NISZ

Nemzeti Infokommunikációs Szolgáltató Zrt.

Bizalmi Szolgáltatási Szabályzat a Digitális Állampolgárság Program keretében nyújtott elektronikus aláírások létrehozása és távoli elektronikus aláírás létrehozó eszköz kezelése minősített bizalmi szolgáltatáshoz (BSZ-DÁP-TK)

Verziószám	1.4
OID	0.2.216.1.200.1100.100.42.3.1.39
Hatályba lépés dátuma	2025.02.05.
Dokumentum besorolása	nyilvános
Jóváhagyó	Adorján István

Adorján István

Digitálisan aláírta: Adorján István
Dátum: 2025.02.04 09:37:44 +01'00'

Változáskövetés

verzió	dátum	a változás leírása	készítette	ellenőrizte	jóváhagyta
0.1	2024.07.17	első változat	NISZ Zrt. Polysys Kft. ACPM Zrt.	Kővári-Szabó Zoltán Németvári Tibor Nagy Benjámin	-
0.2	2024.07.24	elsődleges észrevételeket beépítő, a DÁP-TAN szolgáltatásba tartozó részeket elhagyó változat	ACPM Zrt.	Kővári-Szabó Zoltán Németvári Tibor Nagy Benjámin	-
0.3	2024.07.30	Felügyeleti szervnek benyújtott előzetes változat	ACPM Zrt.	Kővári-Szabó Zoltán Nagy Benjámin	-
0.4	2024.11.05.	Továbbfejlesztett változat	ACPM Zrt. Kővári-Szabó Zoltán	Nagy Benjámin Polysys Kft.	-
0.5	2024.11.28.	További pontosítások, javítások	Kővári-Szabó Zoltán	Nagy Benjámin ACPM Zrt.	-
1.0	2024.11.29	Első jóváhagyott verzió	Kővári-Szabó Zoltán	Nagy Benjámin ACPM Zrt. DÁP szolgáltató	Adorján István
1.1	2024.12.13	Megfelelőségértékelés észrevételeinek alkalmazása	Kővári-Szabó Zoltán	Nagy Benjámin	Adorján István
1.2	2024.12.17	Aláírásformátum pontosítása, hatálybalépés dátumának módosítása.	Kővári-Szabó Zoltán	Nagy Benjámin	Adorján István
1.3	2025.01.24	• Aktivizáló adat rontott bevitelére vonatkozó korlátozás követelményével való kiegészítés • A 2024. évi LXIX. törvény 116. § által hatályon kívül helyezett, az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényre (Ibtv.) hivatkozó szövegrészek törlése. • Elütések javítása.	Kővári-Szabó Zoltán	Nagy Benjámin	Adorján István
1.4	2025.02.03	A Bizalmi felügyelet észrevételei alapján további pontosítások	Gál Ferenc Nagy Benjámin	Kővári-Szabó Zoltán	Adorján István

Tartalomjegyzék

1 BEVEZETÉS

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

A Szolgáltató a fenti tárgykörben a {D9} BSZ-DÁP-TAN szolgáltatási szabályzatban meghatározott szolgáltatás keretében kibocsátott minősített tanúsítványokhoz kapcsolódóan alábbi szolgáltatást nyújtja:

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

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

- *elektronikus aláírások létrehozása;*
- *távoli elektronikus aláírás létrehozó eszköz 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

A szolgáltatási szabályzat célja, hogy összefoglalja mindazokat az információkat, melyeket a Szolgáltató DÁP-TK szolgáltatással kapcsolatba kerülő feleknek ismerni szükséges vagy érdemes. Biztosítja a Szolgáltató működésének átláthatóságát és annak megítélését a Szolgáltatásokat igénybe vevők számára, hogy az ismertetett szolgáltatási gyakorlat és tárolt magánkulcsok mennyiben felelnek meg az elvárásaiknak.

Jelen bizalmi szolgáltatási szabályzat az alábbi bizalmi szolgáltatási rend hatálya alá tartozó Szolgáltatásra vonatkozik:

> "Bizalmi Szolgáltatási Rend a Digitális Állampolgárság Program keretében nyújtott távoli elektronikus aláírás létrehozó eszköz kezelése és elektronikus aláírások létrehozása - minősített bizalmi szolgáltatáshoz"; OID: 0.2.216.1.200.1100.100.42.3.1.37 (BR-DÁP-TK).

Jelen bizalmi szolgáltatási szabályzat 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 BSZ-DÁP-TK kereteiben nincs követelmény előírva; ezekben a fejezetekben a "Nincs kikötés" szöveg szerepel.

Szolgáltató a jelen bizalmi szolgáltatási szabályzathoz kapcsolódó szolgáltatásait a Felügyeleti Szervnek 2024.07.31-én jelentette be. A Bizalmi Felügyelet erre vonatkozó nyilvántartásának elérhetősége: http://webpub-ext.nmhh.hu/esign2016/index.jsp

1.2 Dokumentum neve és azonosítása

1.2.1 A dokumentum neve

Jelen szolgáltatási szabályzat teljes neve: NISZ Zrt. " Bizalmi Szolgáltatási Szabályzat tárolt kulcsos elektronikus aláírás elhelyezés minősített bizalmi szolgáltatásokhoz".

A bizalmi szolgáltatási szabályzat rövid neve: BSZ-DÁP-TK.

A BSZ-DÁP-TK objektum azonosítója és verziószáma a címlapon található.

Jelen BSZ-DÁP-TK tartalmazza a {D10} BR-DÁP-TK bizalmi szolgáltatási rend hatálya alatt tárolt magán kulcsok generálására, tárolására és felhasználására vonatkozó részletes szabályokat.

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

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

1.2.2 A dokumentum azonosítása

A BSZ-DÁP-TK a DÁP tv. 8. § 43. pontja szerinti *szolgáltatási szabályzat*, mely a DÁP-TK szolgáltatás eljárásrendi és működési szabályait tartalmazza és amely egyúttal az ETSI EN 319 401 szerinti ún. *„trust service practice statement"*-nek és az ETSI TS 119 431-1 4.3.1 pontja szerinti ún. *„SSASC practice statement"*-nek tekintendő.

1.2.3 Hitelesítési rendek

A {D10} BR-DÁP-TK bizalmi szolgáltatási rend megfelel 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 szabályzatban szereplő PKI közösség az alábbi felekből áll:

- Szolgáltató: a jelen BSZ-DÁP-TK-nak megfelelő minősített 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 (a DÁP szolgáltató);
- 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, Szolgáltató teljes körű felelősséget vállal azért, hogy a Közreműködő Fél tevékenysége során jelen szabályzatban 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 szolgáltatási szabályzat szempontjából feladatai közé tartozik az Aláírók magánkulcsának tárolása, a távoli elektronikus aláírás létrehozó eszköz kezelése és elektronikus aláírások létrehozása.

