NISZ

Nemzeti Infokommunikációs Szolgáltató Zrt.

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)

Verziószám	1.4
OID	0.2.216.1.200.1100.100.42.3.1.37
Hatályba lépés dátuma	2025.02.05.
Dokumentum besorolása	nyilvános
Jóváhagyó	Adorján István

Adorján István

Digitálisan aláírta: Adorján István
Dátum: 2025.02.04 09:36:55 +01'00'

Változáskövetés

verzió	dátum	a változás leírása	készítette	ellenőrizte	jóváhagyta
0.1	2024.07.30	első változat	NISZ Zrt. Polysys Kft. ACPM Zrt.		
0.2	2024.11.06	Továbbfejlesztett változat	Kővári-Szabó Zoltán	ACPM Zrt. Nagy Benjámin	
1.0	2024.11.29	Első jóváhagyott verzió	Kővári-Szabó Zoltán	ACPM Zrt. Nagy Benjámin	Adorján István
1.1	2024.12.13	Megfelelőségértékelés észrevételeinek alkalmazása	Kővári-Szabó Zoltán	Nagy Benjámin	Adorján István
1.2	2024.12.17	Aláírásformátum pontosítása, hatálybalépés napjának módosítása.	Kővári-Szabó Zoltán	Nagy Benjámin	Adorján István
1.3	2025.01.28	• Aktivizáló adat rontott bevitelére vonatkozó korlátozás követelményével való kiegészítés • A 2024. évi LXIX. törvény 116. § által hatályon kívül helyezett, az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényre (Ibtv.) hivatkozó szövegrészek törlése. • Elütések javítása.	Kővári-Szabó Zoltán	Nagy Benjámin	Adorján István
1.4	2025.02.03	A Bizalmi felügyelet észrevételei alapján további pontosítások	Gál Ferenc Nagy Benjámin	Kővári-Szabó Zoltán	Adorján István

Tartalomjegyzék

1 BEVEZETÉS

Jelen dokumentum a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. (a továbbiakban, mint Kormányzati Hitelesítés Szolgáltató vagy Szolgáltató) Bizalmi Szolgáltatási Rendje, amely a Digitális Állampolgárság Program keretében megvalósított elektronikus aláírás funkcióhoz szükséges minősített bizalmi szolgáltatások nyújtására és igénybevételére vonatkozik.

A Szolgáltató a fenti tárgykörben a {D11} BSZ-DÁP-TK szolgáltatási szabályzatban meghatározott szolgáltatás keretében kibocsátott minősített tanúsítványokhoz kapcsolódóan alábbi szolgáltatást nyújtja:

> A Digitális Állampolgárság Program (DÁP) keretében elektronikus aláírások létrehozása és távoli elektronikus aláírást létrehozó eszközök kezelése (a továbbiakban: DÁP-TK szolgáltatás vagy Szolgáltatás).

A DÁP-TK szolgáltatás a {D9} BSZ-DÁP-TAN szolgáltatási szabályzatban meghatározott DÁP-TAN szolgáltatás kiegészítő szolgáltatása, mely a {J1} eIDAS 3. cikk 16. pont c) és f) alpontjában megfogalmazott, alábbi bizalmi szolgáltatásoknak felel meg:

- *elektronikus aláírások létrehozása;*
- *távoli elektronikus aláírást létrehozó eszközök kezelése.*

Jelen dokumentum a DÁP-TK szolgáltatás eljárásrendi és működési szabályait tartalmazza.

A Szolgáltató a Szolgáltatásait a vele szerződéses viszonyban álló állampolgárok (a továbbiakban: Aláírók) részére nyújtja, de egyes szolgáltatási elemeket hozzáférhetővé tesz az elektronikus aláírások hitelességét ellenőrző Érintett Felek részére is.

1.1 Áttekintés

Jelen bizalmi szolgáltatási rend egy olyan szabálygyűjtemény, amely DÁP-TK szolgáltatás nyújtásának és igénybevételének feltételeit és biztonsági követelményeit rögzíti és meghatározza azokat a követelményeket, melyeket a Szolgáltatónak a Szolgáltatások nyújtása során teljesítenie kell.

Jelen bizalmi szolgáltatási rend az {Sz9} RFC 3647 nemzetközi ajánlás alapján készült, felépítésében és tartalmában – a szükséges, Szolgáltatóra és DÁP-TK szolgáltatásra specifikus eltérésektől eltekintve – szigorúan követi annak előírásait. Az ott meghatározott felépítés szigorú megtartása érdekében azok az ajánlás által meghatározott fejezetek is szerepelnek a dokumentumban, melyeknél jelen {D11} BSZ-DÁP-TK kereteiben nincs követelmény előírva; ezekben a fejezetekben a "Nincs kikötés" szöveg szerepel.

Jelen bizalmi szolgáltatási rend előírja a Szolgáltatás nyújtása során teljesíteni szükséges összes követelményt, melyeket az alábbi nemzetközi szabványok határoznak meg:

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

Ezen követelmények teljesítésének módját, illetve az itt megnevezett eljárások részletes leírását a „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) dokumentum {D11} tartalmazza.

1.2 Dokumentum neve és azonosítása

1.2.1 A dokumentum neve

Jelen bizalmi szolgáltatási rend teljes neve: NISZ Zrt. "Bizalmi Szolgáltatási Rend a Digitális Állampolgárság Program keretében nyújtott elektronikus aláírások létrehozása és távoli elektronikus aláírást létrehozó eszközök kezelése minősített bizalmi szolgáltatáshoz".

A bizalmi szolgáltatási rend rövid neve: BR-DÁP-TK.

A bizalmi szolgáltatási rend objektum azonosítója és verziószáma a címlapon található.

Jelen BR-DÁP-TK hatályba lépését és hatályának megszűnését a 9.10 fejezet tartalmazza.

Jelen BR-DÁP-TK-nak csak a Szolgáltató elektronikus bélyegzőjével vagy a Szolgáltatásokért felelős vezető elektronikus aláírásával ellátott változata tekinthető hitelesnek.

1.2.2 A dokumentum azonosítása

A BR-DÁP-TK a DÁP tv. 8. § 5. pontja szerinti *bizalmi szolgáltatási rend*, mely a DÁP-TK szolgáltatás eljárásrendi és működési szabályait tartalmazza és amely egyúttal az ETSI EN 319 401 szerinti ún. *„trust service policy”*-nek és az ETSI TS 119 431-1 4.3.2 pontja szerinti ún. *„SSASC policy”*-nek tekintendő.

1.2.3 Hitelesítési rendek

A jelen BR-DÁP-TK bizalmi szolgáltatási rend az {Sz3} TS 119 431-1 szabvány 4.3.2 és A.2 fejezetében definiált `eu-remote-qscd` (OID: 0.4.0.19431.1.1.3) hitelesítési rendnek (EUSCP – EU SERVICE COMPONENT POLICY).

1.3 PKI közösség

Jelen bizalmi szolgáltatási rendben szereplő PKI közösség az alábbi felekből áll:

- Szolgáltató: a jelen BR-DÁP-TK-nak megfelelő bizalmi szolgáltató, amely a magánkulcsok tárolásával és aktiválásával kapcsolatos műszaki tevékenységeket végzi;
- Közreműködő Felek: a Szolgáltatóval szerződéses kapcsolatban álló vagy jogszabályban meghatározott, a Szolgáltatások nyújtásában közreműködő felek;
- Előfizetők (Aláírók): a Szolgáltató által tárolt magánkulcsok távoli aktiválásával elektronikus aláírást létrehozó állampolgárok;
- Érintett Felek: a távoli aktiválással létrehozott elektronikus aláírásokat fogadó harmadik felek.

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

1.3.1 Hitelesítő szervezet

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

Jelen bizalmi szolgáltatási rend hatálya alatt Szolgáltató kizárólag az állampolgárok részére, a Digitális Állampolgárság Program keretében biztosít szolgáltatást.

Szerver oldali aláíró alkalmazás szolgáltató

A szerver oldali aláíró alkalmazás szolgáltató (SSASP) a Szolgáltató által megvalósított bizalmi szolgáltatások azon szolgáltatói komponense, mely a más szolgáltatás komponensek által generált magánkulcsok aktiválásával az Aláírók nevében történő elektronikus aláírások létrehozását végzi.

Szabályozási Csoport

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

Telefonos Ügyfélszolgálat

A Szolgáltató Telefonos Ügyfélszolgálatot (Kormányzati Ügyfélvonal - 1818) tart fenn, melynek révén heti hét napban, napi 24 órában biztosítja Aláírók számára a tanúsítvány telefonos visszavonásának kezelését, továbbá ellátja a Szolgáltatásokkal kapcsolatos ügyfélszolgálatot.

