Profiles; Part 1: Overview and common data structures
{Sz5}	EN 319 412-2 V2.3.1 (2023-09)	Certificate Profiles; Part 2: Certificate profiles for certificates issued to natural persons
{Sz6}	EN 319 412-5 V2.4.1 (2023-09)	Certificate Profiles; Part 5: QCStatements
{Sz7}	ETSI TS 119 312 V1.4.3 (2023-08)	Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
{Sz8}	ITU-T X.520 (10/19)	Information technology - Open Systems Interconnection - The Directory: Selected attribute types
{Sz9}	ITU-T X.509 (10/19)	Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate framework
{Sz10}	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
{Sz11}	ISO/IEC 19790:2012	ISO/IEC 19790: Information technology – Security techniques – Security requirements for cryptographic modules
{Sz13}	RFC 3647 (November 2003)	Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework
{Sz14}	RFC 3739 (March 2004)	Internet X.509 Public Key Infrastructure: Qualified Certificates Profile
{Sz15}	RFC 4514 (June 2006)	Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names
{Sz16}	RFC 5280 (May 2008)	Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile
{Sz17}	RFC 6818 (January 2013)	Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
{Sz18}	RFC 6960 (June 2013)	X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol - OCSP

1.6.3.3. Hivatkozott dokumentumok

{D1}	ÁSZF-DÁP	Általános Szerződési Feltételek a NISZ Zrt. Digitális Állampolgárság Programhoz kapcsolódó hitelesítés szolgáltatásaihoz
{D3}		NISZ Zrt. Szervezeti és Működési Szabályzata
{D4}		Adatkezelési tájékoztató a DÁP eAlárás szolgáltatáshoz
{D5}		NISZ Zrt. PKI szolgáltatások informatikai biztonságpolitikája
{D6}		GovCA biztonsági szabályzat
{D7}		NISZ Zrt. PKI szolgáltatások üzletmenet-folytonossági terve
{D8}		DÁP eAláírás tanúsítványprofilok
{D9}	BR-DÁP-TAN	Bizalmi Szolgáltatási Rend a Digitális Állampolgárság Program keretében kibocsátott minősített tanúsítványokhoz
{D10}	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
{D11}	BSZ-DÁP-TAN	Bizalmi Szolgáltatási Szabályzat a Digitális Állampolgárság Program keretében nyújtott minősített tanúsítványszolgáltatásokhoz

2. Azonosítás és hitelesítés

2.1. Kezdeti azonosítás

Az Aláíró szempontjából a Szolgáltatás igénybevételéhez szükséges kezdeti azonosítás az alábbi lépésekből áll:

- a DÁP keretalkalmazás telepítése saját mobileszközére;
- a DÁP azonosítón alapuló felhasználói profil aktiválása;
- a DÁP keretalkalmazás regisztrálási funkciójának aktiválása.

A Szolgáltató az Aláíró kezdeti azonosítását, hitelesítését és jogosultságának ellenőrzését a DÁP szolgáltató, mint külső fél által végzett, a {J2} DÁP tv. 63. § szerinti személyazonosításra alapozva végzi, úgy, hogy annak eredményét a DÁP szolgáltató a tanúsítványkérelemmel együtt, általa hitelesítve küldi meg a Szolgáltató felé, majd a Szolgáltató az ennek keretében átadott adatok hitelességét ellenőrzi a DÁP szolgáltató elektronikus bélyegzőjének érvényesítésével.

A Szolgáltató és a DÁP szolgáltató, mint közreműködő fél, a közöttük lévő jogviszonyt külön megállapodásban rendezik, amelynek része a személyazonosság fentiek szerinti hitelesítésében történő közreműködése is.

A Szolgáltató a DÁP-TK szolgáltatás nyújtása során teljesíti az {Sz5} EN 419 241-1 szabvány 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.

2.1.1. A személyazonosság hitelesítése

Az Aláíró személyazonosságának hitelesítését a DÁP szolgáltató végzi, amelynek eredményt a Szolgáltató hitelesnek és valóságnak megfelelőnek fogad el figyelembe véve a {J2} DÁP tv. 63. § (2) bekezdését.

A Szolgáltató oldalán történő hitelesítés alapja a DÁP szolgáltató részéről, a tanúsítványkérelemmel együtt érkező, a {J2} DÁP tv. 63. § szerinti személyazonosítás eredménye, amely hitelesen tartalmazza az Aláíró névadatát és a DÁP azonosítóját. A DÁP szolgálató által átadott személyazonosság igazolását Szolgáltató akkor fogadja el hitelesnek, amennyiben annak hitelességét és sértetlenségét a DÁP szolgáltató minősített tanúsítványon alapuló elektronikus bélyegzője igazolja.

A {J2} DÁP tv. 63. § szerinti személyazonosítás az {J1} eIDAS rendelet 24. cikk (1a) bekezdés c) pontja szerinti ún. egyéb azonosítási módszernek tekinthető, mely biztosítja a személy magas megbízhatósági szintű azonosítását, és amely megfelelőségét a DÁP szolgáltató megfelelőségértékelő szervezet által kibocsátott megfelelőségértékelési jelentéssel igazolta Szolgáltató felé.

2.1.2. Jogosultság ellenőrzése

Az Aláíró jogosultságának ellenőrzését, azaz, hogy jogosult-e a Szolgáltatótól tanúsítványt igényelni a DÁP szolgáltató a {J2} DÁP tv. szabályai szerint ellenőrzi, bírálja el, a 3.2.3 pont szerinti személyazonosítás részeként. Sikeres személyazonosítás esetén az Aláíró Szolgáltatás igénybevételére való jogosultságát a Szolgáltató igazoltnak tekinti.

2.2. Azonosítás és hitelesítés kulcscsere esetén

A Szolgáltató nem nyújt kulcscsere szolgáltatást.

2.3. Azonosítás és hitelesítés tanúsítvány visszavonás esetén

2.3.1. Visszavonás DÁP keretalkalmazáson keresztül

Az Aláíró szempontjából visszavonás kezdeményezéséhez szükséges felhasználóazonosítás az alábbi lépésekből áll:

- a DÁP keretalkalmazás elindítása saját mobileszközén és visszavonási funkció kiválasztása;
- az azonosításhoz szükséges adat megadása a DÁP keretalkalmazásban.

A Szolgáltató szempontjából az Aláíró felhasználóazonosítását a DÁP szolgáltató, mint külső fél végzi, a 2.1 szerinti személyazonosításra építve.

A Szolgáltató a DÁP szolgáltató által továbbított visszavonási kérést akkor fogadja el hitelesnek, amennyiben annak hitelességét és sértetlenségét a DÁP szolgáltató minősített tanúsítványon alapuló elektronikus bélyegzője igazolja és abból egyértelműen megállapítható a visszavonandó tanúsítvány és a visszavonási kérés oka.

2.3.2. Visszavonás webes felületen keresztül

Az Aláíró szempontjából visszavonás kezdeményezéséhez szükséges felhasználóazonosítás az alábbi lépésekből áll:

- a DÁP portál megfelelő menüpontjának megnyitása böngészőben;
- az azonosításhoz szükséges, a portál által kért adatok megadása;
- a DÁP profil aktiválásakor a DÁP szolgáltató által ellenőrzött e-mail címre a DÁP szolgáltató által kiküldött egyedi URL megnyitása;
- az egyedi URL-en elérhető webes felületen a DÁP szolgáltató által ellenőrzött e-mail címre a DÁP szolgáltató által a tanúsítvány kibocsátásakor küldött egyedi azonosító (visszavonási jelszó) megadása.

A Szolgáltató szempontjából az Aláíró felhasználóazonosítását a DÁP szolgáltató, mint külső fél végzi, a 2.1 fejezet szerinti személyazonosítás keretében ellenőrzött adatokra építve.
A Szolgáltató a DÁP szolgáltató által továbbított visszavonási kérést akkor fogadja el hitelesnek, amennyiben annak hitelességét és sértetlenségét a DÁP szolgáltató minősített tanúsítványon alapuló elektronikus bélyegzője igazolja és abból egyértelműen megállapítható a visszavonandó tanúsítvány és a visszavonási kérés oka.

3. Tanúsítványok életciklusára vonatkozó követelmények

3.1. Tanúsítványigénylés

3.1.1. Ki nyújthat be tanúsítványigénylést

Tanúsítványigénylést benyújthat azon 14. életévét betöltött, személyi adat- és lakcímnyilvántartás hatálya alá tartozó személy, aki jogosult DÁP azonosítóra.