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

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

Szolgáltató – a Telefonos Ügyfélszolgálat (Kormányzati Ügyfélvonal – 1818) kivételével – az állampolgárokkal közvetlen kapcsolatot nem tart, Aláírók a DÁP keretalkalmazáson keresztül vehetik igénybe a tanúsítvány kibocsátásra és visszavonás kezelésre irányuló szolgáltatásokat.

1.3.2 Közreműködő felek

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 az {D1} ÁSZF-DÁP elfogadásával Szolgáltatási Szerződést kötnek a Szolgáltatóval a DÁP-TAN és DÁP-TK szolgáltatások igénybevételére. Mivel az Aláíró a {D9} BSZ-DÁP-TAN-ban foglaltaknak megfelelően csak a saját nevére szóló tanúsítványt igényelhet, így jelen dokumentum fogalomrendszerében az Előfizető és az Aláíró személye azonos.

Jelen bizalmi szolgáltatási szabályzat hatálya alatt a Szolgáltató kizárólag a Digitális Állampolgárság Program keretében, Magyarország azon állampolgárai, mint Aláírók részére biztosít szolgáltatást, akik megfelelnek a {D9} BSZ-DÁP-TAN 4.1.1 pontjában foglaltaknak.

Kizárólag az Aláíró aktivizálhatja saját magánkulcsát a Szolgáltató által felügyelt minősített elektronikus aláírás létrehozó eszközön.

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 érvényesítéséhez, a tanúsítvány érvényességének megállapításához minden esetben szükséges igénybe vennie a Szolgáltató visszavonási információt

szolgáltató Szolgáltatásait (OCSP).

Az Érintett Felek felelősségét a • 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 aláírás érték 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 tanúsítvány 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 szabályzat 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 szabályzat alkalmasságának meghatározása

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

1.5.4 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-TK új verzióját a Szolgáltató vezetése hagyja jóvá és lépteti hatályba.

A BSZ-DÁP-TK új verzióját a Szolgáltató a hatályba lépést megelőzően legalább 30 nappal előzetesen bejelenti a Bizalmi Felügyelet részére. A szolgáltatási szabályzat jogszabályoknak való megfelelőségét a Bizalmi Felügyelet is ellenőrzi.

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

Az új verzió kötelező érvényű az összes Aláíróra, valamint az összes, az új verzió hatálybalépése utáni kulcshasználatra, illetve az így kibocsátott tanúsítványokra

1.6 Fogalmak, rövidítések és hivatkozások

1.6.1 Fogalmak

alany: A Szolgáltató 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 szabályzat 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 szabályzat 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 szabályzat szerinti bizalmi szolgáltatás a c) és az f) pont alatti szolgáltatások, azzal, hogy a Szolgáltató jelen BSZ-DÁP-TK keretében kizárólag elektronikus aláírások létrehozását végzi az állampolgárok mint Aláírók 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 felhasználóazonosítását.

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

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 szabályzat 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 szabályzatban: 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.

Interfész Specifikáció: a DÁP-TK szolgáltatást kiközvetítő DÁP (eID) szolgáltatóra vonatkozó műszaki dokumentáció, amely meghatározza, hogy az Aláíró által használt DÁP keretalkalmazás hogyan kapcsolódhat a DÁP-TK szolgáltatáshoz, abból célból, hogy az Aláíró tárolt magánkulcsával távolról elektronikus aláírásokat hozzon létre.

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

1.6.2 Rövidítések

ÁSZF-DÁP		Általános Szerződési Feltételek a DÁP eAláírás szolgáltatáshoz
BR-DÁP-TAN		Bizalmi Szolgáltatási Rend a Digitális Állampolgárság Program keretében kibocsátott minősített tanúsítványokhoz
BSZ-DÁP-TAN		Bizalmi Szolgáltatási Szabályzat a Digitális Állampolgárság Program keretében kibocsátott minősített tanúsítványokhoz
BR-DÁP-TK		Bizalmi Szolgáltatási Rend a Digitális Állampolgárság Program keretében nyújtott elektronikus aláírások létrehozása és távoli elektronikus aláírás létrehozó eszköz kezelése minősített bizalmi szolgáltatáshoz
BSZ-DÁP-TK		Bizalmi Szolgáltatási Szabályzat a Digitális Állampolgárság Program keretében nyújtott elektronikus aláírások létrehozása és távoli elektronikus aláírás létrehozó eszköz kezelése minősített bizalmi szolgáltatáshoz
CA	Certification Authority	hitelesítő szervezet
CP	Certificate Policy	hitelesítési rend
CPS	Certificate Practice Statement	hitelesítési szolgáltatási szabályzat
CRL	Certification Revocation List	tanúsítvány visszavonási lista
DÁP		Digitális Állampolgárság Program
DÁP-TAN		Szolgáltató BSZ-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	
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
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} 2013. évi V. törvény a Polgári Törvénykönyvről

{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	Bizalmi Szolgáltatási Rend a Digitális Állampolgárság Program keretében nyújtott elektronikus aláírások létrehozása és távoli elektronikus aláírást létrehozó eszközök kezelése minősített bizalmi szolgáltatáshoz
{D11}	BSZ-DÁP-TK	Jelen bizalmi szolgáltatási szabályzat

2 KÖZZÉTÉTEL ÉS ADATTÁRAK

2.1 Adattárak

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

2.2 Szolgáltatói információ közzététele

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

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

2.3 A közzététel gyakorisága

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

2.4 Hozzáférés-ellenőrzések

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

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

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

3 AZONOSÍTÁS ÉS HITELESÍTÉS

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

A kriptográfiai műveletek aktiválásához szükséges felhasználóazonosítás az alábbiak szerint történik.

3.1 Az azonosítás és hitelesítés biztonsági szintje

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

3.2 Az Aláírók felhasználóazonosítása

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 fél végzi, a {D9} BSZ-DÁP-TAN 3.2 fejezete szerinti személyazonosításra építve.

4 A SZOLGÁLTATÁS ÉLETCIKLUSA

4.1 A Szolgáltatás igénylése

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 {D9} 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 {D9} BSZ-DÁP-TAN 4.9 fejezete).

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

4.3 A Szolgáltatás elérhetősége és rendelkezésre állása

A Szolgáltatás a DÁP keretalkalmazáson keresztül érhető el.

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

4.4 A Szolgáltatás használata

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

Az Aláírók a Szolgáltatást a DÁP szolgáltató közvetítésével, a DÁP keretalkalmazásban használhatják.