1.3.2 Közreműködő Felek

DÁP szolgáltató

A DÁP szolgáltató: olyan külső közreműködő fél, mely a Szolgáltató számára elvégzi a Delegált Autentikációt, vagyis az Aláírók felhasználóazonosítását, igazolja az Aláíró aláírási szándékát és az általa aláírni kívánt adatokat.

1.3.3 Előfizetők

A DÁP-TK szolgáltatás előfizetői Magyarország azon állampolgárai, akik a Szolgáltató által tárolt magánkulcsuk távoli aktiválásával a DÁP keretalkalmazás elektronikus aláírás funkcióját használni kívánják és ezt megelőzően a Szolgáltatótól a DÁP keretalkalmazáson keresztül a {D8} BR-DÁP-TAN szerinti tanúsítványt igényelnek a {D9} BSZ-DÁP-TAN-ban foglaltak szerint valamint az {D1} ÁSZF-DÁP elfogadásával Szolgáltatási Szerződést kötnek a Szolgáltatóval a DÁP-TAN és DÁP-TK szolgáltatások igénybevételére.

Az Aláíró felelősségét és kötelezettségeit a 9.6.3 fejezet írja le.

1.3.4 Érintett Felek

Érintett Fél: a tanúsítványon alapuló elektronikus aláírással ellátott elektronikus dokumentumot fogadó természetes vagy jogi személy, aki/amely az elektronikus aláírásra hagyatkozva jár el a dokumentum hitelességének ellenőrzésekor. Az Érintett Fél nem áll szerződéses viszonyban a Szolgáltatóval.

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

Az Érintett Felek felelősségét a 9.6.4 fejezet írja le.

1.3.5 Egyéb felek

1.3.5.1 Felügyeleti Szerv

A jogszabályokban megjelölt Felügyeleti Szerv biztosítja a bizalmi szolgáltatásokra vonatkozó jogszabályok felügyeletét, ellenőrzi a Szolgáltatások jogszabályi megfelelőségét, ellátja az ezzel kapcsolatos felügyeleti feladatokat. Többek között, figyelemmel kíséri az elektronikus aláírásokkal kapcsolatos technológiai és kriptográfiai algoritmusok fejlődését és határozatba foglalja Szolgáltató szolgáltatásainak nyújtása során használható biztonságos kriptográfiai algoritmusokat, és az azok meghatározott paraméterekkel történő alkalmazására vonatkozó követelményeket; határozatában elrendelheti Szolgáltató számára az aláírói tanúsítvány(ok) visszavonását.

1.3.5.2 Kiberbiztonsági Felügyelet

A Kiberbiztonsági törvényben megjelölt Szabályozott Tevékenységek Felügyeleti Hatósága biztosítja a Kiberbiztonsági Felügyeletet.

1.4 A szolgáltatás alkalmazhatósága

A 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 aláírásérték kiszámítására, majd ezen érték szabványos formátumú elektronikus aláírásba foglalására.

A Szolgáltatás PAdES formátumú, PAdES-B-LT szintű minősített elektronikus aláírások létrehozását támogatja.

1.4.1 Engedélyezett használat

A Szolgáltatás keretében tárolt 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.

1.4.2 Tiltott használat

Tilos a tárolt magánkulcsot felhasználni titkosítás visszafejtésére, azonosításra, más tanúsítványok aláírására vagy bármilyen bizalmi szolgáltatás nyújtásához.

A Digitális Állampolgárság Program keretében kiadott tanúsítványhoz kapcsolódó magánkulcsot Aláíró egyedül magánszemélyként használhatja fel; ezek használata bármilyen üzleti, munkahelyi vagy egyéb szakmai tevékenység céljából nem megengedett.

1.5 Szabályzat adminisztráció

1.5.1 Szabályzatot karbantartó szerv

A Szolgáltató szervezetén belül Szabályozási Csoportot működtet, amely többek között jelen bizalmi

szolgáltatási rend karbantartásáért is felelős.

1.5.2 Kapcsolat

Szolgáltató adatai:

NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.

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

1.5.3 A szolgáltatási rend alkalmasságának meghatározása

A Szolgáltatónak legalább évente egyszer meg kell vizsgálnia a bizalmi szolgáltatási rend, illetve a bizalmi szolgáltatási szabályzat tartalmi és formai megfelelőségét a vonatkozó jogszabályok, előírások és műszaki szabványok tekintetében, és ennek eredményeit változtatási igényként figyelembe kell vennie.

1.5.4 A szolgáltatási rend jóváhagyásának eljárása

A Szolgáltatónak rendelkeznie kell a szabályzatainak jóváhagyására és kiadására vonatkozó eljárásrenddel, melyet a szolgáltatási szabályzatában ismertetnie kell. Az eljárásrendben meg kell jelölni az eljárásért felelős személyt, valamint az egyéb fontos részleteket (pl. hatályba lépés napja).

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 bizalmi szolgáltatási rend szerint az Alany az Aláíró (állampolgár).

aláírásérték: Az Aláíró által a DÁP-HSM modulban tárolt magánkulcsának felhasználásával, távolról aktivált és végrehajtott Kriptográfiai Művelet eredménye, azaz az aláírandó dokumentum(ok) lenyomatának a magánkulccsal történő titkosításával előállított digitális jelsorozat.
Jelen dokumentum fogalomrendszerében az Aláírás Érték az elektronikus aláírásban elhelyezett aláírás értéket (`SignatureValue`) jelenti.

aláírás érvényesítési adat: olyan egyedi adat, amelyet az elektronikus aláírt dokumentumot megismerő személy (vagy eszköz) az elektronikus aláírás érvényesítésére használ.
Jellemzően kriptográfiai nyilvános kulcs, korábbi elnevezése: aláírás-ellenőrző adat.

aláírás létrehozásához használt adat: olyan egyedi adat, amelyet az aláíró elektronikus aláírás létrehozásához használ.
Jellemzően kriptográfiai magánkulcs (magánkulcs), korábbi elnevezése: aláírás-létrehozó adat.

aláíró: elektronikus aláírást létrehozó természetes személy.
Jelen bizalmi szolgáltatási rend szerint az Aláíró az állampolgár.

bizalmi felügyelet: lásd „felügyeleti szerv”.

bizalmi lista: a tagállam által összeállított, fenntartott és közzétett elektronikus lista, amelyben kötelezően szerepelnek a tagállam felelőssége alá tartozó minősített bizalmi szolgáltatókra (opcionálisan a nem minősített bizalmi szolgáltatók is) valamint az e szolgáltatók által nyújtott bizalmi szolgáltatásokra vonatkozó információk.
A Bizalmi Lista automatizált feldolgozásra alkalmas, hitelességét elektronikus aláírás vagy elektronikus bélyegző biztosítja.

bizalmi szolgáltatás: rendszerint díjazás ellenében nyújtott, az alábbiakból álló szolgáltatások:
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 rend szerinti bizalmi szolgáltatás a c) és az f) pont alatti szolgáltatások, azzal, hogy a Szolgáltató jelen BR-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 bizonyos mértékig tűz, víz és egyéb katasztrófaeseményektől, egyéb erőszakos behatásoktól.

DÁP-HSM: a Szolgáltatásban működtetett SCDev, melyet az Aláírók távoli elektronikus aláírás létrehozó eszközként, távolról használnak az Aláírás Érték kiszámítására irányuló Kriptográfiai Művelet elvégzésére.

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

DÁP szolgáltató (eID szolgáltató): olyan külső közreműködő fél, mely a Szolgáltató számára elvégzi a Delegált Autentikációt, vagyis az Aláírók azonosítását és hitelesítését.

delegált autentikáció: az {Sz5} EN 419 241-1 szabvány lehetővé teszi, hogy az felhasználóazonosítás külső fél végezze és meghatározza az erre vonatkozó műszaki és biztonsági követelményeket. A delegált autentikáció folyamatábráját az {Sz3} TS 119 431-1 szabvány 4.4 fejezete tartalmazza. Szolgáltató a Szolgáltatás biztosítása előtt ellenőrizte, hogy a külső fél maradéktalanul teljesíti a számára meghatározott követelményrendszerben szereplő, a delegált autentikációra vonatkozó valamennyi műszaki és biztonsági követelményt.

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.

digitális állampolgárság nyilvántartás: a {J2} DÁP tv. által létrehozott 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 érvényesítése: az elektronikusan aláírt elektronikus dokumentum aláíráskori, illetve ellenőrzéskori tartalmának összevetése, továbbá az aláíró személyének azonosítása a dokumentumon szereplő, illetve a bizalmi szolgáltató által közzétett elektronikus aláírás érvényesítési adat, tanúsítvány visszavonási információk, valamint a tanúsítvány felhasználásával.

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 azonosítási rendszer: elektronikus azonosításra alkalmas rendszer, amelynek keretében természetes vagy jogi személy, illetve egy jogi személyt képviselő természetes személy számára elektronikus azonosító eszközöket bocsátanak ki.