A DÁP-TK szolgáltatást közvetlenül nem kell igényelni.

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

- tanúsítványigénylés (lásd {D11} BSZ-DÁP-TAN 4.1 fejezete),

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

- tanúsítvány visszavonás (lásd {D11} BSZ-DÁP-TAN 4.9 fejezete).

3.1.2. Igénylési folyamat és felelősségek

A tanúsítványigénylés folyamata röviden a következő:

- DÁP keretalkalmazás elindítása saját mobil eszközön és az eAláírás funkció indítása;
- tájékoztatás;
- A DÁP keretalkalmazás eAláírás funkciójának későbbi használatához szükséges egyedi jelszó létrehozása és megerősítése, mely egyúttal az aláíró kulcs aktiváló adatának jelszavaként tekintendő;
- regisztráció;
- {D1} ÁSZF, BSZ-DÁP-TAN és a {D10} BSZ-DÁP-TK elfogadása, ami egyúttal a Szolgáltatási Szerződés megkötését is jelenti;
- tanúsítványba kerülő adatok megerősítése;
- tanúsítványkérelem előállítása.

3.1.2.1. Tájékoztatás

Az ÁSZF elfogadása (ami a Szolgáltatási Szerződés megkötését is jelenti) előtt igénylő közérthető tájékoztatást kap az alábbiakról:

- arról, hogy a szolgáltatás minősített bizalmi szolgáltatásnak minősül;
- a Szolgáltatás használati lehetőségeiről és jogszabályi vonatkozásairól;
- az aláírás létrehozásához használt adat (magánkulcs) használatával és védelmével kapcsolatostudnivalókról;
- az aláíró és az aláírást ellenőrizni kívánó felek felelősségéről, kötelezettségeiről;
- tanúsítványok visszavonásának lehetőségéről;
- a tanúsítvány érvényességéről, érvényességi idejének lejártáról, esetleges egyéb korlátozásokról;
- arról, hogy az Aláíró hol tájékozódhat a szolgáltatásra vonatkozó követelményekről (BR-DÁP-TAN, BR-DÁP-TK), a Szolgáltató szolgáltatási gyakorlatáról (BSZ-DÁP-TAN, BSZ-DÁP-TK) valamint a szolgáltatás igénybevételének egyéb üzleti, jogi és technikai feltételeiről (ÁSZF-DÁP);
- arról, hogy a szolgáltatás igénybevétele díjmentes.

3.1.2.2. Regisztráció

Aláíró a Szolgáltatónál történő regisztrációját a DÁP keretalkalmazás tanúsítványigénylő funkciójával kezdeményezheti. Ennek során a DÁP szolgáltató átadja Szolgáltatónak az Aláíró DÁP profiljának aktiválásakor általa rögzített és a BSZ-DÁP szolgáltatás nyújtásához szükséges adatait.

3.1.2.3. Szolgáltatási szerződés megkötése

Az Igénylő a DÁP keretalkalmazásban ellenőrzi és megerősíti az adatai valódiságát, majd elfogadja az {D1} ÁSZF-DÁP tartalmát és ezen keresztül létrejön a Szolgáltatási Szerződés.

A Szolgáltató és a DÁP szolgáltató, mint közreműködő fél, a közöttük lévő jogviszonyt külön megállapodásban rendezik, amelynek része, hogy a DÁP szolgáltató garantálja, hogy csak azon Aláírók tanúsítványkérelmét juttatja el a Szolgáltatóhoz, akik az {D1} ÁSZF-DÁP-ot a fentiek szerint elfogadták.

3.1.2.4. Tanúsítványkérelem előállítása

Az Igénylő a DÁP keretalkalmazásán keresztül a DÁP szolgáltató közvetítésével kezdeményezheti az aláírói tanúsítvány igénylését. Ugyanazon DÁP keretalkalmazáshoz és mobil eszközhöz kapcsolódóan Aláíró egyetlen aláíró kulccsal és tanúsítvánnyal rendelkezhet.

Az igénylés elküldése előtt a DÁP keretalkalmazás egy üzenethitelesítő kulcspárt generál, melynek 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 DÁP-TAN szolgáltatás és a DÁP-TK szolgáltatás keretén belül egyaránt.

A DÁP szolgáltató (az Aláíró azonosítása és hitelesítése után) az Aláíró nevében továbbítja a tanúsítványkérelmet a Szolgáltatónak.

A DÁP szolgáltató és a Szolgáltató között minden üzenetváltás legalább minősített tanúsítványon alapuló fokozott biztonságú elektronikus bélyegzővel hitelesítve történik.

Aláíró – miután elküldte tanúsítványkérelmét – a Szolgáltatótól visszakapja a tanúsítványba kerülő adatokat. Ezek helyességét, valamint az ÁSZF (és ezen keresztül a BR-DÁP-TAN és a BSZ-DÁP-TAN) elfogadását vissza kell igazolnia, ezek a tanúsítvány kiállításának feltételei.

A Szolgáltató a visszaigazolást követően végrehajtja a kulcspár generálását, a tanúsítvány kibocsátását, majd a tanúsítvány Aláírónak történő eljuttatását (DÁP keretalkalmazáson keresztül).

3.2. Tanúsítványigénylés feldolgozása

3.2.1. Azonosítási és hitelesítési műveletek

A Szolgáltató kizárólag a DÁP szolgáltatótól érkezett tanúsítványkérelmet fogad el, az alábbiak szerint:

- a Szolgáltató a DÁP szolgáltatót az üzenetet védő legalább minősített tanúsítványon alapuló fokozott biztonságú elektronikus bélyegző érvényesítésével azonosítja és hitelesíti;
- az elektronikus bélyegző tanúsítványában szerepel a DÁP szolgáltató egyedi azonosítója;
- a DÁP szolgáltató üzenetében legalább az alábbiak szerepelnek
    - az Aláíró tanúsítványba foglalandó adatai,
    - annak ténye, hogy a tanúsítványba foglalandó adatokat és a személyazonosságot a DÁP szolgáltató ellenőrizte,
    - tanúsítvány igénylésére vonatkozó üzenet,
    - a DÁP szolgáltatót igazoló elektronikus bélyegző.

A fentiek teljesülése esetén az Aláíróra vonatkozó adatokat és a tanúsítványkérelmet a Szolgáltató hitelesnek fogadja el.

3.2.2. Tanúsítványigénylés elfogadása vagy visszautasítása

A Szolgáltató elfogadja a sikeresen azonosított DÁP keretalkalmazástól származó hitelesített tanúsítványkérelmet.

A Szolgáltató visszautasítja a tanúsítványkérelmet, ha az nem egy DÁP keretalkalmazástól származik, vagy ha a tanúsítványkérelem hitelesítése sikertelen.

3.2.3. Tanúsítványigénylés feldolgozás időtartama

Szolgáltató a tanúsítványkérelmet a beérkezését követően haladéktalanul, de legkésőbb 24 órán belül feldolgozza.

3.3. Tanúsítvány kibocsátás

3.3.1. Tanúsítványkibocsátás során a Szolgáltató által végzett műveletek

Szolgáltató ellenőrzi a kulcsgenerálási kérelmet is jelentő tanúsítványkérelem DÁP szolgáltatót igazoló elektronikus bélyegzőjét, majd tárolja azt belső nyilvántartásaiban.

A Szolgáltató saját informatikai rendszerében megvalósítja az igényelt kulcspár generálását a DÁP-HSM modulban. A generált magánkulcs nem hagyja el a DÁP-HSM modult.

A Szolgáltató a DÁP-HSM modultól kapott nyilvános kulcs és a tanúsítványkérelemből származó adatok alapján kiállítja a tanúsítványt.

A kiállított tanúsítványt – a DÁP szolgáltató közvetítésével – visszaküldi a DÁP keretalkalmazásnak, egyúttal gondoskodik a kibocsátott tanúsítvány saját adatbázisában történő tárolásáról is.

Az Aláírók a DÁP-TK csak azt követően használhatják, hogy a DÁP-HSM modulban tárolt kulcspárjukhoz kapcsolódó, minősített tanúsítvány kibocsátása és nyilvántartásba vétele rendben megtörtént, a {D11} BSZ-DÁP-TAN szerint.