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

[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.

egyértelműen azonosíthassa az Aláíró által használt keretalkalmazást. Ezt az üzenethitelesítő kulcspárt a DÁP keretalkalmazás a DÁP-TAN szolgáltatás keretében történő tanúsítványigénylés során generálja, majd annak nyilvános kulcsát továbbítja mind a Szolgáltatónak, mind pedig a DÁP szolgáltatónak. Szolgáltató az üzenethitelesítő nyilvános kulcsot a megfelelő aláíróhoz rendelve rögzíti a szolgáltatást megvalósító saját informatikai rendszerében. A későbbiekben a DÁP keretalkalmazás az üzenethitelesítő kulcspár magánkulcsával hitelesíti üzenetét mind a Szolgáltató, mind a DÁP szolgáltató felé – a jelen DÁP-TK szolgáltatás és a DÁP-TAN szolgáltatás keretén belül egyaránt (lásd BSZ-DÁP-TAN 4.1.2.4).

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

4.5 Előfizetés vége

Az előfizetés az {D1} ÁSZF-DÁP-ban meghatározott esetekben és módon szűnik meg.

A Szolgáltatás a tárolt kulcshoz tartozó tanúsítvány érvényességének {D9} BSZ-DÁP-TAN szerinti lejáratával szűnik meg. A Szolgáltatás igénybe vételét a tárolt kulcshoz tartozó tanúsítvány {D9} BSZ-DÁP-TAN szerinti visszavonásával lehet megszüntetni.

5 FIZIKAI, ELJÁRÁSBELI ÉS SZEMÉLYZETI BIZTONSÁGI ÓVINTÉZKEDÉSEK

A Szolgáltató a Szolgáltatások nyújtása során a kellő, az irányadó szabványoknak megfelelő fizikai, eljárásbeli és személyzeti biztonsági óvintézkedéseket és az ezeket érvényre juttató adminisztratív és irányítási eljárásokat alkalmazza.

A Szolgáltató a rendszer kialakításakor kockázat-elemzést végzett üzleti kockázatainak felmérésére, valamint a szükséges biztonsági követelmények és működési eljárások meghatározására; a kockázatok felülvizsgálatáról legalább negyedévente rendszeresen, valamint szükség esetén eseti jelleggel gondoskodik. Szolgáltató a szervezetén belüli biztonságkezeléshez szükséges informatikai biztonsági infrastruktúrát folyamatosan fenntartja. A biztonság szintjére hatást gyakorló bárminemű változtatást a Szolgáltató vezetősége hagy jóvá.

A biztonságkezelési szabályokat a Szolgáltató {D5} PKI szolgáltatások biztonságpolitikája tartalmazza. A Szolgáltató informatikai rendszerei vonatkozásában a Szolgáltató {D6} biztonsági szabályzat érvényesül. Ez a szabályzat szervezeti egység szinten és munkakörökre lebontva rögzíti a biztonságkezeléssel összefüggő feladatokat, felelősségeket és szabályokat, így többek között a bizalmi munkakörök felsorolását, a kinevezési feltételeket és az összeférhetetlenségi kritériumokat.

A Szolgáltató megvalósította és folyamatosan fenntartja a Szolgáltatásokat nyújtó eszközök, rendszerek biztonsági ellenőrzéseit és üzemeltetési eljárásait. A Szolgáltató rendszeres belső ellenőrzései és külső auditjai ezen eljárásokat, a vonatkozó dokumentumokat és a Szolgáltatásokra vonatkozó előírások teljesülését rendszeres időközönként vizsgálja.

A fenti eljárásokat a Szolgáltatóval munkaviszonyban álló, megbízható és szakértő üzemeltető személyzet biztosítja.

A Szolgáltató gondoskodik arról, hogy eszközei és információi a megfelelő szintű védelemben részesüljenek. A Szolgáltató valamennyi informatikai értékéről leltárt vezet, ezek védelmi követelményeit az elvégzett kockázatelemzéssel összhangban osztályokba sorolja és minősíti.

A Szolgáltató a szolgáltatásnyújtásban közreműködő informatikai rendszereit, berendezéseit és eszközeit a legmagasabb védelmi szintet képező központi géptermében helyezi el.

5.1 Fizikai óvintézkedések

5.1.1 Telephelyek elhelyezése és szerkezeti felépítése

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

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

5.1.2 Fizikai hozzáférés

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

Ehhez biztosítja az alábbiakat:

- a géptermekbe történő minden be- és kilépés, valamint a belépés célja 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 és létszámú, 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 Szolgáltató a gépteremben olyan szünetmentes áramellátó rendszert alkalmaz, 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 Szolgáltató a gépteremben olyan légkondicionáló berendezést alkalmaz, 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 üzemi hőmérséklet biztosítására, az eszközök és berendezések túlhevülésének megakadályozására.

5.1.4 Beázás és elárasztás veszélyeztetettség

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

5.1.5 Tűzmegelőzés és tűzvédelem

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

5.1.6 Adathordozók tárolása

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

5.1.7 Selejt kezelése és megsemmisítése

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

5.1.8 Fizikailag elkülönítetten őrzött mentési példányok

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

5.2 Eljárásbeli előírások

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

Az eljárásbeli szabályokat a következő szabályzatok tartalmazzák:

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

5.2.1 Bizalmi munkakörök

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

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

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

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

bizalmi munkakört legalább két személy tölt be.

A bizalmi munkaköröket betöltő személyekről Szolgáltató nyilvántartást vezet. A nyilvántartásban bekövetkező minden változást a változtatás bevezetése előtt a Felügyeleti Szervnek bejelenti.

5.2.2 Az egyes feladatokhoz szükséges személyzeti létszámok

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

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

5.2.3 Bizalmi munkakörökben elvárt azonosítás és hitelesítés

A bizalmi munkaköröket betöltő személyek azonosítása és hitelesítése erős PKI eljárásokkal, pl. tokenen tárolt tanúsítványok és az azt aktivizáló PIN kód megadásával történik meg, mielőtt a Szolgáltatások nyújtásában érintett kritikus informatikai rendszerekhez hozzáférhetnének.