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

előfizető: a természetes személy, aki a Szolgáltatóval érvényes Szolgáltatási Szerződéssel rendelkezik a Szolgáltatások igénybe vételére.
Jelen bizalmi szolgáltatási rend szerint az Előfizető az Aláíró állampolgár.

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.

felhasználó:
(DÁP tv): a digitális szolgáltatást biztosító szervezet feladat- és hatáskörébe tartozó ügyben ügyfélként, félként vagy azeljárás alanyaként, az eljárás egyéb résztvevőjeként, a szolgáltatás igénybe vevőjeként vagy ezek képviselőjeként részt vevő olyan természetes személy vagy egyéb jogalany, ide nem értve a digitális szolgáltatást biztosító szervezetet és az ügyben eljáró digitális szolgáltatást biztosító szervezet tagját vagy alkalmazottját.

(eIDAS): az e rendelettel összhangban nyújtott bizalmi szolgáltatásokat vagy elektronikus azonosító eszközöket igénybe vevő természetes vagy jogi személy, vagy egy másik természetes személyt vagy egy jogi személyt képviselő természetes személy.

Jelen szolgáltatási rendben: olyan entitás, aki/amely a Szolgáltatások keretében előállított kulcsokat és tanúsítványokat és/vagy időbélyegeket rendeltetésüknek megfelelően használja.

felhasználóazonosítás: az Aláírók azonosítását elvégző folyamat, amely meg kell feleljen az ezen dokumentumban szereplő biztonsági és műszaki követelményeknek. A felhasználóazonosítás sikeressége előfeltétele az Aláíró DÁP-HSM modulban tárolt magánkulcsa távolról történő aktiválásának, és így az elektronikus aláírás Aláíró által távolról történő létrehozásának.

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.

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.

Kriptográfiai Művelet: az elektronikus aláírás létrehozásához szükséges, az {Sz10} RFC 6979 szabvány által meghatározott kriptográfiai műveletek összessége, amely kiszámítja az Aláírás Értéket (a hitelesítendő dokumentum(ok) lenyomatának az Aláíró DÁP-HSM-ben tárolt magánkulcsával történő titkosításával előállított digitális jelsorozatot). A Kriptográfiai Műveletet a Felhasználó távolról hajtja végre, azt követően, hogy a Szolgáltatásban tárolt magánkulcsát aktiválta.

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.

magánkulcs aktiválása: az a folyamat, melynek során a jogosult - különféle azonosító elemek (pl. jelszó, PIN kód megadásával - engedélyezi, hogy az elektronikus aláírás létrehozó eszközön tárolt magánkulcs megkezdje üzemszerű működését. Az aktiválás általában a tanúsítványt igénylő környezetben (dokumentum kezelő, levelező rendszer) történik, és érvényes lehet a visszavonásig (deaktiválásig), illetve egyszeri használatra.

magánkulcs deaktiválása: az a folyamat, melynek során az elektronikus aláírás létrehozó eszközön tárolt magánkulcs üzemszerű működésre megszüntetésre kerül.

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

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).

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

minősített elektronikus bélyegzőt létrehozó eszköz: olyan elektronikus bélyegzőt létrehozó eszköz, amely értelemszerűen megfelel a {J1} eIDAS II. mellékletben megállapított követelményeknek.

PADES-B-B szint: Alap szintű aláírás. Addig érvényes, amíg az aláíráshoz használ tanúsítvány érvényes. Csak a legalapvetőbb elemeket tartalmazza, amelyeket egy elektronikus aláírásnak tartalmaznia kell (a használt algoritmusok azonosítója, az aláíró tanúsítványa).

PAdES-B-T szint: A PADES-B-B aláírás kiterjesztése. Az aláíráson elhelyezésre kerül egy időbélyeg is, amely bizonyítja, hogy az adott állomány az adott időpontban, vagyis az időbélyegzés pillanatában már létezett.

PAdES-B-LT szint: A PADES-B-T aláírás kiterjesztése. Az aláíráson az aláírás érvényesítéséhez szükséges adatok is elhelyezésre kerülnek, így tipikusan az aláíró tanúsítványa, az időbélyeg tanúsítványa, CRL és/vagy OCSP visszavonási adatok. Lehetővé teszi az aláírt dokumentum érvényesség ellenőrzését, kizárólag a tárolt aláírt adat alapján.

privilegizált felhasználó: a Szolgáltató informatikai rendszeriben olyan, a hivatkozott szabványok szerinti megbízható felhasználó, aki jogosult biztonsági funkciók beállítására vagy módosítására.

rendkívüli üzemeltetési helyzet: a Szolgáltató üzemmenetében zavart okozó olyan rendkívüli helyzet, amikor a Szolgáltató rendes üzemmenetének folytatására ideiglenesen vagy véglegesen nincs lehetőség, beleértve a szolgáltatói magánkulcsok kompromittálódását is, vagy annak közvetlen veszélyét.

rendszeradminisztrátor: az informatikai rendszer telepítését, konfigurálását, karbantartását végző személy.

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

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.

SCDev: az {Sz3} TS 119 431-1 szabvány 3.1 fejezetében definiált fogalom, azaz olyan konfigurált szoftver és hardver elemek összessége, melynek működési célja a tárolt magánkulcs felhasználásával az Aláírás Érték kiszámítása (a Kriptográfiai Művelet végrehajtásával)

személyazonosító adatok: egy természetes vagy jogi személy, vagy egy másik természetes személyt vagy egy jogi személyt képviselő természetes személy személyazonosságának megállapítását lehetővé tevő, az uniós vagy a nemzeti joggal összhangban kibocsátott adatok.

szolgáltatási szabályzat (Certificate Practice Statement - CPS): a bizalmi szolgáltató nyilatkozata

az egyes bizalmi szolgáltatások nyújtásával kapcsolatosan alkalmazott részletes eljárási vagy más működési követelményekről.

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 keretalkalmazás által generált hitelesítő kulcspár, melynek magánkulcsa az alkalmazás által generált és a Szolgáltató informatikai rendszere felé küldött adatok („üzenetek”) hitelességét hivatott biztosítani, oly’ módon, hogy ezen üzeneteket műszaki értelemben (és nem jogi értelemben) digitálisan aláírja.

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
CA	Certification Authority	hitelesítő szervezet
CP	Certificate Policy	hitelesítési rend
CPS	Certificate Practice Statement	hitelesítési szolgáltatási szabályzat
CRL	Certification Revocation List	tanúsítvány visszavonási lista
DÁP		Digitális Állampolgárság Program
DÁP-TAN		Szolgáltató BR-DÁP-TAN szerinti szolgáltatása
eID	electronic Identification	elektronikus azonosítás
HSM	Hardware Security Module	hardver kriptográfiai eszköz
NTP	Network Time Protocol	időforrás protokoll
OCSP	Online Certificate Status Protocol	valós idejű tanúsítvány-állapot protokoll
PADES	PDF Advanced Electronic Signatures	

PADES-B-B	PADES-basic	
PADES-B-T	PADES-basic + Timestamp token	
PADES-B-LT	PADES-basic + Long term	
PKI	Public Key Infrastructure	nyilvános kulcsú infrastruktúra
QSCD	Qualified Signature Creation Device	minősített elektronikus aláírást létrehozó eszköz
SCAL	Sole Control Assurance Level	
SCDev	Signature Creation Device	aláírás létrehozó eszköz
SSASP	Server Signing Application Service Provider	szerver oldali aláíró alkalmazás szolgáltató
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} 765/2008/EU Európai Parlament és Tanács rendelete a termékek forgalmazása tekintetében az akkreditálás és piacfelügyelet előírásainak megállapításáról és a 339/93/EGK rendelet hatályon kívül helyezéséről

{J4} 24/2016. (VI.30.) BM rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről

{J5} 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} 2024. évi LXIX. törvény Magyarország kiberbiztonságáról (Kiberbiztonsági tv.)