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

3.3.2. Előfizető értesítése a tanúsítvány kibocsátásról

A Szolgáltató az Aláírót a DÁP szolgáltatón keresztül értesíti a tanúsítvány kibocsátásáról. A DÁP szolgáltató a DÁP keretalkalmazáson keresztül és a DÁP profil aktiválása előtt ellenőrzött e-mail címre küldött e-mail útján ad a tájékoztatást a tanúsítvány kibocsátás sikerességéről vagy visszautasításáról.

3.4. Tanúsítványelfogadás

3.4.1. Tanúsítvány Előfizető általi elfogadása

A tanúsítványba kerülő adatokat az Aláíró a tanúsítvány kibocsátása előtt, a tanúsítványigénylési folyamatban előzetesen visszaigazolja a Szolgáltató felé a DÁP keretalkalmazáson keresztül.

Aláíró a tanúsítványba került adatait a DÁP keretalkalmazás tanúsítványmegtekintő funkciójával tekintheti meg. Aláírónak a tanúsítványa kibocsátásáról szóló értesítő kézhez vétele után haladéktalanul ellenőriznie kell a tanúsítványba került adatainak a helyességét.

Amennyiben az Aláíró a kiállított tanúsítványba került adataiban eltérést talál, azt a tanúsítvány haladéktalan visszavonásával kell kezelnie.

3.4.2. Tanúsítvány közzététele

A Szolgáltató nem teszi közzé a tanúsítványokat szabadon kereshető formában, kizárólag az Aláírónak teszi elérhetővé, illetve saját adatbázisában tárolja.

Az Aláíró a DÁP keretalkalmazáson keresztül utólag le tudja tölteni tanúsítványát.

3.4.3. További felek értesítése a tanúsítvány kibocsátásáról

Szolgáltató a tanúsítvány kibocsátásáról automatizált elektronikus úton értesíti a DÁP szolgáltatót is.

3.5. A kulcspár és a tanúsítvány használata

DÁP-TK szolgáltatás a DÁP keretalkalmazáson keresztül érhető el.

A Szolgáltató a DÁP-TK 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.

A DÁP-TK szolgáltatással az Aláíró a saját mobileszközén tárolt, a DÁP szolgáltató által szabott technikai feltételeknek megfelelő PDF formátumú dokumentumok minősített elektronikus aláírással és minősített időbélyegzővel[1] történő ellátását kérheti a Szolgáltatótól. Ennek során 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 követően – az Aláíró mobileszközén SHA-384 algoritmussal egyedi hash lenyomat készül, melyet az eszköz szabványos aláírási kérésként küld el a Szolgáltató informatikai rendszere felé. Az aláírási kérés az Aláíró mobileszközén 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 DÁP-TK szolgáltatás és a DÁP-TAN szolgáltatás keretén belül egyaránt (lásd BSZ-DÁP-TAN 4.1.2.4).

A Szolgáltató ellenőrzi a DÁP szolgáltatótól kapott kérés formai és tartalmi megfelelőségét.

A Szolgáltató visszautasítja a kérést, ha:

- az Aláíró (illetve az általa használt DÁP keretalkalmazás) azonosítása és/vagy jogosultságának ellenőrzése sikertelen;
- a kérés nem felel meg a vonatkozó rendszerkövetelményeknek;
- a tárolt kulcshoz kapcsolódó tanúsítvány lejárt vagy visszavont;
- 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.

A Szolgáltató elfogadja és kiszolgálja a kérést, ha a fenti ellenőrzések mindegyike sikeresen megtörtént. 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 visszaadja

[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.

az Aláíró kérést küldő keretalkalmazása számára, mely PAdEAS formátumú, PAdES-B-T szintű, minősített időbélyeget is tartalmazó minősített elektronikus aláírásba foglalja azt és összekapcsolja a dokumentummal.

3.5.1. Az Előfizető magánkulcs és tanúsítvány használata

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

Aláíró csak sz 1.4. fejezetben ismertetett célokra és módon használhatja a magánkulcsot és a tanúsítványt.

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

3.5.2. Az Érintett Felek nyilvános kulcs- és tanúsítvány használata

A jelen Szolgáltatási Kivonat hatálya alatt kibocsátott tanúsítványon alapuló elektronikus aláírás elfogadása során szükséges, hogy az Érintett Fél megfelelő körültekintéssel és gondossággal járjon el, melyhez javasolt betartania az alábbi ajánlásokat:

- a tanúsítványok, valamint az elektronikus aláírások ellenőrzését olyan megbízható alkalmazással végezze, amely megfelel a BSZ- DÁP-TAN 1.6.3.1 fejezetében felsorolt jogszabályoknak és amely képes a BSZ-DÁP-TAN 1.6.3.2 fejezetben megadott műszaki szabványok támogatására és azokat helyesen valósítja meg;
- az előző pontban említett aláírás ellenőrző alkalmazást megbízható, vírusmentes környezetben használja, továbbá az aláírás ellenőrző alkalmazás beállítási lehetőségei helyesen legyenek konfigurálva;
- a tanúsítványokat csak olyan alkalmazásokban fogadja el, melyek összhangban vannak a tanúsítvány "kulcshasználat" (`KeyUsage`) és "kiterjesztett kulcshasználat" (`ExtendedKeyUsage`) kiterjesztésének tartalmával;
- végezze el a tanúsítványra az RFC 5280 6. fejezetében leírt tanúsítási útvonal felépítést és érvényesítést, valamint visszavonás ellenőrzést, a tanúsítványt, illetve az ezen alapuló elektronikus aláírást csak ezen ellenőrzések pozitív eredménye esetén fogadja el;
- vegyen figyelembe minden korlátozást, amely a tanúsítványban vagy a tanúsítvány által hivatkozott szabályzatokban szerepel;
- vegye figyelembe a szolgáltatói felelősségvállalás maximális értékét, mivel az ezen összeghatárt meghaladó ügyletekben létrehozott és aláírt elektronikus dokumentumokból származó esetleges károkért való felelősségét a Szolgáltató korlátozza.

A Szolgáltató nem vállal felelősséget azokért a károkért, melyek abból adódnak, hogy az Érintett Fél nem a fenti ajánlásokban leírtak szerint jár el.

3.6. Tanúsítványok megújítása

Az {Sz13} RFC 3647 irányadó szabvány szerint a tanúsítványmegújítás az a folyamat, amely során Szolgáltató az Aláíró változatlan nyilvános kulcsát és változatlan adatait hitelesíti új érvényességi időtartamra szóló új tanúsítvány kibocsátásával.

A Szolgáltató nem nyújt a fentiek szerinti, szabványostanúsítvány megújítási szolgáltatást.

Lejárt vagy lejárófélben lévő tanúsítvány esetén új kulcs és új tanúsítvány igénylésével lehet a szolgáltatást fenntartani.

A lejárt, vagy visszavont tanúsítványokat és hozzájuk tartozó magánkulcsokat a Szolgáltató megsemmisíti.

3.7. Kulcscsere

Az {Sz13} RFC 3647 irányadó szabvány szerint a kulcscsere az a folyamat, amely során Szolgáltató az Aláíró részére új kulcspárt készít és annak nyilvános kulcs párját változatlan alanyadatokat tartalmazó, új tanúsítványba foglalja.

A Szolgáltató nem nyújt a fentiek szerinti, szabványos kulcscsere szolgáltatást.

3.8. Tanúsítványmódosítás

Az {Sz13} RFC 3647 irányadó szabvány szerint a tanúsítványmódosítás az a folyamat, amely során Szolgáltató az Aláíró változatlan nyilvános kulcsát hitelesíti új érvényességi időtartamra szóló új, már a módosult alanyadatokat tartalmazó tanúsítvány kibocsátásával.

A Szolgáltató nem nyújt a fentiek szerinti, szabványos tanúsítványmódosítási szolgáltatást.

Az Aláírónak a meglevő tanúsítványában foglalt adatok módosulása esetén azt vissza kell vonnia és új tanúsítványt kell igényelnie.

3.9. Tanúsítvány visszavonás és felfüggesztés

A Szolgáltató felfüggesztési szolgáltatást nem nyújt.

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

A visszavont tanúsítványhoz tartozó magánkulcs használatát azonnal be kell szüntetni. A visszavonási kérelemnek a Szolgáltatóhoz történő benyújtásáig az Aláíró felelős a felmerült károkért (e tekintetben a Szolgáltatóhoz történő benyújtásnak számít a magánkulcshoz tartozó mobileszköz elvesztésének, megrongálódásának DÁP szolgáltató felé történő bejelentése is). A visszavonási kérelem elfogadásától vagy a visszavonási körülmény Szolgáltató általi értesülésétől, a visszavonás tényének közzétételéig a Szolgáltató felelős a felmerülő károkért. Ez alól kivételt képez a bizonyíthatóan csalárd szándékkal történt visszavonás kérés, amely esetben a felmerült károkért a Szolgáltató nem vállal felelősséget. A visszavonás tényének közzététele után az Érintett Fél felelős a felmerülő károkért.