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

- Biztosítani kell a rendszergazdai célokra, például telepítésre, konfigurálásra, kezelésre vagy karbantartásra használt egyedi fiókok beállítását.
- A jogosultsággal rendelkező fiókok csak akkor használhatók, ha a jogosultságok az adott tevékenységhez szükségesek.
- A privilegizált fiókok esetében erős azonosítási, hitelesítési és engedélyezési eljárásokat kell alkalmazni.
- Tervezett időközönként felül kell vizsgálni a privilegizált és rendszergazdai fiókokhoz való hozzáférési jogokat, és ezeket a szervezeti változások alapján módosítani kell. A felülvizsgálat eredményét, beleértve a hozzáférési jogok szükséges módosításait, dokumentálni kell.
- Biztosítani kell, hogy a hozzáférési jogosultságok megfelelően módosuljanak a munkaviszony megszűnésekor vagy a funkcióváltáskor.
- Az információhoz és az alkalmazói rendszer funkcióihoz való hozzáférést belső szabályzatnak megfelelően korlátoznia kell.
- A Szolgáltató rendszerében megfelelő számítógépes biztonsági intézkedéseket kell biztosítani a Szolgáltató gyakorlatában azonosított bizalmi szerepkörök szétválasztásához, beleértve a biztonsági adminisztrációs és üzemeltetési funkciók szétválasztását. Különösen a rendszer-segédprogramok használatát kell korlátozni és ellenőrizni.
- A Szolgáltató személyzetét azonosítani és hitelesíteni kell a szolgáltatáshoz kapcsolódó kritikus alkalmazások használata előtt.
- A Szolgáltató személyzetének elszámoltathatónak kell lennie a végzett tevékenységéért.
- Az érzékeny adatokat védeni kell az újra felhasznált tárolóobjektumokon (pl. törölt fájlok) felfedés ellen, illetve az adathordozókhoz való illetéktelen hozzáféréstől.

5.2.4 Egymást kizáró munkakörök

Szolgáltató biztosítja, hogy a bizalmi munkakörök vonatkozásában:

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

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

5.3 Személyzetre vonatkozó előírások

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

A Szolgáltató kellő számú, a Szolgáltatások nyújtásához szükséges feladatok jellegének, terjedelmének és mennyiségének megfelelő végzettséggel, képzettséggel, szakmai tudással és tapasztalattal rendelkező személyzetet alkalmaz.

A Szolgáltató valamennyi bizalmi munkakört betöltő munkatársa mentes minden olyan ütköző érdektől, ami hátrányosan érinthetné a Szolgáltatások megbízhatóságát és biztonságát.

A munkatársak a feladatok szétválasztása és a legkisebb meghatalmazás szempontjai alapján meghatározott munkaköri leírásokkal rendelkeznek.

5.3.1 Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

A Szolgáltató biztosítja, hogy bizalmi munkakört csak olyan személyek töltsenek be, akiknek a bizalmi munkakör betöltéséhez szükséges befolyásmentességét és szakértelmét erkölcsi bizonyítvánnyal, szakmai gyakorlattal, végzettséggel vagy szakképesítéssel igazolni tudja.

A Szolgáltató informatikai rendszeréért általánosan felelős vezető szakirányú felsőfokú végzettséggel és legalább három év, az informatikai biztonsággal összefüggésben szerzett szakmai gyakorlattal rendelkezik. Szakirányú felsőfokú végzettség a matematikusi, fizikusi egyetemi végzettség vagy a műszaki tudományterületre tartozó mérnöki szakon szerzett főiskolai vagy egyetemi végzettség.

A biztonsági tisztviselők és rendszervizsgálók esetén közép vagy felsőfokú végzettség, középfokú végzettség esetén legalább három, felsőfokú végzettség esetén legalább egy év informatikai biztonsággal összefüggésben szerzett szakmai gyakorlat szükséges.

A rendszerüzemeltető és rendszeradminisztrátor esetén középfokú végzettség és legalább egy év, hasonló munkakörben szerzett szakmai gyakorlat szükséges.

5.3.2 Biztonsági háttér ellenőrzés eljárásai

A Szolgáltató csak olyan alkalmazottakat foglalkoztat, 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.

A Szolgáltatás nyújtásával kapcsolatos valamennyi munkakör betöltését a legmagasabb szintű biztonsági ellenőrzés (a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvényben meghatározott nemzetbiztonsági ellenőrzés) előzi meg.

A bizalmi munkakörhöz történő hozzárendeléskor az érintett személy:

- pontos és írásos munkaköri leírást vesz át a fölérendelt vezetőtől vagy a Szolgáltató humán szervezetétől;
- szükséges mértékű oktatásban részesül, annak érdekében, hogy a feladat-, felelősség és

hatáskörét pontosan megismerje és gyakorolni tudja.

Kilépéskor:

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

5.3.3 Képzési követelmények

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

- a PKI elméleti alapjait;
- 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 Szolgáltató gondoskodik arról, hogy a munkatársak folyamatosan a megfelelő tudással rendelkezzenek, szükség esetén továbbképzést vagy ismétlő jellegű képzést tart vagy biztosít.

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

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

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

A Szolgáltató legalább évente egyszer továbbképzést biztosít 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 Szolgáltató a munkavállalóval kötött munkaszerződésben vagy külső munkatárssal kötött megbízási szerződésben szabályozza a munkavállaló vagy külső munkatárs felelősségre vonásának lehetőségét az elkövetett mulasztások, vétlen vagy szándékos károkozás esetére.

5.3.7 Szerződéses munkavállalókra vonatkozó követelmények

A Szolgáltató bizalmi munkakörben csak munkaviszonyban álló személyt foglalkoztat.

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

5.3.8 A személyzet számára biztosított dokumentációk

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

Minden bizalmi munkakört betöltő munkatárs megkapja írásban:

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

5.4 A biztonsági naplózás folyamatai

5.4.1 Naplózott esemény típusok

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

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

A Szolgáltatások nyújtásával kapcsolatos események különösen az alábbiak:

- a Szolgáltatás nyújtásához használt informatikai rendszer működtetéséhez szükséges infrastrukturális és vezérlő kulcsok életciklusával kapcsolatos minden esemény;
- a Szolgáltatásban kapott kérések és válaszok;
- tárolt végfelhasználói magánkulcs életciklusával kapcsolatos minden esemény;
- tárolt végfelhasználói magánkulcsok használatának eseményei;
- adatok továbbítása;
- jogosultságok, jelszavak módosítása;
- sikeres és sikertelen belépési kísérletek;
- adatok módosítása és továbbítása;
- hálózati események.

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

5.4.2 Naplóállomány feldolgozásának gyakorisága

A Szolgáltató biztosítja a naplóállományok rendszeres ellenőrzését és kiértékelését.

A Szolgáltatások nyújtásával kapcsolatos események naplóállományait naponta feldolgozzák a

rendszervizsgálók.

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

5.4.3 Naplóállomány megőrzési időtartama

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

5.4.4 Naplóállomány védelme

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

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

5.4.5 Naplóállomány mentési folyamatai

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

5.4.6 Naplózás gyűjtési rendszere

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

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

5.4.7 Rendellenes eseményeket kiváltó alanyok értesítése

A rendellenes eseményeket kiváltó alanyokat (személyeket, szervezeteket) Szolgáltató nem feltétlenül értesíti minden esetben. Szolgáltató szükség esetén bevonhatja az eseményt kiváltó alanyt az esemény kivizsgálásába. Ilyen esetben az érintett Közreműködő Fél, Aláíró kötelessége a Szolgáltatóval való együttműködés az esemény feltárása érdekében.