{J8} 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetébenalkalmazandó konkrét védelmi intézkedésekről

{J9} Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS2 irányelv)

{J10} A Bizottság (EU) 2024/2690 végrehajtási rendelete a 2022/2555 irányelvnek (NIS2 irányelv) a kiberbiztonsági kockázatkezelési intézkedések technikai és módszertani követelményei, valamint a DNS-szolgáltatók, a legfelső szintű doménnév-nyilvántartók, a felhőszolgáltatók, az adatközpont-szolgáltatók, a tartalomszolgáltató hálózati szolgáltatók, az irányított szolgáltatók, az irányított biztonsági szolgáltatók, az online piacterek, online keresőprogramok vagy közösségimédia-szolgáltatási platformok szolgáltatói és a bizalmi szolgáltatók tekintetében jelentősnek minősülő biztonsági események eseteinek további pontosítása tekintetében történő alkalmazására vonatkozó szabályok megállapításáról

1.6.3.2 Szabványok és műszaki-technikai hivatkozások

{Sz1}	EN 319 401 V3.1.1 (2024-06)	General policy requirements for Trust Service Providers
{Sz2}	ETSI TS 119 312 V1.4.3 (2023-08)	Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
{Sz3}	ETSI TS 119 431-1 V1.2.1 (2021-05)	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev
{Sz4}	ETSI TS 119 461 V1.1.1 (2021-07)	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects
{Sz5}	EN 419 241-1:2018	Trustworthy Systems Supporting Server Signing; Part 1: General System Security Requirements
{Sz6}	ISO/IEC 15408-1-5:2022	ISO/IEC 15408 (parts 1 to 5): Information Information security, cybersecurity and privacy protection – Evaluation criteria for IT security
{Sz7}	ISO/IEC 19790:2012	ISO/IEC 19790: Information technology – Security techniques – Security requirements for cryptographic modules
{Sz9}	RFC 3647 (November 2003)	Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework
{Sz10}	RFC 6979 (August 2013)	Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA)

1.6.3.3 Hivatkozott dokumentumok

{D1}	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 eAláírás szolgáltatáshoz
{D5}		NISZ Zrt. PKI szolgáltatások informatikai biztonságpolitikája
{D6}		NISZ Zrt. PKI szolgáltatások biztonsági szabályzata
{D7}		NISZ Zrt. PKI szolgáltatások üzletmenet-folytonossági terve
{D8}	BR-DÁP-TAN	Bizalmi Szolgáltatási Rend a Digitális Állampolgárság Program keretében kibocsátott minősített tanúsítványokhoz
{D9}	BSZ-DÁP-TAN	Bizalmi Szolgáltatási Szabályzat a Digitális Állampolgárság Program keretében nyújtott minősített tanúsítvány szolgáltatásokhoz
{D10}	BR-DÁP-TK	Jelen bizalmi szolgáltatási rend
{D11}	BSZ-DÁP-TK	Bizalmi Szolgáltatási Szabályzat a Digitális Állampolgárság Program keretében nyújtott elektronikus aláírások létrehozása és távoli elektronikus aláírás létrehozó eszközök kezelése minősített bizalmi szolgáltatáshoz

2 KÖZZÉTÉTEL ÉS ADATTÁRAK

2.1 Adattárak

Szolgáltató a DÁP-TK szolgáltatás keretében nem tart fenn adattárakat.

2.2 Szolgáltatói információ közzététele

A Szolgáltatónak gondoskodnia kell arról, hogy a Szolgáltatással kapcsolatos szabályzatok, valamint az egyéb közérdekű szolgáltatói információk az Aláírók és az Érintett Felek részére folyamatosan rendelkezésre álljanak. A Szolgáltatónak mindent meg kell tennie annak érdekében, hogy az információk elérhetetlensége ne haladhassa meg a szolgáltatási szabályzatban meghatározott időtartamot.

A Szolgáltatónak a Szolgáltatással kapcsolatos szabályzatokat és az egyéb közérdekű szolgáltatói információkat a Szolgáltatás internetes honlapján közzé kell tennie.

2.3 A közzététel gyakorisága

A Szolgáltatónak a Szolgáltatással kapcsolatos szabályzatokat azok változása esetén legalább 30 nappal a változás hatályba lépését megelőzően közzé kell tennie.

2.4 Hozzáférés-ellenőrzések

A Szolgáltatónak olvasás céljára korlátozás nélküli hozzáférést kell biztosítania a Szolgáltatással kapcsolatos nyilvános szabályzatokhoz.

A Szolgáltatónak biztonsági intézkedésekkel és eljárási szabályokkal gondoskodnia kell az információk jogosulatlan megváltoztatása, törlése, sérülése és megsemmisülése elleni védelemről.

3 AZONOSÍTÁS ÉS HITELESÍTÉS

A Szolgáltató a DÁP-TK szolgáltatást a DÁP-TAN-hoz kapcsolódó, minősített bizalmi szolgáltatásként nyújtja.

A kriptográfiai műveletek aktiválásához szükséges felhasználóazonosítás az alábbiak szerint történik.

3.1 Az azonosítás és hitelesítés biztonsági szintje

A Szolgáltatónak biztosítania kell, hogy a DÁP-TK szolgáltatás nyújtása során teljesüljön az {Sz5} EN 419 241-1 szabvány 5.4 fejezete szerinti – a minősített elektronikus aláírásra vonatkozó – SCAL2 (Sole Control Assurance Level 2) biztonsági szinthez előírt valamennyi követelmény az Aláírók azonosítása, jogosultságuk ellenőrzése, valamint a kriptográfiai műveletek aktiválása során.

3.2 Az Aláírók felhasználóazonosítása

Az Aláíró szempontjából a DÁP-TK szolgáltatás igénybe vételéhez szükséges felhasználóazonosítás az alábbi lépésekből áll:

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

A Szolgáltató szempontjából az Aláíró felhasználóazonosítását a DÁP szolgáltató, mint delegált autentikációt végző külső félnek kell végeznie, a {D9} BSZ-DÁP-TAN 3.2 fejezete szerinti személyazonosításra építve.

4 A SZOLGÁLTATÁS ÉLETCIKLUSA

4.1 A Szolgáltatás igénylése

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

A Szolgáltatónak a Szolgáltatás teljes életciklusában biztosítania kell a tárolt kulcs és az ahhoz tartozó minősített tanúsítvány közötti összerendelés sértetlenségét.

4.2 A Szolgáltatás használatba vétele

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

A Szolgáltatónak a Szolgáltatás teljes életciklusában biztosítania kell a tárolt kulcs és az ahhoz tartozó minősített tanúsítvány közötti összerendelés sértetlenségét.

4.3 A Szolgáltatás elérhetősége és rendelkezésre állása

A Szolgáltatás a DÁP keretalkalmazáson keresztül érhető el.

A Szolgáltatónak a Szolgáltatás elérhetőségét az év minden napján, napi 24 órában, éves szinten 97 %-os rendelkezésre állással kell biztosítania úgy, hogy a kiesés nem lépheti túl esetenként a 24 órás időtartamot.

4.4 A Szolgáltatás használata

A Szolgáltatás használatának előfeltétele az Aláíró sikeres felhasználóazonosítása, a 3.2 fejezetben leírt módon.

Az Aláírók a Szolgáltatást a DÁP szolgáltató közvetítésével használhatják a {D11} BSZ-DÁP-TK-ban foglaltak szerint.

A Szolgáltatónak ellenőriznie kell a DÁP szolgáltatótól kapott kérés formai és tartalmi megfelelőségét a {D11} BSZ-DÁP-TK-ban foglaltak szerint.

A Szolgáltatónak vissza kell utasítania 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 Szolgáltatónak fogadnia kell a kérést, és ha a fenti ellenőrzések mindegyike sikeresen megtörtént, ki kell szolgálnia a kérésben foglaltakat.

A Szolgáltatónak, elfogadott aláírási kérés esetén, a {D11} BSZ-DÁP-TK-ban foglaltak szerint elő kell állítania az aláírás értéket, majd a DÁP szolgáltató közvetítésével kell azt visszaadnia az Aláírónak.

4.5 Előfizetés vége

Az előfizetés a {D1} Általános Szerződési Feltételek által meghatározott esetekben és módon szűnik meg.

5 FIZIKAI, ELJÁRÁSBELI ÉS SZEMÉLYZETI BIZTONSÁGI ÓVINTÉZKEDÉSEK

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

5.1 Fizikai óvintézkedések

5.1.1 Telephely elhelyezése és szerkezeti felépítése

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

5.1.2 Fizikai hozzáférés

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

Ehhez biztosítania kell, az alábbiakat:

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

5.1.3 Áramellátás és légkondicionálás

A Szolgáltatónak a gépteremben olyan szünetmentes áramellátó rendszert kell biztosítania, amely:

- megfelelő teljesítménnyel rendelkezik a gépterem informatikai és kisegítő létesítményi berendezései áramellátásának biztosítására;
- megvédi az informatikai berendezéseket a külső hálózat feszültség ingadozásai, feszültség

kimaradásai és egyéb zavarok ellen;
- tartós áramszünet esetére saját áramellátó berendezés biztosítja - üzemanyag utántöltéssel - tetszőlegesen hosszú időtartamig az áramellátást.

A Szolgáltatónak a gépteremben olyan légkondicionáló berendezést kell alkalmaznia, mely biztosítja az alábbiakat:
- az operátorok biztonságos munkavégzéséhez szükséges mennyiségű oxigén biztosított;
- a levegő nedvességtartalma nem haladja meg az informatikai rendszerek által megkívánt szintet;
- hűtés történik a szükséges üzemeltetési hőmérséklet biztosítására, az eszközök és berendezések túlhevülésének megakadályozására.