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

3.9.1. Visszavonás körülményei

Szolgáltató visszavonja a tanúsítványt, ha:

- az Aláíró ezt kéri, mert:
  - nem kívánja a továbbiakban használni a DÁP keretalkalmazás elektronikus aláírás funkcióját; vagy
  - fennáll az a lehetőség vagy gyanú, hogy a DÁP keretalkalmazás elektronikus aláírás funkciójával illetéktelen személy visszaél; vagy
  - adatváltozás miatt.
- a DÁP szolgáltató ezt kezdeményezi, mert:
  - az Aláíró DÁP felhasználói profilja inaktív;
  - az Aláíró a DÁP szolgáltatónak jelezte, hogy a magánkulcsához tartozó mobiltelefonját elvesztette, eltulajdonították vagy használhatatlanná vált;
  - az Aláíró újratelepíti a DÁP keretalkalmazást;
- Aláíró új tanúsítványt igényel ugyanazon mobil eszközre, melyhez kapcsolódóan érvényes tanúsítvánnyal rendelkezik;
- a Szolgáltató a Szolgáltatásokkal kapcsolatos rendellenességről szerez tudomást;
- a Szolgáltató tudomására jut, hogy a tanúsítványban foglalt adatok nem felelnek meg a valóságnak, illetve a BR-DÁP-TAN-nak, amely hatálya alatt a tanúsítvány kibocsátásra került, vagy a tanúsítványt jogellenesen használták, vagy az elektronikus aláírás létrehozásához használt magánkulcsot aktivizáló adat nem az Aláíró kizárólagos birtokában van;
- a Felügyeleti Szerv jogerős és végrehajtható határozatában elrendeli a visszavonást;
- a visszavonást jogszabály kötelezővé teszi;
- a Szolgáltató befejezi a BSZ-DÁP-TAN, vagy BSZ-DÁP-TK szerinti tevékenységét;
- a tanúsítvány formátuma vagy műszaki tartalma (pl. kriptográfiai algoritmus vagy kulcsméret már nem biztonságos) elfogadhatatlan kockázatot jelent az Érintett Felek részére;
- a tanúsítványban felhasznált kriptográfiai algoritmus, kulcshossz, azok paraméterei már nem biztosítják az Aláíró és a nyilvános kulcs hiteles összekapcsolását a tanúsítvány érvényességének hátralevő időszakára.

3.9.2. Ki kezdeményezheti a visszavonást?

Visszavonást kezdeményezhet:

- az Aláíró;
- a Szolgáltató, ideértve az alábbi eseteket is:
  - a Szolgáltatót a DÁP szolgáltató értesíti egy visszavonási körülmény beálltáról;
  - a visszavonás a Felügyeleti Szerv határozata vagy jogszabályi előírás miatt történik.

3.9.3. Visszavonási kérelemre vonatkozó eljárás

3.9.3.1. Visszavonás DÁP keretalkalmazáson keresztül

Aláíró adott mobileszközhöz és a hozzá regisztrált DÁP keretalkalmazáshoz tartozó tanúsítványa visszavonását a DÁP keretalkalmazáson keresztül az alábbiak szerint kezdeményezheti:

- DÁP keretalkalmazás elindítása saját mobil eszközön;
- tanúsítványvisszavonási funkció indítása a DÁP keretalkalmazásban;
- azonosítási és hitelesítési műveletek elvégzése;
- a tanúsítvány adattartamának ellenőrzése a DÁP keretalkalmazásban;
- a visszavonási igény rögzítése.

A sikeresen rögzített visszavonási igényt a DÁP keretalkalmazás üzenethitelesítő kulcsával hitelesítve továbbítja a DÁP szolgáltatónak, aki saját, legalább minősített tanúsítványon alapuló fokozott biztonságú bélyegzőjével hitelesítve küldi tovább a Szolgáltató informatikai rendszere felé, mely a visszavonási kérés azonosítását és hitelesítését automatikusan végrehajtja, majd sikeres azonosítás és hitelesítés után szintén automatikusan végrehajtja a tanúsítvány visszavonását, azaz rögzíti a tanúsítványt a visszavont tanúsítványok nyilvántartásában. A tanúsítvány visszavont tanúsítványok nyilvántartásában való rögzítését követően a Szolgáltató informatikai rendszere saját, legalább minősített tanúsítványon alapuló fokozott biztonságú bélyegzőjével hitelesítve visszaigazolást küld a DÁP szolgáltatón keresztül az Aláíró részére a tanúsítvány visszavonásáról. A Szolgáltató visszaigazolását a DÁP szolgáltató e-mailbe foglalva az Aláíró DÁP profil aktiválása előtt ellenőrzött e-mail címére küldi ki.

3.9.3.2. Visszavonás webes felületen

Aláíró a saját mobileszközeihez és a hozzájuk regisztrált DÁP keretalkalmazásokhoz tartozó tanúsítványainak visszavonását a DÁP portálon keresztül az alábbiak szerint kezdeményezheti:

- a DÁP portál megfelelő menüpontjának megnyitása böngészőben;
- azonosítási és hitelesítési műveletek elvégzése;
- a visszavonási igény rögzítése.

A sikeresen rögzített visszavonási igényt a DÁP szolgáltató saját, legalább minősített tanúsítványon alapuló fokozott biztonságú bélyegzőjével hitelesítve küldi tovább a Szolgáltató informatikai rendszere felé, mely a visszavonási kérés azonosítását és hitelesítését automatikusan végrehajtja, majd sikeres azonosítás és hitelesítés után szintén automatikusan végrehajtja a tanúsítvány visszavonását, azaz rögzíti a tanúsítványt a visszavont tanúsítványok nyilvántartásában. A tanúsítvány visszavont tanúsítványok nyilvántartásában való rögzítését követően a Szolgáltató informatikai rendszere saját, legalább minősített tanúsítványon alapuló fokozott biztonságú bélyegzőjével hitelesítve visszaigazolást küld a DÁP szolgáltatón keresztül az Aláíró részére a tanúsítvány visszavonásáról. A Szolgáltató visszaigazolását a DÁP szolgáltató e-mailbe foglalva az Aláíró DÁP profil aktiválása előtt ellenőrzött e-mail címére küldi ki.

3.9.4. Kivárási idő visszavonási kérelem esetén

Szolgáltató nem alkalmaz kivárási időt a visszavonási kérelmek teljesítése során.

3.9.5. Visszavonási kérelem feldolgozásának időbelisége

Szolgáltató a benyújtott visszavonási kérelmet haladéktalanul, minden más típusú tevékenysége (így különösen tanúsítvány előállítása vagy kibocsátás) előtt feldolgozza, és az arra jogosult által benyújtott kérelmeket 24 órán belül teljesíti.

3.9.6. Visszavonás ellenőrzésének ajánlása az Érintett Felek számára

Az Érintett Feleknek a tanúsítvány és az ahhoz felépített tanúsítványlánc minden elemének visszavonási állapotát javasolt ellenőriznie a tanúsítványból megállapított vagy Szolgáltató által biztosított visszavonási információkból, melyek mind CRL, mind OCSP formájában elérhetőek.

3.9.7. CRL kibocsátási gyakoriság

A végfelhasználói tanúsítványokra Szolgáltató nem biztosít CRL kibocsátást.

A szolgáltatói tanúsítványokhoz kapcsolódó CRL kibocsátásának gyakorisága: 30 naponként legalább egy CRL. A kibocsátott CRL érvényessége 30 nap. A CRL tartalmazza a következő kibocsátás időpontját (a nextUpdate mezőben). Szolgáltató minden kibocsátáskor törli a CRL-ről azokat a tanúsítványokat, melyek érvényessége a CRL kibocsátásnak időpontjában már lejárt.

3.9.8. CRL előállítása és közzététele között leghosszabb idő

Szolgáltató a szolgáltatói tanúsítványokhoz kapcsolódó CRL-t az előállítását követően haladéktalanul, de legfeljebb egy órán belül közzéteszi.