5.4.8 Sebezhetőség értékelések

A Szolgáltató a vonatkozó szabványok által meghatározott rendszeres időközönként, a naplóállományok és egyéb információk kiértékelésén alapuló sebezhetőség vizsgálatot és behatolás tesztet végez. Ennek segítségével feltérképezi a potenciális belső és külső fenyegetéseket, melyek a Szolgáltató által tárolt végfelhasználói magánkulcsok módosítását, sérülését, megsemmisülését vagy jogosulatlan aktiválását eredményezhetik.

A sebezhetőség vizsgálathoz kapcsolódóan Szolgáltató kockázatelemzésben értékeli az egyes fenyegetések bekövetkeztének valószínűségét és a bekövetkezés esetén várható kárt. Értékeli az alkalmazott folyamatokat, informatikai rendszereket, védelmi intézkedéseket, hogy azok megfelelően képesek-e ellenállni a fenyegetésnek.

A kiértékelést követően a Szolgáltató megteszi a megfelelő intézkedéseket annak érdekében, hogy

a feltárt sebezhetőség kihasználhatósága ne következzen be.

A Szolgáltató folyamatosan figyelemmel kíséri az újonnan ismertté vált, kritikus sebezhetőségeket, és a szükséges ellenintézkedéseket lehetőség szerint 48 órán belül megteszi. Bármely olyan sebezhetőség esetén, melynek kihatása lehet a Szolgáltatások nyújtására, a Szolgáltató vagy cselekvési tervet készít és hajt végre annak érdekében, hogy a sebezhetőség ne legyen kihasználható, illetve annak hatása elhanyagolható legyen, vagy dokumentálja annak ténybeli alapját, hogy az adott sebezhetőség nem igényel intézkedést.

5.5 Adatok archiválása

5.5.1 A tárolt adatok típusai

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

Ehhez legalább az alábbi információkat tárolja papír alapon vagy elektronikusan:

- az Aláíró tárolt magánkulcsával kapcsolatos valamennyi információ a teljes életciklusra vonatkozóan;
- a bizalmi szolgáltatási rendek 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, 5.4.1 pont szerinti naplóállomány.

5.5.2 Archívum megőrzési időtartama

A Szolgáltató az 5.5.1 fejezetben meghatározott archivált adatokat az alábbi időtartamokig őrzi meg:

- az Aláíró tárolt magánkulcsával és a tanúsítványokkal kapcsolatos adatok és naplóállomány esetében a tanúsítvány érvényességnek lejáratáról számított 10 évig, illetve a tanúsítvánnyal előállított elektronikus aláírással kapcsolatos jogvita jogerős lezárásáig;
- szabályzatok, szerződések esetében a hatályon kívül helyezés vagy megszűnés utáni 10 évig;

5.5.3 Archívum védelme

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

5.5.4 Archívum mentési eljárásai

A Szolgáltató a papír alapú iratokat, dokumentumokat a dokumentumtárban, az elektronikus állományokat pedig több példányban, fizikailag elkülönített helyszíneken őrzi meg, illetve tárolja.

A Szolgáltató biztosítja az elektronikus formában archivált állományok adathordozóinak elavulás elleni védelmét a megőrzési időn belül.

5.5.5 Az adatok időbélyegzésére vonatkozó követelmények

Valamennyi naplóbejegyzésben olyan időjel szerepel, amely a 6.8 fejezetben ismertetett időforrásokkal szinkronizált rendszeridőt tartalmazza, melynek pontossága egy másodpercen belüli.

A naplóállományokra óránként legalább fokozott biztonságú elektronikus bélyegző és minősített időbélyeg kerül.

Az elektronikus formában archivált adatokon elhelyezett elektronikus aláírás vagy bélyegző minősített időbélyeget tartalmaz.

A Szolgáltató az archivált adatok megőrzése során szükség esetén (pl. algoritmus váltás) gondoskodik az elektronikus aláírások vagy bélyegzők, valamint az időbélyegzők hitelességnek fenntartásáról.

5.5.6 Archívum gyűjtési rendszere

A naplóállományok és az egyéb elektronikusan keletkezett adatokat a Szolgáltató védett informatikai rendszerén belül gyűjti.

5.5.7 Archívum hozzáférés és ellenőrzés eljárásai

A Szolgáltató az archivált adatokat megvédi a jogosulatlan hozzáféréstől. Szolgáltató a jogosultságot ellenőrzi, és a hozzáféréseket naplózza.

A Szolgáltató az Ügyfélszolgálat közreműködésével biztosítja az Aláírók számára a róluk tárolt személyes adatokra vonatkozó tájékoztatást.

A Szolgáltató a 9.4.6 fejezetben ismertetett hatósági vagy jogi eljárásokban a szükséges mértékben a biztosítja a hozzáférést az archívumban tárolt adatokhoz.

5.6 Kulcsátállás

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

5.7 Helyreállítás rendkívüli üzemeltetési helyzetek esetén

A Szolgáltató minden szükséges intézkedést meghoz annak érdekében, hogy rendkívüli üzemeltetési helyzet, katasztrófa esetén a szolgáltatás kiesésből származó károkat minimalizálja és a Szolgáltatásokat a lehető legrövidebb időn belül helyreállítsa.

Biztonsági esemény esetén – amennyiben az jelentős hatást gyakorol a szolgáltatásra vagy az annak keretében tárolt személyes adatokra –, Szolgáltató haladéktalanul, de legkésőbb az esetről való értesüléstől számított 24 órán belül értesíti az Érintett Feleket, valamint jelenti az incidenst a Felügyeleti Szervnek, valamint személyes adatok érintettsége esetén a {J5} GDPR 51. cikke szerinti illetékes hatóságnak.

A bekövetkezett incidens kiértékelése alapján Szolgáltató meghozza a szükséges módosító, javító intézkedéseket, hogy az incidens jövőbeli előfordulását megakadályozza.

5.7.1 Rendkívüli események és kompromittálódás kezelésének eljárásai

A Szolgáltató rendelkezik {D7} üzletmenet-folytonossági tervvel. Ez a dokumentum biztonsági okokból kifolyólag nem nyilvános.

A rendkívüli üzemeltetési helyzetben a Szolgáltató dokumentálja az eseményeket, azok körülményeit, az elhárításukra megtett intézkedéseket.