5.1.4 Beázás és elárasztás veszélyeztetettség

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

5.1.5 Tűzmegelőzés és tűzvédelem

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

5.1.6 Adathordozók tárolása

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

5.1.7 Selejt kezelése és megsemmisítése

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

5.1.8 Fizikailag elkülönítetten őrzött mentési példányok

A Szolgáltatónak azt az adatmentést, amiből meghibásodás esetén a teljes szolgáltatás helyreállítható, olyan külső helyszínen kell tárolnia, mely megfelelő fizikai és működési védelemmel rendelkezik. Biztosítani kell a helyszínek között a mentett adatok biztonságos továbbítását.

A Szolgáltatónak biztosítania kell, hogy az adatmentést vagy abból a helyreállítást csak rendszerüzemeltető bizalmi munkakört betöltő személy végezze el.

5.2 Eljárásbeli előírások

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

5.2.1 Bizalmi munkakörök

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

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

5.2.2 Az egyes feladatokhoz szükséges személyzeti létszámok

Nincs kikötés.

5.2.3 Az egyes szerepkörökben elvárt azonosítás és hitelesítés

A Szolgáltatónak a „legkisebb jogosultságok” elvét alkalmazva kell adminisztrálnia a bizalmi munkaköröket betöltő személyek felhasználói hozzáférési képességeit. Különösen a {D11} BSZ-DÁP-TK-ban meghatározottak szerint.

5.2.4 Egymást kizáró munkakörök

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

A Szolgáltatónak biztosítania kell, hogy a bizalmi munkakörök vonatkozásában:

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

5.3 Személyzetre vonatkozó előírások

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

5.3.1 Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

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

5.3.2 Biztonsági háttér ellenőrzés eljárásai

A Szolgáltató vezetői munkakörben, illetve bizalmi munkakörben csak olyan alkalmazottakat foglalkoztathat, akik:

- büntetlen előélettel rendelkeznek és nincs ellenük folyamatban olyan eljárás, ami a

büntetlenséget befolyásolhatja (a büntetlen előéletet három hónapnál nem régebbi erkölcsi bizonyítvánnyal kell igazolni);
- nem állnak a bizalmi szolgáltatási tevékenység gyakorlását kizáró foglalkoztatástól eltiltás hatálya alatt.

5.3.3 Képzési követelmények

A bizalmi munkakörökben Szolgáltató olyan személyeket foglalkoztathat, akik az adott munkakör vagy szerepkör ellátásához szükséges mértékben elsajátították:
- a PKI elméletet;
- a Szolgáltató informatikai rendszerének sajátosságait és kezelésének módját;
- a szerepkör ellátáshoz szükséges speciális ismereteket;
- a Szolgáltató nyilvános és belső szabályzataiban meghatározott folyamatokat és eljárásokat;
- az egyes tevékenységek jogi következményeit;
- az alkalmazandó biztonsági szabályokat.

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

5.3.4 Továbbképzési gyakoriságok és követelmények

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

Legalább évente egyszer továbbképzést kell biztosítani az újonnan ismertté vált sebezhetőségekről, az IT biztonság aktuális gyakorlatáról.

5.3.5 Munkabeosztás körforgásának gyakorisága és sorrendje

Nincs kikötés.

5.3.6 Felhatalmazás nélküli tevékenységek büntető következményei

A Szolgáltatónak szerződésben szabályoznia kell a munkatársak felelősségre vonásának lehetőségét az elkövetett mulasztások, vétlen vagy szándékos károkozás esetére.

5.3.7 Szerződéses munkavállalókra vonatkozó követelmények

A Szolgáltató bizalmi munkakörben csak munkaviszonyban álló személyt foglalkoztathat.

Az egyéb feladatok ellátására, vállalkozási vagy megbízási szerződés keretében a beszállítóval vagy közreműködő féllel Szolgáltató írásos megállapodást köt.

5.3.8 A személyzet számára biztosított dokumentációk

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

5.4 A biztonsági naplózás folyamatai

5.4.1 Naplózott esemény típusok

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

5.4.2 Naplóállomány feldolgozásának gyakorisága

A Szolgáltatónak biztosítania kell a naplóállományok rendszeres ellenőrzését és kiértékelését.

5.4.3 Naplóállomány megőrzési időtartama

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

5.4.4 Naplóállomány védelme

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

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

5.4.5 Naplóállomány mentési folyamatai

A naplóállományokról rendszeres mentést kell készíteni.

5.4.6 Naplózás gyűjtési rendszere

A naplóbejegyzések gyűjtését belső komponenssel kell megoldani. A naplóbejegyzések gyűjtésének meg kell kezdődnie rendszer indításkor és rendszer leállításig folyamatosan működnie kell, és közben biztosítania kell a gyűjtött bejegyzések integritását és rendelkezésre állását, szükség esetén a bizalmasságát is.

A naplóbejegyzések gyűjtési rendszerének működési rendellenessége esetén a Szolgáltatónak fel kell függesztenie az érintett területek működését az üzemzavar elhárításáig.

5.4.7 Rendellenes eseményeket kiváltó alanyok értesítése

Nincs kikötés.

5.4.8 Sebezhetőség értékelések

A Szolgáltatónak rendszeres időközönként, a naplóállományok és egyéb információk kiértékelésén alapuló sebezhetőség vizsgálatot és behatolás tesztet kell végeznie, mely segítségével feltérképezi a potenciális belső és külső fenyegetéseket, melyek a Szolgáltató által tárolt végfelhasználói magánkulcsok módosítását, sérülését, megsemmisülését vagy jogosulatlan aktiválását eredményezhetik.

A Szolgáltatónak folyamatosan figyelemmel kell kísérnie az újonnan ismertté vált, kritikus sebezhetőségeket, és a szükséges ellenintézkedéseket lehetőség szerint 48 órán belül meg kell tennie, illetve – ha az ellenintézkedés költsége nem áll arányban a sebezhetőség lehetséges kihatásaival – cselekvési tervet kell készítenie és végrehajtania annak érdekében, hogy a sebezhetőség ne legyen kihasználható vagy annak hatása elhanyagolható legyen.

5.5 Adatok archiválása

5.5.1 A tárolt adatok típusai

A Szolgáltatónak gondoskodnia kell arról, hogy megőrzésre kerüljön minden olyan információ, amely szükséges ahhoz, hogy egy elektronikus aláírás érvényessége bizonyítható legyen, továbbá amely a Szolgáltató és a rendszereinek megfelelő működését alátámasztja.

Ehhez legalább az alábbi információkat tárolja papír alapon vagy elektronikusan:

- tanúsítványok igénylésével, regisztrációval kapcsolatos minden adat vagy irat, különösen az Aláíró által aláírt nyilatkozatok és átvételi elismervények;
- tanúsítványokkal kapcsolatos valamennyi információ a teljes életciklusra vonatkozóan;
- a bizalmi szolgáltatási rend és szolgáltatási szabályzat valamennyi kibocsátott verziója;
- az Általános Szerződési Feltételek valamennyi kibocsátott verziója;
- a Szolgáltató működésével kapcsolatos szerződések, különösen a Közreműködő Felekkel kötött megállapodások;
- valamennyi naplóállomány.

5.5.2 Archívum megőrzési időtartama

A Szolgáltató az 5.5.1 fejezetben meghatározott archivált adatokat köteles megőrizni, a tanúsítványokkal kapcsolatos adatok esetében a tanúsítvány érvényességnek lejáratáról számított 10 évig, illetve a tanúsítvánnyal előállított elektronikus aláírással kapcsolatos jogvita jogerős lezárásáig, szabályzatok, szerződések esetében a hatályon kívül helyezés vagy megszűnés utáni 10 évig.

5.5.3 Archívum védelme

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

5.5.4 Archívum mentési eljárásai

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

5.5.5 Az adatok időbélyegzésére vonatkozó követelmények

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

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

Az archivált adatok megőrzése során szükség esetén (pl. algoritmus váltás) gondoskodni kell az

elektronikus aláírások, bélyegzők és időbélyegzők hitelességének fenntartásáról.

5.5.6 Archívum gyűjtési rendszere

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

5.5.7 Archívum hozzáférés és ellenőrzés eljárásai

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

5.6 Kulcs átállás

A Szolgáltatónak biztosítania kell, hogy a hitelesítőközpontok folyamatosan rendelkezzenek a működésükhöz szükséges érvényes kulccsal és tanúsítvánnyal.

5.7 Helyreállítás rendkívüli üzemeltetési helyzetek esetén

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

Egyéb incidens esetén - amennyiben az jelentős hatást gyakorol a szolgáltatásra vagy az annak keretében tárolt személyes adatokra -, az esetről való értesüléstől számított 24 órán belül értesíteni kell az Érintett Feleket, valamint jelenteni kell az incidenst a Felügyeleti Szervnek, valamint személyes adatok érintettsége esetén a {J5} GDPR 51. cikke szerinti illetékes hatóságnak.