3.9.9. OCSP szolgáltatás biztosítása

Szolgáltató a végfelhasználói és szolgáltatói tanúsítványokhoz OCSP szolgáltatást nyújt, a BSZ- DÁP-TAN 4.10 fejezetében ismertetett elérhetőségen, működési jellemzőkkel és rendelkezésre állással.

3.9.10. OCSP alapú visszavonás ellenőrzés követelményei

Az Érintett Feleknek az OCSP szolgáltatást javasolt elsődlegesen használnia a tanúsítványok visszavonási állapotának megállapítására, mivel ezen szolgáltatás keretében (ellentétben a CRL-el) Szolgáltató a lejárt tanúsítványokhoz is biztosítja a visszavonási állapot információt.

3.9.11. Visszavonási állapotközlés más formái

Szolgáltató nem alkalmaz egyéb visszavonási állapotközlési formát.

3.9.12. Különleges követelmények a kulcs kompromittálódása esetére

A Szolgáltató a szolgáltatói magánkulcsának kompromittálódása esetén az eseményről honlapján tájékoztatást tesz közzé, az Aláírókat a DÁP szolgáltatón keresztül értesíti.

A produktív hitelesítőközpont magánkulcsának kompromittálódása esetén Szolgáltató képes az összes érintett végfelhasználói tanúsítvány visszavonására, majd ezt követően, az adott szolgáltatói tanúsítvány visszavonására és az érintett CRL-nek a 12 órán belüli kibocsátására és közzétételére.

3.9.13. Felfüggesztés körülményei

A Szolgáltató nem nyújt felfüggesztési szolgáltatást.

3.9.14. Ki kérelmezhet felfüggesztést

Nincs kikötés.

3.9.15. Felfüggesztésre vonatkozó eljárás

Nincs kikötés.

3.9.16. A felfüggesztés megengedett időtartama

Nincs kikötés.

3.9.17. Működési jellemzők

Szolgáltató a szolgáltatói tanúsítványokhoz kapcsolódó visszavonási információkat mind CRL, mind OCSP formájában szolgáltatja.

Szolgáltató biztosítja, hogy a szolgáltatói tanúsítványokhoz kapcsolódó visszavonási állapot információ változása mind a CRL, mind az OCSP szolgáltatásban azonosan, konzisztens módon megjelenik, figyelembe véve az egyes szolgáltatásokban eltérő frissítési időket is.

Szolgáltató a végfelhasználói (aláírói) tanúsítványokhoz kapcsolódó visszavonási információkat kizárólag OCSP formájában szolgáltatja.

3.9.18. CRL

A Szolgáltató által a szolgáltatói tanúsítványokhoz kibocsátott CRL megfelel a {Sz16} RFC 5280 szabványnak.

A CRL tartalmaz minden olyan visszavont szolgáltatói tanúsítványt, melyek érvényessége a CRL kibocsátásának időpontjában nem járt még le.

A CRL minden esetben tartalmazza a következő kibocsátás időpontját (`nextUpdate`). A záró CRL (az adott hitelesítőközpont által kiadott utolsó CRL) esetén a `nextUpdate` mező tartalma a „99991231235959Z” RFC 5280 szerinti speciális időpont. Szolgáltató biztosítja, hogy az új CRL kibocsátása a `nextUpdate` mezőben jelzett időpont előtt minden esetben megtörténik

A Szolgáltató záró CRL-t bocsát ki, amikor egy adott hitelesítőközpont működtetését megszünteti:

- kulcs átállás miatt; vagy
- a szolgáltatói magánkulcs kompromittálódása miatt; vagy
- a szolgáltatói tevékenység megszüntetése miatt.

A Szolgáltató csak azt követően bocsátja ki a záró CRL-t, miután minden, az adott hitelesítőközpont által kibocsátott tanúsítvány lejárt vagy azok visszavonását elvégezte. Szolgáltató (illetve a szolgáltatási tevékenység megszüntetése esetén a szolgáltatás átvevő bizalmi szolgáltató) a záró CRL kibocsátását követő 10 évig biztosítja a záró CRL elérhetőségét.
Szolgáltató a CRL aláírásához ugyanazt a szolgáltatói magánkulcsot használja, melyet a kérdéses tanúsítvány aláírására használt.

A szolgáltatói tanúsítványokra vonatkozó CRL elérhetősége: *http://qca.hiteles.gov.hu/crl/GOVCA-ROOT.crl*

3.9.19. OCSP

A Szolgáltató által biztosított OCSP szolgáltatás megfelel az {Sz18} RFC 6960 szabványnak.

Az OCSP szolgáltatást Szolgáltató az {Sz18} RFC 6960 2.2 fejezetében meghatározott "Authorized Responder" elvnek megfelelően működteti.

Az OCSP szolgáltatás keretében csak olyan tanúsítványra vonatkozóan kerül pozitív („good” státuszt tartalmazó) válasz kiadásra, amely tanúsítványt az adott hitelesítőközpont bocsátott ki (azaz szerepel a tanúsítványtárban) és a tanúsítvány nincs visszavont állapotban.

Az OCSP kérésekre vonatkozó szabályok a következők:

- a Nonce (Single Request Extension) használata nem kötelező, de erősen javasolt,

- kritikusnak jelölt kiterjesztést nem szabad használni, az ilyen kéréseket a kiszolgáló MALFORMED hiba válasszal (Responder Error: malformedRequest) elutasítja.

Az OCSP választ aláíró tanúsítvány visszavonási állapotát nem kell ellenőrizni. Ennek jelzésére az OCSP válaszadó tanúsítványában szerepel az id-pkix-ocsp-nocheck kiterjesztés.

Az OCSP szolgáltatás keretében a Szolgáltató biztosítja a visszavonási információt a tanúsítvány lejáratát követően is, 10 évig, illetve az érintett központ működtetési időtartamában.

Végfelhasználói tanúsítványokra vonatkozó OCSP szolgáltatás elérhetősége:

http://dapca.hiteles.gov.hu/ocsp/dap-ca

Szolgáltatói tanúsítványokra vonatkozó OCSP szolgáltatás elérhetősége:

http://qca.hiteles.gov.hu/ecc/ocsp-root

3.9.20. Szolgáltatás rendelkezésre állása

A szolgáltatói tanúsítványokra vonatkozó CRL, illetve az OCSP szolgáltatás az év minden napján, napi 24 órában elérhető, éves szinten 99,9%-os rendelkezésre állással, úgy, hogy egy eseti szolgáltatáskiesés nem lépheti túl a 3 órás időtartamot.

3.9.21. Az előfizetés vége

Aláíró szerződéses viszonya megszűnik a tanúsítvány lejáratával vagy, ha a tanúsítvány érvényességének lejárata előtt az Aláíró kérésére vagy bármely más okból kifolyólag (pl. az Aláíró DÁP felhasználói profiljának inaktiválása esetén) a tanúsítvány visszavonásra kerül.

3.10. Kulcsletét és visszaállítás

Szolgáltató nem nyújt kulcsletét és visszaállítás szolgáltatást.

4. Tanúsítvány profilok

4.1. Tanúsítvány profilok

A Szolgáltató által kiadott tanúsítványok megfelelnek az {Sz9} ITU-T X.509, {Sz16} RFC 5280, {Sz17} RFC 6818, {Sz4} EN 319 412-1, {Sz5} EN 319 412-2, {Sz6} EN 319 412-5 műszaki szabványoknak, valamint a vonatkozó jogszabályi előírásoknak.

A tanúsítványprofil részletes leírását a {D8} dokumentum tartalmazza, melyet Szolgáltató igény esetén az Érintett Felek rendelkezésére bocsát.

4.1.1. Verziószám

A tanúsítványok verziószáma: V3.

4.1.2. Tanúsítvány kiterjesztések

A tanúsítványokban alkalmazott kiterjesztések mindenben követik az {Sz16} RFC 5280 és az {Sz4} EN 319 412-1, {Sz5} EN 319 412-2, {Sz6} EN 319 412-5 műszaki szabványok, valamint a vonatkozó jogszabályok előírásait.