Rendkívüli üzemeltetési helyzetben a Szolgáltató életbe lépteti az üzletmenet folytonossági tervében megtervezett eljárásait annak érdekében, hogy az üzemeltetés helyreálljon az üzletmenet folytonossági tervben megjelölt időn belül.

A helyreállítás időtartamát az esemény súlyossága, azaz az üzletmenet folytonossági terv szerint értelmezett osztályba sorolása határozza meg.

A rendkívüli üzemeltetési helyzet határidőn túli fennállása esetén a Szolgáltató haladéktalanul értesíti a Felügyeleti Szervet, az esemény bekövetkeztéről, annak hatásáról, várható időtartamáról, az elhárítás érdekében tett és tervezett intézkedésekről, továbbá a rendkívüli üzemeltetési helyzet megszűnéséről.

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

5.7.2 Sérült számítási erőforrások, szoftverek és/vagy adatok

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

5.7.3 Magánkulcs kompromittálódása esetén követendő eljárás

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

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

Szolgáltató az általa tárolt végfelhasználói (aláírói) magánkulcsok kompromittálódása esetére akciótervvel rendelkezik, melyet az üzletmenet folytonossági tervében tervezett meg. E szerint megteszi az alábbi főbb lépéseket:

- 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 Szolgáltató rendelkezik tartalék helyszínnel és informatikai rendszerrel, továbbá megtervezett eljárásokkal az áttelepülésre.

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

5.8 A szolgáltatási tevékenység megszüntetése

A Szolgáltató rendelkezik olyan bankgaranciával, mely fedezi a szolgáltatási tevékenység megszüntetésének költségeit abban az esetben, ha Szolgáltató csődeljárás alá kerül vagy más okból kifolyólag nem képes önmaga fedezni a költségeket. Ha Szolgáltató ellen felszámolási, végelszámolási vagy egyéb kényszertörlési eljárás indult, erről és a felszámolóról vagy végelszámolóról Szolgáltató haladéktalanul tájékoztatja a Felügyeleti Szervet.

A Szolgáltató az alábbi, a szolgáltatási tevékenység megszüntetésére vonatkozó tervvel rendelkezik:

- A tervezett megszűnés előtt kellő időben tárgyalásokat kezdeményez más minősített bizalmi szolgáltatókkal a Szolgáltatásokkal járó kötelezettségek - különösen az 5.5.1 fejezetben meghatározott adatoknak a megőrzése az 5.5.2 fejezetben megjelölt időtartamig - átadás-átvételéről.
- A Szolgáltató gondoskodik a Szolgáltatások megszüntetéséből fakadó, a felhasználói közösséget érintő zavarok minimalizálásáról.
- A megszüntetés előtt legalább 90 nappal korábban:
  - értesíti a Felügyeleti Szervet, és internetes honlapján tájékoztatja a felhasználói közösség tagjait;
  - beszünteti az új Szolgáltatás igénylések fogadását;
  - egy másik minősített bizalmi szolgáltatóval megállapodást köt a Szolgáltatásokkal járó kötelezettségek átadás-átvételéről, és ennek másolatát megküldi a Bizalmi Felügyeletnek;
- A megszüntetés előtt legalább 20 nappal korábban:
  - beszünteti a Szolgáltatással kapcsolatos nyilvános szabályzatok közzétételét és gondoskodik arról, hogy ezzel egyidejűleg azok az átvevő szolgáltatónál elérhetővé váljanak;
  - a Szolgáltatás nyújtásához használt informatikai rendszer működtetéséhez szükséges infrastrukturális és vezérlő kulcsokat és azok mentéseit olyan módon semmisíti meg, hogy azok használata a továbbiakban már nem lehetséges;
- A megszüntetés napjával:
  - Szolgáltató az informatikai rendszerében foglalt adatokról teljes körű, időbélyegzővel és elektronikus aláírással vagy bélyegzővel ellátott mentést készít. Szolgáltató a mentett adatállományokat védi a jogosulatlan módosítástól, és biztosítja, hogy az adatállomány tartalmához jogosulatlan személy nem férhet hozzá. Szolgáltató a megkötött szerződés révén biztosítja, hogy az adatok a megőrzési időn belül az arra jogosult személyek számára hozzáférhetőek és értelmezhetőek maradjanak.

6 MŰSZAKI BIZTONSÁGI ÓVINTÉZKEDÉSEK

6.1 Kulcspár előállítás és telepítés

6.1.1 Kulcspár előállítás

6.1.1.1 Szolgáltatói kulcsok előállítása

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

6.1.1.2 Előfizetői kulcspárok előállítása

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

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

6.1.2 Magánkulcs eljuttatása a tulajdonoshoz

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

6.1.3 Nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz

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

6.1.4 A szolgáltatói nyilvános kulcs közzététele

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

6.1.5 Kulcsméretek

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

A Szolgáltató folyamatosan figyelemmel kíséri a technikai fejlődést és ennek függvényében szükség esetén gondoskodik az algoritmus váltásról vagy a kulcshosszak növeléséről.

Az előfizetői kulcspárok algoritmusa és mérete:

végfelhasználó	algoritmus azonosító	görbe
,,DÁP aláíró tanúsítvány"	ecdsaWithSHA384	secp384r1

A Szolgáltató folyamatosan figyelemmel kíséri a technikai fejlődést és ennek függvényében szükség esetén, megfelelő időben gondoskodik az algoritmus váltásról vagy a kulcshosszak növeléséről.

6.1.6 A nyilvános kulcs paraméterek előállítása és megfelelőségének ellenőrzése

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

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

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

6.2 Magánkulcs védelme és kriptográfiai modul műszaki szabályozások

6.2.1 Kriptográfiai modul szabványok és szabályozások

A Szolgáltató a szolgáltatói magánkulcsok előállítására, tárolására és használatára olyan kriptográfiai modult alkalmaz, amely olyan megbízható rendszer, amelynek értékelése az {Sz6} ISO/IEC 15408 szerint, illetve azzal egyenértékű biztonsági kritériumok szerint 4-es vagy magasabb értékelési garancia szinten történt meg (EAL 4+).

A Szolgáltató az Aláíró magánkulcsait olyan DÁP-HSM modulban tárolja és aktiválja, amely rendelkezik kijelölt tanúsító szervezet, vagy az Európai Unió valamely tagállamában nyilvántartásba vett, tanúsításra jogosult szervezet által kiadott igazolással, a minősített elektronikus aláírás létrehozó eszköz (QSCD) követelményeinek való megfelelésről.

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

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

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

6.2.3 Magánkulcs letét

A Szolgáltató nem nyújt az Aláírók számára magánkulcs letét szolgáltatást.