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

5.7.1 Rendkívüli események és kompromittálódás kezelésének eljárásai

A Szolgáltatónak rendelkeznie kell üzletmenet-folytonossági tervvel.

Rendkívüli üzemeltetési helyzetben a Szolgáltatónak dokumentálnia kell az eseményeket, azok körülményeit, az elhárításukra megtett intézkedéseket.

A Szolgáltatónak ki kell alakítani és fenn kell tartania egy tartalék CA rendszert, mely a rendkívüli üzemeltetési helyzetben képes a nyilvános szabályzatok elérhetőségét, a visszavonás kezelési szolgáltatások teljes értékű működését, a CRL-ek közzétételét biztosítani.

A rendkívüli üzemeltetési helyzetben – amennyiben annak hátrányos kihatása van a Szolgáltatást igénybe vevő Előfizetőkre vagy az Érintett felekre – a Szolgáltatónak a lehető legrövidebb időn belül tájékoztatást kell közzé tennie internetes honlapján, valamint - lehetőség szerint - a DÁP szolgáltatón keresztül kell értesítenie azokat a személyeket, akiket az esemény érint.

5.7.2 Sérült számítási erőforrások, szoftverek és/vagy adatok

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

5.7.3 Magánkulcsának kompromittálódása esetén követendő eljárás

A Szolgáltatónak a Szolgáltatás működéséhez szükséges magánkulcsának kompromittálódása esetén haladéktalanul meg kell tennie az alábbi lépéseket:

- megszünteti az érintett magánkulcs használatát;
- új szolgáltatói kulcspárt és tanúsítványt hoz létre;
- értesíti a Felügyeleti Szervet;
- értesíti a DÁP szolgáltatót.

A Szolgáltatónak az általa tárolt végfelhasználói (aláírói) magánkulcsok kompromittálódása esetén haladéktalanul meg kell tennie az alábbi lépéseket:

- megszünteti az érintett magánkulcsok használatát;
- értesíti az Aláírót és kezdeményezi az érintett tanúsítványok visszavonatását;
- intézkedik valamennyi érintett fél értesítéséről;
- értesíti a DÁP szolgáltatót.

5.7.4 Üzletmenet folytonosság helyreállás katasztrófát követően

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

5.8 A szolgáltatási tevékenység megszüntetése

A Szolgáltatónak rendelkeznie kell a szolgáltatási tevékenység megszüntetésére vonatkozó, aktualizált tervvel.

A Szolgáltatónak rendelkeznie kell olyan bankgaranciával, mely fedezi a szolgáltatási tevékenység megszüntetésének költségeit abban az esetben, ha a Szolgáltató csődeljárás alá kerül vagy más okból kifolyólag nem képes önmaga fedezni a költségeket.

A szolgáltatási tevékenység megszüntetésére vonatkozó tervnek tartalmaznia kell legalább az alábbiakat:

- az Aláírók és az Érintett Felek értesítésének módja;
- a Szolgáltatásokban Közreműködő Felek jogosultságainak megvonása;
- a Szolgáltatásokkal kapcsolatos azon kötelezettségeknek átadása egy másik minősített bizalmi szolgáltatónak, melyek arra vonatkoznak, hogy bizonyítékot szolgáltassanak a Szolgáltató működésével kapcsolatban - különösen az 5.5.1 fejezetben meghatározott adatoknak a megőrzése az 5.5.2 fejezetben megjelölt időtartamig;
- a szolgáltatói magánkulcsok és azok mentései megsemmisítésének módja;
- a Szolgáltató informatikai rendszerében foglalt adatokról teljes körű mentés készítése.

6 MŰSZAKI BIZTONSÁGI ÓVINTÉZKEDÉSEK

6.1 Kulcspár előállítás és telepítés

6.1.1 Kulcspár előállítás

Szolgáltatónak a {D11} BSZ-DÁP-TK-ban leírtak szerint kell előállítania a szolgáltatói és a végfelhasználói (aláírói) magánkulcsokat.

6.1.2 Magánkulcs eljuttatása a tulajdonoshoz

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

6.1.3 Nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz

Nincs kikötés.

6.1.4 A szolgáltatói nyilvános kulcs közzététele

Nincs kikötés.

6.1.5 Kulcs méretek

A Szolgáltatónak Szolgáltatásai nyújtása során az {Sz2} ETSI TS 119 312 szabvány mindenkor hatályos verziója szerint megbízható, szabványos algoritmusokat, paramétereket és kulcshosszakat kell használnia.

Szolgáltatónak a {D11} BSZ-DÁP-TK-ban közzé kell tennie a DÁP-TK szolgáltatás keretében alkalmazott, fentieknek megfelelő konkrét algoritmusokat, paramétereket és kulcshosszakat.

6.1.6 A nyilvános kulcs paraméterek előállítása és megfelelőségének ellenőrzése

A Szolgáltatás nyújtása során használt szolgáltatói kulcspárok előállítását a 6.1.1 fejezet szerint védett környezetben és tanúsított HSM modulban, legalább két bizalmi munkakört betöltő személy együttes részvételével, illetéktelen személy jelenlétét kizárva kell megvalósítani.

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

Nincs kikötés.

6.2 Magánkulcs védelme és kriptográfiai modul műszaki szabályozások

6.2.1 Kriptográfiai modul szabványok és szabályozások

A Szolgáltató a Szolgáltatás nyújtása során használt szolgáltatói magánkulcsok előállítására, tárolására és használatára csak olyan kriptográfiai modult alkalmazhat, amely olyan megbízható rendszer, amelynek értékelése az {Sz6} ISO/IEC 15408 szerint, illetve azzal egyenértékű biztonsági

kritériumok szerint 4-es vagy magasabb értékelési garancia szinten történt meg (EAL 4+).

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

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

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

Szolgáltatónak a {D11} BSZ-DÁP-TK-ban meg kell határoznia, hogy mely funkciók esetén alkalmaz több szereplős "n-ből m" ellenőrzést.

6.2.3 Magánkulcs letét

A Szolgáltató nem nyújt az Aláírók számára magánkulcs letét szolgáltatást.

6.2.4 Magánkulcs visszaállítása

Szolgáltatónak az Aláírók magánkulcsának titkosított mentésből történő visszaállítását a DÁP-HSM modul erre szolgáló, tanúsítással rendelkező biztonsági funkciójával kell végeznie a {D11} BSZ-DÁP-TK szerint.

6.2.5 Magánkulcs mentése

Szolgáltatónak az aláírói (végfelhasználói) magánkulcsokat biztonsági okokból mentenie kell. A mentést titkosított formában, speciális eszközök alkalmazásával kell megvalósítani, a {D11} BSZ-DÁP-TK szerint.

6.2.6 Magánkulcs bejuttatása a kriptográfiai modulba

A Szolgáltató az aláírói (végfelhasználói) magánkulcsokat a {D4} BR-DÁP-TAN 6.1.1 fejezetében leírtak szerint QSCD tanúsított kriptográfiai modulban (DÁP-HSM) kell előállítania, a {D11} BSZ-DÁP-TK szerint.

6.2.7 Magánkulcs kriptográfiai modulban történő tárolásának módja

Az Aláírói (végfelhasználói) magánkulcsokat teljes életciklusuk alatt a 6.2.1 fejezetben leírt QSCD tanúsított kriptográfiai modulban (DÁP-HSM) kell tárolni.

6.2.8 Magánkulcs aktiválásának módja

Szolgáltónak a DÁP-TK Szolgáltatás nyújtásához használt informatikai rendszer működtetéséhez szükséges infrastrukturális és vezérlő kulcsok aktiválását a HSM modul gyártói dokumentációjában előírtak szerint kell végeznie.

A Szolgálatónak biztosítania kell a HSM és DÁP-HSM kriptográfiai modulok jogosulatlan hozzáférés ellen védelmét.

Az Aláírónak a Szolgáltató által tárolt magánkulcsának távoli aktiválásához két faktoros azonosítást kell végeznie a {D11} BSZ-DÁP-TK-ban foglaltak szerint.

6.2.9 Magánkulcs aktív állapotának megszüntetési módja

Szolgáltatónak garantálnia kell, hogy minden sikeres elektronikus aláírás létrehozás művelet után a magánkulcs automatikusan inaktív állapotba kerüljön. Egy következő elektronikus aláírás létrehozás művelethez ismét el kell végezni a távoli aktiválást.

6.2.10 Magánkulcs megsemmisítésének módja

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

6.2.11 Kriptográfiai modul értékelése

Lásd a 6.2.1 fejezetben.

6.3 Kulcspár gondozás egyéb szempontjai

6.3.1 Nyilvános kulcs archiválása

Nincs kikötés.

6.3.2 Tanúsítvány érvényességi időszaka és kulcspár felhasználás időtartama

Nincs kikötés.