Szolgáltató az Aláírók tanúsítványaiban az alábbi, minősített tanúsítványokra vonatkozó nyilatkozatokat tartalmazó, nem kritikusnak megjelölt szabványos kiterjesztéseket (`qcStatements`) alkalmazza:

- `etsi-qcs-QcEuCompliance`,
  mely a tanúsítvány megfelelését igazolja az {J1} eIDAS minősített tanúsítványokra vonatkozó követelményeinek;
- `etsi-qcs-QcRetentionPeriod`,
  mely az 5.5.2 Archívum megőrzési időtartama pont szerinti időtartamot jelzi.
- `etsi-qcs-QcQSCD`,
  mely a tanúsítványba foglalt nyilvános kulcs magánkulcs párjának QSCD-n történő kezelését igazolja;
- `etsi-qcs-QcType`,
  mely azt jelzi, hogy a tanúsítvány aláíró tanúsítvány, azaz alanya magánszemély, értéke: `qct-esig`

4.1.3. Algoritmus azonosítók

A tanúsítványok aláírásához alkalmazott algoritmus azonosító az alábbi:

```
ecdsaWithSHA384
{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3)
ecdsa-with-SHA384(3)}
```

4.1.4. Név formák

A név formák leírását és azok értelmezési szabályait a **Hiba! A hivatkozási forrás nem található.** fejezet t artalmazza.

4.1.5. Név megszorítások

A Szolgáltató a tanúsítványokban név megszorításokat (`NameConstraints`) nem tüntet fel.

4.1.6. Hitelesítési rend objektumazonosító

A Szolgáltató a tanúsítványokban feltünteti a hitelesítési rendek objektumazonosítóját. (lásd 1.2.1 fejezet)

4.1.7. Szabályzati megszorítások kiterjesztés használata

Szolgáltató a tanúsítványban szabályzati megszorításokat (`PolicyConstraints`) nem tüntet fel.

4.1.8. Szabályzat minősítők szintaktikája és szemantikája

Szolgáltató a tanúsítványban szabályzat minősítőket (`PolicyQualifiers`) és az ennek megfelelő tanúsítvány alkalmazhatóságra vonatkozó szöveg (`UserNotice`) nem tüntet fel.

4.1.9. A kritikus hitelesítési rendek (Certificate Policies) kiterjesztés feldolgozása

A tanúsítvány hitelesítési rendek (`CertificatePolicies`) kiterjesztése nincs kritikusként megjelölve.

4.2. CRL profil

A Szolgáltató által kiadott, a szolgáltatói tanúsítványokra vonatkozó visszavonási listák megfelelnek az {Sz16} RFC 5280 műszaki szabványnak.

A CRL profil részletes leírását a {D8} dokumentum tartalmazza, melyet Szolgáltató igény esetén az Érintett Felek

rendelkezésére bocsát.

4.2.1. Verziószám

A visszavonási listák verziószáma: V2.

4.2.2. CRL és CRL bejegyzés kiterjesztések

A visszavonási lista az alábbi kiterjesztéseket tartalmazza "nem kritikus" megjelöléssel:

`CRLNumber`	a visszavonási lista szigorúan növekvő sorszáma
`AuthorityKeyIdentifier`	a kibocsátó CA kulcs azonosítója

A visszavonási lista a fentieken túl más szabványos kiterjesztést is tartalmazhat, azonban ezen kiterjesztések nem lehetnek "kritikus" jelzésűek.

Mivel a Szolgáltató a lejárt tanúsítványokhoz CRL formájában nem (csak OCSP formájában) biztosít visszavonási információt, a CRL soha nem tartalmazza az `ExpiredCertsOnCRL`kiterjesztést.

4.3. OCSP profil

A Szolgáltató által biztosított OCSP szolgáltatás megfelel az {Sz18} RFC 6960 műszaki szabványnak.

Ha az OCSP válaszadó olyan tanúsítvány állapotára vonatkozó kérést kap, amelyet még nem adtak ki, akkor a válaszadó nem válaszolhat "good" („rendben”) állapottal az {Sz12} RFC 6960 2.2. fejezete szerint. Ilyen esetekben az OCSP válaszadó „revoked (certificatehold)” választ adja vissza.

Az OCSP profil részletes leírását a {D8} dokumentum tartalmazza, melyet Szolgáltató igény esetén az Érintett Felek rendelkezésére bocsát.

4.3.1. Verziószám

Az OCSP válaszok verziószáma: V1.

4.3.2. OCSP kiterjesztések

A Szolgáltató az {Sz18} RFC 6960 által meghatározott kiterjesztések (Nonce, CRL References, Acceptable Response Types, nocheck, Archive Cutoff, CRL Entry Extensions, Service Locator, Preferred Signature Algorithms) közül az alábbiakat támogatja: Nonce, Archive Cutoff

Az OCSP válasz az alábbi kiterjesztéseket tartalmazza "nem kritikus" megjelöléssel:

`Nonce`	az OCSP kérésben megadott, visszajátszásos támadások megelőzésére szolgáló véletlenszám (csak akkor, ha a kérés tartalmazta azt)
`ArchiveCutoff`	jelzi, hogy a Szolgáltató a tanúsítvány lejárata után is biztosítja a visszavonási státuszt, a 3.9.17 fejezetben megadott időtartamig

Az `ArchiveCutoff` kiterjesztés az {Sz3} EN 319 411-2 szabvány 6.3.10-10 pontja szerinti dátumot, illetve időpontot tartalmazza.

Az OCSP válasz a fentieken túl más szabványos kiterjesztést is tartalmazhat, azonban ezen kiterjesztések nem lehetnek "kritikus" jelzésűek.

5. Megfelelősség vizsgálata

A Szolgáltató felügyeleti szerve a Nemzeti Média- és Hírközlési Hatóság.

A Bizalmi Felügyelet ellátja a Szolgáltató és az általa nyújtott Szolgáltatás felügyeletét, ellenőrzi a Szolgáltatás jogszabályi megfelelőségét. Többek között figyelemmel kíséri a bizalmi szolgáltatásokkal kapcsolatos technológia és kriptográfiai algoritmusok fejlődését és határozatba foglalja a bizalmi szolgáltatók által a szolgáltatásaik nyújtása során használható biztonságos kriptográfiai algoritmusokat, és az azok meghatározott paraméterekkel történő alkalmazására vonatkozó követelményeket, továbbá jogerős és végrehajtható határozatában elrendelheti a bizalmi szolgáltatások keretében kibocsátott tanúsítványok felfüggesztését vagy visszavonását.

A Szolgáltató tevékenységének fentiekben felsorolt jogszabályok és szabványok, valamint műszaki-technikai specifikációknak és a jelen Szolgáltatási Kivonatnak, valamint a vonatkozó Hitelesítési Rendnek történő megfelelőségét külső tanúsító szerv évente ellenőrzi.

A tanúsító szervezettel szembeni követelmények:

- Függetlenég
- Akkreditáció ISO/IEC 17065:2013 szabvány alapján az alábbi tanúsítási területekre:
    - Informatikai biztonsági funkciókat megvalósító szoftver termékek
    - Informatikai biztonsági funkciókat megvalósító elektronikus információs rendszerek
    - Zárt elektronikus információs rendszerek
    - Elektronikus aláírási termékek
    - Elektronikus aláírási rendszerek
- Akkreditáció EN 319 403-1:2020 szabvány alapján az alábbi tanúsítási területekre:
    - 910/2014/EU rendelet szerinti bizalmi szolgáltatást lehetővé tevő rendszerek, elektronikus aláírások és infrastruktúrák
- Rendelkezik a Szolgáltatásra vonatkozó tanúsítási rendszerrel

Az ellenőrzés eredményéről megfelelőségértékelési jelentés készül.

A megfelelőségértékelési igazolás és jelentés azonosítója, valamint az igazolt követelmények hivatkozása:

Az értékelés alapját képező szabályozások és iparági szabványok:

- 910/2014/EU Európai Parlament és a Tanács rendelete a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről (továbbiakban: eIDAS)

- 2023. évi CIII. Törvény a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól (továbbiakban: Dáp tv.)

- 541/2020. (XII. 2.) Korm. Rendelet a bizalmi szolgáltatások esetében a személyes jelenléttel egyenértékű biztosítékot nyújtó, nemzeti szinten elismert egyéb azonosítási módszerekről

- 2013. évi V. törvény a Polgári Törvénykönyvről (továbbiakban: Ptk.)

- 24/2016 (VI. 30.) BM rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről

- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates

- ETSI TS 119 431-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev

- ETSI TS 119 431-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation

- ETSI TS 119 461 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects

- MSZ EN 419241-1 Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements

- MSZ EN 419241-2 Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing

- ITU-T x.509 Public-key and attribute certificate frameworks

- ISO/IEC 27001:2013 Információbiztonsági szabvány

- NIST 800-53 Security and Privacy Controls for Information Systems and Organizations

A Szolgáltató a megfelelő működés biztosítása érdekében folyamatos belső ellenőrzést tart fenn.