6.2.4 Magánkulcs visszaállítása

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

6.2.5 Magánkulcs mentése

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

6.2.6 Magánkulcs bejuttatása a kriptográfiai modulba

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

6.2.7 Magánkulcs kriptográfiai modulban történő tárolásának módja

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

6.2.8 Magánkulcs aktiválásának módja

A DÁP-TK Szolgáltatás nyújtásához használt informatikai rendszer működtetéséhez szükséges infrastrukturális és vezérlő kulcsok aktiválását Szolgáltató a DÁP-HSM modul gyártói dokumentációjában előírtak szerint végzi el.

A Szolgálató biztosítja, hogy az aktivált HSM modul és DÁP-HSM modul jogosulatlan hozzáférés ellen védett legyen.

Az Aláíró magánkulcsának aktiválásához a DÁP keretalkalmazás által előállított üzenethitelesítő kulcspár magánkulcsa szükséges. Szolgáltató akkor aktiválja az Aláíró DÁP-HSM modulban tárolt magánkulcsát, ha az aláírási kérés az Aláíróhoz rendelt üzenethitelesítő nyilvános kulcs magánkulcs párjával került hitelesítésre. Az üzenethitelesítő magánkulccsal történő hitelesítéshez Aláírónak a kapcsolódó tanúsítvány DÁP-TAN szolgáltatás keretében történt igénylésekor megadott és megerősített jelszó megadása szükséges a DÁP keretalkalmazásban.

Lásd még 6.4 Aktivizáló adatok.

6.2.9 Magánkulcs aktív állapotának megszüntetési módja

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

6.2.10 Magánkulcs megsemmisítésének módja

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

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

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

A magánkulcs és az aktiválásához szükséges minden adat megsemmisítését olyan módon végzi, 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

A {D9} BSZ-DÁP-TAN 6.3.1 szerint.

6.3.2 Tanúsítvány érvényességi időszaka és kulcspár felhasználás időtartama

A {D9} BSZ-DÁP-TAN 6.3.2 szerint.

6.4 Aktivizáló adatok

6.4.1 Aktivizáló adatok előállítása

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

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

6.4.2 Aktivizáló adatok védelme

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

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 és a {Sz3} TS 119 431-1 szabványok informatikai biztonsági műszaki követelményeiben határozza meg.

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

6.5.2 Informatikai biztonsági értékelés

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

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.

A fentiek megfelelnek a {J9} NIS2 rendelet és a kapcsolódó {J10} 2024/2690 végrehajtási rendelet vonatkozó követelményeinek.

6.6 Életciklusra vonatkozó műszaki óvintézkedések

6.6.1 Rendszerfejlesztési óvintézkedések

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

Az IT életciklusra vonatkozó rendszerfejlesztési szabályokat a Szolgáltató belső információbiztonsági szabályzata tartalmazza, amely pontosan meghatározza a tervezés és előkészítés, a projekt és kivitelezés, a működtetés és a menedzselés, valamint a visszacsatolás, illetve visszavonás/rekonstrukció ciklus időszakok feladatait és az alkalmazott módszertanokat.

6.6.2 Biztonságkezelési óvintézkedések

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

A biztonságkezelési szabályokat a Szolgáltató PKI informatikai biztonságpolitikája {D5}, illetve biztonsági szabályzata {D6} tartalmazza.

6.6.3 Életciklus biztonsági óvintézkedések

A Szolgáltató a belső szabályzati szerinti rendszerességgel elvégzi a Szolgáltatásokat megvalósító, megbízható informatikai rendszereinek konfigurációs beállításai, az operációs rendszer beállítások, a hálózati konfigurációs beállítások, továbbá az alkalmazott biztonsági mechanizmusok sértetlenségének és helyes működésének ellenőrzését.

6.7 Hálózatbiztonsági óvintézkedések

A hálózati védelmi intézkedéseket a Szolgáltató {D6} biztonsági szabályzatában meghatározott követelményeknek megfelelően valósítja meg.

6.8 Időforrások

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

A megbízható időforrások Szolgáltató saját rendszerén belüli, redundáns kialakítású, speciális célberendezések (referencia időforrások), melyek pontossága egy másodpercen belüli, és amelyek GPS alapúak, így visszavezethetőek az UTC időforrásra.

7 TANÚSÍTVÁNY, CRL ÉS OCSP PROFILOK

7.1 Tanúsítvány profil

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

7.2 CRL profil

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

7.3 OCSP profil

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

8 MEGFELELŐSÉG VIZSGÁLAT ÉS EGYÉB ÉRTÉKELÉSEK

Jelen bizalmi szolgáltatási szabályzat 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 gyakorisága és körülményei megfelelnek a hatályos jogszabályi előírásoknak.

A Szolgáltató legalább 24 havonta egyszer megfelelőségértékelést és 12 havonta egyszer felülvizsgálatot végeztet a {J1} eIDAS 3. cikk 18. bekezdésben meghatározott megfelelőségértékelő szervezettel, a {J1} eIDAS, illetve a {J2} DÁP tv. követelményeinek való megfelelés tárgykörben. Szolgáltató az elkészült megfelelőségértékelés jelentést annak kézhezvételétől számított három munkanapon belül benyújtja 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 és a kiberbiztonsági audit előkészítésére, illetve az információbiztonsági rendszer ellenőrzésére Szolgáltató külső rendszervizsgálót alkalmaz.

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 765/2008/EK 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 a Szolgáltató olyan auditorral végezteti el, amely szerepel a Kiberbiztonsági Felügyelet által nyilvántartott auditor listán, és amely jogosult a Szolgáltató elektronikus információs rendszerének biztonsági osztálya szerinti auditálásra.

Az információbiztonsági rendszer ellenőrzését a Szolgáltató olyan szakértővel vagy szakértői szolgáltatásokat nyújtó szervezettel végezteti el, aki független Szolgáltatótól, illetve az ellenőrzött rendszertől, területtől, és szakértelmét biztosítani tudja a PKI és az informatikai biztonság, valamint az ezen területekre vonatkozó technikai, technológiai, jogi, szabályzati ismeretek és auditálási módszertanok vonatkozásában.

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 Szolgáltató intézkedési tervet készít. A hiányosságokat késlekedés nélkül orvosolja, az intézkedéseket dokumentálja és ellenőrzi.

A Felügyeleti Szerv által végzett rendszeres helyszíni ellenőrzések során feltárt esetleges hiányosságokat Szolgáltató a hatóság által megállapított határidőn belül megszünteti a hatályos jogszabályok alapján és a hatóságtól kapott információk és ajánlások figyelembe vételével.

8.6 Eredmény kommunikációja

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

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

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

A kiberbiztonsági audit eredményét – benne a feltárt hiányosságokat is - az auditor az audit befejezését követően haladéktalanul megküldi a Szolgáltatónak és a Kiberbiztonsági Felügyeletnek.