6.4 Aktivizáló adatok

6.4.1 Aktivizáló adatok előállítása

Az Aláíró magánkulcsának aktiválásához szükséges, a DÁP keretalkalmazás által generált üzenethitelesítő magánkulcs DÁP szolgáltató által továbbított nyilvános kulcs párját a Szolgáltatónak a megfelelő aláíróhoz rendelve rögzítenie kell a szolgáltatást megvalósító saját informatikai rendszerében.

6.4.2 Aktivizáló adatok védelme

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

Szolgáltatónak biztosítani kell, hogy az aktivizáló adatot ne lehessen a kulcsaktiválás során korlátozás nélkül helytelenül megadni.

6.4.3 Aktivizáló adatok egyéb szempontjai

Nincs kikötés.

6.5 Informatikai biztonsági óvintézkedések

6.5.1 Informatikai biztonsági műszaki követelmények meghatározása

Az informatikai biztonság műszaki követelményeit a Szolgáltató az {Sz1} EN 319 401, {Sz5} EN 419 241-1 és {Sz3} ETSI TS 119 431-1 szabványoknak a nyilvános kulcsú tanúsítványokat kibocsátó, minősített bizalmi szolgáltatás nyújtására vonatkozó, informatikai biztonsági műszaki követelményeiben határozza meg.

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

6.5.2 Informatikai biztonsági értékelés

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

A biztonsági osztályba sorolástól függő védelmi intézkedések teljesülésének biztonsági értékelését a {J7} Kiberbiztonsági tv. rendelkezései szerint el kell elvégezni.

A Szolgáltatónak a minősített bizalmi szolgáltatásához kialakított és üzemeltetett informatikai rendszerével kapcsolatban teljesítenie kell a {J9} NIS2 rendelet és a kapcsolódó {J10} 2024/2690 végrehajtási rendelet vonatkozó követelményeit.

6.6 Életciklusra vonatkozó műszaki óvintézkedések

6.6.1 Rendszerfejlesztési óvintézkedések

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

6.6.2 Biztonságkezelési óvintézkedések

A Szolgáltatónak olyan eszközöket és eljárásokat kell alkalmaznia, melyek garantálják a Szolgáltatásokat megvalósító, megbízható informatikai rendszereinek konfigurációs beállításai, az operációs rendszer beállítások, a hálózati konfigurációs beállítások, továbbá az alkalmazott biztonsági mechanizmusok sértetlenségének és helyes működésének ellenőrzését.

6.6.3 Életciklus biztonsági óvintézkedések

A Szolgáltatónak meghatározott rendszeres időközönként el kell végeznie a Szolgáltatásokat megvalósító, megbízható informatikai rendszereinek konfigurációs beállításai, az operációs

rendszer beállítások, a hálózati konfigurációs beállítások, továbbá az alkalmazott biztonsági mechanizmusok sértetlenségének és helyes működésének ellenőrzését.

6.7 Hálózatbiztonsági óvintézkedések

A hálózati védelmi intézkedéseket a Szolgáltató belső biztonsági szabályzatában meghatározott követelményeknek megfelelően kell megvalósítani.

6.8 Időforrások

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

7 TANÚSÍTVÁNY, CRL ÉS OCSP PROFILOK

7.1 Tanúsítvány profil

Az Aláíró kulcspárokhoz kibocsátott minősített tanúsítvány profiljának meg kell felelnie a {D9} BSZ-DÁP-TAN szolgáltatási szabályzat 7.1 fejezetében leírtaknak.

7.2 CRL profil

Az Aláíró kulcspárokhoz – összhangban a {D9} BSZ-DÁP-TAN szolgáltatási szabályzat 7.2 fejezetében leírtakkal – a Szolgáltató nem biztosít CRL-t.

7.3 OCSP profil

Az Aláíró kulcspárokhoz kibocsátott minősített tanúsítványok visszavonási állapotának ellenőrzéséhez használható OCSP válaszok profiljának meg kell felelnie a {D9} BSZ-DÁP-TAN szolgáltatási szabályzat 7.3 fejezetében leírtaknak.

8 MEGFELELŐSÉG VIZSGÁLAT ÉS EGYÉB ÉRTÉKELÉSEK

Jelen bizalmi szolgáltatási rend tartalmazza a DÁP TK bizalmi szolgáltatás nyújtása során teljesítendő valamennyi követelményt, melyeket különösen az alábbi szabványok határoznak meg:

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

8.1 Vizsgálatok gyakorisága és körülményei

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

A Szolgáltatónak legalább 24 havonta egyszer megfelelőségértékelést és 12 havonta egyszer felülvizsgálatot kell végeztetnie a {J1} eIDAS 3. cikk 18. bekezdésben meghatározott megfelelőségértékelő szervezettel, a {J1} eIDAS követelményeinek való megfelelés tárgykörben. A Szolgáltató köteles az elkészült megfelelőségértékelés jelentést annak kézhezvételétől számított három munkanapon belül benyújtani a Felügyeleti Szervnek.

A Szolgáltatónak a {J7} Kiberbiztonsági. törvény 16 §. 1. bekezdése alapján kétévente kiberbiztonsági auditot is kell végeztetnie, az SZTFH által nyilvántartott auditorok egyikével. Ezen felül a szolgáltatónak az illetékes kiberbiztonsági hatóság általi elrendelés esetén kiberbiztonsági auditot kell végeztetnie az SZTFH által nyilvántartott auditorok egyikével. Az audit eredményét az auditor az audit befejezését követően haladéktalanul megküldi a Szolgáltatónak és a kiberbiztonsági hatóságnak.

8.2 Auditor azonosítása és képesítése

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

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

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

A megfelelőségértékelési vizsgálatot a Szolgáltató olyan, a {J3} 765/2008/EU rendelet 2. cikkének 13. pontjában meghatározott megfelelőségértékelő szervezettel végezteti el, melyet az említett rendelettel összhangban illetékesnek ismernek el a minősített bizalmi szolgáltató és az általa nyújtott minősített bizalmi szolgáltatások megfelelőségének értékelésére.

A kiberbiztonsági auditot Szolgáltató olyan auditorral végezteti el, amely szerepel a kiberbiztonsági hatóság által nyilvántartott auditor listán, és amely jogosult a Szolgáltató elektronikus információs rendszerének biztonsági osztálya szerinti auditálásra.

8.3 Auditor függetlensége

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

8.4 Audit során vizsgált területek

A megfelelőségértékelés az alábbi területeket fedi le:

- szabályzatok és dokumentációk;
- irányítási és ellenőrzési követelmények;
- személyzeti biztonsági követelmények;
- a szolgáltatói kulcspár kezeléséhez kapcsolódó követelmények;
- üzemeltetési és hozzáférési biztonság;
- fizikai és környezeti biztonság;
- folyamatos szolgáltatás biztosítása;
- adatbiztonság és archiválás.

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

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

A kiberbiztonsági audit az alábbi – a megfelelőségértékeléssel jelentős átfedésben lévő - kiberbiztonsági követelménycsoportok teljesülését vizsgálja:

- adathordozók védelme;
- azonosítás és hitelesítés;
- biztonsági események kezelése;
- ellátási lánc kockázatkezelése;
- értékelés, engedélyezés és monitorozás;
- fizikai és környezeti védelem;
- hozzáférés-felügyelet;
- karbantartás;
- készenléti tervezés;
- kockázatkezelés;
- konfigurációkezelés;
- naplózás és elszámoltathatóság
- programmenedzsment;
- rendszer- és információ sértetlenség;
- rendszer- és kommunikáció védelem;
- rendszer- és szolgáltatásbeszerzés;
- személyi biztonság;
- tervezés;
- tudatosság és képzés.

8.5 Hiányosságok esetén végrehajtandó tevékenységek

Az üzemszerű ellenőrzések, belső és külső auditok, szakértői elemzések által feltárt hiányosságok, hibás gyakorlatok kezelésére a Szolgáltatónak intézkedési tervet kell készítenie. A hiányosságokat késlekedés nélkül orvosolnia, az intézkedéseket dokumentálni és ellenőriznie kell.

A Felügyeleti Szerv (hatóság) által végzett rendszeres helyszíni ellenőrzések során feltárt esetleges hiányosságokat a Szolgáltatónak a hatósággal megállapodott határidőn belül meg kell szüntetnie a

hatályos jogszabályok alapján és a hatóságtól kapott információk és ajánlások figyelembe vételével.

8.6 Eredmény kommunikációja

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

9 EGYÉB ÜZLETI ÉS JOGI KÉRDÉSEK

9.1 Díjak

A díjazással kapcsolatos információkat a {D11} BSZ-DÁP-TK szolgáltatási szabályzatban kell meghatározni.

9.2 Anyagi felelősség

A Szolgáltatónak az anyagi felelősség mértékéről, illetve annak korlátairól a {D11} BSZ-DÁP-TK szolgáltatási szabályzatban rendelkeznie kell.