A belső megfelelőség értékelést végző bizalmi szerepkört betöltő biztonsági tisztviselő és független rendszervizsgáló függetlenek és befolyásmentesek a Szolgáltatás nyújtásával kapcsolatos szervezeti egységektől.

6. Egyéb üzleti és jogi információk

6.1. Díjak

6.1.1. Tanúsítvány kibocsátás díja

A Szolgáltató a tanúsítvány kibocsátásáért díjat nem számít fel.

6.1.2. Tanúsítványhozzáférés díja

A Szolgáltató a közzétett tanúsítványok eléréséért nem számít fel díjat.

6.1.3. Visszavonási és állapot információ hozzáférés díja

A Szolgáltató nem számít fel díjat a tanúsítványok visszavonási állapotára vonatkozó státusz információk (CRL és OCSP) szolgáltatásáért.

6.1.4. Egyéb szolgáltatások díja

Nincs kikötés.

6.1.5. Visszatérítési szabályzat

Visszatérítéssel kapcsolatos rendelkezéseket a Szolgáltató nem állapít meg.

6.2. Anyagi felelősség

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

6.2.1. Biztosítási fedezet

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.

A szolgáltatói felelősségvállalás maximális összege:

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

A felelősségbiztosítás a fentieken túl kiterjed az alábbiakra is:

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

6.2.2. További követelmények

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

6.2.3. Felelősségbiztosítás vagy garancia végfelhasználók számára

Nincs kikötés.

6.3. Üzleti információk bizalmassága

6.3.1. Bizalmasan kezelendő információk köre

A Szolgáltató minden olyan adatot és információt bizalmasnak tekint, melyek nem kerültek tételes felsorolásra a BSZ-DÁP- TAN 9.3.2 fejezetében.

6.3.2. Bizalmasnak nem tekintett információk köre

Nem bizalmasnak tekintetett információk az alábbiak:

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

6.3.3. Bizalmas információk védelmének felelőssége

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.

6.4. Személyes adatok védelme

6.4.1. Adatvédelem

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.

Szolgáltató adatvédelmi tájékoztatója {D4} elérhető Szolgáltató internetes honlapján.

6.4.2. Bizalmasként kezelendő személyes adatok

A Szolgáltató az Aláírótól, annak kifejezett hozzájárulásával, közvetett módon, a DÁP szolgáltatón keresztül gyűjt személyes adatot, csak olyan mértékben, ami a tanúsítvány kiállításához, valamint az Aláíró tájékoztatásához, személyazonosságának megállapításához szükséges. A Szolgáltató ezen adatokat bizalmasan kezeli.

6.4.3. Bizalmasként nem kezelendő személyes adatok

A Szolgáltató nem tekinti bizalmasként kezelendő személyes adatnak a tanúsítványokhoz kapcsolódó státusz információt. A státusz információba beleértendő a tanúsítvány - esetleges - visszavonásának oka és időpontja is.

6.4.4. Személyes adatok védelmének felelőssége

A Szolgáltató gondoskodik a személyes adatok védelméről, működése és szabályzatai megfelelnek a {J6} GDPR rendelkezéseinek.

6.4.5. Személyes adatok felhasználásának elfogadása

Az Aláírónak az ÁSZF elfogadásával létrejött Szolgáltatási Szerződés keretében tudomásul kell vennie a tanúsítvány kiállításához és a szerződés megkötéséhez szükséges adatok Szolgáltató által történő nyilvántartásba vételét, kezelését és tárolását. Tekintettel arra, hogy a Szolgáltató adatkezelésének jogalapja jogi és szerződési kötelezettség teljesítése, a {J6} GDPR szerinti hozzájárulás nem értelmezhető.

6.4.6. Felfedés hatósági vagy polgári peres eljárás keretében

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. A Szolgáltató rögzíti az adatátadás tényét, de arról nem tájékoztatja az érintett Aláírót.

A Szolgáltató a tanúsítvány érvényességét érintő polgári peres, illetve nem peres eljárás során - az érintettség igazolása esetén - az ellenérdekű peres félnek vagy képviselőjének, valamint a megkereső bíróságnak feltárhatja a jogszabályban meghatározott bizalmas információkat. a Szolgáltató rögzíti az adatátadás tényét, és arról tájékoztatja az érintett Aláírót.

6.4.7. Egyéb, felfedést eredményező körülmények

A Szolgáltató a szolgáltatási tevékenység, illetve a Szolgáltatások nyújtásának megszüntetése esetén az Aláíró adatait a jogszabályi kötelezettségeire tekintettel átadja harmadik félnek.

6.5. Szellemi tulajdonjogok

A Szolgáltató által az Aláíró részére kibocsátott tanúsítvány tulajdonosa az Aláíró. A Szolgáltató a tanúsítványt a kikötéseiben és feltételeiben ismertetett esetekben és módon sokszorosíthatja, visszavonhatja és egyéb módon is kezelheti. A végfelhasználói tanúsítványban szereplő megkülönböztető név használatára az Aláíró jogosult.

A Szolgáltató tulajdonát képezik a szolgáltatói tanúsítványok, visszavonási információk, a végfelhasználói tanúsítványokban szereplő, Szolgáltató által létrehozott azonosítók.

A 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.

6.6. Tevékenységért viselt felelősség és helytállás

6.6.1. Szolgáltató felelőssége és helytállása

A Szolgáltató felel a bizalmi szolgáltatási rendben és a 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.

A Szolgáltató a vele szerződéses jogviszonyban nem álló harmadik személlyel szemben a {J3} Polgári Törvénykönyv 6:519. §-a szerint, a vele szerződéses jogviszonyban álló Aláíróval szemben a szerződésszegésért való felelősség ({J3} Polgári Törvénykönyv 6:142. §) szabályai szerint felelős az elektronikus aláírással hitelesített elektronikus dokumentummal okozott kárért, ha megszegte a bizalmi szolgáltatási rendben és a 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. A Szolgáltató sajátjaként felel a Közreműködő Felek vagy egyéb alvállalkozók által a Szolgáltatások nyújtása során okozott kárért.

A Szolgáltató a felelősségi körén belül keletkezett, bizonyított károkért, az Aláíróval az ÁSZF elfogadásával létrejött Szolgáltatási Szerződésben és a 6. fejezetben foglalt korlátozásokkal kártérítést fizet.

A Szolgáltató nem felel:
- az Érintett Felek tanúsítvány ellenőrzési és felhasználási tevékenységeiért;
- az Érintett Felek vagy mások által kibocsátott szabályzatokért.

Szolgáltató kötelezettsége

Szolgáltató azzal, hogy szolgáltatási szabályzat hatálya alatt kibocsát egy aláírói tanúsítványt, arra vállal kötelezettséget, hogy a Szolgáltatások nyújtása során ő maga és a Szolgáltatások nyújtásában Közreműködő Felek szabályzatban foglaltakat maradéktalanul betartják. Szolgáltató megteszi a szükséges és tőle telhető intézkedéseket ahhoz, hogy Aláírók is a szolgáltatási szabályzat előírásainak megfelelően járjanak el.

6.6.2. A regisztrációs szervezet felelőssége

A Szolgáltató regisztrációs szervezetének felelőssége a tanúsítványkibocsátások BSZ-DÁP-TAN szerinti megfelelőségének időszakos ellenőrzése a Szolgáltató vonatkozó belső szabályzatainak megfelelően.

6.6.3. Aláíró felelőssége és helytállása

6.6.3.1. Aláíró jogai

- Aláíró jogosult a Szolgáltatások igénybevételére szolgáltatási szabályzatban és az Általános Szerződési Feltételekben leírtak szerint.
- Aláíró akkor jogosult tanúsítványt igényelni, ha korábban bekerült a digitális állampolgárság nyilvántartásba és rendelkezik DÁP azonosítóval.
- Aláíró jogosult a számára kiadott tanúsítvány visszavonását kérni.