9 EGYÉB ÜZLETI ÉS JOGI KÉRDÉSEK

9.1 Díjak

Szolgáltató a magánkulcsok tárolásáért, annak távoli aktiválásáért és az aláírás érték kiszámításáért Végfelhasználó részére díjat nem számít fel.

9.2 Anyagi felelősség

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

9.2.1 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.

9.2.2 További követelmények

Szolgáltató rendelkezik a {J4} 24/2016 rendelet 20. §-a szerinti, huszonötmillió forint összegű, feltétel nélküli és visszavonhatatlan bankgaranciával.

9.2.3 Felelősségbiztosítás vagy garancia végfelhasználók számára

Nincs kikötés.

9.3 Üzleti információk bizalmassága

9.3.1 Bizalmasan kezelendő információk köre

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

9.3.2 Bizalmasnak nem tekintett információk köre

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.

9.3.3 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.

9.4 Személyes adatok védelme

9.4.1 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.

9.4.2 Bizalmasként kezelendő személyes adatok

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

9.4.3 Bizalmasként nem kezelendő személyes adatok

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

9.4.4 Személyes adatok védelmének felelőssége

Szolgáltató gondoskodik a személyes adatok védelméről, működése és szabályzatai megfelelnek a {J5} GDPR rendelkezéseinek.

9.4.5 Személyes adatok felhasználásának elfogadása

Aláírónak a {D1} ÁSZF-DÁP elfogadásával létrejött Szolgáltatási Szerződés keretében tudomásul kell vennie a szolgáltatások igénybevételéhez szükséges adatok Szolgáltató által történő kezelését és tárolását. Tekintettel arra, hogy a Szolgáltató adatkezelésének jogalapja jogi és szerződési kötelezettség teljesítése, a {J5} GDPR szerinti hozzájárulás nem értelmezhető.

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

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. Szolgáltató rögzíti az adatátadás tényét, és arról tájékoztatja érintett Aláírót.

9.4.7 Egyéb, felfedést eredményező körülmények

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

9.5 Szellemi tulajdonjogok

A Szolgáltató által az Aláíró részére generált kulcspár tulajdonosa és teljes jogú használója az Aláíró, tekintet nélkül arra a fizikai közegre, amely tárolja és védi a kulcsokat.

Szolgáltató kizárólagos tulajdonát képezik a szabályzatai, szerződéses feltételei és egyéb, a Szolgáltatások internetes honlapján közzétett dokumentumai. Ezen dokumentumok felhasználása csak és kizárólag a Szolgáltatások használatával összefüggésben engedélyezett, minden egyéb kereskedelmi vagy egyéb célú felhasználása szigorúan tilos.

9.6 Tevékenységért viselt felelősség és helytállás

9.6.1 Szolgáltató felelőssége és helytállása

A Szolgáltató felel a bizalmi szolgáltatási rendben és jelen szolgáltatási szabályzatban, valamint az Aláíróval az ÁSZF elfogadásával létrejött Szolgáltatási Szerződésben megfogalmazott valamennyi kötelezettség maradéktalan betartásáért, még akkor is, ha a Szolgáltatások nyújtásához kapcsolódó egyes feladatokat a Közreműködő Felek vagy egyéb alvállalkozók végzik.

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 jelen szolgáltatási szabályzatban, valamint az Aláíróval az ÁSZF elfogadásával létrejött Szolgáltatási Szerződésben előírtakat, vagy a {J1} eIDAS szerinti, rá vonatkozó kötelezettségeket. E kötelezettségek megtartását kétség esetén Szolgáltatónak kell bizonyítania. Szolgáltató sajátjaként felel a Közreműködő Felek vagy egyéb alvállalkozók által a Szolgáltatások nyújtása során okozott kárért.

A Szolgáltató a felelősségi körén belül keletkezett, bizonyított károkért, az Aláíróval, a {D1} ÁSZF-DÁP elfogadásával létrejött szerződéses viszonyban és a 9.8 fejezetben foglalt korlátozásokkal kártérítést fizet.

A Szolgáltató nem felel:

- az Aláírónak a Szolgáltató által tárolt magánkulcsa távoli aktiválásával kapcsolatos tevékenységért;
- az Érintett Felek tanúsítvány ellenőrzési és felhasználási tevékenységeiért;
- az Érintett Felek vagy mások által kibocsátott szabályzatokért.

Szolgáltató kötelezettsége

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

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

9.6.2 A regisztrációs szervezet felelőssége

Jelen bizalmi szolgáltatási szabályzat 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 és jelen szabályzatban leírt módon használni;
- a tárolt kulcshoz kapcsolódó egyéb szolgáltatásokat használni a jelen szabályzatban 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 tőle elvárható magatartás tanúsítása az elektronikus aláírás érvényesítésekor.

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

9.6.5 Egyéb felek felelőssége és helytállása

Nincs kikötés.

9.7 Helytállás érvénytelenségi köre

Szolgáltató kizárja felelősségét, amennyiben:

- az Érintett Fél nem körültekintően jár el az elektronikus aláírások ellenőrzése és felhasználásra során, azaz nem a mérvadó műszaki szabványoknak 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 mérvadó műszaki szabványoknak vagy a hatályos jogszabályoknak;
- 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.

9.8 Felelősség korlátozása

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

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

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

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

9.9 Kártérítések

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

9.10 Hatályosság és megszűnés

9.10.1 Hatályosság

Időbeli hatály

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

Tárgyi hatály

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

Személyi hatály

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

9.10.2 Megszűnés

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

9.10.3 Megszűnés után is hatályban maradó rendelkezések

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

9.11 Egyéni hirdetmények és kommunikáció a részvevőkkel

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

9.12 Módosítások

9.12.1 Módosítás eljárása

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

9.12.2 Értesítés módszere és időtartama

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

9.12.3 OID megváltozását előidéző körülmények

A szolgáltatási szabályzat OID-ja nem változik.

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

Bármely vitás kérdés felmerülése esetén Aláíró jogosult az esetleges bírósági eljárást megelőzően békéltető testülethez fordulni. Az illetékes békéltető testület megnevezését és elérhetőségeit jelen szabályzat 1.5.2 fejezete tartalmazza.

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

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 végzi.

9.16 Vegyes rendelkezések

9.16.1 Teljességi záradék

Nincs kikötés.

9.16.2 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.

9.16.3 Részleges érvénytelenség

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

9.16.4 Igényérvényesítés

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

9.16.5 Force Majeure (Vis maior)

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

voltak előre láthatóak.

A Szolgáltató nem felelős a vis maior esetekből fakadó károkért.

9.17 Egyéb rendelkezések

9.17.1 Hozzáférhetőség a fogyatékossággal élő személyek számára

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