9.2.1 Biztosítási fedezet

A Szolgáltatónak felelősségbiztosítással kell rendelkeznie, mely egyaránt kiterjed az elektronikus aláírással, illetve az ezzel ellátott elektronikus dokumentummal szerződésen kívül okozott károkra és szerződésszegéssel okozott károkra, valamint a Bizalmi Felügyeletnél felmerült jogszabály szerinti költségekre, és amely fedezetet biztosít az összes károsultnak okozott kárra, a {D11} BSZ-DÁP-TK-ban foglaltak szerint.

A felelősségbiztosítási szerződésnek meg kell felelnie a {J4} 24/2016 BM rendelet előírásainak is.

9.2.2 További követelmények

A Szolgáltatónak teljesítenie kell a {J4} 24/2016 BM rendelet 19. §-a szerinti pénzügyi követelményeket is.

9.2.3 Felelősségbiztosítás vagy garancia végfelhasználók számára

Nincs kikötés.

9.3 Üzleti információk bizalmassága

9.3.1 Bizalmasan kezelendő információk köre

A Szolgáltatónak a {D11} BSZ-DÁP-TK szolgáltatási szabályzatban meg kell adnia a bizalmasan kezelendő információk körét.

9.3.2 Bizalmasnak nem tekintett információk köre

Nincs kikötés.

9.3.3 Bizalmas információk védelmének felelőssége

A Szolgáltatónak meg kell védenie a bizalmas információkat.

A bizalmas információk védelmét a személyzet megfelelő képzésével, továbbá a munkavállalókkal, szerződéses partnerekkel megkötött szerződésekkel kell érvényre juttatni.

9.4 Személyes adatok védelme

9.4.1 Adatvédelem

A Szolgáltatónak rendelkeznie kell adatvédelmi szabályozással, valamint a Szolgáltatásokra vonatkozó adatvédelmi tájékoztatóval {D4}, melyeknek összhangban kell lenniük a nemzetközi és hazai vonatkozó jogszabályokkal.

Szolgáltatónak az adatvédelmi tájékoztatóját {D4} elérhetővé kell tennie internetes honlapján.

9.4.2 Bizalmasként kezelendő személyes adatok

A Szolgáltatónak a DÁP-TK szolgáltatás keretében tárolt magánkulcsokat, a magánkulcsok aktiválásához szükséges adatokat, valamint az aláírási kéréseket bizalmasan kell kezelnie.

9.4.3 Bizalmasként nem kezelendő személyes adatok

Nincs kikötés.

9.4.4 Személyes adatok védelmének felelőssége

A Szolgáltatónak gondoskodnia kell a személyes adatok védelméről, működésének és szabályzatainak meg kell felelniük a {J5} GDPR rendelkezéseinek.

9.4.5 Hozzájárulás a személyes adatok felhasználásához

Az Aláírónak az {D1} ÁSZF-DÁP elfogadásával létrejött Szolgáltatási Szerződés keretében tudomásul kell vennie a szolgáltatások igénybevételéhez szükséges adatok Szolgáltató által történő nyilvántartásba vételét, kezelését és tárolását.

9.4.6 Felfedés hatósági vagy polgári peres eljárás keretében

A Szolgáltatónak bűncselekmények felderítése vagy megelőzése céljából, illetve nemzetbiztonsági érdekből - az adatigénylésre meghatározott jogszabályi feltételek teljesülése esetén - a nyomozó hatóságnak és a nemzetbiztonsági szolgálatoknak haladéktalanul és egyéb feltételek nélkül fel kell tárnia a jogszabályban meghatározott bizalmas információkat. Ilyen esetben a Szolgáltató rögzíti az adatátadás tényét, de arról nem tájékoztathatja az érintett Aláírót.

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

9.4.7 Egyéb, felfedést eredményező körülmények

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

9.5 Szellemi tulajdonjogok

A Szolgáltató által az Aláíró részére kibocsátott tanúsítvány és az ahhoz tartozó kulcspár tulajdonosa

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

A szolgáltatói tanúsítványok a Szolgáltató tulajdonát képezik. A visszavonási információk a Szolgáltató tulajdonát képezik. A Szolgáltató szabályzatai, szerződéses feltételei a Szolgáltató tulajdonát képezik.

9.6 Tevékenységért viselt felelősség és helytállás

9.6.1 Szolgáltató felelőssége és helytállása

A Szolgáltató felel a jelen bizalmi szolgáltatási rendben és a {D11} BSZ-DÁP-TK szolgáltatási szabályzatban, valamint a {D1} ÁSZF-DÁP-ban megfogalmazott valamennyi kötelezettség maradéktalan betartásáért, még akkor is, ha a Szolgáltatások nyújtásához kapcsolódó egyes feladatokat a Közreműködő Felek vagy egyéb alvállalkozók végzik.

A Szolgáltató Telefonos Ügyfélszolgálata (Kormányzati Ügyfélvonal – 1818) felelős az alábbiakért:

- az Aláíró telefonos visszavonási igényének fogadása, majd ezt követően – ha az Aláíró sikeresen azonosította magát - a visszavonás kezdeményezése;
- a Szolgáltatásokkal kapcsolatos teljes körű és közérthető tájékoztatás.

9.6.2 A regisztrációs szervezet felelőssége

A jelen bizalmi szolgáltatási rend által tárgyalt Szolgáltatáshoz nem kapcsolódik regisztrációs szervezet.

9.6.3 Aláíró felelőssége és helytállása

Az Aláíró jogosult:

- a számára előállított kulcspárt az 1.4.1 fejezetben leírt célokra a jelen hitelesítési rendben leírt módon használni;
- a tárolt kulcshoz kapcsolódó egyéb szolgáltatásokat használni a jelen hitelesítési rendben leírt módon.

Az Aláíró felelős:

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

Az Aláíró köteles:

- a Szolgáltató által kért, a Szolgáltatás igénybe vételéhez szükséges adatokat hiánytalanul és a valóságnak megfelelően megadni;
- adat változás esetén haladéktalanul írásban értesíteni erről Szolgáltatót, és beszüntetni a kulcspár használatát;
- biztosítani, hogy a Szolgáltatás igénybe vételéhez szükséges adatokhoz és eszközökhöz illetéktelen személy ne férhessen hozzá;
- jogellenes használat gyanúja esetén a Szolgáltató megkereséseire a Szolgáltató által megadott időtartamon belül reagálni;

- haladéktalanul, írásban értesíteni Szolgáltatót, ha a Szolgáltatás felhasználásával létrehozott elektronikus aláírással kapcsolatban jogvita indul.

9.6.4 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 figyelembe vétele, amely a tanúsítványban vagy a szolgáltatási szabályzatban szerepel;
- a tőle elvárható magatartás tanúsítása a tanúsítvány ellenőrzésekor.

9.6.5 Egyéb felek felelőssége és helytállása

Nincs kikötés.

9.7 Helytállás érvénytelenségi köre

A helytállás érvénytelenségi körét a {D11} BSZ-DÁP-TK szolgáltatási szabályzatban meg kell határozni.

9.8 Felelősség korlátozása

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

9.9 Kártérítések

A kártérítésekről a {D11} BSZ-DÁP-TK szolgáltatási szabályzatban kell rendelkezni.

9.10 Hatályosság és megszűnés

9.10.1 Hatályosság

Időbeli hatály

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

Tárgyi hatály

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

Személyi hatály

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

9.10.2 Megszűnés

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

9.10.3 Megszűnés után is hatályban maradó rendelkezések

A megszűnés után is hatályban maradó rendelkezéseket a {D11} BSZ-DÁP-TK szolgáltatási szabályzatban meg kell határozni.

9.11 Egyéni hirdetmények és kommunikáció a részvevőkkel

A {D11} BSZ-DÁP-TK szolgáltatási szabályzatban rendelkezni kell a felek és részvevők között kommunikáció joghatást kiváltó módjairól.

9.12 Módosítások

9.12.1 Módosítás eljárása

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

9.12.2 Értesítés módszere és időtartama

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

9.12.3 OID megváltozását előidéző körülmények

A bizalmi szolgáltatási rend OID-ja nem változik.

9.13 Vitás kérdések rendezése

A {D11} BSZ-DÁP-TK szolgáltatási szabályzatban kell meghatározni.

9.14 Irányadó jog

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

9.15 Hatályos jognak megfelelés

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

9.16 Vegyes rendelkezések

9.16.1 Teljességi záradék

Nincs kikötés.

9.16.2 Átruházás

Nincs kikötés.

9.16.3 Részleges érvénytelenség

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

9.16.4 Igényérvényesítés

A {D11} BSZ-DÁP-TK szolgáltatási szabályzatban kell meghatározni.

9.16.5 Force Majeure (Vis maior)

A {D11} BSZ-DÁP-TK szolgáltatási szabályzatban kell meghatározni.

9.17 Egyéb rendelkezések

9.17.1 Hozzáférhetőség a fogyatékossággal élő személyek számára

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