6.6.3.2. Aláíró felelőssége

- Aláíró felelős a regisztráció során megadott adatai valódiságáért, pontosságáért és érvényességéért.
- Aláíró felelős a tanúsítványban szereplő adatok ellenőrzéséért.
- Aláíró felelős azért, hogy a tanúsítványt érintő összes adatának megváltozását haladéktalanul bejelentse, beleértve mindazon adataiban bekövetkezett változásokat is, melyeket a regisztrációs eljárás és a Szolgáltatási Szerződés megkötése során megadott.
- Aláíró felelős a magánkulcs aktivizáló adatának és a visszavonási jelszónak a biztonságos kezeléséért.
- Aláíró felelős azért, hogy a magánkulcs és a kapcsolódó tanúsítvány használatát haladéktalanul és végérvényesen beszüntesse, amennyiben tudomására jut, hogy a Szolgáltató valamely, a tanúsítvány kibocsátásában érintett hitelesítőközpontja kompromittálódott.
- Aláíró felelős Szolgáltatót haladéktalanul értesíteni és teljeskörűen tájékoztatni a szolgáltatást is érintő vitás ügyekben.
- Aláíró felelős a Szolgáltatási Szerződésben és a {D1} Általános Szerződési Feltételekben meghatározott kötelezettségei betartásáért.

6.6.3.3. Aláíró kötelezettsége

- Aláíró köteles a Szolgáltatások igénybevétele előtt szolgáltatási szabályzatot megismerni.
- Aláíró köteles tudomásul venni, hogy Szolgáltató a tanúsítványt a szolgáltatási szabályzatban leírt módon és eljárásokkal bocsátja ki.
- Aláíró köteles a Szolgáltatások igénybevételéhez szükséges adatokat hiánytalanul és a valóságnak megfelelően szolgáltatni.
- Aláíró köteles tudomásul venni, hogy a számára kibocsátott tanúsítványban a jogszabályokban előírt adatok befoglalásra kerülnek.
- Aláíró köteles a tanúsítványba foglalt bármely adata megváltozása esetén haladéktalanul kérni a tanúsítvány visszavonását.
- Aláíró kötelezettsége, hogy a tanúsítványt és a kapcsolódó magánkulcsot, csak jogszabályokban

megengedett és nem tiltott célra, valamint a szabályzatokban és hivatkozott dokumentumokban foglaltaknak megfelelően használja.
- Aláíró köteles biztosítani, hogy a Szolgáltatások igénybevételéhez szükséges - saját hatáskörébe tartozó - adatokhoz és eszközökhöz illetéktelen személyek ne férhessenek hozzá.
- Aláíró köteles Szolgáltatót haladéktalanul írásban értesíteni, amennyiben valamely a Szolgáltatásokban kiadott tanúsítvánnyal vagy azon alapuló elektronikus aláírással kapcsolatban jogvita indul.
- Aláíró haladéktalanul köteles a magánkulcs nem jogszerű használatának vagy kompromittálódásának gyanúja esetén a tanúsítvány visszavonását kérni.
- Aláíró köteles tudomásul venni, hogy Szolgáltató jogosult a tanúsítványt visszavonni, amennyiben Aláíró a Szolgáltatási Szerződést megszegi vagy Szolgáltató tudomására jut, hogy a tanúsítványt illegális tevékenységhez használták.
- Aláíró köteles tudomásul venni, hogy Szolgáltató a tanúsítványt a Felügyeleti Szerv erre vonatkozó határozata esetén visszavonja.

6.6.4. Érintett Felek felelőssége és helytállása

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 szolgáltatási szabályzatban foglalt követelmények és előírások betartása;
- megbízható informatikai környezet és alkalmazások használata;
- a tanúsítvány felhasználására vonatkozó valamennyi korlátozás figyelembevétele, amely a tanúsítványban vagy a szolgáltatási szabályzatban szerepel
- a tőle elvárható magatartás tanúsítása a tanúsítvány ellenőrzésekor.

Szolgáltató kizárja a felelősségét, amennyiben az Érintett Fél a tanúsítvány vagy az azon alapuló elektronikus aláírás elfogadásakor nem körültekintően, vagy nem a tőle elvárható gondossággal jár el.

6.6.5. Egyéb felek felelőssége és helytállása

Nincs kikötés.

6.7. Helytállás érvénytelenségi köre

A Szolgáltató kizárja felelősségét, amennyiben:
- az Érintett Fél nem körültekintően jár el a tanúsítványok ellenőrzése és felhasználása során, azaz nem a szolgáltatási szabályzatnak vagy a hatályos jogszabályoknak megfelelően jár el;
- az Aláíró nem tartja be a magánkulcs aktiválóadatának kezelésével kapcsolatos előírásokat;
- az Érintett Felek vagy mások által kibocsátott szabályzatok nem felelnek meg a bizalmi szolgáltatási szabályzatnak;
- az Internet, vagy annak egy részének működési hibájából fakadóan tájékoztatási vagy egyéb kommunikációs kötelezettségeit nem tudja ellátni;
- az Aláíró nem tesz eleget a szolgáltatási szabályzatban előírt kötelezettségeinek;.

6.8. Felelősség korlátozása

A Szolgáltató korlátozza a kártérítési felelősségét:
- a szolgáltatói felelősségvállalás maximális összegét meghaladó ügyletekben aláírt elektronikus dokumentumokból származó károk tekintetében, mely tanúsítványonként és káreseményenként maximum 50 millió magyar forint (HUF);
- összességében az összes tanúsítvánnyal és káreseménnyel kapcsolatban fizetendő kártérítési összeg tekintetében, mely éves szinten maximum 1 milliárd magyar forint (HUF).

A Szolgáltató nem felelős az olyan károkért, melyek abból adódnak, hogy az Érintett Fél a tanúsítványok ellenőrzése és felhasználása során nem a hatályos jogszabályok és a mérvadó műszaki szabványok szerint járt el, illetve nem tanúsította a tőle elvárható gondosságot.

A Szolgáltató pénzügyi felelősségének korlátját a Szolgáltatási Szerződés, illetve a {D1} Általános Szerződéses 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.

6.9. Kártérítések

A kártérítésekről a jelen Szolgáltatási Kivonat 6. fejezetében leírtakon túl az {D1} Általános Szerződési Feltételek rendelkeznek.

6.10. Egyéni hirdetmények és kommunikáció a részvevőkkel

Azokban az esetekben, melyekre a 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.

6.11. Módosítások

6.11.1. Módosítás eljárása

A szolgáltatási szabályzat módosítása az 1.4.2 fejezetekben leírt szabályok szerint történik. A szolgáltatási szabályzat módosulását a verziószám megfelelő változása jelzi.

6.11.2. Értesítés módszere és időtartama

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.

6.11.3. OID megváltozását előidéző körülmények

A szolgáltatási szabályzat OID-ja nem változik.

6.12. Vitás kérdések rendezése

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.

Panaszt a Telefonos Ügyfélszolgálat postacímére írásban, 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.

Bármely vitás kérdés felmerülése esetén Aláíró jogosult az esetleges bírósági eljárást megelőzően békéltető testülethez fordulni. Az illetékes békéltető testület megnevezését és elérhetőségeit ÁSZF-DÁP 1.5.1 fejezete tartalmazza.

A jogviták esetén követendő eljárást a {D1} Általános Szerződési Feltételek tartalmazza.

6.13. Irányadó jog

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

6.14. Hatályos jognak megfelelés

A Szolgáltató tevékenységét a mindenkor hatályos Európai Uniós, illetve magyar jogszabályoknak megfelelően végzi.

6.15. Vegyes rendelkezések

6.15.1. Teljességi záradék

Nincs kikötés.

6.15.2. Átruházás

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.

6.15.3. Részleges érvénytelenség

A szolgáltatási szabályzat egyes rendelkezéseinek tetszőleges okból történő érvénytelenné válása esetén a többi rendelkezés változatlan formában érvényben marad.

6.15.4. Igényérvényesítés

A Szolgáltató kártérítésre, az ügyvédi díjak megfizetésére tarthat igényt a partnerei által okozott károk, veszteségek, költségek megtérítése érdekében. Amennyiben 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.

6.15.5. Force Majeure (Vis maior)

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 szükséghelyzet) minősül vis maiornak, amely megakadályozza vagy lehetetlenné teszi a szolgáltatási

szabályzatban foglalt követelmény teljesítését, feltéve, hogy ezen körülmények a szolgáltatási szabályzat hatálybalépését követően keletkeznek, illetőleg azt megelőzően következtek be, ám a szolgáltatási szabályzat teljesítésére kiható következményeik az említett időpontban még nem voltak előre láthatóak.

A Szolgáltató nem felelős a vis maior esetekből fakadó károkért.

6.16. Egyéb rendelkezések

6.16.1. Hozzáférhetőség a fogyatékossággal élő személyek számára

Szolgáltató a Szolgáltatásokat és a Szolgáltatások során alkalmazott végfelhasználó termékeket hozzáférhetővé teszi a fogyatékossággal élő személyek számára.